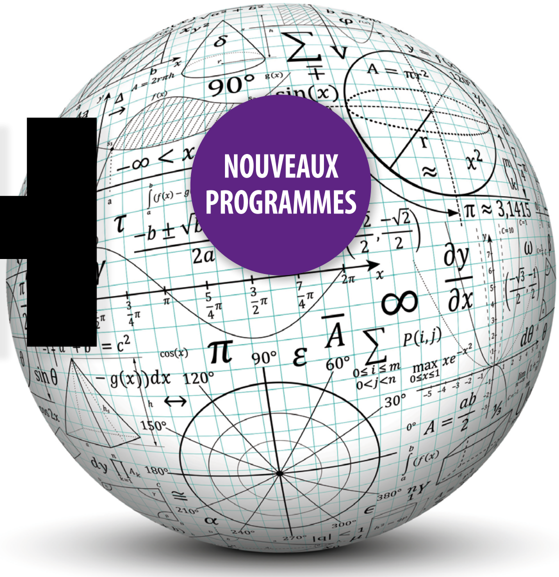
MATH MAX



NOUVEAUX PROGRAMMES

MATHS EXPERTES

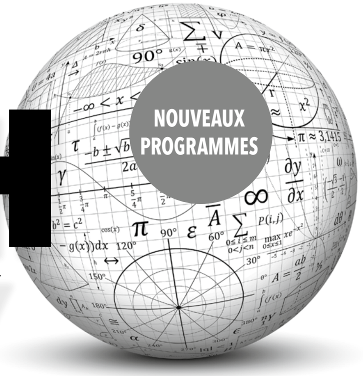
Cours complet
Exercices et devoirs corrigés

T^{le} option

- **Le cours complet** avec des exemples et des conseils
- **Des centaines d'exercices et devoirs, tous corrigés** en détail
- Des cahiers de **logique** et d'**algorithmique**
- Des extras pour réviser ou **anticiper sur les années à venir**
- Une approche **testée et validée auprès des élèves**

ellipses

MATH MAX

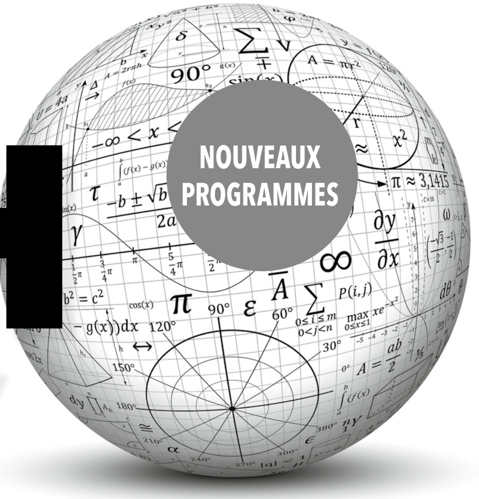


MATHS EXPERTES

Cours complet
Exercices et devoirs corrigés

T[le] option

MATH MAX



NOUVEAUX PROGRAMMES

MATHS EXPERTES

Cours complet
Exercices et devoirs corrigés

T$^{\text{le}}$ option

Sébastien Krief-Détraz

Professeur agrégé de mathématiques
au lycée international Georges Duby d'Aix-en-Provence

ellipses

Du même auteur, aux éditions Ellipses

Math Max – Terminale enseignement de spécialité – Cours complet, exercices et devoirs corrigés – Nouveaux programmes – 2e édition, 624 p., 2022

Math Max – Première enseignement de spécialité – Cours complet, exercices et devoirs corrigés – Nouveaux programmes – 2e édition, 396 p., 2021

Math Max – Seconde – Cours complet, exercices et devoirs corrigés – Nouveaux programmes – 2e édition, 390 p., 2021

ISBN 9782340-074651

8/10 rue la Quintinie 75015 Paris

www.editions-ellipses.fr

À mes parents

Pour mes élèves

AVANT-PROPOS

Vous avez entre les mains un ouvrage entièrement consacré aux mathématiques. Un de plus, direz-vous. Oui et non.

Pour commencer, il contient tout le cours, conforme aux nouveaux programmes comme il se doit, détaillé, avec les démonstrations, les figures, les remarques, les commentaires, les conseils et les exemples d'usage, rectifiés et peaufinés au fil des cours auprès d'élèves de tous horizons.

Puis des exercices, des exercices et des exercices, de difficulté croissante et en lien avec la progression du cours, bien évidemment.

Et tous les corrigés, bien entendu. Et rédigés de plus, pas de simples solutions laconiques.

Ajoutez à cela les devoirs de recherche et de synthèse, vous obtenez déjà un beau traité.

Insérez des cahiers d'algorithmique et de logique, vous aurez un esprit bien construit.

Agrémentez maintenant de quelques exercices en anglais, peu difficiles, vous avez enrichi votre langage.

Complétez d'une rubrique *Extras* dans laquelle on trouve des révisions, des aides, des compléments allant plus loin ou des problèmes ouverts, et de nouvelles perspectives s'ouvrent à vous.

Pimentez le tout d'énoncés un peu alambiqués, tirés par les cheveux ou complètement décalés, aux références regroupées dans une bibliographie quelque peu insolite et vous avez là l'ensemble idéal pour apprendre, réviser ou étudier avec plaisir.

Bonne lecture.

Sommaire

Cours &
Exercices corrigés

Chapitre I

NOMBRES COMPLEXES : ALGÈBRE

Sommaire

Introduction

Une démarche « naturelle »

L'équation $x+9=7$ n'a pas de solution dans $\mathbb{N}$, mais elle en a dans un ensemble plus grand : $\mathbb{Z}$ ($x=-2$). De même, l'équation $3x=1$ n'a pas de solution dans $\mathbb{Z}$, alors que dans un ensemble plus grand, $\mathbb{Q}$ par exemple, il y en a une : $x=\frac{1}{3}$. Et puis, l'équation $x^2=3$ n'a pas de solution dans $\mathbb{Q}$; il faut chercher dans l'ensemble des nombres réels $\mathbb{R}$ pour en trouver ($x=\pm\sqrt{3}$). Bref, quand une équation n'a pas de solution, une démarche naturelle (et historique) consiste à en chercher dans un ensemble plus grand.

Au stade de vos connaissances actuelles, l'ensemble numérique le plus grand que vous ayez rencontré est $\mathbb{R}$. Pourtant, l'équation $x^2 + 1 = 0$ n'a pas de solution dans $\mathbb{R}$... Nous allons donc dans ce chapitre « construire », ou plutôt imaginer, un ensemble plus grand que $\mathbb{R}$ dans lequel l'équation $x^2 + 1 = 0$ possède des solutions. On le nommera $\mathbb{C}$: ensemble des nombres complexes. Le principal élément de $\mathbb{C}$ sera noté $\boldsymbol{i}$ (comme imaginaire). Le nombre i est tel que $\boldsymbol{i^2 = -1}$ c.-à-d. “ $i = \sqrt{-1}$ ” ! L'équation ci-dessus possède alors deux solutions dans $\mathbb{C}$: $x^2 + 1 = 0 \iff x^2 - i^2 = 0 \iff (x - i)(x + i) = 0$ donc $x = i$ ou $x = -i$.

Bref historique

L'histoire des nombres complexes commence vers le milieu du XVI^e^ s. avec une première apparition dans l'œuvre de Jérôme Cardan d'une expression contenant la racine carrée d'un nombre négatif, nombre qu'il appelle *sophistiqué*. Le mathématicien italien Rafaele Bombelli met ensuite en place les règles de calcul sur ces quantités que l'on appelle alors *impossibles* avant de leur donner le nom d'*imaginaires*.

Durant trois siècles, ces nombres sont regardés avec méfiance, n'en étant pas vraiment mais permettant des raccourcis intéressants tant en algèbre que dans le tout nouveau calcul infinitésimal. Au XVIII^e^ s., Leonhard Euler introduit, après e, la notation i et établit la forme exponentielle d'un nombre complexe. Les mathématiciens tentent alors avec audace de généraliser les fonctions de la variable réelle à la variable imaginaire, tantôt avec succès (exponentielle complexe), tantôt avec plus d'aléas (fonction racine n-ième, fonction logarithme complexe). Ce n'est qu'à partir du XIX^e^ s. que se développe l'aspect géométrique des nombres complexes, vus comme des éléments ou des transformations du plan avec les travaux de Gauss et de Cauchy [†].

Utilité et légitimité des nombres complexes

Les nombres complexes permettent notamment de définir des solutions à toutes les équations polynomiales à coefficients réels. L'ensemble $\mathbb{C}$ est muni de l'application *module* qui généralise la valeur absolue des nombres réels, mais il ne peut pas être totalement ordonné de façon cohérente avec ses opérations, contrairement à $\mathbb{R}$.

En algèbre, le théorème de d'Alembert-Gauss identifie le degré d'un polynôme complexe non nul au nombre de ses racines complexes, comptées avec leur ordre de multiplicité.

En analyse, l'exponentielle complexe permet par exemple l'étude des séries et de la transformée de Fourier [††] qui est, entre autres, à la base de tout traitement de signal et donc de l'électronique. La branche de l'*analyse complexe* concerne l'étude des fonctions de variables complexes, dérivables au sens complexe, appelées fonctions holomorphes.

---

†. Fantastique mathématicien dont le nom est inscrit sur la non moins fantastique tour Eiffel.

††. Mémorable mathématicien dont le nom est inscrit sur la non moins mémorable tour Eiffel.

En géométrie, les nombres complexes permettent par exemple de décrire et étudier facilement les transformations du plan. Ils ouvrent aussi tout un pan de l'étude des fractales avec les fameux ensembles de Mandelbrot et de Julia.

En physique, les nombres complexes sont utilisés pour décrire le comportement d'oscillateurs électriques, les phénomènes ondulatoires en électromagnétisme, à peu près tout ce qui oscille.
Par ailleurs, la mécanique quantique nécessite l'utilisation des nombres complexes et selon certaines théories, la dimension *imaginaire* pourrait même correspondre à une réalité physique et ne pas être seulement une commodité d'écriture.

Leur utilité dans tous les domaines de l'algèbre et de l'analyse ainsi que l'utilisation qu'en font les physiciens, tant en optique qu'en électricité et électromagnétisme, en font des outils essentiels des sciences mathématiques et physiques.

1 Forme algébrique d'un nombre complexe

1.1 Premières définitions

Le théorème suivant, que l'on admettra, définit l'ensemble des nombres complexes.

Théorème 1 *Il existe un ensemble, noté $\mathbb{C}$, d'éléments, appelés nombres complexes, tel que :*

- *$\mathbb{C}$ contient l'ensemble $\mathbb{R}$ des nombres réels.*
- *$\mathbb{C}$ contient un élément i tel que* $\boldsymbol{i^2 = -1}$.
- *$\mathbb{C}$ est muni d'une addition et d'une multiplication qui suivent des **règles de calculs analogues** à celles de l'addition et de la multiplication dans $\mathbb{R}$.*
- *Tout nombre complexe z s'écrit de manière **unique** sous la forme* $\boldsymbol{z = a+ib}$ *où a et b sont deux nombres réels. Cette écriture s'appelle la **forme algébrique** du nombre complexe z.*

Définition 1 *Si* $z = a + ib \in \mathbb{C}$,

- *On appelle a, la **partie réelle** de z et l'on note* $a = \mathfrak{Re}(z)$.
- *On appelle b, la **partie imaginaire** de z et l'on note* $b = \mathfrak{Im}(z)$.
- *Si* $\mathfrak{Re}(z) = 0$, *on dit que* $z = ib$ *est **imaginaire pur** et l'on note* $z \in i\mathbb{R}$.

Exemples : $3 - 2i \in \mathbb{C}$, $\sqrt{5} + i\pi \in \mathbb{C}$, $7 \in \mathbb{R} \subset \mathbb{C}$, $\frac{i}{3} \in i\mathbb{R} \subset \mathbb{C}$.

Remarques : • On a $\mathbb{R} \subset \mathbb{C}$ et les réels sont précisément les nombres complexes de partie imaginaire nulle :

$$\mathbb{R} = \{z \in \mathbb{C} \;/\; \mathfrak{Im}(z) = 0\} = \{z = a + ib \in \mathbb{C} \;/\; b = 0\}.$$

• Deux nombres complexes sont égaux si, et seulement si, ils ont même partie réelle et même partie imaginaire : $a + ib = a' + ib' \iff a = a'$ et $b = b'$.

• En particulier, $z = 0\,(\in \mathbb{R}) \iff \mathfrak{Re}(z) = \mathfrak{Im}(z) = 0$.

1.2 Calculs dans $\mathbb{C}$

Commençons par tenter ce qui suit, pour voir :

◦ $(2+4i)+(5-7i)=(5+2)+(4i-7i)=7-3i$.

◦ $(3-2i)(4+5i)=12+15i-8i-2i.5i=12-10i^2+7i=12-10(-1)+7i=22+7i$.

◦ $\frac{1}{3+2i}=\frac{1}{3+2i}\times\frac{3-2i}{3-2i}=\frac{3-2i}{3^2-(2i)^2}=\frac{3-2i}{9-4i^2}=\frac{3-2i}{9+4}=\frac{3}{13}-\frac{2}{13}\,i$

Le théorème 1 justifie les règles de calcul suivantes.

Propriété 1 *Pour tous nombres complexes* $z=a+ib$ *et* $z'=a'+ib'$,

- $\boldsymbol{z+z'}=(a+ib)+(a'+ib')=\boldsymbol{(a+a')+i(b+b')}$.
- $\boldsymbol{zz'}=(a+ib)(a'+ib')=aa'+iab'+ia'b+i^2bb'=\boldsymbol{(aa'-bb')+i(a'b+ab')}$.
- *Si* $z\neq 0$, $\quad\boldsymbol{\frac{1}{z}}=\frac{1}{a+ib}\times\frac{a-ib}{a-ib}=\frac{a-ib}{a^2-(ib)^2}=\boldsymbol{\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2}}$
- *Si* $z\neq 0$, $\quad\boldsymbol{\frac{z'}{z}=z'\times\frac{1}{z}}$.

Définition 2 *L'**opposé** d'un nombre complexe* $z=a+ib$ *est le nombre complexe* $-z=-a-ib$.

Remarque : Si $\lambda\in\mathbb{R}$, $\lambda z=\lambda a+i\lambda b$ *i.e.* $\mathfrak{Re}(\lambda z)=\lambda\mathfrak{Re}(z)$ et $\mathfrak{Im}(\lambda z)=\lambda\mathfrak{Im}(z)$.

Exemples : ◦ $(3-5i)+(-2+3i)=1-2i$.

◦ $(8-i)+(-8+i)=(8-i)-(8-i)=0$.

◦ $(3+2i)(1-i)=3-3i+2i-2i^2=3-2(-1)-i=5-i$.

◦ $\frac{1}{7-3i}=\frac{1}{7-3i}\times\frac{7+3i}{7+3i}=\frac{7+3i}{7^2-(3i^2)}=\frac{7+3i}{49+9}=\frac{7}{58}+i\,\frac{3}{58}$.

◦ $\frac{3-4i}{5+2i}=\frac{3-4i}{5+2i}\times\frac{5-2i}{5-2i}=\frac{15-6i-20i+8i^2}{5^2-(2i)^2}=\frac{15-8-26i}{25-(-4)}=\frac{7}{29}-\frac{26}{29}\,i$.

◦ $\boldsymbol{\frac{1}{i}}=\frac{i}{i.i}=\frac{i}{-1}=\boldsymbol{-i}$.

Propriété 2 $\forall z,z'\in\mathbb{C}\qquad\boldsymbol{zz'=0}\iff\boldsymbol{z=0}$ *ou* $\boldsymbol{z'=0}$.

Démonstration : · Si $z=0$ alors $a=b=0$ donc $aa'-bb'=0$ et $a'b+ab'=0$ d'où $zz'=0$. De même si $z'=0$.

· Si $zz'=0$ alors $aa'-bb'=0$ et $a'b+ab'=0$.

Supposons $z\neq 0$. Si $a\neq 0$, on a $a'=\frac{bb'}{a}$ et $\frac{bb'}{a}\times b+ab'=0$ donc $b'(\frac{b^2}{a}+a)=0\implies b'(a^2+b^2)=0\implies b'=0\ (z\neq 0)$ d'où $a'=\frac{bb'}{a}=0$ et $z'=0$.

Si $a=0$, $b\neq 0$ et il suffit d'écrire $b'=\frac{aa'}{b}$. □

Les propriétés d'associativité, de commutativité et de distributivité de l'addition et de la multiplication des nombres complexes sont encore vérifiées. Il en résulte les identités remarquables suivantes.

- $(a+ib)^2=(a^2-b^2)+i(2ab)$
- $(a-ib)^2=(a^2-b^2)-i(2ab)$
- $\boldsymbol{(a+ib)(a-ib)=a^2+b^2}$ $(\in\mathbb{R}^+)$

Exemples : ◦ $(4+3i)^2 = 4^2 - 3^2 + 2\times 4\times 3i = 7+24i$.
◦ $(7-i)^2 = 7^2 - 1^2 - 2\times 7\times 1 = 48 - 14i$.
◦ $(8-2i)(2i+8) = 8^2 + 2^2 = 68$.

Le mode complexe de la calculatrice (mode, $a+ib$) peut vous permettre de vérifier vos résultats.

2 Conjugué d'un nombre complexe

2.1 Définition

Définition 3 *Le **conjugué** d'un nombre complexe* $z = a+ib$ *est le nombre complexe* $\boldsymbol{\overline{z} = a - ib}$.

Exemples : ◦ $\overline{3+2i} = 3-2i$ ◦ $\overline{5-6i} = 5+6i$, ◦ $\overline{-4+i} = -4-i$,
◦ $\overline{-7i-\sqrt{3}} = 7i - \sqrt{3}$, ◦ $\overline{i\sqrt{2}} = -i\sqrt{2}$, ◦ $\overline{\pi} = \pi$.

Les propriétés suivantes découlent immédiatement de la définition du conjugué.

Propriété 3 $\boldsymbol{z+\overline{z} = 2\,\mathfrak{Re}(z)}$ *et* $\boldsymbol{z-\overline{z} = 2\,i\,\mathfrak{Im}(z)}$
Ainsi, z *est réel* $\iff z = \overline{z}$ *et* z *est imaginaire pur* $\iff z = -\overline{z}$.

Propriété 4 *Pour tout* $z = a+ib \in \mathbb{C}$, $\boldsymbol{z\overline{z} = a^2+b^2}$ *et* $\boldsymbol{\overline{\overline{z}} = z}$.

Exemples : ◦ $(3+2i)\overline{(3+2i)} = 3^2+2^2 = 13$, ◦ $i\sqrt{2}\,\overline{i\sqrt{2}} = \sqrt{2}^2 = 2$,
◦ $(-7i-\sqrt{3})\overline{(-7i-\sqrt{3})} = \sqrt{3}^2 + 7^2 = 52$, ◦ $i\overline{i} = -i^2 = 1$.

Remarque : Ainsi, pour tout $z\in\mathbb{C}$, $z\overline{z}\in\mathbb{R}^+$ et même $z\overline{z} > 0$ pour $z\neq 0$.
On serait presque tenté de définir une fonction $\ln(z\overline{z})$ sur $\mathbb{C}^*$.

2.2 Conjugué et opérations

Propriété 5 *Pour tous nombres complexes* z *et* z' *et tout entier naturel* n *non nul, on a :* $\boldsymbol{\overline{z+z'} = \overline{z}+\overline{z'}}$, $\boldsymbol{\overline{zz'} = \overline{z}\times\overline{z'}}$, $\boldsymbol{\overline{z^n} = (\overline{z})^n}$.

Si, de plus, $z\neq 0$, $\boldsymbol{\overline{\left(\dfrac{1}{z}\right)} = \dfrac{1}{\overline{z}}}$ *et* $\boldsymbol{\overline{\left(\dfrac{z'}{z}\right)} = \dfrac{\overline{z'}}{\overline{z}}}$

Démonstration : Soient $z = a+ib$ et $z' = a'+ib'$. On a
· $\overline{z+z'} = \overline{(a+a')+i(b+b')} = (a+a')-i(b+b') = (a-ib)+(a'-ib') = \overline{z}+\overline{z'}$
· $zz' = [aa'-bb'] + i[a'b+ab']$
et $\overline{z}\times\overline{z'} = [aa'-(-b)(-b')] + i[a'(-b)+a(-b')] = [aa'-bb'] - i[a'b+ab'] = \overline{zz'}$.
· $\frac{1}{z} = \frac{1}{a+ib}\times\frac{a-ib}{a-ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ et $\frac{1}{(\overline{z})} = \frac{1}{a-ib}\times\frac{a+ib}{a+ib} = \frac{a}{a^2+b^2} + i\frac{b}{a^2+b^2} = \overline{\left(\frac{1}{z}\right)}$
· $\overline{z^n} = \overline{z\times z^{n-1}} = \overline{z}\times\overline{z^{n-1}}$ et une simple récurrence donne le résultat. □

Exemple : $\overline{z+i(\overline{z}-1)} = \overline{z} + \overline{i(\overline{z}-1)} = \overline{z} + \overline{i}\,\overline{\overline{z}-1} = \overline{z} - i(\overline{\overline{z}} - \overline{1}) = \overline{z} - i(z-1)$.

Exercices

Nombres complexes : algèbre

Exercice 1 Donner la forme algébrique des nombres complexes suivants.

(a) $(-i)^2$
(b) $(2i)^2$
(c) i^3
(d) $3i(4+5i)$
(e) $(3+i)(4-2i)$
(f) $(6-i)^2$
(g) $(2+i\sqrt{3})(2-i\sqrt{3})$
(h) $(\sqrt{2}+2i)^4$
(i) $(1+i)(4-3i)(1-i)$
(j) $-i(2+3i)(1-i)(-3+2i)$
(k) $\dfrac{2}{1+i}$
(l) $\dfrac{4i}{2-3i}$
(m) $\dfrac{2-5i}{3+2i}$
(n) $\dfrac{2i-\sqrt{2}}{3+i}$
(o) $\dfrac{2}{1-2i}+\dfrac{3}{2+i}$

Exercice 2 Donner une forme algébrique du conjugué des nombres complexes suivants.

(a) $2+5i$
(b) $i-\sqrt{2}$
(c) $\dfrac{2-i}{2i+1}$
(d) $(3-2i)(i+1)$
(e) $\frac{3}{2}i(1+\frac{1}{2}i)-\frac{1}{2}(2i+1)$

Exercice 3 On note $z_1=\dfrac{2i+1}{i+2}$ et $z_2=\dfrac{1-2i}{2-i}$.

1. Sans calcul, justifier que z_1+z_2 est réel et que z_1-z_2 est imaginaire pur.
2. Retrouver ces résultats par le calcul.

Exercice 4 Écrire en fonction de $\overline{z}$ le conjugué des nombres complexes suivants.

(a) $-2i+3z$
(b) $3+i-2iz$
(c) $(2-iz)(2z-4+3i)$
(d) $\dfrac{2i+1-iz}{5i+2z}$

Exercice 5 Soit $z\in\mathbb{C}^*$. Les nombres suivants appartiennent-ils à $\mathbb{R}$, à $i\mathbb{R}$ ou à aucun des deux ?

$a= z+\overline{z}$
$b= z-\overline{z}$
$c= z^2+\overline{z}^2$
$d= z^2-\overline{z}^2$
$e= z^3-\overline{z}^3$
$f= \frac{z+\overline{z}}{z-\overline{z}}$ $(z\notin\mathbb{R})$
$g= \frac{z-\overline{z}}{z+\overline{z}}$ $(z\notin i\mathbb{R})$
$h= \frac{1}{z}+\frac{1}{\overline{z}}$
$j= \frac{1}{z}-\frac{1}{\overline{z}}$
$k= \frac{z^2+\overline{z}^2}{z\overline{z}}$
$l= \frac{z^2-\overline{z}^2}{z\overline{z}}$

Exercice 6 Ordre dans $\mathbb{C}$
Supposons que l'on puisse comparer deux nombres complexes de la même manière qu'avec deux réels. Qui serait le plus grand, i ou 0 ? Montrer qu'aucun cas de figure n'est possible sachant que $-1 < 1$.

Exercice 7 Résoudre dans $\mathbb{C}$ les équations d'inconnue z suivantes.

(a) $iz = 3 + i$

(b) $(2 - i)z - 2i = iz + 2 - 3i$

(c) $\dfrac{z - 2i}{z + 2} = 4i$

(d) $4\overline{z} + 2i - 4 = 0$

(e) $2z + i\overline{z} = 4$

(f) $\dfrac{\overline{z} + i}{\overline{z} - i} = 1$

(g) $\dfrac{\overline{z} + i}{z - i} = 1$

Exercice 8 Résoudre dans $\mathbb{C}$ les systèmes d'équations suivants.

(a) $\begin{cases} 3z + z' &= 2 - 5i \\ z - z' &= -2 + i \end{cases}$

(b) $\begin{cases} 3z + z' &= 5 + 2i \\ -z + z' &= 1 - 2i \end{cases}$

(c) $\begin{cases} z - z' &= 3 - 4i \\ \overline{z} + 2\overline{z'} &= 8 - i \end{cases}$

(d) $\begin{cases} \frac{1}{2}z + z' &= 2 \\ \frac{1}{2}\overline{z} + i\,\overline{z'} &= 0 \end{cases}$

Précipitez-vous en page 275 afin de réaliser le devoir n° 1.

Corrigé des exercices

NOMBRES COMPLEXES : ALGÈBRE

Exercice 1 Forme algébrique.

(a) $(-i)^2 = i^2 = -1$

(b) $(2i)^2 = 2^2 i^2 = -4$

(c) $i^3 = i^2 i = -i$

(d) $3i(4+5i) = -15+12i$

(e) $(3+i)(4-2i) = 3\times 4 - 3\times 2i + 4i - 2i^2 = 14-2i$

(f) $(6-i)^2 = 6^2 + i^2 - 2\times 6i = 35 - 12i$

(g) $(2+i\sqrt{3})(2-i\sqrt{3}) = 2^2 + \sqrt{3}^2 = 7$

(h) $(\sqrt{2}+2i)^4 = [(\sqrt{2}+2i)^2]^2 = [\sqrt{2}^2 + 2\sqrt{2}\times 2i + (2i)^2]^2 = [2-4+4i\sqrt{2}]^2$
$= (-2)^2 - 2\times 2\times 4i\sqrt{2} - (4\sqrt{2})^2 = 4 - 32 - 16i\sqrt{2} = -28 - 16i\sqrt{2}$

(i) $(1+i)(4-3i)(1-i) = (4-3i)(1-i^2) = 8-6i$

(j) $-i(2+3i)(1-i)(-3+2i) = -i(1-i)(-6+4i-9i-6) = -i(-12-5i+12i-5)$
$= -7i^2 - 17(-i) = 7+17i$

(k) $\frac{2}{1+i} = \frac{2(1-i)}{(1+i)(1-i)} = \frac{2}{1+1}(1-i) = 1-i$

(l) $\frac{4i}{2-3i} = \frac{4i(2+3i)}{(2-3i)(2+3i)} = \frac{8i+12i^2}{2^2+3^2} = -\frac{12}{13} + \frac{8}{13}i$

(m) $\frac{2-5i}{3+2i} = \frac{2-5i}{3+2i}.\frac{3-2i}{3-2i} = \frac{1}{13}(-4-19i)$

(n) $\frac{2i-\sqrt{2}}{3+i} = \frac{(2i-\sqrt{2})(3-i)}{(3+i)(3-i)} = \frac{6i-2i^2-3\sqrt{2}+i\sqrt{2}}{3^2-i^2} = \frac{2-3\sqrt{2}}{10} + \frac{6+\sqrt{2}}{10}i$

(o) $\frac{2}{1-2i} + \frac{3}{2+i} = \frac{2(1+2i)}{1^2+2^2} + \frac{3(2-i)}{2^2+1^2} = \frac{2+4i+6-3i}{5} = \frac{1}{5}(8+i)$

Exercice 2 Forme algébrique du conjugué.

(a) $\overline{2+5i} = 2-5i$

(b) $\overline{i-\sqrt{2}} = -\sqrt{2} - i$

(c) $\overline{\left(\frac{2-i}{2i+1}\right)} = i$

(d) $\overline{(3-2i)(i+1)} = 5-i$

(e) $\overline{\frac{3}{2}i(1+\frac{1}{2}i) - \frac{1}{2}(2i+1)} = -\frac{5}{4} - \frac{1}{2}i$

Exercice 3 $z_1 = \frac{2i+1}{i+2}$ et $z_2 = \frac{1-2i}{2-i}$.

1. $\overline{z_1} = \overline{\left(\frac{2i+1}{i+2}\right)} = \frac{\overline{2i+1}}{\overline{i+2}} = \frac{1-2i}{2-i} = z_2$ donc $z_1 + z_2 = z_1 + \overline{z_1} \in \mathbb{R}$ et $z_1 - z_2 = z_1 - \overline{z_1} \in i\mathbb{R}$

2. On a $z_1 \pm z_2 = \frac{2i+1}{i+2} \pm \frac{1-2i}{2-i} = \frac{(2i+1)(2-i)\pm(1-2i)(i+2)}{(i+2)(2-i)} = \frac{(4i+2+2-i)\pm(i+2+2-4i)}{2^2-i^2}$.
Ainsi, $z_1 + z_2 = \frac{(4+3i)+(4-3i)}{5} = \frac{8}{5}$ et $z_1 - z_2 = \frac{(4+3i)-(4-3i)}{5} = \frac{6}{5}i$.

Exercice 4 Conjugué des nombres complexes en fonction de $\overline{z}$.

(a) $\overline{-2i+3z} = 3\overline{z}+2i$

(b) $\overline{3+i-2iz} = 3-i+2i\overline{z}$

(c) $\overline{(2-iz)(2z-4+3i)} = (2+i\overline{z})(2\overline{z}-4-3i)$

(d) $\overline{\left(\frac{2i+1-iz}{5i+2z}\right)} = \frac{1-2i+i\overline{z}}{2\overline{z}-5i}$

Exercice 5 Soit $z = \alpha + i\beta \in \mathbb{C}^*$.

$a = z+\overline{z} = 2\alpha \in \mathbb{R}$

$b = z-\overline{z} = 2i\beta \in i\mathbb{R}$

$c = z^2+\overline{z}^2 = 2(\alpha^2-\beta^2) = 2\mathfrak{Re}(z^2) \in \mathbb{R}$

$d = z^2-\overline{z}^2 = 4i(\alpha^2-\beta^2) = 2\mathfrak{Re}(z).2i\mathfrak{Im}(z)$ ou encore $d = 2i\mathfrak{Im}(z^2) \in i\mathbb{R}$

$e = z^3-\overline{z}^3 = z^3-\overline{z^3} = 2i\mathfrak{Im}(z^3) \in i\mathbb{R}$

$f = \frac{z+\overline{z}}{z-\overline{z}} = \frac{2\alpha}{2i\beta} = -\frac{\alpha}{\beta}i \in i\mathbb{R} \ \ (z \notin \mathbb{R})$

$g = \frac{z-\overline{z}}{z+\overline{z}} = \frac{1}{f} = \frac{\beta}{\alpha}i \in i\mathbb{R} \ \ (z \notin i\mathbb{R})$

$h = \frac{1}{z}+\frac{1}{\overline{z}} = \frac{1}{z}+\overline{\frac{1}{z}} = 2\mathfrak{Re}(\frac{1}{z}) \in \mathbb{R}$

$j = \frac{1}{z}-\frac{1}{\overline{z}} = \frac{1}{z}-\overline{\frac{1}{z}} = 2i\mathfrak{Im}(\frac{1}{z}) \in i\mathbb{R}$

$k = \frac{z^2+\overline{z}^2}{z\overline{z}} = \frac{z}{\overline{z}}+\frac{\overline{z}}{z} = \frac{z}{\overline{z}}+\overline{\frac{z}{\overline{z}}} = 2\mathfrak{Re}(\frac{z}{\overline{z}}) \in \mathbb{R}$

$l = \frac{z^2-\overline{z}^2}{z\overline{z}} = \frac{z}{\overline{z}}-\frac{\overline{z}}{z} = \frac{z}{\overline{z}}-\overline{\frac{z}{\overline{z}}} = 2i\mathfrak{Im}(\frac{z}{\overline{z}}) \in i\mathbb{R}$

Exercice 6 Ordre dans $\mathbb{C}$

Supposons $i > 0$. On aurait alors $-1 < 1 \overset{\times i>0}{\Longrightarrow} -i < i \overset{\times i>0}{\Longrightarrow} -i^2 < i^2$ c.-à-d. $1 < -1$.
En supposant que $i < 0$, on aurait $-1 < 1 \overset{\times i<0}{\Longrightarrow} -i > i \overset{\times i<0}{\Longrightarrow} -i^2 < i^2$ c.-à-d. $1 < -1$.
Comme $i \neq 0$, on ne peut le comparer à 0 de manière cohérente avec les opérations usuelles.

Exercice 7 Résolution dans $\mathbb{C}$.

(a) $iz = 3+i \iff z = -i(3+i) = 1-3i$

(b) $(2-i)z-2i = iz+2-3i \iff (2-i-i)z = 2-3i+2i \iff z = \frac{2-i}{2-2i} = \frac{1}{4}(3+i)$

(c) $\frac{z-2i}{z+2} = 4i \overset{z\neq -2}{\iff} z-2i = 4iz+8i \iff z = \frac{8i+2i}{1-4i} = \frac{1}{17}(-40+10i) \quad (\neq -2)$.

(d) $4\overline{z}+2i-4 = 0 \iff z = \overline{\overline{z}} = \frac{1}{4}\,\overline{4-2i} = 1+\frac{1}{2}i$

(e) $2z+i\overline{z} = 4 \iff 2a+b = 4$ et $2b+a = 0$
$\overset{2(L1)-(L2)}{\iff} 3a = 8$ et $b = 4-2a \iff z = \frac{8}{3}-\frac{4}{3}i$

(f) $\frac{\overline{z}+i}{\overline{z}-i} = 1 \overset{z\neq -i}{\iff} \overline{z}+i = \overline{z}-i \iff i = -i$: Aucune solution.

(g) $\frac{\overline{z}+i}{z-i} = 1 \overset{z\neq i}{\iff} \overline{z}+i = z-i \iff z-\overline{z} = 2i \iff \mathfrak{Im}(z) = 1$ (et $z \neq i$)
$\iff z = a+i$ pour $a \in \mathbb{R}^*$.

Exercice 8 Systèmes dans $\mathbb{C}$.

(a) $\left\{\begin{array}{lll} 3z+z' & = & 2-5i \\ z-z' & = & -2+i \end{array}\right. \overset{(L1)+(L2)}{\Longrightarrow} 4z = 2-5i-2+i = -4i$

$\Longrightarrow z=-i$ et $z' = 2-5i-3z = 2-2i$

(b) $\left\{\begin{array}{lll} 3z+z' & = & 5+2i \\ -z+z' & = & 1-2i \end{array}\right. \overset{(L1)-(L2)}{\Longrightarrow} 4z = 5+2i-1+2i = 4+4i$

$\Longrightarrow z = 1+i$ et $z' = 1-2i+z = 2-i$

(c) $\left\{\begin{array}{lll} z-z' & = & 3-4i \\ \overline{z}+2\overline{z'} & = & 8-i \end{array}\right. \overset{\overline{(L2)}}{\Longrightarrow} \left\{\begin{array}{lll} z-z' & = & 3-4i \\ z+2z' & = & 8+i \end{array}\right.$

$\overset{(L2)-(L1)}{\Longrightarrow} 3z' = 8+i-3+4i \Longrightarrow z' = \frac{5}{3}(1+i)$ et $z = z'+3-4i = \frac{14-7i}{3}$

(d) $\left\{\begin{array}{lll} \frac{1}{2}z+z' & = & 2 \\ \frac{1}{2}\overline{z}+i\,\overline{z'} & = & 0 \end{array}\right. \overset{\overline{(L2)}}{\Longrightarrow} \left\{\begin{array}{lll} \frac{1}{2}z+z' & = & 2 \\ \frac{1}{2}z-iz' & = & 0 \end{array}\right. \overset{(L1)-(L2)}{\Longrightarrow} (1+i)z' = 2$

$\Longrightarrow z' = \frac{2}{1+i} = 1-i$ et $z = 2(2-z') = 2(1+i)$

Chapitre II

DIVISIBILITÉ DANS $\mathbb{Z}$

Sommaire

Introduction

L'arithmétique, du grec ancien *arithmos* (nombre), est le domaine des mathématiques qui explore la science des nombres. On y étudie les entiers, ou les rationnels, et les propriétés des opérations traditionnelles qui sont l'addition, la soustraction, la multiplication et la division. L'origine de l'arithmétique semble être une invention phénicienne. Dans l'école pythagoricienne, au VI^{e} s. av. J.-C., l'arithmétique était, avec la géométrie, l'astronomie et la musique, une des quatre sciences quantitatives ou mathématiques. Les mathématiciens indiens, au VI^{e} s., puis islamiques, au X^{e} s., apportent de grandes avancées, en particulier dans la résolution des équations diophantiennes, à coefficients entiers (de Diophante, II^{e} s.) et dans l'étude de nombres entiers particuliers. Après l'introduction en Europe des chiffres arabes la fin du X^{e} s. et l'invention de l'écriture fractionnaire, l'arithmétique a reçu, parallèlement avec l'algèbre, de grands développements au point de vue théorique au cours des siècles qui suivirent. Citons le fameux théorème de Fermat (XVII^{e} s.) affirmant que l'équation $a^n + b^n = c^n$ n'admet de solutions entières que pour $n \leqslant 2$ et qui n'a été démontré qu'à la toute fin du XX^{e} s. L'histoire de la théorie des nombres fourmille de théorèmes aux énoncés simples mais aux preuves difficiles, ainsi que de conjectures de formulation élémentaire mais non résolues. Des questions issues de l'arithmétique, apparemment gratuites, ont donné lieu à des applications spectaculaires en cryptographie ou en codage. L'arithmétique reste une science où de nombreuses conjectures ne sont pas démontrées, ni même supputées, ce qui est très aguichant pour de futurs chercheurs tels que vous, non ? De plus, vous savez bien qu'il existe trois sortes d'individus : ceux qui savent compter, et les autres.

$\mathbb{N}$ désigne l'ensemble des entiers naturels, $\mathbb{Z}$ celui des entiers relatifs et $[\![m\,; n]\!]$ est l'ensemble des entiers compris entre les entiers m et n.

1 Divisibilité dans $\mathbb{Z}$

Définition 1 *Soient a et b deux entiers relatifs.*
On dit que b divise a lorsqu'il existe un entier relatif k tel que $a = kb$.
On dit alors que b est un diviseur de a, que a est un multiple de b, que a est divisible par b et l'on note $b\,|\,a$.

Exemples : $-5\,|\,2020$; $2\,|\,476$; $4\not|\,57$; $3\,|\,657$; $3\not|\,653$; $-9\,|-4536$; $9\not|\,281$; $17\,|\,0$; $0\not|\,3$; $1\,|\,329$; $0\,|\,0$.

Remarques :
- Tout entier est un diviseur de 0 mais ce dernier ne divise que lui-même.
- Tout entier est un multiple de 1 et de lui-même.
- Si $b \neq 0$, on a $b\,|\,a \iff \frac{a}{b} \in \mathbb{Z}$.
- On notera $b\mathbb{Z}$ l'ensemble de tous les multiples de b et $D(a)$ l'ensemble de tous les diviseurs de a.

Par exemple, $7\mathbb{Z} = \{\,\dots; -14; -7 : 0; 7; 14 : \dots\,\}$
et $D(4) = \{-4; -2; -1; 1; 2; 4\}$.

Propriété 1 *Soit un entier b un diviseur d'un entier non nul a.*
Tout diviseur de b est un diviseur de a : si $c\,|\,b$ et $b\,|\,a$, alors $c\,|\,a$,
$b\,|\,a \Longrightarrow D(b) \subset D(a)$
Tout multiple de a est un multiple de b : si $c = ka$ et $a = k'b$, alors $c = k''b$.
$a = kb \Longrightarrow a\mathbb{Z} \subset b\mathbb{Z}$

Démonstration : Si $b\,|\,a$ et $c\,|\,b$, il existe k et $k' \in \mathbb{Z}$ tels que $a = kb$ et $b = k'c$ donc $a = (kk')c$.
Si $d \in a\mathbb{Z}$, il existe n tel que $d = na = n(kb) = (nk)b \in b\mathbb{Z}$. □

Exemples : ◦ Les diviseurs de 6 sont aussi des diviseurs de 12 car $6\,|\,12$:
$D(6) = \{-6; -3; -2; -1; 1; 2; 3; 6\} \subset D(12) = \{\pm1; \pm2; \pm3; \pm4; \pm6; \pm12\}$.
◦ Les multiples de 24 sont aussi des multiples de 8 car $8\,|\,24$: $24\mathbb{Z} \subset 8\mathbb{Z}$.

Propriété 2 *Soient a et b deux entiers relatifs.*
On a $a\,|\,b \iff -a\,|\,b \iff a\,|-b \iff -a\,|-b$.

Autrement dit, b et $-b$ ont les mêmes diviseurs et si a est un diviseur de b alors son opposé $-a$ aussi. On se restreindra donc souvent à la recherche et à l'étude des diviseurs dans $\mathbb{N}$.

Démonstration : $a|b \Longrightarrow \exists k \in \mathbb{Z}, \quad b = ka \Longrightarrow b = (-k)(-a)$ et $-a|b$.
Les autres sont similaires. ☐

Propriété 3 *Soient m et n deux entiers relatifs tels que $n \neq 0$.*
- *Si $m|n$, alors $|m| \leqslant |n|$.*
- *Tout diviseur d'un entier relatif non nul n est compris entre $-|n|$ et $|n|$.*
- *Un entier relatif non nul a donc un nombre fini de diviseurs.*

Démonstration : $n = km \Longrightarrow |n| = |k|\,|m| \overset{|k|\geqslant 1}{\Longrightarrow} |m| \leqslant |n| \Longrightarrow -|n| \leqslant m \leqslant |n|$ et $[\![-|n|\,;|n|]\!]$ est fini. ☐

<u>Remarque</u> : En revanche, le nombre de multiples d'un entier non nul est infini.

Théorème 1 *Soient a, b et c trois entiers relatifs tels que $a \neq 0$.*
Si a divise b et c, alors a divise toute combinaison linéaire entière de b et c :
$a|b$ *et* $a|c \Longrightarrow \forall u, v \in \mathbb{Z},\ a|(bu + cv)$.

Démonstration : Soit $a \neq 0$ tel que $a|b$ et $a|c$ et soient u et $v \in \mathbb{Z}$. Il existe k et $k' \in \mathbb{Z}$ tels que $b = ka$ et $c = k'a$ donc $bu + cv = kau + k'av = (ku + k'v)a \in a\mathbb{Z}$. ☐

<u>Remarque</u> : On a toujours $a|a$ donc si $a|b$, $a|(a + b)$ et $a|(a - b)$.

Exemple : Si p divise deux entiers consécutifs n et $n + 1$,
alors p divise $1 \times (n + 1) + (-1) \times n = 1$ et $p = \pm 1$.

2 Division euclidienne

Théorème 2 *Soient a un entier relatif et b un entier naturel non nul.*
Il existe un unique couple d'entiers $(q\,,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leqslant r < b$.
Cette relation est la division euclidienne de a par b, q en est le quotient et r le reste.
a s'appelle de dividende et b le diviseur de cette division euclidienne.

Démonstration : L'idée est d'encadrer a par deux multiples consécutifs de b.
On définit la partie entière $Ent(x)$ d'un nombre réel x par le plus grand entier inférieur ou égal à x : $Ent(x) \in \mathbb{Z}$ et $Ent(x) \leqslant x < Ent(x) + 1$.
Par exemple, $Ent(5,7) = 5$, $Ent(2) = 2$, $Ent(0) = 0$, $Ent(-3) = -3$, et $Ent(-4,6) = -5$.
- Existence : Posons $q = Ent(\frac{a}{b})$.

On a $q \leqslant \frac{a}{b} < q + 1 \overset{b\geqslant 1}{\Longrightarrow} bq \leqslant b\frac{a}{b} = a < b(q + 1) = bq + b$
$\overset{-bq}{\Longrightarrow} bq - bq = 0 \leqslant a - bq < bq + b - bq = b$.
Si l'on pose $r = a - bq$, on a bien $a = bq + r$ et $0 \leqslant r < b$: l'existence est assurée.

• Unicité : Supposons que $(q\,,\,r)$ et $(q'\,,\,r')$ vérifient les conditions.
On a $a = bq + r = bq' + r' \implies b(q - q') = r' - r$ donc $b\,|\,(r' - r)$. Or $0 \leqslant r < b$ donc $-b < -r \leqslant 0$ et $-b < r' - r < b$. On sait d'après la propriété 3 que si $r' - r \neq 0$, tout diviseur de $(r' - r)$ est compris entre $-|r' - r|$ et $|r' - r|$ ce qui ne peut être le cas de b donc $r' - r = 0$ et $r' = r$. Alors $q - q' = \frac{r'-r}{b} = 0$ et $q = q'$. Le couple $(q\,,\,r)$ est donc bien unique. □

Exemples : ◦ La division euclidienne de 123 par 24 est $123 = 5 \times 24 + 3$: $q = 5$ et $0 \leqslant r = 3 < 24$.
◦ La division euclidienne de 51 par 17 est $51 = 3 \times 17 + 0$: $q = 3$ et $0 \leqslant r = 0 < 17$.
◦ La division euclidienne de -38 par 6 est $-38 = -7 \times 6 + 4$: $q = -7$ et $0 \leqslant r = 4 < 6$.

Remarques : • Le reste d'une division euclidienne est aussi appelé *résidu*.
• Dans la division euclidienne de a par b, il y a b restes possibles : $0, 1, \ldots, b - 1$.
• Si $b = 1$, la division euclidienne est toujours triviale : $a = 1 \times a + 0$ avec $q = a$ et $r = 0$.
• Il y a une infinité d'écritures de la forme $a = bq + r$ mais une seule vérifie $0 \leqslant r < b$.
Par exemple, $50 = 8 \times 5 + 10 = 8 \times 7 - 6$ mais seule l'écriture $50 = 8 \times 6 + 2$ est la division euclidienne de 50 par 8.

Les résultats suivants sont évidents, il découlent de l'unicité du reste, mais ils sont bien utiles.

Propriété 4 *Soient* $(a\,,\,b) \in \mathbb{Z} \times \mathbb{N}^*$.
$b\,|\,a$ *ssi le reste de la division euclidienne de* a *par* b *est nul.*

Exemple : $42 = 6 \times (-7) + 0$ et 6 est bien un diviseur de -42.

Propriété 5 *Soit* b *un entier supérieur ou égal à* 2.
Tout entier relatif s'écrit sous une et une seule des formes bq, $bq + 1$,... , $bq + (b - 1)$ *où* q *est un entier relatif.*

Remarque : Le reste d'une division euclidienne par 2 ne peut être que 0 ou 1. Tout entier s'écrit donc sous la forme $2k$ ou $2k + 1$; il est donc pair ou impair.

Exemple : Montrons que tout entier relatif de la forme $N = (n - 2)n(n + 2)$ où $n \in \mathbb{Z}$ est divisible par 3.
Le reste de la division de n par 3 ne peut valoir que 0, 1 ou 2.
◦ Si $n = 3q$, alors $N = 3.q(3q - 2)(3q + 2) \in 3\mathbb{Z}$.
◦ Si $n = 3q + 1$, alors
$N = (3q + 1 + 2)(3q + 1)(3q + 1 - 2) = 3.(q + 1)(3q + 1)(3q - 1) \in 3\mathbb{Z}$.
◦ Si $n = 3q + 2$, alors
$N = (3q + 2 - 2)(3q + 2)(3q + 2 + 2) = 3.q(3q + 2)(3q + 4) \in 3\mathbb{Z}$.

3 Congruences

3.1 Définitions

Définition 2 *Soient a et b deux entiers relatifs et m un entier naturel non nul. On dit que a et b sont congrus modulo m lorsqu'ils ont même reste dans la division euclidienne par m.*
On dit aussi que a est congru à b modulo m et que b est congru à a modulo m.
On note alors $a \equiv b\,[m]$, $a \equiv b\,(m)$ *ou* $a \equiv b \bmod m$.

Exemples : ◦ $34 = 11 \times 3 + 1$ et $16 = 5 \times 3 + 1$ donc $34 \equiv 16\,[3]$.
◦ $-18 = -4 \times 5{+}2$ et $2 = 0 \times 5{+}2$ donc $-18 \equiv 2\,[5]$.
◦ $27 = 6 \times 4{+}3$ et $33 = 8 \times 4{+}1$ donc $27 \not\equiv 33\,[4]$.
◦ Pour tout $n \in \mathbb{N}^*$, $n! = 1 \times 2 \times \ldots \times n \equiv 0\,[k]$ pout tout $k \in [\![\,1\,;n\,]\!]$.

Remarques : • Si $a \equiv b\,[m]$, alors $b \equiv a\,[m]$.
• r est le reste de la division euclidienne de a par m *ssi* $a \equiv r\,[m]$ et $0 \leqslant r < m$.
En effet, si $0 \leqslant r < m$, alors r est son propre reste de sa division euclidienne par m.
• La notation est similaire à celle utilisée pour les angles en radian :
$\frac{3\pi}{2} \equiv -\frac{\pi}{2}\,[2\pi]$. On réalise alors une division euclidienne par $2\pi \notin \mathbb{N}^*$.

Théorème 3 *Soient a et $b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$.*
On a $a \equiv b\,[m] \iff m\,|\,(b-a)$.
En particulier, $a \equiv 0\,[m] \iff m\,|\,a$.

Démonstration :
· Si $a \equiv b\,[m]$, alors $a = mq + r$ et $b = mq' + r$
donc $b - a = mq' + r - mq - r = m(q' - q)$ et $m\,|\,(b-a)$.
· Réciproquement, si $m\,|\,(b-a)$, alors $b-a = mk$. Posons $a = mq+r$ et $b = mq' + r'$ par division euclidienne et $b - a = m(q'-q) + (r'-r)$.
On a alors $m(q'-q) + (r'-r) = mk$ et $r' - r = m(k - q' + q) \in m\mathbb{Z}$.
On sait que $r' - r \in\,]-m\,;m\,[$ qui ne contient qu'un seul multiple de m : 0.
Ainsi, $r = r'$ et $a \equiv b\,[m]$.
· Pour $b = 0$, on obtient $a \equiv 0\,[m] \iff m\,|\,(0-a) \iff m\,|\,a$. □

Remarque : • On a toujours $a \equiv a\,[m]$, $a \equiv 0\,[a]$ et $a \equiv 0\,[1]$.

Exemples : ◦ $15 - 7 = 8 = 2 \times 4$ donc $15 \equiv 7\,[2]$ et $15 \equiv 7\,[4]$.
◦ $-5 + 1 = -4 = -1 \times 4$ donc $-5 \equiv -1\,[4]$: c'est un « multiple de quatre retranché de 1 ».
◦ $\{1; 2; 3; 4; 6; 12\} \subset D_+(12)$ donc $12 \equiv 0\,[1]$, $12 \equiv 0\,[2]$, $12 \equiv 0\,[3]$, $12 \equiv 0\,[4]$, $12 \equiv 0\,[6]$ et $12 \equiv 0\,[12]$.

3.2 Propriétés des congruences

Propriété 6 ***Transitivité***
Soient a, b et c trois entiers relatifs et m un entier naturel non nul.
Si $a \equiv b\,[m]$ *et* $b \equiv c\,[m]$, *alors* $a \equiv c\,[m]$.

Démonstration : En effet, a b et c ont alors même reste dans la division euclidienne par m. □

Exemple : $-19 \equiv 1\,[4]$ et $-31 \equiv 1\,[4]$ donc $-19 \equiv -31\,[4]$.

Théorème 4 ***Compatibilité avec les opérations***
Soient a, b, c et d quatre entiers relatifs, m et p deux entiers naturels non nuls.
Si $a \equiv b\,[m]$ *et* $c \equiv d\,[m]$, *on a*

- $a + c \equiv b + d\,[m]$ *(compatibilité avec l'addition).*
- $a \times c \equiv b \times d\,[m]$ *(compatibilité avec la multiplication).*
- $a^p \equiv b^p\,[m]$ *(compatibilité avec les puissances).*

Démonstration : • D'après le théorème 3, m divise $(b - a)$ et $(d - c)$. L'entier m divise donc la combinaison linéaire $(b - a) + (d - c) = (b + d) - (a + c)$ et $a + c \equiv b + d\,[m]$.
• Écrivons les divisions euclidiennes $a = mq_1 + r$, $b = mq_2 + r$, $c = mq_3 + r'$ et $d = mq_4 + r'$.
On a alors $ac = mq_1mq_3 + mq_1r' + mq_3r + rr' = m(mq_1q_3 + q_1r' + q_3r) + rr' \equiv rr'\,[m]$.
De même, $bd \equiv rr'\,[m]$ donc $ac \equiv bd\,[m]$.
• Une simple récurrence avec $c = a$ et $d = b$ donne le résultat puisque l'on vient de démontrer que les congruences sont compatibles avec la multiplication. □

Remarques : • En particulier, si $a \equiv b\,[m]$, alors $a + c \equiv b + c\,[m]$ et $ac \equiv bc\,[m]$.
• En revanche, la congruence n'est pas compatible avec la division :
$45 \equiv 63\,[3]$ $(\equiv 0\,[3])$ mais $\frac{45}{9} = 5 \equiv 2\,[3]$ et $\frac{63}{9} = 7 \equiv 1\,[3]$ ne sont pas congrus modulo 3. Ce que l'on peut faire avec les angles n'est plus possible car on se doit de rester dans $\mathbb{Z}$.

Exemple : Montrons que tout entier relatif de la forme $N = n(n + 1)(2n + 1)$ où $n \in \mathbb{Z}$ est divisible par 3.
◦ Si $n \equiv 0\,[3]$ alors $n + 1 \equiv 0 + 1\,[3]$ et $2n + 1 \equiv 2 \times 0 + 1\,[3]$ donc $N \equiv 0 \times 1 \times 1\,[3] \equiv 0\,[3]$: $N \in 3\mathbb{Z}$.
◦ Si $n \equiv 1\,[3]$ alors $n + 1 \equiv 1 + 1\,[3]$ et $2n + 1 \equiv 2 \times 1 + 1\,[3] \equiv 0\,[3]$ donc $N \equiv 1 \times 1 \times 0\,[3] \equiv 0\,[3]$: $N \in 3\mathbb{Z}$.
◦ Si $n \equiv 2\,[3]$, $n + 1 \equiv 2 + 1\,[3] \equiv 0\,[3]$ et $2n + 1 \equiv 2 \times 2 + 1\,[3] \equiv 2\,[3]$ donc $N \equiv 2 \times 0 \times 2\,[3] \equiv 0\,[3]$: $N \in 3\mathbb{Z}$.
Il sera parfois plus simple de présenter ces études dans un tableau de congruence.

3.3 Inverse modulo m

Définition 3 *Soient a un entier relatif et m un entier naturel non nul.*
On dit que a est inversible modulo m lorsqu'il existe un entier b tel que $a \times b \equiv 1\,[m]$.
b est alors un inverse de a modulo m.

Exemples : ◦ On a $8 \times 2 = 16 \equiv 1\,[3]$ donc 8 est inversible modulo 3 et un inverse est 2. Mais nous avons aussi $8 \times 5 = 40 \equiv 1\,[3]$ ou $8 \times 8 = 64 \equiv 1\,[3]$ donc 5 et 8 sont aussi des inverses de 8 modulo 3. On remarque toutefois que ces trois inverses sont tous congrus à 2 modulo 3.

◦ On remarque que $9 \equiv 27\,[6] \equiv 45\,[6] \equiv 3\,[6]$ et $0 \equiv 18\,[6] \equiv 36\,[6] \equiv 0\,[6]$. D'où, $9k \equiv 0$ ou $3\,[6]$ pour tout $k \in [\![\,0\,;5\,]\!]$ et donc pour tout $k \in \mathbb{Z}$. Ainsi, tout multiple de 9 est congru à 3 ou à 0 modulo 6. L'entier 9 n'admet donc pas d'inverse modulo 6.

Propriété 7
Si a admet un inverse modulo m, alors cet inverse est unique modulo m.

Démonstration : Si $ab \equiv 1\,[m]$ et $ab' \equiv 1\,[m]$,
alors $b' = b' \times 1 \equiv b'ab\,[m] \equiv (ab')b\,[m] \equiv 1 \times b\,[m] \equiv b\,[m]$. □

La recherche d'un inverse modulo m est un problème bien plus difficile que dans $\mathbb{R}$. Il n'en existe pas toujours même si les nombres sont non nuls, et s'il en existe, il est unique modulo m seulement. Nous y reviendrons au cours de l'année.

Exercices

DIVISIBILITÉ DANS $\mathbb{Z}$

Exercice 1

1. Déterminer $D(38) \cap D(30)$ et $D(12) \cap D(50)$.
2. Déterminer le nombre de multiples de 11 compris entre -69 et 65.
3. Montrer que, quel que soit $n \in \mathbb{Z}$,
   (a) $2n+5$ est impair,
   (b) $51n+4$ n'est pas divisible par 17,
   (c) $n(n^2+5)$ est pair.
4. Déterminer les entiers naturels x et y vérifiant :
   (a) $x^2 - y^2 = 35$
   (b) $x^2 - y^2 = 12$
   (c) $x^2 - y^2 = -15$
   (d) $(x-4)(y+3) = 4$
   (e) $x + y = xy$
   (f) $x + y = 2xy$
5. Déterminer tous les entiers relatifs n tels que :
   (a) $(n+4) \mid 6$
   (b) $(2n-7) \mid 5$
   (c) $n+7 \in 7\mathbb{Z}$
   (d) $6 \mid (n+5)$
   (e) $(2n+7) \mid (n-3)$
   (f) $(2n+5) \mid (n-1)$
   (g) $(4n+1) \mid (n-3)$

Exercice 2 On appelle diviseur strict de l'entier naturel n tout diviseur d de n tel que $0 < d < n$. Deux entiers naturels sont dits amicaux lorsque chacun de ces entiers est égal à la somme des diviseurs stricts de l'autre.

1. Vérifier que 220 et 284 sont amicaux.
2. Déterminer les sommes des diviseurs positifs de 48 et de 75. Quelle relation y a-t-il entre ces deux sommes ? Ces nombres sont dits quasi amicaux.

Exercice 3 Soit n un entier naturel différent de 1 et soit f la fonction définie par $f(n) = \frac{n^2+3n-2}{n-1}$.

1. Déterminer les nombres a, b et c tels que pour tout $n \neq 1$, $f(n) = an + b + \frac{c}{n-1}$.
2. En déduire les valeurs de n pour lesquelles $f(n)$ est un entier.

Exercice 4 VouF ?

1. Si a divise bc, alors a divise b ou c.
2. Si c est un multiple de a et de b, alors c est un multiple de ab.
3. Si a divise $a+b$, alors a divise b.
4. Si a divise b, alors a^2 divise b^2.

Exercice 5 On aimerait tant voir Syracuse...
On part d'un nombre entier naturel non nul. S'il est pair, on le divise par 2, s'il est impair, on le multiplie par 3 et l'on ajoute 1. En répétant l'opération, on obtient une suite d'entiers positifs dont chacun ne dépend que de son prédécesseur.
Construire la suite de Syracuse du nombre 14 :
Après que le nombre 1 ait été atteint, la suite des valeurs (1,4,2,1,4,2...) se répète indéfiniment en un cycle de longueur 3, appelé cycle trivial. On dit que la suite est cyclique ou périodique à.p.c.r.
Si l'on était parti d'un autre entier, on aurait obtenu une suite différente. *A priori,* il serait possible que la suite de Syracuse de certaines valeurs de départ n'atteigne jamais la valeur 1, soit qu'elle aboutisse à un cycle différent du cycle trivial, soit qu'elle n'aboutisse à aucun cycle. Or, on n'a jamais trouvé d'exemple de suite obtenue suivant les règles données qui n'aboutisse à 1. La conjecture de Syracuse est qu'une suite de Syracuse de n'importe quel entier strictement positif atteint nécessairement 1 et donc le cycle trivial. En dépit de la simplicité de son énoncé, cette conjecture continue de défier les mathématiciens depuis 1928. Ce problème, devenu célèbre quand il a été présenté à l'Université de Syracuse dans l'état de New York, mobilisa tant les mathématiciens durant les années 1960 qu'une plaisanterie courut selon laquelle ce problème faisait partie d'un complot soviétique visant à ralentir la recherche américaine. Selon certains, les mathématiques ne seraient pas encore prêtes pour de tels problèmes.
On appelle $(S_n)_{\mathbb{N}}$ une suite de Syracuse partant d'un entier non nul S_0.

1. Exprimer S_{n+1} en fonction de S_n.
2. Démontrer la conjecture dans les cas $S_0 = 4$, $S_0 = 2$ et $S_0 = 1$.
3. Calculer les premiers termes de la suite de Syracuse du nombre $S_0 = 17$ puis de celle du nombre $S_0 = 48$.
4. On suppose que pour un certain $p \in \mathbb{N}^*$, S_p est un multiple de 3.
   (a) Démontrer que S_{p-1} est aussi un multiple de 3.
   (b) Justifier que S_{p-1} est pair puis démontrer que $S_0 = 2^p S_p$.

Exercice 6

1. Démontrer par récurrence que, pour tout entier naturel n, $7\,|\,(9^n - 2^n)$.
2. Pour $n \in \mathbb{N}^*$, on pose $a_n = 2^{3n} - 3^n$.
   (a) Calculer a_1, a_2 et a_3 puis conjecturer l'existence d'un diviseur de a_n.
   (b) Démontrer cette conjecture.

Exercice 7 Montrons que, pour tout entier naturel non nul n, $n^2\,|\,(n+1)^n - 1$.

1. Développer l'expression $(n+1)^n$.
2. Exprimer $\binom{n}{n-1}$ et $\binom{n}{1}$ en fonction de n.
3. En déduire la propriété énoncée.

Exercice 8

1. (a) Vérifier que pour tout $n \in \mathbb{N}$, $(n+3)^2 = n(n+6) + 9$.

EXERCICES

   (b) À quelle condition 9 est-il le reste de la division euclidienne de $(n+3)^2$ par n ?

2. Le reste de la division euclidienne par 7 de a est 4 et celui de b est 6.
   Déterminer les restes des divisions euclidiennes par 7 de $a+b$ et de $a-b$.
3. (a) Dans la division euclidienne de $2\,512$ par un entier naturel b, le quotient est 54. Le reste peut-il valoir 7 ?

   (b) Dans la division euclidienne de $31\,631$ par un naturel b, le quotient est 253. Le reste peut-il valoir 6 ?

   (c) Dans la division euclidienne de -37 par un entier naturel non nul b, le reste est 14. Quelles sont les valeurs possibles du diviseur et du quotient ?
4. Sachant que le reste de la division euclidienne d'un entier a par 7 est 6, déterminer le reste de la division euclidienne par 7 de $2a$, de $-3a$ et de $4a$.
5. Démontrer que pour tout $n \in \mathbb{N}$, l'entier $N = n(n+5)(n+2)(n-5)$ est divisible par 4.

Exercice 9 Dans une console Python, // donne le quotient de la division euclidienne et % le reste.
Déterminer les entiers M et N tels que `M//4` retourne 2, `N//5` retourne 2, `M%4` retourne 3 et `N%5` retourne 1.

Exercice 10

1. Déterminer les entiers naturels qui, dans la division euclidienne par 4, ont un quotient double du reste.
2. Déterminer les entiers naturels qui, dans la division euclidienne par 6, ont un reste double du quotient.

Exercice 11 Pour sa surboum d'anniversaire, Colette souhaite réaliser des sacs de friandises équitablement répartis pour ses amis. Elle a 115 sucreries à disposition et ses parents ne lui autorisent pas plus de 60 invités.

1. Sachant qu'elle veut utiliser toutes les confiseries, combien d'amis Colette peut-elle inviter ?
2. Et si on lui accorde une rallonge de 42 berlingots ?

Exercice 12 Soient n un entier naturel et l'on pose $P_n = n^3 - n$.

1. Calculer P_0, P_1, P_2 et P_3 puis donner leur reste dans la division euclidienne par 6.
2. Émettre une conjecture puis la démontrer.

Exercice 13

1. (a) On donne $a \equiv 16\,[5]$. Quel est le reste de la division euclidienne de a par 5 ?

   (b) On donne $b \equiv 17\,[3]$. Quel est le reste de la division euclidienne de b par 3 ?
2. Soient x et y deux entiers tels que $x \equiv 7\,[13]$ et $y \equiv 4\,[13]$.

   (a) Déterminer le reste de la division euclidienne par 13 de $x+y$, de xy, de x^3 et de $x^2 - y^2$.

(b) Que dire de $2y - 3x$?

3. Soient m et n deux entiers tels que $m \equiv 1\,[7]$ et $n \equiv 2\,[7]$.
   Déterminer le reste de la division euclidienne de $5m^2 + 2n^2$ et de $2n^2 - 5m^2$ par 7.
4. En utilisant un tableau de congruence, démontrer que, pour tout entier relatif n, $6 \,|\, n(n+1)(2n+1)$.
5. Montrer que, pour tout entier naturel non nul n, $\quad 7 \,|\, 2^{3n} - 1$.
6. Déterminer les valeurs de l'entier naturel n pour lesquelles $n^2 - 3n + 6$ est divisible par 4.
7. Déterminer le reste de la division euclidienne de 11^{2020} par 3.

Exercice 14

1. Démontrer que 5 admet un inverse modulo 11.
2. Montrer que 6 n'a pas d'inverse modulo 10.
3. 3 admet-il un inverse modulo 12 ?

Exercice 15 $\quad x$ désigne un entier relatif.

1. Dresser et compléter un tableau de congruence modulo 8 pour $5x$.
2. En déduire les solutions de l'équation $\quad 5x \equiv 7\,[8]$.
3. Déterminer un inverse de 5 modulo 8. Retrouver alors les solutions précédentes.
4. Montrer que $5x$ est divisible par 8 si, et seulement si, x est divisible par 8.

Exercice 16 Résoudre les équations suivantes dans $\mathbb{Z}$.

(a) $x + 3 \equiv 2\,[7]$	(c) $x^2 \equiv 0\,[4]$	(e) $7x \equiv 2\,[11]$
(b) $3x \equiv 2\,[5]$	(d) $6x \equiv 2\,[7]$	(f) $5x + 2 \equiv 13\,[5]$

Exercice 17 VouF ?

(a) L'équation $x^2 + x + 1 \equiv 0\,[4]$ n'a pas de solutions dans $\mathbb{Z}$.

(b) $15 \times 3^n - 3 \equiv 0\,[7]$ pour $n \equiv 1\,[6]$.

(c) Si $a \equiv 4\,[6]$ et $b \equiv 5\,[6]$, alors $a^2 + b^2 \equiv -1\,[6]$.

(d) Le chiffre des unités de 113^{13} est 1.

Exercice 18 Quel est le chiffre des unités de la somme $\quad 1! + 2! + \ldots + 2019! + 2020!$?

Exercice 19 On considère le polynôme $P(x) = x^2 + 2x - 3$.
Résoudre dans $\mathbb{Z}$ les équations suivantes.

(a) $P(x) = 0$.	(b) $P(x) \equiv 0\,[2]$.	(c) $P(x) \equiv 0\,[7]$.

Exercice 20 La preuve par 9

Agathe a calculé $28 \times 13 = 341$ mais son vieux père, sans effectuer le calcul, lui affirme que son résultat est faux.

1. (a) Déterminer les divisions euclidiennes de 28 et 13 par 9 et en déduire le reste de la division euclidienne de 28×13 par 9.

   (b) Déterminer le reste de la division euclidienne de 341 par 9 et conclure.

EXERCICES

2. Soient x, y, a et b quatre entiers tels que $x \equiv a\,[9]$ et $y \equiv b\,[9]$.
   Compléter $x + y \equiv \ldots\,[9]$ et $x \times y \equiv \ldots\,[9]$.
3. (a) Colette a écrit que $2\,635 + 1\,271 = 3\,806$. La preuve par neuf remet-elle en cause ce résultat ?
   (b) Agathe a écrit que $457 \times 128 = 58\,396$. La preuve par neuf remet-elle en cause ce résultat ?
4. Leur vieux père a calculé $1\,235 \times 151 = 184\,685$ mais en vérifiant avec difficulté au moyen de sa calculatrice, il obtient $186\,485$. Que donne la preuve par neuf ? Que peut-on en conclure ?

Exercice 21

1. Montrer que, pour tout $n \in \mathbb{N}$, $A = 5^n \times 12 - 12^n \times 5$ est divisible par 7.
2. Montrer que $B = 2\,305^{2019} + 1\,106^{2019}$ est divisible par 9.

Exercice 22

1. Soit x un entier relatif. Démontrer que x est impair *ssi* $x^2 \equiv 1\,[8]$.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $x^2 = 8y + 1$.
3. En déduire l'ensemble des points de coordonnées entières de la parabole d'équation $y = \frac{1}{8}x^2 - \frac{1}{8}$.

Exercice 23 On considère l'équation (E): $4x^2 + 3y^2 = 11$.

1. Montrer que si un couple d'entiers $(\,x\,,\,y\,)$ est solution de (E), alors $4x^2 \equiv 2\,[3]$.
2. En déduire que l'équation (E) n'admet pas de solution entière.

Exercice 24 Tous au club !

Le club Math Max du lycée Henri Matisse de La Fare-en-Dole affecte à chacun de ses membres experts un numéro d'adhérent à sept chiffres $c_0c_1c_2c_3c_4c_5c_6$ lors de son inscription.

• Le premier numéro c_0 correspond à son domaine de prédilection : 1 pour l'ensemble des nombres complexes, 2 pour l'arithmétique et 3 pour les graphes et les matrices.

• Les deux chiffres suivants c_1c_2 correspondent au reste de la division euclidienne de l'année de naissance de ce membre par 100.

• Les trois suivants $c_3c_4c_5$ sont donnés par le président du club lors de l'adhésion.

• Le dernier chiffre est la clef de contrôle, calculée de la manière suivante : c_6 est le reste de la division euclidienne par 9 du nombre $c_0 + c_1 + 2c_2 + 3(c_3 + c_4 + c_5)$.

1. Le numéro $1\,024\,578$ peut-il être un numéro d'adhérent ? Et $2\,923\,517$?
2. Nicolas est né en 1982 et adore l'arithmétique. Le président lui a généreusement attribué le numéro 123. Quelle est sa clef de contrôle ?
3. Agnan aime toutes les mathématiques et se trompe donc souvent sur le chiffre correspondant à l'activité. Cela peut-il être détecté par la clef de contrôle ?
4. Clotaire intervertit très régulièrement les deux chiffres de sa date de naissance. Cela peut-il être détecté par la clef de contrôle ?

Exercice 25 Critères de divisibilité

1. Critères de divisibilité par 2, par 10 et par 5 : les énoncer puis les démontrer.
2. Critère de divisibilité par 3.
   (a) On note $\overline{abc}$ l'écriture en base 10 de l'entier naturel $a \times 10^2 + b \times 10 + c$.
   Démontrer que $\overline{abc} \equiv a + b + c\,[3]$.
   (b) Démontrer la propriété analogue pour $\overline{a_n a_{n-1} \dots a_1 a_0}$.
   (c) Énoncer alors un critère de divisibilité par 3.
3. Critère de divisibilité par 9.
   Démontrer un critère analogue pour la divisibilité par 9.
4. Critère de divisibilité par 11.
   (a) Étudier les congruences des puissances de 10 modulo 11.
   (b) En déduire que le nombre $67\,485$ est divisible par 11.
   (c) Déterminer un critère de divisibilité par 11.

Exercice 26 Jeu de Nim, jeu ultime
On place 20 bâtonnets côte à côte sur une table. Deux joueurs prennent chacun à tour de rôle, un, deux ou trois bâtonnets. Le joueur qui prend le dernier a perdu la partie.
Agathe joue avec son père. Celui-ci commence et prend trois bâtonnets. Agathe s'exclame : « Bien joué ! Comme 17 est congru à 1 modulo 4, en adoptant la bonne stratégie, tu es certain de gagner la partie. » Son père reste interloqué. Aurait-elle raison ?

Dirigez-vous vers la page 277 afin de réaliser le devoir n° 2.

Corrigé des exercices

DIVISIBILITÉ DANS $\mathbb{Z}$

Exercice 1

1. $D(38) \cap D(30) = \{\pm 1; \pm 2; \pm 19; \pm 38\} \cap \{\pm 1; \pm 2; \pm 3; \pm 5; \pm 6; \pm 10; \pm 15; \pm 30\}$
   $= \{-2; -1; 1; 2\}$
   $D(12) \cap D(50)$
   $= \{\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 12\} \cap \{\pm 1; \pm 2; \pm 5; \pm 10; \pm 25; \pm 50\} = \{-2; -1; 1; 2\}$.
2. $-77 = -7 \times 11 < -69 \leqslant -66 = -6 \times 11 < 55 = 5 \times 11 \leqslant 65 < 6 \times 11 = 66$: il y a donc douze multiples de 11 entre -69 et 65, le cardinal de $[\![-6\,; 5]\!]$.
3. Soit $n \in \mathbb{Z}$.
   (a) $2n + 5 = 2n + 4 + 1 = 2(n + 2) + 1$ est impair car $2 | 2(n + 2)$ mais $2 \nmid 1$.
   (b) $51n+4 = 7 \times 3n+4$ n'est pas divisible par 17 car sinon $4 = (51n+4)-(7 \times 3n)$ le serait.
   (c) Si $n = 2k$ est pair, alors $n(n^2 + 5) = 2 \times k((2k)^2 + 5)$ est pair.
   Si $n = 2k + 1$ est impair, alors $n(n^2 + 5) = (2k + 1)((2k + 1)^2 + 5)$
   $n(n^2 + 5) = (2k + 1)(4k^2 + 4k + 6) = 2 \times (2k^2 + 2k + 3)(2k + 1)$ est pair.
4. Soient x et $y \in \mathbb{N}$.
   (a) $x^2 - y^2 = 35 \iff (x + y)(x - y) = 35 \times 1 = 7 \times 5$

$$\overset{0 \leqslant x-y \leqslant x+y}{\iff} \begin{cases} x+y &= 35 \\ x-y &= 1 \end{cases} \text{ ou } \begin{cases} x+y &= 7 \\ x-y &= 5 \end{cases}$$

$$\iff \begin{cases} 2x &= 36 \\ y &= 35-x \end{cases} \text{ ou } \begin{cases} 2x &= 12 \\ y &= 7-x \end{cases}$$

$$\iff \begin{cases} x &= 18 \\ y &= 35-18 = 17 \end{cases} \text{ ou } \begin{cases} x &= 6 \\ y &= 7-6 = 1. \end{cases}$$

   $\mathcal{S}_a = \{(6\,, 1)\,; (18\,, 17)\}$.

   (b) $x^2 - y^2 = 12 \iff (x + y)(x - y) = 12 \times 1 = 6 \times 2 = 4 \times 3$

$$\overset{0 \leqslant x-y \leqslant x+y}{\iff} \begin{cases} x+y = 12 \\ x-y = 1 \end{cases} \text{ ou } \begin{cases} x+y = 6 \\ x-y = 2 \end{cases} \text{ ou } \begin{cases} x+y = 4 \\ x-y = 3 \end{cases}$$

$$\iff \begin{cases} 2x = 13 \\ y = 12-x \end{cases} \text{ ou } \begin{cases} 2x = 8 \\ y = 6-x \end{cases} \text{ ou } \begin{cases} 2x = 7 \\ y = 4-x \end{cases}$$

$$\overset{x \in \mathbb{N}}{\iff} \begin{cases} x = 4 \\ y = 6-4 = 2. \end{cases}$$

   $\mathcal{S}_b = \{(4\,, 2)\}$.

   (c) $x^2 - y^2 = -15 \iff y^2 - x^2 = 15 \iff (y + x)(y - x) = 15 \times 1 = 5 \times 3$

$$\overset{0 \leqslant y-x \leqslant y+x}{\iff} \begin{cases} y+x = 15 \\ y-x = 1 \end{cases} \text{ ou } \begin{cases} y+x = 5 \\ y-x = 3 \end{cases}$$

$$\iff \begin{cases} 2y = 16 \\ x = 15-x \end{cases} \text{ ou } \begin{cases} 2x = 8 \\ x = 5-y \end{cases}$$

$\iff \left\{\begin{array}{l} y=8 \\ x=15-8=7 \end{array}\right.$ ou $\left\{\begin{array}{l} y=4 \\ x=5-4=1. \end{array}\right.$
$\mathcal{S}_c=\{(1,4);(7,8)\}$.

(d) $y+3 \geqslant 0$ donc $x-4 \geqslant 0$ et $(x-4)(y+3)=4=1\times 4=2\times 2$
$\iff \left\{\begin{array}{l} x-4=1 \\ y+3=4 \end{array}\right.$ ou $\left\{\begin{array}{l} x-4=4 \\ y+3=1 \end{array}\right.$ ou $\left\{\begin{array}{l} x-4=2 \\ y+3=2 \end{array}\right.$
$\iff \left\{\begin{array}{l} x=1+4=5 \\ y=4-3=1 \end{array}\right.$ ou $\left\{\begin{array}{l} x=4+4=8 \\ y=1-3=-2 \end{array}\right.$ ou $\left\{\begin{array}{l} x=2+4=6 \\ y=2-3=-1 \end{array}\right.$ et $y\in\mathbb{N}$.
$\mathcal{S}_d=\{(5,1)\}$

(e) $x+y=xy \iff xy-x-y+1=1$
$\iff (x-1)(y-1)=1=1\times 1=(-1)\times(-1)$
$\iff \left\{\begin{array}{l} x-1=1 \\ y-1=1 \end{array}\right.$ ou $\left\{\begin{array}{l} x-1=-1 \\ y-1=-1 \end{array}\right. \iff \left\{\begin{array}{l} x=2 \\ y=2 \end{array}\right.$ ou $\left\{\begin{array}{l} x=0 \\ y=0. \end{array}\right.$
$\mathcal{S}_e=\{(0,0);(2,2)\}$

(f) $x+y=2xy$: Si $x=0$, alors $y=0$ et réciproquement.
Si maintenant $xy\neq 0$, $x+y=2xy \iff \frac{x+y}{xy}=2 \iff \frac{1}{y}+\frac{1}{x}=2$
$\overset{x,y\in\mathbb{N}}{\iff} \frac{1}{x}=\frac{1}{y}=1 \iff x=y=1.$ $\mathcal{S}_f=\{(0,0);(1,1)\}$
Sinon, $x+y=2xy \iff x=y(2x-1) \iff y=x(2y-1)$ donc $y|x$ et $x|y$ d'où $x=y$ qui mène à $2x=2x^2$...

5. Soit $n\in\mathbb{Z}$.

(a) $(n+4)|6 \iff n+4\in D(6)=\{-6;-3;-2;-1;1;2;3;6\}$
donc $\mathcal{S}_a=\{-10;-7;-6;-5;-4;-2;-1;2\}$.

(b) $(2n-7)|5 \iff 2n-7\in D(5)=\{-5;-1;1;5\} \iff 2n\in\{2;6;8;12\}$
et $\mathcal{S}_b=\{1;3;4;6\}$.

(c) $n+7\in 7\mathbb{Z} \iff \exists k\in\mathbb{Z},\ n+7=7k \iff n=7k-7=7(k-1)$ multiple de 7 : $\mathcal{S}_c=7\mathbb{Z}$.

(d) $6|(p+5) \iff \exists k\in\mathbb{Z},\ n+5=6k \iff n=6k-5$:
$\mathcal{S}_d=\{\ldots;-11;-5;1;7;13;20;\ldots;6k-5;\ldots\}=\{1+6k\}_{k\in\mathbb{Z}}$.

(e) $(2n+7)|(n-3)$ et $(2n+7)|(2n+7)$
donc $(2n+7)|((2n+7)-2(n-3))=13$ et $(2n+7)\in D(13)=\{-13;-1;1;13\}$ d'où $n=\frac{-13-7}{2}=-10$, $n=\frac{-1-7}{2}=-4$, $n=\frac{1-7}{2}=-3$ ou $n=\frac{13-7}{2}=3$. Puisque $2n+7$ divise bien $n-3$ pour chacun de ses nombres ($-13|-3$, $-1|-7$, $1|-6$ et $13|0$), on a $\mathcal{S}_e=\{-10;-4;-3;3\}$.

(f) $(2n+5)|(n-1)$ et $(2n+5)|(2n+5)$
donc $(2n+5)|((2n+5)-2(n-1))=7$ et $(2n+5)\in D(7)=\{-7;-1;1;7\}$ d'où $n=\frac{-7-5}{2}=-6$, $\frac{-1-5}{2}=-3$, $\frac{1-5}{2}=-2$ ou $\frac{7-5}{2}=1$. Puisque $2n+5$ divise bien $n-1$ pour chacun de ses nombres ($-7|-7$, $-1|-4$, $1|-3$ et $7|0$), on a $\mathcal{S}_f=\{-6;-3;-2;1\}$.

(g) $(4n+1)|(n-3)$ et $(4n+1)|(4n+1)$
donc $(4n+1)|((4n+1)-4(n-3))=13$ et $(4n+1)\in D(13)=\{-13;-1;1;13\}$ d'où $n=\frac{-13-1}{4}\notin\mathbb{Z}$, $\frac{-1-1}{4}\notin\mathbb{Z}$,

CORRIGÉS

$\frac{1-1}{4} = 0$, $\frac{13-1}{4} = 3$. Puisque $4n+1$ divise bien $n-3$ pour chacun de ses nombres ($1|-3$ et $13|0$), on a $\mathcal{S}_g = \{0;3\}$.

Exercice 2 Entiers amicaux

1. On a $220 = 2 \times 2 \times 5 \times 11$
   donc $D_{strict}(220) = \{1;2;4;5;10;11;20;22;44;55;110\}$
   et $1+2+4+5+10+11+20+22+44+55+110 = 284$.
   On a $284 = 2 \times 2 \times 71$ donc $D_{strict}(284) = \{1;2;4;71;142\}$
   et $1+2+4+71+142 = 220$.
   Les entiers 284 et 220 sont donc amicaux.
2. On a $48 = 2^4 \times 3$ donc $D_+(48) = \{1;2;3;4;6;8;12;16;24;48\}$
   et $1+2+3+4+6+8+12+16+24+48 = 124$.
   On a $75 = 3 \times 5^2$ donc $D_+(75) = \{1;3;5;15;25;75\}$
   et $1+3+5+15+25+75 = 124$.
   Les entiers 48 et 75 sont donc quasi amicaux.

Exercice 3 $f(n) = \frac{n^2+3n-2}{n-1}$ pour $n \neq 1$.

1. Pour $n \neq 1$, $an+b+\frac{c}{n-1} = \frac{(an+b)(n-1)+c}{n-1} = \frac{an^2+(b-a)n+(c-b)}{n-1}$ et en identifiant les coefficients de l'expression de f, on doit avoir $a = 1$, $b-a = 3$, $c-b = -2$ d'où $b = 3+1 = 4$, $c = -2+4 = 2$ et $f(n) = n+4+\frac{2}{n-1}$.
2. Ainsi, $f(n) \in \mathbb{Z} \iff n+4+\frac{2}{n-1} \in \mathbb{Z} \iff \frac{2}{n-1} \in \mathbb{Z} \iff (n-1)|2$
   $\iff n-1 \in D(2) = \{-2;-1;1;2\} \iff n \in \{-1;0;2;3\}$.

Exercice 4 VouF ?

1. Si a divise bc, alors a divise b ou c : Faux, $6|(4 \times 3)$ mais $6 \nmid 4$ et $6 \nmid 3$.
2. Si c est un multiple de a et de b, alors c est un multiple de ab : Faux, $12 \in 6\mathbb{Z}$ et $12 \in 4\mathbb{Z}$ mais $12 \notin 24\mathbb{Z}$.
3. Si a divise $a+b$, alors a divise b : Vrai, $a|a$ et $a|(a+b)$ donc $a|((a+b)-a) = b$.
4. Si a divise b, alors a^2 divise b^2 : Vrai, $b = ka \Longrightarrow b^2 = (ka)^2 = k^2.a^2$.

Exercice 5 On aimerait tant voir Syracuse...
Voici la suite de Syracuse du nombre 14 : 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2...
On a appelle $(S_n)_{\mathbb{N}}$ une suite de Syracuse partant d'un entier non nul S_0.

1. On a $S_{n+1} = \begin{cases} \frac{S_n}{2} \text{ si } S_n \text{ pair} \\ 3S_n+1 \text{ si } S_n \text{ impair.} \end{cases}$
2. Si $S_n = 4$, $S_{n+1} = \frac{4}{2} = 2$, $S_{n+2} = \frac{2}{2} = 1$, $S_{n+3} = 3 \times 1 + 1 = 4 = S_n$.
   Ainsi, que l'on parte de 4, 2 ou 1, on reste dans ce cycle.
3. Si $S_0 = 17$, on obtient 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4,...
   Si $S_0 = 48$, on obtient 48, 24, 12, 6, 3, 10, 5, 16, 8, 4, 2, 1, 4,...
4. On suppose que pour une certain $p \in \mathbb{N}^*$, il existe $k \in \mathbb{N}$ tel que $S_p = 3k$.

(a) On a $S_{p-1} = \begin{cases} 2S_p \text{ si } S_{p-1} \text{ pair} \\ \frac{S_p-1}{3} \text{ si } S_{p-1} \text{ impair.} \end{cases} = \begin{cases} 2\times 3k \text{ si } S_{p-1} \text{ pair} \\ \frac{3k-1}{3} \text{ si } S_{p-1} \text{ impair.} \end{cases}$

$S_{p-1} = \begin{cases} 6k \text{ si } S_{p-1} \text{ pair} \\ k-\frac{1}{3} \text{ si } S_{p-1} \text{ impair.} \end{cases}$ Puisque $S_{p-1} \in \mathbb{N}$, il ne peut être égal à $k-\frac{1}{3}$ et l'on est dans le cas $S_{p-1} = 6k$ multiple de 3.

(b) Ainsi, $S_{p-1} = 6k = 2S_p$ est pair et multiple de trois et donc $S_{p-2} = 2S_{p-1}$ aussi. On a montré que si un terme est multiple de trois alors son précédent aussi et par récurrence descendante, $S_0 = 2^p S_p$.

Exercice 6

1. Soit $\mathscr{P}_n : 7\,|\,(9^n - 2^n)$. On a $9^0 - 2^0 = 0 \in 7\mathbb{Z}$. Supposons $\mathscr{P}_n$ vraie pour $n \in \mathbb{N}$. On a $9^{n+1} - 2^{n+1} = 9.9^n - 2.2^n = 9.9^n - 9.2^n + 7.2^n = 9(9^n - 2^n) + 7.2^n$ multiple de 7 par hypothèse de récurrence. Ainsi, $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.
Avec la factorisation de $z^n - a^n$, on obtient directement, pour $n \geqslant 1$,
$9^n - 2^n = (9-2)\sum_{k=0}^{n-1} 9^{n-1-k}2^k \in 7\mathbb{Z}$.
2. (a) Pour $n \in \mathbb{N}^*$, on pose $a_n = 2^{3n} - 3^n$. On a $a_1 = 2^3 - 3 = 5$, $a_2 = 2^6 - 3^2 = 55$ et $a_3 = 2^9 - 3^3 = 485$. Conjecture : $\mathscr{P}_n : 5\,|\,a_n$.

   (b) $\mathscr{P}_1$ est vraie et supposons que $\mathscr{P}_n$ pour un certain $n \in \mathbb{N}^*$.
   On a $a_{n+1} = 2^{3(n+1)} - 3^{n+1} = 2^3.2^{3n} - 3.3^n = 8.2^{3n} - 8.3^n + 5.3^n$
   $a_{n+1} = 8(2^{3n} - 3^n) + 5.3^n$, multiple de 5 par hypothèse de récurrence.
   Ainsi, $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}^*$.
   Avec la factorisation de $z^n - a^n$, on obtient directement, pour $n \geqslant 1$,
   $2^{3n} - 3^n = (2^3)^n - 3^n = 8^n - 3^n = (8-3)\sum_{k=0}^{n-1} 8^{n-1-k}3^k \in 5\mathbb{Z}$.

Exercice 7 Pour $n \in \mathbb{N}^*$, $n^2\,|\,(n+1)^n - 1$.

1. On a $(n+1)^n = \sum_{k=0}^{n} \binom{n}{k} n^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} n^k$.
2. On a $\binom{n}{n-1} = \binom{n}{1} = n$.
3. Ainsi, pour $n = 1$, $n^2 = 1\,|\,1 = ((1+1)^1 - 1)$ et pour $n \geqslant 2$,
$(n+1)^n - 1 = \sum_{k=0}^{n} \binom{n}{k} n^k - 1 = \binom{n}{0} + \binom{n}{1}n + \binom{n}{2}n^2 + \ldots + \binom{n}{n}n^n - 1$
$= 1 + n.n + \binom{n}{2}n^2 + \ldots + \binom{n}{n}n^n - 1$
$= n^2\left(1 + \binom{n}{2} + \binom{n}{3}n + \binom{n}{4}n^2 + \ldots + \binom{n}{n}n^{n-2}\right)$ qui est un multiple de n^2.

Exercice 8

1. (a) Pour tout $n \in \mathbb{N}$, on a $(n+3)^2 = n^2 + 6n + 9 = n(n+6) + 9$.

   (b) Ainsi, $(n+3)^2 - 9 = n(n+6)$ est un multiple de n donc $(n+3)^2 - 9 \equiv 0\,[n]$ et $(n+3)^2 \equiv 9\,[n]$: 9 est toujours le reste de la division euclidienne de $(n+3)^2$ par n.
2. $a \equiv 4\,[7]$ et $b \equiv 6\,[7]$ donc $a + b \equiv 4 + 6\,[7] \equiv 3\,[7]$: le reste de la division euclidienne de $a + b$ par 7 est $3 \in [\![\,0\,;6\,]\!]$.

CORRIGÉS

$a \equiv 4\,[7]$ et $b \equiv 6\,[7]$ donc $a - b \equiv 4 - 6\,[7] \equiv 5\,[7]$: le reste de la division euclidienne de $a - b$ par 7 est $5 \in [\![\,0\,;6\,]\!]$.

3. (a) Supposons $2512 = 54b + 7$. On a alors $54b = 2512 - 7 = 2505$ qui n'est pas un multiple de 54 car impair. Le reste ne peut donc valoir 7.

   (b) Supposons $31631 = 253b + 6$. On a alors $253b = 31631 - 6 = 31625$ $\iff b = \frac{31625}{253} = 125 \in \mathbb{N}$. Le reste peut donc valoir 6.

   (c) On a $-37 = bq + 14$ *i.e.* $bq = -37 - 14 = -51$ d'où $b,\ q \in D(-51) = \{-51; -17; -3; -1; 1; 3; 17; 51\}$ avec $b > r = 14$: les possibilités pour le couple $(\,b\,,\,q\,)$ sont $(\,17\,,\,-3\,)$ et $(\,51\,,\,-1\,)$.

4. On a $a \equiv 6\,[7]$ donc $2a \equiv 12\,[7] \equiv 5\,[7]$, $-3a \equiv -18\,[7] \equiv 3\,[7]$ et $4a \equiv 24\,[7] \equiv 3\,[7]$ qui sont les restes.

5. Dressons un tableau de congruence modulo 4.

n [4]	0	1	2	3
$n+5$ [4]	$5 \equiv 1$	$6 \equiv 2$	$7 \equiv 3$	$8 \equiv 0$
$n+2$ [4]	2	3	$4 \equiv 0$	$5 \equiv 1$
$n-5$ [4]	$-5 \equiv 3$	$-4 \equiv 0$	$-3 \equiv 1$	$-2 \equiv 2$
N [4]	$0 \times 1 \times 2 \times 3 = 0$	0	0	0

et $N = n(n+5)(n+2)(n-5) \equiv 0\,[4]$ est toujours divisible par 4.

Exercice 9 ∫ On a $M = 2 \times 4 + 3 = 11$ et $M = 2 \times 5 + 1 = 11$ aussi.

Exercice 10

1. On cherche $n \in \mathbb{N}$ tel que $n = 4(2r) + r = 9r$ avec $0 \leqslant r < 4$ donc $n \in \mathcal{S}_1 = \{0; 9; 18; 27\}$.

2. On cherche $n \in \mathbb{N}$ tel que $n = 6q + 2q = 8q$ avec $0 \leqslant 2q < 6$ donc $q \in \{0, 1, 2\}$ et $n \in \mathcal{S}_2 = \{0; 8; 16\}$.

Exercice 11 Surboum

1. Soit n le nombre d'invités de Colette et soit b le nombre de bonbons qu'elle va donner à chacun. On doit avoir $bn = 115$ et $n \leqslant 60$. Or $D_+(115) = \{1; 5; 23; 115\}$. Colette peut donc inviter un ami et lui donner 115 bonbons, cinq amis et leur donner 23 bonbons chacun ou 23 amis et leur donner 5 bonbons chacun.

2. On a $115 + 42 = 157$ qui est premier. Colette ne pourra inviter qu'un seul ami qui devra engloutir les 157 bonbons.

Exercice 12 Pour $n \in \mathbb{N}^*$, $P_n = n^3 - n$.

1. $P_0 = 0^3 - 0 = 0 \equiv 0\,[6]$, $P_1 = 1^3 - 1 = 0 \equiv 0\,[6]$, $P_2 = 2^3 - 2 = 6 \equiv 0\,[6]$ et $P_3 = 3^3 - 3 = 24 \equiv 0\,[6]$.

2. Il semble que P_n soit toujours divisible par 6.
   On a $P_n = n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$.
   Dressons un tableau de congruence modulo 6.

n [6]	0	1	2	3	4	5
$n-1$ [6]	$-1 \equiv 5$	0	1	2	3	4
$n+1$ [6]	1	2	3	4	5	$6 \equiv 0$
P_n [6]	$0 \times 5 \times 1 = 0$	0	$2 \times 1 \times 3 \equiv 0$	$3 \times 2 \times 4 \equiv 0$	$4 \times 3 \times 5 \equiv 0$	0

et $P_n \equiv 0\,[6]$ est toujours divisible par 6.

Exercice 13

1. (a) On a $a \equiv 16\,[5] \iff a = 5q + 16 = 5(q+3) + 1 \equiv 1\,[5]$: le reste de la division euclidienne de a par 5 vaut $1 \in [\![\, 0\,;4 \,]\!]$.

   (b) On a $b \equiv 17\,[3] \iff b = 3q' + 17 = 3(q'+5) + 2 \equiv 2\,[3]$: le reste de la division euclidienne de b par 3 vaut $2 \in [\![\, 0\,;2 \,]\!]$.

2. (a) $x \equiv 7\,[13]$ et $y \equiv 4\,[13]$ donc $x + y \equiv 7 + 4\,[13] \equiv 11\,[13]$, $xy \equiv 7 \times 4\,[13] \equiv 28\,[13] \equiv 2\,[13]$, $x^3 \equiv 7^3\,[13] \equiv 343\,[13] \equiv 5\,[13]$ et $x^2 - y^2 \equiv 7^2 - 4^2\,[13] \equiv 33\,[13] \equiv 7\,[13]$.

   (b) $2y - 3x \equiv 2 \times 4 - 3 \times 7\,[13] \equiv -13\,[13] \equiv 0\,[13]$ donc $2y - 3x$ est divisible par 13.

3. $m \equiv 1\,[7]$ et $n \equiv 2\,[7]$ donc $5m^2 + 2n^2 \equiv 5 \times 1^2 + 2 \times 2^2\,[7] \equiv 13\,[7] \equiv 6\,[7]$ et $2n^2 - 5m^2 \equiv 2 \times 2^2 - 5 \times 1^2\,[7] \equiv 3\,[7]$.

4. Dressons un tableau de congruence modulo 6.

n [6]	0	1	2	3	4	5
$n+1$ [6]	1	2	3	4	5	$6 \equiv 0$
$2n+1$ [6]	1	3	5	$7 \equiv 1$	$9 \equiv 3$	$11 \equiv 5$
Produit [6]	0	$6 \equiv 0$	$30 \equiv 0$	$12 \equiv 0$	$60 \equiv 0$	0

et $n(n+1)(2n+1) \equiv 0\,[6]$ est toujours divisible par 6.

5. Soit $n \in \mathbb{N}^*$. On a $2^{3n} - 1 = (2^3)^n - 1^n = (2^3 - 1) \sum\limits_{k=0}^{n-1} (2^3)^{n-k-1} 1^k$

   $2^{3n} - 1 = 7 \sum\limits_{k=0}^{n-1} 8^{n-k-1}$ multiple de 7.

   Sinon, $2^3 = 8 \equiv 1\,[7]$ donc $2^{3n} \equiv 1^n\,[7]$ et $2^{3n} - 1 \equiv 0\,[7]$.

6. Dressons un tableau de congruence modulo 4.

n [4]	0	1	2	3
n^2 [4]	0	1	$4 \equiv 0$	$9 \equiv 1$
$-3n$ [4]	0	$-3 \equiv 1$	$-6 \equiv 2$	$-9 \equiv 3$
6 [4]	2	2	2	2
$n^2 - 3n + 6$ [4]	2	$4 \equiv 0$	$4 \equiv 0$	$6 \equiv 2$

et $n^2 - 3n + 6$ est divisible par 4 lorsque $n \equiv 1\,[4]$ ou $n \equiv 2\,[4]$: $n \in \{4k+1\}_{k \in \mathbb{N}} \cup n \in \{4k+2\}_{k \in \mathbb{N}}$.

CORRIGÉS

7. On a $11 \equiv 2\,[3]$ donc $11^2 \equiv 4\,[3] \equiv 1\,[3]$. Ainsi, pour tout $n \in \mathbb{N}$, $11^{2n} = (11^2)^n \equiv 1^n\,[3]$. En particulier, $11^{2020} = (11^2)^{1010} \equiv 1\,[3]$ et le reste de la division euclidienne de 11^{2020} par 3 vaut $1 \in [\![\,0\,;2\,]\!]$.

Exercice 14

1. Dressons un tableau de congruence modulo 11.

$n\,[11]$	0	1	2	3	4	5	6	7	8	9	10
$5n\,[11]$	0	5	10	$15 \equiv 4$	$20 \equiv 9$	$25 \equiv 3$	$30 \equiv 8$	$35 \equiv 2$	$40 \equiv 7$	$45 \equiv 1$	$50 \equiv 6$

et l'inverse de 5 modulo 11 est 9.

2. Dressons un tableau de congruence modulo 10.

$n\,[10]$	0	1	2	3	4	5	6	7	8	9
$6n\,[10]$	0	6	$12 \equiv 2$	$18 \equiv 8$	$24 \equiv 4$	$30 \equiv 0$	$36 \equiv 6$	$42 \equiv 2$	$54 \equiv 4$	$63 \equiv 3$

et $6n$ n'est jamais congru à 1 modulo 10 : 6 n'admet pas d'inverse modulo 10.

3. Dressons un tableau de congruence modulo 12.

$n\,[12]$	0	1	2	3	4	5	6	7	8	9	10	11
$3n\,[12]$	0	3	6	9	0	3	6	9	0	3	6	9

et $3n$ n'est jamais congru à 1 modulo 12 : 3 n'admet pas d'inverse modulo 12.
On remarque que ce tableau est cyclique. En effet, si $n \equiv 4+1\,[12]$ alors $3n \equiv 3(4+1)\,[12] \equiv 3 \times 1\,[12]$.
Nous verrons plus tard dans l'année un critère d'existence et d'unicité d'un inverse modulo m.

Exercice 15 Soit $x \in \mathbb{Z}$.

1. Dressons un tableau de congruence modulo 8.

$x\,[8]$	0	1	2	3	4	5	6	7
$5x\,[8]$	0	5	$10 \equiv 2$	$15 \equiv 7$	$20 \equiv 4$	$25 \equiv 1$	$30 \equiv 6$	$35 \equiv 3$

2. Ainsi, $5x \equiv 7\,[8] \iff x \equiv 3\,[8] \iff x \in \{8q+3\}_{q\in\mathbb{Z}}$.
3. D'après le tableau précédent, $5 \times 5 \equiv 1\,[8]$ est 5 est son propre inverse modulo 8.
   On a alors $5x \equiv 7\,[8] \iff 5 \times 5x \equiv 5 \times 7\,[8] \iff 1x \equiv 35\,[8] \iff x \equiv 3\,[8]$.
4. D'après le tableau précédent, $5x \equiv 0\,[8] \iff x \equiv 0\,[8]$ c.-à-d. $8\,|\,x$.

Exercice 16 Résolutions d'équations dans $\mathbb{Z}$.

(a) On a $x+3 \equiv 2\,[7] \iff x \equiv 2-3\,[7] \equiv -1\,[7] \equiv 6\,[7]$:
$\mathcal{S}_a = \{7k-1\}_{k\in\mathbb{Z}} = \{7k+6\}_{k\in\mathbb{Z}}$.

(b) Dressons un tableau de congruence modulo 5.

$x\,[5]$	0	1	2	3	4
$3x\,[5]$	0	3	$6 \equiv 1$	$9 \equiv 4$	$12 \equiv 2$

et $3x \equiv 2\,[5] \iff x \equiv 4\,[5]$: $\mathcal{S}_b = \{5k+4\}_{k\in\mathbb{Z}}$.

Si l'on sait que 2 est l'inverse de 3 modulo 5, on peut résoudre directement :
$3x \equiv 2\,[5] \iff 2 \times 3x \equiv 2 \times 2\,[5] \iff x \equiv 4\,[5]$.

(c) Dressons un tableau de congruence modulo 4.

$x\,[4]$	0	1	2	3
$x^2\,[4]$	0	1	$4 \equiv 0$	$9 \equiv 1$

et $\quad x^2 \equiv 0\,[4] \iff x \equiv 0\,[5]$ ou $x \equiv 2\,[4]$:
$\mathcal{S}_c = \{4k\}_{k\in\mathbb{Z}} \cup \{4k+2\}_{k\in\mathbb{Z}} = \{n$ pair$\} = 2\mathbb{Z}$.

(d) Dressons un tableau de congruence modulo 7.

$x\,[7]$	0	1	2	3	4	5	6
$6x\,[7]$	0	6	$12 \equiv 5$	$18 \equiv 4$	$24 \equiv 3$	$30 \equiv 2$	$36 \equiv 1$

et $\quad 6x \equiv 2\,[7] \iff x \equiv 5\,[7]$: $\quad \mathcal{S}_d = \{7k+5\}_{k\in\mathbb{Z}}$.
Si l'on sait que 6 est son propre inverse modulo 7, on peut résoudre directement :
$6x \equiv 2\,[7] \iff 6 \times 6x \equiv 6 \times 2\,[7] \iff 1x \equiv 12\,[7] \iff x \equiv 5\,[7]$.

(e) Dressons un tableau de congruence modulo 11.

$x\,[11]$	0	1	2	3	4	5	6	7	8	9	10
$7x\,[11]$	0	7	$14 \equiv 3$	$21 \equiv 10$	$28 \equiv 6$	$35 \equiv 2$	$42 \equiv 9$	$49 \equiv 5$	$56 \equiv 1$	$63 \equiv 8$	$70 \equiv$

et $\quad 7x \equiv 2\,[11] \iff x \equiv 5\,[11]$: $\quad \mathcal{S}_e = \{11k+5\}_{k\in\mathbb{Z}}$.
Si l'on sait que 8 est l'inverse de 7 modulo 11, on peut résoudre directement :
$7x \equiv 2\,[11] \iff 8 \times 7x \equiv 8 \times 2\,[11] \iff 1x \equiv 16\,[11] \iff x \equiv 5\,[11]$.

(f) On a $\quad 5x + 2 \equiv 13\,[5] \iff 5x \equiv 13 - 2\,[5] \equiv 11\,[5] \iff 5x \equiv 1\,[5]$.
Or, $\forall x \in \mathbb{Z}$, $5x$ est un multiple de 5 donc $\quad 5x \equiv 0\,[5] \not\equiv 1\,[5] \quad$ et $\quad \mathcal{S}_f = \varnothing$.

Exercice 17 VouF ?

(a) L'équation $x^2 + x + 1 \equiv 0\,[4]$ n'a pas de solutions dans $\mathbb{Z}$: Vrai.
Dressons un tableau de congruence modulo 4.

$x\,[4]$	0	1	2	3
$x^2\,[4]$	0	1	$4 \equiv 0$	$9 \equiv 1$
$1\,[4]$	1	1	1	1
$x^2 + x + 1\,[4]$	1	3	3	$5 \equiv 1$

(b) $15 \times 3^n - 3 \equiv 0\,[7]$ pour $n \equiv 1\,[6]$: Vrai.
On a $\quad n \equiv 1\,[6] \iff n = 6k+1 \quad$ et $\quad 15 \times 3^n = 15 \times 3^{6k+1} = 15 \times 3 \times (3^6)^k$.
Or, $\quad 45 = 42+3 \equiv 3\,[7] \quad$ et $\quad 3^6 = 729 = 728+1 \equiv 1\,[7] \quad$ donc $(3^6)^k \equiv 1^k\,[7]$
et $\quad 15 \times 3^n \equiv 3 \times 1\,[7]$ c.-à-d. $15 \times 3^n - 3 \equiv 0\,[7]$.

(c) Si $a \equiv 4\,[6]$ et $b \equiv 5\,[6]$, alors $a^2 + b^2 \equiv -1\,[6]$: Vrai.
On a $\quad a \equiv 4\,[6]$ et $b \equiv 5\,[6] \quad$ donc $\quad a^2 + b^2 \equiv 4^2 + 5^2\,[6] \equiv 41\,[6] \equiv -1\,[6]$
car $41 = 6 \times 7 - 1$.

(d) Le chiffre des unités de 113^{13} est 1 : Faux.
On a $\quad 113 \equiv 3\,[10] \quad$ donc $113^{13} \equiv 3^{13}\,[10]$. $\quad$ Puisque $3^4 = 81 \equiv 1\,[10]$,
$3^{13} = (3^4)^3 \times 3 \equiv 1^3 \times 3\,[10] \quad$ et le chiffre des unités de 113^{13} est 3.

Exercice 18 On remarque que, dès que $n \geqslant 5$, $10|n!$ donc le chiffre des unités de $n!$ est 0. Ainsi, le chiffe des unités de la somme $1! + 2! + \ldots + 2020!$ est celui de $1! + 2! + 3! + 4! = 1 + 2 + 6 + 24 = 33$: c'est 3.

Exercice 19 On considère le polynôme $P(x) = x^2 + 2x - 3$ et l'on résout dans $\mathbb{Z}$.

(a) $P(x) = 0 \iff x^2 + 2x - 3 = 0 \overset{\text{1 racine}}{\iff} (x-1)(x+3) = 0$
$\iff x = 1$ ou $x = -3$: $\mathcal{S}_a = \{-3; 1\}$.

(b) $P(x) \equiv 0\,[2]$: Dressons un tableau de congruence modulo 2.

$x\,[2]$	0	1
$x^2\,[2]$	0	1
$2x\,[2]$	0	$2 \equiv 0$
$-3\,[2]$	1	1
$P(x)\,[2]$	1	$2 \equiv 0$

et $P(x) \equiv 0\,[2] \iff x \equiv 1\,[2]$: $\mathcal{S}_b = \{2k+1\}_{k\in\mathbb{Z}} = \{x \text{ impair}\}$.

(c) $P(x) \equiv 0\,[7]$: Dressons un tableau de congruence modulo 7.

$x\,[7]$	0	1	2	3	4	5	6
$x^2\,[7]$	0	1	4	$9 \equiv 2$	$16 \equiv 2$	$25 \equiv 4$	$36 \equiv 1$
$2x\,[7]$	0	2	4	6	$8 \equiv 1$	$10 \equiv 3$	$12 \equiv 5$
$-3\,[7]$	4	4	4	4	4	4	4
$P(x)\,[7]$	4	$7 \equiv 0$	$12 \equiv 5$	$12 \equiv 5$	$7 \equiv 0$	$11 \equiv 4$	$10 \equiv 3$

et $P(x) \equiv 0\,[7] \iff x \equiv 1\,[7]$ ou $x \equiv 4\,[7]$: $\mathcal{S}_c = \{7k+1\}_{k\in\mathbb{Z}} \cup \{7k+4\}_{k\in\mathbb{Z}}$.

Exercice 20 La preuve par 9
Agathe a calculé $28 \times 13 = 341$ mais son vieux père, sans effectuer le calcul, lui affirme que son résultat est faux.

1. (a) On a $28 = 3 \times 9 + 1 \equiv 1\,[9]$ et $13 = 1 \times 9 + 4 \equiv 4\,[9]$ donc $28 \times 13 \equiv 1 \times 4\,[9] \equiv 4\,[9]$.

   (b) On a $341 = 37 \times 9 + 8 \equiv 8\,[9] \not\equiv 4\,[9]$ donc Agathe s'est bien trompée.

2. Si $x \equiv a\,[9]$ et $y \equiv b\,[9]$, alors $x + y \equiv a + b\,[9]$ et $x \times y \equiv a \times b\,[9]$.

3. (a) On a $2635 = 292 \times 9 + 7 \equiv 7\,[9]$, $1271 = 141 \times 9 + 2 \equiv 2\,[9]$ et $3806 = 400 \times 9 + 8 \equiv 8\,[9]$. Puisque $7 + 2 = 9 \equiv 0\,[9] \not\equiv 8\,[9]$, la preuve par neuf remet en cause le résultat de Colette.

   (b) On a $457 = 50 \times 9 + 7 \equiv 7\,[9]$, $128 = 14 \times 9 + 2 \equiv 2\,[9]$ et $58396 = 6488 \times 9 + 4 \equiv 4\,[9]$. Puisque $7 \times 2 = 14 \equiv 5\,[9] \not\equiv 8\,[9]$, la preuve par neuf remet en cause le résultat d'Agathe.

4. On a $1235 = 137 \times 9 + 2 \equiv 2\,[9]$, $151 = 16 \times 9 + 7 \equiv 7\,[9]$ et $184685 = 20520 \times 9 + 5 \equiv 5\,[9]$. Puisque $2 \times 7 = 14 \equiv 5\,[9]$, la preuve par neuf ne remet pas en cause le résultat de leur vieux père. Puisque ce résultat est tout de même faux, la preuve par neuf n'est donc pas une véritable preuve mais un test de fiabilité non négligeable.

Pour calculer les restes modulo 9, il est beaucoup plus rapide de calculer le reste de la somme des chiffres.
Par exemple, $1235 \equiv 1+2+3+5\,[9] \equiv 2\,[9]$
et $184\,685 \equiv 1+8+4+6+8+5\,[9] \equiv 9+18+5\,[9] \equiv 5\,[9]$.
Ceci sera justifié dans l'exercice 25.

Exercice 21

1. Puisque $12 \equiv 5\,[7]$, on a $A = 5^n \times 12 - 12^n \times 5 \equiv 5^n \times 5 - 5^n \times 5\,[7] \equiv 0\,[7]$ et A est un multiple de 7.
2. On a $2305 = 256 \times 9 + 1 \equiv 1\,[9]$ et $1106 = 123 \times 9 - 1 \equiv -1\,[9]$ donc $B = 2\,305^{2019} + 1\,106^{2019} \equiv 1^{2019} + (-1)^{2019}\,[9] \equiv 1-1\,[9] \equiv 0\,[9]$ et B est un multiple de 9.

Exercice 22

1. Dressons un tableau de congruence modulo 8.

$x\,[8]$	0	1	2	3	4	5	6	7
$x^2\,[8]$	0	1	4	$9 \equiv 1$	$16 \equiv 0$	$25 \equiv 1$	$36 \equiv 4$	$49 \equiv 1$

   et l'on a bien x impair *ssi* $x^2 \equiv 1\,[8]$.

2. Si $x^2 = 8y+1$, alors $x^t2 \equiv 1\,[8]$ puisque $8y \equiv 0\,[8]$. On en déduit que x est impair. Soit $k \in \mathbb{Z}$ tel que $x = 2k+1$. On a $\frac{(2k+1)^2-1}{8} = \frac{4k^2+4k}{8} = \frac{k(k+1)}{2} \in \mathbb{Z}$ car ce sont deux entiers consécutifs.
   Réciproquement, si $y = \frac{k(k+1)}{2}$, alors $8y+1 = 4k(k+1)+1 = (2k+1)^2$ est le carré d'un impair.
   L'ensemble des couples $(\,x\,,\,y\,) \in \mathbb{Z}^2$ solutions de l'équation $x^2 = 8y+1$ est donc $\left\{\left(\,2k+1\,,\,\frac{k(k+1)}{2}\,\right)\right\}_{k\in\mathbb{Z}}$.
3. Puisque $x^2 = 8y+1 \iff y = \frac{1}{8}x^2 - \frac{1}{8}$, l'ensemble des points de coordonnées entières de la parabole d'équation $y = \frac{1}{8}x^2 - \frac{1}{8}$ est $\left\{\left(\,2k+1\,,\,\frac{k(k+1)}{2}\,\right)\right\}_{k\in\mathbb{Z}}$.

Exercice 23 $(E)\colon 4x^2 + 3y^2 = 11$.

1. On a toujours $3y^2 \equiv 0\,[3]$ car $3y^2$ est un multiple de trois donc si $(\,x\,,\,y\,)$ est un couple d'entiers solution de (E), $4x^2 = 11 - 3y^2 \equiv 11 - 0\,[3] \equiv 2\,[3]$.
2. Dressons un tableau de congruence modulo 3.

$x\,[3]$	0	1	2
$x^2\,[3]$	0	1	$4 \equiv 1$
$4x^2\,[3]$	0	$4 \equiv 1$	$4 \equiv 1$

   et $4x^2 \not\equiv 2\,[3]$. L'équation (E) n'admet donc pas de solution entière.

Exercice 24 Tous au club !

c_6 est le reste de la division euclidienne par 9 du nombre $c_0 + c_1 + 2c_2 + 3(c_3 + c_4 + c_5)$.

1. $1\,024\,578$: On a $1+0+2\times 2+3(4+5+7) = 53 \equiv 8\,[9]$ donc $1\,024\,578$ peut être un numéro d'adhérent.
   $2\,923\,517$: On a $1+9+2\times 2+3(3+5+1) = 41 \equiv 5\,[9] \not\equiv 7\,[9]$ donc $2\,923\,517$ ne peut pas être un numéro d'adhérent.

CORRIGÉS

2. On a $c_0 = 2$, $1982 \equiv 82\,[100]$ donc $c_1 = 8$ et $c_2 = 2$, $c_3 = 1$, $c_4 = 2$ et $c_5 = 3$.
   Puisque $2+8+2\times 2+3(1+2+3) = 32 \equiv 5\,[9]$, la clef de contrôle est $c_6 = 5$.

3. Si le chiffre c_0 varie de 1 ou 2, il en sera de même du calcul $c_0 + c_1 + 2c_2 + 3(c_3 + c_4 + c_5)$ et le reste de la division euclidienne varie aussi de 1 ou 2 modulo 9.
   En effet, $c_0' + c_1 + 2c_2 + 3(c_3 + c_4 + c_5) \equiv c_0 + c_1 + 2c_2 + 3(c_3 + c_4 + c_5)\,[9]$
   $\iff$ $c_0' \equiv c_0\,[9]$ $\iff$ $c_0' = c_0$ car ces derniers valent 1, 2 ou 3. La clef de contrôle peut donc détecter une telle erreur de la part d'Agnan.

4. On a $c_0 + c_2 + 2c_1 + 3(c_3 + c_4 + c_5) \equiv c_0 + c_1 + 2c_2 + 3(c_3 + c_4 + c_5)\,[9]$
   $\iff$ $c_2 + 2c_1 \equiv c_1 + 2c_2\,[9]$ $\iff$ $c_1 \equiv c_2\,[9]$. Ceci se produit lorsque $c_2 = c_1$ mais l'année ne change pas ou lorsque c_2 et c_1 se partagent les nombres 0 et 9 ($9 \equiv 0\,[9]$). L'erreur de Clotaire n'est donc pas détectée s'il est né en 1990 ou en 2009.

Exercice 25 Critères de divisibilité

1. Soit $n \in \mathbb{Z}$.
   • n est divisible par 2 *ssi* son chiffre des unités est 0, 2, 4, 6 ou 8.
   On a $2\,|\,n \iff n = 2k$ et un simple tableau de congruences modulo 10 donne le résultat.
   • n est divisible par 10 *ssi* son chiffre des unités est 0.
   On a $10\,|\,n \iff n = 10k$ et l'on a toujours $10k \equiv 0\,[10]$.
   • n est divisible par 5 *ssi* son chiffre des unités est 0 ou 5.
   On a $5\,|\,n \iff n = 5k$ et un simple tableau de congruences modulo 10 donne le résultat.

2. (a) Puisque $10 \equiv 1\,[3]$, $10^2 \equiv 1^2\,[3]$
   et $\overline{abc} = a \times 10^2 + b \times 10 + c \equiv a \equiv a \times 1^2 + b \times 1 + c\,[3] \equiv a + b + c\,[3]$.
   (b) De même, $10^n \equiv 1\,[3]$ et $\overline{a_n a_{n-1} \dots a_1 a_0} \equiv a_n + a_{n-1} + \dots + a_1 + a_0\,[3]$.
   (c) Un entier est donc divisible par 3 *ssi* la somme de ses chiffres est divisible par 3. Plus généralement, on peut remarquer que le reste de cette somme modulo 3 est précisément celui de cet entier.

3. Puisque $10 \equiv 1\,[9]$, $10^n \equiv 1\,[9]$
   et $\overline{a_n a_{n-1} \dots a_1 a_0} \equiv a_n + a_{n-1} + \dots + a_1 + a_0\,[9]$.
   Un entier est donc divisible par 9 *ssi* la somme de ses chiffres est divisible par 9.
   Plus généralement, on peut remarquer que le reste de cette somme modulo 3 est précisément celui de cet entier.

4. Critère de divisibilité par 11.
   (a) $10^0 = 1 \equiv 1\,[11]$, $10^1 = 10 \equiv 10\,[11] \equiv -1\,[11]$, $10^2 = 100 \equiv 1\,[11]$
   et $10^3 = 1000 \equiv 10\,[11] \equiv -1\,[11]$.
   Plus généralement, $10^{2k} \equiv 1\,[11]$ et $10^{2k+1} \equiv -1\,[11]$. En effet, une simple récurrence donne
   $10 \times 10^{2k} \equiv 10 \times 1\,[11] \equiv 10\,[11] \equiv -1\,[11]$
   et $10 \times 10^{2k+1} \equiv 10 \times 10\,[11] \equiv 100\,[11] \equiv 1\,[11]$.

(b) Ainsi, $67\,485 = 6.10^4 + 7.10^3 + 4.10^2 + 8.10 + 5$
$67\,485 \equiv 6 \times 1 + 7 \times (-1) + 4 \times 1 + 8 \times (-1) + 5\,[11] \equiv 0\,[11]$ et $67\,485$ est divisible par 11.

(c) Un entier est donc divisible par 11 *ssi* la somme alternée (changement de signe) de ses chiffres est divisible par 11.

Exercice 26 Jeu de Nim, jeu ultime
C'est à Agathe de jouer.
S'il ne reste plus qu'un seul bâtonnet, alors elle a évidemment perdu.
S'il en reste $1 + 4 = 5$, alors, qu'elle en prenne un, deux ou trois, son père pourra toujours arriver à la situation où il ne reste plus qu'un seul bâtonnet : il en prend trois, deux ou un.
S'il en reste $1+4+4 = 9$, alors, qu'elle en prenne un, deux ou trois, son père pourra toujours arriver à la situation où il ne reste plus que cinq bâtonnets en en prenant trois, deux ou un et l'on sait que dans ce cas, il peut gagner.
S'il en reste $1 + 4n$, son père pourra toujours revenir à la situation $1 + 4(n - 1)$ et donc à la situation où il n'y a plus qu'un seul bâtonnet : il peut donc toujours gagner.
En revanche, Agathe ne lui a pas divulgué la bonne stratégie et il s'est débrouillé pour perdre, comme d'habitude.

CORRIGÉS

Chapitre III

NOMBRES COMPLEXES : ÉQUATIONS POLYNOMIALES

Sommaire

Historiquement, « l'invention » des nombres complexes est due à la nécessité de la résolution des équations polynomiales. Le premier résultat donne des solutions explicites à toutes les équations du second degré à coefficients réels, un premier pas déterminant avant les degrés supérieurs.

1 Rappels

Il existe un ensemble $\mathbb{C}$ de nombres dits complexes, contenant $\mathbb{R}$, muni de règles d'addition et de multiplication similaires, tel que tout $z \in \mathbb{C}$ s'écrit de manière unique sous la forme algébrique $z = a + ib$ où $a = \mathfrak{Re}(z)$ et $b = \mathfrak{Im}(z)$ sont des réels et i vérifie $i^2 = -1$.
On a $zz' = 0 \iff z = 0$ ou $z' = 0$.
Pour tout $z \in \mathbb{C}$, on définit l'opposé de z par $-z = -a - ib$ et le conjugué de z par $\overline{z} = a - ib$.
On a $\overline{z + z'} = \overline{z} + \overline{z'}$, $\overline{zz'} = \overline{z}\,\overline{z'}$ et, pour $z \neq 0$, $\overline{\frac{1}{z}} = \frac{1}{\overline{z}}$.
Si $z = a + ib$, on a toujours $z\overline{z} = a^2 + b^2$.

2 Équations du second degré à coefficients réels

Commençons par tenter de résoudre quelques équations.

Exemples : ◦ $z^2+9=0 \iff z^2=-9=3^2i^2 \iff z=\pm 3i.$
En effet, on a bien $(z-3i)(z+3i)=z^2-(3i)^2=z^2-(-9)$ et l'on remarque que $\frac{-0\pm i\sqrt{36}}{2\times 1}=\pm 3i.$

◦ $z^2-2z+5=0 \iff z^2-2z+1=-4 \iff (z-1)^2=2^2i^2$
$\iff z-1=\pm 2i \iff z=1\pm 2i.$
En effet, on a bien $(z-1-2i)(z+1+2i)=\ldots=z^2-2z+5$ et l'on remarque que $\frac{-(-2)\pm i\sqrt{16}}{2\times 1}=1\pm 2i.$

Théorème 1 *Soient a, b et c trois nombres **réels** tels que $a\neq 0$.*
*Dans $\mathbb{C}$, l'équation $az^2+bz+c=0$ admet **toujours** des solutions.*
On note Δ le discriminant de cette équation : $\Delta=b^2-4ac$.

- *Si $\Delta>0$, l'équation admet deux solutions réelles distinctes,*
  $$x_1=\frac{-b-\sqrt{\Delta}}{2a} \quad et \quad x_2=\frac{-b+\sqrt{\Delta}}{2a}.$$
- *Si $\Delta=0$, l'équation admet une unique solution « double », réelle,*
  $$x_0=-\frac{b}{2a}.$$
- *Si $\Delta<0$, l'équation admet deux solutions, complexes et conjuguées,*
  $$z_1=\frac{-b-i\sqrt{-\Delta}}{2a} \quad et \quad z_2=\frac{-b+i\sqrt{-\Delta}}{2a}.$$

Ainsi, le trinôme se factorise toujours $az^2+bz+c=a(z-z_1)(z-z_2)$ où z_1 et z_2 sont ses deux racines, éventuellement complexes ou confondues.

Remarques : • L'ensemble des nombres complexes n'est pas ordonné : on ne peut pas comparer (raisonnablement) deux complexes z et z'(cf. exercice 6 p.13). Cela n'a donc pas de sens de dresser un *tableau de signes* du trinôme complexe.

• De même, si le polynôme est à coefficients complexes, le discriminant est aussi complexe et l'on ne peut le comparer à 0 : le critère ne fonctionne plus.

Démonstration : Les règles de calcul étant les mêmes dans $\mathbb{C}$ et dans $\mathbb{R}$, on obtient la forme canonique suivante.
$$az^2+bz+c=a\left[\left(z+\frac{b}{2a}\right)^2-\frac{\Delta}{4a^2}\right]$$

• Si $\Delta\geqslant 0$, on peut directement utiliser la troisième identité remarquable pour factoriser cette forme canonique et obtenir dans $\mathbb{C}$ le résultat déjà connu dans $\mathbb{R}$.

• Si $\Delta<0$, $-\Delta>0$ et l'on peut écrire
$$\left(z+\tfrac{b}{2a}\right)^2-\tfrac{\Delta}{4a^2}=\left(z+\tfrac{b}{2a}\right)^2-\tfrac{i^2(-\Delta)}{4a^2}=\left(z+\tfrac{b}{2a}\right)^2-\left(\tfrac{i\sqrt{-\Delta}}{2a}\right)^2$$
$$=\left(z-\tfrac{-b}{2a}-\tfrac{i\sqrt{-\Delta}}{2a}\right)\left(z-\tfrac{-b-i\sqrt{-\Delta}}{2a}\right)$$ □

Exemples : ◦ Soit le trinôme $P(z) = z^2 + 2z + 2$ de discriminant $\Delta = -4 < 0$ et donc de racines complexes $z_1 = \frac{-2-i\sqrt{-(-4)}}{2\times 1} = -1 - i$ et $z_2 = \overline{z_1} = -1 + i$. Ainsi, pour tout z, $P(z) = (z - (-1 - i))(z - (-1 + i) = (z + 1 + i)(z + 1 - i)$.

◦ Soit $Q(z) = z^3 - 1$. $z = 1$ étant une racine de Q, on peut écrire $Q(z) = (z - 1)(az^2 + bz + c)$. Avant développement, on remarque que l'on doit avoir $a = 1$ et $c = 1$ pour que les coefficients « extrêmes » coïncident. Puisque $(z-1)(z^2+bz+1) = z^3 + bz^2 + z - z^2 - bz - 1 = z^3 + (b - 1)z^2 + (1 - b)z - 1$, on a, en identifiant les coefficients deux à deux, $b-1 = 0$ et $1-b = 0$ d'où $b = 1$ et $Q(z) = (z - 1)(z^2 + z + 1)$. Ce polynôme du second degré est de discriminant $\Delta = 1^2 - 4 = -3 < 0$ donc il admet deux racines complexes conjuguées distinctes $\frac{-1\pm i\sqrt{3}}{2}$ et Q peut alors se factoriser : $Q(z) = (z - 1)(z + \frac{1+i\sqrt{3}}{2})(z + \frac{1-i\sqrt{3}}{2})$.

◦ Résolution dans $\mathbb{C}$ l'équation (E) $z^4 + 9z^2 + 20 = 0$.

Posons $Z = z^2$. On a $(E) \iff Z^2 + 9Z + 20 = 0$ de discriminant $\Delta = 9^2 - 4 \times 20 = 1 > 0$ d'où les deux solutions $Z_1 = \frac{-9-\sqrt{1}}{2} = -5$ et $Z_2 = -4$. On cherche alors à résoudre les équations $z_1^2 = -5$ et $z_2^2 = -4$ qui nous donnent les solutions de (E) : $z_{1,1} = i\sqrt{5}$, $z_{1,2} = -i\sqrt{5}$, $z_{2,1} = 2i$ et $z_{2,2} = -2i$.

Le théorème 1 permet donc de résoudre dans $\mathbb{C}$ toutes les équations du second degré à coefficients réels.

Il est en fait démontré que tout trinôme du second degré à coefficients complexes admet aussi des racines dans $\mathbb{C}$ et même, que tout polynôme non constant à coefficients complexes admet des racines dans $\mathbb{C}$. Il en admet même autant que son degré, certaines pouvant être confondues. On dit que $\mathbb{C}$ est un corps *algébriquement clos*. Ce résultat est connu sous le nom de « théorème fondamental de l'algèbre » ou de « théorème de d'Alembert-Gauss » et il aura fallu près d'un siècle et de multiples tentatives avant d'en obtenir des démonstrations rigoureuses, au début du XIXᵉ s. Regardons d'un peu plus près ce qu'il en est.

3 Équations du second degré à coefficients complexes

Une équation du second degré à coefficients complexes admet toujours deux solutions, éventuellement confondues.
Il s'avère que, pour $\alpha \in \mathbb{C}$, l'équation $z^2 = \alpha$ admet toujours des solutions : le nombre $\pm\sqrt{|\alpha|}\, e^{i\,\frac{\arg(\alpha)}{2}}$ convient mais nous ne connaissons pas encore la notation exponentielle alors nous justifierons l'existence d'une solution en utilisant la forme algébrique dans l'exercice 9 en page 51. Ainsi, pour tous a, b et $c \in \mathbb{C}$, il existe (au moins) une racine carrée $\delta \in \mathbb{C}$ du discriminant $\delta^2 = \Delta = b^2 - 4ac \in \mathbb{C}$. La même forme canonique que dans le cas des coefficients réels mène alors aux deux racines $\dfrac{-b \pm \delta}{2a}$ de l'équation $az^2 + bz + c = 0$. Il est à noter que ces deux racines complexes ne sont plus nécessairement conjuguées.

La notation $\sqrt{\ }$ n'est pas utilisée dans $\mathbb{C}$ pour différents problèmes de définition, continuité, détermination... Parfois, cela désigne l'ensemble de toutes les racines du radicande.

Exemples : ◦ $\delta = 1+i$ est solution de l'équation $z^2 = (1+i)^2 = 2i$.
◦ L'équation $\frac{1}{2}z^2 + (\sqrt{2} + i\sqrt{2})z + i = 0$ a pour discriminant $\Delta = (\sqrt{2}+i\sqrt{2})^2 - 4\frac{1}{2}i = 2i$ et donc pour solutions
$z_1 = \frac{-(\sqrt{2}+i\sqrt{2})-(1+i)}{2.\frac{1}{2}} = -1-\sqrt{2}+i(-1-\sqrt{2})$ et $z_2 = 1-\sqrt{2}+i(1-\sqrt{2})$.

4 Formule du binôme de Newton

La formule suivante sera démontrée par récurrence dans l'exercice n° 2.

Théorème 2 ***Binôme de Newton***
Pour tous nombres complexes u et v et pour tout entier naturel n, on a

$$\boldsymbol{(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^{n-k} v^k}.$$

Les nombres $\binom{n}{k}$ sont les *coefficients binomiaux* que vous définirez plus précisément en cours de spécialité. Il nous suffit ici de savoir que $\binom{n}{k}$ est le nombre de choix possibles de k objets parmi n. Ils vérifient $\binom{n}{n-k} = \binom{n}{k}$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ et $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ (triangle de Pascal). On pourra parfois utiliser la calculatrice pour les obtenir (math - probas - combinaison).

Exemples : ◦ $\binom{7}{1} = 7$ ◦ $\binom{9}{0} = 1$ ◦ $\binom{5}{4} = 5$ ◦ $\binom{4}{2} = 6$ ◦ $\binom{5}{3} = 10$ ◦ $\binom{17}{12} = 6188$

◦ $(2+i)^3 = \sum\limits_{k=0}^{3} \binom{3}{k} 2^{3-k} i^k = \binom{3}{0}2^3 i^0 + \binom{3}{1}2^2 i^1 + \binom{3}{2}2^1 i^2 + \binom{3}{3}2^0 i^3$
$= 1\times 8 + 3\times 4i + 3\times 2(-1) + 1\times 1(-i) = 2+11i$.

◦ $(1-i)^5 = \sum\limits_{k=0}^{5} \binom{5}{k} 1^{5-k}(-i)^k$
$= \binom{5}{0}(-i)^0 + \binom{5}{1}(-i)^1 + \binom{5}{2}(-i)^2 + \binom{5}{3}(-i)^3 + \binom{5}{4}(-i)^4 + \binom{5}{5}(-i)^5$
$= 1\times 1 + 5(-i) + 10(-1) + 10\times i + 5\times 1 + 1\times(-i) = 4i-4$.

5 Équations polynomiales

Définition 1 *Soit n un entier naturel et $a_0, \ldots, a_n$ des nombres réels (ou complexes) tels que $a_n \neq 0$.*
La fonction P définie sur $\mathbb{C}$ par $P(z) = a_0 + a_1 z + \ldots + a_n z^n = \sum\limits_{k=0}^{n} a_k z^k$ *est appelée fonction polynôme (ou plus simplement polynôme) de degré* $\deg(P) = n$.
L'équation $P(z) = 0$ est appelée équation polynomiale de degré n dont toute solution est appelée racine de P.

Remarque : On admettra que si une fonction polynôme est identiquement nulle ($\forall z \in \mathbb{C}$, $P(z) = 0$), alors tous ses coefficients le sont aussi ($\forall k \in \mathbb{N}$, $a_k = 0$). On définit ainsi le polynôme nul et son degré est parfois donné par $-\infty$.

Exemples : ◦ $P(z) = 4 - 2z^3 + z^5$ est un polynôme unitaire ($a_n = 1$) de degré 5.
- ◦ $P(z) = 2$ est un polynôme constant, de degré 0.
- ◦ $P(z) = 5z^7$ est un monôme de degré 7.

Définition 2 *Soient P et Q deux polynômes. On dit que P est factorisable (ou divisible) par Q s'il existe un polynôme R tel que* $P = QR$
c.-à-d. $\forall z \in \mathbb{C},\ P(z) = Q(z)R(z)$.
On a alors $\deg(P) = \deg(Q) + \deg(R)$.

Exemple : $z^2 + 9$ est factorisable par $z - 3i$ et par $z + 3i$.

Propriété 1 *Soient z et a deux nombres complexes et n un entier naturel non nul.*
On a $\boldsymbol{z^n - a^n = (z-a)\sum_{k=0}^{n-1} a^k z^{n-1-k}}$.

Démonstration : En développant, on obtient

$$\begin{aligned}
(z-a)\sum_{k=0}^{n-1} a^k z^{n-1-k} &= z\sum_{k=0}^{n-1} a^k z^{n-1-k} - a\sum_{k=0}^{n-1} a^k z^{n-1-k} \\
&= \sum_{k=0}^{n-1} a^k z^{n-k} - \sum_{k=0}^{n-1} a^{k+1} z^{n-1-k} \\
&= \left(a^0 z^{n-0} + a^1 z^{n-1} + a^2 z^{n-2} + \ldots + a^{n-2} z^{n-(n-2)} + a^{n-1} z^{n-(n-1)}\right) \\
&\qquad - \left(a^1 z^{n-1} + a^2 z^{n-2} + \ldots + a^{n-1} z^{n-(n-1)} + a^n z^{n-n}\right) \\
&= \left(z^n + az^{n-1} + a^2 z^{n-2} + \ldots + a^{n-2} z^2 + a^{n-1} z\right) \\
&\qquad - \left(az^{n-1} + a^2 z^{n-2} + \ldots + a^{n-1} z + a^n\right) \\
&= z^n - a^n \quad \text{par } \textit{téléscopage} \text{ des termes deux à deux.}
\end{aligned}$$

On aurait pu aussi se souvenir avec plaisir de la formule $1 + q + q^2 + \ldots + q^{n-1} = \frac{1-q^n}{1-q}$, remplacer q par $\frac{a}{z}$ puis multiplier par z^n. □

Exemples : ◦ $z^3 - 8 = z^3 - 2^3 = (z-2)\sum_{k=0}^{2} 2^k z^{2-k} = (z-2)(z^2 + 2z + 4)$.
- ◦ $z^5 + 1 = z^5 - (-1)^5 = (z - (-1))\sum_{k=0}^{4} (-1)^k z^{4-k} = (z+1)(z^4 - z^3 + z^2 - z + 1)$.

Ce résultat montre que la racine triviale a de $z^n - a^n$ permet une factorisation par $z - a$. Le théorème suivant généralise ceci à tous les polynômes.

Théorème 3 *Soit P un polynôme de degré supérieur ou égal à 1 et soit $a \in \mathbb{C}$*
P se factorise par $z - a$, c.-à-d. qu'il existe un polynôme Q de degré $\deg(Q) = \deg(P) - 1$ *tel que pour tout $z \in \mathbb{C}$,* $P(z) = (z-a)Q(z)$,
si, et seulement si, a est une racine de P, c.-à-d. $P(a) = 0$.

Démonstration : Trivialement, tout polynôme $(z-a)Q(z)$ admet a pour racine.
Réciproquement, soit $P(z)=\sum_{k=0}^{n}\alpha_k z^k$ un polynôme non nul s'annulant en a.
On a , pour tout $z\in\mathbb{C}$,

$$\begin{aligned}
P(z) &= P(z)-P(a) = \sum_{k=0}^{n}\alpha_k z^k-\sum_{k=0}^{n}\alpha_k a^k = \sum_{k=0}^{n}\alpha_k(z^k-a^k)\\
&= \alpha_0(z^0-a^0)+\sum_{k=1}^{n}\alpha_k(z^k-a^k) = 0+\sum_{k=1}^{n}\alpha_k\left[(z-a)\sum_{p=0}^{k-1}a^p z^{k-1-p}\right]\\
&= (z-a)\sum_{k=1}^{n}\alpha_k\left[\sum_{p=0}^{k-1}a^p z^{k-1-p}\right]\\
&= (z-a)\sum_{k=1}^{n}\alpha_k(z^{k-1}+az^{k-2}+\ldots+a^{k-1}) = (z-a)Q(z)
\end{aligned}$$

où $\deg(Q)=n-1$. □

Corollaire
Tout polynôme non nul de degré $n\in\mathbb{N}$ admet au plus n racines distinctes.

Remarques : • Ceci signifie aussi que le nombre de solutions d'une équation polynomiale est inférieur ou égal à son degré.

• Ainsi, un polynôme de degré inférieur ou égal à n s'annulant pour au moins $n+1$ racines distinctes est nécessairement le polynôme nul.

• Le théorème fondamental de l'algèbre affirme même qu'un polynôme non nul admet autant de racines, avec multiplicité, que son degré dans $\mathbb{C}$. Il est très utile mais dépasse malheureusement notre programme.

Exemple : Le seul polynôme unitaire de degré 3 s'annulant en 0, -7 et i est $z(z+7)(z-i)$.

Démonstration : Procédons par récurrence. Soit $\mathscr{P}_n$, pour $n\in\mathbb{N}$, la proposition « Un polynôme non nul de degré n admet au plus n racines distinctes. »
· Un polynôme non nul de degré 0 est une fonction constante non nulle et n'admet donc aucune racine : la proposition $\mathscr{P}_0$ est vraie.
· Supposons que la proposition $\mathscr{P}_k$ soit vraie pour un certain $k\in\mathbb{N}$ (hypothèse de récurrence) et montrons que la proposition suivante, $\mathscr{P}_{k+1}$, est alors vraie.
Soit donc P un polynôme de degré $\deg(P)=k+1$.
S'il n'admet pas de racine alors il en admet bien moins que son degré.
Sinon, on appelle a une de ses racines. D'après le théorème 3, il se factorise par $z-a$ et il existe un polynôme Q de degré $\deg(Q)=\deg(P)-1=(k+1)-1=k$ tel que $P=(z-a)Q$. D'après l'hypothèse de récurrence, Q n'admet pas plus de k racines distinctes et donc P n'en admet pas plus que $k+1$, celles de Q et a éventuellement. La proposition $\mathscr{P}_{k+1}$ est donc vraie.
· Donc, si une telle proposition est vraie, la suivante l'est aussi. Puisque $\mathscr{P}_0$, est vraie, $\mathscr{P}_1$ est vraie donc $\mathscr{P}_2$ est vraie, donc … $\mathscr{P}_n$ est vraie pour tout $n\in\mathbb{N}$. □

Exercices

NOMBRES COMPLEXES : ÉQUATIONS POLYNOMIALES

Exercice 1 Résoudre dans $\mathbb{C}$ les équations d'inconnue z suivantes.

(a) $2iz^2 + 3z = 0$

(b) $2z^2 - 6z + 5 = 0$

(c) $z^2 + z + 1 = 0$

(d) $2z^2 + 2z + 5 = 0$

(e) $z^2 - (1 + \sqrt{3})z + \sqrt{3} = 0$

(f) $(z^2 + 2)(z^2 - 4z + 4) = 0$

(g) $\dfrac{z-3}{z-2} = z$

(h) $z^2 - 2(1 + \sqrt{2})z + 2(\sqrt{2} + 2) = 0$

(i) $z^3 + z^2 - 2 = 0$

(j) $z^3 - 5z^2 + 9z - 9 = 0$

(k) $z^4 - 2z^2 - 3 = 0$

(l) $z^5 - 2z = 4z^3 + 3z$

Exercice 2 Binôme de Newton

Étudions la démonstration de la propriété $\mathscr{P}_n\colon (a+b)^n = \displaystyle\sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$.

1. Montrer que $\mathscr{P}_0$ est vraie.
2. On suppose que $\mathscr{P}_k$ est vraie pour un certain $k \in \mathbb{N}$.
   Décrire chacune des étapes du calcul suivant.

$$(a+b)^{k+1} \overset{(1)}{=} (a+b)(a+b)^k \overset{(2)}{=} (a+b)\sum_{p=0}^{k}\binom{k}{p}a^p b^{k-p}$$

$$\overset{(3)}{=} a\sum_{p=0}^{k}\binom{k}{p}a^p b^{k-p} + b\sum_{p=0}^{k}\binom{k}{p}a^p b^{k-p}$$

$$\overset{(4)}{=} \sum_{p=0}^{k}\binom{k}{p}a^{p+1} b^{k-p} + \sum_{p=0}^{k}\binom{k}{p}a^p b^{k+1-p}$$

$$\overset{(5)}{=} \sum_{p=0}^{k-1}\binom{k}{p}a^{p+1} b^{k-p} + \binom{k}{k}a^{k+1}b^0 + \binom{k}{0}a^0 b^{k+1-0} + \sum_{p=1}^{k}\binom{k}{p}a^p b^{k+1-p}$$

$$\overset{(6)}{=} \sum_{p=1}^{k}\binom{k}{p-1}a^{p} b^{k-p+1} + a^{k+1} + b^{k+1} + \sum_{p=1}^{k}\binom{k}{p}a^p b^{k+1-p}$$

$$\overset{(7)}{=} b^{k+1} + \sum_{p=1}^{k}\left(\binom{k}{p-1} + \binom{k}{p}\right)a^p b^{k+1-p} + a^{k+1}$$

$$\overset{(8)}{=} \binom{k+1}{k+1}a^0 b^{k+1} + \sum_{p=1}^{k}\binom{k+1}{p}a^p b^{k+1-p} + \binom{k+1}{0}a^{k+1}b^0$$

EXERCICES

$$\overset{(9)}{=} \quad \sum_{p=0}^{k+1} \binom{k+1}{p} a^p b^{k+1-p}$$

3. Conclure.

Exercice 3 Factorisations

1. Factoriser les polynômes suivants sous la forme $(z-a)P(z)$.

$A(z) = z^3 + 1$	$C(z) = z^3 + i$
$B(z) = z^3 - 64$	$D(z) = z^5 - 32i$

2. Factoriser les polynômes suivants en produits de facteurs de la forme $(z-a)$.

$A(z) = z^3 + 4z$	$C(z) = z^4 - 1$
$B(z) = z^3 - 2z^2 + z - 2$	$D(z) = z^5 - z^4 + 5z^3 - 5z^2 + 4z - 4$

Exercice 4 Résolution d'une équation
On pose $P(z) = z^4 - 6z^3 + 23z^2 - 34z + 26$.

1. (a) α est un nombre complexe quelconque. Démontrer que $P\left(\overline{\alpha}\right) = \overline{P(\alpha)}$.
   (b) En déduire que si $P(\alpha) = 0$ alors $P\left(\overline{\alpha}\right) = 0$.
2. Calculer $P(1+i)$ puis indiquer deux solutions complexes de l'équation $P(z) = 0$.
3. On pose $Q(z) = [z-(1+i)]\,[z-(1-i)]$.
   Vérifier que $P(z)$ est le produit du polynôme $Q(z)$ et d'un polynôme $R(z)$ du second degré que l'on déterminera. Résoudre ensuite dans $\mathbb{C}$ l'équation $P(z) = 0$.

Exercice 5 The quadratic equation $az^2 + bz + 10i = 0$, where a and b are real, has a root : $3 - i$. Determine the other root of the equation, giving the answer in the algebraic form $p + iq$.

Exercice 6 Division des polynômes
Soit le polynôme défini par $P(z) = z^4 - 4z^2 - z + 2$

1. Vérifier que 2 est racine de P.
2. Justifier que P peut s'écrire sous la forme $(z-2)(z^3 + Q(z))$ où $\deg(Q) \leqslant 2$.
3. En déduire une expression de $(z-2)Q(z)$ puis justifier que Q peut s'écrire sous la forme $2z^2 + R(z)$ où $\deg(R) \leqslant 1$.
4. Déterminer R puis en déduire une factorisation de P.
5. Présenter cette méthode sous la forme d'une « division potence » puis l'appliquer afin de factoriser le polynôme $2z^4 - 5z^3 + 4z^2 - 3z + 2$.
6. Factoriser entièrement le polynôme $3z^4 + 12z^3 - 57z^2 - 138z + 360$ en utilisant la méthode de la division potence.

Exercice 7 Soit P le polynôme défini par $P(z) = z^3 - (4+i)z^2 + (5+4i)z - 5i$.
Déterminer une racine imaginaire pure de P, factoriser P puis résoudre l'équation $P(z) = 0$.

Exercice 8 Formules de Viètes
Nous admettrons les formules suivantes qui généralisent une propriété vue en première.

> **Propriété** *Soit* $\sum_{k=0}^{n} \alpha_k z^k = \alpha_0 + \alpha_1 z + \ldots + \alpha_n z^n$ *un polynôme de degré* $n \in \mathbb{N}^*$ *à coefficients réels.*
> *La somme de toutes ses racines (avec multiplicité) est égale à* $-\frac{\alpha_{n-1}}{\alpha_n}$.
> *Le produit de toutes ses racines (avec multiplicité) est égal à* $(-1)^n \frac{\alpha_0}{\alpha_n}$.

1. Rappeler la propriété similaire concernant le polynôme $x^2 - sx + p$.
2. Déterminer le polynôme unitaire du second degré s'annulant en $1 + 2i$ et $1 - 2i$.
3. Déterminer les nombres z_1 et z_2 vérifiant les conditions suivantes.
   (a) $z_1 + z_2 = 6, \ \ z_1 z_2 = 13$
   (b) $z_1 + z_2 = -1, \ \ z_1 z_2 = \frac{5}{4}$
   (c) $z_1 + z_2 = -\sqrt{2}, \ \ z_1 z_2 = 1$
4. Existe-t-il une équation du second degré ayant pour solutions $2019 + i$ et $2019 - i$?

Exercice 9 Existence des solutions de l'équation $z^2 = c$ sous forme algébrique

1. En posant $z = \alpha + i\beta$ et $c = a + ib$, déterminer le système d'équation liant ces quatre réels.
2. (a) En supposant que $\alpha \neq 0$, montrer que l'on doit avoir $4\alpha^4 - 4a\alpha^2 - b^2 = 0$.
   (b) Résoudre l'équation $4S^2 - 4aS - b^2 = 0$ puis justifier l'existence d'une solution à l'équation en α.
3. Que dire du cas $\alpha = 0$?
4. Conclure.
5. Résoudre l'équation $z^2 + (3i - 4)z + 1 - 7i = 0$ en cherchant un nombre δ de carré son discriminant.

Exercice 10 Soit P le polynôme défini par $P(z) = z^4 + 2z^3 - z^2 + 2z + 1$.

1. Vérifier que 0 n'est pas une racine de P.
2. Soit $z \neq 0$. On pose $Z = z + \frac{1}{z}$.
   (a) Exprimer $Z^2 - 3$ en fonction de z.
   (b) Calculer $\frac{P(z)}{z^2}$ et l'exprimer en fonction de Z.
3. Déterminer la forme algébrique des racines de P.

Rendez-vous en page 283 afin de réaliser le devoir n° 3.

EXERCICES

Corrigé des exercices

NOMBRES COMPLEXES : ÉQUATIONS POLYNOMIALES

Exercice 1 Résolution dans $\mathbb{C}$.

(a) $2iz^2 + 3z = 0 \iff z(2iz+3) = 0 \iff z = 0$ ou $2iz + 3 = 0$
$\iff z = 0$ ou $z = -\frac{3}{2i} = \frac{3}{2}i$

(b) $2z^2 - 6z + 5 = 0$: $\Delta = -4$ d'où les deux solutions complexes conjuguées $z_{1,2} = \frac{6 \pm i\sqrt{4}}{2\times 2} = \frac{3}{2} \pm \frac{i}{2}$.

(c) $z^2 + z + 1 = 0$: $\Delta = -3$ d'où les deux solutions complexes conjuguées $z_{1,2} = \frac{-1 \pm i\sqrt{3}}{2}$.

(d) $2z^2 + 2z + 5 = 0$: $\Delta = -36$ d'où les deux solutions complexes conjuguées $z_{1,2} = \frac{-2 \pm i\sqrt{36}}{2\times 2} = -\frac{1}{2} \pm \frac{3}{2}i$.

(e) $z^2 - (1+\sqrt{3})z + \sqrt{3} = 0 \iff (z-1)(z-\sqrt{3}) = 0 \iff z = 1$ ou $z = \sqrt{3}$

(f) $(z^2+2)(z^2-4z+4) = 0 \iff (z - i\sqrt{2})(z + i\sqrt{2})(z-2)^2 = 0$
$\iff z \in \{2\,;\,-i\sqrt{2}\,;\,i\sqrt{2}\}$

(g) $\frac{z-3}{z-2} = z \overset{z\neq 2}{\iff} z - 3 = z(z-2) \iff z^2 - 3z + 3 = 0$: $\Delta = -3$ d'où
$z \in \left\{\frac{3-i\sqrt{3}}{2}\,;\,\frac{3+i\sqrt{3}}{2}\right\}$ $(\neq 2)$.

(h) $z^2 - 2(1+\sqrt{2})z + 2(\sqrt{2}+2) = 0$: $\Delta = \ldots = -4$ d'où $z_{1,2} = \frac{2(1+\sqrt{2}) \pm i\sqrt{4}}{2}$ et $z \in \{1 + \sqrt{2} \pm i\}$

(i) $P(z) = z^3 + z^2 - 2$: on a $P(1) = 1 + 1 - 2 = 0$ donc $z_0 = 1$ est une racine évidente et l'on peut écrire $P(z) = (z-1)(az^2 + bz + c)$.
En observant les coefficients « extrêmes » , on obtient $a = 1$ et $c = 2$.
Trouvons b : $(z-1)(z^2 + bz + 2) = z^3 + (b-1)z^2 + (2-b)z - 2$ et l'on doit avoir $b - 1 = 1\,;\,2 - b = 0$ *i.e.* $b = 2$ d'où $P(z) = (z-1)(z^2+2z+2)$.
Puisque $\Delta = 2^2 - 4\times 2 = -4 < 0$, ce polynôme du second degré admet deux racines complexes conjuguées $z_{1,2} = \frac{-2 \pm i\sqrt{4}}{2\times 1} = -1 \pm i$ et les solutions de l'équation sont $\{1\,;\,1-i\,;\,1+i\}$.

(j) $Q(z) = z^3 - 5z^2 + 9z - 9$: on a $Q(3) = 3^3 - 5\times 3^2 + 9\times 3 - 9 = 0$ donc $z_0 = 3$ est une racine évidente et l'on peut écrire $Q(z) = (z-3)(az^2+bz+c)$.
En observant les coefficients « extrêmes » , on obtient $a = 1$ et $c = 3$.
Trouvons b : $(z-3)(z^2+bz+3) = z^3 + (b-3)z^2 + (3-3b)z - 9$ et l'on doit avoir $b - 3 = -5\,;\,3 - 3b = 9$ *i.e.* $b = -2$ d'où $Q(z) = (z-3)(z^2-2z+3)$.
Puisque $\Delta = 2^2 - 4\times 3 = -8 < 0$, ce polynôme du second degré admet deux racines complexes conjuguées $z_{1,2} = \frac{-(-2) \pm i\sqrt{8}}{2\times 1} = 1 \pm i\sqrt{2}$ et les solutions de l'équation sont $\{3\,;\,1 - i\sqrt{2}\,;\,1 + i\sqrt{2}\}$.

(k) $R(z) = z^4 - 2z^2 - 3$. Posons $Z = z^2$. On a $R(z) = Z^2 - 2Z - 3$ de racine évidente -1 et de première factorisation $(Z+1)(Z-3)$ d'où $R(z) = (z^2+1)(z^2-3)$ et les solutions évidentes $\{-i\,;\, i\,;\, -\sqrt{3}\,;\, \sqrt{3}\}$.

(l) $z^5 - 2z = 4z^3 + 3z \iff z^5 - 4z^3 - 5z = 0 \iff z(z^4 - 4z^2 - 5) = 0$. Posons $Z = z^2$. On a $z^4 - 4z^2 - 5 = 0 \iff Z^2 - 4Z - 5 = 0$ de discriminant $\Delta = 36$ et donc de racines réelles $Z_1 = \frac{4-\sqrt{36}}{2} = -1$ et $Z_2 = \frac{4+6}{2} = 5$. Ainsi, $Z^2 - 4Z - 5 = (Z+1)(Z-5) = (z^2+1)(z^2-5) = (z-i)(z+i)(z-\sqrt{5})(z+\sqrt{5})$ d'où les solutions de l'équation $\{-\sqrt{5}\,;\, 0\,;\, \sqrt{5}\,;\, -i\,;\, i\}$.

Exercice 2 Binôme de Newton : pour $ab \neq 0$, $\mathscr{P}_n\colon (a+b)^n = \displaystyle\sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$.

1. $(a+b)^0 = 1$ et $\displaystyle\sum_{p=0}^{0} \binom{0}{p} a^p b^{0-p} = \binom{0}{0} a^0 b^0 = 1 \times 1 \times 1 = 1$. $\mathscr{P}_0$ est vraie.
2. On suppose que $\mathscr{P}_k$ est vraie pour un certain $k \in \mathbb{N}$.
   Voici la description des différentes étapes.
   Étape (1) : évidente ; Étape (2) : hypothèse de récurrence ; Étape (3) : développement du facteur somme sur $(a+b)$; Étape (4) : développements des facteurs a et b sur les sommes ; Étape (5) : sortie du dernier et du premier termes des sommes ; Étape (6) : décalage d'indice dans la première somme ; Étape (7) : factorisation par $a^p b^{k+1-p}$; Étape (8) : formule du triangle de Pascal $\binom{k}{p-1} + \binom{k}{p} = \binom{k+1}{p}$ et $\binom{k+1}{k+1} = \binom{k+1}{0} = 1$; Étape (9) : regroupement des premier et dernier termes dans la somme.
3. Le calcul précédent montre que la propriété $\mathscr{P}_n$ est héréditaire. Puisqu'elle est vraie pour $n = 0$, elle est vraie pour tout entier naturel.

Exercice 3 Factorisations

1.
   - $A(z) = z^3 + 1 = z^3 - (-1)^3$ s'annule en $z = -1$ et se factorise donc par $z+1$. Cherchons un polynôme P tel que $A(z) = (z+1)P(z)$. P est donc du second degré et en observant les termes « extrêmes », on peut écrire $P(z) = z^2 + bz + 1$. En développant, on trouve $(z+1)(z^2+bz-1) = z^3 + (b+1)z^2 + (b+1)z + 1$ et l'on doit avoir $b+1 = 0$. D'où la factorisation $A(z) = (z+1)(z^2 - z + 1)$.
   - $B(z) = z^3 - 64 = z^3 - 4^3$ s'annule en $z = 4$ et se factorise donc par $z - 4$. Cherchons un polynôme Q tel que $B(z) = (z-4)Q(z)$. Q est donc du second degré et en observant les termes « extrêmes », on peut écrire $Q(z) = z^2 + bz + 16$. En développant, $(z-4)(z^2 + bz + 16) = z^3 + (b-4)z^2 + (16-4b)z - 64$ et l'on doit avoir $b - 4 = 0$ et $16 - 4b = 0$: $b = 4$. D'où la factorisation $B(z) = (z-4)(z^2 + 4z + 16)$.
   - $C(z) = z^3 + i = z^3 - i^3$ s'annule en $z = i$ et se factorise donc par $z - i$. Cherchons un polynôme R tel que $C(z) = (z-i)R(z)$. R est donc du second degré et en observant les termes « extrêmes », on peut écrire $R(z) = z^2 + bz - 1$. En développant, on trouve $(z-i)(z^2 + bz - 1) = z^3 + (b-i)z^2 + (-1-ib)z + i$ et l'on doit avoir $b - i = 0$ et $-1 - ib = 0$: $b = i$. D'où la factorisation $C(z) = (z-i)(z^2 + iz - 1)$.

CORRIGÉS

- $D(z) = z^5 - 32i = z^5 - (2i)^5$ s'annule en $z = 2i$ et se factorise donc par $z - 2i$. Cherchons un polynôme S tel que $D(z) = (z-2i)S(z)$. S est donc du quatrième degré et en observant les termes « extrêmes », on peut écrire $S(z) = z^4 + bz^3 + cz^2 + dz + 16$. En développant, on trouve
$$(z-2i)(z^4 + bz^3 + cz^2 + dz + 16)$$
$$= z^5 + (b-2i)z^4 + (c-2ib)z^3 + (d-2ic)z^2 + (16-2id)z - 32i$$
et l'on doit avoir $b - 2i = c - 2ib = d - 2ic = 16 - 2id = 0$ d'où $b = 2i$, $c = 2ib = -4$, $d = 2ic = -8i$. On obtient la factorisation
$$D(z) = (z-2i)(z^4 + 2iz^3 - 4z^2 - 8iz + 16).$$

2. - $A(z) = z^3 + 4z = z(z^2+4) = z(z^2 - (2i)^2) = (z-0)(z-2i)(z+2i)$.
   - $B(z) = z^3 - 2z^2 + z - 2$ s'annule en $z = 2$ et se factorise donc par $z-2$. Cherchons un polynôme Q tel que $B(z) = (z-2)Q(z)$. Q est donc du second degré et en observant les termes « extrêmes », on peut écrire $Q(z) = z^2 + bz + 1$. En développant, on trouve $(z-2)(z^2+bz+1) = z^3 + (b-2)z^2 + (1-2b)z - 2$ et l'on doit avoir $b - 2 = -2$ et $1 - 2b = 1$: $b = 0$.
   D'où $B(z) = (z-2)(z^2+4) = (z-2)(z^2-(2i)^2) = (z-2)(z-2i)(z+2i)$.
   - $C(z) = z^4 - 1 = z^4 - 1^4 = (z-1)\displaystyle\sum_{k=0}^{4-1} a^k z^{n-1-k} = (z-1)(z^3+z^2+z+1)$
   $C(z) = (z-1)(z-(-1))(z^2+bz+1)$ en utilisant la formule de factorisation de $z^n - a^n$ puis en remarquant que -1 est racine de la somme. Après développement du deuxième produit, on obtient $z^3 + z^2 + z + 1 = z^3 + (b+1)z^2 + (b+1)z + 1$ donc $b = 0$ et $C(z) = (z-1)(z+1)(z^2+1) = (z-1)(z+1)(z^2-i^2)$
   $C(z) = (z-1)(z+1)(z-i)(z+i)$.
   Sinon, $C(z) = (z^2)^2 - 1^2 = (z^2-1)(z^2+1) = \ldots$
   - $D(z) = z^5 - z^4 + 5z^3 - 5z^2 + 4z - 4$. On remarque que $D(1) = 0$, $D(i) = i^5 - i^4 + 5i^3 - 5i^2 + 4i - 4 = i - 1 - 5i + 5 + 4i - 4 = 0$ et donc $D(\overline{i}) = \overline{D(i)} = 0$.
   On peut donc écrire, en observant les termes « extrêmes »,
   $D(z) = (z-1)(z-i)(z+i)(z^2+bz+4)$ dont le développement donne $z^5 + (b-1)z^4 + (5-b)z^3 + (b-5)z^2 + (4-b)z - 4$ d'où $b = 0$ et $D(z) = (z-1)(z-i)(z+i)(z^2+4) = (z-1)(z-i)(z+i)(z^2-(2i)^2)$
   $D(z) = (z-1)(z-i)(z+i)(z-2i)(z+2i)$.

Exercice 4 $P(z) = z^4 - 6z^3 + 23z^2 - 34z + 26$.

1. (a) $P(\overline{\alpha}) = \overline{\alpha}^4 - 6\overline{\alpha}^3 + 23\overline{\alpha}^2 - 34\overline{\alpha} + 26 = \overline{\alpha^4} - \overline{6\alpha^3} + \overline{23\alpha^2} - \overline{34\alpha} + \overline{26}$
   $= \overline{\alpha^4 - 6\alpha^3 + 23\alpha^2 - 34\alpha + 26} = \overline{P(\alpha)}$.
   (b) Ainsi, $P(\alpha) = 0$ implique $P(\overline{\alpha}) = \overline{P(\alpha)} = \overline{0} = 0$.
2. On a $(1+i)^2 = 1 + 2i - 1 = 2i$, $(1+i)^3 = 2i(1+i) = -2 + 2i$
   et $(1+i)^4 = (2i)^2 = -4$ donc
   $P(1+i) = -4 - 6(-2+2i) + 23 \times 2i - 34(1+i) + 26$
   $= -4 + 12 - 34 + 26 + i(-12 + 46 - 34) = 0$.
   Ainsi, $1+i$ et donc son conjugué $1-i$ sont solutions de l'équation $P(z) = 0$.

3. On a $[z-(1+i)]\,[z-(1-i)]\,[az^2+bz+c]$
$= [z^2-(1-i)z-(1+i)z+(1-i^2)][az^2+bz+c]$
$= az^4+bz^3+cz^2-2az^3-2bz^2-2cz+2az^2+2bz+2c$
$= az^4+(b-2a)z^3+(c-2b+2a)z^2+(-2c+2b)z+2c$
et, en identifiant les coefficients, $a=1$, $b-2a=-6$, $c-2b+2a=23$, $2b-2c=-34$ et $2c=26$.
D'où, $c=13$, $b=-6+2=-4$ $(c-2b+2a=13+8+2=23$ et $2b-2c=-8-26=-34)$.
Ainsi, $P(z)=[z^2-(1-i)z-(1+i)z+(1-i^2)][z^2-4z+13]$. $\Delta=-36$ donc R a pour racines $z_{1,2}=\frac{4\pm i\sqrt{36}}{2}=2\pm 3i$ et les solutions de l'équation $P(z)=0$ sont $1+i$, $1-i$, $2+3i$ et $2-3i$.

Exercice 5 $a(3-i)^2+b(3-i)+10i=0 \iff (8a+3b)+i(10-6a-b)=0$ $\iff a=3$ and $b=-8$. Hence, $3z^2-8z+10i=(z-(3-i))(3z+c)$ and $-(3-i)c=10i \iff c=\frac{10i}{-3+i}=1-3i$.
So, $3z^2-8z+10i=3(z-(3-i))(z+\frac{c}{3})=3(z-(3-i))(z-(i-\frac{1}{3}))$.
Hence, the other root is $i-\frac{1}{3}$.

Exercice 6 Soit le polynôme défini par $P(z)=z^4-4z^2-z+2$

1. On a bien $P(2)=2^4-4\times 2^2-2+2=0$.
2. P peut donc se factoriser par $z-2$ et, en observant les termes de plus haut degré, on peut écrire $(z-2)(z^3+Q(z))$ où $\deg(Q)\leqslant 2$.
3. On a $z^4-4z^2-z+2=P(z)=(z-2)(z^3+Q(z))=z^4-2z^3+(z-2)Q(z)$ d'où $(z-2)Q(z)=2z^3-4z^2-z+2$. En observant les termes de plus haut degré, Q peut s'écrire sous la forme $2z^2+R(z)$ où $\deg(R)\leqslant 1$.
4. On a $2z^3-4z^2-z+2=(z-2)(2z^2+R(z))=2z^3-4z^2+(z-2)R(z)$ d'où $(z-2)R(z)=-z+2$ et $R(z)=-1$. D'où $P(z)=(z-2)(z^3+Q(z))$
$P(z)=(z-2)(z^3+2z^2+R(z))=(z-2)(z^3+2z^2-1)$.
5. $P(z)=2z^4-5z^3+4z^2-3z+2$ s'annule en 1 et, en étudiant les termes de plus haut degré, on obtient : $P(z)=(z-1)(2z^3+Q(z))=2z^4-2z^3+(z-1)Q(z)$ d'où $(z-1)Q(z)=-3z^3+4z^2-3z+2$ et $Q(z)=-3z^2+R(z)$.
Alors, $-3z^3+4z^2-3z+2=(z-1)Q(z)=(z-1)(-3z^2+R(z))$
$=-3z^3+3z^2+(z-1)R(z)$
et $(z-1)R(z)=z^2-3z+2$: $R(z)=z+b$ et $b=-2$.
Ainsi, $P(z)=(z-1)(2z^3+Q(z))=(z-1)(2z^3-3z^2+R(z))$
$P(z)=(z-1)(2z^3-3z^2+z-2)$
mais tout ceci est bien plus pratique lorsque présenté sous forme de division « potence ».
6. Après avoir remarqué successivement que 2 puis 3 puis -4 sont des racines et avoir effectué les divisions potences correspondantes, on obtient
$3z^4+12z^3-57z^2-138z+360=3(z-2)(z-3)(z+4)(z+5)$.

Exercice 7 $P(z)=z^3-(4+i)z^2+(5+4i)z-5i$.
On a $P(\lambda i)=(\lambda i)^3-(4+i)(\lambda i)^2+(5+4i)\lambda i-5i=-\lambda^3 i+(4+i)\lambda^2+5\lambda i-4\lambda-5i$
$P(\lambda i)=(4\lambda^2-4\lambda)+i(-\lambda^3+\lambda^2+5\lambda-5)=4\lambda(\lambda-1)+i(-\lambda^3+\lambda^2+5\lambda-5)$ qui

CORRIGÉS

s'annule pour $\lambda = 1$ uniquement. Donc $P(i) = 0$ et P se factorise par $z - i$. En observant les termes « extrêmes », on peut écrire $P(z) = (z-i)(z^2 + bz + 5)$ de développement $z^3 + (b-i)z^2 + (5 - ib)z + 5i$ donc $b - i = -(4+i)$ et $5 - ib = 5 + 4i$: $b = -4$ d'où $P(z) = (z-i)(z^2 - 4z + 5)$. Avec $\Delta = -4$, on a les racines supplémentaires $\frac{4 \pm i\sqrt{4}}{2} = 2 \pm i$ et les solutions de l'équation $P(z) = 0$: $\{i\,;\, 2-i\,;\, 2+i\}$.

Exercice 8 Formules de Viètes

1. Le polynôme $x^2 - sx + p$ s'annule en deux nombres de somme s et de produit p.
2. Le polynôme unitaire du second degré s'annulant en $1+2i$ et $1-2i$ est $(z - 1 + 2i)(z - 1 - 2i)$ sous forme factorisée. La somme des racines valant $2 = -\frac{\alpha_1}{\alpha_2} = -\alpha_1$ et leur produit $1^2 - (2i)^2 = 5 = (-1)^2\frac{\alpha_0}{\alpha_2} = \alpha_0$, sa forme développée est $z^2 - 2z + 5$.
3. (a) $z_1 + z_2 = 6$, $z_1 z_2 = 13$: ce sont les racines du polynôme $z^2 - 6z + 13$, de discriminant $\Delta = 36 - 52 = -16$ donc $z_{1,2} = \frac{6 \pm i\sqrt{16}}{2} = 3 \pm 2i$.
   (b) $z_1 + z_2 = -1$, $z_1 z_2 = \frac{5}{4}$: ce sont les racines du polynôme $z^2 + z + \frac{5}{4}$, de discriminant $\Delta = 1 - 5 = -4$ donc $z_{1,2} = \frac{-1 \pm i\sqrt{4}}{2} = \frac{1}{2} \pm i$.
   (c) $z_1 + z_2 = -\sqrt{2}$, $z_1 z_2 = 1$: ce sont les racines du polynôme $z^2 + z\sqrt{2} + 1$, de discriminant $\Delta = 2 - 4 = -2$ donc $z_{1,2} = \frac{-\sqrt{2} \pm i\sqrt{2}}{2} = \frac{\sqrt{2}}{2}(-1 \pm i)$.
4. Puisque $2019 + i + 2019 - i = 4038$ et $(2019 + i)(2019 - i) = 4\,076\,362$, l'équation $z^2 - 4038z + 4\,076\,362 = 0$ a pour solutions $2019 + i$ et $2019 - i$.

Exercice 9 Existence des solutions de l'équation $z^2 = c$ sous forme algébrique

1. En posant $z = \alpha + i\beta$ et $c = a + ib$, on a $z^2 = c \iff (\alpha + i\beta)^2 = a + ib$
$$\iff \alpha^2 - \beta^2 + 2i\alpha\beta = a + ib \iff \begin{cases} \alpha^2 - \beta^2 & = & a \\ 2\alpha\beta & = & b. \end{cases}$$
2. (a) Si $\alpha \neq 0$, on doit avoir $2\alpha\beta = b \Longrightarrow \beta = \frac{b}{2\alpha}$ et $\alpha^2 - \beta^2 = a$ donne $\alpha^2 - (\frac{b}{2\alpha})^2 = a \overset{\times\alpha^2}{\iff} \alpha^4 - \frac{b^2}{4} = a\alpha^2 \overset{\times 4}{\iff} 4\alpha^4 - 4a\alpha^2 - b^2 = 0$.
   (b) Posons $S = \alpha^2$. On a $4\alpha^4 - 4a\alpha^2 - b^2 = 4S^2 - 4aS - b^2$ de discriminant $\Delta = 16a^2 + 16b^2 > 0$ et donc de racines $S_{1,2} = \frac{4a \pm \sqrt{16(a^2+b^2}}{2\times 4} = \frac{a \pm \sqrt{a^2+b^2}}{2}$. Puisque $a + \sqrt{a^2+b^2} \geqslant a + |a|$, au moins l'une de ces racines est positive. Il existe donc un nombre α_0 tel que $\alpha_0^2 = S_1$ qui est donc solution de l'équation $4\alpha^4 - 4a\alpha^2 - b^2 = 0$. En posant $\beta_0 = \frac{b}{2\alpha_0}$, on obtient une solution à l'équation $z^2 = c$.
3. Si $\alpha = 0$, alors $b = 2\alpha\beta = 0$: c est réel et l'équation $-\beta^2 = a \iff \beta^2 = -a$ admet toujours des solutions, $\beta = \pm\sqrt{-a}$ si $a \leqslant 0$ ou $\beta = \pm i\sqrt{a}$ si $a > 0$.
4. Ainsi, l'équation $z^2 = c$ admet toujours des solutions dans $\mathbb{C}$.
5. $P(z) = z^2 + (3i - 4)z + 1 - 7i$ est de discriminant
   $\Delta = (3i-4)^2 - 4(1 - 7i) = 3 - 4i = a + ib$ et cherchons $\delta = \alpha + i\beta$ tel que $\delta^2 = \Delta$. On a $S_{1,2} = \frac{a \pm \sqrt{a^2+b^2}}{2} = \frac{3 \pm \sqrt{3^2+4^2}}{2} = 4 = 2^2$ et -1. Il suffit alors de prendre $\alpha = 2$ et $\beta = \frac{b}{2\alpha} = -\frac{4}{4} = -1$: $\delta = 2 - i$ a bien pour carré $\delta^2 = \Delta$ et P s'annule en $z_1 = \frac{-(3i-4)+i\delta}{2\times 1} = \frac{-3i+4+i(2-i)}{2} = \frac{5-i}{2}$ et $z_2 = \frac{-(3i-4)-i\delta}{2\times 1} = \frac{-3i+4-i(2-i)}{2} = \frac{3-5i}{2}$.

Exercice 10 $P(z) = z^4 + 2z^3 - z^2 + 2z + 1.$

1. On a $P(0) = 1 \neq 0.$
2. On pose $Z = z + \frac{1}{z}$ pour $z \neq 0.$
   (a) On a $Z^2 - 3 = (z + \frac{1}{z})^2 - 3 = z^2 + 2 + \frac{1}{z^2} - 3 = z^2 + \frac{1}{z^2} - 1.$
   (b) $\frac{P(z)}{z^2} = \frac{z^4+2z^3-z^2+2z+1}{z^2} = z^2 + 2z - 1 + \frac{2}{z} + \frac{1}{z^2} = z^2 + \frac{1}{z^2} - 1 + 2(z + \frac{1}{z})$
   $\frac{P(z)}{z^2} = Z^2 - 3 + 2Z = (Z-1)(Z+3).$
3. Puisque 0 n'est pas une racine de P, on a
   $P(z) = 0 \iff \frac{P(z)}{z^2} = 0 \iff (Z-1)(Z+3) = 0 \iff Z = 1$ ou $Z = -3.$
   On a $Z = 1 \iff z + \frac{1}{z} = 1 \iff z^2 + 1 = z \iff z^2 - z + 1 = 0 : \Delta = -3,$
   $z_{1,2} = \frac{1 \pm i\sqrt{3}}{2}$
   et $Z = -3 \iff z + \frac{1}{z} = -3 \iff z^2 + 1 = -3z \iff z^2 + 3z + 1 = 0 :$
   $\Delta = 5,\ z_{3,4} = \frac{-3 \pm \sqrt{5}}{2}.$
   D'où les racines de P : $\{\frac{1-i\sqrt{3}}{2}\ ;\ \frac{1+i\sqrt{3}}{2}\ ;\ \frac{-3-\sqrt{5}}{2}\ ;\ \frac{-3+\sqrt{5}}{2}\}.$

Chapitre IV

MATRICES

Sommaire

Introduction

Bien que le calcul matriciel proprement dit n'apparaisse qu'au début du XIXᵉ s., les matrices, en tant que tableaux de nombres, ont depuis longtemps aidé à la résolution d'équations linéaires. Un texte chinois du IIᵉ s. av. J.-C. est le premier exemple connu de l'utilisation de tableaux pour résoudre des systèmes d'équations. Aux Pays-Bas, Johan de Witt représente des transformations géométriques à l'aide de tableaux en 1659. Au tournant du XVIIIᵉ s., Leibniz montre comment utiliser les tableaux pour noter des données ou des solutions. En 1850, le terme de « matrix », d'après la racine latine *mater*, est introduit par le mathématicien anglais Sylvester. En 1854, Arthur Cayley publie un traité fondamental sur les transformations géométriques en utilisant les matrices de façons beaucoup plus générales que tout ce qui a été fait avant lui. Au début du XXᵉ s., les matrices occupent désormais une place centrale en algèbre linéaire. La formulation de la mécanique quantique au moyen de la mécanique matricielle, due à Heisenberg, Born et Jordan, amena à étudier des matrices comportant un nombre infini de lignes et de colonnes.

Dans ce chapitre, m, n, p, i, j, k et ℓ désignent des entiers naturels non nuls. Les nombres considérés seront généralement réels mais ils pourront aussi être complexes. Aussi, on notera $\mathbb{K}$ l'ensemble $\mathbb{R}$ ou $\mathbb{C}$ et un nombre sera un élément de $\mathbb{K}$.

Les matrices définies dans les exemples pourront être utilisées dans les exemples suivants.

1 Définitions

Définition 1

Une ***matrice*** *de taille (ou de format) $m \times n$ est un tableau de nombres à m lignes et à n colonnes.*
Si l'on note $a_{i,j}$ le coefficient (ou le terme) situé à l'intersection de la i^e ligne et de la j^e colonne de la matrice A, on a

$$A = (a_{i,j})_{m\times n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,j} & \dots & a_{1,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \dots & a_{i,j} & \dots & a_{i,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,j} & \dots & a_{m,n} \end{pmatrix}_{m\times n}$$

Exemples : $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ est une matrice de taille 2×3 et $B = \begin{pmatrix} -3 & 6 \\ 1 & -2 \\ 5 & -1 \end{pmatrix}$ est de taille 3×2. On a $a_{1,2} = 2$, $a_{2,1} = 4$, $b_{3,2} = -1$ et $b_{2,3}$ n'existe pas.

Observons le cas de quelques matrices particulières.

Définition 2

- *Une* ***matrice ligne*** *est une matrice formée d'une seule ligne, de taille $1 \times n$.*
- *Une* ***matrice colonne*** *est une matrice formée d'une seule colonne, de taille $m \times 1$.*
- *Une* ***matrice carrée*** *d'ordre n est une matrice formée de n lignes et de n colonnes, de taille $n \times n$.*
- *Une* ***matrice diagonale*** *est une matrice carrée $(a_{i,j})_{n\times n}$ telle que $i \neq j \Longrightarrow a_{i,j} = 0$.*
  On note $Diag(d_1; \dots; d_n)$ la matrice diagonale d'ordre n dont les coefficients diagonaux sont $d_1, \dots, d_n$.
- *La* ***matrice identité*** *d'ordre n, notée I_n, est la matrice diagonale d'ordre n dont tous les coefficients diagonaux égalent 1. On a $I_n = Diag(1; \dots; 1)$.*
- *La* ***matrice nulle*** *de taille $m \times n$, notée $O_{m,n}$, est la matrice de taille $m \times n$ dont tous les coefficients sont nuls. On la note O_n lorsqu'elle est carrée.*

Exemples : $C = \begin{pmatrix} 3 & 8 & -2 & 1 \end{pmatrix}$ est une matrice ligne, $D = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$ est une matrice colonne, $E = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}$ est une matrice carrée d'ordre 2, $F = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = Diag(3;2;1)$ est une matrice diagonale, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = O_{2,3}$ et $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2$.

Définition 3
Deux matrices sont égales si elles sont de même taille et si leurs coefficients sont égaux deux à deux.

Exemples : $A \neq B$ car elles n'ont pas la même taille
et $E \neq I_2$ car $e_{2,1} = -3 \neq 0 = i_{2,1}$.

2 Premières opérations sur les matrices

2.1 Somme de matrices et produit d'une matrice par un nombre

Activité 1 *Au lycée Henri de la Fare-en-Dole, 32 élèves de seconde, 46 élèves de première et 72 élèves de terminale participent au club Math. Par ailleurs, l'association Échecs comporte 43 élèves de seconde, 24 élèves de première et 17 élèves de terminale.*

Au lycée Matisse voisin, ils sont 29 en seconde, 41 en première et 67 en terminale à participer au club Max et l'association & Maths comporte 21 élèves de seconde, 12 de première et 9 de terminale.

1. *Pour les deux lycées, présenter la répartition élèves du club et de l'association en fonction de leur niveau sous forme matricielle.*

2. *Pour d'obscurs mobiles, les deux établissements fusionnent ainsi que leurs différentes sociétés.*
   Présenter sous forme matricielle la répartition des élèves du club Math Max et de l'association Échecs & Maths du nouveau lycée Henri Matisse de la Fare-en-Dole en fonction de leur niveau.

3. *Pour de mystérieuses raisons, les effectifs des différentes sociétés triplent.*
   Présenter sous forme matricielle la nouvelle répartition des élèves du club Math Max et de l'association Échecs & Maths du lycée Henri Matisse en fonction de leur niveau.

Définition 4 *Soient $A = (a_{i,j})$ et $B = (b_{i,j})$ deux matrices de même taille $m \times n$ et soit $\lambda \in \mathbb{K}$ un nombre.*

- *La **somme des matrices** A et B, notée $\boldsymbol{A + B}$, est la matrice $S = (s_{i,j})$ de taille $m \times n$ telle que, pour tout $(i, j) \in [\![1 ; m]\!] \times [\![1 ; n]\!]$, $\quad s_{i,j} = a_{i,j} + b_{i,j}$.*
- *Le **produit de la matrice** A **par le nombre** λ, notée $\boldsymbol{\lambda A}$, est la matrice $P = (p_{i,j})$ de taille $m \times n$ telle que, pour tout $(i, j) \in [\![1 ; m]\!] \times [\![1 ; n]\!]$, $\quad p_{i,j} = \lambda a_{i,j}$.*

Autrement dit, la somme de deux matrices de même taille est la matrice des sommes de leurs coefficients et le produit d'une matrice par un nombre est la matrice du produit des coefficients par ce nombre.

Exemples : Si $\quad G = \begin{pmatrix} 4 & -1 & -3 \\ 3 & 6 & 2 \end{pmatrix}$

alors $\quad A + G = \begin{pmatrix} 1+4 & 2-1 & 3-3 \\ 4+3 & 5+6 & 6+2 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 0 \\ 7 & 11 & 8 \end{pmatrix}$

et $\quad 2A = \begin{pmatrix} 2\times 1 & 2\times 2 & 2\times 3 \\ 2\times 4 & 2\times 5 & 2\times 6 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \end{pmatrix}$.

Remarques : • On se souvient que si $\overrightarrow{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\overrightarrow{v}\begin{pmatrix} x' \\ y' \end{pmatrix}$ sont deux vecteurs du plan, alors $\quad (\overrightarrow{u} + \overrightarrow{v})\begin{pmatrix} x+x' \\ y+y' \end{pmatrix}$ et $\quad (\lambda\overrightarrow{u})\begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$. Ces opérations sur les matrices correspondent donc à celles définies pour les vecteurs. On dit que l'ensemble des matrices de taille $m \times n$ est muni d'une structure d'espace vectoriel.

• Si $M = (m_{i,j})$ est une matrice à coefficients complexes, on note $\mathfrak{Re}(M)$ et $\mathfrak{Im}(M)$ les matrices de même taille de coefficients respectifs $\mathfrak{Re}(m_{i,j})$ et $\mathfrak{Im}(m_{i,j})$ et l'on a $\quad M = \mathfrak{Re}(M) + i\,\mathfrak{Im}(M)$.

Propriété 1
Soient A, B et C trois matrices de même taille et soient α, $\beta \in \mathbb{K}$ deux nombres.
On a toujours :

- $A + B = B + A$ *(commutativité de la somme de matrices)*
- $A + (B + C) = (A + B) + C = A + B + C$ *(associativité de la somme de matrices)*
- $1 \times A = A \times 1 = A$
- $(\alpha + \beta)A = \alpha A + \beta A$ *(distributivité de la multiplication par une matrice sur la somme des nombres)*
- $\alpha(A + B) = \alpha A + \alpha B$ *(distributivité de la multiplication par un nombre sur la somme des matrices)*

Démonstration : Ceci découle des propriétés similaires de la somme et du produit des nombres dans $\mathbb{K}$. □

Définition 5 *Soient $A = (a_{i,j})$ et B deux matrices de même taille.*
*On appelle **opposée** de A et l'on note $\boldsymbol{-A}$, la matrice $(-1)A$. Elle est de même taille que A et ses coefficients sont les opposés deux à deux de ceux de A : $\quad -A = (-a_{i,j})$.*
De plus, on note $B - A$ la matrice $B + (-A)$.

Remarque : On a toujours $\quad A-A=O \quad$ et $\quad M+A=B \iff M=B-A$.

Exemple : $\quad A-G=\begin{pmatrix}1-4 & 2+1 & 3+3\\ 4-3 & 5-6 & 6-2\end{pmatrix}=\begin{pmatrix}-3 & 3 & 6\\ 1 & -1 & 4\end{pmatrix}$.

2.2 Transposition, symétrie et antisymétrie

Activité 2 *Présenter sous forme matricielle la répartition des élèves de seconde, première et terminale de l'activité 1 p.61 en fonction de la société mathématique à laquelle ils appartiennent.*
Quelle opération matricielle sur la dernière matrice obtenue dans l'activité précédente suffit-il d'effectuer ?

Définition 6 *Soit $A=(a_{i,j})$ une matrice de taille $m\times n$. On appelle* ***transposée*** *de A et l'on note $A^\top$, la matrice $B=(b_{k,\ell})$ de taille $n\times m$ telle que pour tout $(k,\ell)\in[\![1;n]\!]\times[\![1;m]\!]$, $\quad b_{k,\ell}=a_{\ell,k}$.*

Autrement dit, transposer une matrice, c'est échanger ses lignes et ses colonnes. La transposée de A est aussi notée A^{t} ou ${}^{\mathrm{t}}A$.

Exemples : $\quad A^\top=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}_{2\times 3}^\top=\begin{pmatrix}1 & 4\\ 2 & 5\\ 3 & 6\end{pmatrix}_{3\times 2}, \quad D^\top=\begin{pmatrix}5\\ 2\end{pmatrix}_{2\times 1}^\top=\begin{pmatrix}5 & 2\end{pmatrix}_{1\times 2},$

$$B^\top=\begin{pmatrix}-3 & 6\\ 1 & -2\\ 5 & -1\end{pmatrix}_{3\times 2}^\top=\begin{pmatrix}-3 & 1 & 5\\ 6 & -2 & -1\end{pmatrix}_{2\times 3}, \quad E^\top=\begin{pmatrix}4 & -2\\ -3 & 5\end{pmatrix}_{2\times 2}^\top=\begin{pmatrix}4 & -3\\ -2 & 5\end{pmatrix}_{2\times 2}$$

et $\quad F^\top=\begin{pmatrix}3 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 1\end{pmatrix}_{3\times 3}^\top=\begin{pmatrix}3 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 1\end{pmatrix}_{3\times 3}=F.$

Remarque : On a toujours $\quad (M^\top)^\top=M$.

Définition 7 *Soit $M=(m_{i,j})$ une matrice carrée d'ordre n. On dit que*
· *M est symétrique lorsque* $\quad M^\top=M$: $\quad m_{j,i}=m_{i,j} \quad \forall i,\, j\in[\![1;n]\!]$.
· *M est antisymétrique lorsque* $\quad M^\top=-M$: $\quad m_{j,i}=-m_{i,j} \quad \forall i,\, j\in[\![1;n]\!]$.

Exemples : ◦ Si $\quad H=\begin{pmatrix}3 & 5 & 1\\ 5 & -2 & -6\\ 1 & -6 & 4\end{pmatrix}$ alors $\quad H^\top=\begin{pmatrix}3 & 5 & 1\\ 5 & -2 & -6\\ 1 & -6 & 4\end{pmatrix}=H$ et H est symétrique.

◦ Si $\quad K=\begin{pmatrix}0 & -2 & 4\\ 2 & 0 & 3\\ -4 & -3 & 0\end{pmatrix}$ alors $\quad K^\top=\begin{pmatrix}0 & 2 & -4\\ -2 & 0 & -3\\ 4 & 3 & 0\end{pmatrix}=-K$ et K est antisymétrique.

Remarques : • Une matrice diagonale est toujours symétrique.
• Les coefficients diagonaux d'une matrice antisymétrique sont nécessairement nuls.

Observons que $E+E^\top = \begin{pmatrix} 8 & -5 \\ -5 & 10 \end{pmatrix}$ est symétrique et que $E-E^\top = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est antisymétrique. On a même $(E+E^\top)+(E-E^\top) = 2E$. Ce résultat se généralise facilement et l'on obtient la propriété suivante.

Propriété 2 *Toute matrice carrée est somme d'une matrice symétrique et d'une matrice antisymétrique.*

Démonstration : En effet, $M = \frac{M+M}{2} + \frac{M^\top - M^\top}{2} = \frac{M+M^\top}{2} + \frac{M-M^\top}{2}$ et il suffit de vérifier que le premier terme est une matrice symétrique et le second, une matrice antisymétrique :

· si $S = \frac{M+M^\top}{2}$, $S^\top = \left(\frac{M+M^\top}{2}\right)^\top = \frac{1}{2}M^\top + \frac{1}{2}(M^\top)^\top = \frac{M^\top+M}{2} = S$.

· si $A = \frac{M-M^\top}{2}$, $A^\top = \left(\frac{M-M^\top}{2}\right)^\top = \frac{1}{2}M^\top - \frac{1}{2}(M^\top)^\top = \frac{M^\top-M}{2} = -A$. □

3 Produit de matrices

Activité 3 *Les élèves de seconde du lycée Henri Matisse de la Fare-en-Dole envoient en moyenne 5 messages à l'animateur du club Math Max ainsi qu'au président de l'association Échecs et Maths. En première, ils en envoient 3 à chacun et en terminale, 4 à chacun. À l'aide de la dernière matrice obtenue dans l'activité 1 p.61, déterminer combien de messages recevront chacun de ces deux éminents protagonistes.*

Définition 8 *Soient* $L = \begin{pmatrix} \ell_{1,1} & \ell_{1,2} & \dots & \ell_{1,n} \end{pmatrix}$ *une matrice ligne de taille* $1 \times n$ *et* $C = \begin{pmatrix} c_{1,1} \\ c_{2,1} \\ \vdots \\ c_{n,1} \end{pmatrix}$ *une matrice colonne de taille* $n \times 1$. *On définit le produit* $L \times C$, *ou* LC, *par la matrice de taille* 1×1 *dont le seul coefficient est*

$$(LC)_{1,1} = \ell_{1,1} \times c_{1,1} + \ell_{1,2} \times c_{2,1} + \dots + \ell_{1,n} \times c_{n,1} = \sum_{k=1}^{k=n} \ell_{1,k} \times c_{k,1}.$$

Exemple : $\begin{pmatrix} 4 & 5 & -1 & -6 \end{pmatrix} \times \begin{pmatrix} 8 \\ -3 \\ -7 \\ 2 \end{pmatrix} = (4 \times 8 + 5(-3) + (-1)(-7) + (-6).2) = (12).$

Remarque : On se souvient que si $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\vec{v}\begin{pmatrix} x' \\ y' \end{pmatrix}$ sont deux vecteurs du plan dans un repère orthonormé, alors $\vec{u} \cdot \vec{v} = xx' + yy' = \begin{pmatrix} x & y \end{pmatrix} \times \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^\top \times \begin{pmatrix} x' \\ y' \end{pmatrix}$.
Le produit d'une matrice ligne par une matrice colonne correspond au produit scalaire des vecteurs.

Définition 9 *Soient $A = (a_{i,j})$ une matrice de taille $m \times n$ et $B = (b_{k,\ell})$ une matrice de taille $n \times p$.*
*Le **produit** de la matrice A par la matrice B, noté $A \times B$ ou AB, est une matrice $C = (c_{i,j})$ de taille $m \times p$ telle que, pour tout $(i, j) \in [\![1 ; m]\!] \times [\![1 ; p]\!]$,*

$$c_{i,j} = \sum_{k=1}^{k=n} a_{i,k} \times b_{k,j}.$$

Autrement dit, le coefficient $c_{i,j}$ est celui du produit de la i^e ligne de A par la j^e colonne de B.

$$B_{n\times p} = \begin{array}{c} \begin{matrix} C_1 & C_2 & \cdots & C_j & \cdots & C_p \end{matrix} \\ \begin{pmatrix} b_{11} & b_{12} & \cdots & \boxed{b_{1j}} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & \boxed{b_{2j}} & \cdots & b_{2p} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{i1} & b_{i2} & \cdots & \boxed{b_{ij}} & \cdots & b_{ip} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & \boxed{b_{nj}} & \cdots & b_{np} \end{pmatrix} \end{array}$$

$$A_{m\times n} = \begin{array}{c} L_1 \\ L_2 \\ \vdots \\ L_i \\ \vdots \\ L_m \end{array} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ \boxed{a_{i1}} & \boxed{a_{i2}} & \cdots & \boxed{a_{ij}} & \cdots & \boxed{a_{in}} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1p} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2p} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & \boxed{c_{ij}} & \cdots & c_{ip} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mp} \end{pmatrix} = (A \times B)_{m\times p}$$

Exemples :

- $A \times B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} -3 & 6 \\ 1 & -2 \\ 5 & -1 \end{pmatrix}_{3\times 2}$

$$= \begin{pmatrix} 1 \times (-3) + 2 \times 1 + 3 \times 5 & 1 \times 6 + 2 \times (-2) + 3 \times (-1) \\ 4 \times (-3) + 5 \times 1 + 6 \times 5 & 4 \times 6 + 5 \times (-2) + 6 \times (-1) \end{pmatrix}_{2\times 2} = \begin{pmatrix} 14 & -1 \\ 23 & 8 \end{pmatrix}_{2\times 2}$$

- $B \times A = \begin{pmatrix} -3 & 6 \\ 1 & -2 \\ 5 & -1 \end{pmatrix}_{3\times 2} \times \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3}$

$$= \begin{pmatrix} (-3) \times 1 + 6 \times 4 & (-3) \times 2 + 6 \times 5 & (-3) \times 3 + 6 \times 6 \\ 1 \times 1 + (-2) \times 4 & 1 \times 2 + (-2) \times 5 & 1 \times 3 + (-2) \times 6 \\ 5 \times 1 + (-1) \times 4 & 5 \times 2 + (-1) \times 5 & 5 \times 3 + (-1) \times 6 \end{pmatrix}_{3\times 3}$$

$$= \begin{pmatrix} 21 & 24 & 27 \\ -7 & -8 & -9 \\ 1 & 5 & 9 \end{pmatrix}_{3\times 3} = R \neq A \times B$$

- $E \times G = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}_{2\times 2} \times \begin{pmatrix} 4 & -1 & -3 \\ 3 & 6 & 2 \end{pmatrix}_{2\times 3}$

$$= \begin{pmatrix} 4 \times 4 - 2 \times 3 & 4 \times (-1) - 2 \times 6 & 4 \times (-3) - 2 \times 2 \\ -3 \times 4 + 5 \times 3 & -3 \times (-1) + 5 \times 6 & -3 \times (-3) + 5 \times 2 \end{pmatrix}_{2\times 3}$$

$$= \begin{pmatrix} 10 & -16 & -16 \\ 3 & 33 & 19 \end{pmatrix}_{2\times 3}$$

∘ $G \times E = \begin{pmatrix} 4 & -1 & -3 \\ 3 & 6 & 2 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}_{2\times 2}$ n'est pas défini.

∘ $E \times I_2 = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}_{2\times 2} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2} = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}_{2\times 2} = E$

∘ $I_3 \times R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_{3\times 3} \times \begin{pmatrix} 21 & 24 & 27 \\ -7 & -8 & -9 \\ 1 & 5 & 9 \end{pmatrix}_{3\times 3} = \begin{pmatrix} 21 & 24 & 27 \\ -7 & -8 & -9 \\ 1 & 5 & 9 \end{pmatrix}_{3\times 3} = R$

∘ $I_2 \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2} \times \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3} = A$

∘ $A \times I_3 = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_{3\times 3} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times 3} = A$

∘ $Z \times Y = \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ -12 & -6 \end{pmatrix}$

et $Y \times Z = \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2$: on remarque qu'un produit peut très bien être nul sans qu'aucun des facteurs ne le soit. De plus, le produit contraire n'est généralement pas nul. On dit que l'ensemble des matrices n'est pas *intègre*.

Si $P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,

∘ $R \times P = \begin{pmatrix} 21 & 24 & 27 \\ -7 & -8 & -9 \\ 1 & 5 & 9 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 24 & 27 & 21 \\ -8 & -9 & -7 \\ 5 & 9 & 1 \end{pmatrix}$: échange les colonnes.

∘ $P \times R = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 21 & 24 & 27 \\ -7 & -8 & -9 \\ 1 & 5 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 9 \\ 21 & 24 & 27 \\ -7 & -8 & -9 \end{pmatrix}$: échange les lignes.

Une telle matrice P est appelée *matrice de permutation*.

Propriété 3 *Soient $A_{m\times n}$, B et C trois matrices et soit $\lambda \in \mathbb{K}$ un nombre. Sous réserve de définition des produits et des sommes, on a toujours :*

- $(A \times B) \times C = A \times (B \times C) = A \times B \times C$ *(associativité du produit de matrices)*
- $A \times (B + C) = A \times B + A \times C$ *(distributivité du produit par rapport à la somme de matrices)*
- $(\lambda A) \times B = \lambda(A \times B) = A \times (\lambda B)$
- $A \times I_n = I_m \times A = A$ *(élément neutre du produit de matrices)*
- $A \times O_{n\times p} = O_{m\times p}$ *et* $O_{p\times m} \times A = O_{p\times n}$ *(élément absorbant du produit de matrices)*

Démonstration : Nous ne démontrerons que le premier point, les autres sont plus aisés.
Soient A de taille $m \times n$, B de taille $n \times p$ et C de taille $p \times q$. On a AB de taille $m \times p$, BC de taille $n \times q$ et

$$(AB)_{i,k} = \sum_{\ell=1}^{\ell=n} a_{i,\ell} b_{\ell,k} \quad \text{et} \quad (BC)_{\ell,j} = \sum_{k=1}^{k=p} b_{\ell,k} c_{k,j} \quad \text{donc}$$

$$\begin{aligned}\big((AB)C\big)_{i,j} &= \sum_{k=1}^{k=p} (AB)_{i,k} c_{k,j} = \sum_{k=1}^{k=p} \left(\sum_{\ell=1}^{\ell=n} a_{i,\ell} b_{\ell,k} \right) c_{k,j} = \sum_{\ell=1}^{\ell=n} \sum_{k=1}^{k=p} a_{i,\ell} b_{\ell,k} c_{k,j} \\ &= \sum_{\ell=1}^{\ell=n} \left(a_{i,\ell} \sum_{k=1}^{k=p} b_{\ell,k} c_{k,j} \right) = \sum_{\ell=1}^{\ell=n} a_{i,\ell} (BC)_{\ell,j} = \big(A(BC)\big)_{i,j}.\end{aligned}$$

□

Remarques : • On a vu que le produit de matrices n'est pas commutatif :
$\boldsymbol{A \times B \neq B \times A}$. En effet, il n'est même pas certain que le produit soit défini dans les deux sens, et s'il l'est, les résultats sont souvent de tailles différentes et même dans le cas de matrices carrées, les résultats sont généralement différents.
Dans le cas où l'on a l'égalité, on dit que les deux matrices commutent. Par exemple, I_n commute avec toutes les matrices carrées d'ordre n.

• Le produit de deux matrices carré n'est défini que si elles ont même ordre et le résultat est aussi une matrice carrée de même ordre. Ceci nous même naturellement à la définition suivante.

Définition 10 *Soient A une matrice carrée d'ordre n et $k \in \mathbb{N}^*$.*
La ***puisance*** *k^e de A est la matrice* $A^k = \prod_{\ell=1}^{\ell=k} A = \underbrace{A \times A \times \ \ldots \ \times A}_{k\ fois}$.
On pose $A^0 = I_n$ *si* $A \neq O_n$.

Exemples :

◦ $E^3 = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}^3 = \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix} \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix} \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix}$
$= \begin{pmatrix} 22 & -18 \\ -27 & 31 \end{pmatrix} \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix} = \begin{pmatrix} 142 & -134 \\ -201 & 209 \end{pmatrix}$

◦ $F^4 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}^4 = Diag(3;2;1)^4 = \begin{pmatrix} 3^4 & 0 & 0 \\ 0 & 2^4 & 0 \\ 0 & 0 & 1^4 \end{pmatrix} = Diag(3^4;2^4;1^4)$
$= Diag(81;16;1)$, résultat que nous démontrerons dans l'exercice 10 p.75.

◦ Pour tous entiers n et k non nuls, $I_n^k = I_n$.

4 Matrice inverse

Si l'on peut multiplier certaines matrices entre elles, la division matricielle n'existe pas. En revanche, on peut parfois définir un inverse.

Définition 11 *Une matrice carrée A d'ordre n est dite* ***inversible*** *lorsqu'il existe une matrice carrée B de taille n telle que* $AB = BA = I_n$.

Exemples : ◦ Puisque $ST = \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 1/2 & -1/2 \\ 1/4 & 1/4 \end{pmatrix} = I_2$ et $TS = \begin{pmatrix} 1/2 & -1/2 \\ 1/4 & 1/4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix} = I_2$, ces deux matrices sont inversibles.

◦ Pour tout $n \in \mathbb{N}^*$, I_n est inversible et O_n n'est pas inversible.

Propriété 4 *On a* $AB = I \iff BA = I$.

Cette propriété est admise mais bien utile : il suffit de vérifier l'inversibilité d'un seul côté.

Exemple : Puisque $UV = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ -2 & 4 & -1 \end{pmatrix} = I_3$, ces deux matrices sont inversibles.

Propriété 5 *Soit A une matrice inversible.*
La matrice B vérifiant $AB = I$ est unique. Elle est appelée ***matrice inverse*** *de A et elle est notée* $\mathbf{A^{-1}}$.

Démonstration : L'existence est donnée par la définition. Démontrons l'unicité.
Soient B et C deux matrices vérifiant $AB = AC = I$. D'après la propriété précédente, on a $BA = I$ et il vient $B = BI = B(AC) = (BA)C = IC = C$. □

Exemples :

◦ On a $S^{-1} = T$ et $T^{-1} = S$ tout comme $U^{-1} = V$ et $V^{-1} = U$.

◦ Puisque $YZ = O_2$, ni Y ni Z ne sont inversibles. En effet, on aurait alors $Y = YI_2 = YZZ^{-1} = O_2Z^{-1} = O_2$ ce qui est faux,
tout comme $Z = Y^{-1}YZ = Y^{-1}O_2 = O_2$.

Propriété 6 *Soit A une matrice inversible. On a toujours* $\left(A^{-1}\right)^{-1} = A$.

Démonstration : On pose $B = A^{-1}$ et l'on a $BA = A^{-1}A = I$ donc $A = B^{-1} = \left(A^{-1}\right)^{-1}$. □

Exemples : On a $(S^{-1})^{-1} = S = T^{-1}$ et $(U^{-1})^{-1} = U = V^{-1}$.

Propriété 7 *Si A et B sont deux matrices inversibles, alors la matrice produit (AB) est inversible, de matrice inverse* $(AB)^{-1} = B^{-1}A^{-1}$.

Démonstration : En effet,
$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I.$$ □

Exemples : $(S^2)^{-1} = (SS)^{-1} = S^{-1}S^{-1} = TT = T^2$
et $I_3^{-1} = (UV)^{-1} = V^{-1}U^{-1} = UV = I_3$.

Pour déterminer l'inverse d'une matrice, on peut utiliser la calculatrice par exemple mais nous verrons en exercice des techniques de détermination d'un inverse plus satisfaisantes. Dans le cas où $n = 2$, nous pouvons même être beaucoup précis et explicite.

Définition 12 *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *une matrice carrée d'ordre* 2.
Le déterminant de A*, noté* $\det(A)$*, est le nombre défini par* $\det(A) = ad - bc.$

Exemples : ◦ $\det(E) = \det \begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix} = 4 \times 5 - (-2)(-3) = 14,$

◦ $\det(S) = \det \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix} = 1 \times 2 - 2(-1) = 4,$

◦ $\det(T) = \det \begin{pmatrix} 1/2 & -1/2 \\ 1/4 & 1/4 \end{pmatrix} = \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} = \frac{1}{4}.$

Théorème 1 *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *une matrice carrée d'ordre* 2. A *est inversible si, et seulement si,* $\det(A) \neq 0$ *et dans ce cas, on a* $A^{-1} = \dfrac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$

Nous démontrerons ce résultat en exercice (cf. ex. n° 4 p.73).

Remarques : • On se souvient que si $\overrightarrow{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\overrightarrow{v}\begin{pmatrix} x' \\ y' \end{pmatrix}$ sont deux vecteurs du plan, alors $\overrightarrow{u}$ et $\overrightarrow{v}$ sont colinéaires si, et seulement si, $\det(\overrightarrow{u}, \overrightarrow{v}) = xy' - x'y = \det \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} = 0.$ Le déterminant des matrices est précisément celui des vecteurs.

• On a toujours $\det(A^\top) = \det(A).$

• Alors, $\det(A^{-1}) = \det \begin{pmatrix} d/\det(A) & -b/\det(A) \\ -c/\det(A) & a/\det(A) \end{pmatrix} = \frac{da-(-b)(-c)}{\det(A)^2} = \frac{\det(A)}{\det(A)^2} = \dfrac{1}{\det(A)}.$

• On peut définir un déterminant pour les matrices de toutes tailles et le résultat analogue reste vrai mais cela n'est pas au programme de terminale. Il existe même une formule explicite donnant la matrice inverse d'une matrice inversible mais celle-ci est si fastidieuse que jamais personne ne l'utilise.

Exemples : ◦ $\det(E) = 14 \neq 0$ donc E est inversible et $E^{-1} = \frac{1}{14}\begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix}$:

$$\frac{1}{14}\begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & -2 \\ -3 & 5 \end{pmatrix} = \frac{1}{14}\begin{pmatrix} 5 \times 4 + 2(-3) & 5(-2) + 2 \times 5 \\ 3 \times 4 + 4(-3) & 3(-2) + 4 \times 5 \end{pmatrix} = \frac{1}{14}\begin{pmatrix} 14 & 0 \\ 0 & 14 \end{pmatrix} = I_2.$$

◦ $\det(S) = 4 \neq 0$ donc S est inversible et $S^{-1} = \frac{1}{4}\begin{pmatrix} 2 & -2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & -1/2 \\ 1/4 & 1/4 \end{pmatrix} = T.$

◦ $\det(Z) = \det \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = 2 \times 2 - (-1)(-4) = 0$ et Z n'est pas inversible.

5 Quelques applications

Le langage matriciel a de très nombreuses applications, tant dans des domaines mathématiques (suites récurrentes, équations différentielles, géométrie, théorie des graphes, probabilités, algèbre linéaire en dimension finie, codage...) que dans les sciences physiques (mécanique, optique, systèmes dynamiques, mécanique quantique...), en biologie, en finance, en analyse de données, en économie... Nous en verrons plusieurs en exercice et au cours de l'année mais voici d'ors et déjà deux applications directes.

5.1 Résolution de systèmes linéaires

Activité 4 *Résoudre le système* $(S)\left\{\begin{array}{l} 2x-3y+z=1 \\ x-2y+z=2 \\ -2x+4y-z=3. \end{array}\right.$

Définition 13
Soient les nombres $a_{i,j}\in\mathbb{K}$ *pour* $(i\,,\,j)\in[\![1\,;n]\!]^2$ *et* $b_1,\ldots,\,b_n\in\mathbb{K}$.
Le système $(S)\left\{\begin{array}{lcl} a_{1,1}x_1+a_{1,2}x_2+\ldots+a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1+a_{2,2}x_2+\ldots+a_{2,n}x_n & = & b_2 \\ \vdots & & \\ a_{n,1}x_1+a_{n,2}x_2+\ldots+a_{n,n}x_n & = & b_n \end{array}\right.$ *d'inconnues* $x_1,\ldots,\,x_n$
est appelé ***système linéaire*** *de n équations à n inconnues.*

Propriété 8
On définit les matrices suivantes : $A=(a_{i,j})$, $B=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ *et* $X=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$.
On a alors $(S)\iff AX=B$.
Si A est inversible, alors le système admet une solution unique, obtenue par le calcul matriciel $X=A^{-1}B$.

Démonstration : Ceci découle de la définition du produit matriciel et de l'unicité de la matrice inverse. □

Exemple : Le système de l'activité précédente peut s'écrire $VX=\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ donc

$$X=V^{-1}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}=U\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}=\begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}=\begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix}.$$

Remarque : Si la matrice A n'est pas inversible, alors soit le système n'admet aucune solution, soit il en admet une infinité.
Par exemple, on a $\det\begin{pmatrix} 2 & 1 \\ -4 & -2 \end{pmatrix}=0$. Le système $\left\{\begin{array}{l} 2x+y=5 \\ -4x-2y=-10 \end{array}\right.$

admet une infinité de solutions, celles de la forme $(x\,,\,5-2x)$ et le système $\begin{cases} 2x+y=5 \\ -4x-2y=-9 \end{cases}$ n'admet aucune solution.

En effet, la première équation de ce système est associée à une droite de vecteur directeur $\overrightarrow{u}\begin{pmatrix} -1 \\ 2 \end{pmatrix}$ et la seconde à $\overrightarrow{v}\begin{pmatrix} 2 \\ -4 \end{pmatrix}$. Comme $\det(\overrightarrow{u};\overrightarrow{v}) = \det\begin{pmatrix} 2 & 1 \\ -4 & -2 \end{pmatrix} = 0$, ces deux vecteurs sont colinéaires et les droites sont parallèles, strictement ou confondues.

On peut définir de manière similaire un système de m équations à n inconnues qui n'a, en général, de solution unique que lorsque $m{=}n$.

5.2 Transformations du plan

On se place dans un repère orthonormé direct $(O\,;\,\overrightarrow{\imath},\,\overrightarrow{\jmath})$: $\left(\overrightarrow{\imath}\,;\,\overrightarrow{\jmath}\right) = +\frac{\pi}{2}\,[2\pi]$.

Activité 5 *Soient $A(4\,,\,3)$, $B(2\,,\,0)$, $C(0\,,\,-3)$, $D(-1\,,\,2)$, $E(3\,,\,-4)$, $F(-2\,,\,-1)$ et $M(x\,,\,y)$ des points et soient $\overrightarrow{u}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ et $\overrightarrow{v}\begin{pmatrix} -2 \\ 1 \end{pmatrix}$ deux vecteurs.*

1. *Déterminer les coordonnées des images des points A à M par :*
   - *(a) la translation de vecteur $\overrightarrow{u}$,*
   - *(b) la translation de vecteur $\overrightarrow{v}$,*
   - *(c) la symétrie axiale par rapport à l'axe des abscisses,*
   - *(d) la symétrie axiale par rapport à l'axe des ordonnées,*
   - *(e) la symétrie de centre O,*
   - *(f) la rotation de centre O et d'angle $+\frac{\pi}{2}$,*
   - *(g) la rotation de centre O et d'angle $-\frac{\pi}{2}$,*
   - *(h) l'homothétie de centre O et de rapport -2.*
2. *Représenter ces transformations sous forme matricielle.*

Ces résultats se généralisent et l'on obtient les propriétés suivantes.

Propriété 9 ***Translation***
Soient a et b deux nombres réels.
La translation de vecteur $\overrightarrow{t}\begin{pmatrix} a \\ b \end{pmatrix}$ qui, à tout point $M(x\,,\,y)$ du plan, associe le point $M'(x'\,,\,y')$ se définit matriciellement par la somme $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$.

Démonstration : En effet, $\overrightarrow{OM'} = \overrightarrow{OM} + \overrightarrow{MM'} = \overrightarrow{OM} + \overrightarrow{t}$. □

Propriété 10 *Pour chacune des transformations géométriques suivantes qui, à tout point $M\,(\,x\,,\,y\,)$ du plan, associe le point $M'\,(\,x'\,,\,y'\,)$, il existe une **matrice de transition** T telle que* $\begin{pmatrix} x' \\ y' \end{pmatrix} = T \times \begin{pmatrix} x \\ y \end{pmatrix}$.

· *Pour une symétrie axiale par rapport à l'axe des abscisses, on a* $T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

· *Pour une symétrie axiale par rapport à l'axe des ordonnées, on a* $T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

· *Pour une rotation de centre O et d'angle θ, on a* $T = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

· *Pour une homothétie de centre O et de rapport $\lambda \in \mathbb{R}$, on a* $T = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I_2$.

Exercices

Matrices

Pour les exercices **1** à **16**, on donne les matrices suivantes :

$$A=\begin{pmatrix}1&2\\0&1\end{pmatrix},\qquad B=\begin{pmatrix}1&0&1\\0&0&1\\1&0&1\end{pmatrix},\qquad C=\begin{pmatrix}1&2\\3&2\end{pmatrix},\qquad \Delta=\begin{pmatrix}1&0&0\\0&1&1\\3&1&1\end{pmatrix},$$

$$E=\begin{pmatrix}-2&3&1\end{pmatrix},\qquad F=\begin{pmatrix}4\\-5\\7\end{pmatrix},\qquad G=\begin{pmatrix}2&1&-3\\-2&3&-1\end{pmatrix},\qquad H=\begin{pmatrix}4&2\\-1&-5\\3&-2\end{pmatrix},$$

$$J=\begin{pmatrix}1&2\\-1&3\end{pmatrix},\quad K=\begin{pmatrix}1&1&0\\1&1&1\\0&-1&1\end{pmatrix},\quad L=\begin{pmatrix}0&1&-1\\-3&4&-3\\-1&1&0\end{pmatrix},\quad N=\begin{pmatrix}1&1&1\\1&-1&1\\4&2&1\end{pmatrix},$$

$$Q=\begin{pmatrix}2&-6\\-3&9\end{pmatrix},\qquad R=\begin{pmatrix}0&2&-1\\3&-2&0\\-2&2&1\end{pmatrix},\qquad S=\begin{pmatrix}1&4&2\\1&3&-3\\1&-2&2\end{pmatrix},$$

$$T=\begin{pmatrix}-1/\sqrt{2}&1/\sqrt{2}\\1/\sqrt{2}&1/\sqrt{2}\end{pmatrix},\quad U=\begin{pmatrix}3&0\\0&1\end{pmatrix}\quad\text{et}\quad V=\begin{pmatrix}2&3\\1&2\end{pmatrix}.$$

Les calculs effectués dans un exercice pourront être utilisés dans les suivants.

Exercice 1 Lorsque cela est possible, déterminer les matrices suivantes. On pourra vérifier à la calculatrice.

$L+S$	GF	GH	N^2+8N	A^2	CJ
$E+F$	FG	HG	N^3	A^3	TU
EF	EG	$2I_3-3L$	K^2	B^2	T^2
FE	GE	L^2	$2A-3B$	B^3	RS

Exercice 2 Compléter $\begin{pmatrix}5&2\\4&?\end{pmatrix}\begin{pmatrix}?&-1\\3&?\end{pmatrix}=\begin{pmatrix}16&?\\11&0\end{pmatrix}$.

Exercice 3 Calculer $\Delta\times\begin{pmatrix}1&1&1\\0&1&0\\1&0&0\end{pmatrix}$ et $\Delta\times\begin{pmatrix}1&1&1\\1&2&1\\0&-1&-1\end{pmatrix}$.

Qu'en déduire pour la matrice Δ ?

Exercice 4 Inverse d'une matrice 2×2

Soient $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ une matrice carrée d'ordre 2, $\det(M)=ad-bc$ son déterminant et $M'=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$ une matrice associée à M.

Le but de l'exercice est de démontrer que M est inversible si, et seulement si, son déterminant est non nul.

1. Calculer MM' et $M'M$.
2. Implication réciproque : On suppose que $\det(M) \neq 0$.
   Justifier que M est inversible et déterminer son inverse.
3. Implication directe : On suppose que M est inversible et que, par l'absurde, $\det(M) = 0$.
   (a) En calculant $M^{-1}MM'$ de deux manières, montrer que $M' = O_2$.
   (b) Quelle est alors la matrice M ?
   (c) Conclure.

Exercice 5
Déterminer les matrices inverses des matrices A, C, J, Q, T, U et V.

Exercice 6 Calcul d'inverse avec le pivot de Gauss

Pour déterminer l'inverse d'une matrice, on peut appliquer l'algorithme de Gauss. Il consiste à effectuer des opérations élémentaires sur les lignes de la matrice afin de la ramener à la matrice identité et d'effectuer concomitamment les mêmes opérations sur la matrice identité. La matrice obtenue à partir de cette dernière sera la matrice inverse recherchée. Les opérations élémentaires que l'on peut effectuer sont l'échange de deux lignes, la multiplication d'une ligne par un nombre non nul et l'addition d'un multiple d'une ligne à une autre ligne. Remarquons que l'on peut tout aussi bien travailler sur les colonnes mais certainement pas sur les deux.
Voici un exemple pour lequel nous connaissons déjà le résultat.

$$C = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \xrightarrow{L_2 - 3L_1 \to L_2} \begin{pmatrix} 1 & 2 \\ 0 & -4 \end{pmatrix} \xrightarrow{-\frac{1}{4}L_2 \to L_2} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \xrightarrow{L_1 - 2L_2 \to L_1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{L_2 - 3L_1 \to L_2} \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \xrightarrow{-\frac{1}{4}L_2 \to L_2} \begin{pmatrix} 1 & 0 \\ 3/4 & -1/4 \end{pmatrix}$$

$$\xrightarrow{L_1 - 2L_2 \to L_1} \begin{pmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{pmatrix} = C^{-1}$$

Déterminer de manière similaire les éventuelles matrices inverses des matrices S, R et B. En déduire la matrice $(RS)^{-1}$.

Exercice 7 Résolution de systèmes linéaires avec le pivot de Gauss

La méthode du pivot de Gauss pour résoudre les systèmes linéaires consiste à se ramener à un système triangulaire en effectuant des opérations élémentaires sur les lignes du système, ces opérations étant les mêmes qu'à l'exercice 6 précédent. Une fois que l'on a obtenu un système triangulaire, celui-ci se résout aisément en le remontant.
Voici un exemple :

$$\begin{cases} 3x + 2y = 7 \\ 5x - 3y = 18 \end{cases} \overset{L_2 - \frac{5}{3}L_1 \to L_2}{\Longleftrightarrow} \begin{cases} 3x + 2y = 7 \\ (5x - 3y) - \frac{5}{3}(3x + 2y) = 18 - \frac{5}{3} \times 7 \end{cases}$$

$$\Longleftrightarrow \begin{cases} 3x + 2y = 7 \\ -\frac{19}{3}y = \frac{19}{3} \end{cases} \overset{L_1 \leftrightarrow L_2}{\Longleftrightarrow} \begin{cases} y = -1 \\ 3x + 2(-1) = 7 \end{cases} \Longleftrightarrow (x, y) = (3, -1).$$

Résoudre les systèmes linéaires suivants en utilisant la méthode du pivot de Gauss.

$$S_a\colon \begin{cases} x+3y+4z=7 \\ 2x-4y+z=13 \\ 3x-y+2z=11 \end{cases} \quad \Bigg| \quad S_b\colon \begin{cases} 2a+b-4c=-15 \\ 2b+6c=20 \\ a-b-3c=-12 \end{cases} \quad \Bigg| \quad S_c\colon \begin{cases} 3u-4v+5w=-5 \\ 2u+3v-4w=17 \\ 4u-3v+2w=5 \end{cases}$$

Exercice 8 Calcul d'inverse par annulation d'un polynôme

1. Déterminer $L^2-3L+2I_3$. En déduire que L est inversible puis déterminer son inverse.
2. Montrer que $N^3 = N^2+8N+6I$. En déduire que L est inversible puis déterminer son inverse.
3. Calculer $(K-I_3)^3$. En déduire que K est inversible puis déterminer son inverse.
4. Calculer Q^2-11Q. Que peut-on en déduire ?
5. Soit M une matrice carrée telle que $M^3-2M^2-M=O$. Que peut-on en déduire ?

Exercice 9 Puissances

1. Conjecturer l'expression de A^n pour $n \in \mathbb{N}$ puis démontrer votre conjecture.
2. Conjecturer l'expression de B^n pour $n \geqslant 2$ puis démontrer votre conjecture.

Exercice 10 Puissance et diagonalisation

Soient M une matrice carrée, $D = Diag(d_1; d_2; \ldots; d_n)$ une matrice diagonale et P une matrice carrée inversible, toutes d'ordre $n \in \mathbb{N}^*$ et soit k un entier naturel non nul.

1. Conjecturer l'expression de D^k puis démontrer cette conjecture.
2. On suppose que M est diagonalisée, c.-à-d. que l'on peut écrire $M = PDP^{-1}$. Conjecturer l'expression de M^k puis démontrer cette conjecture.
3. On suppose que D est inversible. Montrer que M est inversible et déterminer son inverse.

Exercice 11 Inversion de matrices diagonales

Soient $D = Diag(d_1; \ldots; d_n)$ et $D' = Diag(d'_1; \ldots; d'_n)$ deux matrices diagonales d'ordre n.

1. Calculer DD' et $D'D$.
2. À quelle condition la matrice D semble-t-elle inversible ? Démontrer cette conjecture.
3. En raisonnant par l'absurde, démontrer la propriété réciproque.
4. Conclure.

Exercice 12 Diagonalisation

1. Calculer $W = J^{-1}CJ$. En déduire l'expression de C^n pour $n \in \mathbb{N}^*$.
2. On pose $X = TUT$. Calculer X^{-1} et déterminer l'expression de X^n en fonction de $n \in \mathbb{N}^*$.
3. On pose $Y = V \begin{pmatrix} 1/3 & 0 \\ 0 & 1/2 \end{pmatrix} V^{-1}$. Calculer Y^{-1} et déterminer $\lim\limits_{n\to\infty} Y^n$.
4. Calculer $Z = S^{-1}RS$ puis en déduire l'expression de R^n pour $n \in \mathbb{N}^*$.

EXERCICES

Exercice 13

$M_n = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & 0 \end{pmatrix}$ est la matrice carrée d'ordre $n \geqslant 2$ formée de 0 sur la diagonale et de 1 partout ailleurs.

1. Calculer M_n^2 et exprimer le résultat en fonction de M_n, de I_n et de n.
2. En déduire que M_n est inversible et déterminer M_n^{-1}.

Exercice 14 Résolution de systèmes linéaires et inversion de matrice

Résoudre les systèmes linéaires suivants en utilisant une représentation matricielle.

(a) $S_a : \begin{cases} x + 2y = 3 \\ 3x + 2y = 11 \end{cases}$

(b) $S_b : \begin{cases} a + b = 4 \\ a + b + c = 7 \\ -b + c = -3 \end{cases}$

(c) $S_c : \begin{cases} \beta - \gamma = -2 \\ -3\alpha + 4\beta - 3\gamma = 5 \\ -\alpha + \beta = 1 \end{cases}$

(d) $S_d : \begin{cases} f + g + h = 1 \\ e + g + h = 1 \\ e + f + h = 1 \\ e + f + g = 1 \end{cases}$

(e) $S_e : \begin{cases} 2i - 6j = 5 \\ -3i + 9j = 7 \end{cases}$

(f) u, v et $w \in \mathbb{R}$ tels que

$S_f : \begin{cases} u + w = 3 \\ w = -1 \\ u + w = 3 \end{cases}$

(g) $S_g : \begin{cases} z = 1 \\ x + y = -2 \\ 3z + x + y = 1 \end{cases}$

Exercice 15 Les instructions suivantes sont écrites dans un éditeur Python. Déterminer `X`.

```
from numpy import *
from numpy.linalg import *
A=array([[0,1,-1],[-3,4,-3],[-1,-1,0]])
B=array([[-2],[5],[1]])
X=dot(inv(A),B)
```

Exercice 16 Transposition et produit

1. Déterminer les matrices suivantes.

$E^\top$	$E^\top F^\top$	$(EF)^\top$	$G^\top$	$G^\top H^\top$	$(GH)^\top$
$F^\top$	$F^\top E^\top$	$(FE)^\top$	$H^\top$	$H^\top G^\top$	$(HG)^\top$

2. Émettre une conjecture sur la transposée d'un produit de deux matrices puis la démontrer.

Exercice 17 Matrices de permutation

1. Déterminer la matrice de permutation (cf. cours en page 66)) qui permet de placer la première colonne de toute matrice 3×3 en troisième, la deuxième colonne en première et la troisième colonne en seconde. Où doit-elle agir sur la matrice donnée ?
2. Déterminer la matrice de permutation (cf. cours en page 66)) qui permet de placer la première ligne de toute matrice 3×3 en troisième, la deuxième ligne en première et la troisième ligne en seconde. Où doit-elle agir sur la matrice donnée ?
3. Quel lien relie ces deux matrices de permutation ? Cela vous surprend-il ?

Exercice 18 Soit $\mathcal{J}_n$ la matrice carrée d'ordre n formée uniquement de 1.
Exprimer $\mathcal{J}_n^2$ en fonction de n et de $\mathcal{J}_n$ puis en déduire que $\mathcal{J}_n$ n'est pas inversible.

Exercice 19 Matrices nilpotentes
On dit qu'une matrice carrée M, d'ordre n, est nilpotente s'il existe un entier $p \in \mathbb{N}^*$ tel que $M^p = O_n$.

1. Soient $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ deux matrices.
   (a) Montrer que A et B sont nilpotentes.
   (b) Calculer $A + B$ puis montrer que cette matrice n'est pas nilpotente.
   (c) Calculer AB puis montrer que cette matrice n'est pas nilpotente.
2. Soit N une matrice carrée d'ordre 2 telle que $N^2 = O_2$.
   (a) Calculer $(I_2 + N)(I_2 - N)$ puis en déduire que $I_2 - N$ est inversible.
   (b) Déterminer la matrice inverse de $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ puis celle de $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

Exercice 20

Soit la matrice $M = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$. On pose $N = M - I_3$. Calculer N^3 puis montrer par récurrence que, pour tout $n \in \mathbb{N}^*$, $M^n = I_3 + nN + \frac{n(n-1)}{2} N^2$.

Exercice 21 Identités remarquables et binôme de Newton
On pose $A = \begin{pmatrix} 3 & -1 \\ 7 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 1 \\ -7 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$,

1. (a) Calculer $(A + B)^2$ et $A^2 + 2AB + B^2$.
   (b) Calculer $(C + D)^2$ et $C^2 + 2CD + D^2$.
   (c) Qu'en conclure ? Expliquer.
2. Que dire des autres identités remarquables ?
3. Compléter : On dit que deux matrices P et Q forment une paire commutante (ou commutent) si ... . Dans ce cas, la formule du binôme de Newton est ... :
   $(P + Q)^n = ...$.
   On peut remarquer que ... commute avec toutes les matrices ... .

EXERCICES

4. Appliquer la formule du binôme de Newton afin de retrouver le résultat de l'exercice 20 précédent.

Exercice 22 Compléter la fonction Python suivante afin qu'elle retourne ce que l'on attend.

```
from numpy import *
from numpy.linalg import *
def puissance(a,b,c,d,n) :
    A=array([[a,b],[c,d]])
    B=...
    for i in range(1,n) :
        A=dot(...)
    return ...
```

Exercice 23 Matrices triangulaires

Une matrice triangulaire supérieure est une matrice dont tous les coefficients situés sous la diagonale sont nuls.

1. Soit $T = (t_{i,j})$ une matrice carrée d'ordre n.
   (a) Que dire de ses coefficients $t_{i,j}$ si T est triangulaire supérieure ?
   (b) Et si T est triangulaire inférieure ?
2. Soient T et T' deux matrices triangulaires supérieures d'ordre n et soient α et β deux nombres.
   Montrer que $\alpha T + \beta T'$ et TT' sont triangulaires supérieures.
3. (a) Les matrices $A = \begin{pmatrix} 2 & 4 \\ 0 & -3 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}$ sont-elles inversibles ?
   (b) On donne $C = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$. Calculer $C \times \begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix}$ et $C \times \begin{pmatrix} -9 \\ 1 \\ 3 \end{pmatrix}$.
   C est-elle inversible ?
   (c) La matrice $E = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ est-elle inversible ?
   (d) À quelle condition une matrice triangulaire semble-t-elle inversible ?

Les matrices triangulaires forment donc un ensemble stable pour les opérations usuelles et sont relativement aisées à étudier, à manipuler et à inverser : il est souvent utile de s'y ramener (cf. exercice 7 p.74).

Exercice 24 Équation cartésienne d'un plan

Soient les points $A(1;5;-2)$, $B(7;-1;3)$ et $C(-2;7;2)$ dans r.o.n. de l'espace et l'on note $\mathscr{P}$ le plan (BAC).

On cherche une équation du plan sous la forme $ax + by + cz = 73$ où a, b et c sont des réels.

On définit les matrices $X = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$, $Y = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $M = \begin{pmatrix} 1 & 5 & -2 \\ 7 & -1 & 3 \\ -2 & 7 & -2 \end{pmatrix}$ et $N = \begin{pmatrix} 19 & 4 & -13 \\ -8 & 6 & 17 \\ -47 & 17 & 36 \end{pmatrix}$.

1. Montrer que X vérifie la relation $MX = 73Y$.
2. Calculer MN à la calculatrice puis en déduire que M est inversible et déterminer M^{-1}.
3. En déduire une équation cartésienne de $\mathscr{P}$.

Exercice 25 Transformations du plan

À quelles transformations du plan muni d'un r.o.n. direct ces matrices de transition correspondent-elles ?

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} -4 & 0 \\ 0 & -4 \end{pmatrix} \qquad E = \begin{pmatrix} -\sqrt{3}/2 & 1/2 \\ -1/2 & -\sqrt{3}/2 \end{pmatrix}$$

$$B = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/3 \end{pmatrix} \qquad D = \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix} \qquad F = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercice 26 Rotations quelconques

1. On donne $A(3, 1)$ et $B(5, -4)$ deux points du plan muni d'un r.o.n. direct. À l'aide de représentations matricielles, donner les coordonnées du point B', image de B par la rotation de centre A et d'angle $-\frac{\pi}{2}$.
   Au préalable, on pourra se ramener à l'origine par une translation.
2. Déterminer les coordonnées du point M', image du point $M(x, y)$ par la rotation d'angle $\alpha \in \mathbb{R}$ et de centre $C(a, b)$.

Exercice 27 La règle d'or

Un constructeur d'articles mathématiques pour les enseignants fabrique trois modèles de très haute précision : des règles, des équerres et des compas. La conception de chaque modèle nécessite le passage par trois machines.
La fabrication d'une règle utilise 8 s de la première machine, 10 s de la deuxième et 14 s de la troisième. Une équerre passe 6 s dans la première, 6 s dans la deuxième et 10 s dans la troisième. Un compas passe 12 s, 10 s et 18 s dans chacune des machines. La première machine a un coût horaire de 0,25 €/s, la deuxième 0,20 €/s et la troisième 0,15 €/s.

1. Déterminer le coût de revient de chaque modèle à l'aide de représentations matricielles.
2. Le constructeur souhaite que les coûts de revient par modèle soient les suivants : 5 € la règle, 3,50 € l'équerre et 6,50 € le compas. Déterminer les nouveaux coûts horaires par machine qu'il doit atteindre.

Exercice 28 Les trois militaires

Quatre candidats et néanmoins amis ont obtenu les résultats suivants au concours d'entrée de la prestigieuse école militaire du Mas.

	Français	Maths	Anglais	Culture G.	Total
D'Artagnan	10	8	15	16	211
Athos	17	12	7	11	208
Porthos	8	15	9	13	206
Aramis	12	7	14	10	190

Déterminer, à l'aide d'une représentation matricielle et de la calculatrice, les coefficients qui ont été appliqués.

Exercice 29 Matrices, composition de fonctions homographiques et suite récurrente

1. On considère la fonction homographique f définie pour tout réel $x \neq 3$ par $f(x) = \frac{3x+2}{x-3}$ et l'on associe à la fonction f la matrice $F = \begin{pmatrix} 3 & 2 \\ 1 & -3 \end{pmatrix}$.

   Pour tout réel $x \neq 3$, on pose $X = \begin{pmatrix} x \\ 1 \end{pmatrix}$.

   Calculer le produit FX. À quel nombre peut-on associer cette matrice produit ?
2. Procéder de même pour la fonction homographique g définie pour tout réel $x \neq 2$ par $g(x) = \frac{x-2}{2x-4}$.
3. Déterminer formellement $(f \circ g)(x)$ puis calculer le produit FGX.
4. En utilisant un calcul matriciel, déterminer de manière formelle $(g \circ f)(x)$.
5. (a) Calculer le produit $H = VDV^{-1} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ où V est la matrice de l'ex. 5.

   (b) En déduire l'expression de H^n en fonction de V, D et V^{-1} puis en fonction de $n \in \mathbb{N}$.

   (c) Soit $(u_n)_{\mathbb{N}}$ la suite définie par récurrence par $u_0 = 0$, $u_{n+1} = \frac{5u_n - 9}{3u_n - \frac{11}{2}}$ et l'on pose $U_n = \begin{pmatrix} u_n \\ 1 \end{pmatrix}$.
   Exprimer U_{n+1} en fonction de U_n puis en déduire U_n en fonction de U_0.
   Exprimer u_n en fonction de n puis déterminer la limite de la suite $(u_n)_{\mathbb{N}}$.

Exercice 30 Exponentielle de matrice et système d'équations différentielles

1. Exponentielle de matrice
   Soit A une matrice carrée d'ordre 3 telle que $A^2 \neq O_3$ et $A^3 = O_3$.
   On pose, pour tout $t \in \mathbb{R}$, $E(t) = I_3 + tA + \frac{t^2}{2}A^2$.

   (a) Vérifier que $E(t)E(t') = E(t+t')$.

   (b) Vérifier que $E(t)E(-t) = I_3$. Que peut-on en déduire pour tout $t \in \mathbb{R}$?

   (c) Déterminer $E'(t)$, la matrice des dérivées des coefficients de $E(t)$.
2. Équation différentielle
   Soit $a \in \mathbb{R}$. On s'intéresse aux fonctions dérivables u telles que $u' = au$.
   Vérifier que la fonction f définie par $f(x) = e^{ax}$ vérifie cette équation différentielle.

3. Système d'équations différentielles
   On s'intéresse aux fonctions dérivables u, v et w telles que
   $\left\{\begin{array}{lcl} u' & = & 2u+v+2w \\ v' & = & -u-v-w \\ w' & = & -u-w. \end{array}\right.$ On peut écrire ce système différentiel sous forme matricielle $U' = \begin{pmatrix} u' \\ v' \\ w' \end{pmatrix} = A \begin{pmatrix} u \\ v \\ w \end{pmatrix} = AU.$
   (a) Vérifier que $A^2 \neq O_3$ et $A^3 = O_3$.
   (b) Vérifier que, pour tous a, b et $c \in \mathbb{R}$, les fonctions définies par
   $\begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix} = E(t). \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ sont solutions du système différentiel.

Glissez vers les pages 285 et 289 afin de réaliser les devoirs n^{os} 4 et 5.

EXERCICES

Corrigé des exercices

MATRICES

Activité 1 *à* 3
Voici les matrices que l'on obtient successivement :

$$\begin{array}{c} \\ \textit{Club} \\ \textit{Asso} \end{array}\begin{array}{c} \begin{array}{ccc} \textit{2de} & \textit{1re} & \textit{Tale} \end{array} \\ \begin{pmatrix} 32 & 46 & 72 \\ 43 & 24 & 17 \end{pmatrix} \end{array} = H, \qquad \begin{array}{c} \\ \textit{Club} \\ \textit{Asso} \end{array}\begin{array}{c} \begin{array}{ccc} \textit{2de} & \textit{1re} & \textit{Tale} \end{array} \\ \begin{pmatrix} 29 & 41 & 67 \\ 21 & 12 & 9 \end{pmatrix} \end{array} = M,$$

$$\begin{array}{c} \\ \textit{Club} \\ \textit{Asso} \end{array}\begin{array}{c} \begin{array}{ccc} \textit{2de} & \textit{1re} & \textit{Tale} \end{array} \\ \begin{pmatrix} 61 & 87 & 139 \\ 64 & 36 & 26 \end{pmatrix} \end{array} = H + M,$$

$$\begin{array}{c} \\ \textit{Club} \\ \textit{Asso} \end{array}\begin{array}{c} \begin{array}{ccc} \textit{2de} & \textit{1re} & \textit{Tale} \end{array} \\ \begin{pmatrix} 183 & 261 & 417 \\ 192 & 108 & 78 \end{pmatrix} \end{array} = 3(H+M) = 3H + 3M = L,$$

$$\begin{array}{c} \\ \textit{2nde} \\ \textit{1re} \\ \textit{Tale} \end{array}\begin{array}{c} \begin{array}{cc} \textit{Club} & \textit{Asso} \end{array} \\ \begin{pmatrix} 183 & 192 \\ 261 & 108 \\ 417 & 78 \end{pmatrix} \end{array} = L^{\top} \qquad \textit{(échange lignes et colonnes)}$$

$$\text{et} \quad L \times \begin{pmatrix} 5 \\ 3 \\ 4 \end{pmatrix} = \begin{array}{c} \\ \textit{Club} \\ \textit{Asso} \end{array}\begin{array}{c} \begin{array}{ccc} \textit{2de} & \textit{1re} & \textit{Tale} \end{array} \\ \begin{pmatrix} 183 & 261 & 417 \\ 192 & 108 & 78 \end{pmatrix} \end{array} . \begin{pmatrix} 5 \\ 3 \\ 4 \end{pmatrix}$$

$$= \begin{array}{c} \textit{Club} \\ \textit{Asso} \end{array} \begin{pmatrix} 5 \times 183 + 3 \times 261 + 4 \times 417 \\ 5 \times 192 + 3 \times 108 + 4 \times 78 \end{pmatrix} = \begin{pmatrix} 3366 \\ 1596 \end{pmatrix}.$$

Activité 4 *On peut résoudre ce système par substitutions successives ou par combinaisons linéaires pertinentes mais on peut aussi remarquer que ce système peut s'écrire* $\begin{pmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ -2 & 4 & -1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

Puisque l'on a vu dans le cours que $V = \begin{pmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ -2 & 4 & -1 \end{pmatrix}$ *est inversible, de matrice inverse* $V^{-1} = U = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix}$, *on a* $(S) \iff V \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$

$$\overset{U\times}{\iff} UV \begin{pmatrix} x \\ y \\ z \end{pmatrix} = U \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} . \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix}.$$

Activité 5 *Voici les coordonnées que l'on obtient après les transformations du plan stipulées.*

	$A(4, 3)$	$B(2, 0)$	$C(0, -3)$	$D(-1, 2)$	$E(3, -4)$	$F(-2, -1)$	$M(x, y)$	$\mathcal{M}atrice$
$\mathcal{T}r_{\vec{u}\binom{3}{2}}$	$(7, 5)$	$(5, 2)$	$(3, -1)$	$(2, 4)$	$(6, -2)$	$(1, 1)$	$(x+3, y+2)$	$+\binom{3}{2}$
$\mathcal{T}r_{\vec{v}\binom{-2}{1}}$	$(2, 4)$	$(0, 1)$	$(-2, -2)$	$(-3, 3)$	$(1, -3)$	$(-4, 0)$	$(x-2, y+1)$	$+\binom{-2}{1}$
$\mathscr{S}ym_{Ox}$	$(4, -3)$	$(2, 0)$	$(0, 3)$	$(-1, -2)$	$(3, 4)$	$(-2, 1)$	$(x, -y)$	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$
$\mathscr{S}ym_{Oy}$	$(-4, 3)$	$(-2, 0)$	$(0, -3)$	$(1, 2)$	$(-3, -4)$	$(2, -1)$	$(-x, y)$	$\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$
$\mathscr{S}ym_{O}$	$(-4, -3)$	$(-2, 0)$	$(0, 3)$	$(1, -2)$	$(-3, 4)$	$(2, 1)$	$(-x, -y)$	$\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$
$\mathcal{R}ot_{O,\frac{\pi}{2}}$	$(-3, 4)$	$(0, 2)$	$(3, 0)$	$(-2, -1)$	$(4, 3)$	$(1, -2)$	$(-y, x)$	$\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}$
$\mathcal{R}ot_{O,-\frac{\pi}{2}}$	$(3, -4)$	$(0, -2)$	$(-3, 0)$	$(2, 1)$	$(-4, -3)$	$(-1, 2)$	$(y, -x)$	$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$
$\mathcal{H}om_{O,-2}$	$(-8, -6)$	$(-4, 0)$	$(0, 6)$	$(2, -4)$	$(-6, 8)$	$(4, 2)$	$(-2x, -2y)$	$\begin{pmatrix}-2 & 0\\0 & -2\end{pmatrix}$

et l'on observe que $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix} = \begin{pmatrix}\cos(\pi) & -\sin(\pi)\\ \sin(\pi) & \cos(\pi)\end{pmatrix}$,

$$\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix} = \begin{pmatrix}\cos(\frac{\pi}{2}) & -\sin(\frac{\pi}{2})\\ \sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2})\end{pmatrix} \quad \textit{et} \quad \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix} = \begin{pmatrix}\cos(-\frac{\pi}{2}) & -\sin(-\frac{\pi}{2})\\ \sin(-\frac{\pi}{2}) & \cos(-\frac{\pi}{2})\end{pmatrix}.$$

Pour les exercices 1 à 16, les calculs effectués dans un exercice pourront être utilisés dans les suivants.

Exercice 1

$$L+S = \begin{pmatrix}0 & 1 & -1\\-3 & 4 & -3\\-1 & 1 & 0\end{pmatrix}_{3\times3} + \begin{pmatrix}1 & 4 & 2\\1 & 3 & -3\\1 & -2 & 2\end{pmatrix}_{3\times3} = \begin{pmatrix}0+1 & 1+4 & -1+2\\-3+1 & 4+3 & -3-3\\-1+1 & 1-2 & 0+2\end{pmatrix}_{3\times3}$$
$$= \begin{pmatrix}1 & 5 & 1\\-2 & 7 & -6\\0 & -1 & 2\end{pmatrix}_{3\times3}$$

$E+F$: E est de taille 1×3 et F est de taille 3×1 : on ne peut les ajouter.

$$EF = \begin{pmatrix}-2 & 3 & 1\end{pmatrix}_{1\times3} \times \begin{pmatrix}4\\-5\\7\end{pmatrix}_{3\times1} = \begin{pmatrix}-2\times4+3\times(-5)+1\times7\end{pmatrix}_{1\times1} = \begin{pmatrix}-16\end{pmatrix}_{1\times1}$$

$$FE = \begin{pmatrix}4\\-5\\7\end{pmatrix}_{3\times1} \times \begin{pmatrix}-2 & 3 & 1\end{pmatrix}_{1\times3} = \begin{pmatrix}4\times(-2) & 4\times3 & 4\times1\\(-5)\times(-2) & (-5)\times3 & (-5)\times1\\7\times(-2) & 7\times3 & 7\times1\end{pmatrix}_{3\times3}$$
$$= \begin{pmatrix}-8 & 12 & 4\\10 & -15 & -5\\-14 & 21 & 7\end{pmatrix}_{3\times3}$$

$$GF = \begin{pmatrix} 2 & 1 & -3 \\ -2 & 3 & -1 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} 4 \\ -5 \\ 7 \end{pmatrix}_{3\times 1} = \begin{pmatrix} 2\times 4 - 5\times 1 - 3\times 7 \\ -2\times 4 - 5\times 3 - 1\times 7 \end{pmatrix}_{2\times 1} = \begin{pmatrix} -18 \\ -30 \end{pmatrix}_{2\times 1}$$

FG : F est de taille 3×1 et G de taille 2×3 : on ne peut les multiplier dans ce sens.

EG : E est de taille 1×3 et G de taille 2×3 : on ne peut les multiplier dans ce sens.

GE : G est de taille 2×3 et E de taille 1×3 : on ne peut les multiplier dans ce sens.

$$\begin{aligned} GH &= \begin{pmatrix} 2 & 1 & -3 \\ -2 & 3 & -1 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} 4 & 2 \\ -1 & -5 \\ 3 & -2 \end{pmatrix}_{3\times 2} \\ &= \begin{pmatrix} 2\times 4 - 1\times 1 - 3\times 3 & 2\times 2 - 1\times 5 - 3(-2) \\ -2\times 4 - 3\times 1 - 3\times 1 & -2\times 2 - 5\times 3 - 1(-2) \end{pmatrix}_{2\times 2} = \begin{pmatrix} -2 & 5 \\ -14 & -17 \end{pmatrix}_{2\times 2} \end{aligned}$$

$$\begin{aligned} HG &= \begin{pmatrix} 4 & 2 \\ -1 & -5 \\ 3 & -2 \end{pmatrix}_{3\times 2} \times \begin{pmatrix} 2 & 1 & -3 \\ -2 & 3 & -1 \end{pmatrix}_{2\times 3} \\ &= \begin{pmatrix} 4\times 2 - 2\times 2 & 4\times 1 + 2\times 3 & 4(-3) - 1\times 2 \\ -1\times 2 - 5(-2) & -1\times 1 - 5\times 3 & -1(-3) - 5(-1) \\ 3\times 2 - 2(-2) & 3\times 1 - 2\times 3 & 3(-3) - 2(-1) \end{pmatrix}_{3\times 3} \\ &= \begin{pmatrix} 4 & 10 & -14 \\ 8 & -16 & 8 \\ 10 & -3 & -7 \end{pmatrix}_{3\times 3} \end{aligned}$$

$$\begin{aligned} 2I_3 - 3L &= 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_{3\times 3} - 3\begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}_{3\times 3} \\ &= \begin{pmatrix} 2\times 1 - 3\times 0 & 2\times 0 - 3\times 1 & 2\times 0 - 3(-1) \\ 2\times 0 - 3(-3) & 2\times 1 - 3\times 4 & 2\times 0 - 3(-3) \\ 2\times 0 - 3(-1) & 2\times 0 - 3\times 1 & 2\times 1 - 3\times 0 \end{pmatrix}_{3\times 3} \\ &= \begin{pmatrix} 2 & -3 & 3 \\ 9 & -10 & 9 \\ 3 & -3 & 2 \end{pmatrix}_{3\times 3} \end{aligned}$$

$$\begin{aligned} L^2 &= \begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}_{3\times 3} \begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}_{3\times 3} \\ &= \begin{pmatrix} 0\times 0 - 3\times 1 - 1(-1) & 0\times 1 + 1\times 4 - 1\times 1 & 0(-1) - 1\times 3 - 1\times 0 \\ -3\times 0 - 4\times 3 - 3(-1) & -3\times 1 + 4\times 4 - 3\times 1 & -3(-1) - 4\times 3 - 3\times 0 \\ -1\times 0 - 1\times 3 - 0\times 1 & -1\times 1 + 1\times 4 + 0\times 1 & -1(-1) - 1\times 3 + 0\times 0 \end{pmatrix}_{3\times 3} \\ &= \begin{pmatrix} -2 & 3 & -3 \\ -9 & 10 & -9 \\ -3 & 3 & -2 \end{pmatrix} \end{aligned}$$

$$N^2 + 8N = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix} + 8\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix}$$

$$N^2+8N=\begin{pmatrix}6&2&3\\4&4&1\\10&4&7\end{pmatrix}+\begin{pmatrix}8&8&8\\8&-8&8\\32&16&8\end{pmatrix}=\begin{pmatrix}14&10&11\\12&-4&9\\42&20&15\end{pmatrix}$$

$$N^3=N^2.N=\begin{pmatrix}6&2&3\\4&4&1\\10&4&7\end{pmatrix}.\begin{pmatrix}1&1&1\\1&-1&1\\4&2&1\end{pmatrix}=\begin{pmatrix}20&10&11\\12&2&9\\42&20&21\end{pmatrix}$$

$$K^2=\begin{pmatrix}1&1&0\\1&1&1\\0&-1&1\end{pmatrix}.\begin{pmatrix}1&1&0\\1&1&1\\0&-1&1\end{pmatrix}=\begin{pmatrix}2&2&1\\2&1&2\\-1&-2&0\end{pmatrix}$$

$2A-3B$: A et donc $2A$ sont de taille 2×2 ; B et $-3B$, sont de taille 3×3 : on ne peut donc les ajouter.

$$A^2=\begin{pmatrix}1&2\\0&1\end{pmatrix}.\begin{pmatrix}1&2\\0&1\end{pmatrix}=\begin{pmatrix}1&4\\0&1\end{pmatrix}$$

$$A^3=AA^2=\begin{pmatrix}1&4\\0&1\end{pmatrix}.\begin{pmatrix}1&2\\0&1\end{pmatrix}=\begin{pmatrix}1&6\\0&1\end{pmatrix}$$

$$B^2=\begin{pmatrix}1&0&1\\0&0&1\\1&0&1\end{pmatrix}.\begin{pmatrix}1&0&1\\0&0&1\\1&0&1\end{pmatrix}=\begin{pmatrix}2&0&2\\1&0&1\\2&0&2\end{pmatrix}$$

$$B^3=B^2B=\begin{pmatrix}2&0&2\\1&0&1\\2&0&2\end{pmatrix}.\begin{pmatrix}1&0&1\\0&0&1\\1&0&1\end{pmatrix}=\begin{pmatrix}4&0&4\\2&0&2\\4&0&4\end{pmatrix}$$

$$CJ=\begin{pmatrix}1&2\\3&2\end{pmatrix}.\begin{pmatrix}1&2\\-1&3\end{pmatrix}=\begin{pmatrix}-1&8\\1&12\end{pmatrix}$$

$$TU=\begin{pmatrix}-1/\sqrt2&1/\sqrt2\\1/\sqrt2&1/\sqrt2\end{pmatrix}.\begin{pmatrix}3&0\\0&1\end{pmatrix}=\begin{pmatrix}-3/\sqrt2&1/\sqrt2\\3/\sqrt2&1/\sqrt2\end{pmatrix}$$

$$T^2=\begin{pmatrix}-1/\sqrt2&1/\sqrt2\\1/\sqrt2&1/\sqrt2\end{pmatrix}.\begin{pmatrix}-1/\sqrt2&1/\sqrt2\\1/\sqrt2&1/\sqrt2\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2$$

$$RS=\begin{pmatrix}0&2&-1\\3&-2&0\\-2&2&1\end{pmatrix}.\begin{pmatrix}1&4&2\\1&3&-3\\1&-2&2\end{pmatrix}=\begin{pmatrix}1&8&-8\\1&6&12\\1&-4&-8\end{pmatrix}$$

Exercice 2 On a $\begin{pmatrix}5&2\\4&1\end{pmatrix}\begin{pmatrix}2&-1\\3&4\end{pmatrix}=\begin{pmatrix}16&3\\11&0\end{pmatrix}$.

Exercice 3 On a $\Delta\times\begin{pmatrix}1&1&1\\0&1&1\\1&0&0\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&1\\3&1&1\end{pmatrix}\begin{pmatrix}1&1&1\\0&1&0\\1&0&0\end{pmatrix}=\begin{pmatrix}1&1&1\\1&1&0\\4&4&3\end{pmatrix}$

et $\Delta\times\begin{pmatrix}1&1&1\\1&2&1\\0&-1&-1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&1\\3&1&1\end{pmatrix}\begin{pmatrix}1&1&1\\1&2&1\\0&-1&-1\end{pmatrix}=\begin{pmatrix}1&1&1\\1&1&0\\4&4&3\end{pmatrix}$.

Il existe donc deux matrices distinctes, Ω et Ω', telles que $\Delta\Omega=\Delta\Omega'$. La matrice Δ n'est donc pas inversible. En effet, si elle l'était, on aurait $\Delta^{-1}\Delta\Omega=\Delta^{-1}\Delta\Omega'$ ce qui contredit $\Omega\neq\Omega'$.

Exercice 4 Inverse d'une matrice 2×2

1. On a $MM' = M'M = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \det(M) I_2$.
2. Si $\det(M) \neq 0$, on a $\left(\frac{1}{\det(M)} M'\right).M = I_2$: M est alors inversible, de matrice inverse
$M^{-1} = \frac{1}{\det(M)} M' = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
3. (a) Si M est inversible et $\det(M) = 0$, on a
$$\begin{aligned} M' &= I_2 M' = \left(M^{-1}M\right).M' = M^{-1}\left(MM'\right) = M^{-1}.\left(\det(M) I_2\right) \\ &= 0.M^{-1} = O_2. \end{aligned}$$
   (b) Ainsi, Les coefficients de M', et donc de M, sont tous nuls et $M = O_2$.
   (c) Puisque la matrice nulle n'est pas inversible ($\forall A,\ A \times O_2 \neq I_2$), ceci contredit notre hypothèse sur M. Le déterminant de M ne peut donc être nul lorsque M est inversible.

On a ainsi démontré que $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible *ssi,* $\det(M) = ad - bc \neq 0$

et que dans ce cas, sa matrice inverse est $M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Exercice 5

$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$: $\det(A) = 1 \times 1 - 2 \times 0 = 1 \neq 0$ donc A est inversible et $A^{-1} = \frac{1}{1}\begin{pmatrix} 1 & -2 \\ -0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$.

$C = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$: $\det(C) = 1 \times 2 - 3 \times 2 = -4 \neq 0$ donc C est inversible

et $C^{-1} = \frac{1}{-4}\begin{pmatrix} 2 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{pmatrix}$.

$J = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}$: $\det(J) = 1 \times 3 + 1 \times 2 = 5 \neq 0$ donc J est inversible et $J^{-1} = \frac{1}{5}\begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}$.

$Q = \begin{pmatrix} 2 & -6 \\ -3 & 9 \end{pmatrix}$: $\det(Q) = 2 \times 9 - (-6)(-3) = 0$ donc Q n'est pas inversible.

On a vu que $T^2 = I_2$ donc T est inversible et $T^{-1} = T = \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$.

$U = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$: $\det(U) = 3 \times 1 - 0 = 3 \neq 0$ donc U est inversible

et $U^{-1} = \frac{1}{3}\begin{pmatrix} 1 & -0 \\ -0 & 3 \end{pmatrix} = \begin{pmatrix} 1/3 & 0 \\ 0 & 1 \end{pmatrix}$.

$V = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$: $\det(V) = 2 \times 2 - 3 \times 1 = 1 \neq 0$ donc V est inversible et $V^{-1} = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$.

Exercice 6 Calcul d'inverse avec le pivot de Gauss

· $S = \begin{pmatrix} 1 & 4 & 2 \\ 1 & 3 & -3 \\ 1 & -2 & 2 \end{pmatrix} \xrightarrow[L_1-L_3 \to L_3]{L_1-L_2 \to L_2} \begin{pmatrix} 1 & 4 & 2 \\ 0 & 1 & 5 \\ 0 & 6 & 0 \end{pmatrix} \xrightarrow[L_3-6L_2 \to L_3]{L_1-4L_2 \to L_1}$
$\begin{pmatrix} 1 & 0 & -18 \\ 0 & 1 & 5 \\ 0 & 0 & -30 \end{pmatrix} \xrightarrow{-\frac{1}{30}L_3 \to L_3} \begin{pmatrix} 1 & 0 & -18 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[L_2-5L_3 \to L_2]{L_1+18L_3 \to L_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$

$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[L_1-L_3 \to L_3]{L_1-L_2 \to L_2} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \xrightarrow[L_3-6L_2 \to L_3]{L_1-4L_2 \to L_1}$
$\begin{pmatrix} -3 & 4 & 0 \\ 1 & -1 & 0 \\ -5 & 6 & -1 \end{pmatrix} \xrightarrow{-\frac{1}{30}L_3 \to L_3} \begin{pmatrix} -3 & 4 & 0 \\ 1 & -1 & 0 \\ 1/6 & -1/5 & 1/30 \end{pmatrix} \xrightarrow[L_2-5L_3 \to L_2]{L_1+18L_3 \to L_1}$
$\begin{pmatrix} 0 & 2/5 & 3/5 \\ 1/6 & 0 & -1/6 \\ 1/6 & -1/5 & 1/30 \end{pmatrix} = \frac{1}{30}\begin{pmatrix} 0 & 12 & 18 \\ 5 & 0 & -5 \\ 5 & -6 & 1 \end{pmatrix} = S^{-1}$

· $R = \begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix} \xrightarrow{L_2+L_3 \to L_2} \begin{pmatrix} 0 & 2 & -1 \\ 1 & 0 & 1 \\ -2 & 2 & 1 \end{pmatrix} \xrightarrow{L_3+2L_2-L_1 \to L_3} \begin{pmatrix} 0 & 2 & -1 \\ 1 & 0 & 1 \\ 0 & 0 & 4 \end{pmatrix}$
$\xrightarrow[\frac{1}{4}L_3 \to L_3]{L_1 \leftrightarrow L_2} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & -1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[\frac{1}{2}L_2+\frac{1}{2}L_3 \to L_2]{L_1-L_3 \to L_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$

$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{L_2+L_3 \to L_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{L_3+2L_2-L_1 \to L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ -1 & 2 & 3 \end{pmatrix} \xrightarrow[\frac{1}{4}L_3 \to L_3]{L_1 \leftrightarrow L_2}$
$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ -1/4 & 1/2 & 3/4 \end{pmatrix} \xrightarrow[\frac{1}{2}L_2+\frac{1}{2}L_3 \to L_2]{L_1-L_3 \to L_1} \begin{pmatrix} 1/4 & 1/2 & 1/4 \\ 3/8 & 1/4 & 3/8 \\ -1/4 & 1/2 & 3/4 \end{pmatrix} = \frac{1}{8}\begin{pmatrix} 2 & 4 & 2 \\ 3 & 2 & 3 \\ -2 & 4 & 6 \end{pmatrix} = R^{-1}$

· $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \xrightarrow[L_3-L_1 \to L_1]{L_1-L_2 \to L_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ qui ne peut être ainsi transformée en I_3 donc B n'est pas inversible.

· Ainsi, $(RS)^{-1} = S^{-1}R^{-1} = \frac{1}{30}\begin{pmatrix} 0 & 12 & 18 \\ 5 & 0 & -5 \\ 5 & -6 & 1 \end{pmatrix} \times \frac{1}{8}\begin{pmatrix} 2 & 4 & 2 \\ 3 & 2 & 3 \\ -2 & 4 & 6 \end{pmatrix}$

$(RS)^{-1} = \begin{pmatrix} 0 & 2/5 & 3/5 \\ 1/12 & 0 & -1/12 \\ -1/24 & 1/20 & -1/120 \end{pmatrix}$.

CORRIGÉS

Exercice 7 Résolution de systèmes linéaires avec le pivot de Gauss

$$S_a:\left\{\begin{array}{rcl} x+3y+4z &=& 7\\ 2x-4y+z &=& 13\\ 3x-y+2z &=& 11\end{array}\right. \underset{L_3-3L_1\to L_3}{\overset{L_2-2L_1\to L_2}{\Longleftrightarrow}} \left\{\begin{array}{rcl} x+3y+4z &=& 7\\ 0x-10y-7z &=& -1\\ 0x-10y-10z &=& -10\end{array}\right.$$

$$\underset{L_3-L_2\to L_2}{\Longleftrightarrow}\left\{\begin{array}{rcl} x+3y+4z &=& 7\\ -10y-7z &=& -1\\ 0y-3z &=& -9\end{array}\right. \underset{-\frac{1}{3}L_3\to L_3}{\overset{-\frac{1}{10}L_2\to L_2}{\Longleftrightarrow}} \left\{\begin{array}{rcl} x+3y+4z &=& 7\\ y+\frac{7}{10}z &=& \frac{1}{10}\\ z &=& 3\end{array}\right.$$

$$\overset{L_1\leftrightarrow L_2}{\Longleftrightarrow}\left\{\begin{array}{rclcl} z &=& 3 && \\ y &=& \frac{1}{10}-\frac{7}{10}z &=& -2\\ x &=& 7-3y-4z &=& 1\end{array}\right. : \quad \mathscr{S}_a=\{(1;-2;3)\}.$$

$$S_b:\left\{\begin{array}{rcl} 2a+b-4c &=& -15\\ 2b+6c &=& 20\\ a-b-3c &=& -12\end{array}\right. \underset{\frac{1}{2}L_2\to L_2}{\overset{L_1\leftrightarrow L_3}{\Longleftrightarrow}} \left\{\begin{array}{rcl} a-b-3c &=& -12\\ b+3c &=& 10\\ 2a+b-4c &=& -15\end{array}\right.$$

$$\underset{L_3-2L_1\to L_3}{\Longleftrightarrow}\left\{\begin{array}{rcl} a-b-3c &=& -12\\ b+3c &=& 10\\ 0a+3b+2c &=& 9\end{array}\right. \underset{L_3-3L_2\to L_3}{\Longleftrightarrow} \left\{\begin{array}{rcl} a-b-3c &=& -12\\ b+3c &=& 10\\ 0b-7c &=& -21\end{array}\right.$$

$$\underset{-\frac{1}{7}L_3\to L_3}{\Longleftrightarrow}\left\{\begin{array}{rcl} a-b-3c &=& -12\\ b+3c &=& 10\\ c &=& 3\end{array}\right. \overset{L_1\leftrightarrow L_3}{\Longleftrightarrow} \left\{\begin{array}{rclcl} c &=& 3 &&\\ b &=& 10-3c &=& 1\\ a &=& -12+b+3c &=& -2\end{array}\right. :$$

$\mathscr{S}_b=\{(-2;1;3)\}$.

$$S_c:\left\{\begin{array}{rcl} 3u-4v+5w &=& -5\\ 2u+3v-4w &=& 17\\ 4u-3v+2w &=& 5\end{array}\right. \underset{3L_3-4L_1\to L_3}{\overset{3L_2-2L_1\to L_2}{\Longleftrightarrow}} \left\{\begin{array}{rcl} 3u-4v+5w &=& -5\\ 0u+17v-22w &=& 61\\ 0u+7v-14w &=& 35\end{array}\right.$$

$$\underset{17L_3-7L_2\to L_3}{\overset{\frac{1}{3}L_1\to L_1}{\Longleftrightarrow}}\left\{\begin{array}{rcl} u-\frac{4}{3}v+\frac{5}{3}w &=& -\frac{5}{3}\\ 17v-22w &=& 61\\ 0v-84w &=& 168\end{array}\right. \underset{-\frac{1}{84}L_3\to L_3}{\overset{\frac{1}{17}L_2\to L_2}{\Longleftrightarrow}} \left\{\begin{array}{rcl} u-\frac{4}{3}v+\frac{5}{3}w &=& -\frac{5}{3}\\ v-\frac{22}{17}w &=& \frac{61}{17}\\ w &=& -2\end{array}\right.$$

$$\overset{L_1\leftrightarrow L_2}{\Longleftrightarrow}\left\{\begin{array}{rclcl} w &=& -2 &&\\ v &=& \frac{61}{17}+\frac{22}{17}w &=& 1\\ u &=& -\frac{5}{3}+\frac{4}{3}v-\frac{5}{3}w &=& 3\end{array}\right. : \quad \mathscr{S}_c=\{(3;1;-2)\}.$$

Exercice 8 Calcul d'inverse par annulation d'un polynôme

On utilise les calculs effectués dans l'exercice 1.

1. On a $L^2-3L+2I_3=\begin{pmatrix}-2&3&-3\\-9&10&-9\\-3&3&-2\end{pmatrix}+\begin{pmatrix}2&-3&3\\9&-10&9\\3&-3&2\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}=O_3$

   d'où $I_3=\frac{1}{2}\left(3L-L^2\right)=\frac{1}{2}\left(3I_3-L\right).L$: L est donc inversible et
   $$L^{-1}=\frac{1}{2}\left(3I_3-L\right)=\frac{1}{2}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}-\frac{1}{2}\begin{pmatrix}0&1&-1\\-3&4&-3\\-1&1&0\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3&-1&1\\3&-1&3\\1&-1&3\end{pmatrix}.$$

2. $N^2+8N+6I_3=\begin{pmatrix}14&10&11\\12&-4&9\\42&20&15\end{pmatrix}+6\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}20&10&11\\12&2&9\\42&20&21\end{pmatrix}=N^3$

   d'où $I_3=\frac{1}{6}\left(N^3-N^2-8N\right)=\frac{1}{6}\left(N^2-N-8I_3\right).N$: N est donc inversible
   $$N^{-1}=\frac{1}{6}\left(N^2-N-8I_3\right)$$

$$N^{-1} = \frac{1}{6}\begin{pmatrix} 6 & 2 & 3 \\ 4 & 4 & 1 \\ 10 & 4 & 7 \end{pmatrix} - \frac{1}{6}\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix} - \frac{8}{6}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$N^{-1} = \frac{1}{6}\begin{pmatrix} -3 & 1 & 2 \\ 3 & -3 & 0 \\ 6 & 2 & -2 \end{pmatrix}.$$

3. On a $\quad K - I_3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$

   d'où $\quad (K - I_3)^3 = ... = O_3$.

   Puisque $\quad (K-I_3)^2 = (K-I_3)(K-I_3) = K^2 - I_3K - KI_3 + I_3^2 = K^2 - 2K + I_3$,

   $$(K - I_3)^3 = (K - I_3)(K^2 - 2K + I_3) = K^3 - 2K^2 + K - I_3K^2 + 2I_3K - I_3^2$$
   $$= K^3 - 3K^2 + 3K - I_3.$$

   Ainsi, $\quad I_3 = K^3 - 3K^2 + 3K = K\left(K^2 - 3K + 3I_3\right)$: $\quad K$ est donc inversible et

   $$K^{-1} = K^2 - 3K + 3I_3 = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ -1 & -2 & 0 \end{pmatrix} - 3\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} + 3\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

   $$K^{-1} = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 1 & -1 \\ -1 & 1 & 0 \end{pmatrix}.$$

4. On a $\quad Q^2 - 11Q = \begin{pmatrix} 22 & -66 \\ -33 & 99 \end{pmatrix} - 11\begin{pmatrix} 2 & -6 \\ -3 & 9 \end{pmatrix} = O_2$. $\quad$ Pour autant, on a vu que Q n'est pas inversible puisque son déterminant est nul. Il ne suffit donc pas de trouver un polynôme annulateur pour obtenir une matrice inversible.

5. Supposons que M soit inversible. On a

   $$M^3 - 2M^2 - M = O \iff M(M^2 - 2M - I) = O$$
   $$\iff M^{-1}M(M^2 - 2M - I) = M^{-1}O \iff M^2 - 2M - I = O$$
   $$\iff M^2 - 2M = I \iff M(M - 2I) = I$$
   $$\iff M^{-1}M(M - 2I) = M^{-1}I \iff M^{-1} = M - 2I.$$

   On a démontré que si M est inversible, alors son inverse est $M - 2I$. Pour autant, M n'est pas nécessairement inversible. En effet, la matrice nulle vérifie très bien l'identité de départ.

   En revanche, si le polynôme annulateur a un coefficient constant non nul, alors la matrice est inversible et l'on détermine son inverse en suivant la méthode des premiers items.

Exercice 9 Puissances

1. D'après les calculs effectués dans l'exercice 1, on conjecture que, pour tout $n \in \mathbb{N}$, $A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$.

   Soit $\mathscr{P}_n$ cette proposition que nous allons démontrer par récurrence.

   · On a $\quad A^0 = I_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \times 0 \\ 0 & 1 \end{pmatrix}$: $\quad \mathscr{P}_0$ est vraie.

   · Supposons que $\mathscr{P}_n$ soit vraie pour un certain $n \in \mathbb{N}$.

CORRIGÉS

$$A^{n+1} = A^n.A = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\times 1 + 2n \times 0 & 2\times 1 + 2n\times 1 \\ 0\times 1 + 1\times 0 & 0\times 2 + 1 \times 1 \end{pmatrix}$$

$$A^{n+1} = \begin{pmatrix} 1 & 2n+2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2(n+1) \\ 0 & 1 \end{pmatrix}$$ et $\mathscr{P}_{n+1}$ est vraie.

· $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

2. D'après l'exercice 1, on conjecture que, pour tout $n \geqslant 2$,

$$B^n = \begin{pmatrix} 2^{n-1} & 0 & 2^{n-1} \\ 2^{n-2} & 0 & 2^{n-2} \\ 2^{n-1} & 0 & 2^{n-1} \end{pmatrix}.$$

Soit $\mathscr{Q}_n$ cette proposition que nous allons démontrer par récurrence.

· On a $B^2 = \begin{pmatrix} 2 & 0 & 2 \\ 1 & 0 & 1 \\ 2 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 2^1 & 0 & 2^1 \\ 2^0 & 0 & 2^0 \\ 2^1 & 0 & 2^1 \end{pmatrix}$: $\mathscr{Q}_2$ est vraie.

· Supposons que $\mathscr{Q}_n$ soit vraie pour un certain $n \geqslant 2$. On a

$$B^{n+1} = B^n.B = \begin{pmatrix} 2^{n-1} & 0 & 2^{n-1} \\ 2^{n-2} & 0 & 2^{n-2} \\ 2^{n-1} & 0 & 2^{n-1} \end{pmatrix} . \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2^{n-1}+2^{n-1} & 0 & 2^{n-1}+2^{n-1} \\ 2^{n-2}+2^{n-2} & 0 & 2^{n-2}+2^{n-2} \\ 2^{n-1}+2^{n-1} & 0 & 2^{n-1}+2^{n-1} \end{pmatrix} = \begin{pmatrix} 2\times 2^{n-1} & 0 & 2\times 2^{n-1} \\ 2\times 2^{n-2} & 0 & 2\times 2^{n-2} \\ 2\times 2^{n-1} & 0 & 2\times 2^{n-1} \end{pmatrix}$$

$$B^{n+1} = \begin{pmatrix} 2^n & 0 & 2^n \\ 2^{n-1} & 0 & 2^{n-1} \\ 2^n & 0 & 2^n \end{pmatrix}$$ et $\mathscr{Q}_{n+1}$ est vraie.

· $\mathscr{Q}_n$ est vraie pour tout $n \geqslant 2$.

Exercice 10 Diagonalisation

1. Soit $D = Diag(d_1; d_2; \dots; d_n)$ et pour $k \in \mathbb{N}^*$, la proposition
   $\mathscr{P}_k$: « $D^k = Diag(d_1^k; d_2^k; \dots; d_n^k)$ ».
   · On a $D^1 = D = Diag(d_1; d_2; \dots; d_n) = Diag(d_1^1; d_2^1; \dots; d_n^1)$: $\mathscr{P}_1$ est vraie.
   · Supposons que $\mathscr{P}_k$ est vraie pour un certain $k \in \mathbb{N}^*$.

   On a $(D^{k+1})_{i,j} = (D^k.D)_{i,j} = \sum_{\ell=1}^{n} (D^k)_{i,\ell}.d_{\ell,j}$

   $$(D^{k+1})_{i,j} = 0 + (D^k)_{i,i}.d_{i,j} = \begin{cases} (D^k)_{i,i}.d_{i,i} = d_i^k.d_i = d_i^{k+1} \text{ si } i = j \\ (D^k)_{i,i} \times 0 = 0 \text{ si } i \neq j. \end{cases}$$

   et $D^{k+1} = Diag(d_1^{k+1}; d_2^{k+1}; \dots; d_n^{k+1})$: $\mathscr{P}_{k+1}$ est vraie.
   · $\mathscr{P}_k$ est vraie pour tout $k \in \mathbb{N}^*$.

2. On a $M^2 = (PDP^{-1})^2 = (PDP^{-1})(PDP^{-1}) = PD(P^{-1}P)DP^{-1}$
   $M^2 = P(DI_nD)P^{-1} = PD^2P^{-1}$.
   Soit, pour $k \in \mathbb{N}^*$, la proposition $\mathscr{Q}_k$: « $M^k = PD^kP^{-1}$ ».
   · $\mathscr{Q}_1$: $M = PDP^{-1}$ est vraie par hypothèse sur M.
   · Supposons que $\mathscr{Q}_k$ est vraie pour un certain $k \in \mathbb{N}^*$.
   On a $M^{k+1} = M^kM = (PD^kP^{-1})(PDP^{-1}) = PD^k(P^{-1}P)DP^{-1}$
   $M^{k+1} = P(D^kI_nD)P^{-1} = PD^{k+1}P^{-1}$ et $\mathscr{Q}_{k+1}$ est vraie.
   · $\mathscr{Q}_k$ est vraie pour tout $k \in \mathbb{N}^*$.

3. Si D est inversible, on a
$$M(PD^{-1}P^{-1}) = PDP^{-1}PD^{-1}P^{-1} = PDD^{-1}P^{-1} = PP^{-1} = I_n$$
donc M est inversible, de matrice inverse $\quad M^{-1} = PD^{-1}P^{-1}$.

Ces propriétés sont vraies même si D n'est pas diagonale mais elle ne nous sera vraiment utile dans ce cas.

Exercice 11 Inversion de matrices diagonales

Soient $\quad D = Diag(d_1; \ldots; d_n) \quad$ et $\quad D' = Diag(d'_1; \ldots; d'_n) \quad$ deux matrices diagonales d'ordre n.

1. On a $\quad (D.D')_{i,j} = \displaystyle\sum_{k=1}^{n} d_{i,k}.d'_{k,j} = 0 + d_{i,i}.d'_{i,j} = \begin{cases} d_{i,i}.d'_{i,i} \text{ si } i=j \\ d_{i,i} \times 0 = 0 \text{ si } i \neq j. \end{cases}$
donc $\quad DD' = Diag(d_1d'_1; d_2d'_2; \ldots; d_nd'_n) = D'D \quad$ car la multiplication est commutative dans $\mathbb{K}$.
2. Il semble que la matrice D soit inversible lorsque tous ses éléments diagonaux sont non nuls. En effet, si $d_i\ \emptyset$ pout tout $i \in [\![1\,; n]\!]$, alors
$Diag(d_1; ...; d_n)Diag(\frac{1}{d_1}; ...; \frac{1}{d_n}) = Diag(d_1.\frac{1}{d_1}; ...; d_n\frac{1}{d_n})Diag(1; ...; 1) = I_n$.
La matrice $Diag(d_1; \ldots; d_n)$ est inversible, de matrice inverse $Diag(\frac{1}{d_1}; \ldots; \frac{1}{d_n})$.
3. Soit D inversible et supposons qu'il existe un indice k tel que $d_k = 0$.
On appelle δ_k la matrice telle que son seul coefficient non nul soit $(\delta)_{k,k} = 1$.
On a alors $\quad (D\delta_k)_{i,j} = \displaystyle\sum_{\ell=1}^{n} d_{i,\ell}\delta_{\ell,j} = d_{i,k}\delta_{k,j}$
$$(D\delta_k)_{i,j} = \begin{cases} d_{i,k}\delta_{k,k} = d_{k,k}\delta_{k,k} = 0 \times \delta_k = 0 \ \text{ si } i = j = k \\ 0 \ \text{ sinon.} \end{cases}$$
On a alors $\quad \delta_k = I_n\delta_k = D^{-1}D\delta_k = D^{-1}O_n = O_n \quad$ ce qui est absurde.
4. Une matrice diagonale est inversible *ssi* ses coefficients diagonaux sont tous non nuls. Sa matrice inverse est alors la matrice diagonale d'éléments diagonaux, les inverses de ses éléments diagonaux.

Exercice 12 Puissance de la diagonalisation

On utilise le résultat des exercices 10 et 11 ainsi que les calculs effectués précédemment.

1. $W = J^{-1}CJ = \frac{1}{5}\begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix}$ est diagonale.
Ainsi, $\quad C = I_2CI_2 = JJ^{-1}CJJ^{-1} = JWJ^{-1}$
et $\quad C^n = JW^nJ^{-1} = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} (-1)^n & 0 \\ 0 & 4^n \end{pmatrix}.\frac{1}{5}\begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}$
$$C^n = \frac{1}{5}\begin{pmatrix} 3(-1)^n + 2 \times 4^n & -2(-1)^n + 2 \times 4^n \\ 3(-1)^{n+1} + 3 \times 4^n & -2(-1)^{n+1} + 3 \times 4^n \end{pmatrix}$$
$$C^n = \frac{1}{5}\begin{pmatrix} 3(-1)^n + 2^{2n+1} & 2(-1)^{n+1} + 2^{2n+1} \\ 3(-1)^{n+1} + 3 \times 4^n & 2(-1)^n + 3 \times 4^n \end{pmatrix}.$$
2. U est diagonale donc U^{-1} et U^n sont aisées à déterminer et l'on a vu que $\quad T^2 = I$ donc $\quad T^{-1} = T$.
D'où $\quad X = TUT = TUT^{-1} \quad$ donc
$$X^{-1} = TU^{-1}T^{-1} = TU^{-1}T = \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

$$X^{-1} = \frac{1}{(\sqrt{2})^2}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1/3 & 0\\ 0 & 1/1\end{pmatrix}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix} = \frac{1}{3}\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}$$

et $X^n = \begin{pmatrix}-1/\sqrt{2} & 1/\sqrt{2}\\ 1/\sqrt{2} & 1/\sqrt{2}\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & 1\end{pmatrix}^n\begin{pmatrix}-1/\sqrt{2} & 1/\sqrt{2}\\ 1/\sqrt{2} & 1/\sqrt{2}\end{pmatrix}$

$$X^n = \frac{1}{(\sqrt{2})^2}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}3^n & 0\\ 0 & 1^n\end{pmatrix}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1+3^n & 1-3^n\\ 1-3^n & 1+3^n\end{pmatrix}.$$

3. Pour $Y = V\begin{pmatrix}1/3 & 0\\ 0 & 1/2\end{pmatrix}V^{-1}$,

$$Y^{-1} = V\begin{pmatrix}1/3 & 0\\ 0 & 1/2\end{pmatrix}^{-1}V^{-1} = \begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}2 & -3\\ -1 & 2\end{pmatrix} = \begin{pmatrix}6 & -6\\ 2 & -1\end{pmatrix}.$$

Par continuité de la multiplication des matrices, on a :

$$Y^n = V\begin{pmatrix}1/3 & 0\\ 0 & 1/2\end{pmatrix}^n V^{-1} = V\begin{pmatrix}1/3^n & 0\\ 0 & 1/2^n\end{pmatrix}V^{-1} \xrightarrow[n\to\infty]{} VO_2V^{-1} = O_2.$$

Sinon, on peut calculer $Y^n = \begin{pmatrix}4/3^n - 3/2^n & 6/2^n - 6/3^n\\ 2/3^n - 2/2^n & 4/2^n - 3/3^n\end{pmatrix} \xrightarrow[n\to\infty]{} = O_2$.

4. $Z = S^{-1}(RS) = \frac{1}{30}\begin{pmatrix}0 & 12 & 18\\ 5 & 0 & -5\\ 5 & -6 & 1\end{pmatrix}\begin{pmatrix}1 & 8 & -8\\ 1 & 6 & 12\\ 1 & -4 & -8\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & -4\end{pmatrix}$ est diagonale.

Ainsi, $R = I_3RI_3 = SS^{-1}RSS^{-1} = SZS^{-1}$

et $R^n = SZ^nS^{-1} = \begin{pmatrix}1 & 4 & 2\\ 1 & 3 & -3\\ 1 & -2 & 2\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & -4\end{pmatrix}^n \cdot\frac{1}{30}\begin{pmatrix}0 & 12 & 18\\ 5 & 0 & -5\\ 5 & -6 & 1\end{pmatrix}$

$$R^n = \frac{1}{30}\begin{pmatrix}5\times 2^{n+2} + 10(-4)^n & 12 + 3(-4)^{n+1} & 18 - 5\times 2^{n+2} + 2(-4)^n\\ 15\times 2^n - 15(-4)^n & 12 + 18(-4)^n & 18 - 15\times 2^n + 15(-4)^n\\ -5\times 2^{n+1} + 10(-4)^n & 12 + 3(-4)^{n+1} & 18 + 5\times 2^{n+1} + 2(-4)^n\end{pmatrix}.$$

Exercice 13

1. On remarque que $M_2^2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ et $M_3^2 = \begin{pmatrix}2 & 1 & 1\\ 1 & 2 & 1\\ 1 & 1 & 2\end{pmatrix}$.

Plus généralement, $M_n^2 = \begin{pmatrix}n-1 & n-2 & \dots & n-2\\ n-2 & n-1 & \ddots & \vdots\\ \vdots & \ddots & \ddots & n-2\\ n-2 & \dots & n-2 & n-1\end{pmatrix}_{n\times n}$.

En effet, tous les 1 des termes diagonaux s'ajoutent et il y en a $n-1$ mais seuls $n-2$ s'ajoutent pour les autres termes car il y a un coefficient nul sur la ligne et un sur la colonne et ils ne se multiplient pas entre eux. Ainsi,

$$M_n^2 = \begin{pmatrix}n-1 & 0 & \dots & 0\\ 0 & n-1 & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \dots & 0 & n-1\end{pmatrix} + \begin{pmatrix}0 & n-2 & \dots & n-2\\ n-2 & 0 & \ddots & \vdots\\ \vdots & \ddots & \ddots & n-2\\ n-2 & \dots & n-2 & 0\end{pmatrix}$$

$M_n^2 = (n-1)I_n + (n-2)M_n$.

2. D'où, $I_n = \frac{1}{n-1}\left(M_n^2 - (n-2)M_n\right) = \frac{1}{n-1}\left(M_n - (n-2)I_n\right).M_n$: M_n est donc inversible, de matrice inverse

$$M_n^{-1} = \frac{1}{n-1}\left(M_n - (n-2)I_n\right) = \frac{1}{n-1}\begin{pmatrix} 2-n & 1 & \dots & 1 \\ 1 & 2-n & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & 2-n \end{pmatrix}.$$

Exercice 14 Résolution de systèmes linéaires et inversion de matrice

On utilise les résultats des exercices précédents.

(a) $S_a : \begin{cases} x+2y=3 \\ 3x+2y=11 \end{cases}$ peut s'écrire $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ 11 \end{pmatrix}$

$$\iff C\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ 11 \end{pmatrix} \overset{C^{-1}\times}{\iff} C^{-1}C\begin{pmatrix} x \\ y \end{pmatrix} = C^{-1}\begin{pmatrix} 3 \\ 11 \end{pmatrix}$$

$$\iff \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{pmatrix}.\begin{pmatrix} 3 \\ 11 \end{pmatrix} = \begin{pmatrix} 4 \\ -1/2 \end{pmatrix} : \quad \mathscr{S}_a = \left\{\left(4\,,\,-\tfrac{1}{2}\right)\right\}.$$

(b) $S_b : \begin{cases} a+b=4 \\ a+b+c=7 \\ -b+c=-3 \end{cases}$ peut s'écrire $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \\ -3 \end{pmatrix}$

$$\iff K\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \\ -3 \end{pmatrix} \overset{K^{-1}\times}{\iff} K^{-1}K\begin{pmatrix} a \\ b \\ c \end{pmatrix} = K^{-1}\begin{pmatrix} 4 \\ 7 \\ -3 \end{pmatrix}$$

$$\iff \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 1 & -1 \\ -1 & 1 & 0 \end{pmatrix}.\begin{pmatrix} 4 \\ 7 \\ -3 \end{pmatrix} = \begin{pmatrix} -2 \\ 6 \\ 3 \end{pmatrix} : \quad \mathscr{S}_b = \{(-2;6;3)\}.$$

(c) $S_c : \begin{cases} \beta-\gamma=-2 \\ -3\alpha+4\beta-3\gamma=5 \\ -\alpha+\beta=1 \end{cases}$ peut s'écrire $\begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} -2 \\ 5 \\ 1 \end{pmatrix}$

$$\iff L\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} -2 \\ 5 \\ 1 \end{pmatrix} \overset{L^{-1}\times}{\iff} L^{-1}L\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = L^{-1}\begin{pmatrix} -2 \\ 5 \\ 1 \end{pmatrix} \iff$$

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 3 & -1 & 1 \\ 3 & -1 & 3 \\ 1 & -1 & 3 \end{pmatrix}.\begin{pmatrix} -2 \\ 5 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -10 \\ -8 \\ -4 \end{pmatrix} = \begin{pmatrix} -5 \\ -4 \\ -2 \end{pmatrix} : \mathscr{S}_c = \{(-5;-4;-2)\}.$$

(d) $S_d : \begin{cases} f+g+h=1 \\ e+g+h=1 \\ e+f+h=1 \\ e+f+g=1 \end{cases}$ peut s'écrire $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

$$\iff M_4\begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \overset{M_4^{-1}\times}{\iff} M_4^{-1}M_4\begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix} = M_4^{-1}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

CORRIGÉS

$$\iff \begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix} = \frac{1}{3}\begin{pmatrix} -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \\ 1/3 \end{pmatrix} \quad : \mathscr{S}_d = \left\{\left(\tfrac{1}{3}; \tfrac{1}{3}; \tfrac{1}{3}; \tfrac{1}{3}\right)\right\}.$$

(e) $S_e\colon \begin{cases} 2i - 6j = 5 \\ -3i + 9j = 7 \end{cases}$ peut s'écrire $\begin{pmatrix} 2 & -6 \\ -3 & 9 \end{pmatrix}\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix} \iff$

$Q\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$ et puisque Q n'est pas inversible, il n'y a pas de solution unique.

En effet, $2L_2 + 3L_1 \to L_2$ mène à

$S_e \implies 2(-3i + 9j) + 3(2i - 6j) = 2 \times 7 - 3 \times 5 \iff 0i + 0j = -1$ qui n'admet aucune solution : $\mathscr{S}_e = \varnothing$.

(f) $S_f\colon \begin{cases} u + w = 3 \\ w = -1 \\ u + w = 3 \end{cases}$ peut s'écrire $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix} \iff$

$B\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix}$ et puisque B n'est pas inversible, il n'y a pas de solution unique.

En effet, $S_f\colon \begin{cases} u + w = 3 \\ w = -1 \\ u + w = 3 \end{cases} \iff \begin{cases} w = -1 \\ u = 3 - w = 3 + 1 = 4 \\ v \in \mathbb{R} \end{cases}$ et l'on a une infinité de solutions : $\mathscr{S}_f = \left\{(4; v; -1) \,/\, v \in \mathbb{R}\right\}$.

(g) $S_g\colon \begin{cases} z = 1 \\ x + y = -2 \\ 3z + x + y = 1 \end{cases}$ peut s'écrire $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix}\begin{pmatrix} z \\ x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \iff$

$\Delta\begin{pmatrix} z \\ x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$ et puisque Δ n'est pas inversible, il n'y a pas de solution unique.

En effet, $S_g\colon \begin{cases} z = 1 \\ x + y = -2 \\ 3z + x + y = 1 \end{cases} \iff \begin{cases} z = 1 \\ y = -x - 2 \\ y = 1 - x - 3 \end{cases}$ et l'on a une infinité de solutions : $\mathscr{S}_g = \left\{(x; -x - 2; 1) \,/\, x \in \mathbb{R}\right\}$.

Exercice 15 ∫ Ce programme calcule la matrice solution du système c de l'exercice précédent et l'on a donc `X=array([[-5],[-4],[-2]])`.

Exercice 16 Transposition et produit

1. On utilise les résultats obtenus dans l'exercice 1.

$$E^\top = \begin{pmatrix} -2 & 3 & 1 \end{pmatrix}^\top_{1\times 3} = \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix}_{3\times 1}$$

$$F^\top = \begin{pmatrix} 4 \\ -5 \\ 7 \end{pmatrix}^\top_{3\times 1} = \begin{pmatrix} 4 & -5 & 7 \end{pmatrix}_{1\times 3}$$

$$E^\top F^\top = \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix}_{3\times 1} \times \begin{pmatrix} 4 & -5 & 7 \end{pmatrix}_{1\times 3} = \begin{pmatrix} -8 & 10 & -14 \\ 12 & -15 & 21 \\ 4 & -5 & 7 \end{pmatrix}_{3\times 3}$$

$$F^\top E^\top = \begin{pmatrix} 4 & -5 & 7 \end{pmatrix}_{1\times 3} \times \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix}_{3\times 1} = \begin{pmatrix} -16 \end{pmatrix}_{1\times 1}$$

$$(EF)^\top = \begin{pmatrix} -16 \end{pmatrix}_{1\times 1}^\top = \begin{pmatrix} -16 \end{pmatrix}_{1\times 1}$$

$$(FE)^\top = \begin{pmatrix} -8 & 12 & 4 \\ 10 & -15 & -5 \\ -14 & 21 & 7 \end{pmatrix}_{3\times 3}^\top = \begin{pmatrix} -8 & 10 & -14 \\ 12 & -15 & 21 \\ 4 & -5 & 7 \end{pmatrix}_{3\times 3}$$

$$G^\top = \begin{pmatrix} 2 & 1 & -3 \\ -2 & 3 & -1 \end{pmatrix}_{2\times 3}^\top = \begin{pmatrix} 2 & -2 \\ 1 & 3 \\ -3 & -1 \end{pmatrix}_{3\times 2}$$

$$H^\top = \begin{pmatrix} 4 & 2 \\ -1 & -5 \\ 3 & -2 \end{pmatrix}_{3\times 2}^\top = \begin{pmatrix} 4 & -1 & 3 \\ 2 & -5 & -2 \end{pmatrix}_{2\times 3}$$

$$G^\top H^\top = \begin{pmatrix} 2 & -2 \\ 1 & 3 \\ -3 & -1 \end{pmatrix}_{3\times 2} \times \begin{pmatrix} 4 & -1 & 3 \\ 2 & -5 & -2 \end{pmatrix}_{2\times 3} = \begin{pmatrix} 4 & 8 & 10 \\ 10 & -16 & 3 \\ -14 & 10 & -6 \end{pmatrix}_{3\times 3}$$

$$H^\top G^\top = \begin{pmatrix} 4 & -1 & 3 \\ 2 & -5 & -2 \end{pmatrix}_{2\times 3} \times \begin{pmatrix} 2 & -2 \\ 1 & 3 \\ -3 & -1 \end{pmatrix}_{3\times 2} = \begin{pmatrix} -2 & -14 \\ 5 & -17 \end{pmatrix}_{2\times 2}$$

$$(GH)^\top = \begin{pmatrix} -2 & 5 \\ -14 & -17 \end{pmatrix}_{2\times 2}^\top = \begin{pmatrix} -2 & -14 \\ 5 & -17 \end{pmatrix}_{2\times 2}$$

$$(HG)^\top = \begin{pmatrix} 4 & 10 & -14 \\ 8 & -16 & 10 \\ 10 & -3 & -6 \end{pmatrix}_{3\times 3}^\top = \begin{pmatrix} 4 & 8 & 10 \\ 10 & -16 & 3 \\ -14 & 10 & -6 \end{pmatrix}_{3\times 3}$$

2. Remarquons que $(EF)^\top = F^\top E^\top$, $(FE)^\top = E^\top F^\top$, $(GH)^\top = H^\top G^\top$ et $(HG)^\top = G^\top H^\top$.
   Conjecturons que, pour toutes matrices A de taille $m \times n$ et B de taille $n \times p$, on a $(AB)^\top = B^\top A^\top$.
   Posons $C = AB = (c_{i,j})_{m\times p}$, $(AB)^\top = C^\top = (c^t_{i,j})_{p\times m}$, $A^\top = (a^t_{i,j})_{n\times m}$, $B^\top = (b^t_{i,j})_{p\times n}$ et $D = B^\top A^\top = (d_{i,j})_{p\times m}$.
   On sait que $c_{i,j} = \displaystyle\sum_{k=1}^{k=n} a_{i,k}b_{k,j}$, $d_{i,j} = \displaystyle\sum_{k=1}^{k=n} b^t_{i,k}a^t_{k,j}$ $c^t_{i,j} = c_{j,i}$, $a^t_{i,j} = a_{j,i}$ et $b^t_{i,j} = b_{j,i}$.
   Ainsi, $c^t_{i,j} = c_{j,i} = \displaystyle\sum_{k=1}^{k=n} a_{j,k}b_{k,i} = \sum_{k=1}^{k=n} a^t_{k,j}b^t_{i,k} = \sum_{k=1}^{k=n} b^t_{i,k}a^t_{k,j} = d_{i,j}$ et l'on a bien $C^\top = D$.

CORRIGÉS

Exercice 17 Matrices de permutation

1. La matrice $C_{13,21,32} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ permet, en la multipliant à droite d'une matrice 3×3 donnée, de placer la première colonne en troisième, la seconde colonne en premier et la troisième colonne en second.
   Par exemple, $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 6 & 4 \\ 8 & 9 & 7 \end{pmatrix}$.

2. La matrice $L_{13,21,32} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ permet, en la multipliant à gauche d'une matrice 3×3 donnée, de placer la première ligne en troisième, la seconde ligne en premier et la troisième ligne en second.
   Par exemple, $L_{13,21,32} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 4 & 5 & 6 \\ 7 & 8 & 9 \\ 1 & 2 & 3 \end{pmatrix}$.

3. On a $C_{13,21,32} = L^{\top}_{13,21,32}$. Ce n'est pas étonnant car lorsque l'on transpose une matrice, on échange les lignes et les colonnes et l'on a vu dans l'exercice précédent que si une matrice est multipliée d'un côté, la transposée multiplie de l'autre.

Exercice 18 On a $\mathcal{J}_n = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}_{n\times n}$

donc $\mathcal{J}_n^2 = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}^2_{n\times n} = \begin{pmatrix} n & \dots & n \\ \vdots & \ddots & \vdots \\ n & \dots & n \end{pmatrix}_{n\times n} = n\mathcal{J}_n$. Si $\mathcal{J}$ était inversible, on aurait $I_n = \mathcal{J}_n\mathcal{J}_n^{-1} = \frac{1}{n}\mathcal{J}_n^2\mathcal{J}_n^{-1} = \frac{1}{n}\mathcal{J}_n\mathcal{J}_n\mathcal{J}_n^{-1} = \frac{1}{n}\mathcal{J}_n$ ce qui est faux.

Exercice 19 Matrices nilpotentes

Une matrice carrée M est nilpotente s'il existe un entier $p \in \mathbb{N}^*$ tel que $M^p = O$.

1. Soient $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
   (a) On a $A^2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2$
   et $B^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2$ donc A et B sont nilpotentes.
   (b) On a $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $(A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.
   On en déduit facilement que $(A+B)^{2n} = I_n \neq O_2$
   et $(A+B)^{2n+1} = A + B \neq O_2$.
   La matrice $A+B$ n'est donc pas nilpotente.

(c) $AB = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\quad (AB)^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

On en déduit facilement que $(AB)^n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq O_2$. La matrice AB n'est donc pas nilpotente.

2. Soit N une matrice carrée d'ordre 2 telle que $N^2 = O_2$.

(a) On a $(I_2 + N)(I_2 - N) = I_2^2 - I_2N + NI_2 - N^2 = I_2 - N + N + O_2 = I_2$ donc $I_2 - N$ est inversible, de matrice inverse $(I_2 - N)^{-1} = I_2 + N$.

(b) On a $C = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = I_2 - A$ avec $A^2 = O_2$ donc C est inversible et

$C^{-1} = I_2 + A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

On a $D = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = I_2 - B$ avec $B^2 = O_2$ donc D est inversible et

$D^{-1} = I_2 + B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Exercice 20

On a $M = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ et $N = M - I_3 = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$.

Ainsi, $N^2 = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$

et $N^3 = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = O_3$.

Soit, pour $n \in \mathbb{N}^*$, la proposition $\mathscr{P}$: « $M^n = I_3 + nN + \frac{n(n-1)}{2}N^2$ ».

· On a $I_3 + 1.N + \frac{1(1-1)}{2}N^2 = I_3 + N = M = M^1$ et $\mathscr{P}_1$ est vraie.

· Supposons que $\mathscr{P}_n$ est vraie pour un certain $n \in \mathbb{N}^*$.

On a
$$\begin{aligned} M^{n+1} &= M^n.M = (I_3 + nN + \tfrac{n(n-1)}{2}N^2)(I + N) \\ &= I_3 + nN + \tfrac{n(n-1)}{2}N^2 + I_3.N + nN.N + \tfrac{n(n-1)}{2}N^2.N \\ &= I_3 + (n+1)N + \left(\tfrac{n(n-1)}{2} + n\right) N^2 + \tfrac{n(n-1)}{2}N^3 \\ &= I_3 + (n+1)N + \tfrac{n^2-n+2n}{2}N^2 + \tfrac{n(n-1)}{2}O_3 \end{aligned}$$

$M^{n+1} = I_3 + (n+1)N + \frac{(n+1)n}{2}N^2$: $\quad \mathscr{P}_{n+1}$ est vraie.

· $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

Exercice 21 Identités remarquables et binôme de Newton

On pose $A = \begin{pmatrix} 3 & -1 \\ 7 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 1 \\ -7 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$,

1. (a) On a $A + B = \begin{pmatrix} 3 & -1 \\ 7 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ -7 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

donc $(A + B)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$.

CORRIGÉS

Par ailleurs,

$$A^2+2AB+B^2 = \begin{pmatrix}3 & -1\\ 7 & 1\end{pmatrix}^2 + 2\begin{pmatrix}3 & -1\\ 7 & 1\end{pmatrix}\begin{pmatrix}-1 & 1\\ -7 & 1\end{pmatrix} + \begin{pmatrix}-1 & 1\\ -7 & 1\end{pmatrix}^2 = \dots$$

$$A^2+2AB+B^2 = \begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix}.$$

(b) On a $\quad C+D = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 2\\ 3 & 2\end{pmatrix} = \begin{pmatrix}2 & 4\\ 3 & 3\end{pmatrix}$

donc $\quad (C+D)^2 = \begin{pmatrix}2 & 4\\ 3 & 3\end{pmatrix}^2 = \begin{pmatrix}16 & 20\\ 15 & 21\end{pmatrix}.$

Par ailleurs, $\quad C^2+2CD+D^2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}^2 + 2\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 2\end{pmatrix} + \begin{pmatrix}1 & 2\\ 3 & 2\end{pmatrix}^2$

$$C^2+2CD+D^2 = \dots = \begin{pmatrix}22 & 22\\ 15 & 15\end{pmatrix}.$$

(c) On en déduit que la première identité remarquable n'est pas toujours vraie. En effet, $\quad (P+Q)^2 = (P+Q)(P+Q) = P^2+PQ+QP+Q^2 \quad$ et il n'est pas fréquent que les matrices PQ et QP soient égales.

2. De même, les autres identités remarquables sont fausses en général. Elles ne seront vraies que lorsque les produits croisés seront égaux.

3. On dit que deux matrices P et Q forment une paire commutante si $PQ = QP$. Dans ce cas, la formule du binôme de Newton est vraie :

$$(P+Q)^n = \sum_{i=0}^{i=n} \binom{i}{n} P^{n-i}Q^i.$$

On peut remarquer que I_k commute avec toutes les matrices carrées d'ordre k.

4. Dans l'exercice 20 précédent, on avait $\quad M = I_3 + N. \quad$ Puisque $\quad NI_3 = I_3N$, on peut appliquer la formule du binôme de Newton et l'on obtient le calcul suivant, pour $n \geqslant 2$.

$$M^n = (I_3+N)^n = \sum_{i=0}^{i=n} \binom{i}{n} I_3^{n-i}N^i = \binom{0}{n}N^0 + \binom{1}{n}N^1 + \binom{2}{n}N^2 + O_3$$

$$M^n = I_3 + nN + \frac{n(n-1)}{2}N^2, \quad \text{formule qui reste vraie pour } n = 1.$$

Exercice 22 Cette fonction Python retourne la puissance n^{e} (et non $(n+1)^{\text{e}}$) de la matrice 2×2 entrée.

```
from numpy import *
from numpy.linalg import *
def puissance(a,b,c,d,n) :
   A=array([[a,b],[c,d]])
   B=A
   for i in range(1,n) :
      A=dot(A,B)
   return A
```

Exercice 23 Matrices triangulaires

Une matrice triangulaire supérieure est une matrice dont tous les coefficients situés sous la diagonale sont nuls.

1. Soit $T = (t_{i,j})$ une matrice carrée d'ordre n.
   (a) Si $T = (t_{i,j})$ est triangulaire supérieure, alors pour tout i, $j \in [\![0 ; n]\!]$,
   $i > j \Longrightarrow t_{i,j} = 0$.
   (b) Si T est triangulaire inférieure, alors pour tout i, $j \in [\![0 ; n]\!]$,
   $i < j \Longrightarrow t_{i,j} = 0$.
2. Soient $T = (t_{i,j})$ et $T' = (t'_{i,j})$ deux matrices triangulaires supérieures d'ordre n et soient α et $\beta \in \mathbb{K}$.
   On a, pour i, $j \in [\![0 ; n]\!]$ tels que $i > j$,
   $(\alpha T + \beta T')_{i,j} = \alpha t_{i,j} + \beta t'_{i,j} = \alpha \times 0 + \beta \times 0 = 0$: $\alpha T + \beta T'$ est triangulaire supérieure.
   $$\text{et} \quad (TT')_{i,j} = \sum_{k=1}^{n} t_{i,k}t'_{k,j} = 0 + \sum_{k=i}^{n} t_{i,k}t'_{k,j} \quad (t_{i,k} = 0 \text{ si } i > k)$$
   $$= 0 \quad (t'_{k,j} = 0 \text{ si } k \geqslant i > j) : \quad TT' \text{ est triangulaire supérieure.}$$
3. (a) $\det(A) = \det \begin{pmatrix} 2 & 4 \\ 0 & -3 \end{pmatrix} = 2(-3) - 0 \times 4 = -6 \neq 0$ donc A est inversible
   et $\det(B) = \det \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix} = 0 \times 3 - 0 \times 1 = 0$ donc B n'est pas inversible.
   (b) On a $C \begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 6 \end{pmatrix}$ et $C \begin{pmatrix} -9 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 6 \end{pmatrix}$
   donc C n'est pas inversible. Sinon, en multipliant à gauche par C^{-1}, $\begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix}$ et $\begin{pmatrix} -9 \\ 1 \\ 3 \end{pmatrix}$ seraient tous deux égaux à $C^{-1} \begin{pmatrix} 2 \\ 3 \\ 6 \end{pmatrix}$.
   (c) En utilisant l'algorithme de Gauss, on obtient
   $$E = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[L_2 - 2L_3 \to L_2]{L_1 - 3L_3 \to L_1} \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{\frac{1}{2}(L_1 - L_2) \to L_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$
   donc E est inversible.
   (d) Une matrice triangulaire semble inversible lorsque ses éléments diagonaux sont tous non nuls. En effet, l'algorithme de Gauss nous permet dans ce cas de toujours nous ramener à la matrice identité.

Les matrices triangulaires forment donc un ensemble stable pour les opérations usuelles et sont relativement aisées à étudier, à manipuler et à inverser : il est souvent utile de s'y ramener (cf. exercice 7 p.74).

CORRIGÉS

Exercice 24 Équation cartésienne d'un plan

1. Puisque les points $A(1;5;-2)$, $B(7;-1;3)$ et $C(-2;7;2)$ appartiennent au plan (BAC), leurs coordonnées vérifient l'équation cartésienne $ax+by+cz=73$ de ce plan et l'on a donc le système
$$\begin{cases} 1a+5b-2c &= 73 \\ 7a-1b+3c &= 73 \\ -2a+7b+2c &= 73 \end{cases} \Leftrightarrow \begin{pmatrix} 1 & 5 & -2 \\ 7 & -1 & 3 \\ -2 & 7 & -2 \end{pmatrix} . \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 73 \\ 73 \\ 73 \end{pmatrix} \Leftrightarrow MX = 73Y.$$
2. La calculatrice donne $MN = 73I_3$ donc M est inversible et $M^{-1} = \frac{1}{73}N$.
3. Ainsi, $MX = 73Y \Leftrightarrow M^{-1}MX = M^{-1}.73Y \Leftrightarrow X = \frac{73}{73}NY \Leftrightarrow \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 10 \\ 15 \\ 6 \end{pmatrix}$
et le plan (BAC) admet pour équation cartésienne $10x+15y+6z=73$.

Exercice 25 Transformations du plan

Soit $\begin{pmatrix} x \\ y \end{pmatrix}$ la matrice colonne associée au point $M\,(\,x\,,\,y\,)$ du plan.

A: $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}$: coordonnées du symétrique de M par rapport à l'axe des ordonnées.

B: $\begin{pmatrix} 1/3 & 0 \\ 0 & 1/3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x/3 \\ y/3 \end{pmatrix}$: coordonnées de l'image de M par l'homothétie de centre O et de rapport $\frac{1}{3}$.

C: $\begin{pmatrix} -4 & 0 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -4x \\ -4y \end{pmatrix}$: coordonnées de l'image de M par l'homothétie de centre O et de rapport -4.

D: $\begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(\frac{\pi}{4}) & -\sin(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(\frac{\pi}{4})x - \sin(\frac{\pi}{4})y \\ \sin(\frac{\pi}{4})x + \cos(\frac{\pi}{4})y \end{pmatrix}$: coordonnées de l'image de M par la rotation de centre O et d'angle $\frac{\pi}{4}$.

E: $\begin{pmatrix} -\sqrt{3}/2 & 1/2 \\ -1/2 & -\sqrt{3}/2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(-\frac{5\pi}{6}) & -\sin(-\frac{5\pi}{6}) \\ \sin(-\frac{5\pi}{6}) & \cos(-\frac{5\pi}{6}) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$
$= \begin{pmatrix} \cos(-\frac{5\pi}{6})x - \sin(-\frac{5\pi}{6})y \\ \sin(-\frac{5\pi}{6})x + \cos(-\frac{5\pi}{6})y \end{pmatrix}$: coordonnées de l'image de M par la rotation de centre O et d'angle $-\frac{5\pi}{6}$.

F: $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(\pi) & -\sin(\pi) \\ \sin(\pi) & \cos(\pi) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(\pi)x - \sin(\pi)y \\ \sin(\pi)x + \cos(\pi)y \end{pmatrix}$
$= \begin{pmatrix} -x \\ -y \end{pmatrix}$: coordonnées de l'image de M par la rotation de centre O et d'angle π c.-à-d. la symétrie de centre O.

Exercice 26 Rotations quelconques

1. On donne $A\,(\,3\,,\,1\,)$ et $B\,(\,5\,,\,-4\,)$ deux points du plan muni d'un r.o.n. direct. On définit $B_1\,(\,x_1\,,\,y_1\,)$ l'image de B par la translation de vecteur $\overrightarrow{AO}\begin{pmatrix} -3 \\ -1 \end{pmatrix}$, $B_2\,(\,x_2\,,\,y_2\,)$ l'image de B_1 par la rotation de centre O et d'angle $-\frac{\pi}{2}$ et

$B'\,(\,x'\,,\,y'\,)$ l'image de B_2 par la translation de vecteur $\overrightarrow{OA}\binom{3}{1}$. Le point B' est alors l'image de B par la rotation de centre A et d'angle $-\frac{\pi}{2}$ c.-à-d. le point recherché. On a $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 5 \\ -4 \end{pmatrix} + \begin{pmatrix} -3 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -5 \end{pmatrix}$, $\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ -5 \end{pmatrix} = \begin{pmatrix} -5 \\ -2 \end{pmatrix}$
et $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -5 \\ -2 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}$ d'où $B'\,(\,-2\,,\,-1\,)$.

2. En procédant de la même manière (translation $\overrightarrow{CO}$ puis rotation O, α puis translation $\overrightarrow{OC}$), on obtient $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \left[\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} a \\ b \end{pmatrix} \right] + \begin{pmatrix} a \\ b \end{pmatrix}$
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos(\alpha)(x-a) - \sin(\alpha)(y-b) + a \\ \sin(\alpha)(x-a) + \cos(\alpha)(y-b) + b \end{pmatrix}.$$

Exercice 27 La règle d'or

1. En centimes, on calcule
$$\begin{pmatrix} 8 & 10 & 14 \\ 6 & 6 & 10 \\ 12 & 10 & 18 \end{pmatrix} \times \begin{pmatrix} 25 \\ 20 \\ 15 \end{pmatrix} = \begin{pmatrix} 8\times 25 + 10\times 20 + 14\times 15 \\ 6\times 25 + 6\times 20 + 10\times 15 \\ 12\times 25 + 10\times 20 + 18\times 15 \end{pmatrix} = \begin{pmatrix} 610 \\ 420 \\ 770 \end{pmatrix}.$$
Une règle a donc un coût de 6,10 €, une équerre de 4,20 € et un compas 7,70 €.

2. On cherche r, e et c tels que $\begin{pmatrix} 8 & 10 & 14 \\ 6 & 6 & 10 \\ 12 & 10 & 18 \end{pmatrix} \times \begin{pmatrix} r \\ e \\ c \end{pmatrix} = \begin{pmatrix} 500 \\ 350 \\ 650 \end{pmatrix}$. À l'aide de la calculatrice, on obtient
$$\begin{pmatrix} r \\ e \\ c \end{pmatrix} = \begin{pmatrix} 8 & 10 & 14 \\ 6 & 6 & 10 \\ 12 & 10 & 18 \end{pmatrix}^{-1} \begin{pmatrix} 500 \\ 350 \\ 650 \end{pmatrix} = \begin{pmatrix} 1/2 & -5/2 & 1 \\ 3/4 & -3/2 & 1/4 \\ -3/4 & 5/2 & -3/4 \end{pmatrix} \begin{pmatrix} 500 \\ 350 \\ 650 \end{pmatrix} = \begin{pmatrix} 25 \\ 25/2 \\ 25/2 \end{pmatrix}.$$
La première machine doit avoir un coût horaire de 0,25 €/s, la deuxième 0,125 €/s et la troisième 0,125 €/s.

Exercice 28 Les trois militaires

Si l'on appelle f, m, a et c les coefficients appliqués aux différentes matières, le problème revient à résoudre le système matriciel suivant. En utilisant la calculatrice pour inverser la matrice, on le résout aisément.
$$\begin{pmatrix} 10 & 8 & 15 & 16 \\ 17 & 12 & 7 & 11 \\ 8 & 15 & 9 & 13 \\ 12 & 7 & 14 & 10 \end{pmatrix} \begin{pmatrix} f \\ m \\ a \\ c \end{pmatrix} = \begin{pmatrix} 211 \\ 208 \\ 206 \\ 190 \end{pmatrix}$$
$$\iff \begin{pmatrix} f \\ m \\ a \\ c \end{pmatrix} = \begin{pmatrix} 10 & 8 & 15 & 16 \\ 17 & 12 & 7 & 11 \\ 8 & 15 & 9 & 13 \\ 12 & 7 & 14 & 10 \end{pmatrix}^{-1} \begin{pmatrix} 211 \\ 208 \\ 206 \\ 190 \end{pmatrix}$$
$$\iff \begin{pmatrix} f \\ m \\ a \\ c \end{pmatrix} = \frac{1}{8159} \begin{pmatrix} -100 & 731 & -587 & 119 \\ -988 & -284 & 1054 & 523 \\ -551 & -786 & 274 & 1390 \\ 1583 & 422 & -417 & -1639 \end{pmatrix} \begin{pmatrix} 211 \\ 208 \\ 206 \\ 190 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \\ 5 \\ 3 \end{pmatrix}.$$
Le français est de coefficient 4, les mathématiques 6, l'anglais 5 et la culture générale 3.

Exercice 29 Matrices, composition de fonctions homographiques et suite récurrente

1. On a $FX = \begin{pmatrix} 3 & 2 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 3x+2 \\ x-3 \end{pmatrix}$ que l'on peut associer à l'image de $x \neq 3$ par f : $f(x) = \frac{3x+2}{x-3}$.

2. De même, on associe à $g(x) = \frac{x-2}{2x-4}$, la matrice $G = \begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix}$.

3. On a, formellement, $(f \circ g)(x) = f\left(g(x)\right) = \dfrac{3g(x)+2}{g(x)-3} = \dfrac{3\,\frac{x-2}{2x-4}+2}{\frac{x-2}{2x-4}-3}$
$$(f \circ g)(x) = \dfrac{\frac{3x-6+2(2x-4)}{2x-4}}{\frac{x-2-3(2x-4)}{2x-4}} = \dfrac{7x-14}{-5x+10}$$
et $FGX = \begin{pmatrix} 3 & 2 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 7 & -14 \\ -5 & 10 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 7x-14 \\ -5x+10 \end{pmatrix}$

4. De même, $GFX = \begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 2 & 16 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x+8 \\ 2x+16 \end{pmatrix}$
qui est formellement associé à $(g \circ f)(x) = \dfrac{x+8}{2x+16}$.

5. (a) On a $H = VDV^{-1} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & -9 \\ 3 & -11/2 \end{pmatrix}$.

   (b) En utilisant les propriétés démontrées dans l'exercice 10, on obtient
   $$H^n = (VDV^{-1})^n = VD^nV^{-1} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1/2^n & 0 \\ 0 & (-1)^n \end{pmatrix} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$$
   et $H^n = \begin{pmatrix} \frac{1}{2^{n-2}} + 3(-1)^{n+1} & \frac{-3}{2^{n-1}} + 6(-1)^n \\ \frac{1}{2^{n-1}} + 2(-1)^{n+1} & \frac{-3}{2^n} + 4(-1)^n \end{pmatrix}$.

   (c) On définit la fonction h par $h(x) = \frac{5x-9}{3x-\frac{11}{2}}$, associée à la matrice H. Puisque $u_{n+1} = h(u_n)$, u_{n+1} est associé à HU_n. Par une simple récurrence, $u_n = h^{\circ n}(u_0)$ est associé à H^nU_0. Ainsi,
   $$u_n = \dfrac{\left(\frac{1}{2^{n-2}} + 3(-1)^{n+1}\right)u_0 + \left(\frac{-3}{2^{n-1}} + 6(-1)^n\right)}{\left(\frac{1}{2^{n-1}} + 2(-1)^{n+1}\right)u_0 + \left(\frac{-3}{2^n} + 4(-1)^n\right)}$$
   $$u_n = \dfrac{0 + 6(-1)^n\left(1 \mp \frac{1}{2^n}\right)}{0 + 4(-1)^n\left(1 \mp \frac{\mp 3}{2^{n+2}}\right)} \xrightarrow[n\to\infty]{} \dfrac{6(0+1)}{4(0+1)} = \dfrac{3}{2}.$$
   On peut vérifier que $h(\frac{3}{2}) = \frac{5.\frac{3}{2}-9}{3.\frac{3}{2}-\frac{11}{2}} = \frac{3}{2}$ est bien un point fixe de h.

Exercice 30 Exponentielle de matrice et système d'équations différentielles

1. Exponentielle de matrice
   $A^2 \neq O_3$, $A^3 = O_3$ et, pour tout $t \in \mathbb{R}$, $E(t) = I_3 + tA + \frac{t^2}{2}A^2$.

   (a) Pour tous t, $t' \in \mathbb{R}$, $E(t)E(t') = \left(I_3 + tA + \frac{t^2}{2}A^2\right)\left(I_3 + t'A + \frac{t'^2}{2}A^2\right)$
   $$\begin{aligned} E(t)E(t') &= I_3 + t'A + \tfrac{t'^2}{2}A^2 + tA + tt'A^2 + t\tfrac{t'^2}{2}A^3 + \tfrac{t^2}{2}A^2 + t'\tfrac{t^2}{2}A^3 + \tfrac{t^2}{2}\tfrac{t'^2}{2}A^4 \\ &= I_3 + (t+t')A + \left(\tfrac{t^2}{2} + tt' + \tfrac{t'^2}{2}\right)A^2 + O_3 \\ &= I_3 + (t+t')A + \tfrac{(t+t')^2}{2}A^2 = E(t+t') \end{aligned}$$

(b) Ainsi, pour tout $t \in \mathbb{R}$, $E(t)E(-t) = E(t-t) = E(0) = I_3+0A+\frac{0^2}{2}A^2 = I_3$ et, pour tout $t \in \mathbb{R}$, la matrice $E(t)$ est inversible, de matrice inverse $E(-t)$.

(c) Puisque les coefficients de $E(t)$ sont des polynômes en t, on a

$$E'(t) = \left(I_3 + tA + \frac{t^2}{2}A^2\right)' = I_3'+(tA)'+(\frac{t^2}{2}A^2)' = O_3+(t)'A+(\frac{t^2}{2})'A^2 = A+tA^2.$$

2. Équation différentielle

On a $f(x) = e^{ax}$ donc $f'(x) = (ax)'e^{ax} = ae^{ax} = af(x)$ donc f est solution sur $\mathbb{R}$ de l'équation différentielle $u' = au$.

3. Système d'équations différentielles

(a) On a $\begin{cases} u' &= 2u+v+2w \\ v' &= -u-v-w \\ w' &= -u-w. \end{cases} \iff U' = \begin{pmatrix} u' \\ v' \\ w' \end{pmatrix} = A\begin{pmatrix} u \\ v \\ w \end{pmatrix} = AU$ pour

$A = \begin{pmatrix} 2 & 1 & 2 \\ -1 & -1 & -1 \\ -1 & 0 & -1 \end{pmatrix}$. Avec $A^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{pmatrix} \neq O_3$ et $A^3 = O_3$.

(b) On remarque que $E'(t) = A+tA^2 = A\left(I_3 + tA + \frac{t^2}{2}A^2\right) = AE(t)$ donc, pour $U = E(t)X$, on a $U' = E'(t)X = A.E(t)X = AU$ et U est solution du système différentiel.

Si l'on n'est pas convaincu, on calcule tout ceci en détail.

On a $E(t) = I_3 + tA + \frac{t^2}{2}A^2 = \ \dots = \begin{pmatrix} 1+2t+\frac{t^2}{2} & t+\frac{t^2}{2} & 2t+\frac{t^2}{2} \\ -t & 1-t & -t \\ -t-\frac{t^2}{2} & -\frac{t^2}{2} & 1-t-\frac{t^2}{2} \end{pmatrix}$

d'où, pour tous a, b et $c \in \mathbb{R}$, on a

$$\begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix} = E(t).\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} (1+2t+\frac{t^2}{2})a + (t+\frac{t^2}{2})b + (2t+\frac{t^2}{2})c \\ -at+(1-t)b-tc \\ (-t-\frac{t^2}{2})a - \frac{t^2}{2}b + (1-t-\frac{t^2}{2})c \end{pmatrix}$$

$$\begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix} = \begin{pmatrix} (a+b+c)\frac{t^2}{2} + (2a+b+2c)t + a \\ -(a+b+c)t+b \\ -(a+b+c)\frac{t^2}{2} - (a+c)t + c \end{pmatrix}$$

donc $\begin{pmatrix} u'(t) \\ v'(t) \\ w'(t) \end{pmatrix} = \begin{pmatrix} (a+b+c)t+2a+b+2c \\ -(a+b+c) \\ -(a+b+c)t-(a+c) \end{pmatrix}$ et

$$AU = \begin{pmatrix} 2 & 1 & 2 \\ -1 & -1 & -1 \\ -1 & 0 & -1 \end{pmatrix}\begin{pmatrix} (a+b+c)\frac{t^2}{2} + (2a+b+2c)t + a \\ -(a+b+c)t+b \\ -(a+b+c)\frac{t^2}{2} - (a+c)t + c \end{pmatrix}$$

$$AU = \begin{pmatrix} (a+b+c)t+2a+b+2c \\ -(a+b+c) \\ -(a+b+c)t-(a+c) \end{pmatrix}.$$

On a bien $AU = U'$.

CORRIGÉS

Chapitre V

NOMBRES COMPLEXES : GÉOMÉTRIE

Sommaire

Nous poursuivons ici l'étude des nombres complexes. On donne tout d'abord une représentation graphique de ces nombres, dans le plan et non plus seulement sur une droite, puis nous apprendrons à les écrire de manières différentes.

1 Rappels

Il existe un ensemble $\mathbb{C}$ de nombres dits complexes, contenant $\mathbb{R}$, muni de règles d'addition et de multiplication similaires, tel que tout $z \in \mathbb{C}$ s'écrit de manière unique sous la forme algébrique $z = a + ib$ où $a = \mathfrak{Re}(z)$ et $b = \mathfrak{Im}(z)$ sont des réels et i vérifie $i^2 = -1$. On a $zz' = 0 \iff z = 0$ ou $z' = 0$.
Pour tout $z \in \mathbb{C}$, on définit l'opposé de z par $-z = -a - ib$ et le conjugué de z par $\overline{z} = a - ib$.

On a $\overline{z+z'} = \overline{z} + \overline{z'}$, $\overline{zz'} = \overline{z}\,\overline{z'}$ et, pour $z \neq 0$, $\overline{\frac{1}{z}} = \frac{1}{\overline{z}}$.
Si $z = a + ib$, on a toujours $z\overline{z} = a^2 + b^2$.

Si a, b et c sont trois nombres **réels** tels que $a \neq 0$, l'équation $az^2 + bz + c = 0$ admet **toujours** des solutions.
On note Δ le discriminant de cette équation : $\Delta = b^2 - 4ac$.

- Si $\Delta > 0$, l'équation admet deux solutions réelles distinctes, $x_1 = \frac{-b-\sqrt{\Delta}}{2a}$ et $x_2 = \frac{-b+\sqrt{\Delta}}{2a}$.
- Si $\Delta = 0$, l'équation admet une unique solution « double », réelle, $x_0 = -\frac{b}{2a}$.
- Si $\Delta < 0$, l'équation admet deux solutions, complexes et conjuguées, $z_1 = \frac{-b-i\sqrt{-\Delta}}{2a}$ et $z_2 = \frac{-b+i\sqrt{-\Delta}}{2a}$.

Ainsi, le trinôme se factorise toujours $az^2 + bz + c = a(z - z_1)(z - z_2)$ où z_1 et z_2 sont ses deux racines, éventuellement complexes ou confondues.
Dans $\mathbb{C}$, tout polynôme non nul de degré n admet au plus n racines distinctes. Il en admet même autant que son degré lorsqu'on les compte avec leur multiplicité.
Tout polynôme s'annulant en $a \in \mathbb{C}$ se factorise par $z - a$.

En particulier, $z^n - a^n = (z-a)\displaystyle\sum_{i=0}^{n-1} a^k z^{n-1-k}$.

Formule du binôme de Newton : $\forall u,\, v \in \mathbb{C}$, $(u+v)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} u^{n-k} v^k$.

2 Représentation géométrique d'un complexe

Dans ce paragraphe et pour la suite du chapitre, le plan est muni d'un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$. On pourra se référer à la figure de la page 108.

Définition 1 *Soient a et b deux nombres réels.*

- *À tout nombre complexe $z = a + ib$, on associe le point $M\,(a\,,\,b)$ du plan, appelé* ***point image****, et le vecteur $\overrightarrow{w}\,\binom{a}{b}$ du plan, appelé* ***vecteur image****.*
  On note souvent $M(z)$ ou M_z le point image de z.
- *À tout point $M\,(a\,,\,b)$ et à tout vecteur $\overrightarrow{w}\,\binom{a}{b}$ du plan, on associe le nombre complexe $z = a + ib$ appelé* ***affixe*** *de M et* ***affixe*** *de $\overrightarrow{w}$.*
  On note souvent z_M et $z_{\overrightarrow{w}}$.
- *Le plan est alors appelé* ***plan complexe****.*

<u>*Remarques :*</u> • $z \in \mathbb{R} \iff M(z) \in (x'Ox)$: $M(z)$ est sur l'axe des abscisses.
- $z \in i\mathbb{R} \iff M(z) \in (y'Oy)$: $M(z)$ est sur l'axe des ordonnées.
- Les points $M(z)$ et $M'(\overline{z})$ sont symétriques par rapport à l'axe des abscisses.
- Les points $M(z)$ et $M''(-z)$ sont symétriques par rapport à l'origine.

Propriété 1 *Soient $M(z)$, $M'(z')$ les points images et $\overrightarrow{w}$, $\overrightarrow{w'}$ les vecteurs images des complexes z et z'.*

- *Le vecteur $\overrightarrow{MM'}$ a pour affixe le nombre complexe* $z' - z$.
- *Le milieu du segment $[MM']$ a pour affixe le nombre complexe* $\dfrac{z+z'}{2}$.
- $\overrightarrow{w} = \overrightarrow{w'} \iff z = z'$.
- *Le vecteur* $\overrightarrow{w} + \overrightarrow{w'}$ *a pour affixe le nombre complexe* $z + z'$.
- *Le vecteur* $\lambda\overrightarrow{w}$ *a pour affixe le nombre complexe* λz, *pour tout réel* λ.

Démonstration : Nous ne démontrons que le premier point, les suivants découlent des règles de calcul des coordonnées de vecteurs.

Si $z = a + ib$ et $z' = a' + ib'$, alors $M\,(a\,,b)$, $M'\,(a'\,,b')$ et $\overrightarrow{MM'}\begin{pmatrix} a'-a \\ b'-b \end{pmatrix}$ qui est précisément d'affixe $(a'-a) + i(b'-b) = z' - z$. □

<u>Remarque</u> : La relation de Chasles[†] s'écrit alors : pour tous points A, B, C du plan, $z_{\overrightarrow{AC}} = z_{\overrightarrow{AB}} + z_{\overrightarrow{BC}}$.
En effet, $z_{\overrightarrow{AB}} + z_{\overrightarrow{BC}} = (z_B - z_A) + (z_C - z_B) = z_C - z_A = z_{\overrightarrow{AC}}$.

Ainsi, nous identifions les points du plan, les vecteurs du plan et les nombres complexes. Le plan, de dimension réelle 2, devient le plan complexe, de dimension complexe 1 : $\mathbb{R}^2 \approxeq \mathbb{C}^1$.

Du point de vue de l'analyse, il est bien tentant de remplacer une expression $f(x)$ par sa variante complexe $f(z) = f(a+ib)$: deux variables réelles, a et b, ou une variable complexe, z. Sous certaines conditions, les fonctions de deux variables réelles deviennent aussi des fonctions d'une variable complexe. Graphiquement, les ensembles de départ et d'arrivée ne sont plus des droites mais des plans et la représentation graphique d'une fonction à variable complexe devient un véritable challenge. Parfois, on colorie le plan de départ afin d'illustrer certains comportements d'une telle fonction (cf. ensembles de Mandelbrot et de Julia par exemple). Et que dire du point de vue de la continuité, de la dérivabilité ou de l'intégration ? Les théorèmes connus dans $\mathbb{R}$ sont-ils encore valides dans $\mathbb{C}$? En obtient-on d'autres ? Nous devinons ici le bel univers de l'analyse complexe.

3 Module et arguments d'un nombre complexe

Le plan reste muni d'un repère orthonormé direct $(O\,; \overrightarrow{u}, \overrightarrow{v})$.

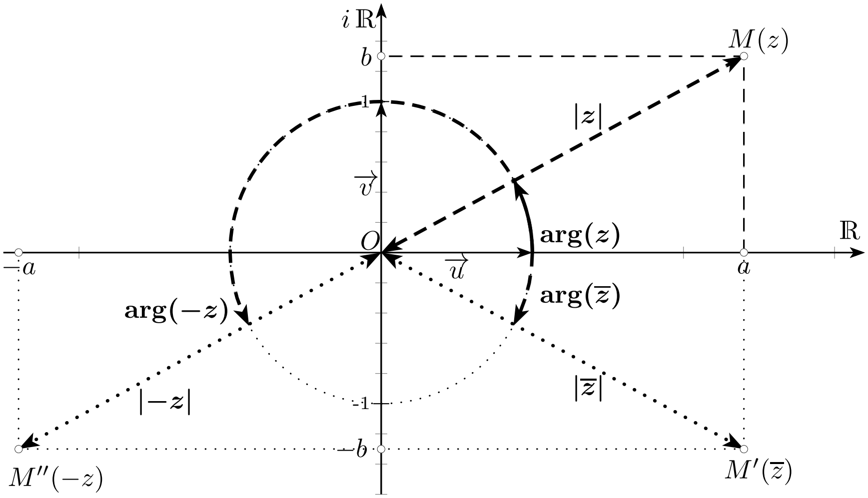
---

†. Michel Chasles (1793-1880), éminent mathématicien français dont le nom est inscrit sur la non moins éminente tour Eiffel.

3.1 Définitions et premières propriétés

Définition 2 *Soit z un nombre complexe non nul, affixe du point M du plan.*

- *Le* ***module*** *de z, noté $|z|$, est la distance OM :* $\boldsymbol{|z| = \sqrt{\mathfrak{Re}^2(z) + \mathfrak{Im}^2(z)}}$.
- ***Un argument*** *de z, noté* $\mathbf{arg}(\boldsymbol{z})$, *est une mesure de l'angle orienté* $\left(\overrightarrow{u}\,;\overrightarrow{OM}\right)$.



<u>*Remarques :*</u>

• 0 n'a pas d'argument. En revanche, on a bien $|0| = 0$ et même, $|z| = 0 \Leftrightarrow z = 0$.

• Pour tout réel x, on a $|x|_{\mathbb{R}} = \sqrt{x^2} = |x|_{\mathbb{C}}$. Le module d'un réel correspond bien à sa valeur absolue ce qui justifie la notation utilisée $|\,.\,|$.

• Deux arguments d'un même nombre complexe diffèrent d'un multiple de 2π : arg est défini *modulo* 2π. Lorsque $\arg(z) \in \,]-\pi\,;\pi\,]$, on l'appelle *argument principal* de z. C'est celui que l'on préfère utiliser.

Exemples : ◦ $z = 1$: $|z| = 1$, $\arg(z) \equiv 0\ [2\pi]$

◦ $z = i$: $|z| = 1$, $\arg(z) \equiv \frac{\pi}{2}\ [2\pi]$

◦ $z = -2$: $|z| = 2$, $\arg(z) \equiv \pi\ [2\pi]$

◦ $z = 1 + i$: $|z| = \sqrt{2}$, $\arg(z) \equiv \frac{\pi}{4}\ [2\pi]$

◦ $z = -2 + 2i$: $|z| = \sqrt{2^2 + 2^2} = 2\sqrt{2}$, $\arg(z) \equiv \frac{3\pi}{4}\ [2\pi]$

◦ $z = -4i$: $|z| = 4$, $\arg(z) \equiv -\frac{\pi}{2}\ [2\pi]$

Le résultat suivant traduit, entre autres, les propriétés de symétrie dans un repère orthonormé.

Propriété 2 *Soit z un nombre complexe non nul.*

- $z \in \mathbb{R} \iff \arg(z) \equiv 0\ [\pi]$
- $z \in i\mathbb{R} \iff \arg(z) \equiv \dfrac{\pi}{2}\ [\pi]$
- $\arg(\overline{z}) \equiv -\arg(z)\ [2\pi]$
- $\arg(-z) \equiv \arg(z) + \pi\ [2\pi]$
- $|\overline{z}| = |z|$
- $|-z| = |z|$

On pourrait même être plus précis. Par exemple, $z \in \mathbb{R}_- \iff \arg(z) \equiv \pi\ [2\pi]$.

Démonstration : De simples illustrations graphiques suffisent à nous convaincre. □

Propriété 3 *Pour tout nombre complexe z, on a* $\boldsymbol{z\overline{z} = |z|^2}$.

Démonstration : $z\overline{z} = (a+ib)(a-ib) = a^2-(ib)^2 = a^2+b^2 = \left(\sqrt{a^2+b^2}\right)^2 = |z|^2$. □

La propriété suivante sera davantage exploitée dans un chapitre ultérieur mais elle peut d'ors et déjà être utile.

Propriété 4 *Soient $A(a)$ et $B(b)$ deux points du plan complexe.*
On a $\|\overrightarrow{AB}\| = AB = |b-a|$.

Démonstration : En effet, le vecteur $\overrightarrow{AB}$ a pour affixe $b-a$ donc sa norme est bien $|b-a|$. □

3.2 Ensemble $\mathbb{U}$ des nombres complexes de module 1

Définition 3
L'ensemble des nombres complexes de module 1 *est noté* $\mathbb{U}$ *:* $\mathbb{U} = \{z \in \mathbb{C}\ /\ |z| = 1\}$.

Dans le plan complexe, l'ensemble des points images des éléments de $\mathbb{U}$ est le cercle trigonométrique.

Propriété 5 *Pour tous* $(z\,,\, z') \in \mathbb{U}^2$,
$z \neq 0$, $-z \in \mathbb{U}$, $\overline{z} \in \mathbb{U}$, $zz' \in \mathbb{U}$, $\frac{1}{z} \in \mathbb{U}$ *et* $\frac{z}{z'} \in \mathbb{U}$.

On dit que $\mathbb{U}$ est stable par conjugaison, produit et quotient. Ceci sera démontré à l'exercice 26 en page 127.

Exemple : Si $z = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$ et $z' = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$, on a $|z| = \sqrt{2\left(\frac{\sqrt{2}}{2}\right)^2} = \sqrt{\frac{4}{4}} = 1$ donc $z \in \mathbb{U}$, $|z'| = \sqrt{\left(-\frac{\sqrt{3}}{2}\right)^2 + \frac{1}{2^2}} = \sqrt{\frac{3}{4}+\frac{1}{4}} = 1$ donc $z' \in \mathbb{U}$ et l'on a bien $|zz'| = \left|(-\frac{\sqrt{6}}{4} + \frac{\sqrt{2}}{4}) + i(\frac{\sqrt{6}}{4} + \frac{\sqrt{2}}{4})\right| = 1$ qui confirme $zz' \in \mathbb{U}$.

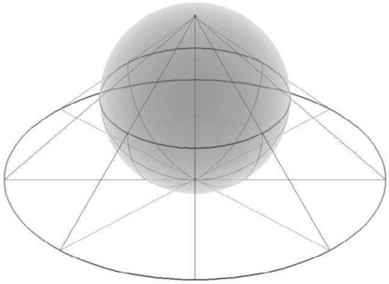
3.3 Limites complexes

Définition 4 • *On dit que* $z \in \mathbb{C} \longrightarrow 0$ *lorsque* $|z| \in \mathbb{R} \longrightarrow 0$.
• *On dit que* $z \in \mathbb{C} \longrightarrow a \in \mathbb{C}$ *lorsque* $|z-a| \in \mathbb{R} \longrightarrow 0$.
• *On dit que* $z \in \mathbb{C}$ *tend vers l'infini lorsque* $|z| \in \mathbb{R} \longrightarrow +\infty$.

Remarques : • $z \longrightarrow a$ signifie donc que l'on se rapproche de a indépendamment de θ, on peut donc « tourner » autour de a tout en s'en approchant.

• L'infini dans le plan complexe est donc ce qui se situe en dehors de tout cercle, ce n'est pas un « lieu » particulier. Pour affiner cela, Gauss et surtout son élève

Riemann ont eu l'idée ($\approx$ 1850) « d'envelopper » le plan complexe autour de la sphère en dimension trois afin d'obtenir ce que l'on appelle aujourd'hui la *sphère de Riemann* : le plan complexe complété d'un « point à l'infini », l'un des pôles de la sphère. C'est un peu l'inverse de ce qui se passe lors d'une projection azimutale afin de cartographier la Terre (cf. l'emblème de l'ONU).



4 Forme trigonométrique d'un nombre complexe non nul

4.1 Forme trigonométrique

Théorème 1
Pour tout nombre complexe non nul z, il existe un ***unique*** *réel strictement* ***positif*** $\boldsymbol{r}$ *et un nombre réel* $\boldsymbol{\theta}$, ***unique modulo*** $\boldsymbol{2\pi}$, *tel que z s'écrive sous la* ***forme trigonométrique*** $\boldsymbol{z = r(\cos\theta + i\sin\theta)}$.
On a $\boldsymbol{r = |z|}$ *et* $\boldsymbol{\theta \equiv \arg(z)\,[2\pi]}$
donc $\boldsymbol{z = |z|\,(\cos(\arg(z)) + i\sin(\arg(z)))}$.
Ainsi, pour r et r' positifs,
$r(\cos\theta + i\sin\theta) = r'(\cos\theta' + i\sin\theta') \iff r = r'$ *et* $\theta \equiv \theta'\,[2\pi]$,
c.-à-d. $\forall z,\, z' \in \mathbb{C}^*$, $z = z' \iff |z| = |z'|$ *et* $\arg(z) \equiv \arg(z')\,[2\pi]$.

Remarque : Attention, une telle écriture n'est la forme trigonométrique d'un nombre complexe que si $\boldsymbol{r > 0}$. Par exemple,
$-2(\cos(-\frac{5\pi}{6}) + i\sin(-\frac{5\pi}{6})) = -2(-\cos\frac{\pi}{6} - i\sin\frac{\pi}{6}) = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6})$
et l'on a $r = 2$, $\theta \equiv \frac{\pi}{6}\,[2\pi]$.

Démonstration : La propriété 6 suivante donne des formules explicites pour trouver une forme trigonométrique. Il reste à démontrer l'unicité de cette forme, autrement dit, $r = |z|$ et $\theta \equiv \arg(z)\,[2\pi]$.
· On a $|z| = |r(\cos\theta + i\sin\theta)| = |(r\cos\theta) + i(r\sin\theta)| = \sqrt{r^2\cos^2\theta + r^2\sin^2\theta}$
et $|z| = \sqrt{r^2 \times 1} = r$ si $r > 0$.
· Si $|z|\,(\cos(\arg(z)) + i\sin(\arg(z))) = |z|\,(\cos\theta + i\sin\theta)$ alors, par unicité de la forme algébrique, $\cos(\arg(z)) = \cos\theta$ et $\sin(\arg(z)) = \sin\theta$ donc $\theta \equiv \arg(z)\,[2\pi]$. $\square$

Exemples : Il est conseillé de commencer par factoriser par le module.

- $z = 1 - i = \sqrt{2}(\frac{1}{\sqrt{2}} - \frac{\sqrt{2}}{2}\, i) = \sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4))$,
  $r = \sqrt{1^2 + 1^2} = \sqrt{2}, \quad \theta \equiv -\pi/4\,[2\pi]$.
- $z = 3i + 3 = 3(1 + i) = 3\sqrt{2}(\cos(\pi/4) + i\sin(\pi/4)), \quad r = 3\sqrt{2}, \quad \theta \equiv \pi/4\,[2\pi]$.
- $z = 5 - 5i\sqrt{3} = 10\left(\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right) = 10(\cos(-\pi/3) + i\sin(-\pi/3))$,
  $r = 5\sqrt{1^2 + \sqrt{3}^2} = 10, \quad \theta \equiv -\pi/3\,[2\pi]$.
- $z = -11 = 11(-1) + 0i = 11(\cos(\pi) + i\sin(\pi)), \qquad r = 11, \quad \theta \equiv \pi\,[2\pi]$.

Propriété 6 ***Lien entre formes algébrique et trigonométrique***
Soit $z = a + ib = r(\cos\theta + i\sin\theta)$ *un nombre complexe non nul* ($r > 0$). *On a :*

- $a = r\cos\theta$ *et* $b = r\sin\theta$.
- $r = |z| = \sqrt{a^2 + b^2}$,
  θ *est défini par* $\cos\theta = \dfrac{a}{\sqrt{a^2+b^2}}$ *et* $\sin\theta = \dfrac{b}{\sqrt{a^2+b^2}}$.

Démonstration : Il suffit d'appliquer les règles de trigonométrie. □

Exemples : ◦ $z = 1+i\sqrt{3}$:$r = \sqrt{1^2 + \sqrt{3}^2} = 2$, $\cos\theta = \frac{1}{2}$, $\sin\theta = \frac{\sqrt{3}}{2}$ et $\theta \equiv \frac{\pi}{3}\,[2\pi]$.

◦ $z = 6(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$:$a = 6\cos\frac{\pi}{4} = 6\frac{\sqrt{2}}{2} = 3\sqrt{2} = b$.

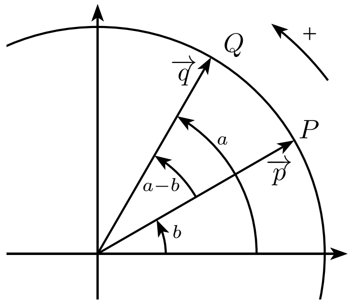
4.2 Formules de trigonométrie

Propriété 7 ***Fondamentale*** *Pour tout réel a, on a* $\boldsymbol{\cos^2(a) + \sin^2(a) = 1}$.

Propriété 8 ***Addition*** *Pour tous réels a et b, on a :*

$\boldsymbol{\cos(a+b) = \cos a\ \cos b - \sin a\ \sin b}$	$\boldsymbol{\cos(a-b) = \cos a\ \cos b + \sin a\ \sin b}$
$\boldsymbol{\sin(a+b) = \sin a\ \cos b + \sin b\ \cos a}$	$\boldsymbol{\sin(a-b) = \sin a\ \cos b - \sin b\ \cos a}$

Démonstration : Soient a, et b deux réels et soient les vecteurs unitaires $\overrightarrow{OP} = \overrightarrow{p}$ et $\overrightarrow{OQ} = \overrightarrow{q}$ dans le repère orthonormé $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$ tels que $(\overrightarrow{u}\,;\,\overrightarrow{p}) = b\,[2\pi]$ et $(\overrightarrow{u}\,;\,\overrightarrow{q}) = a\,[2\pi]$.
D'après la relation de Chasles, on a
$(\overrightarrow{p}\,;\,\overrightarrow{q}) = (\overrightarrow{p}\,;\,\overrightarrow{u}) + (\overrightarrow{u}\,;\,\overrightarrow{q}) = -b + a = a - b\,[2\pi]$.



On a $\overrightarrow{p}\begin{pmatrix}\cos b\\ \sin b\end{pmatrix}$ i.e. $z_P = \cos(b) + i\sin(b)$ et $\overrightarrow{q}\begin{pmatrix}\cos a\\ \sin a\end{pmatrix}$ i.e. $z_Q = \cos(a) + i\sin(a)$.
D'une part, $\overrightarrow{p}\cdot\overrightarrow{q} = \cos a\cos b + \sin a\sin b$.
D'autre part,
$\overrightarrow{p}\cdot\overrightarrow{q} = ||\overrightarrow{p}||.||\overrightarrow{q}||.\cos(\overrightarrow{p}\,;\,\overrightarrow{q}) = 1\times 1\cos(a-b)$.
Ainsi, $\cos(a-b) = \cos a\cos b + \sin a\sin b$.
Pour $\cos(a+b)$, il suffit de changer b en $-b$.

Pour les sinus, on utilise $\cos(\frac{\pi}{2}-\alpha)=\sin(\alpha)$ et $\sin(\frac{\pi}{2}-\alpha)=\cos(\alpha)$:

$$\sin(a+b)=\cos\left((\tfrac{\pi}{2}-(a+b)\right)=\cos\left((\tfrac{\pi}{2}-a)-b\right)$$
$$=\cos(\tfrac{\pi}{2}-a)\cos(b)+\sin(\tfrac{\pi}{2}-a)\sin(b)=\sin(a)\cos(b)+\cos(a)\sin(b).$$

Pour $\sin(a-b)$, il suffit de changer b en $-b$. □

Exemples :

- $\cos\frac{7\pi}{12}=\cos\left(\frac{3\pi}{12}+\frac{4\pi}{12}\right)=\cos\frac{\pi}{4}\cos\frac{\pi}{3}-\sin\frac{\pi}{4}\sin\frac{\pi}{3}=\frac{\sqrt{2}}{2}\frac{1}{2}-\frac{\sqrt{2}}{2}\frac{\sqrt{3}}{2}=\frac{\sqrt{2}(1-\sqrt{3})}{4}$.
- $\sin\frac{\pi}{12}=\sin\left(\frac{\pi}{3}-\frac{\pi}{4}\right)=\sin\frac{\pi}{3}\cos\frac{\pi}{4}-\sin\frac{\pi}{4}\cos\frac{\pi}{3}=\frac{\sqrt{3}}{2}\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}\frac{1}{2}=\frac{\sqrt{2}(\sqrt{3}-1)}{4}$.

Propriété 9 ***Duplication*** *Pour tout réel a, on a :*

$$\boldsymbol{\cos 2a=\cos^2 a-\sin^2 a=2\cos^2 a-1=1-2\sin^2 a}$$
$$\boldsymbol{\sin 2a=2\sin a\ \cos a}$$

Démonstration : Il suffit d'utiliser les formules d'additions et la formule fondamentale de la trigonométrie. □

Exemples : ◦ $\sin\frac{\pi}{2}=\sin\frac{2\pi}{4}=2\sin\frac{\pi}{4}\cos\frac{\pi}{4}=2\frac{\sqrt{2}}{2}\frac{\sqrt{2}}{2}=1$.

◦ $\cos\frac{2\pi}{3}=\cos^2\frac{\pi}{3}-\sin^2\frac{\pi}{3}=\left(\frac{1}{2}\right)^2-\left(\frac{\sqrt{3}}{2}\right)^2=-\frac{1}{2}\quad=2\left(\frac{1}{2}\right)^2-1\quad=1-2\left(\frac{\sqrt{3}}{2}\right)^2$.

Propriété 10 ***Linéarisation*** *Pour tout réel a, on a :*

$$\boldsymbol{\cos^2 a=\frac{1+\cos 2a}{2}}\qquad\qquad \boldsymbol{\sin^2 a=\frac{1-\cos 2a}{2}}$$

Démonstration : Il suffit d'utiliser les formules de duplication. □

Exemples : ◦ $\cos^2\frac{\pi}{12}=\frac{1+\cos\frac{\pi}{6}}{2}=\frac{1+\frac{\sqrt{3}}{2}}{2}=\frac{1}{2}+\frac{\sqrt{3}}{4}$.

◦ $\sin^2\left(-\frac{\pi}{8}\right)=\frac{1-\cos(-\frac{\pi}{4})}{2}=\frac{1-\frac{\sqrt{2}}{2}}{2}=\frac{1}{2}-\frac{\sqrt{2}}{4}$.

5 Notation exponentielle d'un nombre complexe

5.1 Définitions

Faisons un simple calcul introductif.

Soient θ et θ' deux réels. On a, d'après le paragraphe précédent,

$$(\cos\theta+i\sin\theta)\times(\cos\theta'+i\sin\theta')=(\cos\theta\cos\theta'-\sin\theta\sin\theta')+i(\cos\theta\sin\theta'+\sin\theta\cos\theta')$$
$$=\cos(\theta+\theta')+i\sin(\theta+\theta').$$

On observe donc une somme « se transformant » en un produit ce qui amène la notation suivante.

Définition 5 *Pour $\theta\in\mathbb{R}$, on note* $\boldsymbol{e^{i\theta}=\cos\theta+i\sin\theta}\in\mathbb{C}$.

En effet, d'après le calcul introductif précédent, on a bien :

- $e^{i\theta}\times e^{i\theta'}=e^{i(\theta+\theta')}$,
- $e^{0i}=\cos 0+i\sin 0=1=e^0$,
- $\dfrac{1}{e^{i\theta}}=\frac{1}{\cos\theta+i\sin\theta}\times\frac{\cos\theta-i\sin\theta}{\cos\theta-i\sin\theta}=\frac{\cos\theta-i\sin\theta}{\cos^2\theta+\sin^2\theta}=\cos\theta-i\sin\theta=\overline{e^{i\theta}}$
  $=\cos(-\theta)+i\sin(-\theta)=e^{-i\theta}$.

Ainsi, **la notation exponentielle suit bien les règles de calcul des puissances** dans le cadre réel.

Remarque : $\arg(e^{i\theta}) \equiv \theta\,[2\pi]$ et $\left|e^{i\theta}\right| = 1$ donc $e^{i\theta} \in \mathbb{U}$
et même, $\mathbb{U} = \{e^{i\theta} \;/\; \theta \in \mathbb{R}\}$.

Exemples : $e^{i\pi} = -1$, $e^{i\frac{\pi}{2}} = i$, $e^{-i\frac{\pi}{2}} = -i$, $e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Théorème 2 *Tout nombre complexe non nul de module r et d'argument θ peut s'écrire sous la forme suivante, appelée* ***notation exponentielle***, $\boldsymbol{z = re^{i\theta}}$.

Dém. : Ceci découle de la forme trigonométrique $z = |z|\,(\cos\theta + i\sin\theta)$. □

5.2 Notation exponentielle et opérations

Théorème 3
Soient r et r' deux réels strictement positifs et soient θ et $\theta' \in \mathbb{R}$.
On pose $z = re^{i\theta}$ *et* $z' = r'e^{i\theta'}$.

- $\overline{z} = \overline{re^{i\theta}} = re^{-i\theta}$ *i.e.* $|\overline{z}| = |z|$ *et* $\arg(\overline{z}) \equiv -\arg(z)\,[2\pi]$.
- $zz' = rr'e^{i(\theta+\theta')}$ *i.e.* $|zz'| = |z|\,|z'|$ *et* $\arg(zz') \equiv \arg(z) + \arg(z')\,[2\pi]$.
- $\dfrac{z}{z'} = \dfrac{r}{r'}e^{i(\theta-\theta')}$ *i.e.* $\left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$ *et* $\arg\left(\dfrac{z}{z'}\right) \equiv \arg(z) - \arg(z')\,[2\pi]$.
- $z^n = r^n e^{in\theta}$ *i.e.* $|z^n| = |z|^n$ *et* $\arg(z^n) \equiv n\arg(z)\,[2\pi]$.

- *D'où la formule de Moivre* $\boldsymbol{[\cos\theta + i\sin\theta]^n = \cos(n\theta) + i\sin(n\theta)}$.

- *Formules d'Euler :* $\cos\theta = \dfrac{e^{i\theta} + e^{-i\theta}}{2}$ *et* $\sin\theta = \dfrac{e^{i\theta} - e^{-i\theta}}{2i}$.

Démonstration : Les trois premiers points découlent du précédent calcul introductif de la notation exponentielle. La formule de Moivre est une simple réécriture de $z^n = r^n e^{in\theta}$, cette dernière se démontrant par récurrence :
$z^{n+1} = z \times z^n = re^{i\theta} \times r^n e^{in\theta} = r^{n+1}e^{in\theta+i\theta} = r^{n+1}e^{i(n+1)\theta}$.
Les formules d'Euler n'utilisent que la propriété $e^{-i\theta} = \overline{e^{i\theta}}$. □

Remarque : La notation exponentielle d'un nombre complexe permet de retrouver facilement les formules de trigonométrie démontrées précédemment.
En effet, $\overline{e^{i\theta}} = e^{-i\theta}$ redonne les propriétés de parité de cos et sin,
$e^{i\theta}e^{i\theta'} = e^{i(\theta+\theta')}$ redonne les formules d'addition,
$e^{i\theta}\overline{e^{i\theta}} = e^{i(\theta-\theta)} = e^{0i} = 1$ redonne la formule fondamentale $\cos^2\theta + \sin^2\theta = 1$,
$(e^{i\theta})^2 = e^{2i\theta}$ redonne les formules de duplication,
les formules d'Euler redonnent les formules de linéarisation (et celles de degré supérieur),
et en dérivant formellement,
$\cos'(t) + i\sin'(t) = (e^{it})' = ie^{it} = i\cos(t) + i^2\sin(t) = -\sin(t) + i\cos(t) = e^{i(t+\frac{\pi}{2})}$,
on obtient les dérivées des lignes trigonométriques en *tournant* de $\frac{\pi}{2}$.

Exemples : Si $z_1 = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}) = \sqrt{2}e^{i\frac{\pi}{4}}$ et $z_2 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = e^{i\frac{\pi}{3}}$,

- $z_1 z_2 = \sqrt{2}e^{i\frac{7\pi}{12}}$: $|z_1 z_2| = 1 \times \sqrt{2} = \sqrt{2}$, $\arg(z_1 z_2) \equiv \frac{\pi}{4} + \frac{\pi}{3} \equiv \frac{7\pi}{12}\,[2\pi]$.
- $\frac{z_1}{z_2} = \sqrt{2}e^{-i\frac{\pi}{12}}$: $\left|\frac{z_1}{z_2}\right| = \frac{\sqrt{2}}{1} = \sqrt{2}$, $\arg(\frac{z_1}{z_2}) \equiv \frac{\pi}{4} - \frac{\pi}{3} \equiv -\frac{\pi}{12}\,[2\pi]$.
- $z_1^8 = 16e^{2i\pi} = 16$: $\left|z_1^8\right| = \sqrt{2}^8 = 16$, $\arg(z_1^8) \equiv 8\frac{\pi}{4} \equiv 0\,[2\pi]$.

Si $\boldsymbol{j = e^{i\frac{2\pi}{3}}}$, $|j| = 1$, $j^2 = e^{4i\pi/3}$ et $j^3 = e^{2i\pi} = 1$.
On a aussi $(j^2)^3 = e^{4i\pi} = 1$ et $\frac{1}{j} = e^{-i\frac{2\pi}{3}} = j^2 = \overline{j}$. On connaît donc toutes les racines de $z^3 - 1$.

La propriété suivante étend celle valable dans $\mathbb{R}$ avec la valeur absolue.

Propriété 11 ***Inégalité triangulaire***
Pour tous nombres complexes z et z', $\boldsymbol{|z + z'| \leqslant |z| + |z'|}$.

Démonstration : On a :
$|z + z'|^2 = (a+a')^2 + (b+b')^2 = a^2 + 2aa' + a'^2 + b^2 + 2bb' + b'^2 = |z|^2 + 2(aa' + bb') + |z'|^2$.
Or $aa' + bb' = \mathfrak{Re}(z\overline{z'}) \leqslant \left|z\overline{z'}\right| = |z|\left|\overline{z'}\right| = |z|\,|z'|$
donc $|z + z'|^2 \leqslant |z|^2 + 2\,|z|\,|z'| + |z'|^2 = (|z| + |z'|)^2$.
Nous avons utilisé le th. 3 ainsi qu'un lemme évident : $\boldsymbol{\forall Z \in \mathbb{C},\ \mathfrak{Re}(Z) \leqslant |Z|}$. □

5.3 Exponentielle complexe

Nous ne donnons ici qu'une définition (naturelle) de la généralisation de la fonction exponentielle à tout le plan complexe.

Définition 6 *Soit $z \in \mathbb{C}$. On pose* $\boldsymbol{\exp(z) = e^z = e^{\mathfrak{Re}(z)}.e^{i\mathfrak{Im}(z)}}$.

Autrement dit, $e^{a+ib} = e^a.e^{ib}$ est de module e^a et d'argument $b\,[2\pi]$.
Ceci prolonge bien l'exponentielle réelle : si $\mathfrak{Im}(z) = 0$ alors $e^{i\mathfrak{Im}(z)} = 1$ et $e^{a+0i} = e^a \times 1 = e^a$.

En revanche, la définition d'un logarithme complexe est bien plus délicate. L'argument n'étant défini que modulo 2π, les antécédents d'une exponentielle ne peuvent être unique. Et ce n'est pas le seul problème.

Exercices

NOMBRES COMPLEXES : GÉOMÉTRIE

Le plan est muni d'un repère orthonormé direct $(O\,;\,\vec{u},\,\vec{v})$ dès que cela est nécessaire.

Exercice 1 Placer les points A, B et C d'affixes respectives $a = 1+2i$, $b = -3-i$ et $c = 3-2i$ puis déterminer l'affixe du point D tel que le quadrilatère $ABCD$ soit un parallélogramme.

Exercice 2 Soient A, B, C D les points d'affixe respective $z_A = 6+5i$, $z_B = 7+2i$, $z_C = 10+i$ et $z_D = 9+4i$. Quelle est la nature du quadrilatère $ABCD$?

Exercice 3 Soient A, B, C et D les points d'affixe respective $z_A = 3i-1$, $z_B = 2+i$, $z_C = 8-3i$ et $z_D = 3-i$.

1. Démontrer que les points A, B et C sont alignés.
2. Déterminer l'affixe du point E de l'axe des imaginaires purs tel que les droites (ED) et (BC) soient parallèles.

Exercice 4 À tout point M du plan complexe d'affixe z, on associe le point M' d'affixe z' définie par $z' = z^2 + 2iz$ et l'on désigne par $\mathscr{E}$ l'ensemble des point M tel que $z' \in \mathbb{R}$.

1. Démontrer que les points $A(2-i)$ et $B(-3i)$ appartiennent à $\mathscr{E}$.
2. En posant $z = x+iy$, montrer que $M \in \mathscr{E}$ si, et seulement si, $x(y+1) = 0$.
3. En déduire l'ensemble $\mathscr{E}$.

Exercice 5 Calculer le module de chacun des nombres complexes suivants.

(a) $-3+4i$

(b) $\sqrt{6} - i\sqrt{2}$

(c) $(3-4i)(\sqrt{6} - i\sqrt{2})$

(d) $(\sqrt{6} + i\sqrt{2})^2$

Exercice 6 Déterminer une forme trigonométrique (ou exponentielle) de chacun des nombres complexes suivants.

(a) $3 + 3i\sqrt{3}$

(b) $-\sqrt{2} + i\sqrt{2}$

(c) $2-2i$

(d) $-3i$

(e) -7

(f) $\dfrac{3}{1-i}$

(g) $(1-i\sqrt{3})(1+i)$

(h) $-\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$

(i) $\sin\frac{\pi}{9} + i\cos\frac{\pi}{9}$

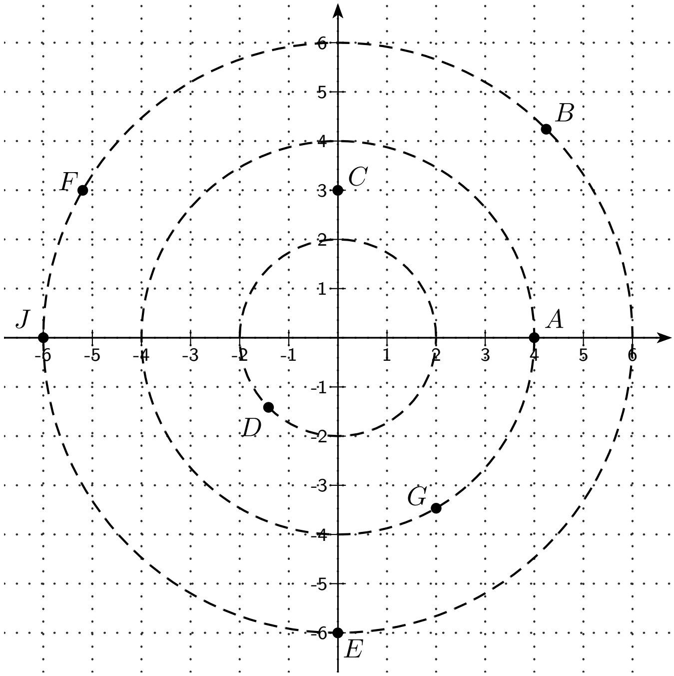
(j) $\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)^{10}$

(k) $(\sqrt{2} - i\sqrt{2})(-\cos\frac{\pi}{7} + i\sin\frac{\pi}{7})$

(l) $(1+i)^{2012}(1-i)^{2013}$

Exercice 7 Le plan complexe est muni du repère orthonormé direct $(O; \overrightarrow{u}; \overrightarrow{v})$ suivant. Les points A, B, C, D, E, F, G, H, I et J ont pour affixes respectives z_A, z_B, z_C, z_D, z_E, z_F, z_G, z_H, Z_I et z_J.
Dans cet exercice, on ne demande aucune justification.

1. Placer les points H et I pour $z_H = 3 + 2i$ et $z_I = 4e^{i\frac{2\pi}{3}}$.
2. Donner le module et un argument de z_B.
3. Donner une forme trigonométrique de z_D.
4. Donner une forme exponentielle de z_A, z_C, z_E, z_F, z_G et z_J
5. Donner la forme algébrique du nombre complexe z_F, puis la forme algébrique de $\overline{z_F}$, le conjugué de z_F. Placer alors le point $\widetilde{F}$ correspondant.



Exercice 8 Dans chacun des cas, représenter l'ensemble des points M dont l'affixe z vérifie l'égalité donnée.

(a) $\mathfrak{Re}(z) = -2$

(b) $\mathfrak{Im}(z) = 3$

(c) $|z| = 4$

(d) $|z - 1| = 2$

(e) $\arg(z) \equiv \frac{\pi}{3}\,[2\pi]$

(f) $\arg(-z) \equiv -\frac{\pi}{6}\,[2\pi]$

(g) $\arg(iz) \equiv \frac{5\pi}{4}\,[\pi]$

(h) $\arg\left(\dfrac{z}{1+i}\right) \equiv \frac{\pi}{4}\,[\pi]$

(j) $\dfrac{i}{1+z} \in \mathbb{R}$

Exercice 9 Calculer $(1+i)^2$, $(1+i)^4$ et $(1+i)^8$.
Pour $n \in \mathbb{N}$, M_n est le point d'affixe $(1+i)^n$.
Pour quelles valeurs de $n \in \mathbb{N}$ le point M_n appartient-il à l'axe des abscisses ?

Exercice 10 On considère le nombre complexe $z = (\sqrt{3}+1) + i(\sqrt{3}-1)$.

1. Écrire z^2 sous forme algébrique puis en déterminer le module et un argument.
2. En déduire le module et un argument de z.
3. Déterminer la valeur exacte de $\cos\frac{\pi}{12}$ et $\sin\frac{\pi}{12}$.

Exercice 11 Calculer les valeurs exactes des sinus et cosinus des nombres suivants.

(a) $\frac{7\pi}{12}$ (b) $\frac{\pi}{12}$ (c) $\frac{5\pi}{12}$ (d) $\frac{\pi}{8}$ (e) $\frac{7\pi}{24}$

Exercice 12 Déterminer une forme trigo. (ou expo.) de chacun des nombres complexes suivants où $x \in \mathbb{R}$.

(a) $\cos(x) + i\sin(x)$
(b) $\cos(x) - i\sin(x)$
(c) $-3\cos(x) - 3i\sin(x)$
(d) $\sin(x) + i\cos(x)$
(e) $2\sin(x) - 2i\cos(x)$
(f) $-\sqrt{3}\sin(x) - i\sqrt{3}\cos(x)$

Exercice 13 Étudier la limite de la suite $(z_n)_{\mathbb{N}}$ définie par $z_n = \frac{\ln(n+3)}{n+3}e^{ni\frac{\pi}{12}}$.

Exercice 14 On pose $z = \rho e^{i\theta}$.
Déterminer la forme exponentielle de $-z$, iz, $-iz$, $\overline{z}$, $-\overline{z}$, $\overline{iz}$ et $-\overline{iz}$.

Exercice 15 Donner une forme exponentielle des nombres complexes suivants.

(a) $-2ie^{i\frac{\pi}{3}}$
(b) $(1-i)e^{i\frac{\pi}{6}}$
(c) $\dfrac{3}{e^{i\frac{\pi}{7}}}$
(d) $\dfrac{3i}{e^{i\frac{2\pi}{5}}}$
(e) $\dfrac{-4i}{i\sqrt{3}-1}$
(f) $\dfrac{1+i}{\sqrt{3}-i}$

Exercice 16 Soient $z_1 = e^{i\frac{\pi}{3}}$, $z_2 = 3e^{-i\frac{\pi}{4}}$ et $z_3 = \sqrt{2}e^{i\frac{2\pi}{3}}$.
Donner une forme exponentielle des nombres complexes suivants.

(a) z_1z_2 (b) $\dfrac{z_1}{z_2}$ (c) z_1^3 (d) $z_1z_2z_3$ (e) z_3^4 (f) $\dfrac{z_2}{z_3}$

Exercice 17 Écrire z sous forme exponentielle et en déduire la forme algébrique de $\overline{z}$ et celle de $\dfrac{1}{z}$ lorsque :

(a) $z = \dfrac{6}{1+i}$
(b) $z = (1+i\sqrt{3})^4$
(c) $z = 3ie^{i\frac{\pi}{3}}$
(d) $z = -12e^{i\frac{\pi}{4}}$

Exercice 18 Soient p et $q \in \mathbb{R}$.

1. Vérifier que $p = \frac{p+q}{2} + \frac{p-q}{2}$.
2. Montrer que $e^{ip} + e^{iq} = 2\cos(\frac{p-q}{2})e^{i\frac{p+q}{2}}$.
3. Montrer une expression analogue pour $e^{ip} - e^{iq}$.
4. En déduire une expression factorisée de $\cos(p) + \cos(q)$, $\sin(p) + \sin(q)$, $\cos(p) - \cos(q)$ et $\sin(p) - \sin(q)$.
5. Résoudre dans $\mathbb{R}$ l'équation $\mathscr{E}:\ \sin(2x) - \sin(6x) = 0$.

Exercice 19
Déterminer tous les entiers naturels n tels que $(-\sqrt{3}+i)^n$ soit un imaginaire pur.

Exercice 20 Déterminer la forme algébrique des nombres suivants.

$a = 3e^{i\frac{\pi}{6}}.e^{i\frac{5\pi}{3}}$	$c = e^{-i\frac{2\pi}{3}} + e^{i\frac{3\pi}{4}}$
$b = \left(\sqrt{3}e^{-i\frac{5\pi}{2}}\right)^4$	$d = 4e^{-i\frac{4\pi}{3}} - 2e^{i\frac{\pi}{6}}$

Exercice 21 Déterminer la forme exponentielle du nombre $Z = 1 + i\sqrt{3}$ puis en déduire la forme algébrique des nombres $Z' = (1+i\sqrt{3})^5$,
$Z'' = (1+i\sqrt{3})^5 + (1-i\sqrt{3})^5$ et $Z''' = (1+i\sqrt{3})^5 - (1-i\sqrt{3})^5$.

Exercice 22 Soient A_{5+2i} et B_{2+5i} dans le plan complexe.
Déterminer une mesure en radian de l'angle $\left(\overrightarrow{u}\,;\overrightarrow{AB}\right)$.

Exercice 23 Soit $(u_n)_{\mathbb{N}}$ la suite définie par $u_n = \left(\frac{1+i\sqrt{3}}{1-i}\right)^n$.
Déterminer la forme trigonométrique de u_n en fonction de n.

Exercice 24 VouF. Pour chacune des implications suivantes, dire si elle est vraie, formuler l'implication réciproque puis dire si cette dernière est vraie. Justifier.

(a) Si $z \in \mathbb{U}$ alors $\overline{z} = \dfrac{1}{z}$.

(b) Si $z = z'$ ou $z = -z'$ alors $|z| = |z'|$.

(c) Soit $z \neq 0$. Si $\dfrac{z}{\overline{z}} \in \mathbb{R}$ alors $z \in \mathbb{R}$ ou $z \in i\mathbb{R}$.

Exercice 25 z est un nombre complexe non nul et $z' = \dfrac{-2}{z}$.

1. Quelle relation lie les modules de z et z' ? Les arguments de z et z' ?
2. Dans le plan complexe, M est le point d'affixe z et M' celui d'affixe z', $\mathscr{D}^*$ est le disque fermé de centre O et de rayon 2, privé de O et A est le point d'affixe a tel que $|a| = 2$ et $\arg(a) \equiv \frac{\pi}{4}\,[2\pi]$.
   (a) Quel est l'ensemble des points M' lorsque le point M décrit $\mathscr{D}^*$?
   (b) Quel est l'ensemble des points M' lorsque le point M décrit le segment $[OA]$ privé de O ?

Exercice 26 Nombres complexes de module 1

1. Soient z et $z' \in \mathbb{U}$. Montrer que $zz' \in \mathbb{U}$ et, après avoir justifié son existence, montrer que $\dfrac{z}{z'} \in \mathbb{U}$.
2. Montrer que $z \in \mathbb{U} \iff \overline{z} = \frac{1}{z}$.
3. Soient a, b et $c \in \mathbb{U}$. Montrer que $|ab+bc+ca| = |a+b+c|$.
4. Soit $z \in \mathbb{U}$. Calculer $|1+z|^2 + |1-z|^2$.

Exercice 27 Soit $z \in \mathbb{U}$.

1. Démontrer que $z + \dfrac{1}{z} \in \mathbb{R}$.
2. Démontrer que $z^2 - \dfrac{1}{z^2} \in i\mathbb{R}$.

Exercice 28 Pour tout nombre complexe différent de 1, on pose $z' = \dfrac{z+1}{z-1}$. Démontrer que l'ensemble des complexes z tels que z' soit imaginaire pur est l'ensemble $\mathbb{U} \setminus \{1\}$.

Exercice 29

1. Soit x un réel.
   (a) Développer $(\cos(x) + i\sin(x))^3$.
   (b) Exprimer $\cos(3x) + i\sin(3x)$ en fonction de $\cos(x)$ et $\sin(x)$.
   (c) Montrer que $\cos(3x) = 4\cos^3(x) - 3\cos(x)$
   et $\sin(3x) = -4\sin^3(x) + 3\sin(x)$.
2. Linéariser les expressions suivantes c.-à-d. les exprimer comme somme de sinus et de cosinus d'argument nx.

(a) $\cos^2(x)$	(d) $\cos^2(x)\sin(x)$	(g) $\cos^2(x)\sin^3(x)$
(b) $\sin^2(x)$	(e) $\cos^4(x)$	
(c) $\sin^3(x)$	(f) $\sin^5(x)$	(h) $\cos^3(x) + 2\sin^3(x)$

3. En utilisant les formules d'Euler, démontrer que pour tout réel x,
   (a) $\cos(2x) = 2\cos^2(x) - 1$ (b) $\sin(2x) = 2\cos(x)\sin(x)$.
4. Déterminer la valeur exacte de $I = \displaystyle\int_0^{\frac{\pi}{3}} \cos^2(x)\,\mathrm{d}x$, $J = \displaystyle\int_0^{\frac{\pi}{3}} \sin^3(x)\,\mathrm{d}x$ et $K = \displaystyle\int_0^{\frac{\pi}{3}} \cos^2(x)\sin^3(x)\,\mathrm{d}x$.

Exercice 30 À tout complexe $z = a + ib$, on associe $\exp(z) = e^a.e^{ib}$.

1. Vérifier que, pour tous complexes z_1, z_2, $\exp(z_1 + z_2) = \exp(z_1).\exp(z_2)$.
2. Déterminer la forme algébrique de $\exp(2 + 3i)$.
3. Déterminer une solution de l'équation $\exp(z) = 1 + i\sqrt{3}$. En existe-t-il d'autres ?

Exercice 31 Spirale
Dans le plan complexe, on considère la suite de points M_n d'affixes z_n définies par

$$\begin{cases} z_0 & = & 1 \\ z_{n+1} & = & \left(1 + i\frac{\sqrt{3}}{3}\right) z_n. \end{cases}$$

1. Déterminer la forme exponentielle de $q = 1 + i\frac{\sqrt{3}}{3}$ et en déduire celles de z_1 et de z_2.
2. Déterminer la forme exponentielle de z_n en fonction de $n \in \mathbb{N}$.
3. Pour tout entier n, on pose $d_n = |z_{n+1} - z_n|$.
   (a) Interpréter graphiquement d_n.
   (b) Calculer d_0.
   (c) Démontrer que, pour tout $n \in \mathbb{N}$, $z_{n+2} - z_{n+1} = \left(1 + i\frac{\sqrt{3}}{3}\right)(z_{n+1} - z_n)$.

EXERCICES

   (d) En déduire que (d_n) est géométrique et donner une expression de d_n en fonction de n.

4. (a) Montrer que, pour tout n, $\quad |z_{n+1}|^2 = |z_n|^2 + d_n^2$.

   (b) En déduire que, pour tout entier n, le triangle OM_nM_{n+1} est rectangle.

5. Comment construire la suite des points M_n ?

Tournez jusqu'aux pages 293 et 297 afin de réaliser les devoirs n^{os} 6 et 7.

Corrigé des exercices

Nombres complexes : géométrie

J'ai souvent tapé des formes exponentielles alors que des formes trigonométriques étaient demandées : c'est bien plus court, préserve le bout des doigts et économise le papier. Ne faites pas de même le jour $\mathfrak{J}$.

Exercice 1 $ABCD$ parallélogramme $\iff \overrightarrow{CD} = \overrightarrow{BA}$
$\iff d - c = a - b \iff d = a - b + c = 7 + i.$
Ou alors $Milieu[AC] = Milieu[BD] \iff \frac{a+c}{2} = \frac{b+d}{2} \iff \ldots$

Exercice 2 On a $z_{\overrightarrow{AB}} = z_B - z_A = (7+2i) - (6+5i) = 1 - 3i$
et $z_{\overrightarrow{DC}} = z_C - z_D = (10+i) - (9+4i) = 1 - 3i = z_{\overrightarrow{AB}}$ donc $\overrightarrow{AB} = \overrightarrow{DC}$: $ABCD$ est un parallélogramme.
De plus, $AB^2 = \left|z_{\overrightarrow{AB}}\right|^2 = 1^2 + 3^2 = 10$ et
$AD^2 = \left|z_{\overrightarrow{AD}}\right|^2 = |z_D - z_A|^2 = |9 + 4i - 6 - 5i|^2 = 3^2 + (-1)^2 = 10$
donc $AB = AD$: $ABCD$ est un losange.
Puisque $AC^2 = \left|z_{\overrightarrow{AC}}\right|^2 = |z_C - z_A|^2 = |10 + i - 6 - 5i|^2 = 4^2 + (-4)^2 = 32$ et $BD^2 = \left|z_{\overrightarrow{BD}}\right|^2 = |z_D - z_B|^2 = |9 + 4i - 7 - 2i|^2 = 2^2 + 2^2 = 8$, $AC \neq BD$: $ABCD$ n'est pas un carré.

Exercice 3

1. On a $z_{\overrightarrow{AB}} = z_B - z_A = (2+i) - (3i-1) = 3 - 2i$
   et $z_{\overrightarrow{BC}} = z_C - z_B = (8-3i) - (2+i) = 6 - 4i = 2(z_B - z_A) = 2z_{\overrightarrow{AB}}$
   donc $\overrightarrow{BC} = 2\overrightarrow{AB}$ et les points A, B et C sont alignés.
2. Soit $z_E = iy$. On a $z_{\overrightarrow{ED}} = z_D - z_E = 3 - i(1+y)$.
   Les droites(ED) et (BC) sont parallèles *ssi* $\overrightarrow{ED}$ et $\overrightarrow{BC}$ colinéaires
   ssi il existe $\lambda \in \mathbb{R}$ tel que $\overrightarrow{BC} = \lambda\overrightarrow{ED}$
   ssi il existe $\lambda \in \mathbb{R}$ tel que $6 - 4i = \lambda(3 - i(1+y)) = 3\lambda - \lambda i(1+y)$
   d'où $\lambda = 2$ et $-2i(1+y) = -4i$ c.-à-d. $y = 1$: $E\,(0\,,\,1)$.

Exercice 4 $\mathscr{E} = \{M(z)/z' = z^2 + 2iz \in \mathbb{R}\}$.

1. On a $(2-i)' = (2-i)^2 + 2i(2-i) = 4 - 4i + i^2 + 4i - 2i^2 = 4 - 1 + 2 = 5 \in \mathbb{R}$
   donc $A(2-i) \in \mathscr{E}$
   et $(-3i)' = (-3i)^2 + 2i(-3i) = 9i^2 - 6i^2 = -9 + 6 = -3 \in \mathbb{R}$
   donc $B(-3i) \in \mathscr{E}$.
2. Posons $z = x + iy$.
   On a $z' = z^2 + 2iz = (x+iy)^2 + 2i(x+iy) = x^2 + 2ixy + (iy)^2 + 2ix + 2i^2y$
   $z' = (x^2 - y^2 - 2y) + i(2xy + 2x)$
   et $M \in \mathscr{E} \iff \mathfrak{Im}(z') = 0 \iff 2xy + 2x = 0 \iff x(y+1) = 0.$

3. Ainsi, $M(x+iy) \in \mathscr{E} \iff x=0$ ou $y+1=0$ èt $\mathscr{E} = \mathscr{D}(x=1) \cup \mathscr{D}(y=-1)$, union de deux droites.

Exercice 5 Module des nombres complexes.

(a) $|-3+4i| = \sqrt{3^2+4^2} = 5$

(b) $|\sqrt{6} - i\sqrt{2}| = \sqrt{6+2} = 2\sqrt{2}$

(c) $|(3-4i)(\sqrt{6} - i\sqrt{2})| = 5 \times 2\sqrt{2} = 10\sqrt{2}$

(d) $|(\sqrt{6} + i\sqrt{2})^2| = (2\sqrt{2})^2 = 8$

Exercice 6 Forme trigonométrique ou exponentielle.

(a) $3+3i\sqrt{3} = 6(\frac{1}{2} + \frac{\sqrt{3}}{2}i) = 6\,e^{i\frac{\pi}{3}}$

(b) $-\sqrt{2} + i\sqrt{2} = 2(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) = 2\,e^{i\frac{3\pi}{4}}$

(c) $2-2i = 2\sqrt{2}(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i) = 2\sqrt{2}\,e^{-i\frac{\pi}{4}}$

(d) $-3i = 3(-i) = 3\,e^{-i\frac{\pi}{2}}$

(e) $-7 = 7(-1) = 7\,e^{i\pi}$

(f) $\frac{3}{1-i} = \frac{3}{\sqrt{2}\,e^{-i\frac{\pi}{4}}} = \frac{3\sqrt{2}}{2}\,e^{i\frac{\pi}{4}}$

(g) $(1-i\sqrt{3})(1+i) = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}i).\sqrt{2}(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) = 2\sqrt{2}\,e^{i(-\frac{\pi}{3}+\frac{\pi}{4})} = 2\sqrt{2}\,e^{-i\frac{\pi}{12}}$

(h) $-\cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \cos(\pi - \frac{\pi}{3}) + i\sin(\pi - \frac{\pi}{3}) = e^{i\frac{2\pi}{3}}$

(i) $\sin\frac{\pi}{9} + i\cos\frac{\pi}{9} = \cos(\frac{\pi}{2} - \frac{\pi}{9}) + i\sin(\frac{\pi}{2} - \frac{\pi}{9}) = e^{i\frac{7\pi}{18}}$

(j) $\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)^{10} = (e^{i\frac{\pi}{4}})^{10} = e^{i\frac{10\pi}{4}} = e^{i\frac{\pi}{2}}$

(k) $(\sqrt{2} - i\sqrt{2})(-\cos\frac{\pi}{7} + i\sin\frac{\pi}{7}) = 2(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i)(\cos(\pi - \frac{\pi}{7}) + i\sin(\pi - \frac{\pi}{7})$
$= 2\,e^{-i\frac{\pi}{4}+i\frac{6\pi}{7}} = 2\,e^{i\frac{17\pi}{28}}$

(l) $(1+i)^{2012}(1-i)^{2013} = [(1+i)(1-i)]^{2012}(1-i) = 2^{2012}\sqrt{2}\,e^{-i\frac{\pi}{4}}$

Exercice 7

2. On lit sur le graphique que le module de z_B est 6 car $OB = 6$ et qu'un argument de z_B est $\frac{\pi}{4}$ car l'angle orienté $(\overrightarrow{u};\overrightarrow{OB})$ a pour mesure $\frac{\pi}{4}$. Ainsi, $z_B = 6e^{i\frac{\pi}{4}}$. De même pour les autres points.
3. $z_D = 2(\cos(-\frac{3\pi}{4}) + i\sin(-\frac{3\pi}{4}))$.
4. $z_A = 4e^{i0}$, $z_C = 3e^{i\frac{\pi}{2}}$, $z_E = 6e^{-i\frac{\pi}{2}}$, $z_F = 6e^{i\frac{5\pi}{6}}$, $z_G = 4e^{-i\frac{\pi}{3}}$ et $z_J = 6e^{i\pi}$.
5. On lit $z_F = 6(\cos(\frac{5\pi}{6}) + i\sin(\frac{5\pi}{6})) = 6(-\frac{\sqrt{3}}{2} + \frac{1}{2}i) = -3\sqrt{3} + 3i$.
   On en déduit que $z_{\widetilde{F}} = \overline{z_F} = 6(-\frac{\sqrt{3}}{2} - \frac{1}{2}i) = -3\sqrt{3} - 3i$.

Exercice 8 Lieux géométriques.

(a) $\mathfrak{Re}(z) = -2$: droite d'équation $x = -2$.

(b) $\mathfrak{Im}(z) = 3$: droite d'équation $y = 3$.

(c) $|z| = 4$: cercle de centre O et de rayon 4.

(d) $|z-1| = 2$: cerlce de centre $(\,1\,,\,0\,)$ et de rayon 2.

(e) $\arg(z) \equiv \frac{\pi}{3}\,[2\pi]$: demi-droite issue de O et passant par $\left(\frac{1}{2}\,,\,\frac{\sqrt{3}}{2}\right)$, privée de l'origine.

(f) $\arg(-z) \equiv -\frac{\pi}{6}\,[2\pi] \iff \arg(z) \equiv \pi - \frac{\pi}{6}\,[2\pi] \equiv \frac{5\pi}{6}\,[2\pi]$: demi-droite issue de O et passant par $\left(-\frac{\sqrt{3}}{2}\,,\,\frac{1}{2}\right)$, privée de l'origine.

(g) $iz = ze^{i\frac{\pi}{2}}$ donc $\arg(iz) \equiv \arg(z) + \frac{\pi}{2} \equiv \frac{5\pi}{4}\,[\pi] \iff \arg(z) \equiv \frac{5\pi}{4} - \frac{\pi}{2}\,[\pi]$
$\arg(iz) \equiv \frac{3\pi}{4}\,[\pi]$: droite passant par $\left(-\frac{\sqrt{2}}{2}\,,\,\frac{\sqrt{2}}{2}\right)$ et $\left(\frac{\sqrt{2}}{2}\,,\,-\frac{\sqrt{2}}{2}\right)$, privée de O.

(h) $\frac{z}{1+i} = \frac{z}{\sqrt{2}\,e^{i\frac{\pi}{4}}} = \frac{ze^{-i\frac{\pi}{4}}}{\sqrt{2}}$ donc $\arg(\frac{z}{1+i}) \equiv \frac{\pi}{4}\,[\pi] \iff \arg(z) \equiv \frac{\pi}{4} + \frac{\pi}{4}\,[\pi]$
$\arg(iz) \equiv \frac{\pi}{2}\,[\pi]$: axe des ordonnées privé de l'origine.

(j) Pour $z \neq -1$, $\frac{i}{1+z} \in \mathbb{R} \iff \frac{i}{1+z} = \overline{\left(\frac{i}{1+z}\right)} \iff \frac{i}{1+z} = \frac{-i}{1+\overline{z}}$
$\iff 1+\overline{z} = -(1+z) \iff z+\overline{z} = -2 \iff 2\mathfrak{Re}(z) = -2$
$\iff \mathfrak{Re}(z) = -1$: droite $x = -1$ privée du point $(-1\,,\,0)$.

Exercice 9 On a $1+i = \sqrt{2}e^{i\frac{\pi}{4}}$ donc $(1+i)^2 = 2e^{2i\frac{\pi}{4}} = 2e^{i\frac{\pi}{2}} = 2i$, $(1+i)^4 = (2i)^2 = -4$ et $(1+i)^8 = (-4)^2 = 16$.
Sinon, $(1+i)^2 = 1^2 + 2i + i^2 = 2i$, $(1+i)^4 = (2i)^2 = -4$ et $(1+i)^8 = (-4)^2 = 16$. Puisque $(1+i)^n = \sqrt{2}^{\,n}\, e^{ni\frac{\pi}{4}}$, M_n appartient à l'axe des abscisses si, et seulement si, $n\frac{\pi}{4} \equiv 0[\pi] \iff \frac{n}{4} \equiv 0[1] \iff n$ est un multiple de 4.

Exercice 10 $z = (\sqrt{3}+1) + i(\sqrt{3}-1)$.

1. $z^2 = (\sqrt{3}+1)^2 + 2i(\sqrt{3}+1)(\sqrt{3}-1) - (\sqrt{3}-1)^2$
$= 3+2\sqrt{3}+1-3+2\sqrt{3}-1+2i(3-1) = 4(\sqrt{3}+i). = 4\times 2(\frac{\sqrt{3}}{2}+\frac{1}{2}i) = 8e^{i\frac{\pi}{6}}$.
2. On a $|z|^2 = |z^2| = 8$ donc $|z| = 2\sqrt{2}$ et puisque $\mathfrak{Re}(z) > 0$ et $\mathfrak{Im}(z) > 0$, on a $\arg(z) \in \left]\,0\,;\frac{\pi}{2}\,\right[\ [2\pi]$.
Ainsi, $\arg(z) \equiv \frac{1}{2}\arg(z^2)\,[2\pi] \equiv \frac{\pi}{12}\,[2\pi]$.
3. Alors, $\cos(\frac{\pi}{12}) = \frac{\mathfrak{Re}(z)}{|z|} = \frac{\sqrt{3}+1}{2\sqrt{2}}$ et $\sin(\frac{\pi}{12}) = \frac{\mathfrak{Im}(z)}{|z|} = \frac{\sqrt{3}-1}{2\sqrt{2}}$.

Exercice 11

(a) $\frac{7\pi}{12} = \frac{\pi}{3} + \frac{\pi}{4}$
donc $\cos(\frac{7\pi}{12}) = \cos(\frac{\pi}{3})\cos(\frac{\pi}{4}) - \sin(\frac{\pi}{3})\sin(\frac{\pi}{4}) = \frac{1}{2}\frac{\sqrt{2}}{2} - \frac{\sqrt{3}}{2}\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{4}(1-\sqrt{3})$
et $\sin(\frac{7\pi}{12}) = \sin(\frac{\pi}{3})\cos(\frac{\pi}{4}) + \cos(\frac{\pi}{3})\sin(\frac{\pi}{4}) = \frac{\sqrt{3}}{2}\frac{\sqrt{2}}{2} + \frac{1}{2}\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{4}(\sqrt{3}+1)$

(b) $\frac{\pi}{12} = \frac{\pi}{3} - \frac{\pi}{4}$
donc $\cos(\frac{\pi}{12}) = \cos(\frac{\pi}{3})\cos(\frac{\pi}{4}) + \sin(\frac{\pi}{3})\sin(\frac{\pi}{4}) = \frac{1}{2}\frac{\sqrt{2}}{2} + \frac{\sqrt{3}}{2}\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{4}(1+\sqrt{3})$
et $\sin(\frac{\pi}{12}) = \sin(\frac{\pi}{3})\cos(\frac{\pi}{4}) - \cos(\frac{\pi}{3})\sin(\frac{\pi}{4}) = \frac{\sqrt{3}}{2}\frac{\sqrt{2}}{2} - \frac{1}{2}\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{4}(\sqrt{3}-1)$

(c) $\frac{5\pi}{12} = \frac{\pi}{2} - \frac{\pi}{12}$ donc $\cos(\frac{5\pi}{12}) = \sin(\frac{\pi}{12}) = \frac{\sqrt{2}}{4}(\sqrt{3}-1)$
et $\sin(\frac{5\pi}{12}) = \cos(\frac{\pi}{12}) = \frac{\sqrt{2}}{4}(1+\sqrt{3})$

(d) $\frac{\pi}{8} = 2\times\frac{\pi}{4}$ donc $\cos^2(\frac{\pi}{8}) = \frac{1+\cos(\frac{\pi}{4})}{2} = \frac{2+\sqrt{2}}{4}$ d'où $\cos(\frac{\pi}{8}) = \frac{\sqrt{2+\sqrt{2}}}{2}$
et $\sin^2(\frac{\pi}{8}) = \frac{1-\cos(\frac{\pi}{4})}{2} = \frac{2-\sqrt{2}}{4}$ d'où $\sin(\frac{\pi}{8}) = \frac{\sqrt{2-\sqrt{2}}}{2}$

(e) $\frac{7\pi}{24} = \frac{5\pi}{12} - \frac{\pi}{8}$ donc $\cos(\frac{7\pi}{24}) = \cos(\frac{5\pi}{12})\cos(\frac{\pi}{8}) + \sin(\frac{5\pi}{12})\sin(\frac{\pi}{8})$
$\cos(\frac{7\pi}{24}) = \frac{\sqrt{2}}{4}(\sqrt{3}-1)\frac{\sqrt{2+\sqrt{2}}}{2} + \frac{\sqrt{2}}{4}(1+\sqrt{3})\frac{\sqrt{2-\sqrt{2}}}{2} = \ldots$

et $\sin(\frac{7\pi}{24}) = \sin(\frac{5\pi}{12})\cos(\frac{\pi}{8}) - \cos(\frac{5\pi}{12})\sin(\frac{\pi}{8})$

$\sin(\frac{7\pi}{24}) = \frac{\sqrt{2}}{4}(1+\sqrt{3})\frac{\sqrt{2+\sqrt{2}}}{2} - \frac{\sqrt{2}}{4}(\sqrt{3}-1)\frac{\sqrt{2-\sqrt{2}}}{2} = ...$

Exercice 12

(a) $\cos(x) + i\sin(x) = e^{ix}$

(b) $\cos(x) - i\sin(x) = \cos(-x) + i\sin(-x) = e^{-ix}$

(c) $-3\cos(x) - 3i\sin(x) = 3(\cos(\pi+x) + i\sin(\pi+x)) = 3e^{i(\pi+x)}$

(d) $\sin(x) + i\cos(x) = \cos(\frac{\pi}{2}-x) + i\sin(\frac{\pi}{2}-x) = e^{i(\frac{\pi}{2}-x)}$

(e) $2\sin(x) - 2i\cos(x) = 2(\cos(x-\frac{\pi}{2}) + i\sin(x-\frac{\pi}{2})) = 2e^{i(x-\frac{\pi}{2})}$

(f) $-\sqrt{3}\sin(x) - i\sqrt{3}\cos(x) = \sqrt{3}(\cos(-x-\frac{\pi}{2}) + i\sin(-x-\frac{\pi}{2})) = \sqrt{3}e^{i(-x-\frac{\pi}{2})}$

Exercice 13

Pour tout $n \in \mathbb{N}$, on a $|z_n| = \frac{\ln(n+3)}{n+3} = \frac{\ln(N)}{N} \xrightarrow[N,n\to+\infty]{} 0$ par croissance comparée donc $z_n \xrightarrow[n\to\infty]{} 0$. Par ailleurs, $\arg(z_n) = n\frac{\pi}{12}$ et $\arg(z_{n+1}) = \arg(z_n) + \frac{\pi}{12}$. La suite $(z_n)_{\mathbb{N}}$ converge donc vers 0 en *spirale*.

Exercice 14 Pour $z = \rho e^{i\theta}$, on a $-z = -1 \times z = e^{i\pi}\rho e^{i\theta} = \rho e^{i(\theta+\pi)}$,

$iz = e^{i\frac{\pi}{2}}\rho e^{i\theta} = \rho e^{i(\theta+\frac{\pi}{2})}$,

$-iz = -1 \times iz = e^{i\pi}\rho e^{i(\theta+\frac{\pi}{2})} = \rho e^{i(\theta+\frac{\pi}{2}+\pi)} = \rho e^{i(\theta-\frac{\pi}{2})}$,

$\overline{z} = \overline{\rho e^{i\theta}} = \overline{\rho(\cos\theta + i\sin\theta)} = \rho(\cos\theta - i\sin\theta) = \rho(\cos(-\theta) + i\sin(-\theta)) = \rho e^{-i\theta}$,

$-\overline{z} = -1\rho e^{-i\theta} = e^{i\pi}\rho e^{-i\theta} = \rho e^{i(\pi-\theta)}$, $\overline{iz} = \overline{\rho e^{i(\theta+\frac{\pi}{2})}} = \rho e^{-i(\theta+\frac{\pi}{2})}$

et $-\overline{iz} = \rho e^{-i(\theta+\frac{\pi}{2})+i\pi} = \rho e^{i(\frac{\pi}{2}-\theta)}$.

Exercice 15 Forme exponentielle.

(a) $-2ie^{i\frac{\pi}{3}} = 2e^{-i\frac{\pi}{2}}e^{i\frac{\pi}{3}} = 2e^{i(\frac{\pi}{3}-\frac{\pi}{2})} = 2e^{-i\frac{\pi}{6}}$

(b) $(1-i)e^{i\frac{\pi}{6}} = \sqrt{2}e^{-i\frac{\pi}{4}}e^{i\frac{\pi}{6}} = \sqrt{2}e^{-i\frac{\pi}{12}}$

(c) $\frac{3}{e^{i\frac{\pi}{7}}} = 3e^{-i\frac{\pi}{7}}$

(d) $\frac{3i}{e^{i\frac{2\pi}{5}}} = 3e^{i\frac{\pi}{2}}e^{-i\frac{2\pi}{5}} = 3e^{i\frac{\pi}{10}}$

(e) $\frac{-4i}{i\sqrt{3}-1} = \frac{4e^{i\frac{3\pi}{2}}}{2(-\frac{1}{2}+i\frac{\sqrt{3}}{2})} = 2e^{i(\frac{3\pi}{2}-\frac{2\pi}{3})} = 2e^{i\frac{5\pi}{6}}$

(f) $\frac{1+i}{\sqrt{3}-i} = \frac{\sqrt{2}e^{i\frac{\pi}{4}}}{2e^{-i\frac{\pi}{6}}} = \frac{\sqrt{2}}{2}e^{i(\frac{\pi}{4}+\frac{\pi}{6})} = \frac{1}{\sqrt{2}}e^{i\frac{5\pi}{12}}$.

Exercice 16 Forme exponentielle.

(a) $z_1z_2 = e^{i\frac{\pi}{3}}.3e^{-i\frac{\pi}{4}} = 3e^{i\frac{\pi}{12}}$

(b) $\frac{z_1}{z_2} = \frac{e^{i\frac{\pi}{3}}}{3e^{-i\frac{\pi}{4}}} = \frac{1}{3}e^{i\frac{7\pi}{12}}$

(c) $z_1^3 = (e^{i\frac{\pi}{3}})^3 = e^{i\pi} = -1$

(d) $3\sqrt{2}e^{i(\frac{\pi}{3}-\frac{\pi}{4}+\frac{2\pi}{3})} = 3\sqrt{2}e^{i\frac{3\pi}{4}}$

(e) $(\sqrt{2}e^{i\frac{2\pi}{3}})^4 = 4e^{i\frac{8\pi}{3}} = 4e^{i\frac{2\pi}{3}}$

(f) $\frac{z_2}{z_3} = \frac{3e^{-i\frac{\pi}{4}}}{\sqrt{2}e^{i\frac{2\pi}{3}}} = \frac{3\sqrt{2}}{2}e^{-i\frac{11\pi}{12}}$

Exercice 17 Forme exponentielle et forme algébrique de $\overline{z}$ et de $\frac{1}{z}$.

(a) $z = \frac{6}{1+i} = \frac{6}{\sqrt{2}}e^{-i\frac{\pi}{4}}$, $\overline{z} = \frac{6}{\sqrt{2}}e^{i\frac{\pi}{4}} = \frac{6}{\sqrt{2}}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = 3+3i$,

$\frac{1}{z} = \frac{\sqrt{2}}{6}e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{6}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \frac{1}{6} + \frac{i}{6}$.

(b) $z = (1+i\sqrt{3})^4 = [2(\frac{1}{2}+i\frac{\sqrt{3}}{2})]^4 = (2e^{i\frac{\pi}{3}})^4 = 16e^{i\frac{4\pi}{3}} = 16e^{-i\frac{2\pi}{3}}$,
$\overline{z} = 16e^{i\frac{2\pi}{3}} = 16(-\frac{1}{2}+\frac{\sqrt{3}}{2}i) = -8+8i\sqrt{3}$,
$\frac{1}{z} = \frac{1}{16e^{-i\frac{2\pi}{3}}} = \frac{1}{16}e^{i\frac{2\pi}{3}} = -\frac{1}{32}+\frac{\sqrt{3}}{32}i.$

(c) $z = 3ie^{i\frac{\pi}{3}} = 3e^{i(\frac{\pi}{2}+\frac{\pi}{3})} = 3e^{\frac{5i\pi}{6}}$,
$\overline{z} = 3e^{-\frac{5i\pi}{6}} = 3(-\frac{\sqrt{3}}{2}-\frac{1}{2}i) = -\frac{3\sqrt{3}}{2}-\frac{3}{2}i, \quad \frac{1}{z} = \frac{1}{3}e^{-\frac{5i\pi}{6}} = -\frac{\sqrt{3}}{6}-\frac{1}{6}i.$

(d) $z = -12e^{i\frac{\pi}{4}} = 12e^{i\pi}e^{i\frac{\pi}{4}} = 12e^{-\frac{3i\pi}{4}}$,
$\overline{z} = 12e^{\frac{3i\pi}{4}} = 12(-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i) = -6\sqrt{2}+6i\sqrt{2}$,
$\frac{1}{z} = \frac{1}{12e^{-\frac{3i\pi}{4}}} = \frac{1}{12}e^{\frac{3i\pi}{4}} = -\frac{\sqrt{2}}{24}+\frac{\sqrt{2}}{24}i.$

Exercice 18 Soient p et $q \in \mathbb{R}$.

1. On a $\frac{p+q}{2}+\frac{p-q}{2} = \frac{p+q+p-q}{2} = \frac{2p}{2} = p$ et, de même, $q = \frac{q+p}{2}+\frac{q-p}{2}$.
2. D'où $e^{ip}+e^{iq} = e^{i(\frac{p+q}{2}+\frac{p-q}{2})}+e^{i(\frac{q+p}{2}+\frac{q-p}{2})} = e^{i\,\frac{p+q}{2}}\left(e^{i\,\frac{p-q}{2}}+e^{i\,\frac{q-p}{2}}\right)$
$e^{ip}+e^{iq} = e^{i\,\frac{p+q}{2}}\left(e^{i\,\frac{p-q}{2}}+e^{-i\,\frac{p-q}{2}}\right)$ $e^{ip}+e^{iq} = \left(e^{i\,\frac{p-q}{2}}+\overline{e^{i\,\frac{p-q}{2}}}\right)e^{i\,\frac{p+q}{2}}$
$= 2\mathfrak{Re}(e^{i\,\frac{p-q}{2}})e^{i\,\frac{p+q}{2}} = 2\cos(\frac{p-q}{2})e^{i\frac{p+q}{2}}.$
3. De même,
$e^{ip}-e^{iq} = \left(e^{i\,\frac{p-q}{2}}-\overline{e^{i\,\frac{p-q}{2}}}\right)e^{i\,\frac{p+q}{2}} = 2i\mathfrak{Im}(e^{i\,\frac{p-q}{2}})e^{i\,\frac{p+q}{2}} = 2i\sin(\frac{p-q}{2})e^{i\frac{p+q}{2}}.$
4. $\cos(p)+\cos(q) = \mathfrak{Re}(e^{ip}+e^{iq}) = \mathfrak{Re}(2\cos(\frac{p-q}{2})e^{i\frac{p+q}{2}}) = 2\cos(\frac{p-q}{2})\mathfrak{Re}(e^{i\frac{p+q}{2}})$
$= 2\cos(\frac{p-q}{2})\cos(\frac{p+q}{2})$,
$\sin(p)+\sin(q) = \mathfrak{Im}(e^{ip}+e^{iq}) = \mathfrak{Im}(2\cos(\frac{p-q}{2})e^{i\frac{p+q}{2}}) = 2\cos(\frac{p-q}{2})\mathfrak{Im}(e^{i\frac{p+q}{2}})$
$= 2\cos(\frac{p-q}{2})\sin(\frac{p+q}{2})$,
$\cos(p)-\cos(q) = \mathfrak{Re}(e^{ip}-e^{iq}) = \mathfrak{Re}(2i\sin(\frac{p-q}{2})e^{i\frac{p+q}{2}}) = 2\sin(\frac{p-q}{2})\mathfrak{Re}(ie^{i\frac{p+q}{2}})$
$= -2\sin(\frac{p-q}{2})\sin(\frac{p+q}{2})$,
$\sin(p)-\sin(q) = \mathfrak{Im}(e^{ip}-e^{iq}) = \mathfrak{Im}(2i\sin(\frac{p-q}{2})e^{i\frac{p+q}{2}}) = 2\sin(\frac{p-q}{2})\mathfrak{Im}(ie^{i\frac{p+q}{2}})$
$= 2\sin(\frac{p-q}{2})\cos(\frac{p+q}{2})$.
5. On a $\sin(2x)-\sin(6x) = 2\sin(\frac{2x-6x}{2})\cos(\frac{2x+6x}{2}) = 2\sin(-2x)\cos(4x)$
$\sin(2x)-\sin(6x) = -2\sin(2x)\cos(4x) = -4\sin(x)\cos(x)\cos(4x)$ et
$\mathscr{E}:\ \sin(2x)-\sin(6x) = 0 \iff \sin(x)=0$ ou $\cos(x)=0$ ou $\cos(4x)=0$
$\iff x\equiv 0\,[\pi]$ ou $x\equiv\frac{\pi}{2}\,[\pi]$ ou $4x\equiv\frac{\pi}{2}\,[\pi] \iff x\equiv 0\,[\frac{\pi}{2}]$ ou $x\equiv\frac{\pi}{8}\,[\frac{\pi}{4}]$:
$\mathscr{S} = \{-\frac{7\pi}{8};-\frac{5\pi}{8};-\frac{\pi}{2};-\frac{3\pi}{8};-\frac{\pi}{8};0;\frac{\pi}{8};\frac{3\pi}{8};\frac{\pi}{2};\frac{5\pi}{8};\frac{7\pi}{8};\pi\}$.

Exercice 19 On a $z = -\sqrt{3}+i = 2(-\frac{\sqrt{3}}{2}+i\frac{1}{2}) = 2(\cos(\frac{5\pi}{6})+\sin(\frac{5\pi}{6})) = 2e^{i\frac{5\pi}{6}}$
donc $z^n = 2^n e^{in\frac{5\pi}{6}} \in i\mathbb{R} \iff n\frac{5\pi}{6}\equiv\frac{\pi}{2}\,[\pi] \iff n\equiv\frac{\pi}{2}\frac{6}{5\pi}\,[\pi.\frac{6}{5\pi}]$
$\iff n\equiv\frac{3}{5}\,[\frac{6}{5}] \iff n = \frac{3}{5}+k\frac{6}{5},\ k\in\mathbb{N}$ et $5n = 3+6k$.
L'équation $5n-6k=3$ admet des solutions car 3 est un multiple du pgcd de 5 et 6 (qui vaut 1, ils sont premiers entre eux). On a $5\times 3-6\times 2 = 3$ donc $(n\,,\,k) = (3\,,\,2)$ est une solution particulière et si $(n\,,\,k)$ est une solution, on a $5n-6k = 3 = 5\times 3-6\times 2$ donc $5(n-3) = 6(k-2)$. Puisque 5 et 6 sont premiers entre eux, $6\,|\,(n-3)$ et $n-3 = 6p$ d'où $n = 3+6p$ (et $k = 2+5p$).
Les entiers naturels n tels que $z^n\in i\mathbb{R}$ sont donc $\{3,9,15,21,\dots\} = \{3+6p/p\in\mathbb{N}\}$.

CORRIGÉS

Exercice 20 Forme algébrique

$a = 3e^{i\frac{\pi}{6}}.e^{i\frac{5\pi}{3}} = 3e^{i(\frac{\pi}{6}+\frac{5\pi}{3})} = 3e^{i\frac{11\pi}{6}} = 3e^{-i\frac{\pi}{6}} = 3(\cos(-\frac{\pi}{6}) + \sin(-\frac{\pi}{6})) = 3(\frac{\sqrt{3}}{2} - i\frac{1}{2})$
$= \frac{3\sqrt{3}}{2} - \frac{3}{2}i.$

$b = \left(\sqrt{3}e^{-i\frac{5\pi}{2}}\right)^4 = \sqrt{3}^4 e^{-i4.\frac{5\pi}{2}} = 9e^{-10\pi i} = 9e^{0i} = 9 + 0i.$

$c = e^{-i\frac{2\pi}{3}} + e^{i\frac{3\pi}{4}} = \cos(-\frac{2\pi}{3}) + i\sin(-\frac{2\pi}{3}) + \cos(\frac{3\pi}{4}) + i\sin(\frac{3\pi}{4}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$
$= \frac{-1-\sqrt{2}}{2} + i\frac{\sqrt{2}-\sqrt{3}}{2}.$

$d = 4e^{-i\frac{4\pi}{3}} - 2e^{i\frac{\pi}{6}} = 4(\cos(-\frac{4\pi}{3}) + i\sin(\frac{2\pi}{3})) - 2(\cos(\frac{\pi}{6}) + i\sin(\frac{\pi}{6}))$
$= 4(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) - 2(\frac{\sqrt{3}}{2} + i\frac{1}{2}) = (-2 - \sqrt{3}) + i(2\sqrt{3} - 1).$

Exercice 21 $Z = 1 + i\sqrt{3} = \sqrt{1^2 + \sqrt{3}^2}(\frac{1}{\sqrt{4}} + \frac{\sqrt{3}}{\sqrt{4}}i) = 2(\frac{1}{2} + \frac{\sqrt{3}}{2}i)$
$Z = 2(\cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3})) = 2e^{i\frac{\pi}{3}}$ donc $Z' = (1 + i\sqrt{3})^5 = Z^5 = \left(2e^{i\frac{\pi}{3}}\right)^5$
$Z' = 32e^{i\frac{5\pi}{3}} = 32e^{-i\frac{\pi}{3}} = 32(\cos(-\frac{\pi}{3}) + i\sin(-\frac{\pi}{3})) = 32(\frac{1}{2} - i\frac{\sqrt{3}}{2}) = 16 - 16i\sqrt{3},$
$Z'' = (1+i\sqrt{3})^5 + (1-i\sqrt{3})^5 = Z^5 + \overline{Z}^5 = Z^5 + \overline{Z^5} = Z' + \overline{Z'} = 2\mathfrak{Re}(Z') = 2\times 16 = 32$
et $Z''' = (1 + i\sqrt{3})^5 - (1 - i\sqrt{3})^5 = Z^5 - \overline{Z}^5 = Z^5 - \overline{Z^5} = Z' - \overline{Z'} = 2i\mathfrak{Im}(Z')$
$Z''' = 2i(-16\sqrt{3}) = -32i\sqrt{3}.$

Exercice 22 On a $z_{\overrightarrow{AB}} = z_B - z_A = (2 + 5i) - (5 + 2i) = -3 + 3i$ de module $\sqrt{3^2 + 3^2} = 3\sqrt{2}$ donc $z_{\overrightarrow{AB}} = 3\sqrt{2}(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}) = 3\sqrt{2}(\cos(\frac{3\pi}{4}) + i\sin(\frac{3\pi}{4}))$
$z_{\overrightarrow{AB}} = 3\sqrt{2}e^{i\frac{3\pi}{4}}$ d'où $\left(\overrightarrow{u}\,;\overrightarrow{AB}\right) \equiv \frac{3\pi}{4}\,[2\pi].$

Exercice 23 On a $u_1 = \frac{1+i\sqrt{3}}{1-i} = \frac{2(\frac{1}{2}+i\frac{\sqrt{3}}{2})}{\sqrt{2}(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})} = \frac{2e^{i\frac{\pi}{3}}}{\sqrt{2}e^{-i\frac{\pi}{4}}} = \sqrt{2}e^{i(\frac{\pi}{3}+\frac{\pi}{4})} = \sqrt{2}e^{i\frac{7\pi}{12}}$
donc $u_n = \left(\frac{1+i\sqrt{3}}{1-i}\right)^n = u_1^n = (\sqrt{2}e^{i\frac{7\pi}{12}})^n = \sqrt{2}^n e^{i\frac{7n\pi}{12}} = \sqrt{2}^n(\cos(\frac{7n\pi}{12}) + i\sin(\frac{7n\pi}{12})).$

Exercice 24 VouF ?

(a) Si $z \in \mathbb{U}$, alors $\overline{z} = \frac{1}{z}$: Vrai car $|z| = 1$ donc $|z|^2 = z\overline{z} = 1$ donc $\overline{z} = \frac{1}{z}$.
Si $\overline{z} = \frac{1}{z}$ alors $z \in \mathbb{U}$: Vrai car
$\overline{z} = \frac{1}{z} \Longrightarrow |z|^2 = z\overline{z} = 1 \Longrightarrow |z| = 1 \Longrightarrow z \in \mathbb{U}.$

(b) Si $z = z'$ ou $z = -z'$ alors $|z| = |z'|$: Vrai car $|-z| = |z|$.
Si $|z| = |z'|$ alors $z = z'$ ou $z = -z'$: Faux. $|i| = |1| = 1$ par exemple.

(c) $\frac{z}{\overline{z}} = \frac{re^{i\theta}}{re^{-i\theta}} = e^{2i\theta} \in \mathbb{R} \iff 2\theta \equiv 0\,[\pi] \iff \theta \equiv 0\,[\frac{\pi}{2}]$
$\iff z \in \mathbb{R}$ ou $z \in i\mathbb{R}$. Vrai et réciproque.

Exercice 25 $z \neq 0$ et $z' = \frac{-2}{z}$.

1. On a $zz' = -2 = 2e^{i\pi}$ donc $|z|\,|z'| = 2$ i.e. $|z'| = \frac{2}{|z|}$ et $\arg(z) + \arg(z') \equiv \pi\,[2\pi]$.
2. (a) Si M décrit $\mathscr{D}^*$, $|z|$ décrit $]\,0\,;2\,]$ donc $|z'|$ décrit $\left[\,\frac{2}{2}\,;+\infty\,\right[= [\,1\,;+\infty\,[$ et $\arg(z) \in\,]-\pi\,;\pi\,]$ tout comme $\arg(z')$. Le point M' décrit donc l'extérieur du disque de centre O et de rayon 1.

(b) Si M décrit $]OA]$, $|z|$ décrit $]\,0\,;2\,]$ donc $|z'|$ décrit $[\,1\,;+\infty\,[$ et $\arg(z) \equiv \frac{\pi}{4}\,[2\pi]$ donc $\arg(z') \equiv \pi\frac{\pi}{4}\,[2\pi] \equiv \frac{3\pi}{4}\,[2\pi]$. M' décrit la demi-droite issue de $\left(-\frac{\sqrt{2}}{2}\,,\,\frac{\sqrt{2}}{2}\right)$ passant par $(\,-3\,,\,3\,)$.

Exercice 26 Nombres complexes de module 1

1. Soient z et $z' \in \mathbb{U}$. On a $|z| = |z'| = 1$ donc $|zz'| = |z|\,.\,|z'| = 1 \times 1 = 1 : zz' \in \mathbb{U}$. Puisque $|z'| = 1$, $z' \neq 0$ et $\frac{z}{z'}$ est définie. De plus, $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|} = \frac{1}{1} = 1 : \frac{z}{z'} \in \mathbb{U}$.

2. On a $z \in \mathbb{U} \iff |z| = 1 \iff |z|^2 = 1 \iff z\overline{z} = 1 \overset{z\neq 0}{\iff} \overline{z} = \frac{1}{z}$.

3. Soient a, b et $c \in \mathbb{U}$. On a $|a| = |b| = |c| = 1$ donc $a\overline{a} = b\overline{b} = c\overline{c} = 1$.
$$\begin{aligned}|ab+bc+ca|^2 &= \overline{(ab+bc+ca)}(ab+bc+ca) = (\overline{ab}+\overline{bc}+\overline{ca})(ab+bc+ca)\\ &= ab\overline{ab}+ab\overline{bc}+ab\overline{ca}+bc\overline{ab}+bc\overline{bc}+bc\overline{ca}+ca\overline{ab}+ca\overline{bc}+ca\overline{ca}\\ &= |ab|^2+|bc|^2+|ca|^2+ab\overline{b}\overline{c}+a\overline{a}b\overline{c}+b\overline{b}c\overline{a}+\overline{a}bc\overline{c}+ca\overline{a}\overline{b}+c\overline{c}a\overline{b}\\ &= 1^2+1^2+1^2+a\overline{c}+b\overline{c}+\overline{a}c+b\overline{a}+c\overline{b}+a\overline{b}\end{aligned}$$
De plus, $$\begin{aligned}|a+b+c|^2 &= \overline{(a+b+c)}(a+b+c) = (\overline{a}+\overline{b}+\overline{c})(a+b+c)\\ &= a\overline{a}+b\overline{b}+c\overline{c}+b\overline{a}+c\overline{a}+a\overline{b}+c\overline{b}+a\overline{c}+b\overline{c}\\ &= 1^2+1^2+1^2+b\overline{a}+c\overline{a}+a\overline{b}+c\overline{b}+a\overline{c}+b\overline{c}\end{aligned}$$
Donc $|ab+bc+ca|^2 = |a+b+c|^2$ et $|ab+bc+ca| = |a+b+c|$.

4. Soit $z \in \mathbb{U}$. On a $|z| = 1$ et
$$\begin{aligned}|1+z|^2+|1-z|^2 &= \overline{(1+z)}(1+z)+\overline{(1-z)}(1-z)\\ &= (1+\overline{z})(1+z)+(1-\overline{z})(1-z) = 1+z+\overline{z}+z\overline{z}+1-z-\overline{z}+z\overline{z}\\ &= 2+2z\overline{z} = 2+2\,|z|^2 = 2+2 = 4.\end{aligned}$$

Exercice 27 Soit $z = e^{i\theta} \in \mathbb{U}$.

1. On a $z+\dfrac{1}{z} = e^{i\theta}+\dfrac{1}{e^{i\theta}} = e^{i\theta}+e^{-i\theta} = e^{i\theta}+\overline{e^{i\theta}} = 2\mathfrak{Re}(e^{i\theta}) \in \mathbb{R}$.

2. On a $z^2-\dfrac{1}{z^2} = e^{2i\theta}-\dfrac{1}{e^{2i\theta}} = e^{2i\theta}-e^{-2i\theta} = e^{2i\theta}-\overline{e^{2i\theta}} = 2i\mathfrak{Im}(e^{2i\theta}) \in i\mathbb{R}$.

Exercice 28 Soit $z \neq 1$.

On a $z' \in i\mathbb{R} \iff \overline{z'} = -z' \iff \overline{\left(\frac{z+1}{z-1}\right)} = -\frac{z+1}{z-1} \iff \frac{\overline{z}+1}{\overline{z}-1} = \frac{z+1}{1-z}$
$\iff (\overline{z}+1)(1-z) = (z+1)(\overline{z}-1) \iff \overline{z}-z\overline{z}+1-z = z\overline{z}-z+\overline{z}-1$
$\iff 2z\overline{z} = 2 \iff |z|^2 = 1 \iff z \in \mathbb{U}\,(\backslash\{1\})$.

Exercice 29

1. (a) $$\begin{aligned}[\cos(x)+i\sin(x)]^3 &= [\cos(x)+i\sin(x)]^2 \times [\cos(x)+i\sin(x)]\\ &= \left[\cos^2(x)+2i\cos(x)\sin(x)-\sin^2(x)\right] \times [\cos(x)+i\sin(x)]\\ &= \cos^3(x)+3i\cos^2(x)\sin(x)-3\cos(x)\sin^2(x)-i\sin^3(x).\end{aligned}$$

   (b) À l'aide de la formule de Moivre, on a
   $$\cos(3x)+i\sin(3x) = [\cos(x)+i\sin(x)]^3.$$

   (c) D'après les questions précédentes, on a
   $$\cos(3x)+i\sin(3x) = \cos^3(x)-3\cos(x)\sin^2(x)+i\left[3\cos^2(x)\sin(x)-\sin^3(x)\right].$$
   Par identification des parties réelles et imaginaires, on obtient
   $$\cos(3x) = \cos^3(x)-3\cos(x)\sin^2(x) = \cos^3(x)-3\cos(x)\left[1-\cos^2(x)\right]$$

CORRIGÉS

donc $\cos(3x) = \cos^3(x) - 3\cos(x) + 3\cos^3(x) = 4\cos^3(x) - 3\cos(x)$,

$\sin(3x) = 3\cos^2(x)\sin(x) - \sin^3(x) = 3\left[1 - \sin^2(x)\right]\sin(x) - \sin^3(x)$

et donc $\sin(3x) = 3\sin(x) - 3\sin^3(x) - \sin^3(x) = -4\sin^3(x) + 3\sin(x)$.

2. (a) On a $\cos(x) = \frac{e^{ix}+e^{-ix}}{2}$. Donc

$$\cos^2(x) = \frac{\left[e^{ix}+e^{-ix}\right]^2}{2^2} = \frac{\left[e^{ix}\right]^2+2e^{ix}\times e^{-ix}+\left[e^{-ix}\right]^2}{4} = \frac{e^{2ix}+2+e^{-2ix}}{4}$$
$$= \frac{\frac{e^{2ix}+e^{-2ix}}{2}+1}{2} = \frac{\cos(2x)+1}{2}$$

(b) On a $\sin(x) = \frac{e^{ix}-e^{-ix}}{2}$. Donc

$$\sin^2(x) = \frac{\left[e^{ix}-e^{-ix}\right]^2}{2^2} = \frac{\left[e^{ix}\right]^2-2e^{ix}\times e^{-ix}+\left[e^{-ix}\right]^2}{4} = \frac{e^{2ix}-2+e^{-2ix}}{4}$$
$$= \frac{\frac{e^{2ix}+e^{-2ix}}{2}-1}{2} = \frac{\sin(2x)-1}{2}$$

(c) On a $\sin^3(x) = \frac{\left[e^{ix}-e^{-ix}\right]^3}{(2i)^3} = \frac{e^{3ix}-e^{ix}-2e^0e^{ix}+2e^0e^{-ix}+e^{-ix}-e^{-3ix}}{-8i}$

$$\sin^3(x) = \frac{e^{3ix}-e^{-3ix}+3e^{-ix}-3e^{ix}}{-8i} = \frac{\frac{e^{3ix}-e^{-3ix}}{2i}-3\times\frac{e^{ix}-e^{-ix}}{2i}}{-4}$$
$$= \frac{\sin(3x)-3\sin(x)}{-4} = \frac{-\sin(3x)+3\sin(x)}{4}$$

(d) On a $\cos^2(x)\sin(x) = \left[1-\sin^2(x)\right]\sin(x) = \sin(x) - \sin^3(x)$.

D'après la question précédente, $\cos^2(x)\sin(x) = \sin(x) - \frac{-\sin(3x)+3\sin x}{4}$

$$\cos^2(x)\sin(x) = \frac{4\sin(x)+\sin(3x)-3\sin x}{4} = \frac{\sin(x)+\sin(3x)}{4}$$

(e) On a $\cos^4(x) = \frac{\left(e^{ix}+e^{-ix}\right)^4}{16}$.

Or $\left(e^{ix}+e^{-ix}\right)^4 = \left(e^{ix}+e^{-ix}\right)^2 \times \left(e^{ix}+e^{-ix}\right)^2$

$\left(e^{ix}+e^{-ix}\right)^4 = \left(e^{4ix}+e^{-4ix}\right) + 4\left(e^{2ix}+e^{-2ix}\right) + 6$ et donc

$$\cos^4(x) = \frac{\left(e^{4ix}+e^{-4ix}\right)+4\left(e^{2ix}+e^{-2ix}\right)+6}{16} = \frac{1}{8}\times\frac{e^{4ix}+e^{-4ix}}{2}+\frac{1}{2}\times\frac{e^{2ix}+e^{-2ix}}{2}+\frac{3}{8}$$
$$= \frac{1}{8}\cos(4x) + \frac{1}{2}\cos(2x) + \frac{3}{8}.$$

(f) De même, on a $\sin^5(x) = \dfrac{\left(e^{ix}-e^{-ix}\right)^5}{32i}$

et $\left(e^{ix}-e^{-ix}\right)^5 = \left(e^{5ix}-e^{-5ix}\right) - 5\left(e^{3ix}-e^{-3ix}\right) + 10\left(e^{ix}-e^{-ix}\right)$

donc $\sin^5(x) = \frac{\left(e^{ix}-e^{-ix}\right)^5}{32i} = \frac{1}{16}\sin(5x) - \frac{5}{16}\sin(3x) + \frac{5}{8}\sin(x)$.

(g) On a d'une part, $\cos^2(x) = \frac{\cos(2x)+1}{2}$

et d'autre part, $\sin^3(x) = -\frac{\left(e^{ix}-e^{-ix}\right)^3}{8i} = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)$.

D'où, $\cos^2(x)\sin^3(x) = \frac{\cos(2x)+1}{2} \times \left(-\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)\right)$

$$\cos^2(x)\sin^3(x) = -\frac{1}{8}\sin(3x)\cos(2x) + \frac{3}{8}\sin(x)\cos(2x) - \frac{1}{8}\sin(3x) + \frac{3}{8}\sin(x).$$

(h) On a d'une part, $\sin^3(x) = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)$

et d'autre part, $\cos^3(x) = \left(\frac{e^{ix}+e^{-ix}}{2}\right)^3 = \frac{1}{4}\cos(3x) + \frac{3}{4}\cos(x)$.

D'où, $\cos^3(x) + 2\sin^3(x) = \frac{1}{4}\cos(3x) + \frac{3}{4}\cos(x) - \frac{1}{2}\sin(3x) + \frac{3}{2}\sin(x)$.

3. (a) Pour tout réel x, d'après les formules d'Euler, on a $\cos(2x) = \frac{e^{2ix}+e^{-2ix}}{2}$

donc $\cos(2x) = \frac{(e^{ix})^2+(e^{-ix})^2}{2} = \frac{[\cos(x)+i\sin(x)]^2+[\cos(-x)+i\sin(-x)]^2}{2}$

$$\cos(2x) = \frac{[\cos(x)+i\sin(x)]^2+[\cos(x)-i\sin(x)]^2}{2} = \frac{2\cos^2(x)-2\sin^2(x)}{2}$$

$= \cos^2(x) - \sin^2(x) = 2\cos^2 x - 1$ car $\cos^2(x) + \sin^2(x) = 1$.

(b) De même, $\sin(2x) = \frac{e^{2ix}-e^{-2ix}}{2i} = \frac{4i\cos(x)\sin(x)}{2i} = 2\cos(x)\sin(x)$.

4. • D'après les formules de duplication, on a $\cos(2x) = 2\cos^2(x) - 1$ donc $\cos^2(x) = \frac{\cos(2x)+1}{2}$ qui est une fonction continue sur $\mathbb{R}$. Ainsi,
$$I = \int_0^{\frac{\pi}{3}} \cos^2(x)\,\mathrm{d}x = \int_0^{\frac{\pi}{3}} \frac{\cos(2x)}{2} + \frac{1}{2}\,\mathrm{d}x = \left[\frac{\sin(2x)}{4} + \frac{1}{2}x\right]_0^{\frac{\pi}{3}} = \frac{3\sqrt{3}+4\pi}{24}.$$
• On a vu ci-dessus que $\sin^3(x) = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)$ qui est une fonction continue sur $\mathbb{R}$ donc
$$J = \int_0^{\frac{\pi}{3}} \sin^3(x)\,\mathrm{d}x = \int_0^{\frac{\pi}{3}} -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)\,\mathrm{d}x$$
$$= \left[\frac{1}{4}\frac{\cos(3x)}{3} - \frac{3}{4}\cos(x)\right]_0^{\frac{\pi}{3}} = \frac{1}{12}$$
• On a $\cos^2(x) = 1 - \sin^2(x)$ donc, pour tout $x \in \mathbb{R}$,
$\cos^2(x)\sin^3(x) = \sin^3(x) - \sin^5(x)$. On sait que
$\sin^3(x) = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)$
et $\sin^5(x) = \frac{1}{16}\sin(5x) - \frac{5}{16}\sin(3x) + \frac{5}{8}\sin(x)$
donc $\cos^2(x)\sin^3(x) = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x) - \frac{1}{16}\sin(5x) + \frac{5}{16}\sin(3x) - \frac{5}{8}\sin(x)$
$\cos^2(x)\sin^3(x) = -\frac{1}{16}\sin(5x) + \frac{1}{16}\sin(3x) + \frac{1}{8}\sin(x)$ et
$$K = \int_0^{\frac{\pi}{3}} \cos^2(x)\sin^3(x)\,\mathrm{d}x = \int_0^{\frac{\pi}{3}} -\frac{1}{16}\sin(5x) + \frac{1}{16}\sin(3x) + \frac{1}{8}\sin(x)\,\mathrm{d}x$$
$$= \left[\frac{1}{16}\frac{1}{5}\cos(5x) - \frac{1}{16}\frac{1}{3}\cos(3x) - \frac{1}{8}\cos(x)\right]_0^{\frac{\pi}{3}} = -\frac{31}{160}$$

Exercice 30 À tout complexe $z = a + ib$, on associe $\exp(z) = e^a.e^{ib}$.

1. Pour tous complexes z_1, z_2, on a
$$\begin{aligned}\exp(z_1 + z_2) &= \exp(a_1 + ib_1 + a_2 + ib_2) = \exp((a_1 + a_2) + i(b_1 + b_2))\\ &= e^{a_1+a_2}.e^{i(b_1+b_2)} = e^{a_1}.e^{ib_1}e^{a_2}.e^{ib_2}\\ &= \exp(a_1 + ib_1)\exp(a_2 + ib_2) = \exp(z_1).\exp(z_2).\end{aligned}$$
2. On a $\exp(2 + 3i) = e^2.e^{3i} = e^2\cos(3) + ie^2\sin(3)$.
3. On a $1 + i\sqrt{3} = 2(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = e^{\ln(2)}.e^{i\frac{\pi}{3}} = \exp(\ln(2) + i\frac{\pi}{3}) = \exp(z)$ pour $z = \ln(2) + i\frac{\pi}{3}$.
Le module d'un complexe est unique mais l'argument est défini modulo 2π donc les nombres complexes solutions de $\exp(z) = 1 + i\sqrt{3}$ sont de la forme
$\ln(2) + i(\frac{\pi}{3} + k.2\pi)$ où $k \in \mathbb{Z}$.

Exercice 31 Spirale : $\begin{cases} z_0 &= 1\\ z_{n+1} &= \left(1 + i\frac{\sqrt{3}}{3}\right) z_n.\end{cases}$

1. On a $|q|^2 = \left|1 + i\frac{\sqrt{3}}{3}\right|^2 = 1^2 + (\frac{\sqrt{3}}{3})^2 = 1 + \frac{3}{9} = \frac{4}{3}$ donc $|q| = \sqrt{\frac{4}{3}} = \frac{2}{\sqrt{3}}$
et $q = 1 + i\frac{\sqrt{3}}{3} = \frac{2}{\sqrt{3}}(\frac{\sqrt{3}}{2} \times 1 + \frac{\sqrt{3}}{2} \times i\frac{\sqrt{3}}{3}) = \frac{2}{\sqrt{3}}(\frac{\sqrt{3}}{2} + \frac{1}{2}i)$
$q = \frac{2}{\sqrt{3}}(\cos(\frac{\pi}{6}) + i\sin(\frac{\pi}{6})) = \frac{2}{\sqrt{3}}e^{i\frac{\pi}{6}}$
d'où $z_1 = qz_0 = q \times 1 = \frac{2}{\sqrt{3}}e^{i\frac{\pi}{6}}$ et $z_2 = qz_1 = q^2 = \left(\frac{2}{\sqrt{3}}\right)^2 e^{2i\frac{\pi}{6}} = \frac{4}{3}e^{i\frac{\pi}{3}}$.
2. Pour tout entier naturel n, posons $\mathscr{P}_n :\ z_n = \left(\frac{2}{\sqrt{3}}\right)^n e^{ni\frac{\pi}{6}}$.
   • On a $z_0 = 1 = 1 \times 1 = \left(\frac{2}{\sqrt{3}}\right)^0 e^{0.i\frac{\pi}{6}}$: $\mathscr{P}_0$ est vraie.

CORRIGÉS

- Supposons $\mathscr{P}_n$ vraie pour un certain $n \in \mathbb{N}$. On a
$z_{n+1} = \left(1 + i\frac{\sqrt{3}}{3}\right) z_n = qz_n = \frac{2}{\sqrt{3}} e^{i\frac{\pi}{6}} z_n = \frac{2}{\sqrt{3}} e^{i\frac{\pi}{6}} \left(\frac{2}{\sqrt{3}}\right)^n e^{ni\frac{\pi}{6}}$
$z_{n+1} = \left(\frac{2}{\sqrt{3}}\right)^{n+1} e^{(n+1)i\frac{\pi}{6}}$ et $\mathscr{P}_{n+1}$ est vraie.
- $\mathscr{P}_n$ est vraie pour tout entier naturel n.

Sinon, $z_{n+1} = qz_n$ donc (z_n) est géométrique (complexe) de raison $q \in \mathbb{C}$ et de premier terme $z_0 = 1$ donc $z_n = q^n$ pour tout $n \in \mathbb{N}$.

3. (a) On a $z_{n+1} - z_n = z_{M_{n+1}} - z_{M_n} = Z_{\overrightarrow{M_n M_{n+1}}}$
donc $d_n = |z_{n+1} - z_n| = \|\overrightarrow{M_n M_{n+1}}\| = M_n M_{n+1}$ est la distance entre les deux points M_n et M_{n+1}.

   (b) On a $d_0 = |z_1 - z_0| = |q - 1| = \left|1 + i\frac{\sqrt{3}}{3} - 1\right| = \left|i\frac{\sqrt{3}}{3}\right| = \frac{\sqrt{3}}{3}$.

   (c) Soit $n \in \mathbb{N}$. On a
$$z_{n+2} - z_{n+1} = qz_{n+1} - qz_n = q(z_{n+1} - z_n) = \left(1 + i\frac{\sqrt{3}}{3}\right)(z_{n+1} - z_n)$$

   (d) Ainsi, $d_{n+1} = |z_{n+2} - z_{n+1}| = |q(z_{n+1} - z_n)| = |q|\,|z_{n+1} - z_n| = \frac{2}{\sqrt{3}} d_n$: (d_n) est géométrique (réelle) de raison $\frac{2}{\sqrt{3}}$ et de premier terme $d_0 = \frac{\sqrt{3}}{3}$ donc, pout tout entier n, $d_n = \frac{\sqrt{3}}{3}\left(\frac{2}{\sqrt{3}}\right)^n$.

4. (a) $|z_{n+1}|^2 = |qz_n|^2 = |q|^2 |z_n|^2 = \frac{4}{3}|z_n|^2 = |z_n|^2 + \frac{1}{3}|z_n|^2 = |z_n|^2 + \frac{1}{3}\left((\frac{2}{\sqrt{3}})^n\right)^2$
$= |z_n|^2 + \left(\frac{\sqrt{3}}{3}\right)^2 \left((\frac{2}{\sqrt{3}})^n\right)^2 = |z_n|^2 + \left(\frac{\sqrt{3}}{3}(\frac{2}{\sqrt{3}})^n\right)^2 = |z_n|^2 + d_n^2$

   (b) Pour tout $n \in \mathbb{N}$, $|z_n| = |z_n - 0| = \left|Z_{\overrightarrow{OM_n}}\right| = OM_n$ et l'égalité précédente peut s'écrire $OM_{n+1}^2 = OM_n^2 + M_n M_{n+1}^2$: le triangle $OM_n M_{n+1}$ est donc rectangle en M_n.

5. Pour tout $n \in \mathbb{N}$, $\arg(z_n) = n\frac{\pi}{6}$ donc le point M_n est situé sur la demi-droite $\mathscr{D}'_n$ passant par l'origine et par le point d'affixe $e^{ni\frac{\pi}{6}}$. Ces demi-droites sont au nombre de douze. Supposons le point M_n placé. Puisque le triangle $OM_n M_{n+1}$ est rectangle en M_n, le point M_{n+1} est donc situé à l'intersection de la demi-droite $\mathscr{D}'_{n+1}$ et de la perpendiculaire à $\mathscr{D}'_n$ en M_n. Il suffit maintenant de placer $M_0(1)$ et d'appliquer cet algorithme.

Chapitre VI

PGCD ET APPLICATIONS

Sommaire

Deuxième chapitre d'arithmétique de l'année dans lequel de grands noms de mathématiciens apparaissent : Euclide, Gauss, Bézout, Diophante. L'arithmétique est une des plus anciennes disciplines des mathématiques et des savants exceptionnels s'y sont illustrés.

On rappelle quelques notations : $\mathbb{N}$ désigne l'ensemble des entiers naturels, $\mathbb{Z}$ celui des entiers relatifs, $[\![\, m\,;n\,]\!]$ est l'ensemble des entiers compris entre les entiers m et n, $D(a)$ est l'ensemble des diviseurs de a, $D\,(\,a\,,\,b\,) = D(a) \cap D(b)$ et $p|q$ signifie que p est un diviseur de q.
Nous traiterons souvent des cas de nullité des nombres entiers mais cela nous sera rarement nécessaire en pratique.

1 Plus Grand Commun Diviseur

1.1 Définitions et premières propriétés

Pour tout $a \in \mathbb{Z}^*$, on a toujours $1\,|\,a$, $a\,|\,a$ et si $p\,|\,a$, alors $|p| \leqslant |a|$.
En revanche, cette dernière propriété est fausse si $a = 0$ puisque tout entier divise 0.

Définition 1 ***PGCD***
Soient a et b deux entiers relatifs non simultanément nuls.
L'ensemble des diviseurs communs à a et b est une partie non vide et majorée de $\mathbb{Z}$ qui contient donc un plus grand élément appelé Plus Grand Commun Diviseur de a et b et noté $\mathrm{PGCD}(a, b)$ *(ou $a \wedge b$).*
Par commodité, on posera $\mathrm{PGCD}(0, 0) = 0$.

En effet, on a toujours $1 \in D(a, b) = D(a) \cap D(b)$
et $\forall p \in D(a, b)$, $p \leqslant |a|$ (et $|b|$).

Exemple : $D(9, 15) = D(9) \cap D(15) = \{-3; -1; 1; 3\}$ donc $\mathrm{PGCD}(9, 15) = 3$.

Propriété 1 *Soient a et b deux entiers relatifs. On a*

- $\mathrm{PGCD}(b, a) = \mathrm{PGCD}(a, b)$,
- $\mathrm{PGCD}(a, b) \leqslant |a|$ *si* $a \neq 0$,
- $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|)$,
- $\mathrm{PGCD}(1, a) = 1$,
- $\mathrm{PGCD}(0, a) = |a|$,
- $\mathrm{PGCD}(a, b) \geqslant 1$ *si* $ab \neq 0$,
- $a\,|\,b$ *ssi* $\mathrm{PGCD}(a, b) = |a|$,
- $\mathrm{PGCD}(a - b, b) = \mathrm{PGCD}(a, b)$.

Démonstration :

- $\mathrm{PGCD}(b, a) = \mathrm{PGCD}(a, b)$
  puisque $D(a, b) = D(a) \cap D(b) = D(b) \cap D(a) = D(b, a)$.
- $\mathrm{PGCD}(a, b) \leqslant |a|$ si $a \neq 0$ puisqu'alors, pour tout $p \in D(a)$, $p \leqslant |a|$.
- $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|)$ puisque $|c|$ et c ont les mêmes diviseurs.
- $\mathrm{PGCD}(1, a) = 1$ puisque $D(1) = \{\pm 1\}$ et $1\,|\,a$.
- $\mathrm{PGCD}(0, a) = |a|$ puisque $\mathrm{PGCD}(0, a) \leqslant |a|$ et $|a|$ divise a et 0.
- $\mathrm{PGCD}(a, b) \geqslant 1$ puisque $1\,|\,a$ et $1\,|\,b$ (sauf si $(a, b) = (0, 0)$ de PGCD nul).
- a divise b *ssi* $\mathrm{PGCD}(a, b) = |a|$: Si $\mathrm{PGCD}(a, b) = |a|$, $|a|$ divise b donc $a\,|\,b$.
  Réciproquement, si $a\,|\,b$ alors $|a|$ divise b et $|a| \leqslant \mathrm{PGCD}(a, b)$. Puisque $\mathrm{PGCD}(a, b) \leqslant |a|$, on a bien $\mathrm{PGCD}(a, b) = |a|$.
- *Méthode de la soustraction.* Notons $u = \mathrm{PGCD}(a - b, b)$ et $v = \mathrm{PGCD}(a, b)$.
  On a $u\,|\,a - b$ et $u\,|\,b$ donc $u\,|\,(a - b) + b = a$ et $u \leqslant \mathrm{PGCD}(a, b) = v$.
  De même, $v\,|\,a$ et $v\,|\,b$ donc $v\,|\,a - b$ et $v \leqslant \mathrm{PGCD}(a - b, b) = u$. $\square$

On se restreindra souvent à l'étude du PGCD pour des entiers positifs, leurs opposés ayant les mêmes diviseurs.

Exemple : $\mathrm{PGCD}(431, 439) = \mathrm{PGCD}(431 - 439, 439) = \mathrm{PGCD}(8, 439) = 1$ car 439 est impair.

1.2 Algorithme d'Euclide

On considère dans cette section deux entiers naturels non nuls a et b tels que $\boldsymbol{a > b}$ et l'on désigne par q le quotient et par r le reste de la division euclidienne de a par b : $\quad a = bq + r \quad$ avec $0 \leqslant r < b$.

Propriété 2 *Avec les notations précédentes, on a* $\quad \mathrm{PGCD}\,(a\,,\,b) = \mathrm{PGCD}\,(b\,,\,r)$.

Démonstration : Soit d un diviseur commun à a et b. On a $\quad a = bq + r \quad$ donc $r = a - bq$, $\quad$ combinaison linéaire entière de a et b donc r est divisible par d et d est un diviseur commun à b et r.
Réciproquement, si d est un diviseur commun à b et r, il divise la combinaison linéaire entière $bq + r$ et $d|a$.
Ainsi, les diviseurs de a et de b sont exactement ceux b et de r : $D\,(a\,,\,b) = D\,(b\,,\,r)$.
Ces ensembles donc le même plus grand élément : $\mathrm{PGCD}\,(a\,,\,b) = \mathrm{PGCD}\,(b\,,\,r)$. $\square$

Exemple : $552 = 60 \times 9 + 12$
donc $\mathrm{PGCD}\,(552\,,\,60) = \mathrm{PGCD}\,(60\,,\,12) = \mathrm{PGCD}\,(12 \times 5\,,\,12) = 12$.

Dans son livre VII des *Éléments*, Euclide décrit en l'an 300 av. J.-C. l'un des plus vieux algorithmes de l'histoire de l'Humanité. Il est vrai qu'il n'avait pas la touche *MATH*, option *NBRE* d'une calculatrice $\boxed{\text{TI}}$ mais cet artifice, bien qu'efficace, n'est pas pleinement satisfaisant pour les mathématiciens que nous sommes. Voici donc ce que nous a donné Euclide le grand.

Propriété 3 ***Algorithme d'Euclide***
On définit par récurrence la suite des entiers $r_0, r_1, \ldots, r_n$ par :
- *r_0 est le reste de la division euclidienne de a par b ;*

Si $r_0 = 0$, on pose $r_n = 0 \ \forall n \in \mathbb{N}$ et $\mathrm{PGCD}\,(a\,,\,b) = b$.
Sinon
- $\begin{cases} r_{n+1} = \text{ le reste de la division euclidienne de } r_{n-1} \text{ par } r_n \text{ si } r_n \neq 0 \ (r_{-1} = b) \\ r_{n+1} = 0 \text{ si } r_n = 0. \end{cases}$

Cette suite est alors nulle à partir d'un certain rang et la dernière valeur non nulle prise par cette suite est le PGCD *de a et b.*

Exemples : ◦ On a $\quad 1551 = 132 \times 11 + 99, \quad 132 = 99 \times 1 + 33, \quad 99 = 33 \times 3 + 0$ donc $\quad \mathrm{PGCD}\,(1551\,,\,132) = 33$. $\quad$ On a $\quad 1551 = 33 \times 47 \quad$ et $\quad 132 = 33 \times 4$.
◦ $450 = 198 \times 2 + 54, \quad 198 = 54 \times 3 + 36, \quad 54 = 36 \times 1 + 18 \quad 36 = 18 \times 2 + 0$ donc $\quad \mathrm{PGCD}\,(450\,,\,198) = 18$. $\quad$ On a $\quad 450 = 18 \times 25 \quad$ et $\quad 198 = 18 \times 11$.

Démonstration : On a $\quad 0 \leqslant r_0 < b \quad$ et $\quad \mathrm{PGCD}\,(a\,,\,b) = \mathrm{PGCD}\,(b\,,\,r_0) \quad$ d'après la propriété 2.
Si $r_0 = 0$, on a alors $\quad \mathrm{PGCD}\,(a\,,\,b) = \mathrm{PGCD}\,(b\,,\,0) = b \quad$ et l'on a obtenu ce que l'on voulait.
Si $r_0 \neq 0$ et $n \in \mathbb{N}$. Supposons que l'on a construit $r_0, r_1, \ldots, r_{n-1}$ non nuls et r_n tels que, pour tout $k \in [\![\, 1\,; n-1 \,]\!]$, $\quad r_{k+1}$ est le reste de la division euclidienne de r_{k-1} par r_k.
On a alors, par construction $\quad 0 \leqslant r_n < r_{n-1} < \ldots < r_{k+1} < r_k < \ldots < b$

et PGCD$(a, b) =$ PGCD$(b, r_0) = ... =$ PGCD$(r_k, r_{k-1}) = ...$ PGCD(r_{n-1}, r_n).
Si $r_n = 0$, alors $r_{n+1} = 0$ et PGCD$(r_{n-1}, r_n) =$ PGCD$(r_{n-1}, 0) = r_{n-1}$.
Si $r_n \neq 0$, alors le reste r_{n+1} de la division euclidienne de r_{n-1} par r_n vérifie $0 \leqslant r_{n+1} < r_n < \ldots < b$
et PGCD$(a, b) =$ PGCD$(r_{n-1}, r_n) =$ PGCD(r_n, r_{n+1}).
Par récurrence, on en déduit que (r_n) est une suite d'entiers naturels bien définie strictement décroissante jusqu'à son premier terme nul. Soit alors r_{n_0} ce premier terme. Il vérifie $r_{n_0} = 0$, $r_{n_0-1} > 0$
et PGCD$(a, b) =$ PGCD$(r_0, r_1) =$ PGCD(r_{n_0-1}, r_{n_0})
PGCD$(a, b) =$ PGCD$(r_{n_0-1}, 0) = r_{n_0-1}$. □

1.3 Corollaires de l'algorithme d'Euclide

Propriété 4 *Soient a, b et k trois entiers naturels.*
On a PGCD$(ka, kb) = k \times$ PGCD(a, b).

Démonstration : Si $\alpha = \beta q + r$ avec $0 \leqslant r < \beta$, $k\alpha = k(\beta q + r) = k\beta q + kr$ avec $0 \leqslant kr < k\beta$ donc $(k\beta)q + kr$ est bien la division euclidienne de $k\alpha$ par $k\beta$ et son reste est kr. Ainsi, dans l'algorithme d'Euclide associé à ka et kb, la suite des restes (r'_n) est celle des restes multipliés par k de l'algorithme d'Euclide associé à a et b : $r'_n = k.r_n$. Le dernier reste non nul, $r'_{n_0-1} =$ PGCD(ka, kb), est donc $k.r_{n_0-1}$, le PGCD(a, b) multiplié par k. □

Remarque : Si a, b et k sont relatifs, on a facilement
PGCD$(ka, kb) = |k| \times$ PGCD$(|a|, |b|)$.

Exemple : PGCD$(210, 462) =$ PGCD$(2.3.7 \times 5, 2.3.7 \times 11)$
PGCD$(210, 462) = 2.3.7 \times$ PGCD$(5, 11) = 42 \times 1 = 42$.

Propriété 5 *Soient a et b deux entiers non simultanément nuls.*
d est un diviseur commun à a et b ssi d divise PGCD(a, b).

Démonstration : Soient a et $b \in \mathbb{Z}$ non simultanément nuls et soit $d \in D(a, b)$. Montrons par récurrence que d divise tous les termes de la suite des restes de l'algorithme d'Euclide associé à a et b.
On a $a = bq + r$ et, par hypothèse, $d|a$ et $d|b$ donc $d|bq$ et $d|r = a - bq = r_0$.
Supposons que $d|r_k$ pour tout $k \in [\![0 ; n]\!]$. On a $r_{n-1} = r_n q_{n+1} + r_{n+1}$ donc $r_{n+1} = r_{n-1} - r_n q_{n+1}$ qui est divisible par d par combinaison linéaire entière de deux entiers divisibles par d.
Ainsi, $d|r_n$ pour tout $n \in \mathbb{N}$. En particulier, $d|r_{n_0-1} =$ PGCD(a, b).
Réciproquement, si $d|$ PGCD(a, b), alors d divise tous les multiples de PGCD(a, b), en particulier a et b puisque PGCD(a, b) divise a et b. □

Exemple : Puisque $14|42 =$ PGCD$(210, 462)$, on a $14|210$ et $14|462$.
Puisque $22 \nmid 42$, on a $22 \nmid 210$ ou $22 \nmid 462$ c.-à-d. $22 \notin D(210, 462)$.
Attention, il divise toutefois l'un, 462 (mais pas l'autre, 210).

Propriété 6 *Soient a et b deux entiers non simultanément nuls. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de* $\text{PGCD}(a, b)$ *:*
$D(a, b) = D(\text{PGCD}(a, b))$.

Démonstration : Ceci n'est qu'une simple réécriture de la propriété précédente. □

Exemples : ◦ $D(210, 462) = D(\text{PGCD}(210, 462)) = D(42) = D(2.3.7)$
$D(210, 462) = \pm\{1; 2; 3; 6; 7; 14; 21; 42\}$.
◦ Cherchons les entiers naturels n inférieurs à 450 tels que $\text{PGCD}(n, 270) = 45$.
On a $45|n$ donc il existe $m \in \mathbb{N}$ tel que $n = 45m$. Puisque $n \leqslant 450$, $m \leqslant 10$.
De plus, $45 = \text{PGCD}(n, 270) = \text{PGCD}(45m, 45 \times 6) = 45 \times \text{PGCD}(m, 6)$ donc $\text{PGCD}(m, 6) = 1$ et $m \in \{1; 5; 7\}$. Puisque
$\text{PGCD}(1 \times 45, 6 \times 45) = \text{PGCD}(5 \times 45, 6 \times 45) = \text{PGCD}(7 \times 45, 6 \times 45) = 45$, les entiers recherchés sont bien 45, 225 et 315.

2 Nombres premiers entre eux

2.1 Définition et premières propriétés

Définition 2 *Deux entiers relatifs non nuls a et b sont dits* ***premiers entre eux****, ou* ***copremiers****, lorsque leurs seuls diviseurs communs sont -1 et 1 c.-à-d. lorsque* $\text{PGCD}(a, b) = 1$.
On dira aussi que a est premier avec b et que b est premier avec a.

Exemples : ◦ 18 et 35 sont premiers entre eux car $D(18) = \pm\{1; 2; 3; 6; 9; 18\}$ et $D(35) = \pm\{1; 5; 7; 35\}$ donc $\text{PGCD}(18, 35) = 1$.
◦ 42 et 63 ne sont pas premiers entre eux car $7|42$ et $7\big|63$ donc $\text{PGCD}(42, 63) \geqslant 7 > 1$.

Remarque : Si p et q sont deux nombres premiers distincts (cf. chap.IX p.219), alors p et q sont trivialement premiers entre eux.

Reprenons alors une définition bien connue et très utile. En effet, le comble pour un irréductible mathématicien n'est-il pas se faire piquer sa moitié par un tiers dans un car ?

Définition 3 *Soient a un entier relatif et b un entier relatif non nul.*
On dit que la fraction $\frac{a}{b}$ est irréductible si les entiers a et b sont premiers entre eux.

Exemples : $\frac{18}{35}$ est irréductible car $\text{PGCD}(18, 35) = 1$ et $\frac{1551}{132}$ n'est pas irréductible car $\text{PGCD}(1551, 132) = 33 \neq 1$.

Propriété 7 *Soient a et b deux entiers relatifs non nuls.*
Si a' et b' sont les entiers tels que $a = a'.\text{PGCD}(a, b)$ et $b = b'.\text{PGCD}(a, b)$, alors a' et b' sont premiers entre eux.
Réciproquement, s'il existe deux entiers relatifs premiers entre eux a' et b' et un entier naturel d tels que $a = a'd$ et $b = b'd$, alors $d = \text{PGCD}(a, b)$.

Démonstration : Soient $d = \text{PGCD}(a, b)$, $d' = \text{PGCD}(a', b')$ et k_1, k_2 tels que $a' = k_1 d'$, $b' = k_2 d'$. Montrons que $d' = 1$.
On a $a = a'd = k_1(dd')$ et $b = b'd = k_2(dd')$ donc dd' est un diviseur commun à a et b et $dd' \leqslant \text{PGCD}(a, b) = d$. Puisque $d > 0$, on a $d' = 1$ et les entiers a' et b' sont premiers entre eux.
Réciproquement, $\text{PGCD}(a, b) = \text{PGCD}(a'd, b'd) = d.\text{PGCD}(a', b') = d.1 = d$ car a' et b' sont premiers entre eux. □

Exemples : ◦ $\text{PGCD}(210, 462) = 42$ et l'on a bien $\frac{210}{42} = 5$ et $\frac{462}{42} = 11$ premiers entre eux.

◦ On a $42 = 7 \times 6$ et $63 = 7 \times 9$. Puisque $\text{PGCD}(6, 9) = 3 \neq 1$, $\text{PGCD}(42, 63) \neq 7$.

◦ On a $42 = 21 \times 2$ et $63 = 21 \times 3$. Puisque $\text{PGCD}(2, 3) = 1$, $\text{PGCD}(42, 63) = 21$.

2.2 Théorème de Bézout

Voici un fameux théorème d'existence (mais pas d'unicité). Il porte le nom d'Étienne Bézout, mathématicien français du XVIII$^{\text{e}}$ s. qui a généralisé un résultat déjà démontré un siècle auparavant.

Théorème 1 ***Théorème de Bézout*** *Soient a et b deux entiers relatifs non nuls.*
a et b sont premiers entre eux
ssi il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Démonstration : On pose $d = \text{PGCD}(a, b)$ et l'on considère des entiers u et v tels que $au + bv = 1$. On sait que $d|a$ et $d|b$ donc, par combinaison linéaire entière, d divise $au + bv = 1$ d'où $d = 1$: a et b sont premiers entre eux.
Réciproquement, supposons que $\text{PGCD}(a, b) = 1$. On désigne par E l'ensemble des entiers strictement positifs qui peuvent s'écrire sous la forme $au + bv$.
E n'est pas une partie vide de $\mathbb{N}^*$ puisque $|a + b| \in E$: en effet, $|a + b| = a + b$ ou $|a + b| = -(a + b) = -a - b$ et $|a + b| > 0$ car $a \neq -b$ (a, b premiers entre eux).
Étant non vide, E admet un plus petit élément que l'on note $c \in \mathbb{N}^*$, élément pour lequel il existe deux entiers relatifs u et v tels que $c = au + bv$.
Supposons $a > 0$. On a $c \leqslant a$ car $a = 1a + 0b \in E$. La division euclidienne de a par c donne alors $a = cq + r$ donc $a = (au + bv)q + r$ et $r = a(1 - qu) - bvq = aU + bV$. Si maintenant $r > 0$, alors $r \in E$ et $r \geqslant c$, plus petit élément de E, ce qui est contradictoire avec la définition de r en tant que reste d'une division euclidienne par c : $0 \leqslant r < c$. Donc $r = 0$ et $a = cq$: $c|a$. Si $a < 0$, on a $-a = -1a + 0b \in E$ et $c \leqslant -a$: on divise alors $-a$ par c et on obtient de même $c| - a$ d'où $c|a$.
En divisant b par c, on obtient de même, $c|b$ et c est un diviseur commun à a et b.
Puisque $c > 0$ et $\text{PGCD}(a, b) = 1$, on a $c = 1 \in E$. Ainsi, il existe u et v relatifs tels que $au + bv = 1$. □

Remarques : • Si l'on a $ua + vb = 1$ (avec u et v non nuls), alors u et v sont aussi premiers entre eux, tout comme a et v ainsi que u et b.

Par exemple, on a $7 \times 3 - 5 \times 4 = 1$ donc $(7;5)$, $(7;4)$, $(3;5)$ et $(3;4)$ sont des couples d'entiers premiers entre eux.

- Deux entiers consécutifs sont toujours premiers entre eux.

En effet, $1 \times (n+1) - 1 \times n = 1$.

Ce théorème donne une condition d'existence mais ne donne pas de méthode de détermination des entiers u et v. Traitons un exemple pour voir comment l'on peut procéder.

Exemple : 29 est un nombre premier et 26 n'est pas multiple de 29 donc 29 et 26 sont premiers entre eux. Cherchons les entiers relatifs u et v tels que $29u + 26v = 1$ en appliquant l'algorithme d'Euclide :
$(E_1)\colon 29 = 1 \times 26 + 3$, $(E_2)\colon 26 = 3 \times 8 + 2$ et $(E_3)\colon 3 = 2 \times 1 + 1$.
D'après (E_3), $1 = 3 - 2 \times 1$ et d'après (E_2), $2 = 26 - 3 \times 8$
donc $1 = 3 - (26 - 8 \times 3) \times 1 = 3 \times 9 - 26 \times 1$. D'après (E_1), $3 = 29 - 1 \times 26$
donc $1 = (29 - 1 \times 26) \times 9 - 26 \times 1 = 9 \times 29 - 9 \times 26 - 1 \times 26 = 9 \times 29 - 10 \times 26$
et l'on a obtenu $u = 9$ et $v = -10$ (qui sont premiers entre eux).
Il s'avère que $-17 \times 29 + 19 \times 26 = 1$ aussi, tout comme $35 \times 29 - 39 \times 26 = 1$ et l'on voit que le couple de premiers entre eux (u, v) est loin d'être unique.
La méthode mis en œuvre ici consiste à appliquer l'algorithme d'Euclide afin de connaître la suite des restes successifs puis de le remonter en exprimant ces restes en fonction des restes précédents.

Nous pouvons enfin donner un critère d'inversibilité modulaire.

Propriété 8 *Soient m un entier relatif et n un entier relatif non nul.*
m est inversible modulo n si, et seulement si, m et n sont premiers entre eux.

Démonstration : $\exists x \in \mathbb{Z},\ mx \equiv 1\,[n] \iff \exists (x, y) \in \mathbb{Z}^2,\ mx = 1 + ny$
$\iff \exists (x, y) \in \mathbb{Z}^2,\ mx + n(-y) = 1$
$\iff \mathrm{PGCD}(m, n) = 1$ d'après le théorème de Bézout. □

Exemple : On cherche un éventuel inverse de 30 modulo 23 c.-à-d. un entier n tel que $30n \equiv 1\,[23]$.
Puisque $\mathrm{PGCD}(30, 23) = 1$, il existe n et p tels que $30n + 23p = 1$ c.-à-d. $30n = 1 - 23p \equiv 1\,[23]$: 30 admet donc bien un inverse modulo 23. L'algorithme d'Euclide donne $30 = 23 \times 1 + 7$, $23 = 7 \times 3 + 2$, $7 = 2 \times 3 + 1$ et sa remontée permet d'écrire

$$1 = 7 - 2 \times 3 = 7 - (23 - 7 \times 3) \times 3 = 10 \times 7 - 23 \times 3 = 10(30 - 23) - 23 \times 3$$
$$1 = 30 \times 10 - 23 \times 13.$$

On en déduit que $(10; -13)$ est un couple solution de l'équation $30n + 23p = 1$ et que $n = 10$ est un inverse de 30 modulo 23 : $30 \times 10 = 1 + 23 \times 13 \equiv 1\,[23]$.
On obtient aussi $23 \times 13 \equiv 1\,[30]$.

2.3 Généralisation et équations diophantiennes

Théorème 2 ***Bézout généralisé***
Pour tous entiers relatifs a et b, il existe deux entiers relatifs u et v tels que
$au + bv = \text{PGCD}\,(a\,,\,b)$.
Réciproquement, s'il existe deux entiers relatifs tels que $au + bv = d$ où d divise a et b, alors $|d| = \text{PGCD}\,(a\,,\,b)$.

Démonstration : Traitons premièrement les cas de nullité.
Si $a = 0$, on a $0 \times 5 + b \times 1 = b = \text{PGCD}\,(0\,,\,b)$.
Si $au + bv = d = 0$ divise a et b, alors $a = b = 0$ et $\text{PGCD}\,(0\,,\,0) = 0 = d$.
Supposons maintenant a et b non nuls et posons $d = \text{PGCD}\,(a\,,\,b) \geqslant 1$. D'après la propriété 7, il existe a' et b' premiers entre eux tels que $a = a'd$ et $b = b'd$. D'après le théorème de Bézout, il existe u et v tels que $a'u + b'v = 1$. On en déduit que $d(a'u + b'v) = d$ et $(da')u + (db')v = d$ c.-à-d. $au + bv = d$.
Réciproquement, on suppose que d est un diviseur de a et de b et qu'il existe u et v tels que $au + bv = d$.
Si d' est un diviseur de a et de b, alors d' divise $au + bv$ donc $d' \,|\, d$: $|d|$ est donc bien le plus grand diviseur commun à a et b. □

Exemples : ◦ $\text{PGCD}\,(210\,,\,462) = 42$ et l'on a $1 \times 462 + (-2) \times 210 = 42$.
◦ $5 \times 72 - 4 \times 88 = 8$ et 8 divise 72 et 88 donc $\text{PGCD}\,(72\,,\,88) = 8$.
◦ On a $3 \times 12 - 2 \times 15 = 6$ mais 6 ne divise pas 15 donc on ne peut conclure sur le PGCD de 12 et 15.

Pour déterminer des entiers u et v, on peut se ramener au théorème de Bézout en divisant l'équation par le PGCD puis appliquer la méthode de remontée de l'algorithme d'Euclide.

Exemple : $\text{PGCD}\,(84\,,\,18) = 6$ donc il existe u et $v \in \mathbb{Z}$ tels que $84u + 18v = 6$.
En divisant par le PGCD, on se ramène à $14u + 3v = 1$.
Puisque $1 = 3 - (14 - 3 \times 4) = -14 \times 1 + 3 \times 5$, une solution de cette dernière est le couple $(-1\,,\,5)$ et l'on a alors $84 \times (-1) + 18 \times 5 = 6$.

Un équation à coefficients entiers dont on cherche des solutions entières (ou rationnelles) est appelée *équation diophantienne*, du nom du mathématicien grec Diophante d'Alexandrie (IIᵉ s. - IIIᵉ s. ap. J.-C.), parfois surnommé le « père de l'algèbre ».

Théorème 3 ***Équation diophantienne***
Soient a, b et c trois entiers relatifs tels que a et b ne sont pas simultanément nuls. L'équation diophantienne $ax + by = c$ admet des couples d'entiers $(x\,,\,y)$ solutions si, et seulement si, l'entier c est un multiple de $\text{PGCD}\,(a\,,\,b)$.

Démonstration : Supposons que l'équation $ax + by = c$ admette des solutions entières et l'on pose $d = \text{PGCD}\,(a\,,\,b)$. On sait qu'il existe des entiers a' et b' premiers entre eux tels que $a = a'd$ et $b = b'd$.
Ainsi, $c = a'dx + b'dy = d(a'x + b'y)$ et c est un multiple de d.
Réciproquement, si $a = 0$, l'équation $ax + by = c$ devient $c = yb$ qui n'admet des

solutions que si c est un multiple de $b = \text{PGCD}(0, b)$.
Si $a \neq 0$, $b \neq 0$ et c multiple de $d = \text{PGCD}(a, b)$, alors il existe des entiers u, v et c' tels que $au + bv = d$ et $c = c'd$. Ainsi, $c'(au + bv) = c'd$ c.-à-d. $a(c'u) + b(c'v) = c$: l'équation $ax + by = c$ admet donc des solutions entières. □

Exemples : ◦ Puisque $\text{PGCD}(42, 63) = 21$ et $21|147$, il existe des entiers x et y tels que $42x + 63y = 147$. Le couple $(2; 1)$ par exemple vérifie $42 \times 2 + 63 \times 1 = 147$.

◦ L'équation $16x + 12y = 7$ n'admet pas de solutions entières car 7 n'est pas un multiple de $4 = \text{PGCD}(16, 12)$.

◦ $(E)\colon 32u + 24v = 16$. On a $\text{PGCD}(32, 24) = 8$. Puisque $8|16$, (E) admet des solutions entières et l'on a $(E) \overset{\times\frac{1}{8}}{\Longleftrightarrow} (E')\colon 4u + 3v = 2$. Résolvons trivialement $(E_1)\colon 4u_1 + 3v_1 = 1$: $(u_1, v_1) = (1, -1)$ est une solution de (E_1) donc $4 \times 1 + 3 \times (-1) = 1$ et $4(2 \times 1) + 3(2 \times (-1)) = 2 \times 1$: le couple $(u, v) = (2, -2)$ est une solution de (E') donc de (E).
La démarche consiste à diviser l'équation par le PGCD, résoudre l'équation de Bézout puis multiplier les solutions pour obtenir le bon multiple du PGCD.

Nous avons alors un critère de résolution des congruences linéaires.

Propriété 9 *Soient a et b deux entiers relatifs, n un entier naturel non nul. L'équation modulaire $ax \equiv b\,[n]$ admet des solutions ssi b est un multiple de* $\text{PGCD}(a, n)$.

Démonstration : $\exists x \in \mathbb{Z},\ ax \equiv b\,[n] \iff \exists (x, y) \in \mathbb{Z},\ ax = b + ny$
$\iff \exists (x, y) \in \mathbb{Z},\ ax + n(-y) = b$
$\iff \text{PGCD}(a, n)\,|b$ d'après le théorème 3. □

Exemple : $(E_m)\colon 32x \equiv 16\,[24]$ admet des solutions entières puisque $\text{PGCD}(32, 24) = 8|16$.
On a vu ci-dessus que $32 \times 2 + 24 \times (-2) = 16$ donc $x = 2$ est une solution de (E_m).

3 Théorème de Gauss et applications

Johann Carl Friedrich Gauss est un immense scientifique allemand de la première moitié du XIXᵉ s. Considéré comme l'un des plus grands mathématiciens de tous les temps, son nom ne vous est certainement pas inconnu : il a été évoqué dans de nombreux chapitres au cours de vos études.

Théorème 4 ***Théorème de Gauss***
Soient a, b et c trois entiers relatifs.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c :
$a|bc$ et $\text{PGCD}(a, b) = 1 \Longrightarrow a|c$.

Démonstration : Puisque $a|bc$, il existe un relatif w tel que $bc = aw$. Puisque $\text{PGCD}(a, b) = 1$, le théorème de Bézout permet d'affirmer qu'il existe des relatifs u et v tels que $1 = ua + vb$.

Ainsi, $c = c \times 1 = cua + cvb = auc + (bc)v = auc + awv = a(uc + wv)$: c est un multiple de a. □

Remarque : La condition a et b premiers entre eux est essentielle. En effet, $4|12 = 2\times 6$ mais 4 ne divise ni 2 ni 6 (qui ne sont pas premiers entre eux).

Exemples : ◦ Si n est un diviseur impair de $150 = 75 \times 2$, alors n et 2 sont premiers entre eux et n divise 75.

◦ Résolvons l'équation (E_1): $65x = 91y$. Grâce à l'algorithme d'Euclide, on montre que $\text{PGCD}(65, 91) = 13$. En divisant (E_1) par 13, on obtient $5x = 7y$. On a $\text{PGCD}(5, 7) = 1$. Puisque $7|5x$, on a $7|x$ et $x = 7k$, $k \in \mathbb{Z}$. L'équation s'écrit alors $5 \times 7k = 7y$ donc $y = 5k$.
Réciproquement, si $x = 7k$ et $y = 5k$,
alors $65x = 13 \times 5 \times x = 13 \times 5 \times 7k = 13 \times 7 \times 5k = 13 \times 7 \times y = 91y$.
L'ensemble des solutions de (E_1) est donc $\{(7k; 5k)/k \in \mathbb{Z}\}$.

◦ On a vu précédemment que l'équation (E_2): $32u+24v = 16 \iff 4u+3v = 2$ admet le couple $(u_0, v_0) = (2, -2)$ pour solution particulière : $4(2) + 3(-2) = 2$. Ainsi, pour tout couple (u, v) solution de (E_2), on a

$(4u + 3v) - (4(2) + 3(-2)) = 2 - 2 = 0 \iff 4(u - 2) + 3(v + 2) = 0$

$\iff 4(u-2) = -3(v+2)$. Puisque 4 est premier avec 3, le théorème de Gauss affirme que 4 divise $v+2$ et $v = -2 + 4k$ pour $k \in \mathbb{Z}$. D'où $4(u-2) = -3(4k)$ et $u = 2 - 3k$.
Réciproquement, si $u = 2 - 3k$ et $v = -2 + 4k$,
alors $32u + 24v = 32(2 - 3k) + 24(-2 + 4k) = 64 - 96k - 48 + 96k = 16$ et (u, v) est solution de (E).
L'ensemble des solutions de (E_2) est donc $\{(2 - 3k; -2 + 4k)/k \in \mathbb{Z}\}$.
On trouvera en fin de chapitre un paragraphe donnant le schéma de résolution des équations diophantiennes.

Propriété 10 *Soient a, b et c trois entiers relatifs.*
Si b et c sont premiers entre eux et divisent tous les deux a, alors bc divise a :

$$\text{PGCD}(b, c) = 1, \quad b|a \quad \text{et} \quad c|a \quad \Longrightarrow \quad bc|a.$$

Démonstration : Si $a = 0$, bc divise a. Si $a \neq 0$ et b, c deux diviseurs de a premiers entre eux. Il existe b' et c' tels que $a = bb'$ et $a = cc'$. Donc $bb' = cc'$ et $b|cc'$. Puisque b et c sont premiers entre eux, le théorème de Gauss permet d'affirmer que b divise c' et $c' = mb$. Ainsi, $a = cc' = cmb$ et bc divise a. □

Remarque : La condition b et c premiers entre eux est essentielle. En effet, $4|12$ et $6|12$ mais $4 \times 6 = 24$ ne divise pas 12.

Exemples : ◦ $\text{PGCD}(4, 15) = 1$, $4|120$ et $15|120$ donc $4\times 15 = 60|120$.

◦ $15|30$, $6|30$ mais $15 \times 6 = 90 \nmid 30$ donc $\text{PGCD}(15, 6) \neq 1$.

◦ Pour $n \in \mathbb{N}$, on pose $N = n(n + 1)(n + 2)$. Trivialement, 2 divise $n(n + 1)$ puisque l'un d'entre eux est pair. De même, 3 divise $n(n + 1)(n + 2)$ puisque l'un d'entre eux est dans la table de trois.
Comme $\text{PGCD}(2, 3) = 1$, $2 \times 3 = 6$ divise N.

Propriété 11 *Soient a, b et c trois entiers relatifs.*
a est premier avec b et avec c si, et seulement si, a est premier avec le produit bc : $\text{PGCD}(a, b) = 1$ *et* $\text{PGCD}(a, c) = 1 \iff \text{PGCD}(a, bc) = 1.$

Démonstration : Si a est premier avec bc, on pose $b' = \text{PGCD}(a, b)$. On a $b' \big| b$ donc $b' \big| bc$ et puisque b' divise aussi a, on a $b' = 1$. De même pour c.
Réciproquement, si a est premier avec b et c, on pose $d = \text{PGCD}(a, bc)$.
On a $bc = md$ et $a = nd$ avec $\text{PGCD}(m, n) = 1$.
On a $\text{PGCD}(d, b) \leqslant \text{PGCD}(nd, b) = \text{PGCD}(a, b) = 1$ car les diviseurs de d sont des diviseurs de nd. D'où $\text{PGCD}(d, b) = 1$. Ainsi, d est premier avec b et divise bc. Le théorème de Gauss affirme que d divise c. Or d divise aussi a. Puisque a et c sont premiers entre eux, $d = 1$. □

Exemples : ◦ 7 est premier avec 11 et avec 25 donc 7 est premier avec 275.
◦ 13 n'est pas premier avec 39 donc 13 n'est pas premier avec $195 = 39 \times 5$.

Voici un corollaire immédiat ($c = b$) et néanmoins utile.

Propriété 12 *Soient a et b deux entiers relatifs et n un entier naturel.*
a est premier avec b si, et seulement si, a est premier avec b^n.
$\text{PGCD}(a, b) = 1 \iff \text{PGCD}(a, b^n) = 1.$

La propriété 11 ainsi que la propriété 8 de la page 137 mènent au critère de double inversibilité suivant.

Propriété 13 *Soient a un entier relatif, m et n deux entiers naturels non nuls.*
a est inversible modulo mn si, et seulement si, a est inversible modulo m et inversible modulo n.

Exemple : On a vu que $30 \times 10 = 1 + 13 \times 23 \equiv 1\,[23]$.
De manière similaire, $30 \times 4 = 1 + 17 \times 7 \equiv 1\,[7]$.
Ainsi, 30 est inversible modulo 23 et 7 donc 30 est inversible modulo $23 \times 7 = 161$.
En effet, $30 \times 102 = 1 + 19 \times 161 \equiv 1\,[161]$.

Schéma de résolution des équations diophantiennes

Soit l'équation diophantienne $(E)\colon ax + by = c$ d'inconnues x et y.

- On commence par calculer $\boldsymbol{a \wedge b}$.
- Si $a \wedge b$ ne divise pas c, (E) n'admet pas de solutions entières.
- Si $\boldsymbol{a \wedge b | c}$, alors on divise (E) par $a \wedge b$ et l'on se ramène à l'équation diophantienne équivalente $(E')\colon a'x + b'y = c'$ où $a' \wedge b' = 1$.
- On cherche ensuite une solution particulière $\boldsymbol{(x_0\,,\,y_0)}$ de l'équation $(E_1)\colon a'x + b'y = 1$ en remontant l'algorithme d'Euclide.
- On multiplie cette solution par c' afin d'obtenir une solution particulière $\boldsymbol{(x_1\,,\,y_1)} = (c'x_0\,,\,c'y_0)$ de l'équation (E') et donc de (E).

- On justifie que, si (x, y) est solution de (E'), alors $(x - x_1, y - y_1)$ vérifie $a'X + b'Y = c' - c' = 0$ et donc $a'X = -b'Y$.
- Puisque $a' \wedge b' = 1$, a' divise $Y = y - y_1$ et il existe $k \in \mathbb{Z}$ tel que $y - y_1 = ka' \iff \boldsymbol{y = y_1 + a'k}$.
- D'où $a'(x - x_1) = -b'ka' \iff x - x_1 = -kb' \iff \boldsymbol{x = x_1 - b'k}$.
- Pour terminer, on vérifie que de telles solutions (x, y) sont bien solutions de (E') et donc de (E).
- On obtient alors $\boldsymbol{\mathscr{S} = \{(x_1 - b'k, y_1 + a'k) \ / \ k \in \mathbb{Z}\}}$.

Exemple : Soit l'équation diophantienne $(E)\colon 35x - 21y = 14$.

- On a $35 = 21 \times 1 + 14$, $21 = 14 \times 1 + 7$, $14 = 7 \times 2 + 0$ donc $35 \wedge 21 = 21 \wedge 14 = 14 \wedge 7 = 7$.
- Puisque $7|14$, (E) admet des solutions et $(E) \iff \frac{1}{7}(E) = (E')\colon 5x - 3y = 2$.
- On a $5 = 3 \times 1 + 2$, $3 = 2 \times 1 + 1$ donc $1 = 3 - 2 = 3 - (5 - 3)$
  $1 = 5 \times (-1) - 3 \times (-2)$ et le couple $(x_0, y_0) = (-1, -2)$ est une solution particulière de l'équation $(E_1)\colon 5x - 3y = 1$.
- Le couple $(x_1, y_1) = (2x_0, 2y_0) = (-2, -4)$ est alors une solution particulière de l'équation $(E')\colon 5x - 3y = 2$.
- Si (x, y) est solution de (E'), alors $(E') - (E')$ donne
  $5(x + 2) - 3(y + 4) = (5x - 3y) - (5(-2) - 3(-4)) = 2 - 2 = 0$
  donc $5(x + 2) = 3(y + 4)$.
- Puisque $5 \wedge 3 = 1$, le théorème de Gauss permet d'affirmer que $5|y + 4$ et il existe $k \in \mathbb{Z}$ tel que $y + 4 = 5k \iff y = 5k - 4$.
- Ainsi, $5(x + 2) = 3(y + 4) \iff 5(x + 2) = 3 \times 5k \iff x + 2 = 3k$
  $\iff x = 3k - 2$.
- Réciproquement, si $(x, y) = (3k - 2, 5k - 4)$, alors
  $5x - 3y = 5(3k - 2) - 3(5k - 4) = 15k - 10 - 15k + 12 = 2$: (x, y) est solution de (E') donc de (E).
- Les solutions de (E) sont donc
  $\mathscr{S} = \{(3k - 2, 5k - 4) \ / \ k \in \mathbb{Z}\} = \{(3k + 1, 5k + 1) \ / \ k \in \mathbb{Z}\}$.

Exercices

PGCD ET APPLICATIONS

Exercice 1 Déterminer l'ensemble des entiers naturels n tels que $n \leqslant 72$ et $\mathrm{PGCD}\,(72\,,\,n) = 6$.

Exercice 2 Soit $n \in \mathbb{N}$.

1. Démontrer que $\mathrm{PGCD}\,(26n+7\,,\,n) = \begin{cases} 7 & \text{si } n \equiv 0\,[7], \\ 1 & \text{sinon.} \end{cases}$
2. Démontrer que $\mathrm{PGCD}\,(2n+1\,,\,n+3) = 5 \iff n \equiv 2\,[5]$.

Exercice 3
Soient a et b deux entiers naturels non nuls. On pose $A = 3a+4b$ et $B = 4a+5b$.

1. Démontrer que $D\,(a\,,\,b) \subset D\,(A\,,\,B)$.
2. (a) Exprimer a et b en fonction de A et de B.
   (b) En déduire que $D\,(A\,,\,B) \subset D\,(a\,,\,b)$.
3. Conclure.

Exercice 4

1. Soit $n \geqslant 2$. Déterminer le PGCD de n^2+2n-3 et n^2+4n+3 selon la parité de n.
2. Soit $n \in \mathbb{N}^*$. Montrer que $\mathrm{PGCD}\left(2n^3+5n^2+4n+1\,,\,2n^2+n\right) = 2n+1$.

Exercice 5 Déterminer le PGCD des couples d'entiers suivants (avec $n \in \mathbb{N}$).

(a)	189 et 246	(c)	365 et -12	(e)	$21\,312$ et 840
(b)	828 et 432	(d)	301 et 24	(f)	$21n+4$ et $16n+3$

Exercice 6
Montrer que, pour $n \in \mathbb{N}^*$, la fraction $\frac{19n+24}{8n+10}$ est irréductible *ssi* n est impair.

Exercice 7 Démontrer les propositions suivantes.

1. Tout entier est premier avec son successeur.
2. Tout entier impair est premier avec l'entier impair suivant.
3. Le PGCD deux entiers pairs successifs est 2.

Exercice 8
Déterminer l'ensemble des couples $(a\,,\,b) \in \mathbb{N}^2$ vérifiant les conditions suivantes.

(a) $ab = 300$ et $\mathrm{PGCD}\,(a\,,\,b) = 5$.

(b) $a+b = 72$ et $\mathrm{PGCD}\,(a\,,\,b) = 9$.

Exercice 9 Dans chaque cas, justifier l'existence de couples $(u, v) \in \mathbb{Z}^2$ vérifiant l'équation donnée puis en déterminer un.

(a)	$24u + 13v = 1$	(g)	$426u - 68v = 2$
(b)	$25u + 72v = 1$	(h)	$12x + 16y = 28$
(c)	$31u - 70v = 1$	(i)	$21a + 15b = 27$
(d)	$11u + 19v = 1$	(j)	$132u - 234v = 12$
(e)	$23u + 32v = 1$	(k)	$301u + 24v = 3$
(f)	$28u - 33v = 1$	(l)	$234u - 462v = 30$

Exercice 10 Soit $n \in \mathbb{Z}$.

1. Démontrer que $(n+2)^2$ et $(n+3)(n+1)$ sont premiers entre eux.
2. Les nombres $8n+3$ et $6n+2$ sont-ils premiers entre eux ?

Exercice 11 Déterminer tous les couples $(x, y) \in \mathbb{N}^2$ tels que $x + y = 5\,664$ et $\mathrm{PGCD}(x, y) = 354$.

Exercice 12

1. 56 est-il inversible modulo 147 ?
2. Après avoir justifié leur existence, déterminer les inverses modulo 11, modulo 13 et modulo 143 de 17.
3. Après avoir justifié leur existence, déterminer les inverses modulo 5, modulo 15 et modulo 45 de 62.
4. Après avoir justifié leur existence, déterminer les inverses modulo 7, modulo 14 et modulo 98 de 31.

Exercice 13 Soit $n \in \mathbb{N}^*$.

1. Justifier que si $n \not\equiv 0\,[3]$, alors n et 3 sont premiers entre eux.
2. Démontrer que si n est premier avec 3, alors n^3 est premier avec 9. On pourra utiliser le théorème de Bézout.
3. Qu'en déduire pour n si n^3 est divisible par 9 ?

Exercice 14 VouF ? Justifier.

1. Il existe un entier naturel n tel que $\frac{n-7}{18}$ et $\frac{n-8}{15}$ soient tous les deux entiers.
2. Il existe un entier naturel n tel que $\frac{n-3}{16}$ et $\frac{n-11}{12}$ soient tous les deux entiers.

Exercice 15 On pose $x = 4 + \sqrt{15}$ et $y = 4 - \sqrt{15}$.

1. Démontrer que, pour tout entier n, $x^n = \alpha_n + \beta_n\sqrt{15}$ et $y^n = \alpha_n - \beta_n\sqrt{15}$ où α_n et β_n sont des entiers naturels.
2. Écrire α_{n+1} et β_{n+1} en fonction de α_n et β_n.
3. Démontrer que $\alpha_n^2 - 15\beta_n^2 = 1$ puis que $\alpha_n\beta_{n+1} - \alpha_{n+1}\beta_n = 1$.
4. Justifier que les fractions $\frac{\alpha_n}{\beta_n}$, $\frac{\alpha_{n+1}}{\alpha_n}$ et $\frac{\beta_{n+1}}{\beta_n}$ sont irréductibles.

Exercice 16 Déterminer si les nombres $a = 3$, $b = 8$, $c = 44$, $d = 10$ et $e = 5$ sont inversibles modulo 33 et déterminer leur inverse le cas échéant.

Exercice 17 Résoudre les équations suivantes d'inconnues dans $\mathbb{Z}$.

(a) $47x = 28y$	(d) $5(x-1) = 2(y+3)$	(g) $54x \equiv 0\,[62]$
(b) $38x - 65y = 0$	(e) $12(x+3) = 5(y-4)$	
(c) $76x = 112y$	(f) $8x \equiv 0\,[55]$	(h) $6x \equiv 12\,[35]$

Exercice 18 Équations diophantiennes

1. (a) Résoudre dans $\mathbb{Z}$ l'équation $(E_0)\colon 11x - 15y = 0$.
   (b) Déterminer une solution particulière $(x_0\,,\,y_0)$ de l'équation $(E)\colon 11x - 15y = 3$.
   (c) Montrer que $(x\,,\,y)$ est solution de (E) *ssi* $(x - x_0\,,\,y - y_0)$ est solution de (E_0).
   (d) En déduire toutes les solutions de (E).
2. Résoudre dans $\mathbb{Z}$ les équations suivantes.

$(F)\colon 4x + 6y = 8$	$(H)\colon 748x - 1254y = 66$	$(J)\colon 56x - 21y = 105$
$(G)\colon 20x - 14y = 7$	$(I)\colon 65x + 104y = 26$	$(K)\colon 944x - 544y = 160$

Exercice 19

1. Déterminer les entiers naturels n tels que $n \equiv 6\,[22]$ et $n \equiv 6\,[40]$.
2. Déterminer les entiers naturels n tels que $n \equiv 2\,[23]$ et $n \equiv 8\,[17]$.

Exercice 20 Montrer les affirmations suivantes pour $n \in \mathbb{N}$. On pourra s'aider de tableaux de congruences.

(a) 10 divise $n(n^4 - 1)$.
(b) 6 divise $n(2n+1)(n+1)$.
(c) 120 divise $n(n^2 - 1)(n^2 - 4)$.

Exercice 21

1. Déterminer l'unique couple $(p\,,\,q) \in \mathbb{N}$ tel que $\mathrm{PGCD}\,(p\,,\,q) = 21$ et $3p - 5q = 0$.
2. Déterminer l'ensemble des couples $(m\,,\,n) \in \mathbb{Z}^2$ tels que $\mathrm{PGCD}\,(m\,,\,n) = 18$ et $7m - 4n = 0$.

Exercice 22 Soit $n \in \mathbb{N}$ tel que $n \equiv 9\,[17]$ et $n \equiv 3\,[5]$.

1. Justifier qu'il existe un couple $(u\,,\,v) \in \mathbb{Z}^2$ tel que $n = 17u + 9$, $n = 5v + 3$ et $5v - 17u = 6$.
2. Justifier que l'équation $5v - 17u = 6$ admet des solutions entières et en déterminer une.
3. En déduire l'ensemble des solutions de l'équation $5v - 17u = 6$ puis en déduire que $n \in \{43 + 85k,\ k \in \mathbb{Z}\}$.
4. Montrer que, pour tout entier relatif k, $43 + 85k$ est solution du système puis conclure.

Exercice 23 Un sac de billes
Un sac contient entre 150 et 200 billes. En faisant des paquets de 5 billes ou des paquets de 4 billes ou des paquets de 3 billes, il en reste toujours 2.
Combien y a-t-il de billes dans ce sac ?

Exercice 24 L'épaisseur d'une pièce de un euro est égale à 2,3 mm et celle d'une pièce de dix centimes est égale à 1,9 mm. Est-il possible de faire une pile de pièces de un euro et de dix centimes d'exactement 10 cm ? Si oui, avec combien de pièces de chaque sorte ?

Exercice 25 Chiffrement affine
On fait correspondre à chaque lettre de l'alphabet un nombre entier x de $[\![0\,; 25]\!]$ en suivant l'ordre alphabétique. On définit un système de codage en associant ensuite à chaque entier x, le reste y de la division euclidienne de $15x + 7$ par 26. À chaque entier y, on associe enfin la lettre correspondante afin d'obtenir la lettre codée.

1. Coder les mots MATH et MAX.
2. (a) Résoudre l'équation diophantienne $(E)\colon\ 15u - 26v = 1$.
   (b) En déduire qu'il existe un unique $u_0 \in [\![0\,; 25]\!]$ tel que $15u_0 \equiv 1\,[26]$.
   (c) Justifier que $x \equiv u_0 y - 7u_0\,[26]$.
   (d) En déduire une description du système de codage.
3. Déchiffrer le mot $POGCH$.

Exercice 26
Soit $(u_n)_{\mathbb{N}}$ la suite définie par $u_0 = 0$ et, pour tout $n \in \mathbb{N}$, $u_{n+1} = 3u_n + 1$.

1. Justifier que, pour tout $n \in \mathbb{N}$, $u_n \in \mathbb{N}$.
2. Démontrer que, pour tout $n \in \mathbb{N}^*$, u_n et u_{n+1} sont premiers entre eux.
3. Démontrer que les termes de la suite $(u_n)_{\mathbb{N}}$ sont alternativement pairs et impairs.
4. (a) Démontrer que, pour tout $n \in \mathbb{N}$, $2u_n = 3^n - 1$.
   (b) Déterminer le plus petit entier naturel non nul n tel que $3^n \equiv 1\,[7]$.
   (c) En déduire que u_{2022} est divisible par 7.

Exercice 27 Soient les suites $(u_n)_{\mathbb{N}}$ et $(v_n)_{\mathbb{N}}$ définie par $u_0 = v_0 = 1$ et, pour $n \in \mathbb{N}$, $u_{n+1} = 2u_n + 3v_n$, $v_{n+1} = 2u_n + v_n$.

1. Justifier que tous les termes de ces suites sont des entiers.
2. Calculer les premiers termes des suites $(u_n)_{\mathbb{N}}$ et $(v_n)_{\mathbb{N}}$ puis conjecturer la valeur de $w_n = 2u_n - 3v_n$.
3. Démontrer cette conjecture et en déduire le $\mathrm{PGCD}\,(\,u_n\,,\,v_n\,)$.

Exercice 28 PPCM
Soient a et b deux entiers naturels non nuls.

1. Justifier que l'ensemble des multiples communs strictement positifs à a et b est non vide et minoré puis en déduire l'existence d'un plus petit élément de cet ensemble. On l'appelle le *plus petit commun multiple* à a et b et on le note $\mathrm{PPCM}\,(\,a\,,\,b\,)$ (ou $a \vee b$).

2. (a) Lister les premiers multiples strictement positifs de 6 et de 8 et en déduire $\mathrm{PPCM}(8, 6)$.
   (b) Déterminer $\mathrm{PGCD}(6, 8)$ puis calculer les différents produits possible. Que remarque-t-on ?
   (c) Mêmes questions pour les nombres 24 et 36.
   (d) Quelle conjecture peut-on émettre ?
3. Soient $d = \mathrm{PGCD}(a, b)$ et a', b' tels que $a = a'd$ et $b = b'd$.
   (a) Que dire de a' et b' ?
   (b) Que dire de $a'b'd$?
4. (a) Si $m \in \mathbb{N}$ est un multiple commun à a et b, que dire de m ?
   (b) Qu'en déduire pour $a'b'd$?
5. Conclure.

Exercice 29 Restes chinois

Dix-sept pirates ont raflé un gros butin qu'ils comptent se partager en parts égales. Il reste alors trois pièces d'or pour le cuisinier chinois. Lors du partage, une rixe éclate et six pirates sont occis : les survivants comptent qu'en se répartissant également le butin, il reste quatre pièces pour le cuisinier mais avant qu'ils ne récupèrent la mise, cinq autres malandrins viennent à périr du scorbut. Le cuisinier chinois récupère alors cinq pièces.

1. Si b est le nombre de pièces du butin initial, traduire l'énoncé par un système de trois congruences.
2. À l'issue du dernier partage, chaque pirate dispose de 84 pièces de plus que dans la distribution initiale.
   Montrer qu'il existe alors trois entiers naturels x, y et z tels que $17x - 11y = 1$, $11y - 6z = 1$ et $z - x = 84$.
3. Déterminer l'ensemble des solutions de chacune des deux premières équations.
4. En utilisant la troisième, établir une relation entre les paramètres définissant les solutions précédentes.
5. En déduire la valeur de ces paramètres puis le montant du butin.

Exercice 30 Racines rationnelles

1. Soit $P(x) = 15x^3 - 7x + 3$.
   (a) Si $x \in \mathbb{Z}$, que dire de $\mathrm{PGCD}\left(x, x^3\right)$?
   (b) Montrer que les racines entières de P ne peuvent alors être que -3, -1, 1 ou 3 puis conclure sur l'existence de racines entières de P.
   (c) Soit $\frac{p}{q}$ une fraction irréductible racine de P.
   Montrer que $15p^3 - 7pq^2 = -3q^3$ puis en déduire que $p|3$.
   (d) Montrer de même que $q|15p^3$ puis que $q|15$.
   (e) En déduire les valeurs positives possibles de $\frac{p}{q}$. Sont-elles solutions ?

EXERCICES

2. On considère l'équation $(E)\colon 78x^3 + 11x^2 + 25x - 14 = 0$.
   (a) On suppose que l'équation (E) admet une solution rationnelle $\frac{p}{q}$ irréductible. Montrer que $p|14$ et $q|78$.
   (b) En déduire le nombre de racines rationnelles non entières pouvant être solution de (E).
3. De manière analogue, déterminer toutes les racines rationnelles de ces polynômes.

$$A(x) = 3x^4 + 5x^3 + 2x^2 - 6x - 4 \qquad B(x) = 6x^3 + 13x^2 - 22x - 8$$

Exercice 31 Soient a et b deux réels non nuls.
Quelle est la plus petite période de la fonction f définie sur $\mathbb{R}$ par
$f(x) = \cos(ax) + \sin(bx)$?

Sautez en pages 303, 305 et 307 afin de réaliser les devoirs n^{os} 8, 9 et 10.

Corrigé des exercices

PGCD ET APPLICATIONS

Exercice 1 $\operatorname{PGCD}(72, n) = 6$ donc $6|n$ et $n = 6k$. Puisque $72 = 2^3.3^2$, k n'est pas pair (sinon, $\operatorname{PGCD}(72, n) \geqslant 12$ qui divise aussi 72), ni un multiple de 3 (sinon, $\operatorname{PGCD}(72, n) \geqslant 18$ qui divise aussi 72). Puisque $n \leqslant 72$, $k \leqslant \frac{72}{6} = 12$. Les seules valeurs de k possibles sont donc : 1, 5, 7, 11, valeurs qui vérifient $\operatorname{PGCD}(72, 6k) = 6$. Ainsi, $n \in \{6; 30; 42; 66\}$.

Exercice 2 Soit $n \in \mathbb{N}$.

1. Par soustraction,
   $\operatorname{PGCD}(26n + 7, n) = \operatorname{PGCD}(26n + 7 - n, n) = \ldots = \operatorname{PGCD}(7, n)$.
   Si $n \equiv 0\,[7]$, $n = 7k$ et
   $\operatorname{PGCD}(26n + 7, n) = \operatorname{PGCD}(7, 7k) = 7\operatorname{PGCD}(1, k) = 7 \times 1 = 7$.
   Sinon, 7 ne divise pas n d'où $\operatorname{PGCD}(7, n) \in [\![1 ; 6]\!]$.
   Puisque $\operatorname{PGCD}(26n + 7, n) = \operatorname{PGCD}(7, n)$ divise 7, ce ne peut être que 1.
2. On a $\operatorname{PGCD}(2n + 1, n + 3) = \operatorname{PGCD}((2n + 1) - 2(n + 3), n + 3)$
   $= \operatorname{PGCD}(-5, n + 3)$
   et $\operatorname{PGCD}(n + 3, 5) = 5 \iff 5|n + 3 \iff n + 3 \equiv 0\,[5]$
   $\iff n \equiv -3\,[5] \iff n \equiv 2\,[5]$.

Exercice 3 Soient a et b deux entiers naturels non nuls.
On pose $A = 3a + 4b$ et $B = 4a + 5b$.

1. Si $d \in D(a, b)$, alors divise a et b et donc tout combinaison linéaire entière de a et de b, en particulier $3a + 4b = A$ et $4a + 5b = B$. Ainsi, $d \in D(A, B)$ et $D(a, b) \subset D(A, B)$.
2. (a) On a $\begin{cases} A = 3a + 4b \\ B = 4a + 5b \end{cases} \iff \begin{cases} 4B - 5A = 4(4a + 5b) - 5(3a + 4b) \\ 4A - 3B = 4(3a + 4b) - 3(4a + 5b) \end{cases}$
   $\iff \begin{cases} 4B - 5A = 16a + 20b - 15a - 20b \\ 4A - 3B = 12a + 16b - 12a - 15b \end{cases} \iff \begin{cases} a = 4B - 5A \\ b = 4A - 3B. \end{cases}$
   (b) Puisque a et b sont des combinaisons entières de A et B, le même raisonnement que dans la question 1 permet d'affirmer que $D(A, B) \subset D(a, b)$.
3. Puisque $D(a, b) \subset D(A, B)$ et $D(A, B) \subset D(a, b)$, on a $D(a, b) = D(A, B)$.

Exercice 4

1. Soit $n \geqslant 2$. $A = n^2+2n-3 = (n-1)(n+3)$ et $B = n^2+4n+3 = (n+1)(n+3)$
   donc $\operatorname{PGCD}(A, B) = (n + 3)\operatorname{PGCD}(n - 1, n + 1)$ puisque $n + 3 \geqslant 1$.
   Par ailleurs, $\operatorname{PGCD}(n - 1, n + 1) = \operatorname{PGCD}(n - 1, 2)$ par soustraction.
   Si $n \geqslant 2$ est impair, alors $n - 1 \geqslant 1$ est pair et $\operatorname{PGCD}(n - 1, 2) = 2$.

Si $n \geqslant 2$ est pair, alors $n-1 \geqslant 1$ est impair et $\mathrm{PGCD}\,(n-1\,,\,2) = 1$.
Ainsi, le PGCD de n^2+2n-3 et n^2+4n+3 vaut $2(n+3)$ si n est impair, $n+3$ si n est pair.

2. Soit $n \in \mathbb{N}^*$. On a $A = n(2n+1)$
et $B = 2n^3+5n^2+4n+1 = (2n+1)(n^2+2n+1) = (2n+1)(n+1)^2$ puisque $-\frac{1}{2}$ est racine et l'on factorise (on trouve le deuxième coeff. par division des polynômes par exemple).
D'où, $\mathrm{PGCD}\,(B\,,\,A) = (2n+1)\,\mathrm{PGCD}\big((n+1)^2\,,\,n\big)$.
Or, avec $n+2$ soustractions, on obtient
$$\begin{aligned}\mathrm{PGCD}\big((n+1)^2\,,\,n\big) &= \mathrm{PGCD}\big(n^2+2n+1-(n+2)n\,,\,n\big)\\ &= \mathrm{PGCD}\,(1\,,\,n) = 1.\end{aligned}$$
Ainsi, $\mathrm{PGCD}\big(2n^3+5n^2+4n+1\,,\,2n^2+n\big) = (2n+1)\times 1 = 2n+1$.

Exercice 5

(a) On a $246 = 189\times1+57$, $189 = 57\times3+18$, $57 = 18\times3+3$, $18 = 3\times6+0$ donc $\mathrm{PGCD}\,(246\,,\,189) = 3$.
Aussi, $\mathrm{PGCD}\,(246\,,\,189) = \mathrm{PGCD}\,(3\times82\,,\,3\times63) = 3\,\mathrm{PGCD}\,(82\,,\,63)\ldots$

(b) On a $828 = 432\times1+396$, $432 = 396\times1+36$, $396 = 36\times11+0$ donc $\mathrm{PGCD}\,(828\,,\,432) = 36$. En effet, $828 = 36\times23$, $432 = 36\times12$ et 12 et 23 n'ont pas de diviseurs communs outre ±1.

(c) On a $365 = 12\times30+5$, $12 = 5\times2+2$, $5 = 2\times2+1$, $(2 = 2\times1+0)$ donc $\mathrm{PGCD}\,(365\,,\,-12) = 1$.

(d) On a $301 = 24\times12+13$, $24 = 13\times1+11$, $13 = 11\times1+2$, $11 = 2\times5+1$, $(2 = 2\times1+0)$ donc $\mathrm{PGCD}\,(301\,,\,24) = 1$.

(e) On a $21312 = 840\times25+312$, $840 = 312\times2+216$, $312 = 216\times1+96$, $216 = 96\times2+24$, $96 = 24\times4+0$ donc $\mathrm{PGCD}\,(21312\,,\,840) = 24$.

(f) Pour $n \geqslant 2$, on a $21n+4 = (16n+3)\times1+(5n+1)$ car $0 \leqslant 5n+1 < 16n+3$, $16n+3 = (5n+1)\times3+n$ car $n < 5n+1$, $5n+1 = n\times5+1$ car $1 < n$, $(n = 1\times n+0)$ donc $\mathrm{PGCD}\,(21n+4\,,\,16n+3) = 1$.
Pour $n = 0$, $\mathrm{PGCD}\,(21n+4\,,\,16n+3) = \mathrm{PGCD}\,(4\,,\,3) = 1$
et pour $n = 1$, $\mathrm{PGCD}\,(21n+4\,,\,16n+3) = \mathrm{PGCD}\,(25\,,\,19) = 1$ car $19 \not| 25$.

Exercice 6 Soit $n \in \mathbb{N}^*$.
On a $19n+24 = (8n+10)\times2+(3n+4)$ car $0 \leqslant 3n+4 < 8n+10$,
$8n+10 = (3n+4)\times2+(2n+2)$ car $2n+2 < 3n+4$, $3n+4 = (2n+2)\times1+(n+2)$ car $n+2 < 2n+2$, $2n+2 = (n+2)\times1+n$ car $n < n+2$
et $\mathrm{PGCD}\,(19n+24\,,\,8n+10) = \mathrm{PGCD}\,(n+2\,,\,n) = \mathrm{PGCD}\,(n+2-n\,,\,n)$
$= \mathrm{PGCD}\,(n\,,\,2)$ qui vaut 1 si n est impair, 2 sinon.
La fraction $\frac{19n+24}{8n+10}$ est donc irréductible *ssi* n est impair.

Exercice 7 Soit $n \in \mathbb{Z}$.

1. Par soustraction, on a
$\mathrm{PGCD}\,(n\,,\,n+1) = \mathrm{PGCD}\,(n\,,\,n+1-n) = \mathrm{PGCD}\,(n\,,\,1) = 1$: n est premier avec son successeur.

2. On a $\mathrm{PGCD}\,(\,2n+1\,,\,2n+3\,) = \mathrm{PGCD}\,(\,2n+1\,,\,(2n+3)-(2n+1)\,)$
$= \mathrm{PGCD}\,(\,2n+1\,,\,2\,) = 1$ car $2n+1$ est impair : $2n+1$ est premier avec $2n+3$.

3. Par soustraction,
$$\mathrm{PGCD}\,(\,2n\,,\,2n+2\,) = \mathrm{PGCD}\,(\,2n\,,\,2n+2-2n\,) = \mathrm{PGCD}\,(\,2n\,,\,2\,) = 2.$$

Exercice 8

(a) $ab = 300$ et $\mathrm{PGCD}\,(\,a\,,\,b\,) = 5$:
Soient a', b' tels que $a = 5a'$, $b = 5b'$ et $\mathrm{PGCD}\,(\,a'\,,\,b'\,) = 1$.
On a alors $a'b' = \frac{300}{5^2} = 12$ et a', b' sont des diviseurs positifs de 12 premiers entre eux. Ainsi, $(\,a'\,,\,b'\,) \in \{(\,1\,,\,12\,)\,;(\,3\,,\,4\,)\}$ et leur symétrique.
Réciproquement, leur quintuple vérifient les conditions et l'on a
$$(\,a\,,\,b\,) \in \{(\,5\,,\,60\,)\,;(\,15\,,\,20\,)\,;(\,60\,,\,5\,)\,;(\,20\,,\,15\,)\}.$$

(b) $a+b = 72$ et $\mathrm{PGCD}\,(\,a\,,\,b\,) = 9$:
Soient a', b' tels que $a = 9a'$, $b = 9b'$ et $\mathrm{PGCD}\,(\,a'\,,\,b'\,) = 1$.
On a $a' \geqslant 1$, $b' \geqslant 1$ et $a'+b' = \frac{72}{9} = 8$, premiers entre eux.
Ainsi, $(\,a'\,,\,b'\,) \in \{(\,1\,,\,7\,)\,;(\,3\,,\,5\,)\}$ et leur symétrique.
Réciproquement, leur nonuple ($\times 9$) vérifient les conditions et l'on a
$$(\,a\,,\,b\,) \in \{(\,9\,,\,63\,)\,;(\,27\,,\,45\,)\,;(\,45\,,\,27\,)\,;(\,63\,,\,9\,)\}.$$

Exercice 9

(a) On a $24 = 13\times 1+11$, $13 = 11\times 1+2$, $11 = 2\times 5+2$, donc $\mathrm{PGCD}\,(\,24\,,\,13\,) = 1$: 24 et 13 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $24u+13v = 1$.
Ainsi, $11 = 24-13$, $2 = 13-11 = 13-(24-13) = 2\times 13-24$,
$1 = 11-2\times 5 = (24-13)-5(2\times 13-24) = 6\times 24-11\times 13$.
Le couple $(\,u\,,\,v\,) = (\,6\,,\,-11\,)$ est donc solution de l'équation $24u+13v = 1$.

(b) On a $72 = 25\times 2+22$, $25 = 22\times 1+3$, $22 = 3\times 7+1$, donc $\mathrm{PGCD}\,(\,72\,,\,25\,) = 1$: 72 et 25 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $25u+72v = 1$.
Ainsi, $22 = 72-2\times 25$, $3 = 25-22 = 25-(72-2\times 25) = 3\times 25-72$,
$1 = 22-3\times 7 = (72-2\times 25)-7(3\times 25-72) = -23\times 25+8\times 72$.
Le couple $(\,u\,,\,v\,) = (\,-23\,,\,8\,)$ est donc solution de l'équation $25u+72v = 1$.

(c) On a $70 = 31\times 2+8$, $31 = 8\times 3+7$, $8 = 7\times 1+1$ donc $\mathrm{PGCD}\,(\,70\,,\,31\,) = 1$: 31 et -70 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $31u-70v = 1$.
Ainsi, $8 = 70-2\times 31$, $7 = 31-3\times 8 = 31-3(70-2\times 31) = 7\times 31-3\times 70$,
$1 = 8-7 = (70-2\times 31)-(7\times 31-3\times 70) = -9\times 31+4\times 70$.
Le couple $(\,u\,,\,v\,) = (\,-9\,,\,-4\,)$ est donc solution de l'équation $31u-70v = 1$.

(d) On a $19 = 11\times 1+8$, $11 = 8\times 1+3$, $8 = 3\times 2+2$, $3 = 2\times 1+1$ donc $\mathrm{PGCD}\,(\,11\,,\,19\,) = 1$: 11 et 19 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $11u+19v = 1$.
Ainsi, $8 = 19-11$, $3 = 11-8 = 11-(19-11) = 2\times 11-19$,
$2 = 8-3\times 2 = (19-11)-(2\times 11-19)\times 2 = 3\times 19-5\times 11$,

$1 = 3 - 2 = (2 \times 11 - 19) - (3 \times 19 - 5 \times 11) = 7 \times 11 - 4 \times 19.$

Le couple $(u, v) = (7, -4)$ est donc solution de l'équation $11u + 19v = 1.$

(e) On a $32 = 23 \times 1 + 9$, $23 = 9 \times 2 + 5$, $9 = 5 \times 1 + 4$, $5 = 4 \times 1 + 1$ donc $\text{PGCD}(23, 32) = 1$: 23 et 32 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $23u + 32v = 1$.

Ainsi, $9 = 32 - 23$, $5 = 23 - 9 \times 2 = 23 - 2(32 - 23) = 3 \times 23 - 2 \times 32$,

$4 = 9 - 5 = (32 - 23) - (3 \times 23 - 2 \times 32) = 3 \times 32 - 4 \times 23,$

$1 = 5 - 4 = (3 \times 23 - 2 \times 32) - (3 \times 32 - 4 \times 23) = 7 \times 23 - 5 \times 32.$

Le couple $(u, v) = (7, -5)$ est donc solution de l'équation $23u + 32v = 1.$

(f) On a $33 = 28 \times 1 + 5$, $28 = 5 \times 5 + 3$, $5 = 3 \times 1 + 2$, $3 = 2 \times 1 + 1$ donc $\text{PGCD}(28, 33) = 1$: 28 et -33 sont premiers entre eux et il existe des solutions dans $\mathbb{Z}$ à l'équation $28u - 33v = 1$.

Ainsi, $5 = 33 - 28$, $3 = 28 - 5 \times 5 = 28 - 5(33 - 28) = 6 \times 28 - 5 \times 33$,

$2 = 5 - 3 = (33 - 28) - (6 \times 28 - 5 \times 33) = -7 \times 28 + 6 \times 33,$

$1 = 3 - 2 = (6 \times 28 - 5 \times 33) - (-7 \times 28 + 6 \times 33) = 13 \times 28 - 11 \times 33.$

Le couple $(u, v) = (13, 11)$ est donc solution de l'équation $28u - 33v = 1.$

(g) On a $426 = 68 \times 6 + 18$, $68 = 18 \times 3 + 14$, $18 = 14 \times 1 + 4$, $14 = 4 \times 3 + 2$, $4 = 2 \times 2 + 0$ donc $\text{PGCD}(426, -68) = 2$ et il existe des solutions dans $\mathbb{Z}$ à l'équation $426u - 68v = 2$.

Ainsi, $18 = 426 - 68 \times 6$,

$14 = 68 - 18 \times 3 = 68 - 3(426 - 68 \times 6) = -3 \times 426 + 19 \times 68,$

$4 = 18 - 14 = (426 - 68 \times 6) - (-3 \times 426 + 19 \times 68) = 4 \times 426 - 25 \times 68,$

$2 = 14 - 3 \times 4 = (-3 \times 426 + 19 \times 68) - 3(4 \times 426 - 25 \times 68) = -15 \times 426 + 94 \times 68.$

Le couple $(u, v) = (-15, -94)$ est donc solution de l'équation $426u - 68v = 2.$

On aurait pu diviser l'équation par le PGCD, 2, afin d'avoir de plus petits nombres mais les mêmes solutions.

(h) On a $16 = 12 \times 1 + 4$, $12 = 4 \times 3 + 0$ donc $\text{PGCD}(16, 12) = 4$ qui divise 28 et il existe des solutions dans $\mathbb{Z}$ à l'équation $12x + 16y = 28$ qui peut s'écrire $3x + 4y = 7$.

On a $4 = 3 \times 1 + 1$ donc $1 = 4 - 3$ et $7 = 7 \times 1 = 7(4 - 3) = -7 \times 3 + 7 \times 4$.

Le couple $(x, y) = (-7, 7)$ est solution de l'équation $3x + 4y = 7$ et donc de $12x + 16y = 28$.

On a trivialement $3 \times 1 + 4 \times 1 = 7$ donc $12 \times 1 + 16 \times 1 = 28$: $(1, 1)$ est une autre solution.

(i) On a $21 = 15 \times 1 + 6$, $15 = 6 \times 2 + 3$, $6 = 3 \times 2 + 0$ donc $\text{PGCD}(21, 15) = 3$ qui divise 27 et il existe des solutions dans $\mathbb{Z}$ à l'équation $21a + 15b = 27$ qui peut s'écrire $7a + 5b = 9$.

On a $7 = 5 \times 1 + 2$, $5 = 2 \times 2 + 1$

donc $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = -2 \times 7 + 3 \times 5$

et $9 = 9 \times 1 = 9(-2 \times 7 + 3 \times 5) = -18 \times 7 + 27 \times 5.$

Le couple $(a, b) = (-18, 27)$ est solution de l'équation $7a + 3b = 9$ et donc de $21a + 15b = 27$.

(j) On a $234 = 132 \times 1 + 102$, $132 = 102 \times 1 + 30$, $102 = 30 \times 3 + 12$,

$30 = 12 \times 2 + 6, \quad 12 = 6 \times 2 + 0$ donc $\mathrm{PGCD}(234, 132) = 6$ qui divise 12 et il existe des solutions dans $\mathbb{Z}$ à l'équation $132u - 234v = 12$ qui peut s'écrire $22u - 39v = 2$.

On a $39 = 22 \times 1 + 17, \quad 22 = 17 \times 1 + 5, \quad 17 = 5 \times 3 + 2, \quad 5 = 2 \times 2 + 1$ donc

$$1 = 5 - 2 \times 2 = 5 - 2(17 - 3 \times 5) = -2 \times 17 + 7 \times 5 = -2 \times 17 + 7(22 - 17)$$
$$1 = 7 \times 22 - 9 \times 17 = 7 \times 22 - 9(39 - 22) = -9 \times 39 + 16 \times 22$$

et $2 = 2 \times 1 = 2(-9 \times 39 + 16 \times 22) = 22 \times 32 - 39 \times 18$.

Le couple $(u, v) = (32, 18)$ est solution de l'équation $22u - 39v = 2$ et donc de $132u - 234v = 12$.

(k) On a $301 = 24 \times 12 + 13, \quad 24 = 13 \times 1 + 11, \quad 13 = 11 \times 1 + 2, \quad 11 = 2 \times 5 + 1$ donc $\mathrm{PGCD}(301, 24) = 1$ qui divise 3 et il existe des solutions dans $\mathbb{Z}$ à l'équation $301u + 24v = 3$.

Ainsi, $13 = 301 - 24 \times 12, \quad 11 = 24 - 13 = 24 - (301 - 24 \times 12) = 24 \times 13 - 301$,

$$2 = 13 - 11 = (301 - 24 \times 12) - (24 \times 13 - 301) = 2 \times 301 - 24 \times 25,$$
$$1 = 11 - 5 \times 2 = (24 \times 13 - 301) - 5(2 \times 301 - 24 \times 25) = -11 \times 301 + 138 \times 24$$

et $3 = 3 \times 1 = 3(-11 \times 301 + 138 \times 24) = -33 \times 301 + 414 \times 24$.

Le couple $(u, v) = (-33, 414)$ est donc solution de l'équation $301u + 24v = 3$.

(l) On a $462 = 234 \times 1 + 228, \quad 234 = 228 \times 1 + 6, \quad 228 = 6 \times 38 + 0$ donc $\mathrm{PGCD}(234, -462) = 6$ qui divise 30 et il existe des solutions dans $\mathbb{Z}$ à l'équation $234u - 462v = 30$ qui peut s'écrire $39u - 77v = 5$.

On a $77 = 39 \times 1 + 38, \quad 39 = 38 \times 1 + 1$ donc $38 = 77 - 39$,

$$1 = 39 - 38 = 39 - (77 - 39) = 2 \times 39 - 77$$

et $5 = 5 \times 1 = 5(2 \times 39 - 77) = 10 \times 39 - 5 \times 77$.

Le couple $(u, v) = (10, 5)$ est solution de l'équation $39u - 77v = 5$ et donc de $234u - 462v = 30$.

Exercice 10 Soit $n \in \mathbb{Z}$.

1. On a $(n+2)^2 = n^2 + 4n + 4$ et $(n+3)(n+1) = n^2 + 4n + 3$ donc $(n+2)^2 - (n+3)(n+1) = 1$ et le théorème de Bézout permet d'affirmer que $(n+2)^2$ et $(n+3)(n+1)$ sont premiers entre eux.
2. On a $3(8n+3) - 4(6n+2) = 24n + 9 - 24n - 8 = 1$ et le théorème de Bézout permet d'affirmer que $8n + 3$ et $6n + 2$ sont premiers entre eux.

Exercice 11 Soit $(x, y) \in \mathbb{N}^2$. On a $\mathrm{PGCD}(x, y) = 354$ donc il existe x' et $y' \in \mathbb{N}$ premiers entre eux tels que $x = 354x'$ et $y = 354y'$ et l'on a $354x' + 354y' = 5664 = 354 \times 16$ c.-à-d. $x' + y' = 16$. Les couples d'entiers premiers entre eux de somme égale à 16 sont peu nombreux : $\mathscr{S}' = \{(1, 15); (3, 13); (5, 11); (7, 9);$ et leur symétrique$\}$. Après avoir vérifié qu'en multipliant par 354, on obtient bien la somme 5 664, on peut affirmer que les solutions du problème sont les couples « $\mathscr{S} = 354 \times \mathscr{S}'$ ».

Exercice 12 On utilise ici le critère d'inversibilité modulaire (cf. prop. 8 p. 137).

1. $56 = 7 \times 8$ n'est pas premier avec 7 donc il n'est pas premier avec $7 \times 21 = 147$ et il n'est donc pas inversible modulo 147.

CORRIGÉS

2. 17 est premier avec 11, 13 et 143 donc 17 admet de tels inverses modulaires.
   · On a $17 = 11 + 6$, $11 = 6 + 5$, $6 = 5 + 1$ donc
   $1 = 6 - 5 = 6 - (11 - 6) = 2 \times 6 - 11 = 2(17 - 11) - 11 = 2 \times 17 - 3 \times 11$
   et $17 \times 2 = 1 + 3 \times 11 \equiv 1\,[11]$: l'inverse de 17 modulo 11 est 2.
   · On a $17 = 13 + 4$, $13 = 4 \times 3 + 1$ donc $1 = 13 - 3 \times 4$
   $1 = 13 - 3(17 - 13) = 4 \times 13 - 3 \times 17$ et $17 \times (-3) = 1 - 4 \times 13 \equiv 1\,[13]$.
   Puisque $-3 = 10 - 13 \equiv 10\,[13]$, l'inverse de 17 modulo 13 est 10.
   · On a $143 = 17 \times 8 + 7$, $17 = 7 \times 2 + 3$, $7 = 3 \times 2 + 1$ donc
   $1 = 7 - 2 \times 3 = 7 - 2(17 - 2 \times 7) = 5 \times 7 - 2 \times 17 = 5(143 - 17 \times 8) - 2 \times 17$
   $1 = 143 \times 5 - 17 \times 42$ et $17 \times (-42) = 1 - 5 \times 143 \equiv 1\,[143]$.
   Puisque $-42 = 101 - 143 \equiv 101\,[143]$, l'inverse de 17 modulo 143 est 101.

3. $62 = 2 \times 31$ est premier avec 5, 15 et 45 donc 62 admet de tels inverses modulaires.
   · On a $62 = 5 \times 12 + 2$, $5 = 2 \times 2 + 1$, donc $1 = 5 - 2 \times 2$
   $1 = 5 - 2(62 - 5 \times 12) = 25 \times 5 - 2 \times 62$ et $62 \times (-2) = 1 - 25 \times 5 \equiv 1\,[5]$.
   Puisque $-2 = 3 - 5 \equiv 3\,[5]$, l'inverse de 62 modulo 5 est 3.
   · On a $62 = 15 \times 4 + 2$, $15 = 7 \times 2 + 1$, donc $1 = 15 - 7 \times 2$
   $1 = 15 - 7(62 - 15 \times 4) = 15 \times 29 - 7 \times 62$ et $62 \times (-7) = 1 - 29 \times 15 \equiv 1\,[15]$.
   Puisque $-7 = 8 - 15 \equiv 8\,[15]$, l'inverse de 62 modulo 15 est 8.
   · On a $62 = 45 + 17$, $45 = 17 \times 2 + 11$, $17 = 11 + 6$, $11 = 6 + 5$, $6 = 5 + 1$ donc $1 = 6 - 5 = 6 - (11 - 6) = 2 \times 6 - 11 = 2(17 - 11) - 11$
   $1 = 2 \times 17 - 3 \times 11 = 2 \times 17 - 3(45 - 2 \times 17) = 8 \times 17 - 3 \times 45 = 8(62 - 45) - 3 \times 45$
   $1 = 8 \times 62 - 11 \times 45$ et $62 \times 8 = 1 + 11 \times 45 \equiv 1\,[45]$: l'inverse de 62 modulo 45 est 8.

4. 31 est premier avec 7, 14 et 98 donc 31 admet de tels inverses modulaires.
   · On a $31 = 7 \times 4 + 3$, $7 = 3 \times 2 + 1$, donc $1 = 7 - 2 \times 3 = 7 - 2(31 - 4 \times 7)$
   $1 = 9 \times 7 - 2 \times 31$ et $31 \times (-2) = 1 - 9 \times 7 \equiv 1\,[7]$.
   Puisque $-2 = 5 - 7 \equiv 5\,[7]$, l'inverse de 31 modulo 7 est 5.
   · On a $31 = 14 \times 2 + 3$, $14 = 3 \times 4 + 2$, $3 = 2 + 1$ donc
   $1 = 3 - 2 = 3 - (14 - 4 \times 3) = 5 \times 3 - 14 = 5(31 - 14 \times 2) - 14 = 5 \times 31 - 11 \times 14$
   et $31 \times 5 = 1 + 11 \times 14 \equiv 1\,[14]$: l'inverse de 31 modulo 14 est 5.
   · On a $98 = 31 \times 3 + 5$, $31 = 5 \times 6 + 1$, donc $1 = 31 - 6 \times 5$
   $1 = 31 - 6(98 - 3 \times 31) = 19 \times 31 - 6 \times 98$ et $31 \times 19 = 1 + 6 \times 98 \equiv 1\,[98]$: l'inverse de 31 modulo 98 est 19.

Exercice 13 Soit $n \in \mathbb{N}^*$.

1. Si $n \equiv 1\,[3]$, alors il existe $k \in \mathbb{N}$ tel que $n = 1 + 3k$ donc $n - 3k = 1$ et le théorème de Bézout permet d'affirmer que n et 3 sont premiers entre eux.
   Si $n \equiv -1\,[3]$, alors il existe $k \in \mathbb{N}$ tel que $n = -1 + 3k$ donc $3k - n = 1$ et le théorème de Bézout permet d'affirmer que n et 3 sont premiers entre eux.

2. Si n est premier avec 3, alors il existe u et v tels que $nu + 3v = 1$ donc $(1) : n^2u + 3vn = n$ et $(2) : n^3u + 3vn^2 = n^2$. Par l'absurde, si $3 | n^3$, alors $3 | n^2$ d'après (2) et 3 divise alors n, d'après (1) ce qui contredit l'hypothèse. Puisque $3 \nmid n^3$, on a $9 \nmid n^3$ et $D(9; n^3) = \{\pm 1\}$: 9 est premier avec n^3.

3. Si n^3 est divisible par 9, par contraposition, n n'est pas premier avec 3, qui n'admet que ± 1 et ± 3 comme diviseurs : n est donc un multiple de 3 (et n^3 un multiple de 27).

Exercice 14 VouF ?

1. On a $\frac{n-7}{18} \in \mathbb{Z}$ *ssi* il existe $k \in \mathbb{Z}$ tel que $n-7 = 18k$ donc $n-8 = 18k-1$ et $\frac{n-8}{15} \in \mathbb{Z}$ *ssi* il existe $k' \in \mathbb{Z}$ tel que $n-8 = 15k'$. On doit donc avoir $18k-1 = 15k'$ *i.e.* $18k - 15k' = 1$. Puisque $\mathrm{PGCD}\,(18\,,\,15) = 3 \neq 1$, 18 et 15 ne sont pas premiers entre eux et le théorème de Bézout permet d'affirmer qu'il n'existe pas de tel couple $(k\,,\,k')$. $\frac{n-7}{18}$ et $\frac{n-8}{15}$ ne peuvent pas simultanément être entiers.
2. $\frac{n-3}{16} \in \mathbb{Z} \iff \exists k$ tq. $n-3 = 16k$ et $\frac{n-11}{12} \in \mathbb{Z} \iff \exists k'$ tq. $n-11 = 12k'$.
On doit avoir $16k - 12k' = (n-3) - (n-11) \iff 16k - 12k' = 8$
$\iff 4k - 3k' = 2$. Puisque $\mathrm{PGCD}\,(4\,,\,3) = 1|2$, il existe un tel couple $(k\,,\,k')$ et les fractions correspondantes sont bien entières.

Exercice 15 $x = 4 + \sqrt{15}$ et $y = 4 - \sqrt{15}$

1. Posons, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $x^n = \alpha_n + \beta_n\sqrt{15}$, $y^n = \alpha_n - \beta_n\sqrt{15}$ où α_n, $\beta_n \in \mathbb{N}$ ».
· On a $x^0 = 1 = 1 + 0\sqrt{15} = \alpha_0 + \beta_0\sqrt{15}$
et $y^0 = 1 = 1 - 0\sqrt{15} = \alpha_0 - \beta_0\sqrt{15}$.
· Supposons $\mathscr{P}_n$ vraie pour un $n \in \mathbb{N}$.
On a $x^{n+1} = x.x^n = (4+\sqrt{15})(\alpha_n + \beta_n\sqrt{15}) = (4\alpha_n + 15\beta_n) + (\alpha_n + 4\beta_n)\sqrt{15}$
et $y^{n+1} = y.y^n = (4-\sqrt{15})(\alpha_n - \beta_n\sqrt{15}) = (4\alpha_n + 15\beta_n) - (\alpha_n + 4\beta_n)\sqrt{15}$.
Puisque $4\alpha_n + 15\beta_n$ et $\alpha_n + 4\beta_n \in \mathbb{N}$ par hypothèse, $\mathscr{P}_{n+1}$ est vraie.
· Ainsi, $\mathscr{P}_n$ est vraie pout tout $n \in \mathbb{N}$.
2. Ainsi, $\alpha_{n+1} = 4\alpha_n + 15\beta_n$ et $\beta_{n+1} = \alpha_n + 4\beta_n$.
3. On a $xy = 4^2 - \sqrt{15}^2 = 16 - 15 = 1$ donc, pour tout $n \in \mathbb{N}$,
$1 = 1^n = (xy)^n = x^n.y^n = (\alpha_n + \beta_n\sqrt{15})(\alpha_n - \beta_n\sqrt{15}) = \alpha_n^2 - (\beta_n\sqrt{15})^2$
$1 = \alpha_n^2 - 15\beta_n^2$.
Ainsi, $\alpha_n\beta_{n+1} - \alpha_{n+1}\beta_n = \alpha_n(\alpha_n + 4\beta_n) - (4\alpha_n + 15\beta_n)\beta_n$
$\alpha_n\beta_{n+1} - \alpha_{n+1}\beta_n = \alpha_n^2 + 4\alpha_n\beta_n - 4\alpha_n\beta_n - 15\beta_n^2 = \alpha_n^2 - 15\beta_n^2 + 0 = 1$.
4. Puisque $\alpha_n\beta_{n+1} - \alpha_{n+1}\beta_n = 1$, le théorème de Bézout permet d'affirmer que $(\alpha_n\,,\,\beta_n)$, $(\alpha_{n+1}\,,\,\alpha_n)$ et $(\beta_{n+1}\,,\,\beta_n)$ sont des couples de nombres premiers entre eux et les fractions $\frac{\alpha_n}{\beta_n}$, $\frac{\alpha_{n+1}}{\alpha_n}$ et $\frac{\beta_{n+1}}{\beta_n}$ sont alors irréductibles.

Exercice 16 On a n inversible modulo 33 *ssi* il existe $m \in \mathbb{Z}$ tel que $mn \equiv 1\,[33]$ *ssi* il existe m, $p \in \mathbb{Z}$ tel que $mn = 1 + 33p \iff \exists m, p \in \mathbb{Z}, mn - 33p = 1 \iff n$ et 33 sont premiers entre eux (et m est alors son inverse).
· Puisque $\mathrm{PGCD}\,(3\,,\,33) = 3 \neq 1$, $a = 3$ n'est pas inversible modulo 33.
· Puisque $\mathrm{PGCD}\,(8\,,\,33) = 1$, $b = 8$ est inversible modulo 33. On a $33 = 8 \times 4 + 1$ donc $1 = 33 - 8 \times 4$ et $-4 \equiv 29\,[33]$ est l'inverse de $b = 8$ modulo 33.
· Puisque $\mathrm{PGCD}\,(44\,,\,33) = 11 \neq 1$, $c = 44$ n'est pas inversible modulo 33.
· Puisque $\mathrm{PGCD}\,(10\,,\,33) = 1$, $d = 10$ est inversible modulo 33. On a
$33 = 10 \times 3 + 3$, $10 = 3 \times 3 + 1$ donc $1 = 10 - 3 \times 3 = 10 - 3(33 - 10 \times 3) = 4 \times 10 - 3 \times 33$

CORRIGÉS

et 4 est l'inverse de $d = 10$ modulo 33.
· Puisque $\text{PGCD}(5, 33) = 1$, $e = 5$ est inversible modulo 33. On a $33 = 5\times6+3$, $5 = 3\times1+2$, $3 = 2\times1+1$ donc $1 = 3-2 = 3-(5-3) = 2\times3-5$
$1 = 2(33-5\times6)-5 = 2\times33-13\times5$ et $-13 \equiv 20\,[33]$ est l'inverse de $e = 5$ modulo 33.

Exercice 17

(a) Puisque $\text{PGCD}(47, 28) = 1$ en testant les diviseurs de 28, si $47x = 28y$, alors $28|x$ et $47|y$ d'après le théorème de Gauss. On a donc $x = 28x'$ et $y = 47y'$ et $47x = 28y$ devient $47\times28x' = 28\times47y'$ c.-à-d. $x' = y'$. Réciproquement, un tel couple $(28k, 47k)$ est bien solution de l'équation $47x = 28y$.
On a donc $\mathscr{S}_a = \{(28k, 47k)/k \in \mathbb{Z}\}$.

(b) Puisque $\text{PGCD}(38, 65) = 1$ en testant les diviseurs de 65, si $38x = 65y$, alors $65|x$ d'après le théorème de Gauss. On a donc $x = 65k$ pour $k \in \mathbb{Z}$ et $38x = 65y$ devient $38\times65k = 65y$ c.-à-d. $y = 38k$. Réciproquement, un tel couple $(65k, 38k)$ est bien solution de l'équation $38x - 65y = 0$.
On a donc $\mathscr{S}_b = \{(65k, 38k)/k \in \mathbb{Z}\}$.

(c) On a $112 = 76\times1+36$, $76 = 36\times2+4$, $36 = 4\times9+0$, donc $\text{PGCD}(112, 76) = 4$ et l'équation s'écrit $4\times19x = 4\times28y$ c.-à-d. $19x = 28y$ où $\text{PGCD}(28, 19) = 1$. Le théorème de Gauss permet d'affirmer que $28|x$. On a donc $x = 28k$ pour $k \in \mathbb{Z}$ et $19x = 28y$ devient $19\times28k = 28y$ c.-à-d. $y = 19k$. Réciproquement, un tel couple $(28k, 19k)$ est bien solution de l'équation $76x = 112y$. On a donc $\mathscr{S}_c = \{(28k, 19k)/k \in \mathbb{Z}\}$.

(d) Puisque $\text{PGCD}(5, 2) = 1$, si $5(x-1) = 2(y+3)$, alors $2|(x-1)$ et $5|(y+3)$ d'après le théorème de Gauss. On a donc $x-1 = 2k$ pour $k \in \mathbb{Z}$ et $5(x-1) = 2(y+3)$ devient $5\times2k = 2(y+3)$ c.-à-d. $y+3 = 5k$: $x = 2k+1$, $y = 5k-3$. Réciproquement, un tel couple $(2k+1, 5k-3)$ est bien solution de l'équation $5(x-1) = 2(y+3)$. On a donc $\mathscr{S}_d = \{(2k+1, 5k-3)/k \in \mathbb{Z}\}$.

(e) Puisque $\text{PGCD}(12, 5) = 1$, si $12(x+3) = 5(y-4)$, alors $5|(x+3)$ et $12|(y-4)$ d'après le théorème de Gauss. On a donc $x+3 = 5k$ pour $k \in \mathbb{Z}$ et $12(x+3) = 5(y-4)$ devient $12\times5k = 5(y-4)$ c.-à-d. $y-4 = 12k$: $x = 5k-3$, $y = 12k+4$. Réciproquement, un tel couple $(5k-3, 12k+4)$ est bien solution de l'équation $12(x+3) = 5(y-4)$. On a donc $\mathscr{S}_e = \{(5k-3, 12k+4)/k \in \mathbb{Z}\}$.

(f) $8x \equiv 0\,[55] \iff \exists y \in \mathbb{Z}$, $8x = 55y$. Puisque $\text{PGCD}(8, 55) = 1$, si $8x = 55y$, alors $55|x$ d'après le théorème de Gauss. On a donc $x = 55k$. Réciproquement, un tel nombre $55k$ est bien solution de l'équation $8x \equiv 0\,[55]$.
On a donc $\mathscr{S}_f = \{55k/k \in \mathbb{Z}\}$.

(g) $54x \equiv 0\,[62] \iff \exists y \in \mathbb{Z}$, $54x = 62y$. On a $62 = 54\times1+8$, $54 = 8\times6+6$, $8 = 6\times1+2$, $6 = 2\times3+0$ donc $\text{PGCD}(54, 62) = 2$ et l'équation devient $27x = 31y$ où $\text{PGCD}(27, 31) = 1$. D'après le théorème de Gauss, $31|x$ et $x = 31k$. Réciproquement, un tel nombre $31k$ est bien solution de l'équation $54x \equiv 0\,[62]$. On a donc $\mathscr{S}_g = \{31k/k \in \mathbb{Z}\}$.

(h) $6x \equiv 12\,[35] \iff 6x-12 \equiv 0\,[35] \iff 6(x-2) \equiv 0\,[35]$
$\iff \exists y \in \mathbb{Z}$, $6(x-2) = 35y$. Puisque $\text{PGCD}(6, 35) = 1$, on a $35|(x-2)$

d'après le théorème de Gauss. On a donc $x-2=35k$ et $x=35k+2$.
Réciproquement, un tel nombre $35k+2$ est bien solution de l'équation $6x \equiv 12\,[35]$.
On a donc $\mathscr{S}_h = \{35k+2 / k \in \mathbb{Z}\}$.

Exercice 18

1. (a) Puisque $\mathrm{PGCD}\,(11\,,15)=1$, si $11x=15y$, alors $15|x$ et $11|y$ d'après le théorème de Gauss. On a donc $x=15x'$ et $y=11y'$ et $11x=15y$ devient $11\times 15x' = 15\times 11y'$ c.-à-d. $x'=y'$ et $x=15k$, $y=11k$. Réciproquement, un tel couple $(15k\,,11k)$ est bien solution de l'équation $11x-15y=0$.
On a donc $\mathscr{S}_{E_0} = \{(15k\,,11k)/k\in\mathbb{Z}\}$.

   (b) On a $15=11\times 1+4$, $11=4\times 2+3$, $4=3\times 1+1$
donc $1=4-3=4-(11-4\times 2)=3\times 4-11=3(15-11)-11$
$1=-4\times 11+3\times 15$ et $3=(-12)\times 11-(-9)\times 15$:
$(x_0\,,y_0)=(-12\,,-9)$ est solution $(E)\colon 11x-15y=3$.

   (c) On a $(x\,,y)$ est solution de $(E) \iff 11x-15y=3$
$\iff (11x-15y)-(11(-12)-15(-9))=3-3$
$\iff 11(x+12)-15(y+9)=0 \iff (x-x_0\,,y-y_0)$ solution de (E_0).

   (d) Ainsi, $(x\,,y)$ est solution de $(E) \iff (x+12\,,y+9)$ est solution de (E_0)
$\iff \exists k\in\mathbb{Z},\quad x+12=15k,\ y+9=11k$
et $\mathscr{S}_E = \{(15k-12\,,11k-9)/k\in\mathbb{Z}\}$.

2. • $(F)\colon 4x+6y=8$.
On a $6=4\times 1+2$ et $4=2\times 2+0$ donc $\mathrm{PGCD}\,(6\,,4)=2$. Puisque $2|8$, l'équation $(F)\colon 4x+6y=8$ admet des solutions entières et
$(F) \overset{\times 1/2}{\iff} (F')\colon 2x+3y=4$. On a $3=2\times 1+1$
donc $1=3-2=2(-1)+3\times 1$ d'où, en multipliant par 4,
$2\times(-4)+3\times 4=1\times 4$: $(-4\,,4)$ est une solution particulière de (F').
Soit $(x\,,y)$ une solution de (F'). On a alors $2x+3y=4$
donc $2(x-(-4))+3(y-4)=4-4 \iff 2(x+4)=-3(y-4)$ et $2|-3(y-4)$. Puisque 2 et 3 sont premiers entre eux, le théorème de Gauss affirme que $2|y-4$ et il existe $k\in\mathbb{Z}$ tel que $y-4=2k \iff y=4+2k$.
Alors, $2(x+4)=-3\times 2k$ et $x+4=-3k \iff x=-3k-4$.
Réciproquement, les couples $(x\,,y)=(-3k-4\,,2k+4)$ vérifient
$2(-3k-4)+3(2k+4)=-8+12=4$. L'ensemble des solutions entières de (F') et donc de (F) est $\mathscr{S}_F = \{(-3k-4\,,2k+4)/k\in\mathbb{Z}\}$.
• $(G)\colon 20x-14y=7$.
On a $20=14\times 1+6$, $14=6\times 2+2$ et $6=2\times 3+0$ donc $\mathrm{PGCD}\,(20\,,14)=2$. Puisque 2 ne divise pas 7, l'équation $(G)\colon 20x-14y=7$ n'admet pas de solutions entières : $\mathscr{S}_G=\varnothing$.
• $(H)\colon 748x-1254y=66$.
On a $1254=748\times 1+506$, $748=506\times 1+242$, $506=242\times 2+22$ et $242=22\times 11+0$ donc $\mathrm{PGCD}\,(1254\,,748)=22$. Puisque $22|66$, l'équation $(H)\colon 748x-1254y=66$ admet des solutions entières et
$(H) \overset{\times 1/22}{\iff} (H')\colon 34x-57y=3$. On a $57=34\times 1+23$, $34=23\times 1+11$

CORRIGÉS

et $23 = 11\times 2+1$ donc $1 = 23-2\times 11 = 23-2(34-23) = 3\times 23-2\times 34$
$1 = 3(57-34)-2\times 34$ $1 = 34\times(-5)-57\times(-3)$ d'où, en multipliant par 3, $34\times(-15)-57\times(-9) = 1\times 3$: $(-15\,,\,-9)$ est une solution particulière de (H').
Soit $(x\,,\,y)$ une solution de (H').
On a alors $34x-57y = 3$ donc $34(x-(-15))-57(y-(-9)) = 3-3$
$\iff 34(x+15) = 57(y+9)$ et $34|57(y+9)$. Puisque 34 et 57 sont premiers entre eux, le théorème de Gauss affirme que $34|y+9$ et il existe $k\in\mathbb{Z}$ tel que $y+9 = 34k \iff y = 34k-9$. Alors, $34(x+15) = 57\times 34k$ et $x+15 = 57k \iff x = 57k-15$.
Réciproquement, les couples $(x\,,\,y) = (57k-15\,,\,34k-9)$ vérifient
$34(57k-15)-57(34k-9) = 3$. L'ensemble des solutions entières de (H') et donc de (H) est $\mathscr{S}_H = \{(57k-15\,,\,34k-9)\,/\,k\in\mathbb{Z}\}$.

• (I): $65x+104y = 26$.
On a $104 = 65\times 1+39$, $65 = 39\times 1+26$, $39 = 26\times 1+13$ et $26 = 13\times 2+0$ donc $\text{PGCD}(104\,,\,65) = 13$. Puisque $13|26$, l'équation (I): $65x+104y = 26$ admet des solutions entières et $(I) \overset{\times 1/13}{\iff} (I')$: $5x+8y = 2$.
On a $8 = 5\times 1+3$, $5 = 3\times 1+2$ et $3 = 2\times 1+1$ donc $1 = 3-2 = 3-(5-3) = 2\times 3-5 = 2(8-5)-5 = 5\times(-3)+8\times 2$ d'où, en multipliant par 2, $5\times(-6)+8\times 4 = 1\times 2$: $(-6\,,\,4)$ est une solution particulière de (I').
Soit $(x\,,\,y)$ une solution de (I').
On a alors $5x+8y = 2$ donc $5(x-(-6))+8(y-4) = 2-2$
$\iff 5(x+6) = -8(y-4)$ et $5|8(y-4)$. Puisque 5 et 8 sont premiers entre eux, le théorème de Gauss affirme que $5|y-4$ et il existe $k\in\mathbb{Z}$ tel que $y-4 = 5k \iff y = 4+5k$. Alors, $5(x+6) = -8\times 5k$ et $x+6 = -8k \iff x = -6-8k$.
Réciproquement, les couples $(x\,,\,y) = (-6-8k\,,\,4+5k)$ vérifient
$5(-6-8k)+8(4+5k) = 2$. L'ensemble des solutions entières de (I') et donc de (I) est $\mathscr{S}_I = \{(-6-8k\,,\,4+5k)\,/\,k\in\mathbb{Z}\}$.

• (J): $56x-21y = 105$.
On a $56 = 21\times 2+14$, $21 = 14\times 1+7$ et $14 = 7\times 2+0$ donc $\text{PGCD}(56\,,\,21) = 7$. Puisque $7|105$, l'équation (J): $56x-21y = 105$ admet des solutions entières et $(J) \overset{\times 1/7}{\iff} (J')$: $8x-3y = 15$. On a $8 = 3\times 2+2$ et $3 = 2\times 1+1$ donc $1 = 3-2 = 3-(8-3\times 2) = 8\times(-1)-3\times(-3)$ d'où, en multipliant par 15, $8\times(-15)-3\times(-45) = 1\times 15$: $(-15\,,\,-45)$ est une solution particulière de (J'). Soit $(x\,,\,y)$ une solution de (J').
On a alors $8x-3y = 15$ donc $8(x-(-15))-3(y-(-45)) = 15-15$
$\iff 8(x+15) = 3(y+45)$ et $8|3(y+45)$. Puisque 8 et 3 sont premiers entre eux, le théorème de Gauss affirme que $5|y+45$ et il existe $k\in\mathbb{Z}$ tel que $y+45 = 8k \iff y = 8k-45$. Alors, $8(x+15) = 3\times 8k$ et $x+15 = 3k \iff x = 3k-15$. Réciproquement, les couples $(x\,,\,y) = (3k-15\,,\,8k-45)$ vérifient $8(3k-15)-3(8k-45) = 15$.
L'ensemble des solutions entières de (J') et donc de (J) est
$\mathscr{S}_J = \{(3k-15\,,\,8k-45)\,/\,k\in\mathbb{Z}\}$.

• $(K)\colon 944x-544y=160$.
On a $944=544\times 1+400$, $544=400\times 1+144$, $400=144\times 2+112$, $144=112\times 1+32$, $122=32\times 3+16$ et $32=16\times 2+0$ donc $\mathrm{PGCD}\,(944\,,\,544)=16$. Puisque $16|160$, l'équation $(K)\colon 944x-544y=160$ admet des solutions entières et $(K)\overset{\times 1/16}{\iff}(K')\colon 59x-34y=10$.
On a $59=34\times 1+25$, $34=25\times 1+9$, $25=9\times 2+7$, $9=7\times 1+2$ et $7=2\times 3+1$ donc $1=7-3\times 2=(25-9\times 2)-3(9-7)$

$1=25-2\times 9-3\times 9+3(25-9\times 2)=4\times 25-11\times 9$

$1=4(59-34)-11(34-25)=4\times 59-15\times 34+11(59-34)=59\times 15-34\times 26$

d'où, en multipliant par 10, $59\times 150-34\times 260=1\times 10$: $(150\,,\,260)$ est une solution particulière de (K').
Soit $(x\,,\,y)$ une solution de (K').
On a $59x-34y=10$ donc $59(x-150)-34(y-260)=10-10$ $\iff$ $59(x-150)=34(y-260)$ et $59|34(y-260)$. Puisque 59 et 34 sont premiers entre eux, le théorème de Gauss affirme que $59|y-260$ et il existe $k\in\mathbb{Z}$ tel que $y-260=59k \iff y=260+59k$. Alors, $59(x-150)=34\times 59k$ et $x-150=34k \iff x=150+34k$.
Réciproquement, les couples $(x\,,\,y)=(150+34k\,,\,260+59k)$ vérifient $59(150+34k)-34(260+59k)=10$. L'ensemble des solutions entières de (K') et donc de (K) est $\mathscr{S}_K=\{(150+34k\,,\,260+59k)\,/k\in\mathbb{Z}\}$.

Exercice 19

1. Soit $n\in\mathbb{N}$. On a $n\equiv 6\,[22] \iff n-6\equiv 0\,[22] \iff \exists k\in\mathbb{N},\ n-6=22k$ et $n\equiv 6\,[40] \iff n-6\equiv 0\,[40] \iff \exists k'\in\mathbb{N},\ n-6=40k'$.
On cherche donc k, $k'\in\mathbb{N}$ tels que $22k=40k'$. Puisque $\mathrm{PGCD}\,(22\,,\,40)=2$, cette équation devient $11k=20k'$ où 11 et 20 sont premiers entre eux. D'après le théorème de Gauss, $11|k'$ et $20|k$ donc $k'=11\ell'$, $k=20\ell$. Puisque $11k=20k'$, on a $\ell=\ell'$. Ainsi, $n=6+22k=6+22\times 20\ell$ et $n=6+40k'=6+40\times 11\ell$. Réciproquement, un tel nombre $6+440\ell$ est solution du système et l'on a donc $\mathscr{S}_1=\{440\ell+6/\ell\in\mathbb{N}\}$.

2. Soit $n\in\mathbb{N}$. On a $n\equiv 2\,[23] \iff \exists u\in\mathbb{N},\ n=23u+2$ et $n\equiv 8\,[17] \iff \exists v\in\mathbb{N},\ n=17v+8$.
On cherche donc u, $v\in\mathbb{N}$ tels que $23u+2=17v+8 \iff 23u-17v=6$. On a $23=17\times 1+6$, $17=6\times 2+5$, $6=5\times 1+1$, et $\mathrm{PGCD}\,(23\,,\,17)=1$. Puisque $\mathrm{PGCD}\,(23\,,\,17)=1|6$, cette équation admet des solutions.
On a $1=6-5=6-(17-6\times 2)=3\times 6-17=3(23-17)-17=3\times 23-4\times 17$ donc $6=18\times 23-24\times 17$ et le couple $(u\,,\,v)=(18\,,\,24)$ est solution de $23u-17v=6$. Par ailleurs, si u et v sont solutions d'une telle équation, alors $23(u-18)=17(v-24)$ et, d'après le théorème de Gauss, $17|(u-18)$ et $23|(v-24)$ d'où $u-18=17k$, $v-24=23k'$. Puisque $23(u-18)=17(v-24)$, $k=k'$ et $u=17k+18$, $v=23k+24$ ce qui donne
$n=23(17k+18)+2=17(23k+24)+8=391k+416$. Réciproquement, un tel nombre $n=391k+416$ est solution de $n\equiv 2\,[23]$ et $n\equiv 8\,[17]$. Pour que n soit positif, il faut que $k\geqslant -1$ et l'on a $\mathscr{S}_2=\{391k+416/k\in\mathbb{N}\cup\{-1\}\}$.

On peut aussi remarquer que $(1, 1)$ est une solution particulière de l'équation $23u - 17v = 6$ et l'on obtient alors $23(u-1) - 17(v-1) = 0$ ce qui mène à $u = 1+17k, v = 1+23k$ puis $n = 23(1+17k)+2 = 17(1+23k)+8 = 391k+25$ qui marche pour tout $k \in \mathbb{N}$ et en effet, $25 = 416 - 1 \times 391$.

Exercice 20

(a) Si n est pair alors $2|n(n^4 - 1)$ et si n est impair, alors n^4 et impair et $2|n^4 - 1$. Si $n \equiv 0\,[5]$, $5|n(n^4-1)$. Si $n \equiv \pm 1\,[5]$, alors $n^4 \equiv (\pm 1)^4\,[5] \equiv 1\,[5]$ et $5|n^4-1$. Si $n \equiv \pm 2\,[5]$, alors $n^4 \equiv (\pm 2)^4\,[5] \equiv 16\,[5] \equiv 1\,[5]$ et $5|n^4 - 1$. Ainsi, pour tout n, on a $2|n(n^4 - 1)$ et $5|n(n^4 - 1)$. Comme 2 et 5 sont premiers entre eux, le corollaire du théorème de Gauss permet d'affirmer que $10|n(n^4 - 1)$.

(b) On construit les tables de congruence modulo 2 et modulo 3.

n modulo 2	0	1
$n+1$ modulo 2	1	0
$2n+1$ modulo 2	1	1
$n(2n+1)(n+1)$ [2]	0	0

n modulo 3	0	1	2
$n+1$ modulo 3	1	2	0
$2n+1$ modulo 3	1	0	2
$n(2n+1)(n+1)$ [3]	0	0	0

D'après les deux tableaux, $n(2n + 1)(n + 1)$ est divisible par 2 et par 3. Or 2 et 3 sont premiers entre eux, donc, d'après le corollaire du théorème de Gauss, $n(2n+1)(n+1)$ est divisible par 6.

(c) On remarque que $n\left(n^2 - 1\right)\left(n^2 - 4\right) = n(n-1)(n+1)(n-2)(n+2)$ et $120 = 8 \times 3 \times 5$. Pour ne pas construire une table de congruences par 120, on construit donc les tables suivantes.

n modulo 8	0	1	2	3	4	5	6	7
$n-1$ modulo 8	7	0	1	2	3	4	5	6
$n+1$ modulo 8	1	2	3	4	5	6	7	0
$n-2$ modulo 8	6	7	0	1	2	3	4	5
$n+2$ modulo 8	2	3	4	5	6	7	0	1
$n\left(n^2-1\right)\left(n^2-4\right)$ [8]	0	0	0	$120 \equiv 0$	$720 \equiv 0$	$2520 \equiv 0$	0	0

n modulo 5	0	1	2	3	4
$n-1$ modulo 5	4	0	1	2	3
$n+1$ modulo 5	1	2	3	4	0
$n-2$ modulo 5	3	4	0	1	2
$n+2$ modulo 5	2	3	4	0	1
$n\left(n^2-1\right)\left(n^2-4\right)$ modulo 5	0	0	0	0	0

n modulo 3	0	1	2
$n-1$ modulo 3	2	0	1
$n+1$ modulo 3	1	2	0
$n-2$ modulo 3	1	2	0
$n+2$ modulo 3	2	0	1
$n\left(n^2-1\right)\left(n^2-4\right)$ modulo 3	0	0	0

Finalement, pour $n \in \mathbb{N}$, $n\left(n^2 - 1\right)\left(n^2 - 4\right)$ est divisible par 3 et par 5. Comme 3 et 5 sont premiers entre eux, le corollaire du théorème de Gauss prouve que $n\left(n^2 - 1\right)\left(n^2 - 4\right)$est divisible par 15. De même, 15 et 8 étant premiers entre eux, on en déduit que $n\left(n^2 - 1\right)\left(n^2 - 4\right)$ est divisible par 120.

Exercice 21

1. Soient p' et $q' \in \mathbb{N}$ premiers entre eux tels que $p = 21p'$ et $q = 21q'$. L'équation $3p - 5q = 0$ s'écrit alors $3 \times 21p' = 5 \times 21q'$ c.-à-d. $3p' = 5q'$. Puisque 3 et 5 sont premier entre eux, le théorème de Gauss permet d'affirmer que $5 \,|\, p'$ donc $p' = 5k$ et puisque $3p' = 3 \times 5k = 5q'$, on a $q' = 3k$. Comme p' et q' sont premiers entre eux, on a $k = 1$, car k est un diviseur commun de p' et q'. Ainsi, $p' = 5$, $q' = 3$ donc $p = 21 \times 5$, $q = 21 \times 3$: $(p\,,\,q) = (105\,,\,63)$ est l'unique couple recherché.
2. Soient m' et $n' \in \mathbb{Z}$ premiers entre eux tels que $m = 18m'$ et $n = 18n'$. L'équation $7m - 4n = 0$ s'écrit alors $7 \times 18m' = 4 \times 18n'$ c.-à-d. $7m' = 4n'$. Puisque 7 et 4 sont premier entre eux, le théorème de Gauss permet d'affirmer que $4 \,|\, m'$ donc $m' = 4k$ et puisque $7m' = 7 \times 4k = 4n'$, on a $n' = 7k$. Comme m' et n' sont premiers entre eux, on a $k = \pm 1$, car k est un diviseur commun de m' et n'. Ainsi, $m' = \pm 4$, $n' = \pm 7$ donc $m = \pm 4 \times 18$, $n = \pm 7 \times 18$: $\mathscr{S} = \{(-72\,,\,-126)\,;(72\,,\,126)\}$.

Exercice 22 Soit $n \in \mathbb{N}$ tel que $n \equiv 9\,[17]$ et $n \equiv 3\,[5]$.

1. Puisque $n \equiv 9\,[17]$, il existe $u \in \mathbb{Z}$ tel que $n = 9 + 17u$. De même, $n \equiv 3\,[5]$ donc il existe $v \in \mathbb{Z}$ tel que $n = 3 + 5v$. Ainsi, $n - n = (3 + 5v) - (9 + 17u)$ et donc $5v - 17u = 6$.
2. On a $17 = 5 \times 3 + 2$, $5 = 2 \times 2 + 1$ donc $\mathrm{PGCD}\,(17\,,\,5) = 1 | 6$ et l'équation $5v - 17u = 6$ admet des solutions dans $\mathbb{Z}$.
   On a $1 = 5 - 2 \times 2 = 5 - 2(17 - 5 \times 3) = 7 \times 5 - 2 \times 17$ donc $42 \times 5 - 12 \times 17 = 6$ et le couple $(u\,,\,v) = (12\,,\,42)$ est solution de $5v - 17u = 6$.
3. Si $5v - 17u = 6$, alors $5(v-42) - 17(u-12) = 6 - 6 = 0$ donc $5(v-42) = 17(u-12)$ et, d'après le théorème de Gauss, $17 \,|\, v - 42$ puisque 17 est premier avec 5. On a donc $v - 42 = 17k$ et $u - 12 = 5k$ pour $k \in \mathbb{Z}$.
   On a alors $n = 9 + 17(5k + 12) = 3 + 5(17k + 42) = 85k + 213$ pour $k \in \mathbb{Z}$ ce qui peut s'écrire $n = 85k + 43$ car $213 = 2 \times 85 + 43$.
4. Soit $k \in \mathbb{Z}$ et $n = 43 + 85k$. On a $85 = 17 \times 5$, $43 = 17 \times 2 + 9$ et $43 = 5 \times 8 + 3$ donc $n \equiv 9\,[17]$ et $n \equiv 3\,[5]$. Pour que n soit naturel, il faut et il suffit que $k \in \mathbb{N}$. Ainsi, les entiers n recherchés sont de la forme $43 + 85k$ pour $k \in \mathbb{N}$.

Exercice 23 Un sac de billes

Soit b le nombre de billes dans le sac. On a $b \in [\![\, 150\,;200 \,]\!]$, $b \equiv 2\,[5]$, $b \equiv 2\,[4]$ et $b \equiv 2\,[3]$.
Ainsi, $b - 2 \equiv 0\,[5]$, $b - 2 \equiv 0\,[4]$ et $b - 2 \equiv 0\,[3]$. D'où, $b - 2 = 5c = 4q = 3t$.
Puisque 4 et 5 sont premiers entre eux, 5 divise q et $b - 2 = 4 \times 5q' = 3t$.
Puisque 3 et 20 sont premiers entre eux, 3 divise q' et $b - 2 = 4 \times 5 \times 3q''$: $b - 2 \equiv 0\,[60]$ et $b \equiv 2\,[60]$.
Puisque $b \in [\![\, 150\,;200 \,]\!]$, on a $b = 182$.

Exercice 24 On cherche e et $c \in \mathbb{N}$ tels que $2{,}3e + 1{,}9c = 100 \iff 23e + 19c = 1000$.
On a $23 = 19 \times 1 + 4$, $19 = 4 \times 4 + 3$, $4 = 3 \times 1 + 1$ donc $\mathrm{PGCD}\,(23\,,\,19) = 1$ qui divise 1000 et il existe des solutions dans $\mathbb{Z}$ à l'équation $23e + 19c = 1000$.
Ainsi, $1 = 4 - 3 = 4 - (19 - 4 \times 4) = 5 \times 4 - 19 = 5(23 - 19) - 19 = 5 \times 23 - 6 \times 19$

CORRIGÉS

et $1000 = 5000 \times 23 - 6000 \times 19$: $(5000\,,\,-6000)$ est une solution particulière de $23e + 19c = 1000$.
Si $(e\,,\,c)$ est solution de l'équation $23e + 19c = 1000$, alors

$$23(e-5000) + 19(c+6000) = 1000 - 1000 \iff 23(e-5000) = -19(c+6000)$$

et d'après le théorème de Gauss, $-19 \,|\, e - 5000$ donc $e = 5000 - 19k$ et l'équation devient $23 \times (-19k) = -19(c+6000)$ donc $c = 23k - 6000$.
Les solutions dans $\mathbb{Z}$ de l'équation $23e + 19c = 1000$ sont donc de la forme $(e\,,\,c) = (5000 - 19k\,,\,23k - 6000)$ où $k \in \mathbb{Z}$.
Pour que e et c soient des entiers naturels, il faut que $5000 - 19k \geqslant 0$ et $23k - 6000 \geqslant 0$ c.-à-d. $\frac{6000}{23} \simeq 260,8 \leqslant k \leqslant \frac{5000}{19} \simeq 263,1$ donc $k \in [\![\, 261\,;263 \,]\!]$ ce qui correspond aux couples $(e\,,\,d) \in \{(41\,,\,3)\,;(22\,,\,26)\,;(3\,,\,49)\}$ qui ont une valeur de 41,30 €, 24,60 € et 7,90 € respectivement.
Par ailleurs, si l'on juxtapose une pile de 5000 pièces de un euro et une pile de 6000 pièces de dix centimes, la différence de hauteur sera de 10 cm, pile-poil.

Exercice 25 Chiffrement affine

1. M correspond à l'entier $x_M = 12$. On a $15x_M + 7 = 187 = 26 \times 7 + 5$ donc $y_M = 5$ qui correspond à la lettre chiffrée F. De même, $x_A = 0$, $y_A = 7$ qui correspond à la lettre chiffrée H ; $x_T = 19$, $y_T = 6$ qui correspond à la lettre chiffrée G ; $x_H = 7$, $y_H = 8$ qui correspond à la lettre chiffrée I ; $x_X = 23$, $y_X = 14$ qui correspond à la lettre chiffrée O. Ainsi, MATH MAX se chiffre par $FHGI\ FHO$.
   Sur une calculatrice T.I., on peut utiliser un tableau de valeurs avec la fonction $\mathrm{reste}(15\mathrm{X}{+}7\,,26)$.

2. (a) On a $26 = 15 \times 1 + 11$, $15 = 11 \times 1 + 4$, $11 = 4 \times 2 + 3$, $4 = 3 \times 1 + 1$ donc $\mathrm{PGCD}\,(26\,,\,15) = 1$ et l'équation (E): $15u - 26v = 1$ admet des solutions dans $\mathbb{Z}$. On a $1 = 4 - 3 = 4 - (11 - 4 \times 2) = 3 \times 4 - 11$
   $1 = 3(15 - 11) - 11 = 3 \times 15 - 4 \times 11 = 3 \times 15 - 4(26 - 15) = 7 \times 15 - 4 \times 26$
   et le couple $(u_0\,,\,v_0) = (7\,,\,4)$ est solution de (E).
   Soit $(u\,,\,v)$ un couple solution de (E). On a $15(u - u_0) - 26(v - v_0) = 0$ donc $15(u-7) = 26(v-4)$. Puisque 15 est premier avec 26, on a $15 \,|\, v - 4$ et $v - 4 = 15k$, $k \in \mathbb{Z}$. Alors, $u - 7 = 26k$ et les solutions de (E) sont $\mathscr{S}_{(E)} = \{(7 + 26k\,,\,4 + 15k)\,/\,k \in \mathbb{Z}\}$.

   (b) On a $15u \equiv 1\,[26] \iff \exists v \in \mathbb{Z},\ 15u = 1 + 26v$
   $\iff \exists v \in \mathbb{Z},\ 15u - 26v = 1 \iff \exists v \in \mathbb{Z},\ (u\,,\,v) \in \mathscr{S}_{(E)}$. Or, il existe un unique couple $(u\,,\,v) \in \mathscr{S}_{(E)}$ tel que $u \in [\![\, 0\,;25 \,]\!]$, celui pour $k = 0$: $(7\,,\,4)$ et $u_0 = 7$ est l'unique solution dans $[\![\, 0\,;25 \,]\!]$ de l'équation $15u \equiv 1\,[26]$.

   (c) On a $15x + 7 \equiv y\,[26] \iff 15x \equiv y - 7\,[26]$
   $\iff u_0 \times 15x \equiv u_0(y-7)\,[26] \iff x \equiv u_0 y - 7u_0\,[26]$.

   (d) Pour déchiffrer un message, il faut retrouver le numéro de la lettre originale, x, à partir de celui de la lettre chiffrée, y.
   Puisque $u_0 = 7$, $x \equiv 7y - 7 \times 7\,[26] \equiv 7y + 3\,[26]$ et pour retrouver x, il suffit de prendre le reste de la division euclidienne par 26 de $7y + 3$.

3. On a $y_P = 15$ donc $7y_P + 3 = 108$ et $x_P = 4$ qui correspond à la lettre en clair E.
De même, $O \to 14 \to 23 \to X$, $G \to 6 \to 19 \to T$, $C \to 2 \to 17 \to R$, $H \to 7 \to 0 \to A$ et $POGCH$ se déchiffre en EXTRA.

Exercice 26 $u_0 = 0$, $u_{n+1} = 3u_n + 1$.

1. On a $u_0 \in \mathbb{N}$ et une récurrence triviale permet d'affirmer que $u_n \in \mathbb{N}$ pout tout entier naturel n.
2. Soit $n \in \mathbb{N}^*$. Par soustraction,
$\mathrm{PGCD}\,(\,u_{n+1}\,,\,u_n\,) = \mathrm{PGCD}\,(\,3u_n + 1\,,\,u_n\,) = \mathrm{PGCD}\,(\,1\,,\,u_n\,) = 1.$
3. Soit $n \in \mathbb{N}$.
Si u_n est pair, $u_n = 2k$ et $u_{n+1} = 3u_n + 1 = 3 \times 2k + 1 = 2(3k) + 1$ est impair.
Si u_n est impair, $u_n = 2k + 1$
et $u_{n+1} = 3u_n + 1 = 3(2k + 1) + 1 = 2 \times 3k + 4 = 2(3k + 2)$ est pair.
Puisque pour tout $n \in \mathbb{N}$, $u_n \in \mathbb{N}$, les termes de la suite $(u_n)_{\mathbb{N}}$ sont alternativement pairs et impairs.
4. (a) Posons, pour $n \in \mathbb{N}$, $\mathscr{P}_n$: « $2u_n = 3^n - 1.$ »
· On a $2u_0 = 2 \times 0 = 0 = 1 - 1 = 3^0 - 1$ et $\mathscr{P}_0$ est vraie.
· Supposons $\mathscr{P}_n$ vraie pour un certain $n \in \mathbb{N}$.
On a $2u_{n+1} = 2(3u_n + 1) = 3 \times 2u_n + 2 = 3(3^n - 1) + 2 = 3^{n+1} - 1$ et $\mathscr{P}_{n+1}$ est vraie.
· Ainsi, $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.
(b) Au moyen de la calculatrice, on détermine que le plus petit $n \in \mathbb{N}^*$ tel que $3^n \equiv 1\,[7]$ est $n = 6$.
(c) Ainsi, $3^6 \equiv 1\,[7]$ et, pour tout $k \in \mathbb{N}$, $3^{6k} = (3^6)^k \equiv 1^k\,[7]$.
On a alors $2u_{2022} = 2u_{6\times 337} = 3^{6\times 337} - 1 \equiv 0\,[7]$ et $2u_{2022}$ est divisible par 7. Puisque 2 est premier avec 7, le théorème de Gauss permet d'affirmer que u_{2022} est divisible par 7.

Exercice 27 $u_0 = v_0 = 1$ et, pour $n \in \mathbb{N}$, $u_{n+1} = 2u_n + 3v_n$, $v_{n+1} = 2u_n + v_n$.

1. On a u_0 et $v_0 \in \mathbb{N}$ et une récurrence triviale permet d'affirmer que u_n et $v_n \in \mathbb{N}$ pout tout entier naturel n.
2. On a $u_0 = v_0 = 1$, $u_1 = 2u_0 + 3v_0 = 5$, $v_1 = 2u_0 + v_0 = 3$, $u_2 = 2u_1 + 3v_1 = 19$, $v_2 = 2u_1 + v_1 = 13$ et $u_3 = 2u_2 + 3v_2 = 77$, $v_3 = 2u_2 + v_2 = 51$. Ainsi, $w_0 = 2u_0 - 3v_0 = -1$, $w_1 = 2u_1 - 3v_1 = 1$, $w_2 = 2u_2 - 3v_2 = -1$ et $w_3 = 2u_3 - 3v_3 = 1$.
On peut conjecturer que, pour tout $n \in \mathbb{N}$, $w_n = 2u_n - 3v_n = (-1)^{n+1}$.
3. Par récurrence rapide, on a $w_{n+1} = 2u_{n+1} - 3v_{n+1}$
$w_{n+1} = 2(2u_n + 3v_n) - 3(2u_n + v_n) = -2u_n + 3v_n = -(2u_n - 3v_n) = -w_n$
$w_{n+1} = -(-1)^{n+1} = (-1)^{n+2}$.
Ainsi, pour tout $n \in \mathbb{N}$, $2u_n - 3v_n = 1$ ou $-2u_n + 3v_n = 1$. Autrement dit, pour tout $n \in \mathbb{N}$, il existe $(\,a\,,\,b\,)$ tel que $au_n + bv_n = 1$. D'où $\mathrm{PGCD}\,(\,u_n\,,\,v_n\,) = 1$ et les termes u_n et v_n sont premiers entre eux.

CORRIGÉS

Exercice 28 PPCM

Soient a et b deux entiers naturels non nuls.

1. L'entier ab est un multiple strictement positif de a et de b. Par ailleurs, l'ensemble des entiers positifs multiples de a et de b est trivialement minoré par 0. Cet ensemble non vide et minoré de $\mathbb{Z}$ admet donc un plus petit élément, le PPCM de a et de b.
2. (a) Les premiers multiples strictement positifs de 6 sont 6, 12, 18, 24 et 30. Ceux de 8 sont 8, 16, 24, 32. Ainsi, $\mathrm{PPCM}\,(\,8\,,\,6\,) = 24$.
   (b) On a $\mathrm{PGCD}\,(\,6\,,\,8\,) = \mathrm{PPCM}\,(\,2\times 3\,,\,2\times 4\,) = 2\,\mathrm{PGCD}\,(\,3\,,\,4\,) = 2\times 1 = 2$. On remarque que $8\times 6 = 48 = 2\times 24$.
   (c) De manière similaire, $\mathrm{PPCM}\,(\,24\,,\,36\,) = 72$ $(3\times 24$ et $2\times 36)$ et $\mathrm{PGCD}\,(\,24\,,\,36\,) = 12$ $(2\times 12$ et $3\times 12)$.
   On a aussi $24\times 36 = 864 = 72\times 12$.
   (d) On conjecture que $ab = \mathrm{PGCD}\,(\,a\,,\,b\,)\times \mathrm{PPCM}\,(\,a\,,\,b\,)$.
3. (a) Si $d = \mathrm{PGCD}\,(\,a\,,\,b\,)$, $a = a'd$ et $b = b'd$ alors on sait que a' et b' sont premiers entre eux.
   (b) De plus, $a'b'd = b'(a'd) = b'a$ et $a'b'd = a'(b'd) = a'b$ donc $a'b'd$ est un multiple commun à a et b.
4. (a) Si $m \in \mathbb{N}$ est un multiple commun à a et b, alors $m = pa = pa'd$ et $m = qb = qb'd$ donc $pa' = qb'$. Puisque a' et b' sont premiers entre eux, le théorème de Gauss permet d'affirmer que $q\,|\,a'$: $q = ka'$ où $k \in \mathbb{N}$. Ainsi, $m = qb'd = ka'b'd$ et m est un multiple de $a'b'd$.
   (b) On a vu que $a'b'd$ est un multiple positif de a et de b qui divise tout multiple commun à a et à b : c'est donc le plus petit de tous. $\mathrm{PPCM}\,(\,a\,,\,b\,) = a'b'd$.
5. On a alors $\mathrm{PPCM}\,(\,a\,,\,b\,)\times \mathrm{PGCD}\,(\,a\,,\,b\,) = a'b'd\times d = (a'd)(b'd) = a\times b$.

Exercice 29 Restes chinois

1. D'après l'énoncé, on a $b \equiv 3[17]$, $b \equiv 4[11]$ et $b \equiv 5[6]$ puisqu'en divisant le butin en 17 parts, il reste 3 pièces, en le divisant par 11, il en reste 4, et en le divisant en 6 parts, il en reste 5.
2. Ce système de congruences est équivalent à l'existence d'un triplet $(x;y;z) \in \mathbb{N}^3$ tel que $b = 17x+3$, $b = 11y+4$ et $b = 6z+5$ où x, y et z sont le nombre de pièces reçues par chaque pirate lors du premier, du deuxième et du troisième partage respectivement. On a donc $b = 17x+3 = 11y+4 = 6z+5$. De plus, comme chaque pirate reçoit 84 pièces de plus lors du troisième que lors du premier partage, on peut aussi écrire $z = x+84$. Ainsi, $(x;y;z)$ vérifie donc $17x-11y = 1$, $11y-6z = 1$ et $z-x = 84$.
3. · $(2;3)$ est une solution particulière de $17x - 11y = 1$ (en effet, $17\times 2 - 11\times 3 = 34 - 33 = 1)$ et si $(x;y)$ est une autre solution de cette équation, alors $17x - 11y = 17\times 2 - 11\times 3$ donc $17\,(x-2) = 11\,(y-3)$. D'après le théorème de Gauss, comme 17 et 11 sont premiers entre eux, 11 divise $x-2$. Il existe donc $k \in \mathbb{Z}$ tel que $x - 2 = 11k$. En remplaçant $x-2$ par $11k$ dans l'équation, on obtient $17\times 11k = 11\,(y-3)$ donc $y - 3 = 17k$.

D'où $x = 11k + 2$ et $y = 17k + 3$. Réciproquement, pour tout $k \in \mathbb{Z}$, $17 \times (11k + 2) - 11 \times (17k + 3) = 17 \times 11k + 34 - 11 \times 17k - 33 = 1$.
Donc, pour tout $k \in \mathbb{Z}$, $(11k + 2; 17k + 3)$ est solution de $17x - 11y = 1$.
L'ensemble des solutions entières de $17x - 11y = 1$ est donc
$\mathscr{S}_1 = \{(11k + 2; 17k + 3) / k \in \mathbb{Z}\}$.
· $(5; 9)$ est une solution particulière de $11y - 6z = 1$ (en effet, $11 \times 5 - 6 \times 9 = 55 - 54 = 1$) et si $(y; z)$ est une autre solution, alors $11y - 6z = 11 \times 5 - 6 \times 9$ donc $11\,(y - 5) = 6\,(z - 9)$. D'après le théorème de Gauss, comme 6 et 11 sont premiers entre eux, 11 divise $z - 9$. Il existe donc $k \in \mathbb{Z}$ tel que $z - 9 = 11k$. En remplaçant $z - 9$ par $11k$ dans l'équation, on obtient alors $11\,(y - 5) = 6 \times 11k$ donc $y - 5 = 6k$. D'où $y = 6k + 5$ et $z = 11k + 9$. Réciproquement, pour tout $k \in \mathbb{Z}$, $11 \times (6k + 5) - 6 \times (11k + 9) = 11 \times 6k + 55 - 6 \times 11k - 54 = 1$. Donc, pour tout $k \in \mathbb{Z}$, $(6k + 5; 11k - 9)$ est solution de $11y - 6z = 1$. L'ensemble des solutions entières de $11y - 6z = 1$ est donc $\mathscr{S}_2 = \{(6k + 5; 11k + 9) / k \in \mathbb{Z}\}$.

4. Soient $(x; y; z) \in \mathbb{N}^3$ une solution du système et $(k; k') \in \mathbb{Z}^2$ tel que $x = 11k + 2$, $y = 17k + 3$, $y = 6k' + 5$ et $z = 11k' + 9$. Comme $z - x = 84$, on a $11k' + 9 - 11k - 2 = 84$ c.-à-d. $11\,(k' - k) = 77$ et l'on obtient $k' = k + 7$.
5. On sait que $y = 17k + 3 = 6k' + 5$ et que $k' = k + 7$ d'où $17k + 3 = 6\,(k + 7) + 5$ c.-à-d. $11k = 44$. D'où $k = 4$ et $k' = k + 7 = 11$. En remplaçant k et k' par leur valeur, on obtient enfin $x = 46$, $y = 71$, $z = 130$ et $b = 17x + 3 = 785$.
On a bien $785 = 17 \times 46 + 3 \equiv 3\,[17]$, $785 = 11 \times 71 + 4 \equiv 4\,[11]$, $785 = 6 \times 130 + 5 \equiv 5\,[6]$ et $130 - 46 = 84$.
Le butin des pirates est donc de 785 pièces.

Exercice 30 Racines rationnelles

1. Soit $P(x) = 15x^3 - 7x + 3$.
   (a) Si $x \in \mathbb{Z}$, alors $x^2 \in \mathbb{Z}$ et $x^3 = x \times x^2$ donc $x | x^3$ et $\mathrm{PGCD}\left(x\,,\,x^3\right) = |x|$.
   (b) Si $x \in \mathbb{Z}$ est racine de P, alors $15x^3 - 7x + 3 = 0 \iff x(15x^2 - 7) = -3$ et puisque $15x^2 - 7 \in \mathbb{Z}$, on a $x | 3$ c.-à-d. $x \in \{\pm 1; \pm 3\}$.
   Après calculs, on a $P(x) \neq 0$ pour tout $x \in \{\pm 1; \pm 3\}$: P n'admet donc aucune racine entière.
   (c) Soit $\frac{p}{q}$ une fraction irréductible racine de P.
   On a donc $P(\frac{p}{q}) = 0 \iff 15(\frac{p}{q})^3 - 7\frac{p}{q} + 3 = 0$
   $$\overset{\times q^3 \neq 0}{\iff} 15p^3 - 7pq^2 = -3q^3 \iff p(15p^2 - 17q^2) = -3q^3.$$
   Comme $15p^2 - 17q^2 \in \mathbb{Z}$, on a $p | 3q^3$. Puisque p et q sont premiers entre eux, le théorème de Gauss donne $p | 3q^2$ puis $p | 3q$ et enfin $p | 3$.
   (d) On a $15p^3 - 7pq^2 = -3q^3 \iff 15p^3 = q(7pq - 3q^2)$ où $7pq - 3q^2 \in \mathbb{Z}$ donc $q | 15p^3$. Puisque p et q sont premiers entre eux, le théorème de Gauss permet d'affirmer que $q | 15p^2$ puis $q | 15p$ et enfin $q | 15$.
   (e) On a donc $p \in \{\pm 1; \pm 3\}$, $q \in \{\pm 1; \pm 3; \pm 5\ \pm 15\}$ et $\mathrm{PGCD}\,(p\,,\,q) = 1$. Les valeurs possibles de $\frac{p}{q}$ sont donc $\pm\frac{1}{1}$, $\pm\frac{1}{3}$, $\pm\frac{1}{5}$, $\pm\frac{3}{5}$ et $\pm\frac{1}{15}$. En les

CORRIGÉS

testant, il s'avère qu'aucune n'est racine de P.
P n'admet donc pas de racine rationnelle.

2. (a) On suppose que l'équation (E) : $78x^3+11x^2+25x-14=0$ admet une solution rationnelle $\frac{p}{q}$ irréductible. On a alors
$$78(\tfrac{p}{q})^3+11(\tfrac{p}{q})^2+25\tfrac{p}{q}-14=0 \overset{\times q^3\neq 0}{\iff} 78p^3+11p^2q+25pq^2-14q^3=0$$
$$\iff p(78p^2+11pq+25q^2)=14q^3 \iff q(11p^2+25pq-14q^2)=-78p^3.$$
Ainsi, $p\,|\,14q^3$. Puisque p et q sont premiers entre eux, le théorème de Gauss permet d'affirmer que $p\,|\,14q^2$ puis $p\,|\,14q$ et enfin $p\,|\,14$.
De même, $q\,|\,78p^3$. Puisque p et q sont premiers entre eux, le théorème de Gauss permet d'affirmer que $q\,|\,78p^2$ puis $q\,|\,78p$ et enfin $q\,|\,78$.
(b) Si $\frac{p}{q}$ est une solution non entière de (E), on a $\mathrm{PGCD}\,(p\,,\,q)=1$, $p\in\{\pm1;\pm2;\pm7;\pm14\}$ et $q\in\{\pm1;\pm2;\pm3;\pm6;\pm13;\pm26;\pm39;\pm78\}$.
Il existe donc $7+3+7+3=20$ racines rationnelles non entières pouvant être solution de (E).

3. · $A(x)=3x^4+5x^3+2x^2-6x-4$. Soit $\frac{p}{q}$ une racine rationnelle irréductible de A.
On a $3(\tfrac{p}{q})^4+5(\tfrac{p}{q})^3+2(\tfrac{p}{q})^2-6\tfrac{p}{q}-4=0 \overset{\times q^4\neq 0}{\iff} 3p^4+5p^3q+2p^2q^2-6pq^3-4q^4=0$
$$\iff p(3p^3+5p^2q+2pq^2-6q^3)=4q^4 \iff q(5p^3+2p^2q-6pq^2-4q^3)=-3p^4.$$
Puisque p et q sont premiers entre eux, le théorème de Gauss appliqué plusieurs fois permet d'affirmer que $p\big|4$ et $q\,|\,3$. Ainsi, $\mathrm{PGCD}\,(p\,,\,q)=1$, $p\in\{\pm1;\pm3\}$ et $q\in\{\pm1;\pm2;\pm4\}$ et les solutions rationnelles appartiennent donc à $\{\pm\frac{1}{1};\pm\frac{1}{2};\pm\frac{1}{4};\pm\frac{3}{1};\pm\frac{3}{2};\pm\frac{3}{4}\}$. En testant les différentes valeurs possibles, il s'avère que 1 est la seule racine rationnelle de A.
· $B(x)=6x^3+13x^2-22x-8$. Soit $\frac{p}{q}$ une racine rationnelle irréductible de B.
On a $6(\tfrac{p}{q})^3+13(\tfrac{p}{q})^2-22\tfrac{p}{q}-8=0 \overset{\times q^3\neq 0}{\iff} 6p^3+13p^2q-22pq^2-8q^3=0$
$$\iff p(6p^2+13pq-22q^2)=8q^3 \iff q(13p^2-22pq-8q^2)=-6p^3.$$
Puisque p et q sont premiers entre eux, le théorème de Gauss appliqué plusieurs fois permet d'affirmer que $p\big|8$ et $q\,|\,6$. Ainsi, $\mathrm{PGCD}\,(p\,,\,q)=1$, $p\in\{\pm1;\pm2;\pm4;\pm8\}$ et $q\in\{\pm1;\pm2;\pm3;\pm6\}$ et les solutions rationnelles appartiennent donc à $\{\pm\frac{1}{1};\pm\frac{1}{2};\pm\frac{1}{3};\pm\frac{1}{6};;\pm\frac{2}{1};\pm\frac{2}{3};\pm\frac{4}{1};\pm\frac{4}{3};\pm\frac{8}{1};\pm\frac{8}{3}\}$.
En testant les différentes valeurs possibles, il s'avère que $\frac{4}{3}$ est la seule racine rationnelle de B.

Exercice 31 Pour $a,\,b\in\mathbb{R}^*$, la plus petite période de $f(x)=\cos(ax)+\sin(bx)$ est $\dfrac{2\pi}{\mathrm{PGCD}\,(a\,,\,b)}$.

· Montrons tout d'abord que $T_0=\dfrac{2\pi}{c}$ où $c=a\wedge b$ est une période de f.
Il existe deux entiers a' et b' tels que $a=ca'$ et $b=cb'$ et pour tout réel x,
$$\begin{aligned} f(x+T_0) &= \cos(a(x+T_0))+\cos(b(x+T_0))=\cos(ax+aT_0)+\cos(bx+bT_0)\\ &= \cos(ax+a\tfrac{2\pi}{c})+\cos(bx+b\tfrac{2\pi}{c})=\cos(ax+2\pi a')+\cos(bx+2\pi b')\end{aligned}$$
$$f(x+T_0)=\cos(ax)+\sin(bx)=f(x).$$
T_0 est donc une période de f.
· Montrons ensuite que toute période de f est de la forme $\dfrac{2\pi k}{a\wedge b}$.

Soit T une période de la fonction f.
On a alors $\cos(ax + aT) = \cos(ax)$ et $\cos(bx + bT) = \cos(bx)$.
Or, la plus petite période de la fonction sinus et de la fonction cosinus est 2π donc il existe k et k' deux entiers tels que $bT = 2\pi k$ et $aT = 2\pi k'$. Ainsi, $T = \dfrac{2\pi k}{b} = \dfrac{2\pi}{\frac{b}{k}}$ et $T = \dfrac{2\pi k'}{a} = \dfrac{2\pi}{\frac{a}{k'}}$.
Posons $c = a \wedge b$. Il existe alors deux entiers a' et b' tels que $a = ca'$ et $b = cb'$ où $a' \wedge b' = 1$. On a alors $T = \dfrac{2\pi}{\frac{cb'}{k}}$ et $T = \dfrac{2\pi}{\frac{ca'}{k'}}$. Par conséquent, $\dfrac{b'}{k} = \dfrac{a'}{k'}$ ainsi $k'b' = ka'$. D'où a' divise $k'b'$ et d'après le théorème de Gauss, comme a' et b' sont premiers entre eux, a' divise k' : $k' = a'k''$ où k'' est un entier. On a donc $T = \dfrac{2\pi}{\frac{c}{k''}}$.
De même, b' divise alors ka' et d'après le théorème de Gauss, comme a' et b' sont premiers entre eux, b' divise k : $k = b'k'''$ où k''' est un entier. On a donc $T = \dfrac{2\pi}{\frac{c}{k'''}}$.
Finalement, $k'' = k'''$ et toute période de f est donc de la forme $T = \dfrac{2\pi k''}{c}$ où k'' est un entier naturel non nul et $c = a \wedge b$.
• Or $T_0 = \dfrac{2\pi}{a \wedge b}$ est une période de f. C'est donc la plus petite.

CORRIGÉS

Chapitre VII

GRAPHES

Sommaire

La théorie des graphes est la discipline mathématiques qui étudie les dessins abstraits de réseaux reliant des objets. Ces graphes peuvent modéliser de très nombreux réseaux (sociaux, informatiques, communications, transports mais aussi cartographiques, génétiques...) et sont utiles dans de nombreux domaines mathématiques (algèbre, probabilités, topologie...).

Nous ne traiterons ici que de graphes finis dans le plan. Je vous sens quelque peu déçus mais nous aurons déjà la possibilité d'utiliser les matrices et, plus tard, d'en voir des applications en probabilité.

Le résultat fondateur de cette théorie est dû à Leonhard Euler (1707 - 1783), éminent mathématicien et physicien suisse, membre de l'Académie royale des sciences de Prusse à Berlin. Euler fit d'importantes découvertes dans des domaines aussi variés que le calcul infinitésimal et la théorie des graphes. Il introduisit une grande partie de la terminologie et de la notation des mathématiques modernes : $f(x)$, e, i, $\sum$. Il est aussi connu pour ses travaux en mécanique, en dynamique des fluides, en optique et en astronomie ou en géométrie du triangle. Euler est considéré comme l'un des plus grands et des plus prolifiques mathématiciens de tous les temps et nous l'aurons croisé avec grande satisfaction tout au long de cette année.

Le problème historique, résolu par Euler en 1735, est le suivant. La ville de Königsberg (aujourd'hui Kaliningrad) est construite autour de deux îles situées sur le Pregel et reliées entre elles par un pont. Six autres ponts relient les rives de la rivière aux îles, l'une bénéficie d'un pont pour rejoindre chacune des rives et l'autre, deux.

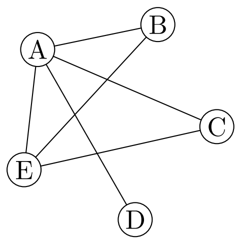
Le problème consiste à déterminer s'il existe ou non une promenade dans les rues de Königsberg permettant, à partir d'un point de départ au choix, de passer une et une seule fois par chaque pont, et de revenir à son point de départ, étant entendu qu'on ne peut traverser le Pregel qu'en passant sur les ponts. Qu'en pensez-vous ?

1 Graphes non orientés

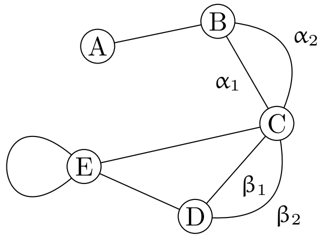
1.1 Définitions et premières propriétés

Définition 1
Un ***graphe non orienté*** *est un ensemble de sommets reliés par des arêtes.*
Deux sommets reliés par une arête sont dits ***adjacents*** *et une arête reliant deux sommets adjacents est dite* ***incidente*** *à ces deux sommets.*
Une arête est une ***boucle*** *si elle relie un sommet à lui-même.*
Un ***sous-graphe*** *d'un graphe est un graphe constitué de certains sommets ainsi que certaines arêtes reliant ces sommets.*
*L'***ordre*** *d'un graphe est le nombre total de ses sommets.*
Le ***degré*** *d'un sommet est le nombre d'arêtes incidentes à ce sommet, les boucles comptant pour deux.*
Un graphe est dit ***simple*** *si au plus une arête relie deux sommets et s'il ne contient aucune boucle.*

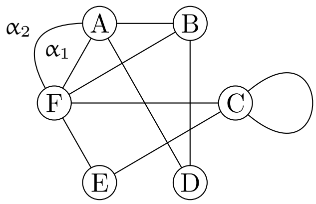
Exemples : Nous nous reporterons aux exemples numérotés tout au long de ce chapitre.



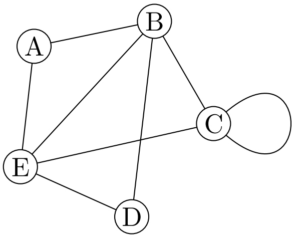
Graphe n° 1 :
Graphe simple d'ordre 5.
Les sommets A et B sont adjacents, tout comme B et E.
Les sommets B et C ne sont pas adjacents, tout comme D et E.
Ce graphe comporte 6 arêtes et les degrés de ses sommets sont deg(A) = 4, deg(B) = 2, deg(C) = 2, deg(D) = 1, deg(E) = 3.



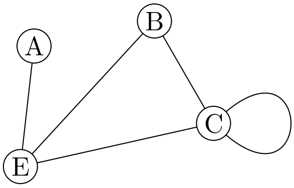
Graphe n° 2 :
Graphe d'ordre 5.
Les sommets A et B sont adjacents, tout comme E et C.
Les sommets B et E ne sont pas adjacents, tout comme A et C.
L'arête E-E est une boucle.
Les arêtes α_1 et α_2 sont incidentes aux sommets B et C.
Ce graphe comporte 8 arêtes et les degrés de ses sommets sont deg(A) = 1, deg(B) = 3, deg(C) = 5, deg(D) = 3, deg(E) = 4.



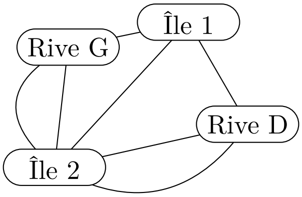
<u>Graphe n° 3</u> :
Graphe d'ordre 6.
Les sommets B et F sont adjacents et les sommets B et C ne le sont pas.
L'arête C-C est une boucle.
Ce graphe comporte 10 arêtes et les degrés de ses sommets sont $\deg(A) = 4$, $\deg(B) = 3$, $\deg(C) = 4$, $\deg(D) = 2$, $\deg(E) = 2$, $\deg(F) = 5$.



<u>Graphe n° 4</u> :
Graphe d'ordre 5.
Les sommets A et B sont adjacents, C et D ne le sont pas.
Ce graphe comporte 8 arêtes et les degrés de ses sommets sont $\deg(A) = 2$, $\deg(B) = 4$, $\deg(C) = 4$, $\deg(D) = 2$, $\deg(E) = 4$.



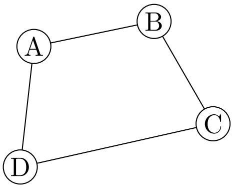
<u>Graphe n° 5</u> :
Graphe d'ordre 4, sous-graphe du graphe n° 4 précédent.
Les sommets A et B ne sont plus adjacents, B et E le restent.
Ce sous-graphe comporte 5 arêtes et les degrés de ses sommets sont $\deg(A) = 1$, $\deg(B) = 2$, $\deg(C) = 4$, $\deg(E) = 3$.

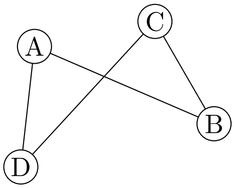


<u>Graphe des ponts de Königsberg</u> :
Graphe d'ordre 4.
Ce graphe comporte 7 arêtes et les degrés de ses sommets sont $\deg(G) = 3$, $\deg(D) = 3$, $\deg(1) = 3$, $\deg(2) = 5$.

<u>*Remarque*</u> :

Il ne faut pas confondre un graphe et son dessin. Un même graphe peut être représenté de différentes manières et la lisibilité de la visualisation est une question à ne pas négliger lors de la modélisation d'une situation.





Propriété 1
La somme des degrés de tous les sommets d'un graphe non orienté égale le double du nombre de ses arêtes.

Démonstration : En effet, pour chaque arête, il existe deux sommets donc chaque arête produit deux degrés. □

Exemples : Dans les graphes précédents, on a bien $\displaystyle\sum_{s \text{ sommet}} \deg(s) = 2 \times \#\,\text{arêtes}.$

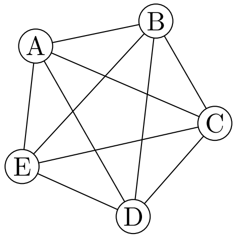
Propriété 2
Dans un graphe non orienté, le nombre de sommets de degré impair est pair.

Démonstration : S'il y en avait un nombre impair, alors la somme de tous les degrés serait impaire et ne pourrait alors être égale au double du nombre d'arêtes. □

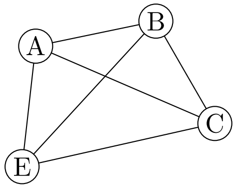
Exemples : Dans les graphes précédents, on a bien zéro, deux ou quatre sommets de degré impair.

Définition 2 *Un graphe simple non orienté est **complet** si tous ses sommets sont adjacents deux à deux.*

Exemples :



Graphe n° 6 :
Graphe complet d'ordre 5.
Ce graphe comporte 10 arêtes et les degrés de ses sommets sont deg(A) = 4, deg(B) = 4, deg(C) = 4, deg(D) = 4, deg(E) = 4.



Graphe n° 7 :
Graphe complet d'ordre 4, sous-graphe du graphe n° 6 précédent.
Ce graphe comporte 6 arêtes et les degrés de ses sommets sont deg(A) = 3, deg(B) = 3, deg(C) = 3, deg(E) = 3.

Il est parfois utile de faire appel à la notion suivante.

Définition 3 *Le graphe **complémentaire** d'un graphe simple non orienté G est un graphe simple H ayant les mêmes sommets et tel que deux sommets distincts de H sont adjacents si, et seulement si, ils ne sont pas adjacents dans G.*

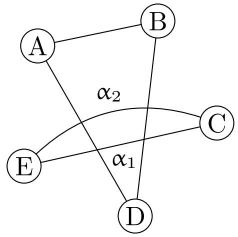
1.2 Parcourir un graphe

Définition 4 *Dans un graphe non orienté, on appelle **chaîne** toute suite de sommets consécutivement adjacents, éventuellement confondus.*
*La **longueur** d'une chaîne est le nombre d'arêtes la composant.*
*Une chaîne est dite **fermée** lorsque le premier et le dernier sommet de cette chaîne sont confondus.*
*Un **cycle** est une chaîne fermée dont toutes les arêtes sont distinctes.*

Exemples : Dans le graphe n° 1, BEACAE est une chaîne de longueur 5, DACEAD est une chaîne fermée de longueur 5 et ABECA est un cycle de longueur 4.

Définition 5
*Un graphe est **connexe** si deux sommets distincts quelconques peuvent être reliés par une chaîne.*

Exemple :



Graphe n° 8 :
Graphe non connexe d'ordre 5 car aucune chaîne ne relie les sommets A et C par exemple.
Ce graphe comporte 5 arêtes et les degrés de ses sommets sont deg(A) = 2, deg(B) = 2, deg(C) = 2, deg(D) = 2, deg(E) = 2.

Remarques : • S'il existe une chaîne passant par tous les sommets d'un graphe, alors celui-ci est connexe.

- Un graphe complet est toujours connexe. La réciproque est fausse (cf. n° 5).

Définition 6 *Une **chaîne eulérienne** est une chaîne contenant toutes les arêtes du graphe une et une seule fois.*
*Un **cycle eulérien** est une chaîne eulérienne fermée. Dans ce cas, on dit que l'on a un **graphe eulérien**.*

Exemples : Dans le graphe n° 1, DAEBACE est une chaîne eulérienne.
Dans le graphe n° 3, Fα_1Aα_2FECCFBADB est une chaîne eulérienne.
Dans le graphe n° 4, CCBAEBDEC est un cycle eulérien.

Théorème 1 ***Théorème d'Euler***
Un graphe non orienté connexe admet une chaîne eulérienne si, et seulement si, le nombre de sommets de degré impair vaut 0 *ou* 2.

Démonstration : On suppose qu'il existe une chaîne eulérienne dans un certain graphe. Notons v le sommet de départ et w le sommet d'arrivée de cette chaîne. Puisque cette chaîne passe par toutes les arêtes, on peut facilement compter les degrés de chaque sommet en suivant le chemin. En effet, on initialise tous les degrés à 0 et, à chaque fois que l'on passe par un sommet en suivant notre chaîne, on augmente son degré de 2 : une fois en arrivant en ce sommet et une fois en repartant. Au départ et à l'arrivée de la chaîne, on incrémente le degré de 1 seulement pour v et pour w. D'où, si $v \neq w$, ce sont les deux seuls sommets ayant un degré impair, alors que si $v = w$, tous les sommets sont de degré pair.
La réciproque est plus délicate. On suppose que v et w sont les deux seuls sommets de degré impair (s'il n'y en a pas, on prend $v = w$ quelconques). Puisque le graphe est connexe, il existe une chaîne reliant v à w. Si elle est eulérienne, on a fini. Sinon, le sous-graphe restant après suppression des arêtes parcourues n'admet que des sommets de degré pair et l'on peut agrandir notre chaîne en ajoutant une sous-chaîne tournant autour d'un sommet n'ayant pas toutes ses arêtes supprimées : cela est possible car les sommets étant de degré pairs, il y a toujours une sortie possible. Et l'on reproduit ceci pour chaque arête non encore parcourue. $\square$

Exemple : Construction d'une chaîne eulérienne sur le graphe 3.
Les seuls sommets de degré impairs sont B et F. Commençons donc par la chaîne BF puisqu'elle existe.
Autour de B, il reste deux arêtes et l'on remplace B par la chaîne BADB pour obtenir BADBF.
Autour de A, il reste deux arêtes et l'on remplace A par la chaîne AFA pour obtenir BAFADBF.
Autour de F, il reste deux arêtes et l'on remplace F par la chaîne FCEF pour obtenir BAFCEFADBF.
Autour de C, il reste une boucle et l'on remplace C par la chaîne CC pour obtenir BAFCCEFADBF.
Toutes les arêtes sont parcourues une seule fois par la chaîne eulérienne BAFCCEFADBF.

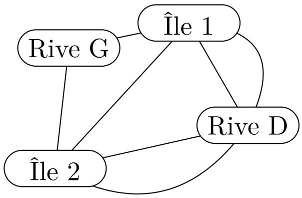
Les résultats suivants sont des conséquences du théorème d'Euler et de sa démonstration.

Propriété 3 *On considère un graphe non orienté connexe.*
• *S'il possède plus de deux sommets de degré impair, alors il ne possède pas de chaîne eulérienne.*
• *S'il possède deux sommets de degré impair, alors ce sont les extrémités de ses chaînes eulériennes.*
• *Il admet un cycle eulérien si, et seulement si, tous ses sommets sont de degré pair.*

Démonstration : • Le premier point est évident avec le théorème d'Euler.
• La démonstration du théorème d'Euler a montré que seules les extrémités d'une chaîne eulérienne peuvent être de degré impair.
• S'il admet un cycle eulérien, il faut qu'il admette une chaîne eulérienne donc qu'il possède zéro ou deux sommets de degré impair. D'après le point précédent, s'il en possède deux, ce sont les extrémités des chaînes eulériennes qui ne peuvent alors être des cycles. Il ne peut donc pas avoir de sommets de degré impair.
Réciproquement, s'il n'admet pas de sommets de degré impair, alors il admet nécessairement une chaîne eulérienne et d'après la démonstration du théorème d'Euler, on peut prendre $v = w$ comme début et fin de cette chaîne : c'est alors un cycle. □

Exemples : Les graphes n^{os} 2 et 7 possèdent quatre sommets de degré impair et le graphe n^{o} 8 n'est pas connexe donc ils n'admettent pas de chaîne eulérienne.
Les graphes n^{os} 1, 3 et 5 possèdent deux sommets de degré impair donc ils admettent des chaînes eulériennes.
Les graphes n^{os} 4 et 6 ne possèdent pas de sommet de degré impair donc ils admettent des cycles eulériens.
Par exemple, AEBCCE est une chaîne eulérienne du graphe n^{o} 5 et ABCDEACEBDA est un cycle eulérien du graphe n^{o} 6.
Puisque le graphe des ponts de Königsberg admet 4 sommets de degré impair, il n'était pas possible de s'y balader en franchissant chacun des ponts une unique fois, encore moins en revenant à son point de départ.

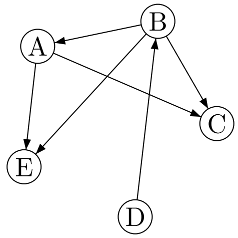
En revanche, si les habitants de Königsberg l'avaient vraiment voulu, il aurait été possible de faire une telle ballade après avoir déplacé un seul pont et sans modifier radicalement le système de circulation.
Le graphe ci-contre admet quatre sommets, tous de degré pair, donc il existe des cycles eulériens. Par exemple, G1D12D2G.
Un déplacement du type île1-riveD en île2-riveG aurait par contre modifié radicalement le plan de circulation.



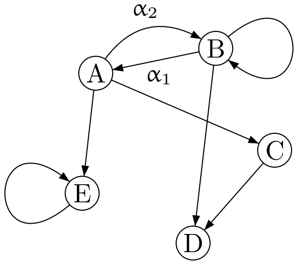
2 Graphes orientés

Définition 7 *Un graphe est dit* ***orienté*** *lorsque ses arêtes sont munies d'un sens de parcours, d'une origine à une extrémité. Les arêtes sont alors appelées* ***arcs*** *et les chaînes, appelées* ***chemins****, tiennent compte du sens de parcours. On parle alors de* ***degré entrant*** *pour le nombre d'arcs dirigés vers un sommet et de* ***degré sortant*** *pour le nombre d'arcs partant d'un sommet.*

Exemples :



Graphe n° 9 :
Graphe orienté simple d'ordre 5.
DBAC est un chemin de longueur 3.
Ce graphe comporte 6 arcs.
Les degrés entrants de ses sommets sont $\deg_e(A) = 1$, $\deg_e(B) = 1$, $\deg_e(C) = 2$, $\deg_e(D) = 0$, $\deg_e(E) = 2$.
Les degrés sortants de ses sommets sont $\deg_s(A) = 2$, $\deg_s(B) = 3$, $\deg_s(C) = 0$, $\deg_s(D) = 1$, $\deg_s(E) = 0$.



Graphe n° 10 :
Graphe orienté d'ordre 5.
ABBACD est un chemin de longueur 5.
Ce graphe comporte 8 arcs.
Les degrés entrants de ses sommets sont $\deg_e(A) = 1$, $\deg_e(B) = 2$, $\deg_e(C) = 1$, $\deg_e(D) = 2$, $\deg_e(E) = 2$.
Les degrés sortants de ses sommets sont $\deg_s(A) = 3$, $\deg_s(B) = 3$, $\deg_s(C) = 1$, $\deg_s(D) = 0$, $\deg_s(E) = 1$.

Remarques : • Les définitions et les propriétés précédentes s'appliquent dans le cas d'un graphe orienté, excepté la notion de graphe complet et le théorème d'Euler.

• Dans un graphe orienté, la somme des degrés entrants égale la somme des degrés sortants ainsi que le nombre d'arcs (il suffit de reprendre la démonstration de la propriété 1 en page 171).

3 Matrice d'adjacence d'un graphe

Définition 8 *Soit un graphe (orienté ou non) d'ordre $n \in \mathbb{N}^*$ dont les sommets sont numérotés de 1 à n.*
*La **matrice d'adjacence** de ce graphe est la matrice carrée de taille n où le terme $m_{i,j}$ de la i^e ligne et de la j^e colonne est égal au nombre d'arêtes (ou d'arcs) partant du sommet i et arrivant au sommet j.*

Exemples : On note M_i la matrice d'adjacence du graphe n° i précédent en classant les sommets par ordre alphabétique (G,D, 1, 2 pour Königsberg). Les voici.

$$M_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad M_5 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$M_6 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad M_7 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad M_8 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \end{pmatrix}$$

$$M_9 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad M_{10} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad M_K = \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \end{pmatrix}$$

Remarques : • La matrice d'adjacence d'un graphe non orienté est symétrique car toute arête reliant le sommet i au sommet j relie aussi le sommet j au sommet i.

• La matrice d'adjacence d'un graphe simple ne contient que des 0 sur la diagonale et des 0 ou des 1 partout ailleurs.

• On admettra que si l'ordre des sommets est modifié, la nouvelle matrice d'adjacence est semblable à la précédente : il existe une matrice inversible (dite de permutation) telle que $M' = PMP^{-1}$.

Théorème 2
Soient $n,\, k \in \mathbb{N}^*$ et M la matrice d'adjacence d'un graphe d'ordre n.
Le nombre de chaînes (ou de chemins) de longueur k reliant deux sommets i et j est donné par le terme $m_{i,j}^{(k)}$ de la i^e ligne et de la j^e colonne de la matrice M^k.

Démonstration : Elle s'effectue par récurrence sur k.
• On a $M^1 = M$ et, par définition de la matrice d'adjacence M, $m_{i,j}^{(1)} = m_{i,j}$ est

le nombre de chaînes (ou de chemins) de longueur 1 reliant le sommet i au sommet j : la propriété est vraie au rang $k = 1$.

• Supposons cette propriété vraie au rang $k \geqslant 1$. On a $M^{k+1} = M^k \times M^1$ donc, par définition de la multiplication matricielle, $m_{i,j}^{(k+1)} = \sum_{p=1}^{p=n} m_{i,p}^{(k)} m_{p,j}^{(1)}$.

On sait que $m_{i,p}^{(k)}$ est le nombre de chaînes (ou de chemins) de longueur k reliant le sommet i au sommet p

et $m_{p,j}^{(1)}$ est le nombre de chaînes (ou de chemins) de longueur 1 reliant le sommet p au sommet j

donc $m_{i,p}^{(k)} m_{p,j}^{(1)}$ est le nombre de chaînes (ou de chemins) de longueur $k+1$ reliant le sommet i au sommet j ayant le sommet p pour avant-dernier sommet.

On en déduit que $\sum_{p=1}^{p=n} m_{i,p}^{(k)} m_{p,j}^{(1)}$ est le nombre de chaînes (ou de chemins) de longueur $k+1$ reliant le sommet i au sommet j ayant l'un des sommets pour avant-dernier sommet, ce qui n'apporte pas de contrainte supplémentaire. La propriété est donc vraie au rang $k+1$.

• La propriété est vraie pour tout $k \in \mathbb{N}^*$. □

Exemples : ◦ On a $M_5^3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 5 & 5 \\ 2 & 5 & 7 & 6 \\ 3 & 5 & 6 & 3 \end{pmatrix}$ donc il existe 5 chaînes de longueur 3 reliant le sommet C et le sommet B dans le graphe n° 5 : CCEB, CECB, CBCB, CBEB et CCCB.

◦ On a $M_{10}^5 = \begin{pmatrix} 3 & 5 & 2 & 4 & 5 \\ 5 & 8 & 3 & 7 & 7 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ donc il existe 3 chemins de longueur 5 reliant le sommet B au sommet C dans le graphe n° 10 : BBABAC, BBBBAC et BABBAC mais aucun ne relie C à B.

<u>*Remarque*</u> : Si l'ordre des sommets est modifié, la nouvelle matrice d'adjacence est $M' = PMP^{-1}$, permutation de M, et l'on a

$(M')^k = (PMP^{-1})^k = PMP^{-1}PM...PMP^{-1} = PMI...IMP^{-1} = PM^kP^{-1}$, qui est la même permutation de M^k : ce théorème est bien indépendant de l'ordre des sommets.

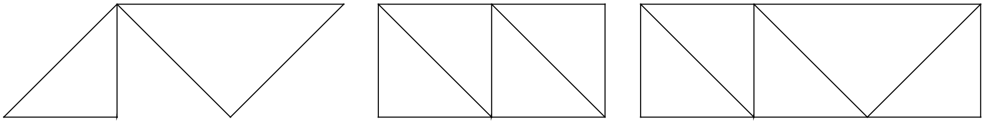
Exercices

GRAPHES

Lors de la construction d'une matrice d'adjacence, on classera les sommets par ordre alphabétique.

Exercice 1 Exercice de stylo

Dessiner les figures suivantes sans lever le stylo et sans passer deux fois sur les mêmes côtés.



Exercice 2 Salut toi, ça va toi ?

Lors d'une soirée, chacune des quatre personnes présentes serre la main à chacune des autres. Combien y a-t-il de poignées de main ?

Exercice 3 Le petit Nicolas et les copains

Clotaire s'est disputé avec Rufus, Eudes ne peut plus voir ni Agnan, ni Rufus, ni Marie-Edwige et Rufus est en colère contre Agnan. Combien d'amis Nicolas peut-il inviter au maximum sans risque ?

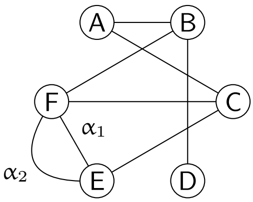
Exercice 4 Fight club

Les clubs de mathématiques des sept écoles de Villeneuve-la-Vieille souhaitent organiser des défis mutuels de telle sorte que chaque club en rencontre trois autres.

Peuvent-ils proposer un planning de rencontres ? Et si chaque club doit en rencontrer quatre ?

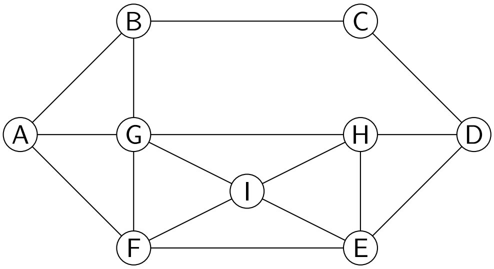
Exercice 5 Le graphe de sept sommets de degré quatre construit à l'exercice précédent admet-il un cycle eulérien ? En donner un le cas échéant.

Exercice 6 On considère le graphe ci-dessous.



1. Quel est son ordre ?
2. Est-il complet ?
3. Est-il simple ?
4. Admet-il une chaîne eulérienne ?
5. Combien de chaînes de longueur 3 relient les sommets E et C ? Les déterminer.

Exercice 7
Un touriste visite Villleneuve-la-Vieille dont le plan est schématisé ci-dessous.



1. Peut-il déambuler dans cette charmante cité et visiter chacun des points d'intérêt ?
2. Peut-il passer une et une seule fois dans chacune des rues du centre ?
3. (a) Peut-il passer une et une seule fois dans chacune des rues sauf une et si oui, laquelle ? Quel est alors un parcours possible ?

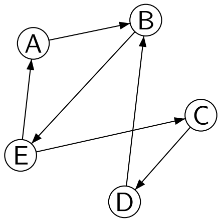
   (b) Peut-il le faire en revenant à son point de départ ?

Exercice 8 On considère un graphe complet d'ordre n.
Exprimer en fonction de n le degré des sommets ainsi que le nombre d'arêtes de ce graphe.

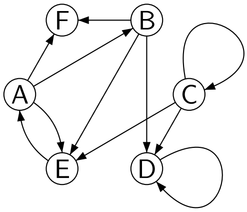
Exercice 9 Construire un graphe orienté dont les sommets sont les entiers de $[\![1\,;12]\!]$ et les arcs représentent la relation « est diviseur strict de ».

Exercice 10 On considère les graphes suivants.

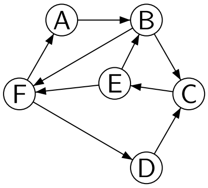
Graphe n° 1



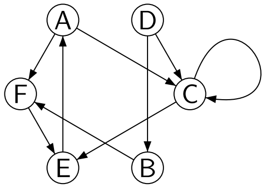
Graphe n° 2



Graphe n° 3



Graphe n° 4



1. Dans cette question, on ne tient pas compte de l'orientation.

   (a) Existe-t-il une chaîne reliant le sommet A au sommet D dans chacun des graphes ?

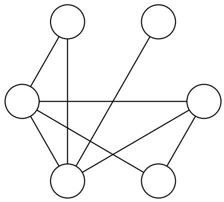
   (b) Ces graphes possèdent-ils une chaîne eulérienne ? Un cycle eulérien ? En déterminer le cas échéant.

   (c) Déterminer les matrices d'adjacence de ces graphes.

   (d) Combien de chaînes de longueur 3 reliant le sommet A au sommet D possèdent ces graphes ?

2. Mêmes questions en tenant compte de l'orientation cette fois-ci.

Exercice 11 On considère le graphe ci-dessous.



1. Retrouver l'emplacement des sommets A, B, C, D, E et F sachant que la matrice d'adjacence de ce graphe est
$$M = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$
2. Ce graphe admet-il une chaîne eulérienne ? En déterminer une le cas échéant.
3. Déterminer le nombre de chaînes de longueur 5 reliant le sommet C à lui-même puis les lister.

Exercice 12 Tracer des graphes de matrices d'adjacence suivantes.
$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 2 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \qquad M_3 = \begin{pmatrix} 0 & 2 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Exercice 13 Répondre aux questions suivantes sans tracer les graphes dont on donne la matrice d'adjacence $M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ puis vérifier en les traçant.

(a) Quel est l'ordre du graphe ?

(b) Quel est le degré de chacun des sommets ?

(c) Quel est le nombre d'arêtes du graphe ?

(d) Le graphe est-il complet ? Est-il simple ?

(e) La graphe admet-il une chaîne eulérienne ?

(f) Le graphe admet-il un cycle eulérien ?

Exercice 14 Que la montagne est belle

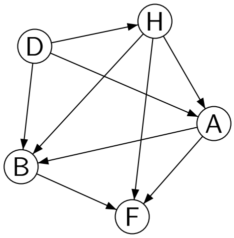
Un club alpin souhaite proposer à ses membres des randonnées itinérantes dans les Alpes avec des possibilités de nuitées dans les refuges suivants : Arête du Diable, Belvédère, Corne du Bouc, Drédanlpentu, Entonnoir, Fonduvallon, Grand Pic et Haute-Pointe. Ces refuges sont accessibles entre eux par des chemins de randonnées répartis de la manière suivante.

Refuge	A	B	C	D	E	F	G	H
Liaison	B,D	A,F,G,H	E,F	A,E	C,D,F,H	B,C,E,H	B,H	B,E,F,G

1. Le club peut-il proposer un itinéraire au départ du refuge du Fonduvallon qui emprunterait une et une seule fois chacun des sentiers ? Si oui, en proposer un.
2. Peut-il proposer un itinéraire de trois jours entre le refuge de l'Entonnoir et celui du Belvédère ? Si oui, combien peut-il en proposer et quelles sont-elles ?

Exercice 15 Parcours sportif

Le parcours sportif préféré de votre professeur de mathématiques favori est composé d'un banc pour les abdominaux, de haies et d'anneaux, d'un point de début et un de fin de parcours, organisés selon le plan ci-contre.



1. En petite forme aujourd'hui, votre professeur souhaite réaliser un parcours de trois sentiers seulement. Est-ce possible ? Combien a-t-il de possibilités ? Les lister.
2. Des travaux sont envisagés afin d'ajouter une barre de traction et des nouveaux sentiers. La nouvelle matrice d'adjacence serait alors $N = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$.

   Dresser le plan du parcours rénové.

Exercice 16 Listes graphiques

1. Une liste décroissante d'entiers est graphique s'il existe un graphe simple non orienté connexe dont les degrés des sommets correspondent à cette liste. Les listes suivantes sont-elles graphiques ?
   (a) $3, 3, 2, 1, 1.$
   (b) $3, 3, 2, 2.$
   (c) $4, 2, 1, 1, 1, 1.$
   (d) $5, 3, 2, 1, 1, 1.$
   (e) $3, 2, 2, 2, 1.$
   (f) $5, 4, 2, 2, 1.$
2. Pour les graphes simples orientés connexes, il faut considérer les couples d'entiers où le premier élément correspond au degré entrant et le second, au degré sortant. Les listes suivantes sont-elles graphiques ?
   (a) $(0, 1), (1, 1), (1, 1), (1, 1), (1, 0).$
   (b) $(1, 1), (1, 1), (1, 1), (1, 1), (1, 1).$
   (c) $(0, 2), (1, 1), (1, 1), (1, 1).$
   (d) $(0, 2), (1, 1), (1, 1), (2, 0).$
   (e) $(1, 2), (1, 2), (2, 1), (2, 1).$
   (f) $(1, 2), (1, 2), (2, 1), (2, 2), (1, 1).$

Exercice 17 Deux fois sept ponts...

Peut-on traverser les sept ponts de Königsberg en empruntant deux fois chaque pont, une fois dans un sens, une fois dans l'autre ?

EXERCICES

Exercice 18 Tchin-tchin

Lors d'une soirée festive, les convives ont tous trinqué une fois les uns avec les autres et j'ai entendu 45 tintements de verres. Combien étions-nous ?

Exercice 19 Vroum vroum

Les onze grandes villes de l'Autostan, dont la capitale Carville, sont chacune reliées par autoroute à cinq autres au moins. Peut-on aller, en empruntant l'autoroute, de Carville à chacune des autres grandes villes ?

Exercice 20 Qui est-ce ?

Montrez que dans un groupe de six personnes, il y en a nécessairement trois qui se connaissent mutuellement ou trois qui ne se connaissent pas mutuellement.
Montrer que cela n'est plus vrai dans un groupe de cinq personnes.

Exercice 21 Drôles d'associations

Un groupe de personnes est tel que chaque personne est membre d'exactement deux associations, chaque association comprend exactement trois membres et deux associations quelconques ont toujours exactement un membre en commun. Combien y a-t-il de personnes et d'associations ?

Exercice 22 Les amis de mes amis

Dans un groupe, y a-t-il toujours deux personnes ayant le même nombre d'amis présents ?

Pointez vers la page 311 afin de réaliser le devoir n° 11.

Corrigé des exercices

Graphes

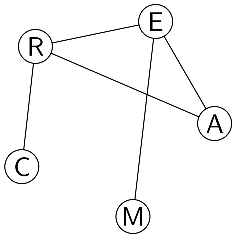
Exercice 1 Exercice de stylo

Pas si difficile, non ? On sait maintenant que cela est possible car les sommets de degré impairs sont au plus deux.

Exercice 2 Salut toi, ça va toi ?

Si on décompte les poignées de mains convive par convive, Agathe a serré trois mains, Betty en a serré deux autres, Colette une de plus et les poignées de mains de Jeanne ont déjà été comptées. Il y a donc eu 3+2+1=6 poignées de mains. Sinon, la somme des degrés (4×3) égale le double du nombre d'arêtes (2×6).

Exercice 3 Le petit Nicolas et les copains



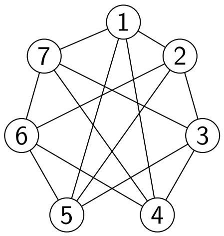
Ce graphe illustre les relations difficiles entre les amis de Nicolas. Il comporte 5 arêtes donc le graphe complémentaire des relations amicales en comporte 5 puisque le graphe complet en comporte $4+3+2+1=10$. Avec 5 arêtes, on ne peut tracer un graphe complet d'ordre 4 (qui comporte 6 arêtes) mais on peut en tracer un d'ordre 3 et, en effet, le sous-graphe A, M, C est bien un graphe complet de relations amicales.

Nicolas peut donc sans risque inviter trois amis : Agnan, Marie-Edwige et Clotaire.

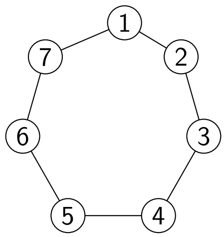
Exercice 4 Fight club

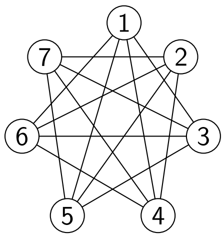
Une répartition de sept clubs rencontrant chacun trois autres clubs mènerait à un graphe comportant 7 sommets, tous de degré 3. La somme des degré serait alors égale à $7 \times 3 = 21$ ce qui est impossible car cette somme doit être le double du nombre des arêtes du graphe.

Si les clubs doivent en rencontrer quatre autres, on peut proposer l'organisation ci-contre.



On peut aussi passer par le graphe complémentaire des rencontres non disputées où les sommets sont tous de degré 2 ce qui est plus facile à construire et ensuite revenir au graphe des rencontres disputées. Cela donne la construction suivante.





Exercice 5 Le graphe l'exercice précédent ne comporte que des sommets de degré pair et admet donc des cycles eulériens. En voici un pour la première répartition 126 523 415 374 671 et pour la seconde, 137 524 614 736 251.

Exercice 6 Ce graphe est d'ordre 6. Il n'est pas complet car A et F ne sont pas adjacents par exemple. Il n'est pas simple car E et F admettent deux arêtes incidentes. Il n'admet pas de chaîne eulérienne car 4 sommets sont de degré impair : B, C, D et E. Il y a 7 chaînes de longueur 3 reliant E et C : Eα_1Fα_2EC, Eα_2Fα_1EC, Eα_1Fα_1EC, Eα_2Fα_2EC, ECEC, ECAC, ECFC.

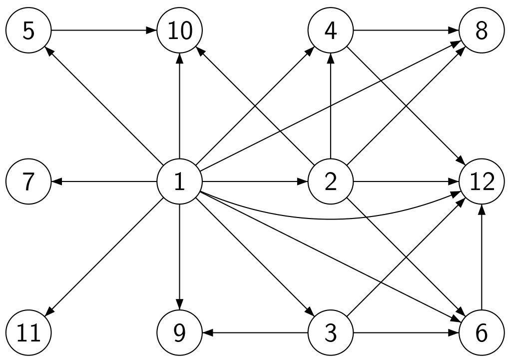
Exercice 7 Tourisme dans Villleneuve-la-Vieille

1. Ce touriste peut déambuler dans cette charmante cité et visiter chacun des points d'intérêt car le graphe est connexe.
2. Puisque le graphe comporte au moins trois sommets de degré impair (A, B et G par exemple), il n'admet pas de chaîne eulérienne et le touriste ne peut pas passer une et une seule fois dans chacune des rues du centre
3. (a) En évitant la rue AG (ou la rue BG ou AB), le graphe ne comporte plus que deux sommets de degré impair et admet donc une chaîne eulérienne. Le touriste peut alors passer dans chacune des rues restantes une et une seule fois, par exemple, en suivant le parcours BAFEIHGIFGBCDEHD.

   (b) En revanche, il ne peut pas le faire en revenant à son point de départ car le graphe comporte encore des sommets de degré impair donc il n'admet pas de cycle eulérien.

Exercice 8 On considère un graphe complet d'ordre n. Puisque chaque sommet est adjacent à tous les autres sommets, il est de degré $n-1$. Il y a donc la moitié de la somme des degrés, c.-à-d. $\frac{1}{2}n(n-1)$, arêtes.
On peut en effet les compter : $n-1$ arêtes partent d'un premier sommet, $n-2$ restent pour un second, $n-3$ pour le suivant,... , 1 pour l'avant-dernier et 0 pour le dernier car elles ont toutes déjà été comptabilisées.
Il y a donc $(n-1)+(n-2)+\ldots+1=\frac{(n-1+1)(n-1)}{2}=\frac{1}{2}n(n-1)$ arêtes dans un graphe complet d'ordre n.

Exercice 9
Voici un graphe orienté lisible représentant la relation « est diviseur strict de ».



Exercice 10

1. Sans orientation.
   (a) Ces graphes non orientés étant tous les quatre trivialement connexes, il existe bien une chaîne reliant le sommet A au sommet D.
   (b) · Le graphe n° 1 comporte deux sommets de degré impair (B et E) donc il n'admet pas de cycle eulérien mais bien des chaînes eulériennes. En voici une : BDCEABE.
   · Le graphe n° 2 ne comporte que des sommets de degré pair donc il admet des cycles et donc des chaînes eulériennes. En voici un : BFAEABECCDDB.
   · Le graphe n° 3 comporte deux sommets de degré impair (C et E) donc il n'admet pas de cycle eulérien mais bien des chaînes eulériennes. En voici une : EBFABCDFEC.
   · Le graphe n° 4 comporte quatre sommets de degré impair (A, C, E et F) donc il n'admet ni cycle ni chaînes eulériens.
   (c) Voici les matrices d'adjacence de ces graphes :

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 2 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \quad \text{et} \quad M_4 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

   (d) En calculant le terme $m_{1,4}^{(3)}$ de la première ligne et quatrième colonne des matrices cubes des matrices précédentes, on obtient le nombre de chaînes de longueur 3 reliant le sommet A au sommet D : 2 chaînes pour le graphe n° 1, 6 chaînes pour le graphe n° 2, 2 chaînes pour le graphe n° 3 et 3 chaînes pour le graphe n° 4.
2. Avec orientation.
   (a) Ces graphes étant orientés, il nous faut trouver le chemin éventuel reliant le sommet A au sommet D : ABECD pour le graphe n° 1, ABD pour le graphe n° 2, ABCEFD pour le graphe n° 3. Quant au graphe n° 4, il n'en existe pas car le sommet D est inaccessible.
   (b) Ces graphes étant orientés, les éventuels chemins et cycles eulériens non orientés n'en sont plus nécessairement. En revanche, s'ils n'en n'admettent pas lorsque non orientés, il ne peuvent en admettre lorsqu'orientés.
   · Le graphe n° 1 n'admet toujours pas de cycle eulérien mais bien un chemin eulérien orienté : EABECDB.
   · Le graphe n° 2 ne comporte ni chemin ni cycle eulériens car on devrait atteindre deux fois le sommet F sans pouvoir en repartir.
   · Le graphe n° 3 n'admet toujours pas de cycle eulérien mais bien un chemin eulérien orientée : EFABFDCEBC.
   · Le graphe n° 4 n'admet toujours pas de cycle ni de chemin eulériens.

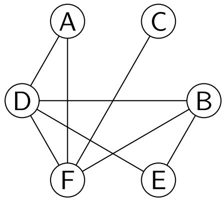
(c) Voici les matrices d'adjacence de ces graphes :

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{et} \quad M_4 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

(d) En calculant le terme $m_{1,4}^{(3)}$ de la première ligne et quatrième colonne des matrices cubes des matrices précédentes, on obtient le nombre de chemins de longueur 3 reliant le sommet A au sommet D : 0 chemin pour le graphe n° 1, 1 chemin pour le graphe n° 2, 1 chemin pour le graphe n° 3 et 0 chemin pour le graphe n° 4 (nous le savions).

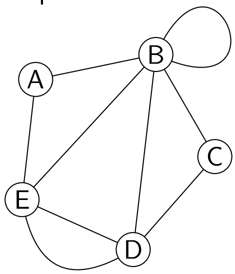
Exercice 11



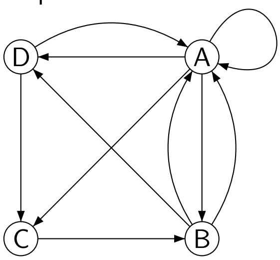
1. D'après la matrice d'adjacence, le sommet C n'est relié qu'au sommet F ce qui permet de les retrouver dans le graphe. On place ensuite le sommet A, relié à F et à D, sommet que l'on positionne alors. Le dernier sommet relié à F manquant est B. Il ne nous reste plus qu'à écrire E.
2. Ce graphe admet deux sommets de degré impair donc des chaînes (mais pas de cycle eulérien). Par exemple, CFDAFBEDB
3. Le troisième terme diagonal de la matrice M^5 donne le nombre de chaînes de longueur 5 reliant le sommet C à lui-même. Il y en a quatre qui sont : CFDAFC, CFADFC, CFBDFC, CFDBFC

Exercice 12 Voici des graphes correspondants aux matrices d'adjacence données.

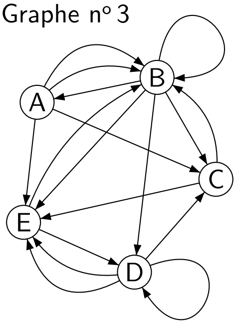
Graphe n° 1



Graphe n° 2



Graphe n° 3



Exercice 13

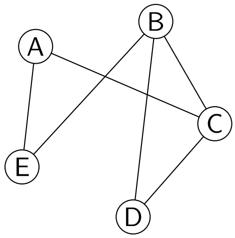
1. La matrice d'adjacence M_1 du graphe Γ_1 est symétrique donc on peut supposer le graphe non orienté.
   (a) Γ_1 est d'ordre 5.
   (b) En sommant les coefficients ligne par ligne, on obtient $\deg(\mathsf{A}) = 2$, $\deg(\mathsf{B}) = 3$, $\deg(\mathsf{C}) = 3$, $\deg(\mathsf{D}) = 2$ et $\deg(\mathsf{E}) = 2$.

(c) La somme des degrés valant $2+3+3+2+2=12$, le graphe Γ_1 comporte $\frac{12}{2}=6$ arêtes.

(d) Le graphe Γ_1 n'est pas complet car le sommet A n'est pas relié au sommet B par exemple.
Γ_1 est simple car il ne comporte ni boucle ni adjacence multiple.

(e) Ayant exactement deux sommets de degré impair, Γ_1 admet une chaîne eulérienne.

(f) Ayant des sommets de degré impair, Γ_1 n'admet pas de cycle eulérien.
Voici un graphe Γ_1 compatible.



2. La matrice d'adjacence M_2 du graphe Γ_2 n'est pas symétrique donc le graphe est non orienté.

(a) Γ_2 est d'ordre 5.

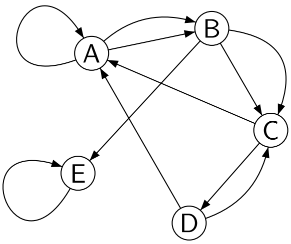
(b) En sommant les coefficients ligne par ligne, on obtient $\deg_s(\mathsf{A})=3$, $\deg_s(\mathsf{B})=3$, $\deg_s(\mathsf{C})=2$, $\deg_s(\mathsf{D})=2$ et $\deg_s(\mathsf{E})=1$.
En sommant les coefficients colonne par colonne, on obtient $\deg_e(\mathsf{A})=3$, $\deg_e(\mathsf{B})=2$, $\deg_e(\mathsf{C})=3$, $\deg_e(\mathsf{D})=1$ et $\deg_e(\mathsf{E})=2$.

(c) La somme des degrés entrants valant 11 (tout comme celle des degrés sortants), le graphe Γ_2 comporte 11 arcs.

(d) La notion de graphe complet n'est pas pertinente dans le cadre orienté.
Γ_2 n'est pas simple car il comporte une boucle en A entre autres.

(e) En sommant les degrés entrant et sortants, on obtient les degrés non orientés suivants : $\deg(\mathsf{A})=6$, $\deg(\mathsf{B})=5$, $\deg(\mathsf{C})=5$, $\deg(\mathsf{D})=3$ et $\deg(\mathsf{E})=3$. Ayant au moins trois sommets de degré impair, Γ_2 n'admet pas de chaîne eulérienne non orientée donc certainement pas de chemin eulérien orienté.

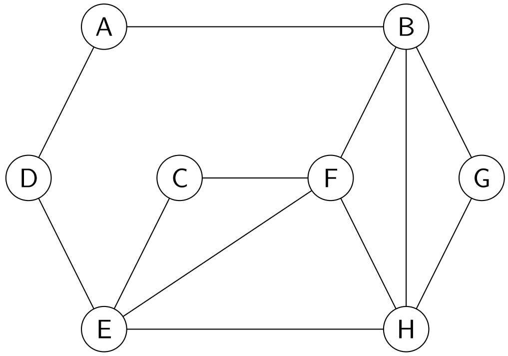
(f) N'admettant pas de chaîne eulérienne, Γ_2 ne peut admettre de cycle eulérien.
Voici un graphe Γ_2 compatible.



CORRIGÉS

Exercice 14 Que la montagne est belle

Voici un plan compatible avec le tableau des liaisons pédestres.



1. Aucun refuge n'est de degré impair. Il existe donc des cycles eulériennes dans le graphe modélisant cette situation. En voici un : FCEDABGHBFEHF.
2. La matrice d'adjacence de ce graphe est $M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

   et le terme $m_{5,2}^{(3)}$ de la cinquième ligne et troisième colonne de la matrice M^3 donne cinq randonnées de trois jours possibles entre le refuge de l'Entonnoir et celui du Belvédère. Ce sont EDAB, EHGB, EHFB, ECFB et EFHB.

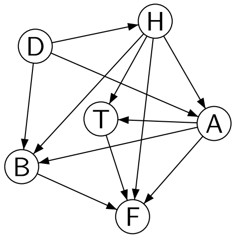
Exercice 15 Parcours sportif

1. Votre professeur peut par exemple réaliser le parcours de trois sentiers suivant : DABF.

   La matrice du graphe de ce parcours est, par ordre alphabétique ABDFH,

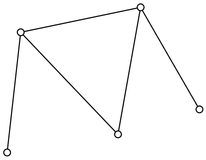
   $M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ et le terme $m_{3,4}^{(3)}$ de la troisième ligne et quatrième colonne de la matrice M^3 vaut 3.

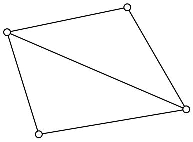
   Les trois parcours de trois sentiers possibles sont : DABF, DHAF et DHBF.

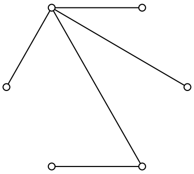


2. T étant la dernière lettre par ordre alphabétique, on complète le graphe en regardant la dernière ligne et la dernière colonne de la matrice N : on ajoute les arcs AT, HT et TF et l'on obtient le graphe ci-contre.

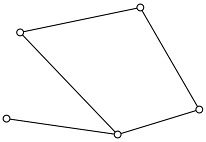
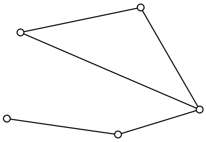
Exercice 16 Listes graphiques

1. (a) $3,\ 3,\ 2,\ 1,\ 1$ est graphique : 

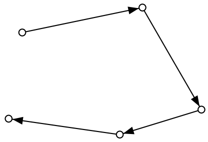
   (b) $3,\ 3,\ 2,\ 2$ est graphique : 

   (c) $4,\ 2,\ 1,\ 1,\ 1,\ 1$ est graphique : 

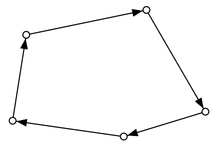
   (d) $5,\ 3,\ 2,\ 1,\ 1,\ 1$ n'est pas une liste graphique car la somme des degrés serait impaire.

   (e) $3,\ 2,\ 2,\ 2,\ 1$ est graphique :  et 

   (f) $5,\ 4,\ 2,\ 2,\ 1$ n'est pas graphique car un sommet d'un graphe simple d'ordre 5 est de degré inférieur ou égal à 4.

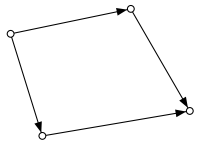
2. (a) $(0\,,1)$, $(1\,,1)$, $(1\,,1)$, $(1\,,1)$, $(1\,,0)$ est graphique : 

(b) $(1\,,1)$, $(1\,,1)$, $(1\,,1)$, $(1\,,1)$, $(1\,,1)$ est graphique :

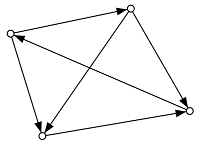


(c) $(0\,,2)$, $(1\,,1)$, $(1\,,1)$, $(1\,,1)$ n'est pas graphique car la somme des degrés entrants n'égale pas celle des degrés sortants.

(d) $(0\,,2)$, $(1\,,1)$, $(1\,,1)$, $(2\,,0)$ est graphique :



(e) $(1\,,2)$, $(1\,,2)$, $(2\,,1)$, $(2\,,1)$ est graphique :



(f) $(1\,,2)$, $(1\,,2)$, $(2\,,1)$, $(2\,,2)$, $(1\,,1)$ n'est pas graphique car la somme des degrés entrants n'égale pas celle des degrés sortants.

Exercice 17 Deux fois sept ponts...
Il est possible de traverser les sept ponts de Königsberg en empruntant deux fois chaque pont, une fois dans un sens, une fois dans l'autre en empruntant le chemin 1G1D12D2D2G2G21.

Exercice 18 Tchin-tchin
Puisque tous ont trinqué les uns avec les autres, nous cherchons l'ordre un graphe complet comportant 45 arêtes. On a vu à l'exercice 8 que le nombre d'arêtes d'un graphe complet d'ordre n vaut $\frac{n(n-1)}{2}$ et l'on résout l'équation $\frac{n(n-1)}{2} = 45 \Leftrightarrow n^2 - n - 90 = 0$ $\Leftrightarrow n = -9$ ou $n = 10$. Nous étions donc dix convives.

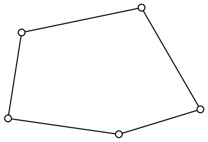
Exercice 19 Vroum vroum
Le graphe est-il connexe ? Supposons qu'il ne l'est pas et que six des grandes villes sont reliées entre elles uniquement et forment donc un sous-graphe complet d'ordre 6, tous les sommets étant d'ordre 5. Les cinq villes restantes ne peuvent alors être reliées qu'à quatre villes seulement et seraient alors d'ordre au plus 4 et non 5. Cet argument est encore plus évident si l'on tente de séparer quatre villes ou moins. Le graphe est donc connexe et l'on peut donc relier Carville à chacune des autres grandes villes de l'Autostan en empruntant l'autoroute.

Exercice 20 Qui est-ce ?

Supposons tout d'abord qu'il existe une personne, disons A, qui en connaît trois autres, disons B, C et D, et considérons les relations entre B, C et D. Si deux d'entre elles se connaissent (par exemple B et C) alors elles forment avec A un trio de personnes se connaissant mutuellement. Dans le cas contraire, B, C et D forment un trio ne se connaissant pas.

Si aucune personne n'en connaît trois autres, on raisonne de façon symétrique en considérant la personne A et trois personnes qu'elle ne connaît pas : si ces trois personnes se connaissent mutuellement, c'est gagné. Sinon, deux personnes parmi ces trois ne se connaissant pas forment avec A un trio de personnes ne se connaissant pas.

Le graphe suivant montre que la situation est différente pour un groupe de cinq personnes : tout triplet de personnes contient 1 ou 2 arêtes.



Exercice 21 Drôles d'associations

Supposons que nous avons n associations et considérons le graphe complet K_n dont les sommets représentent les associations : toute paire d'associations est donc reliée par une arête. Deux associations ayant toujours exactement un membre en commun, nous pouvons étiqueter l'arête reliant ces deux associations par le membre en question. Par ailleurs, chaque personne étant membre d'exactement deux associations, une même personne ne peut pas étiqueter deux arêtes distinctes, sinon elle appartiendrait à au moins trois associations. Il y a donc autant d'arêtes que de personnes. Finalement, chaque association comprenant exactement trois personnes, tous les sommets du graphe complet sont de degré 3. Il s'agit donc de K_4 : le nombre d'associations est donc de 4 (nombre de sommets) et le nombre de personnes de 6 ($\frac{4\times3}{2}$).

Exercice 22 Les amis de mes amis

Construisons un graphe dont les sommets représentent les personnes et plaçons une arête entre deux sommets lorsque les personnes correspondantes sont amies. Dire que deux personnes ont le même nombre d'amis revient à dire que deux sommets dans le graphe ont même degré. Nous allons montrer qu'il n'existe aucun graphe dont tous les sommets ont des degrés distincts. Supposons qu'un tel graphe existe et qu'il possède n sommets. Le degré maximal d'un sommet est donc $n-1$. Si tous les degrés des sommets sont distincts, on a donc nécessairement un sommet de degré 0, un sommet de degré 1, ..., un sommet de degré $n-1$. Du fait de la présence d'un sommet de degré 0, il est impossible d'avoir un sommet de degré $n-1$: en effet, celui-ci devrait être relié à tous les autres, y compris celui de degré 0. On obtient ainsi une contradiction et dans un groupe, il y a toujours deux personnes ayant le même nombre d'amis présents

Chapitre VIII

NOMBRES COMPLEXES : COMPLÉMENTS

Sommaire

Voici déjà le dernier chapitre de l'année sur les nombres complexes. Celui-ci n'est constitué que de diverses applications plus ou moins directes et d'une seule notion nouvelle mais il n'en est pour autant pas moins utile ou intéressant. Ce sera l'occasion de résoudre des problèmes plus complets et généraux dans la planche d'exercices qui lui est dédiée.

1 Rappels

Puisque le rédacteur est naturellement compatissant et magnanime, il a rédigé ce paragraphe qui recense quelques-unes des définitions et propriétés déjà étudiées. L'ensemble des nombres complexes est en effet bien plus riche que compliqué.

Le plan est muni d'un repère orthonormé direct $(O\,;\,\vec{u},\,\vec{v})$.

$\mathbb{C} = \{z = a + ib \;/\; a \in \mathbb{R} \text{ et } b \in \mathbb{R}\} = \{z = re^{i\theta} = r(\cos\theta + i\sin\theta) \;/\; r \geqslant 0 \text{ et } \theta \in \mathbb{R}\}$

Les opérations usuelles dans $\mathbb{R}$ se prolongent naturellement dans $\mathbb{C}$ avec $i^2 = -1$.

$$|z| = \sqrt{a^2+b^2} = r \qquad \arg(z) \equiv \theta\,[2\pi] \qquad \overline{z} = a - ib \qquad z\overline{z} = |z|^2$$

Les opérations usuelles « passent à travers » la conjugaison complexe :

$$\overline{z+z'} = \overline{z} + \overline{z'}, \quad \overline{zz'} = \overline{z}\,\overline{z'}, \quad \text{etc}$$

$$e^{i\theta} = \cos\theta + i\sin\theta \qquad e^{i\theta}e^{i\theta'} = e^{i(\theta+\theta')} \qquad \overline{e^{i\theta}} = e^{-i\theta} = \frac{1}{e^{i\theta}} \qquad (e^{i\theta})^n = e^{in\theta}$$

L'ensemble $\mathbb{U}$ est l'ensemble des nombres complexes de module 1 :
$\mathbb{U} = \{z \in \mathbb{C} / |z| = 1\} = \{e^{i\theta} / \theta \in \mathbb{R}\}$.
Dans le plan complexe, $\mathbb{U}$ correspond précisément aux points du cercle trigonométrique.
La notation exponentielle permet de retrouver les formules de trigonométrie :
$\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$, $\sin(a+b) = \sin(a)\cos(b) + \sin(b)\cos(a)$,
$\cos(2a) = \cos^2(a) - \sin^2(a) = 2\cos^2(a) - 1 = 1 - 2\sin^2(a)$,
$\sin(2a) = 2\sin(a)\cos(a)$,...
On obtient de plus la formule de Moivre : $[\cos\theta + i\sin\theta]^n = \cos(n\theta) + i\sin(n\theta)$.
$|zz'| = |z|\,|z'|$, $\arg(zz') \equiv \arg(z) + \arg(z')\,[2\pi]$, etc
Le polynôme à coefficients réels $az^2 + bz + c$ admet toujours des racines.
Si $\Delta < 0$, ce sont $\dfrac{-b \pm i\sqrt{-\Delta}}{2a}$.
Tout polynôme non nul de degré n admet au plus n racines distinctes.
Tout polynôme s'annulant en $a \in \mathbb{C}$ se factorise par $z - a$.
En particulier, $z^n - a^n = (z-a)\sum_{i=0}^{n-1} a^k z^{n-1-k}$.
Formule du binôme de Newton : $\forall u, v \in \mathbb{C}$, $(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^{n-k} v^k$.

2 Interprétations géométriques

Propriété 1
Si A et B sont deux points du plan complexe d'affixes respectives a et b, alors
$$\boldsymbol{AB = |b-a|} \quad \textit{et} \quad \left(\overrightarrow{u}\,;\overrightarrow{AB}\right) \equiv \mathbf{arg}(\boldsymbol{b-a})\,[\boldsymbol{2\pi}].$$

Démonstration : • Soit M l'unique point tel que $\overrightarrow{OM} = \overrightarrow{AB}$.
On a alors $z_M = z_{\overrightarrow{OM}} = z_{\overrightarrow{AB}} = z_B - z_A = b - a$.
Il en résulte que $|z_M| = |b-a|$
et donc $AB = OM = \|\overrightarrow{OM}\| = \left|z_{\overrightarrow{OM}}\right| = |z_M| = |b-a|$.
• Par ailleurs, $\left(\overrightarrow{u}\,;\overrightarrow{AB}\right) \equiv \left(\overrightarrow{u}\,;\overrightarrow{OM}\right) = \arg(z_{\overrightarrow{OM}}) = \arg(z_M) = \arg(b-a)$. □

Exemple : Soient $P(1+2i)$, $Q(2)$ et $R(-1+i)$ trois points du plan complexe.
On a $PQ^2 = |z_Q - z_P|^2 = |2-(1+2i)|^2 = |1+2i|^2 = 1^2 + 2^2 = 5$ et
$PR^2 = |z_R - z_P|^2 = |(-1+i)-(1+2i)|^2 = |-2-i|^2 = 2^2 + 1^2 = 5$: le triangle PQR est isocèle en P.

Propriété 2 *Si A, B, C et D sont quatre points du plan complexe d'affixes respectives a, b, c et d, alors*
$$\left(\overrightarrow{AB}\,;\overrightarrow{CD}\right) \equiv \mathbf{arg}\left(\frac{\boldsymbol{d-c}}{\boldsymbol{b-a}}\right)\,[\boldsymbol{2\pi}].$$

Démonstration : $\left(\overrightarrow{AB}\,;\overrightarrow{CD}\right) \equiv \left(\overrightarrow{AB}\,;\overrightarrow{u}\right) + \left(\overrightarrow{u}\,;\overrightarrow{CD}\right)$
$\left(\overrightarrow{AB}\,;\overrightarrow{CD}\right) \equiv \left(\overrightarrow{u}\,;\overrightarrow{CD}\right) - \left(\overrightarrow{u}\,;\overrightarrow{AB}\right) \equiv \arg(d-c) - \arg(b-a) \equiv \arg\left(\frac{d-c}{b-a}\right)\ [2\pi]$
en utilisant la notation exponentielle par exemple (cf. théorème 3 p.113). □

Exemple : Soient les trois points $P(1+2i)$, $Q(2)$ et $R(-1+i)$ de l'exemple précédent et soit $S(4i)$.
◦ On a $\frac{z_S-z_Q}{z_P-z_S} = \frac{-2+4i}{1-2i} = \frac{-2(1-2i)}{1-2i} = -2$
donc $\left(\overrightarrow{SP}\,;\overrightarrow{QS}\right) \equiv \arg(-2)\,[2\pi] \equiv \pi\,[2\pi]$ et les points P, Q et S sont alignés.
◦ On a $\frac{z_Q-z_S}{z_P-z_R} = \frac{2-4i}{2+i} = \frac{(2-4i)(2-i)}{2^2+1^2} = \frac{4-2i-8i+4i^2}{5} = -2i$ donc
$\left(\overrightarrow{RP}\,;\overrightarrow{SQ}\right) \equiv \arg(-2i)\,[2\pi] \equiv -\frac{\pi}{2}\,[2\pi]$ et les droites (RP) et (SQ) sont perpendiculaires.
Le triangle PQR est donc aussi rectangle en P.

Le théorème suivant se déduit immédiatement de la propriété 1 et traduit en termes de nombres complexes des propriétés de géométrie classique.

Théorème 1
- $M_z \in Cercle(A_a; r) \iff |z-a| = r.$
- $M_z \in Médiatrice[A_aB_b] \iff |z-a| = |z-b|.$
- $M_z \in Cercle(\varnothing(A_aB_b)) \setminus \{A; B\} \iff \arg\left(\dfrac{z-b}{z-a}\right) \equiv \dfrac{\pi}{2}\,[\pi].$

Démonstration : · $M_z \in Cercle(A_a; r) \iff AM = r \iff |z-a| = r.$
· $M_z \in Médiatrice[A_aB_b] \iff AM = BM \iff |z-a| = |z-b|.$
· $M_z \in Cercle(\varnothing[A_aB_b]) \setminus \{A; B\} \iff (MA) \perp (MB) \iff \left(\overrightarrow{AM}\,;\overrightarrow{BM}\right) \equiv \frac{\pi}{2}\,[\pi]$
$\iff \arg\left(\frac{z-b}{z-a}\right) \equiv \frac{\pi}{2}\,[\pi].$ □

Exemples : Soient les quatre points $P(1+2i)$, $Q(2)$, $R(-1+i)$ et $S(4i)$ des exemples précédents.
On a $\frac{z_Q-z_R}{z_S-z_R} = \frac{3-i}{1+3i} = \frac{(3-i)(1-3i)}{1^2+3^2} = \frac{3-9i-i+3i^2}{10} = \frac{-10i}{10} = -i.$
Puisque $\frac{RQ}{RS} = \left|\frac{z_Q-z_R}{z_S-z_R}\right| = |-i| = 1$, $RQ = RS$, $R \in Mediatrice[QS]$ et $Q \in Cercle(R; RS)$. Puisque $\left(\overrightarrow{RS}\,;\overrightarrow{RQ}\right) \equiv \arg(\frac{z_Q-z_R}{z_S-z_R}) \equiv \arg(-i) \equiv -\frac{\pi}{2}\,[2\pi]$, les droites (RS) et (RQ) sont perpendiculaires et $R \in Cercle(\varnothing[SQ])$.

<u>Remarque</u> : Un point de méthode
Soient $A(a)$, $B(b)$ et $C(c)$ trois points distincts du plan.
On pose $d = \frac{b-a}{c-a}$ et l'on calcule son module et un argument.
· Si $|d| = 1$, alors $AB = AC$, $A \in Médiatrice[BC]$ et $C \in Cercle(A; AB)$.
· Si $\arg(d) \equiv 0\,[\pi]$, alors les points A, B et C sont alignés.
· Si $\arg(d) \equiv \frac{\pi}{2}\,[\pi]$, alors les droites (AB) et (AC) sont perpendiculaires et $A \in Cercle(\varnothing[BC])$.

La propriété suivante a déjà été démontrée dans le chapitre précédent (cf. page 114) mais nous la complétons ici par le cas d'égalité.

Propriété 3 ***Inégalité triangulaire***
Pour tous nombres complexes z et z', $\quad |\boldsymbol{z}+\boldsymbol{z}'| \leqslant |\boldsymbol{z}|+|\boldsymbol{z}'|.$
De plus, $\quad |z+z'|=|z|+|z'| \iff z=0$ *ou* $\exists\lambda\in\mathbb{R}_+$ *tel que* $\quad z'=\lambda z$ *.*

Démonstration : Cette démonstration a déjà été faite mais nous en avons besoin pour le cas d'égalité.
On a $\quad |z+z'|^2=(a+a')^2+(b+b')^2=a^2+2aa'+a'^2+b^2+2bb'+b'^2$
$|z+z'|^2=|z|^2+2(aa'+bb')+|z'|^2.$
Or $\quad aa'+bb'=\mathfrak{Re}(z\overline{z'})\leqslant\left|z\overline{z'}\right|=|z|\left|\overline{z'}\right|=|z|\,|z'|$
donc $\quad |z+z'|^2\leqslant|z|^2+2\,|z|\,|z'|+|z'|^2=(|z|+|z'|)^2,$
en utilisant le théorème 3 p.113 ainsi qu'un lemme évident : $\forall Z\in\mathbb{C},\quad \mathfrak{Re}(Z)\leqslant|Z|.$
Étudions maintenant le cas d'égalité.
Remarquons que $\quad \mathfrak{Re}(Z)=|Z|=\sqrt{\mathfrak{Re}(Z)^2+\mathfrak{Im}(Z)^2}\iff Z\in\mathbb{R}_+.$
Si $z=0$, l'égalité est évidente.
Si $z\neq0$, on a, d'après ce qui précède,
$|z+z'|=(|z|+|z'|)\iff|z+z'|^2=(|z|+|z'|)^2\iff\mathfrak{Re}(z\overline{z'})=\left|z\overline{z'}\right|$
$\iff z\overline{z'}\in\mathbb{R}_+\iff\exists\mu\in\mathbb{R}_+,\ z\overline{z'}=\mu$
$\iff\exists\mu\in\mathbb{R}_+,\ \overline{z'}=\mu\frac{1}{z}=\mu\,\frac{1}{z}\,\frac{\overline{z}}{\overline{z}}=\frac{\mu}{z\overline{z}}\overline{z}\iff\exists\lambda=\frac{\mu}{z\overline{z}}\in\mathbb{R}_+,\ z'=\lambda z.$ □

Interprétation graphique : Dans le plan, le chemin le plus court est la ligne droite.
En effet, pour tous points A, B, C du plan,
$AC=\left|z_{\overrightarrow{AC}}\right|=\left|z_{\overrightarrow{AB}}+z_{\overrightarrow{BC}}\right|\leqslant\left|z_{\overrightarrow{AB}}\right|+\left|z_{\overrightarrow{BC}}\right|=AB+BC$
avec égalité si, et seulement si, $\quad B\in[AC].$

Exemple : Soient les deux points $P(1+2i)$ et $R(-1+i)$ des exemples précédents et soit $T(5+4i)$.
On a $\quad \left|z_{\overrightarrow{RP}}\right|^2=|z_P-z_R|^2=|2+i|^2=2^2+1^2=5,$
$\left|z_{\overrightarrow{PT}}\right|^2=|z_T-z_P|^2=|4+2i|^2=4^2+2^2=20$
et $\quad \left|z_{\overrightarrow{RP}}+z_{\overrightarrow{PT}}\right|^2=|(2+i)+(4+2i)|^2=6^2+3^2=45.$
Ainsi, $\quad \left|z_{\overrightarrow{RP}}+z_{\overrightarrow{PT}}\right|=\sqrt{45}=3\sqrt{5}$
et $\quad \left|z_{\overrightarrow{RP}}\right|+\left|z_{\overrightarrow{PT}}\right|=\sqrt{5}+\sqrt{20}=\sqrt{5}(1+\sqrt{4})=3\sqrt{5}.$
Puisque, $\quad \left|z_{\overrightarrow{RP}}+z_{\overrightarrow{PT}}\right|=\left|z_{\overrightarrow{RP}}\right|+\left|z_{\overrightarrow{PT}}\right|$ non nuls, $\quad$ il existe $\lambda\in\mathbb{R}_+$ tel que
$z_{\overrightarrow{RP}}=\lambda z_{\overrightarrow{PT}}=z_{\lambda\overrightarrow{PT}}$ $\quad$ c.-à-d. $\quad \overrightarrow{RP}=\lambda\overrightarrow{PT}$ $\quad$ et les points R, P et T sont alignés dans cet ordre.

3 Racines n-ièmes de l'unité

Définition 1 *Soit n un entier naturel non nul.*
On appelle racine n-ième de l'unité, tout nombre complexe z tel que $\quad z^n=1.$

Exemples : $1=e^{2i\pi}$ est une racine unième de l'unité, $\quad -1=e^{i\pi}$ est une racine seconde (ou carrée) de l'unité, $\quad i=e^{i\frac{\pi}{2}}$ en est une racine quatrième, $\quad e^{i\frac{\pi}{3}}$ une racine sixième, $\quad e^{i\frac{2\pi}{5}}$ et $e^{i\frac{8\pi}{5}}$, des racines cinquièmes.

Remarques : • Pour tout $n \in \mathbb{N}^*$, 1 est une racine n-ième de l'unité.
• Les racines n-ième de l'unité sont exactement les racines du polynôme $z^n - 1$ dont nous savons qu'il admet au plus n racines.

Propriété 4 *Pour tout entier naturel non nul n, il existe exactement n racines n-ièmes de l'unité distinctes.*
Ce sont les nombres complexes de la forme $e^{i\frac{2k\pi}{n}}$ pour $k \in [\![0 ; n-1]\!]$.

Démonstration : Soit $n \in \mathbb{N}^*$.
· Soit $k \in [\![0 ; n-1]\!]$. On a bien $\left(e^{i\frac{2k\pi}{n}}\right)^n = e^{i\frac{2k\pi}{n}\times n} = e^{ik\times 2\pi} = e^0 = 1$.
Si l'on obtient n racines distinctes, alors on les a toutes.
· Soit $z = re^{i\theta}$ une racine n-ième de l'unité.
On a alors $\left(re^{i\theta}\right)^n = 1 \iff r^n e^{in\theta} = 1e^{0i} \iff r^n = 1$ et $n\theta \equiv 0\,[2\pi]$
$\iff r = 1$ et $\theta \equiv 0\,[\frac{2\pi}{n}] \iff r = 1$ et $\exists k' \in \mathbb{Z},\ \theta = \frac{2k'\pi}{n}$
$\iff \exists k' \in \mathbb{Z},\ z = e^{i\frac{2k'\pi}{n}}$.
En effectuant la division euclidienne de k' par n, on obtient $k' = mn + k$ où $k \in [\![0 ; n-1]\!]$ et l'on a
$z = e^{i\frac{2k'\pi}{n}} = e^{i\frac{2(mn+k)\pi}{n}} = e^{i\frac{2mn\pi}{n}}.e^{i\frac{2k\pi}{n}} = (e^{i\times 2\pi})^m.e^{i\frac{2k\pi}{n}} = 1e^{i\frac{2k\pi}{n}} = e^{i\frac{2k\pi}{n}}$:
il existe donc exactement n racines n-ièmes de l'unité, le nombre d'entiers dans $[\![0 ; n-1]\!]$. □

Remarque : Plus généralement, pour $n \in \mathbb{N}^*$ et $a \in \mathbb{C}$, nous pouvons aussi résoudre l'équation $z^n = a^n$ et même l'équation $z^n = a$. Nous verrons cela en exercice.

Définition 2 *Pour tout $n \in \mathbb{N}^*$, on désigne par $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité.*
On a donc $\mathbb{U}_n = \left\{e^{i\frac{2k\pi}{n}} \,/\, k \in [\![0 ; n-1]\!]\right\}$.

Exemples : ◦ $\mathbb{U}_1 = \{1\}$ et $1 = e^0 = e^{i\frac{2\times 0\pi}{1}}$.
◦ $U_2 = \{-1; 1\}$ et $1 = e^0 = e^{i\frac{2\times 0\pi}{2}}$, $-1 = e^{i\pi} = e^{i\frac{2\times 1\pi}{2}}$.

Propriété 5
• *Les points images des éléments de $\mathbb{U}_n$, pour $n \in \mathbb{N}^*$, appartiennent au cercle trigonométrique : $\mathbb{U}_n \subset \mathbb{U}$.*
• *Pour $n \geqslant 3$, les points images des éléments de $\mathbb{U}_n$ sont les sommets d'un polygone régulier à n côtés.*

Démonstration : · Soit $z \in \mathbb{U}_n$ et M son point image. On a $OM = |z| = \left|e^{i\frac{2k\pi}{n}}\right| = 1$ donc $M \in \mathscr{C}\,(O\,,1)$.
· Soit $n \geqslant 3$ et, pour $k \in [\![0 ; n-1]\!]$, on appelle A_k le point image de $z_k = e^{i\frac{2k\pi}{n}}$.
On a $\left(\overrightarrow{OA_k}\,;\overrightarrow{OA_{k+1}}\right) \equiv \arg\left(\dfrac{z_{k+1} - z_O}{z_k - z_O}\right)\,[2\pi] \equiv \arg\left(\dfrac{e^{i\frac{2(k+1)\pi}{n}} - 0}{e^{i\frac{2k\pi}{n}} - 0}\right)\,[2\pi]$
$\left(\overrightarrow{OA_k}\,;\overrightarrow{OA_{k+1}}\right) \equiv \arg\left(e^{i\frac{2(k+1)\pi}{n} - i\frac{2k\pi}{n}}\right)\,[2\pi] \equiv \arg\left(e^{i\frac{2\pi}{n}}\right)\,[2\pi] \equiv \frac{2\pi}{n}\,[2\pi]$.
De plus, $OA_k = \left|e^{i\frac{2k\pi}{n}} - 0\right| = 1$.

Les triangles OA_kA_{k+1} sont donc tous isocèles en O et de même mesure d'angle en O : ils sont isométriques. Les côtés du polygone $A_0A_1\dots A_{n-1}$ ont donc tous même longueur et ses sommets sont sur un même cercle : c'est un polygone régulier à n sommets. □

Remarque : Attention, si toute racine n-ième de l'unité est un nombre complexe de module 1, la réciproque est fausse : $\forall n \in \mathbb{N}^*,\ \mathbb{U} \not\subset \mathbb{U}_n$.
En effet, $\left(e^{i\theta}\right)^n = 1 \iff e^{in\theta} = e^{i0} \iff n\theta \equiv 0\,[2\pi]$
$\iff \exists m \in \mathbb{Z},\ n\theta = 2m\pi \iff \exists m \in \mathbb{Z},\ \pi = \frac{n\theta}{2m}$ ce qui ne peut arriver si $\theta \in \mathbb{Q}$ par exemple car nous savons que $\pi \notin \mathbb{Q}$.
On voit ici que *la plupart* des points du cercle unité ne correspondent donc pas à des racines de l'unité. Néanmoins, ces dernières y sont denses mais cela dépasse notre programme.

Exemples : Traitons deux cas particuliers.

◦ Pour $n = 3$. Les racines cubiques de l'unité sont les nombres complexes de la forme $e^{i\frac{2k\pi}{3}}$ pour $k \in \{0;1;2\}$. On pose $j = e^{i\frac{2\pi}{3}}$.
On a $e^{i\frac{4\pi}{3}} = j^2 = e^{-i\frac{2\pi}{3}} = \overline{j} = \frac{1}{j}$ et $\mathbb{U}_3 = \{1; j : j^2\} = \{1; j : \overline{j}\}$ dont les sommets images $A(1)$, $B(j)$ et $C(\overline{j}\,)$ forment un triangle équilatéral.
On obtient alors la factorisation du polynôme $z^3 - 1 = (z-1)(z-j)(z-\overline{j})$.
On peut remarquer que $1+j+j^2 = 1+j+\overline{j} = 1+2\,\mathfrak{Re}(j) = 1+2\cos(\frac{2\pi}{3}) = 1-\frac{2}{2} = 0$ et $1 \times j \times j^2 = 1 \times j \times \frac{1}{j} = 1$.

◦ Pour $n = 4$. Les racines quatrièmes de l'unité sont les nombres complexes de la forme $e^{i\frac{2k\pi}{4}} = e^{i\frac{k\pi}{2}}$ pour $k \in \{0;1;2;3\}$ donc $\mathbb{U}_4 = \{1; i : -1; -i\}$ dont les sommets images $A(1)$, $D(i)$, $E(-1)$ et $F(-i)$ forment un carré.
On obtient alors la factorisation du polynôme $z^4 - 1 = (z-1)(z-i)(z+1)(z+i)$.
On peut remarquer que $1 + i - 1 - i = 0$ et $1 \times i \times (-1) \times (-i) = +i^2 = -1$.

Propriété 6 *Soit $n \geqslant 2$. On a toujours*
$$\sum_{\omega_k \in \mathbb{U}_n} \omega_k = 0 \quad \textit{et} \quad \prod_{\omega_k \in \mathbb{U}_n} \omega_k = (-1)^{n-1}.$$

Démonstration : Pour $n \geqslant 2$, on a
$$\sum_{\omega_k \in \mathbb{U}_n} \omega_k = \sum_{k=0}^{n-1} e^{i\frac{2k\pi}{n}} = (e^{i\frac{2\pi}{n}})^0 + (e^{i\frac{2\pi}{n}})^1 + (e^{i\frac{2\pi}{n}})^2 + \dots + (e^{i\frac{2k\pi}{n}})^{n-1}$$
$$= \frac{1-(e^{i\frac{2k\pi}{n}})^n}{1-e^{i\frac{2\pi}{n}}} = \frac{1-1}{1-e^{i\frac{2\pi}{n}}} = 0 \quad \text{et}$$
$$\prod_{\omega_k \in \mathbb{U}_n} \omega_k = \prod_{k=0}^{n-1} e^{i\frac{2k\pi}{n}} = e^{i\frac{2\pi}{n}(0+1+\dots+(n-1))} = e^{i\frac{2\pi}{n}\frac{(n-1)n}{2}} = (e^{i\pi})^{n-1} = (-1)^{n-1}.$$
□

Exercices

NOMBRES COMPLEXES : COMPLÉMENTS

Le plan est muni d'un repère orthonormé direct $(O\,;\,\vec{u},\,\vec{v})$ dès que cela est nécessaire.

Exercice 1 Soient A, B et C les points d'affixes respectives $z_A = -1 - i$, $z_B = 2 - 2i$ et $z_C = 1 + 5i$.

1. Déterminer la forme trigonométrique de z_A et z_B puis placer les points A, B et C.
2. Déterminer les formes algébrique et exponentielle de $z = \frac{z_C - z_A}{z_B - z_A}$.
3. Interpréter $|z|$ et $\arg(z)$ à l'aide de A, B et C.
4. En déduire la nature du triangle ABC.

Exercice 2
Soient A, B, C et D les points d'affixes $a = 2$, $b = 1+i\sqrt{3}$, $c = \overline{b}$ et $d = a+b$.

1. Démontrer que le quadrilatère $OBAC$ est un losange.
2. Quelle est la nature du triangle DOC ?

Exercice 3 Soit Γ l'ensemble des points M du plan complexe dont l'affixe z vérifie : $|z - 2 + i| = \sqrt{2}$.

1. On note A le point d'affixe $a = 2 - i$.
   (a) Démontrer que $M \in \Gamma$ si, et seulement si, $AM = \sqrt{2}$.
   (b) En déduire l'ensemble Γ. Représenter Γ.
2. En utilisant la forme algébrique, donner une autre caractérisation de l'ensemble Γ.

Exercice 4 Δ est l'ensemble des points du plan complexe d'affixe z telle que $|z - 1 - 2i| = |z + 3 - i|$.

1. On note A et B les points d'affixes respectives $a = 1 + 2i$ et $b = i - 3$.
   (a) Démontrer que $M \in \Delta$ si, et seulement si, $MA = MB$.
   (b) En déduire l'ensemble Δ. Représenter Δ.
2. En utilisant la forme algébrique, donner une autre caractérisation de l'ensemble Δ.

Exercice 5 Décrire l'ensemble $\mathscr{E}$ des points M d'affixe z tels que $|z - 1| = |z + i|$.

Exercice 6 Relier chaque ensemble à la relation correspondante.

1. Médiatrice de $[AB]$ avec $A(-1-3i)$ et $B(2+i)$.
2. Cercle de centre $A(3-4i)$ et de rayon $\sqrt{3}$.
3. Médiatrice de $[AB]$ avec $A(1+3i)$ et $B(-2-i)$.
4. Point d'affixe $-3+4i$.
5. Cercle de centre $A(-3+4i)$ et de rayon $\sqrt{3}$.
6. Cercle de centre $A(0)$ et de rayon $\sqrt{3}$.

(a) $|z-3+4i| = \sqrt{3}$.

(b) $|z+3-4i| = 0$.

(c) $|z+3-4i| = \sqrt{3}$.

(d) $|z-2-i| = |z+1+3i|$

(e) $|z| = \sqrt{3}$.

(f) $|z-1-3i| = |z+2+i|$.

Exercice 7 Déterminer puis représenter l'ensemble des points M du plan complexe d'affixes z telles que :

(a) $\left|\frac{z+3-i}{z-1-2i}\right| = 1$

(b) $\left|\overline{z}-2+\frac{3}{4}i\right| = 3$

(c) $|iz-2i| = 1$

(d) $|3iz| = |3iz+3-9i|$

(e) $|\overline{z}-1+i| = |\overline{z}-5+i|$

(f) $\left|\frac{z-1}{z-i}\right| = 1$ et $|z-3-i| \leqslant 2$

(g) $\arg(z-1+i) \equiv \pi\ [2\pi]$

(h) $\arg(z-3-2i) \equiv \frac{\pi}{4}\ [2\pi]$

(i) $\arg\left(\frac{z-3i}{z-2}\right) \equiv \frac{\pi}{2}\ [\pi]$

(j) $\arg\left(\frac{z+1-2i}{z-3+i}\right) \equiv \frac{\pi}{2}\ [\pi]$

Exercice 8 Dans le plan complexe, on donne les points A, B et C d'affixes respectives $z_A = -4$, $z_B = 2+2i\sqrt{3}$ et $z_C = 2-2i\sqrt{3}$.

1. Démontrer que les points A, B et C appartiennent à un même cercle dont on précisera le centre et le rayon.
2. Déterminer les formes algébrique et exponentielle du quotient $\frac{z_B-z_A}{z_C-z_A}$.
3. En déduire la nature du triangle BAC.

Exercice 9 Soient $A(a)$, $B(b)$, $C(c)$ et $D(d)$ quatre points distincts du plan complexe tels que $\begin{cases} a+c=b+d \\ a+ib=c+id. \end{cases}$ Démontrer que le quadrilatère $ABCD$ est un carré.

Exercice 10 Soit f la fonction qui, à tout nombre complexe z, associe le nombre complexe $f(z) = z^2 - 2z$.

1. Calculer $f(1+2i)$, $f(-i)$ et $f(3+i\sqrt{3})$.
2. Résoudre l'équation $f(z) = -2$.
3. Soit A le point d'affixe $1+i$ et B le point d'affixe $1-i$.
   Déterminer la nature du triangle BOA.
4. Pour tout réel a, on considère l'équation $\mathscr{E}_a\colon f(z) = a$.
   Comment doit-on choisir a pour que les solutions de l'équation $\mathscr{E}_a$ soient des nombres complexes conjugués ?

Exercice 11 Inégalités triangulaires

1. Soient a et b deux nombres complexes.
   (a) Rappeler l'inégalité triangulaire, son cas d'égalité et en donner une interprétation dans le plan complexe.
   (b) Compléter $a = a + b \ldots$ puis démontrer la deuxième inégalité triangulaire : $\big|\,|a| - |b|\,\big| \leqslant |a + b|$.
2. (a) Soient $z_1, z_2, \ldots, z_n$ des nombres complexes.
   Montrer que $|z_1 + z_2 + \ldots + z_n| \leqslant |z_1| + |z_2| + \ldots + |z_n|$.
   (b) En déduire que $|1 + a| + |a + b| + |b| \geqslant 1$.

Exercice 12 Le plan complexe est muni d'un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$. On considère l'application f du plan dans lui-même qui, à tout point M d'affixe z, associe le point M' d'affixe $z' = z^2 - 4z$.

1. On note A et B les points d'affixes respectives $z_A = 1 - i$ et $z_B = 3 + i$.
   (a) Calculer les affixes des points A' et B', images respectives de A et B par f.
   (b) Soient deux points ayant la même image par f. Démontrer qu'ils sont confondus ou que l'un est l'image de l'autre par une symétrie centrale que l'on précisera.
2. I est le point d'affixe -3.
   (a) Démontrer que le quadrilatère $OMIM'$ est un parallélogramme si, et seulement si, $z^2 - 3z + 3 = 0$.
   (b) Résoudre dans $\mathbb{C}$ l'équation $z^2 - 3z + 3 = 0$.
3. (a) Exprimer $z' + 4$ en fonction de $z - 2$. En déduire une relation entre $|z' + 4|$ et $|z - 2|$ puis entre $\arg(z' + 4)$ et $\arg(z - 2)$.
   (b) Les points J et K ont pour affixes respectives $z_J = 2$ et $z_K = -4$.
   Démontrer que tous les points M du cercle $\mathscr{C}$ de centre J et de rayon 2 ont leur image M' sur un même cercle que l'on déterminera.
   (c) E est le point d'affixe $z_E = -4 - 3i$. Donner la forme trigonométrique de $z_E + 4$ et, à l'aide du 3a, démontrer qu'il existe deux points dont l'image par f est E. En préciser la forme algébrique.

Exercice 13

1. (a) (r_n) est la suite géométrique réelle de premier terme r_0 strictement positif et de raison $\frac{2}{3}$. Exprimer r_n en fonction de r_0 et de n.
   (b) (θ_n) est la suite arithmétique réelle de premier terme $\theta_0 \in \left[0\,;\frac{\pi}{3}\right[$ et de raison $\frac{2\pi}{3}$. Exprimer θ_n en fonction de θ_0 et de n.
   (c) On pose $z_n = r_n(\cos\theta_n + i\sin\theta_n)$ pour $n \in \mathbb{N}$.
   Sachant que z_0, z_1 et z_2 vérifient $z_0 z_1 z_2 = 8$, déterminer le module et un argument de z_1 et de z_2.
   (d) Exprimer z_{n+1} en fonction de n puis en fonction de z_n. Qu'en déduire pour la suite $(z_n)_{\mathbb{N}}$?

EXERCICES

2. On appelle M_n le point d'affixe z_n dans un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$.
   (a) Pour tout n de $\mathbb{N}$, exprimer M_nM_{n+1} en fonction de n.
   (b) On pose, pour tout entier naturel n, $I_n = \sum\limits_{k=0}^{n} M_kM_{k+1}$. Exprimer I_n en fonction de n et déterminer la limite de I_n quand n tend vers l'infini.

Exercice 14 Le plan complexe est muni d'un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$ d'unités graphiques 2 cm. On réalisera une figure que l'on complétera tout au long de l'exercice. On considère les points A d'affixe i, B d'affixe $-2i$ et D d'affixe 1. On appelle E le point tel que le triangle ADE est équilatéral direct. Soit f l'application qui, à tout point M d'affixe z $(z \neq i)$, associe le point M' d'affixe z' définie par $z' = \dfrac{2z-i}{iz+1}$.

1. Vérifier que le point E a pour affixe $\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)(1+i)$.
2. Exprimer sous forme algébrique l'affixe du point D' associé au point D par l'application f.
3. (a) Démontrer que pour tout nombre complexe z différent de i,
   $(z'+2i)(z-i) = 1$.
   (b) En déduire que, pour tout $M(z)$ $(z \neq i)$, $BM' \times AM = 1$ et $\left(\overrightarrow{u}\,;\overrightarrow{BM'}\right) \equiv -\left(\overrightarrow{u}\,;\overrightarrow{AM}\right)\ [2\pi]$.
4. (a) Justifier que les points D et E appartiennent au cercle $\mathscr{C}$ de centre A et de rayon $\sqrt{2}$.
   (b) En utilisant les résultats de la question 3b, placer le point E' associé au point E par l'application f.
5. Quelle est la nature du triangle $BE'D'$? Justifier.

Exercice 15 QCM vu au BAC
Pour chaque question, plusieurs réponses peuvent être exactes. Justifier vos réponses.
Le plan complexe est rapporté à un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$.

1. $\mathscr{E}$ est l'ensemble des points M d'affixe z vérifiant $z = 1-2i+e^{i\theta}$ pour $\theta \in \mathbb{R}$.
   (a) $\mathscr{E}$ est une droite passant par le point d'affixe $2-2i$.
   (b) $\mathscr{E}$ est le cercle de centre d'affixe $-1+2i$ et de rayon 1.
   (c) $\mathscr{E}$ est le cercle de centre d'affixe $1-2i$ et de rayon 1.
   (d) $\mathscr{E}$ est le cercle de centre d'affixe $1-2i$ et de rayon $\sqrt{5}$.
2. f est l'application qui, à tout point M d'affixe z, associe le point M' d'affixe $z' = -iz-2i$.
   (a) Le point d'affixe $-1-2i$ est un antécédent du point d'affixe i par f.
   (b) Si $z = -1-i$, alors les points M et M' sont confondus.
   (c) Si $|z'| = 1$, alors M est un point du cercle de centre A d'affixe -2 et de rayon 1.
   (d) Si $\arg(z) \equiv \frac{\pi}{2}\ [2\pi]$, alors le point M' décrit une droite.

3. On considère, dans $\mathbb{C}$, l'équation $(E): \quad z+|z|^2=7+i$.
   (a) (E) admet deux solutions distinctes qui ont 1 pour partie imaginaire.
   (b) (E) admet une solution qui a pour partie imaginaire 2.
   (c) Si z_1 et z_2 sont les solutions de (E), alors $\sqrt{2}\,e^{i\frac{3\pi}{4}}$ est la forme exponentielle du nombre complexe $\dfrac{z_1}{z_2}$ avec $\mathfrak{Re}(z_2)>0$.

Exercice 16 Two loci L_1 and L_2 in the complex plane are defined by the following equations : $L_1 : |z+2-3i|=1$ and $L_2 : \arg(z)=\frac{\pi}{4}\,[2\pi]$.

1. Sketch the two loci.
2. Find the smallest possible value of $|z_1-z_2|$ where the points z_1 and z_2 lie on the loci L_1 and L_2 respectively.

Exercice 17 Soit $(z_n)_{\mathbb{N}}$ la suite de nombres complexes définie par $z_0=1$ et $z_{n+1}=\frac{1}{3}z_n+\frac{2}{3}i$.
Pour tout $n\in\mathbb{N}$, on pose $u_n=z_n-i$ et l'on note A_n le point d'affixe z_n, B_n le point d'affixe u_n et C le point d'affixe i.

1. Pour tout $n\in\mathbb{N}$, exprimer u_{n+1} en fonction de u_n et en déduire une expression de u_n en fonction de n.
2. (a) Calculer le module de u_n en fonction de $n\in\mathbb{N}$.
   (b) Déterminer $\lim\limits_{n\to\infty}|z_n-i|$.
   (c) Quelle interprétation géométrique peut-on en déduire ?
3. (a) Pour tout $n\in\mathbb{N}$, déterminer un argument de u_n.
   (b) Démontrer que, lorsque n décrit $\mathbb{N}$, les points B_n sont alignés.
   (c) Démontrer que, pour tout $n\in\mathbb{N}$, le point A_n appartient à la droite d'équation $y=1-x$.

Exercice 18 Soit $(z_n)_{\mathbb{N}}$ la suite de nombres complexes définie par $z_0=0$ et $z_{n+1}=3iz_n-1$.

1. Résoudre dans $\mathbb{C}$ l'équation $\mathscr{E}: z=3iz-1$.
2. Pour tout $n\in\mathbb{N}$, on pose $u_n=z_n+\frac{1}{10}+\frac{3}{10}i$.
   (a) Démontrer que, pour tout $n\in\mathbb{N}$, $u_{n+1}=3iu_n$.
   (b) En déduire une expression de u_n en fonction de $n\in\mathbb{N}$.
3. M_n est le point d'affixe z_n, A est le point image de la solution a de l'équation $\mathscr{E}$.
   (a) Montrer que la distance AM_n diverge vers $+\infty$.
   (b) Démontrer que, pour tout $n\in\mathbb{N}$, les points A, M_n et M_{n+2} sont alignés.
   (c) Démontrer que, pour tout $n\in\mathbb{N}$, les droites (AM_n) et (AM_{n+1}) sont perpendiculaires.

Exercice 19
À tout point M d'affixe $z\neq 2-i$ du plan complexe, on associe le point M' d'affixe z' définie par $z'=\dfrac{z+1+3i}{z-2+i}$.

EXERCICES

1. Déterminer l'ensemble des points M tels que z' soit un réel.
2. Déterminer l'ensemble des points M tels que z' soit un imaginaire pur.

Exercice 20

A. Soit l'équation $\mathscr{E}\colon z^4 = -4$.

1. Montrer que si z_0 est solution de $\mathscr{E}$, alors $-z_0$ et $\overline{z_0}$ sont solutions de $\mathscr{E}$.
2. (a) Soit $z_0 = 1 + i$. Écrire z_0 sous forme exponentielle.
   (b) Vérifier que z_0 est solution de $\mathscr{E}$.
   (c) En déduire les trois autres solutions de $\mathscr{E}$.

B. Soient A, B, C et D les points du plan complexe d'affixes respectives $z_A = 1 + i$, $z_B = -1 + i$, $z_C = -1 - i$ et $z_D = 1 - i$.

1. Déterminer les affixes des points E et F définies par
   $z_E - z_C = (z_B - z_C)e^{i\frac{\pi}{3}}$ et $z_F - z_C = (z_D - z_C)e^{i\frac{\pi}{3}}$.
2. Démontrer que le quotient $\frac{z_A - z_E}{z_A - z_F}$ est réel.
3. Qu'en déduire pour les points A, E et F ?

Exercice 21 Résoudre dans $\mathbb{C}$ les équations suivantes.

(a) $(z + i)^4 = 1$
(b) $z^4 = 81$
(c) $(z - 8)^5 = 1$
(d) $z^5 = 4\sqrt{2}$
(e) $z^4 = (1 + 3i)^4$
(f) $z^5 = (2 + i)^5$
(g) $z^5 = 32i$
(h) $z^4 = -9i$
(i) $(z - 1)^5 = (z + 1)^5$
(j) $(z - i)^4 - (z + i)^4 = 0$
(k) $z^6 - 9z^3 + 8 = 0$
(l) $z^4 + (1 - i)z^2 - i = 0$

Exercice 22 Résoudre dans $\mathbb{C}$ l'équation $\left(\frac{2z+1}{z-1}\right)^4 = 1$.
Démontrer que les points images de ces solutions sont sur un même cercle que l'on précisera.

Exercice 23 Racines n-ièmes d'un nombre complexe
Soit n un entier naturel non nul et a un nombre complexe non nul.

1. Résoudre l'équation $\mathscr{E}_0\colon z^n = 0$.
2. Rappeler les solutions de l'équation $\mathscr{E}_1\colon z^n = 1$.
3. (a) Résoudre l'équation $z^3 = -8$ en se ramenant à une équation du type $\mathscr{E}_1$.
   (b) Résoudre l'équation $\mathscr{E}_{a^n}\colon z^n = a^n$.
   (c) Vérifier que $z_0 = 2 - i$ est solution de l'équation $z^4 + 7 + 24i = 0$ puis résoudre cette dernière.
4. (a) Résoudre l'équation $z^3 = 27i$ en passant par la forme exponentielle.
   (b) Résoudre l'équation $\mathscr{E}_a\colon z^n = a$.
   (c) Déterminer les racines carrées de i.

Exercice 24 Le pentagone

1. (a) Résoudre l'équation $\mathscr{E}\colon z^2 + z - 1 = 0$.

   (b) Déterminer une forme exponentielle des racines cinquièmes de l'unité. Quel polygone les points images de ces racines forment-ils ?
2. On note $\omega = e^{i\frac{2\pi}{5}}$. Démontrer que $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$, $\omega^3 = \overline{\omega^2}$ et $\omega^4 = \overline{\omega}$.
3. (a) En déduire que $\omega + \overline{\omega}$ est solution de $\mathscr{E}$.
   (b) Déterminer alors les valeurs exactes des lignes trigonométriques de $\frac{2\pi}{5}$.
4. Dans le plan complexe muni du r.o.n. $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$, on considère les points U, V et A d'affixes respectives $z_U = 1$, $z_V = i$ et $z_A = -\frac{1}{2}$. On désigne par $\mathscr{C}$ le cercle de centre A passant par V.
   (a) Déterminer l'affixe z_W du point d'intersection W de $\mathscr{C}$ et de la demi-droite $[OU)$ et en déduire un point B d'affixe $\cos(\frac{2\pi}{5})$.
   (b) En déduire une méthode de construction d'un pentagone régulier à la règle non graduée et au compas.

Exercice 25 Transformée de Fourier discrète

La transformée de Fourier[†] discrète, ou TDF, d'une séquence de $n \in \mathbb{N}^*$ nombres complexes $(z_0; z_1; \ldots; z_{n-1}) \in \mathbb{C}^n$ est la séquence de n nombres complexes $(Z_0; Z_1; \ldots; Z_{n-1}) \in \mathbb{C}^n$ définis pour tout $p \in [\![\,0\,;n-1\,]\!]$ par $Z_p = \displaystyle\sum_{k=0}^{n-1} z_k \omega^{-kp}$ où $\omega = e^{\frac{2i\pi}{n}}$.

La TDF est un outil mathématique permettant, entre autres, l'étude et la transmission aissé des signaux numériques. Dans le cas où le signal *temporel* connu z est périodique et constitué de plusieurs fréquences de différentes amplitudes, cette transformation donne dans Z, les différentes fréquences ainsi que leur intensité. Ces informations sont souvent beaucoup plus légères et nous allons voir que cette transformation est réversible, ce qui signifie que si l'on transmet Z, il est possible de retrouver z. Quel bon début pour une gestion efficace de signaux périodiques !

1. Calculer la TDF des séquences $(\,1\,,\,1\,)$, $(\,0\,,\,1\,,\,1\,)$ et $(0; 1; i; 0)$.
2. (a) Exprimer Z_ℓ puis justifier que $\displaystyle\sum_{\ell=0}^{n-1} Z_\ell \omega^{\ell p} = \sum_{k=0}^{n-1}\left(z_k \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell}\right)$.
   (b) Calculer, pour $k = p$ puis pour $k \neq p$, $\displaystyle\sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell}$.
   (c) En déduire que $z_p = \displaystyle\frac{1}{n}\sum_{\ell=0}^{n-1} Z_\ell \omega^{\ell p}$. Cette opération s'appelle la transformée de Fourier discrète inverse de la séquence $(Z_0; Z_1; \ldots; Z_{n-1})$. Elle permet de retrouver la séquence originale.
   (d) Vérifier ceci en calculant la TDF inverse des résultats obtenus à la question 1.

Projetez-vous en pages 315 et 317 afin d'étudier les devoirs n$^{\text{os}}$ 12 et 13.

†. Immense mathématicien dont le nom est inscrit sur la non moins immense tour Eiffel.

EXERCICES

Corrigé des exercices

NOMBRES COMPLEXES : COMPLÉMENTS

Exercice 1 $z_A = -1 - i$, $z_B = 2 - 2i$ et $z_C = 1 + 5i$.

1. $z_A = -1-i = \sqrt{1+1}\left(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = \sqrt{2}\left(\cos(-\frac{3\pi}{4}) + i\sin(-\frac{3\pi}{4})\right) = \sqrt{2}e^{-i\frac{3\pi}{4}}$,
   $z_B = 2 - 2i = 2\sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = 2\sqrt{2}\left(\cos(-\frac{\pi}{4}) + i\sin(-\frac{\pi}{4})\right) = 2\sqrt{2}e^{-i\frac{\pi}{4}}$.
2. On a $z = \frac{z_C - z_A}{z_B - z_A} = \frac{(1+5i)-(-1-i)}{(2-2i)-(-1-i)} = \frac{2+6i}{3-i}\,\frac{3+i}{3+i} = \frac{6+2i+18i-6}{3^2+1^2} = \frac{20i}{10} = 2i = 2e^{i\frac{\pi}{2}}$.
3. On a $|z| = \frac{|z_C - z_A|}{|z_B - z_A|} = 2$ donc $AC = 2AB$ et $\arg(z) = \left(\overrightarrow{AB}\,;\overrightarrow{AC}\right) \equiv \frac{\pi}{2}\,[2\pi]$.
4. Ainsi, le triangle ABC est rectangle non isocèle en A.

Exercice 2 $a = 2$, $b = 1 + i\sqrt{3}$, $c = \overline{b}$ et $d = a + b$.

1. On a $(b-0) + (c-0) = b + c = b + \overline{b} = 2\mathfrak{Re}(b) = 2 = a - 0$ donc $\overrightarrow{OB} + \overrightarrow{OC} = \overrightarrow{OA}$ et $OBAC$ est un parallélogramme.
   De plus, $|b| = |c|$ donc $OB = OC$ et $OBAC$ est un losange.
2. $\frac{d-0}{c-0} = \frac{2+1+i\sqrt{3}}{1-i\sqrt{3}} = \frac{(3+I\sqrt{3})(1+i\sqrt{3})}{1+3} = \frac{1}{4}(3+i\sqrt{3}+3i\sqrt{3}-3) = i\sqrt{3} = \sqrt{3}e^{i\frac{\pi}{2}}$ donc $\left(\overrightarrow{OC}\,;\overrightarrow{OD}\right) \equiv \frac{\pi}{2}\,[2\pi]$ et $OC \neq OD$: DOC est rectangle non isocèle en O.

Exercice 3 Soit Γ l'ensemble des points $M(z)$ du plan tels que $|z - 2 + i| = \sqrt{2}$.

1. (a) $$M_z \in \Gamma \iff |z-2+i| = \sqrt{2} \iff |z-(2-i)| = \sqrt{2}$$
   $$\iff |z-a| = \sqrt{2} \iff AM = \sqrt{2}.$$
   (b) Ainsi, Γ est l'ensemble des points du plan complexe à distance $\sqrt{2}$ du point A : le cercle $\mathscr{C}(A;\sqrt{2})$.
2. Pour $z = x + iy$, $|z-2+i|^2 = |(x-2)+i(y+1)|^2 = (x-2)^2 + (y+1)^2$
   $|z-2+i|^2 = x^2 - 4x + 4 + y^2 + 2y + 1$
   et $\Gamma = \left\{(x;y) \in \mathbb{R}^2 \ / \ x^2 - 4x + 2y + y^2 - 1 = 0\right\}$.

Exercice 4 Δ est l'ensemble des points $M(z)$ tels que $|z - 1 - 2i| = |z + 3 - i|$.

1. (a) $M_z \in \Delta \Leftrightarrow |z-(1+2i)| = |z-(i-3)| \Leftrightarrow |z-a| = |z-b| \Leftrightarrow MA = MB$
   (b) Ainsi, Δ est l'ensemble des points du plan équidistants de A et de B : la médiatrice du segment $[AB]$.
2. Pour $z = x + iy$,
   $|z-1-2i|^2 - |z+3-i|^2 = |(x-1)+i(y-2)|^2 - |(x+3)+i(y-1)|^2$
   $= x^2 - 2x + 1 + y^2 - 4y + 4 - x^2 - 6x - 9 - y^2 + 2y - 1 = -8x - 2y - 5$
   d'où $MA = MB \iff -8x - 2y - 5 = 0$
   et $\Gamma = \left\{(x;y) \in \mathbb{R}^2 \ / \ y = -4x - \frac{5}{2}\right\}$.

Exercice 5 Soient P et Q les points d'affixes respectives $z_P = 1$ et $z_Q = -i$.

$|z-1| = |z+i| \iff |z - z_P| = |z - z_Q| \iff MP = MQ$

$\iff M \in \mathscr{E} =$ Médiatrice du segment $[PQ]$.

Ceci n'est pas malheureusement pas très explicite. Posons donc $z = a + ib$.

On a alors $|z-1| = |z+i| \iff |a+ib-1|^2 = |a+ib+i|^2$

$\iff (a-1)^2 + b^2 = a^2 + (b+1)^2 \iff a^2 - 2a + 1 + b^2 = a^2 + b^2 + 2b + 1$

$\iff b = -a \iff M \in \mathscr{E} = 2^{\text{de}}$ Bissectrice.

Exercice 6 Voici les liaisons : 1.(d), 2.(a), 3.(f), 4.(b), 5.(c) et 6.(e).

Exercice 7

(a) $\left|\frac{z+3-i}{z-1-2i}\right| = 1 \iff |z-(-3+i)| = |z-(1+2i)|$

$\iff M_zA_{-3+i} = M_zB_{1+2i} \iff M(z) \in$ Médiatrice$[A(-3+i)B(1+2i)]$.

(b) $\left|\overline{z} - 2 + \frac{3}{4}i\right| = 3 \iff \left|\overline{z - 2 - \frac{3}{4}i}\right| = 3 \iff \left|z - (2 + \frac{3}{4}i)\right| = 3$

$\iff M_zC_{2+\frac{3}{4}i} = 3 \iff M(z) \in$ Cercle$(C(2+\frac{3}{4}i); 3)$.

(c) $|iz - 2i| = 1 \Leftrightarrow |i|\,|z-2| = 1 \Leftrightarrow 1 \times M_zD_2 = 1 \Leftrightarrow M(z) \in$ Cercle$(D(2); 1)$.

(d) $|3iz| = |3iz + 3 - 9i| \Leftrightarrow |3i|\,|z| = |3i|\left|z + \frac{1}{i} - 3\right| \Leftrightarrow |z - 0| = |z - (3+i)|$

$\Leftrightarrow M_zO_0 = M_zE_{3+i} \Leftrightarrow M(z) \in$ Médiatrice$[OE(3+i)]$.

(e) $|\overline{z} - 1 + i| = |\overline{z} - 5 + i| \iff \left|\overline{z-1-i}\right| = \left|\overline{z-5-i}\right|$

$\iff |z-(1+i)| = |z-(5+i)| \iff M_zF_{1+i} = M_zG_{5+i}$

$\iff M(z) \in$ Médiatrice$[F(1+i)G(5+i)]$.

(f) $\left|\frac{z-1}{z-i}\right| = 1$ et $|z-3-i| \leqslant 2 \iff |z-1| = |z-i|$ et $|z-(3+i)| \leqslant 2$

$\iff M_zH_1 = M_zK_i$ et $M_zE_{3+i} \leqslant 2$

$\iff M(z) \in$ Médiatrice$[H(1)K(i)] \cap$ Disque$(E(3+i); 2)$.

(g) $\arg(z-1+i) \equiv \pi\,[2\pi] \iff \arg(z-(1-i)) \equiv \pi\,[2\pi]$

$\iff \left(\overrightarrow{u}\,; \overrightarrow{L_{1-i}M_z}\right) \equiv \pi\,[2\pi] \iff M(z) \in$ Demi-droite$[L(1-i), -\overrightarrow{u})$.

(h) $\arg(z-3-2i) \equiv \frac{\pi}{4}\,[2\pi] \iff \arg(z-(3+2i)) \equiv \frac{\pi}{4}\,[2\pi]$

$\iff \left(\overrightarrow{u}\,; \overrightarrow{N_{3+2i}M_z}\right) \equiv \frac{\pi}{4}\,[2\pi] \iff (\overrightarrow{u} + \overrightarrow{v}; \overrightarrow{N_{3+2i}M_z}) \equiv 0\,[2\pi]$

$\iff M(z) \in$ Demi-droite$[N(3+2i), \overrightarrow{u} + \overrightarrow{v})$.

(i) $\arg\left(\frac{z-3i}{z-2}\right) \equiv \frac{\pi}{2}\,[\pi] \iff \left(\overrightarrow{P_2M_z}\,; \overrightarrow{Q_{3i}M_z}\right) \equiv \frac{\pi}{2}\,[\pi] \iff (P_2M_z) \perp (Q_{3i}M_z)$

$\iff M(z) \in$ Cercle$(\varnothing[P(2)Q(3i)])$.

(j) $\arg\left(\frac{z+1-2i}{z-3+i}\right) \equiv \frac{\pi}{2}\,[\pi] \iff \arg\left(\frac{z-(-1+2i)}{z-(3-i)}\right) \equiv \frac{\pi}{2}\,[\pi]$

$\iff \left(\overrightarrow{R_{3-i}M_z}\,; \overrightarrow{S_{-1+2i}M_z}\right) \equiv \frac{\pi}{2}\,[\pi] \iff (R_{3-i}M_z) \perp (S_{-1+2i}M_z)$

$\iff M(z) \in$ Cercle$(\varnothing[R(3-i)S(-1+2i)])$.

Exercice 8 $z_A = -4$, $z_B = 2 + 2i\sqrt{3}$ et $z_C = 2 - 2i\sqrt{3}$.

1. $|z_A|^2 = 4^2 = 16$ et $|z_B|^2 = |z_C|^2 = 2^2 + (\pm 2\sqrt{3})^2 = 16$
   donc $OA = OB = OC = \sqrt{16} = 4$ et les points A, B et C appartiennent au cercle de centre O et de rayon 4.
2. On a $\frac{z_B - z_A}{z_C - z_A} = \frac{2+2i\sqrt{3}-(-4)}{2-2i\sqrt{3}+4} = \frac{6+2i\sqrt{3}}{6-2i\sqrt{3}}.\frac{6+2i\sqrt{3}}{6+2i\sqrt{3}} = \frac{36+24i\sqrt{3}-(2\sqrt{3})^2}{6^2+(2\sqrt{3})^2} = \frac{24+24i\sqrt{3}}{48}$
   $\frac{z_B - z_A}{z_C - z_A} = \frac{1}{2} + i\frac{\sqrt{3}}{2} = 1.e^{i\frac{\pi}{3}}$.

CORRIGÉS

3. Ainsi, $AB = |z_B - z_A| = |z_C - z_A| = AC$ et le triangle BAC est isocèle en A.
   De plus, $\left(\overrightarrow{AC}\,;\overrightarrow{AB}\right) \equiv \frac{\pi}{3}\,[2\pi]$ donc le triangle BAC est équilatéral.

Exercice 9 On a $a - b = d - c \neq 0$ donc $\frac{a-b}{d-c} = 1$
d'où $AB = |b-a| = |d-c| = CD$ et $\left(\overrightarrow{CD}\,;\overrightarrow{BA}\right) \equiv 0\,[2\pi]$ et $ABCD$ est un quadrilatère non croisé dont deux côtés sont parallèles et de même longueur : c'est un parallélogramme.
Par ailleurs, $a - c = i(d-b) \neq 0$ donc $\frac{a-c}{d-b} = i$
d'où $AC = |c-a| = |d-b| = DB$. Les diagonales du parallélogramme $ABCD$ sont de même longueur : c'est un rectangle.
Enfin, $\left(\overrightarrow{BD}\,;\overrightarrow{CA}\right) \equiv \arg(i)\,[2\pi] \equiv \frac{\pi}{2}\,[2\pi]$ donc les diagonales du rectangle $ABCD$ sont perpendiculaires : c'est un carré.

Exercice 10 $f(z) = z^2 - 2z$.

1. On a $f(1+2i) = (1+2i)^2 - 2(1+2i) = 1 + 4i + 4i^2 - 2 - 4i = -5$, $f(-i) = (-i)^2 - 2(-i) = -1 + 2i$ et
   $f(3+i\sqrt{3})(3+i\sqrt{3})^2 - 2(3+i\sqrt{3}) = 9 + 6i\sqrt{3} - \sqrt{3}^2 - 6 - 6i\sqrt{3} = 0.$
2. On a $f(z) = -2 \iff z^2 - 2z + 2 = 0$ de discriminant
   $\Delta = 2^2 - 4 \times 2 = -4 = (2i)^2 < 0$ et donc de racines complexes conjuguées $z_1 = \frac{-(-2)-i\sqrt{4}}{2\times 1} = 1 - i$ et $z_2 = \overline{z_1} = 1 + i$.
3. On a $OA^2 = OB^2 = |1 \pm i|^2 = 1^2 + 1^2 = 2$
   et $AB^2 = |z_B - z_A|^2 = |-2i|^2 = 4 = OA^2 + OB^2$ donc le triangle BOA est isocèle rectangle en O.
4. Pour tout $a \in \mathbb{R}$, $f(z) = a \iff z^2 - 2z - a = 0$
   de discriminant $\Delta_a = 4 + 4a = 4(1+a)$ qui est du signe de $a + 1$.
   Ainsi, les solutions de l'équation $\mathscr{E}_a : f(z) = a$ sont des nombres complexes conjugués *ssi* $a < -1$.

Exercice 11 Inégalités triangulaires

1. (a) Pour tous $(a\,,\,b) \in \mathbb{C}^2$, $|a+b| \leqslant |a| + |b|$
   et $|a+b| = |a| + |b| \iff a = 0$ ou $\exists\lambda \in \mathbb{R}_+,\ b = \lambda a$.
   Ceci signifie que la longueur de la diagonale du parallélogramme $O_0A_aC_{a+b}B_b$ est inférieure à la somme de la longueur des deux côtés adjacents OA et OB et qu'elle est lui est égale *ssi* l'un de ces côtés est inclus dans l'autre : $A \in [OB)$.
   Autrement dit, dans le plan complexe, le chemin le plus court est la ligne droite.
   (b) On a $a = a+b-b$ donc $|a| = |(a+b) - b| \leqslant |a+b| + |-b| = |a+b| + |b|$
   et $|a| - |b| \leqslant |a+b|$. De même, $|b| - |a| \leqslant |b+a| = |a+b|$.
   D'où $\big||a| - |b|\big| \leqslant |a+b|$.
2. (a) Soient z_1, z_2,... , z_n des nombres complexes. On a, par récurrence finie triviale,
$$\begin{aligned} |z_1 + z_2 + \ldots + z_n| &= |z_1 + (z_2 + \ldots + z_n)| \\ &\leqslant |z_1| + |z_2 + (z_3 + \ldots z_n)| \\ &\leqslant |z_1| + |z_2| + |z_3 + (z_4 + \ldots z_n)| \\ &\ldots \\ &\leqslant |z_1| + |z_2| + \ldots + |z_n|. \end{aligned}$$

(b) Ainsi,
$1 = |1 + a - a - b + b| = |(1 + a) - (a + b) + b| \leqslant |1 + a| + |-(a + b)| + |b|$
et $\quad 1 \leqslant |1 + a| + |a + b| + |b|$.

Exercice 12 $\quad z' = z^2 - 4z$

1. (a) On a $\quad z_{A'} = f(1 - i) = (1 - i)^2 - 4(1 - i) = 1 - 2i - 1 - 4 + 4i = 2i - 4$
et $\quad z_{B'} = f(3+i) = (3+i)^2 - 4(3+i) = 9+6i-1-12-4i = 2i-4 = z_{A'}$.

(b) Soient $m \neq n \in \mathbb{C}$. On a $\quad f(m) = f(n) \iff m^2 - 4m = n^2 - 4n$
$\iff m^2 - n^2 = 4(m - n) \iff (m + n)(m - n) = 4(m - n)$
$\overset{m-n\neq 0}{\iff} m + n = 4 \iff (m - 2) = -(n - 2)$: $\quad M_m$ et N_n sont symétriques par rapport au point $(2, 0)$.

2. (a) $\quad OMIM'$ parallélogramme $\iff \overrightarrow{OM'} = \overrightarrow{MI} \iff z' - z_O = z_I - z$
$\iff z^2 - 3z + 3 = 0$.

(b) $\quad z^2 - 3z + 3 = 0 \quad$ de déterminant $\quad \Delta = -3 \quad$ donc de racines complexes conjuguées $\quad z_{1,2} = \frac{3 \pm i\sqrt{3}}{2}$.

3. (a) On a $\quad z' + 4 = z^2 - 4z + 4 = (z - 2)^2 \quad$ donc $\quad |z' + 4| = |z - 2|^2 \quad$ et $\arg(z' + 4) \equiv 2\arg(z - 2)\,[2\pi]$.

(b) Si $\quad M \in \mathscr{C}(J; 2)$, $\quad$ alors $\quad |z - 2| = 2 \quad$ et $\quad |z' - (-4)| = |z - 2|^2 = 4$: $M' \in \mathscr{C}(K; 4)$.

(c) $\quad z_E + 4 = -3i = 3e^{-i\frac{\pi}{2}}$. $\quad$ On cherche donc z tel que $\quad |z - 2|^2 = 3 \quad$ et $2\arg(z - 2) \equiv -\frac{\pi}{2}\,[2\pi]$: $\quad z - 2 = \sqrt{3}e^{-i\frac{\pi}{4}} \quad$ ou $\quad z - 2 = \sqrt{3}e^{-i\frac{\pi}{4} + i\pi}$
i.e. $\quad z = 2 + \sqrt{3}(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}) \quad$ ou $\quad z = 2 + \sqrt{3}(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$.

Exercice 13

1. (a,b) On a, $\quad \forall n \in \mathbb{N}, \quad r_n = r_0\left(\frac{2}{3}\right)^n \quad$ et $\quad \theta_n = \theta_0 + \frac{2\pi}{3}n$.

(c) On a $z_n = r_n.e^{i\theta_n}$ et $\quad z_0 z_1 z_2 = 8 \iff r_0 e^{i\theta_0} r_1 e^{i\theta_1} r_2 e^{i\theta_2} = 8$

$$\iff r_0 r_1 r_2 e^{i(\theta_0 + \theta_1 + \theta 2)} = 8e^{0i} \iff \begin{cases} r_0.r_1.r_2 = 8 \\ \theta_0 + \theta_1 + \theta_2 \equiv 0\,[2\pi] \end{cases}$$

$$\iff \begin{cases} r_0^3\,\frac{2}{3}\,\frac{4}{9} = 8 \\ \theta_0 + \theta_0 + \frac{2\pi}{3} + \theta_0 + \frac{4\pi}{3} \equiv 0\,[2\pi] \end{cases} \iff \begin{cases} r_0^3 = 27 \\ 3\theta_0 + 2\pi \equiv 0\,[2\pi] \end{cases}$$

$$\iff \begin{cases} r_0 = \sqrt[3]{27} \\ \theta_0 \equiv 0\,[\frac{2\pi}{3}] \end{cases} \overset{0 \leqslant \theta < \frac{\pi}{3}}{\iff} \begin{cases} r_0 = 3 \\ \theta_0 \equiv 0\,[2\pi]. \end{cases}$$

D'où $z_0 = 3$, $\; z_1 = 3\frac{2}{3}e^{i\frac{2\pi}{3}} = 2e^{i\frac{2\pi}{3}}$, $\; z_2 = \frac{4}{3}e^{i\frac{4\pi}{3}}$.

(d) On a $\quad z_{n+1} = r_{n+1}.e^{i\theta_{n+1}} = r_0\left(\frac{2}{3}\right)^n.e^{i(\theta_0 + n\frac{2\pi}{3})} = 3\left(\frac{2}{3}\right)^n.e^{i\frac{2\pi n}{3}}$
et $\quad z_{n+1} = r_{n+1}.e^{i\theta_{n+1}} = \frac{2}{3}r_n.e^{i(\theta_n + \frac{2\pi}{3})} = \frac{2}{3}.e^{i\frac{2\pi}{3}} \times r_n.e^{i\theta_n} = \frac{2}{3}.e^{i\frac{2\pi}{3}}.z_n$.
$(z_n)_{\mathbb{N}}$ est donc une suite géométrique complexe de raison $q = \frac{2}{3}.e^{i\frac{2\pi}{3}}$ et de premier terme $z_0 = 3$.

2. (a)
$$\begin{aligned} M_nM_{n+1}^2 &= |z_{n+1} - z_n|^2 \\ &= |r_{n+1}(\cos\theta_{n+1} + i\sin\theta_{n+1}) - r_n(\cos\theta_n + i\sin\theta_n)|^2 \\ &= (r_{n+1}\cos\theta_{n+1} - r_n\cos\theta_n)^2 + (r_{n+1}\sin\theta_{n+1} - r_n\sin\theta_n)^2 \\ &= r_{n+1}^2\cos^2\theta_{n+1} + r_{n+1}^2\sin^2\theta_{n+1} + r_n^2\cos^2\theta_n + r_n^2\sin^2\theta_n \\ &\quad - 2r_nr_{n+1}(\cos\theta_{n+1}\cos\theta_n + \sin\theta_{n+1}\sin\theta_n) \end{aligned}$$

CORRIGÉS

$$\begin{aligned} M_nM_{n+1}^2 &= r_{n+1}^2 + r_n^2 - 2r_nr_{n+1}\cos(\theta_{n+1}-\theta_n) \\ &= r_n^2\left[(\tfrac{2}{3})^2 + 1 - 2\tfrac{2}{3}\cos(\tfrac{2\pi}{3})\right] \\ &= 3^2\left(\tfrac{2}{3}\right)^{2n}\left[\tfrac{4}{9}+1+\tfrac{2}{3}\right] \quad = \quad 19\left(\tfrac{2}{3}\right)^{2n} \text{ unités de longueur.} \end{aligned}$$

Ainsi, $M_nM_{n+1} = \sqrt{19}\,\left(\frac{2}{3}\right)^n$ cm.

(b) $I_n = \sum\limits_{k=0}^{n} M_kM_{k+1} = \sqrt{19}\sum\limits_{k=0}^{n}\left(\frac{2}{3}\right)^k = \sqrt{19}\frac{1-\left(\frac{2}{3}\right)^{n+1}}{1-\frac{2}{3}}$
$= 3\sqrt{19}\left[1-\left(\frac{2}{3}\right)^{n+1}\right] \xrightarrow[n\to\infty]{} 3\sqrt{19}.$

Exercice 14 $z' = \frac{2z-i}{iz+1}$.

1. $\left|(\frac{1}{2}+\frac{\sqrt{3}}{2})(1+i)-i\right|^2 = (\frac{1}{2}+\frac{\sqrt{3}}{2})^2+(\frac{1}{2}+\frac{\sqrt{3}}{2}-1)^2 = (\frac{1}{2}+\frac{\sqrt{3}}{2}-1)^2+(\frac{1}{2}+\frac{\sqrt{3}}{2})^2 = 2.$
   De même, $\left|(\frac{1}{2}+\frac{\sqrt{3}}{2})(1+i)-1\right|^2 = 2.$
   De plus, $|AD|^2 = ... = 2$ donc $AD^2 = EA^2 = ED^2$.
   Par ailleurs, $\frac{e-a}{d-a} = ... = \frac{1}{2}+i\frac{\sqrt{3}}{2} = e^{i\frac{\pi}{3}}$ donc $\left(\overrightarrow{AD}\,;\overrightarrow{AE}\right) \equiv \frac{\pi}{3}\,[2\pi]$ et ADE est équilatéral direct.
2. On a $f(1) = \frac{2\times 1-i}{i\times 1+1} = \frac{(2-i)(1-i)}{(1+i)(1-i)} = \frac{1}{2}(2-2i-i-1) = \frac{1}{2}-\frac{3}{2}i$ affixe de D'.
3. (a) Pour $z\neq i$, $(z'+2i)(z-i)=1$
   $\iff (\frac{2z-i}{iz+1}+2i)(z-i)=1 \iff (2z-i+2i(iz+1))(z-i)=iz+1$
   $\iff (2z-i-2z+2i)(z-i)=iz+1 \iff i(z-i)=iz+1$ □
   (b) Ainsi, $(z'-b)(z-a)=1$ donc $|z'-b|\,|z-a|=1$: $BM'\times AM=1$ et $\arg(z'-b)+\arg(z-a)\equiv 0\,[2\pi]$ i.e. $\arg(z'-b)\equiv -\arg(z-a)\,[2\pi]$: $\left(\overrightarrow{u}\,;\overrightarrow{BM'}\right) \equiv -\left(\overrightarrow{u}\,;\overrightarrow{AM}\right)\ [2\pi]$ □
4. (a) On a $|e-a| = |d-a| = |1-i| = \sqrt{1+1} = \sqrt{2}$ donc D et E appartiennent au cercle $\mathscr{C}(A;\sqrt{2})$.
   (b) $\left(\overrightarrow{u}\,;\overrightarrow{BE'}\right) \equiv -\left(\overrightarrow{u}\,;\overrightarrow{AE}\right) \equiv \left(\overrightarrow{AE}\,;\overrightarrow{AD}\right)+\left(\overrightarrow{AD}\,;\overrightarrow{u}\right) \equiv -\frac{\pi}{3}+\frac{\pi}{4} \equiv -\frac{\pi}{12}\,[2\pi].$
   De plus, $BE'\times AE = 1$ donc $BE' = \frac{1}{AE} = \frac{1}{\sqrt{2}}$. On peut alors placer E'.
5. On a $\left(\overrightarrow{BE'}\,;\overrightarrow{BD'}\right) \equiv \left(\overrightarrow{BE'}\,;\overrightarrow{u}\right)+\left(\overrightarrow{u}\,;\overrightarrow{BD'}\right) \equiv \left(\overrightarrow{u}\,;\overrightarrow{AE}\right)-\left(\overrightarrow{u}\,;\overrightarrow{AD}\right)$
   $\equiv \left(\overrightarrow{AD}\,;\overrightarrow{AE}\right) \equiv \frac{\pi}{3}\,[2\pi].$
   De plus, $BD' = \frac{1}{AD} = \frac{1}{AE} = BE'$ donc $BE'D'$ est équilatéral direct.

Exercice 15 QCM vu au BAC

1. On a $|z-(1-2i)| = \left|e^{i\theta}\right| = 1$ donc $\mathscr{E}$ est le cercle de centre d'affixe $1-2i$ et de rayon 1 : (c).
2. (a) Faux : $f(-1-2i) = -i(-1-2i)-2i = i+2i^2-2i = -2-i \neq i.$
   (b) Vrai : $f(-1-i) = -i(-1-i)-2i = i+i^2-2i = -1-i.$
   (c) Vrai : $1 = |z'| = |-iz-2i| = |-i|\,.\,|z+2| = |z-(-2)| = AM.$
   (d) Faux : si $\arg(z)\equiv\frac{\pi}{2}\,[2\pi]$, alors $z = ib\in i\mathbb{R}^+$ et $z' = -iz-2i = b-2i.$
   Le point M' décrit la demi-droite $\{y=-2\ /\ x>0\}$.

3. Posons, $z = x + iy$. (E) devient alors $x + iy + x^2 + y^2 = 7 + i$
$\iff (x + x^2 + y^2 - 7) + i(y-1) = 0$ d'où $y = 1$ et $x^2 + x - 6 = 0$
c.-à-d. $x = 2$ ou $x = -3$.
Ainsi, (E) admet deux solutions $z_1 = -3 + i$ et $z_2 = 2 + i$: (a)
et $\frac{z_1}{z_2} = \frac{-3+i}{2+i} = \frac{(-3+i)(2-i)}{2^2+1^2} = \frac{-6+3i+2i+1}{5} = -1 + i$
$\frac{z_1}{z_2} = \sqrt{2}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \sqrt{2}\, e^{i\frac{3\pi}{4}}$: (c).

Exercice 16 $L_1 : |z + 2 - 3i| = 1$ and $L_2 : \arg(z) = \frac{\pi}{4}\,[2\pi]$.

1. L_1 is the circle centered at $A(3i - 2)$ and of radius 1.
L_2 is the open half-line (ray) initiated from the origin, through the point $B(1 + i)$.
2. Let Δ be the perpendicular line to (OB) through the point A and I be the intersection point of Δ and $L_2 = (OB)$. A simple Pythagorean argument will convince you that the smallest distance between L_1 and L_2 is IJ where the latest is the intersection point of the line Δ and the circle L_1. Since $I \in L_2$, $x_I = y_I$.
Moreover, $(OB) \perp (AI) \iff \overrightarrow{OB} \cdot \overrightarrow{AI} = 0$
$\iff 1 \times (x_I + 2) + 1 \times (y_I - 3) = 0 \iff 2x_I - 1 = 0,$ so $x_I = y_I = \frac{1}{2}$.
Hence, the smallest distance is
$IJ = IA - AJ = \sqrt{(-2 - \frac{1}{2})^2 + (3 - \frac{1}{2})^2} - 1 \simeq 2,54.$

Exercice 17 $z_0 = 1,$ $z_{n+1} = \frac{1}{3}z_n + \frac{2}{3}i,$ $u_n = z_n - i,$ $A_n(z_n),$ $B_n(u_n),$ $C(i)$.

1. Soit $n \in \mathbb{N}$. On a $u_{n+1} = z_{n+1} - i = (\frac{1}{3}z_n + \frac{2}{3}i) - i = \frac{1}{3}z_n - \frac{1}{3}i = \frac{1}{3}(z_n - i) = \frac{1}{3}u_n$
donc $(u_n)_{\mathbb{N}}$ est géométrique de raison $\frac{1}{3}$ et de premier terme $u_0 = z_0 - i = 1 - i$.
Ainsi, pour tout $n \in \mathbb{N}$, $u_n = \frac{1}{3^n}(1 - i)$.
2. (a) Ainsi, $|u_n| = \left|\frac{1}{3^n}(1 - i)\right| = \frac{\sqrt{1^2+1^2}}{3^n} = \frac{\sqrt{2}}{3^n}$.
   (b) D'où $\lim\limits_{n\to\infty} |z_n - i| = \lim\limits_{n\to\infty} |u_n| = \lim\limits_{n\to\infty} \frac{\sqrt{2}}{3^n} = \lim\limits_{n\to\infty} \sqrt{2}(\frac{1}{3})^n = 0$ car $\frac{1}{3} \in\,]-1\,;1[$.
   (c) Ceci signifie que la distance $CA_n = |z_n - i|$ tend vers 0 : les points A_n tendent vers le point C.
3. (a) Soit $n \in \mathbb{N}$. On a $\arg(u_n) \equiv \arg(\frac{1}{3^n}(1 - i))\,[2\pi] \equiv \arg(1 - i)\,[2\pi]$
   $\arg(u_n) \equiv \arg(\sqrt{2}e^{-i\frac{\pi}{4}})\,[2\pi] \equiv -\frac{\pi}{4}\,[2\pi]$.
   (b) Les points $B_n(u_n)$ sont donc tous situés sur la demi-droite ouverte passant par l'origine et par le point d'affixe $1-i$: ils sont donc bien alignés et appartiennent à la droite d'équation $y = -x$.
   (c) On a vu que les points B_n sont sur la droite d'équation $y = -x$ donc $\mathfrak{Im}(u_n) = -\mathfrak{Re}(u_n)$. Puisque $z_n = u_n + i$,
   $\mathfrak{Im}(z_n) = \mathfrak{Im}(u_n + i) = \mathfrak{Im}(u_n) + 1$ et $\mathfrak{Re}(z_n) = \mathfrak{Re}(u_n + i) = \mathfrak{Re}(u_n)$.
   D'où, $\mathfrak{Im}(z_n) = \mathfrak{Im}(u_n) + 1 = -\mathfrak{Re}(u_n) + 1 = -\mathfrak{Re}(z_n) + 1$: les points A_n sont donc situés sur la droite d'équation $y = 1 - x$.

Exercice 18 $z_0 = 0,$ $z_{n+1} = 3iz_n - 1$ et $u_n = z_n + \frac{1}{10} + \frac{3}{10}i$

1. $z = 3iz - 1 \iff (1 - 3i)z = -1 \iff z = -\frac{1}{1-3i} \times \frac{1+3i}{1+3i} = \frac{-1-3i}{1^2+3^2} = -\frac{1}{10} - i\frac{3}{10}$.

CORRIGÉS

2. (a) Soit $n \in \mathbb{N}$. On a
$u_{n+1} = z_{n+1} + \frac{1}{10} + \frac{3}{10}i = (3iz_n - 1) + \frac{1}{10} + \frac{3}{10}i = 3iz_n - \frac{9}{10} \times \frac{3i}{3i} + 3i\frac{1}{10}$
$u_{n+1} = 3iz_n - 3i\frac{3}{10}(-i) + 3i\frac{1}{10} = 3i(z_n + \frac{3}{10}i + \frac{1}{10}) = 3iu_n$.
   (b) Ainsi, $(u_n)_{\mathbb{N}}$ est géométrique, de raison $3i$ et de premier terme
$u_0 = z_0 + \frac{1}{10} + \frac{3}{10}i = \frac{1}{10} + \frac{3}{10}i$.
On a donc, pour tout $n \in \mathbb{N}$, $u_n = (\frac{1}{10} + \frac{3}{10}i)(3i)^n$.
3. (a) Pour $n \in \mathbb{N}$, on a
$A(a)M_n(z_n) = \left|z_n - (-\frac{1}{10} - i\frac{3}{10})\right| = |u_n| = \left|(\frac{1}{10} + \frac{3}{10}i)(3i)^n\right|$
$AM_n = \left|\frac{1}{10} + \frac{3}{10}i\right| |3|^n |i|^n = \frac{\sqrt{1^2+3^2}}{10} \times 3^n \times 1^n = \frac{1}{\sqrt{10}}.3^n \xrightarrow[n\to\infty]{} +\infty$
car $3 > 1$.
   (b) Pour $n \in \mathbb{N}$, on a $\frac{z_{n+2}-a}{z_n-a} = \frac{u_{n+2}}{u_n} = \frac{(3i)^2 u_n}{u_n} = -9$ donc
$\left(\overrightarrow{AM_n}\,;\overrightarrow{AM_{n+2}}\right) \equiv \arg(-9)\,[2\pi] \equiv \pi\,[2\pi]$ et les points A, M_n et M_{n+2} sont alignés.
   (c) Pour $n \in \mathbb{N}$, on a $\frac{z_{n+1}-a}{z_n-a} = \frac{u_{n+1}}{u_n} = \frac{(3i)u_n}{u_n} = 3i$ donc
$\left(\overrightarrow{AM_n}\,;\overrightarrow{AM_{n+1}}\right) \equiv \arg(3i)\,[2\pi] \equiv \frac{\pi}{2}\,[2\pi]$: les vecteurs $\overrightarrow{AM_n}$ et $\overrightarrow{AM_{n+1}}$ sont donc orthogonaux et les droites (AM_n) et (AM_{n+1}) sont perpendiculaires.

Exercice 19 $z' = \dfrac{z+1+3i}{z-2+i}$ et M_0 est la point d'affixe $z_0 = 2 - i$.

1. On a, pour $z = a + ib \neq 2 - i$,
$z' = \frac{z+1+3i}{z-2+i} = \frac{(a+1)+i(b+3)}{(a-2)+i(b+1)} = \frac{[(a+1)+i(b+3)][(a-2)-i(b+1)]}{[(a-2)+i(b+1)][(a-2)-i(b+1)]}$
$= \frac{[(a+1)(a-2)+(b+3)(b+1)]+i[(a-2)(b+3)-(a+1)(b+1)]}{(a-2)^2+(b+1)^2}$
$= \frac{(a^2-a+b^2+4b+1)+i(2a-3b-7)}{(a-2)^2+(b+1)^2}$ et
$z' \in \mathbb{R} \Leftrightarrow 2a - 3b - 7 = 0 \Leftrightarrow b = \frac{2}{3}a - \frac{7}{3} \Leftrightarrow M(z) \in \text{Droite}(y = \frac{2}{3}x - \frac{7}{3}) \setminus \{M_0\}$.
2. Autre méthode :
$z' \in i\mathbb{R} \iff z' = -\overline{z'} \iff \frac{z+1+3i}{z-2+i} = -\frac{\overline{z}+1-3i}{\overline{z}-2-i}$
$\iff (z+1+3i)(\overline{z}-2-i) = -(\overline{z}+1-3i)(z-2+i)$
$\iff z\overline{z} + z(-2-i) + \overline{z}(1+3i) - 2 - i - 6i + 3i^2$
$= -z\overline{z} - \overline{z}(-2+i) - z(1-3i) + 2 - i - 6i + 3i^2$
$\iff 2z\overline{z} + (-1-4i)z + (-1+4i)\overline{z} + 2 = 0 \overset{\alpha=-1-4i}{\iff} 2z\overline{z} + \alpha z + \overline{\alpha z} + 2 = 0$
$\iff 2z\overline{z} + 2\mathfrak{Re}(\alpha z) + 2 = 0 \iff z\overline{z} + \mathfrak{Re}(\alpha z) + 1 = 0$.
On a, pour $z = a + ib$, $z\overline{z} = a^2 + b^2$
et $\alpha z = (-1-4i)(a+ib) = (4b-a) + i(-b-4a)$.
L'équation devient
$a^2 - a + b^2 + 4b + 1 = 0 \iff (a^2 - 2.\frac{1}{2}a + \frac{1}{4}) - \frac{1}{4} + (b^2 + 2b + 4) - 4 + 1 = 0$
$\iff (a - \frac{1}{2})^2 + (b+2)^2 = \frac{13}{4} \iff (M\Omega_{\frac{1}{2}-2i})^2 = \frac{13}{4}$
$\iff M(z) \in \text{Cercle}(\Omega(\frac{1}{2} - 2i); \frac{\sqrt{13}}{2}) \setminus \{M_0\}$.

Exercice 20

A. 1. Soit $z_0 \in \mathbb{C}$ une solution de l'équation $\mathscr{E}: z^4 = -4$.
On a alors $(-z_0)^4 = (-1)^4 z_0^4 = z_0^4 = -4$ et $(\overline{z_0})^4 = \overline{z_0^4} = \overline{-4} = -4$ donc $-z_0$ et $\overline{z_0}$ sont solutions de $\mathscr{E}$.

2. (a) On a $z_0 = 1+i = \sqrt{2}(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}) = \sqrt{2}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})$
$z_0 = \sqrt{2}(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})) = \sqrt{2}e^{i\frac{\pi}{4}}$.
(b) Ainsi, $z_0^4 = \left(\sqrt{2}e^{i\frac{\pi}{4}}\right)^4 = \sqrt{2}^4 e^{i\frac{\pi}{4}\times 4} = 4\times(-1) = -4$: z_0 est solution de $\mathscr{E}$.
(c) D'où, $-z_0 = -1-i$ et $\overline{z_0} = 1-i$ sont solutions de $\mathscr{E}$ et puisque $-z_0$ est solution de $\mathscr{E}$, la question précédente permet d'affirmer que
$\overline{-z_0} = \overline{-1-i} = -1+i$ est aussi une solution de $\mathscr{E}$:
$\mathscr{S} = \{1+i; 1-i; -1+i; -1-i\}$.

B. $z_A = 1+i$, $z_B = -1+i$, $z_C = -1-i$ et $z_D = 1-i$.

1. On a $z_E - z_C = (z_B - z_C)e^{i\frac{\pi}{3}} \iff z_E - (-1-i) = ((-1+i)-(-1-i))(\cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3}))$
$\iff z_E = -1-i+2i(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = -1-\sqrt{3}$ et
$z_F - z_C = (z_D - z_C)e^{i\frac{\pi}{3}} \iff z_F - (-1-i) = ((1-i)-(-1-i))(\cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3}))$
$\iff z_F = -1-i+2(\frac{1}{2} + i\frac{\sqrt{3}}{2}) \iff z_F = (\sqrt{3}-1)i$.

2. On a $\frac{z_A - z_E}{z_A - z_F} = \frac{1+i+1+\sqrt{3}}{1+i-(\sqrt{3}-1)i} = \frac{(2+\sqrt{3})+i}{1+(2-\sqrt{3})i} \times \frac{1-(2-\sqrt{3})i}{1-(2-\sqrt{3})i}$
$\frac{z_A - z_E}{z_A - z_F} = \frac{(2+\sqrt{3})+i-(2+\sqrt{3})(2-\sqrt{3})i-(2-\sqrt{3})i^2}{1^2+(2-\sqrt{3})^2} = \frac{(2+\sqrt{3}+2-\sqrt{3})+i(1-2^2+\sqrt{3}^2)}{1^2+(2-\sqrt{3})^2}$
$= \frac{4}{1^2+(2-\sqrt{3})^2} \in \mathbb{R}$.

3. Ainsi, $\left(\overrightarrow{FA}; \overrightarrow{EA}\right) \equiv \arg\left(\frac{z_A - z_E}{z_A - z_F}\right) [2\pi] \equiv 0\,[\pi]$ et les points A, E et F sont alignés. Puisque ce quotient est positif, on a même $\left(\overrightarrow{FA}; \overrightarrow{EA}\right) \equiv 0\,[2\pi]$ donc $F \in [EA]$.

Exercice 21

(a) $(z+i)^4 = 1 \iff z+i \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} = e^{ki\frac{\pi}{2}} \ / \ k \in [\![0\,;3]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}$
$\iff z \in \mathscr{S}_a = \{1-i\,;\, 0\,;\, -1-i\,;\, -2i\}$.

(b) $z^4 = 81 = 3^4 \iff \frac{z^4}{3^4} = (\frac{z}{3})^4 = 1$
$\iff \frac{z}{3} \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} = e^{ki\frac{\pi}{2}} \ / \ k \in [\![0\,;3]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}$
$\iff z \in \mathscr{S}_b = \{3\,;\, 3i\,;\, -3\,;\, -3i\}$.

(c) $(z-8)^5 = 1$
$\iff z-8 \in \mathbb{U}_5 = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![0\,;4]\!]\} = \{1\,;\, e^{i\frac{2\pi}{5}}\,;\, e^{i\frac{4\pi}{5}}\,;\, e^{-i\frac{4\pi}{5}}\,;\, e^{-i\frac{2\pi}{5}}\}$
$\iff z \in \mathscr{S}_c = \{9\,;\, 8+e^{i\frac{2\pi}{5}}\,;\, 8+e^{i\frac{4\pi}{5}}\,;\, 8+e^{-i\frac{4\pi}{5}}\,;\, 8+e^{-i\frac{2\pi}{5}}\}$.

(d) $z^5 = 4\sqrt{2} = (\sqrt{2})^5 \iff \frac{z^5}{\sqrt{2}^5} = (\frac{z}{\sqrt{2}})^5 = 1$
$\iff \frac{z}{\sqrt{2}} \in \mathbb{U}_5 = \{1\,;\, e^{i\frac{2\pi}{5}}\,;\, e^{i\frac{4\pi}{5}}\,;\, e^{-i\frac{4\pi}{5}} ve^{-i\frac{2\pi}{5}}\}$
$\iff z \in \mathscr{S}_d = \{\sqrt{2}\,;\, \sqrt{2}e^{i\frac{2\pi}{5}}\,;\, \sqrt{2}e^{i\frac{4\pi}{5}}\,;\, \sqrt{2}e^{-i\frac{4\pi}{5}}\,;\, \sqrt{2}e^{-i\frac{2\pi}{5}}\}$.

(e) $z^4 = (1+3i)^4 \iff \left(\frac{z}{1+3i}\right)^4 = 1$
$\iff \frac{z}{1+3i} \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} = e^{ki\frac{\pi}{2}} \ / \ k \in [\![0\,;3]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}$
$\iff z \in \mathscr{S}_e = \{1+3i\,;\, (1+3i)i\,;\, -1-3i\,;\, -(1+3i)i\}$
$= \{1+3i\,;\, -3+i\,;\, -1-3i\,;\, 3-i\}$.

(f) $z^5 = (2+i)^5$
$\iff \frac{z}{2+i} \in \mathbb{U}_5 = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![0\,;4]\!]\} = \{1\,;\, e^{i\frac{2\pi}{5}}\,;\, e^{i\frac{4\pi}{5}}\,;\, e^{-i\frac{4\pi}{5}}\,;\, e^{-i\frac{2\pi}{5}}\}$
$\iff z \in \mathscr{S}_f = \{2+i\,;\, (2+i)e^{i\frac{2\pi}{5}}\,;\, (2+i)e^{i\frac{4\pi}{5}}\,;\, (2+i)e^{-i\frac{4\pi}{5}}\,;\, (2+i)e^{-i\frac{2\pi}{5}}\}$.

CORRIGÉS

(g) $z^5 = 32i = (2i)^5 \iff \left(\frac{z}{2i}\right)^5 = 1$
$\iff \frac{z}{2e^{i\frac{\pi}{2}}} \in \mathbb{U}_5 = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![0\,;4]\!]\} = \{1\,;\, e^{i\frac{2\pi}{5}}\,;\, e^{i\frac{4\pi}{5}}\,;\, e^{-i\frac{4\pi}{5}}\,;\, e^{-i\frac{2\pi}{5}}\}$
$\iff z \in \mathscr{S}_g = \{2i\,;\, 2ie^{i\frac{2\pi}{5}}\,;\, 2ie^{i\frac{4\pi}{5}}\,;\, 2ie^{-i\frac{4\pi}{5}}\,;\, 2ie^{-i\frac{2\pi}{5}}\}$
$\iff z \in \mathscr{S}_g = \{2i\,;\, 2e^{i(\frac{\pi}{2}+\frac{2\pi}{5})}\,;\, 2e^{i(\frac{\pi}{2}+\frac{4\pi}{5})}\,;\, 2e^{-i(\frac{4\pi}{5}-\frac{\pi}{2})}\,;\, 2e^{-i(\frac{2\pi}{5}-\frac{\pi}{2})}\}.$

(h) $z^4 = -9i = 9(-i) = 9e^{i\pi} = (\sqrt{3}e^{i\frac{\pi}{4}})^4 \iff \left(\frac{z}{\sqrt{3}e^{i\frac{\pi}{4}}}\right)^4 = 1$
$\iff \frac{z}{\sqrt{3}e^{i\frac{\pi}{4}}} \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} = e^{ki\frac{\pi}{2}} \ / \ k \in [\![0\,;3]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}$
$\iff z \in \mathscr{S}_h = \{\sqrt{3}e^{i\frac{\pi}{4}}\,;\, \sqrt{3}e^{i\frac{\pi}{4}}e^{i\frac{\pi}{2}}\,;\, \sqrt{3}e^{i\frac{\pi}{4}}e^{-i\pi}\,;\, \sqrt{3}e^{i\frac{\pi}{4}}e^{-i\frac{\pi}{2}}\}$
$\iff z \in \mathscr{S}_h = \{\sqrt{3}e^{i\frac{\pi}{4}}\,;\, \sqrt{3}e^{i\frac{3\pi}{4}}\,;\, \sqrt{3}e^{-i\frac{3\pi}{4}}\,;\, \sqrt{3}e^{-i\frac{\pi}{4}}\}.$

(i) On a $z-1 \neq z+1$ et, pour $z \neq 1$ qui n'est pas solution,
$(z-1)^5 = (z+1)^5 \iff \left(\frac{z+1}{z-1}\right)^5 = 1$
$\iff \frac{z+1}{z-1} \in \mathbb{U}_5 \setminus \{1\} = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![0\,;4]\!]\} \setminus \{1\}$
$\iff \frac{z+1}{z-1} \in \{(\omega_5)^k \ / \ \omega_5 = e^{i\frac{2\pi}{5}},\ k \in [\![1\,;4]\!]\}.$
Or, $\frac{z+1}{z-1} = (\omega_5)^k \iff z+1 = (\omega_5)^k(z-1) \iff z(1-(\omega_5)^k) = -(\omega_5)^k - 1$
$\iff z = \frac{(\omega_5)^k+1}{(\omega_5)^k-1}$ d'où $\mathscr{S}_i = \{\frac{(\omega_5)^k+1}{(\omega_5)^k-1} = \frac{e^{i\frac{2k\pi}{5}}+1}{e^{i\frac{2k\pi}{5}}-1} \ / \ k \in [\![1\,;4]\!]\}.$

(j) On a $z-i \neq z+i$ et, pour $z \neq i$ qui n'est pas solution,
$(z-i)^4 - (z+i)^4 = 0 \iff \left(\frac{z+i}{z-i}\right)^4 = 1$
$\iff \frac{z+i}{z-i} \in \mathbb{U}_4 \setminus \{1\} = \{e^{i\frac{2k\pi}{4}} \ / \ k \in [\![1\,;3]\!]\} = \{i\,;\, -1\,;\, -i\}$
$\iff \frac{z+i}{z-i} \in \{(\omega_4)^k \ / \ \omega_4 = e^{i\frac{k\pi}{2}},\ k \in [\![1\,;3]\!]\}.$
Or, $\frac{z+i}{z-i} = (\omega_4)^k \iff z+i = (\omega_4)^k(z-i) \iff z(1-(\omega_4)^k) = -i(\omega_4)^k - i$
$\iff z = \frac{i(\omega_4)^k+i}{(\omega_4)^k-1}$ d'où
$\mathscr{S}_j = \{\frac{i(\omega_4)^k+i}{(\omega_4)^k-1} \ / \ k \in [\![1\,;3]\!]\} = \{\frac{i\omega+i}{\omega-1} \ / \ \omega \in \{i\,;\, -1\,;\, -i\}\} = \{1\,;\, 0\,;\, -1\}.$

(k) Posons $Z = z^3$. On a $z^6 - 9z^3 + 8 = 0 \iff Z^2 - 9Z + 8 = 0$
$\overset{1\text{racine}}{\iff} (Z-1)(Z-8) = 0$
$\iff Z = z^3 = 1$ ou $Z = z^3 = 8 = 2^3$
$\iff z \in \mathbb{U}_3$ ou $\frac{z}{2} \in \mathbb{U}_3 = \{e^{i\frac{2k\pi}{3}} \ / \ k \in [\![0\,;2]\!]\} = \{1\,;\, j\,;\, j^2\}$
$\iff z \in \mathscr{S}_k = \{1\,;\, j\,;\, j^2\,;\, 2\,;\, 2j\,;\, 2j^2\}.$

(l) Posons $Z = z^2$. On a $z^4 + (1-i)z^2 - i \iff Z^2 + (1-i)Z - i = 0$
$\overset{-1\text{racine}}{\iff} (Z+1)(Z-i) = 0$
$\iff Z = z^2 = -1 = i^2$ ou $Z = z^2 = i = e^{i\frac{\pi}{2}} = \left(e^{i\frac{\pi}{4}}\right)^2$
$\iff \left(\frac{z}{i}\right)^2 = 1$ ou $\left(\frac{z}{e^{i\frac{\pi}{4}}}\right)^2 = 1$
$\iff \frac{z}{i} \in \mathbb{U}_2$ ou $\frac{z}{e^{i\frac{\pi}{4}}} \in \mathbb{U}_2 = \{e^{i\frac{2k\pi}{2}} \ / \ k \in [\![0\,;1]\!]\} = \{-1\,;\, 1\}$
$\iff z \in \mathscr{S}_l = \{-i\,;\, i\,;\, e^{i\frac{\pi}{4}}\,;\, -e^{i\frac{\pi}{4}}\}.$

Exercice 22 $\left(\frac{2z+1}{z-1}\right)^4 = 1.$

Soit $z \neq 1$. On a
$$\left(\frac{2z+1}{z-1}\right)^4 = 1 \iff \frac{2z+1}{z-1} \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} = e^{ki\frac{\pi}{2}} \ / \ k \in [\![0\,;3]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}.$$
Par ailleurs, $\frac{2z+1}{z-1} = \omega \iff 2z+1 = \omega(z-1) \iff (2-\omega)z = -\omega-1 \iff z = \frac{\omega+1}{\omega-2}$

d'où les solutions de l'équation $\mathscr{S} = \{-2\,;\, \frac{i+1}{i-2}\,;\, 0\,;\, \frac{i-1}{2+i}\}$.
Soient $A(-2)$, $B(\frac{i+1}{i-2})$, $O(0)$ et $C(\frac{i-1}{2+i})$ les points images de ces solutions et soit $D(-1)$.
On a $z_B = \frac{i+1}{i-2} = \frac{(i+1)(-i-2)}{(i-2)(-i-2)} = -\frac{1}{5} - \frac{3}{5}i$ et $z_C = \frac{i-1}{i+2} = -\frac{1}{5} + \frac{3}{5}i$.
Ainsi, $DO = |0-(-1)| = 1$, $DA = |z_A - z_D| = 1$,
$DB^2 = \left|-\frac{1}{5} - \frac{3}{5}i - (-1)\right|^2 = (\frac{4}{5})^2 + (\frac{3}{5})^2 = 1^2$
et $DC^2 = \left|-\frac{1}{5} + \frac{3}{5}i - (-1)\right|^2 = (\frac{4}{5})^2 + (\frac{3}{5})^2 = 1^2$.
Les points A, B, C et O appartiennent donc au cercle de centre D et de rayon 1.
Autre méthode : On montre qu'un argument de $\left(\overrightarrow{BA}\,;\overrightarrow{BO}\right)$ et de $\left(\overrightarrow{CO}\,;\overrightarrow{CA}\right)$ est $\frac{\pi}{2}$ grâce aux quotients $\frac{z_O - z_B}{z_A - z_B}$ et $\frac{z_O - z_C}{z_A - z_C}$. Les triangles BOA et COA sont alors rectangles en B et C et les points B et C appartiennent au cercle de diamètre $[OA]$.

Exercice 23 Racines n-ièmes d'un nombre complexe
Soit n un entier naturel non nul et a un nombre complexe non nul.

1. On a $z^n = 0 \iff z = 0$ ou $z = 0$ ou... ou $z = 0 \iff z = 0$: $\mathscr{S}_0 = \{0\}$.
2. On a $z^n = 1 \iff z \in \mathscr{S}_1 = \mathbb{U}_n = \{e^{i\frac{2k\pi}{n}} \;/\; k \in [\![0\,; n-1]\!]\}$.
3. (a) On a $z^3 = -8 = (-2)^3 \iff \frac{z^3}{(-2)^3} = \left(\frac{z}{-2}\right)^3 = 1$
$\iff \frac{z}{-2} \in \mathbb{U}_3 = \{e^{i\frac{2k\pi}{3}} \;/\; k \in [\![0\,; 3-1]\!]\}$
$\iff z \in \{-2e^{i\frac{2k\pi}{3}} \;/\; k \in [\![0\,; 2]\!]\} = \{-2\,;\, -2e^{i\frac{2\pi}{3}}\,;\, -2e^{i\frac{4\pi}{3}}\}$
$\iff z \in \{-2\,;\, 2e^{-i\frac{\pi}{3}}\,;\, 2e^{i\frac{\pi}{3}}\}$
(b) De même, $z^n = a^n \iff \left(\frac{z}{a}\right)^n = 1$
$\iff \frac{z}{a} \in \mathbb{U}_n = \{e^{i\frac{2k\pi}{n}} \;/\; k \in [\![0\,; n-1]\!]\}$
$\iff z \in \{ae^{i\frac{2k\pi}{n}} \;/\; k \in [\![0\,; n-1]\!]\}$.
(c) On a $z_0^2 = (2-i)^2 = 2^2 - 4i + i^2 = 3 - 4i$
et $z_0^4 = (z_0^2)^2 = (3-4i)^2 = 9 - 24i + 16i^2 = -7 - 24i$
donc $z_0 = 2 - i$ est bien solution de l'équation $z^4 + 7 + 24i = 0$.
Cette dernière devient donc $z^4 = -7 - 24i = z_0^4 \iff \left(\frac{z}{z_0}\right)^4 = 1$
$\iff \frac{z}{z_0} \in \mathbb{U}_4 = \{e^{i\frac{2k\pi}{4}} \;/\; k \in [\![0\,; 4-1]\!]\} = \{1\,;\, i\,;\, -1\,;\, -i\}$
$\iff z \in \{1z_0\,;\, iz_0\,;\, -1z_0\,;\, -iz_0\} = \{2-i\,;\, 1+2i\,;\, -2+i\,;\, -1-2i\}$.
4. (a) On a $z^3 = 27i = 27e^{i\frac{\pi}{2}} = 3^3(e^{i\frac{\pi}{6}})^3 \iff \left(\frac{z}{3e^{i\frac{\pi}{6}}}\right)^3 = 1$
$\iff \frac{z}{3e^{i\frac{\pi}{6}}} \in \mathbb{U}_3 = \{e^{i\frac{2k\pi}{3}} \;/\; k \in [\![0\,; 3-1]\!]\} = \{1\,;\, e^{i\frac{2\pi}{3}}\,;\, e^{i\frac{-2\pi}{3}}\}$
$\iff z \in \{3e^{i\frac{\pi}{6}}\,;\, 3e^{i\frac{\pi}{6}}e^{i\frac{2\pi}{3}}\,;\, 3e^{i\frac{\pi}{6}}e^{i\frac{-2\pi}{3}}\} = \{3e^{i\frac{\pi}{6}}\,;\, 3e^{i\frac{5\pi}{6}}\,;\, 3e^{-i\frac{\pi}{2}}\}$.
(b) Puisque $a \neq 0$, on écrit $a = \rho e^{i\theta}$, $z = re^{i\alpha}$ et l'on a
$z^n = a \iff r^n e^{in\alpha} = \rho e^{i\theta} \iff r^n = \rho$ et $n\alpha \equiv \theta\,[2\pi]$
$\iff r = \sqrt[n]{\rho}$ et $\alpha \equiv \frac{\theta}{n}\,[\frac{2\pi}{n}]$
$\iff z = \sqrt[n]{\rho}\, e^{i\frac{\theta + k\times 2\pi}{n}}$ pour $k \in [\![0\,; n-1]\!]$
$\iff z \in \{\sqrt[n]{\rho}\, e^{i\frac{\theta+2k\pi}{n}} \;/\; k \in [\![0\,; n-1]\!]\}$.
(c) $n = 2$, $i = 1e^{i\frac{\pi}{2}}$
et $z^2 = i \iff z \in \{\sqrt[2]{1}\, e^{i\frac{\frac{\pi}{2}+2k\pi}{2}} \;/\; k \in [\![0\,; 2-1]\!]\} = \{e^{i\frac{\pi}{4}}\,;\, e^{-i\frac{3\pi}{4}}\}$.

CORRIGÉS

Exercice 24 Le pentagone

1. (a) Le discriminant de z^2+z-1 valant $1+4=5>0$, l'équation $\mathscr{E}\colon z^2+z-1=0$ admet deux solutions réelles $z_{1,2}=\frac{-1\pm\sqrt{5}}{2}$.

   (b) On a $\mathbb{U}_5=\{e^{i\frac{2k\pi}{5}}\ /\ k\in[\![0\,;4]\!]\}=\{1\,;e^{i\frac{2\pi}{5}}\,;e^{i\frac{4\pi}{5}}\,;e^{i\frac{6\pi}{5}}\,;e^{i\frac{8\pi}{5}}\}$.
   Les points images des racines cinquièmes de l'unité forment donc un polygone régulier à cinq sommets : c'est un pentagone régulier.

2. Puisque $\omega=e^{i\frac{2\pi}{5}}\neq 1$, on a $1+\omega+\omega^2+\omega^3+\omega^4=\frac{1-\omega^5}{1-\omega}=\frac{1-1}{1-\omega}=0$.
   De plus, $\omega^3=(e^{i\frac{2\pi}{5}})^3=e^{i\frac{6\pi}{5}}=e^{-i\frac{4\pi}{5}}=(e^{-i\frac{2\pi}{5}})^2=\overline{\omega}^2$
   et $\omega^4=(e^{i\frac{2\pi}{5}})^4=e^{i\frac{8\pi}{5}}=e^{-i\frac{2\pi}{5}}=\overline{\omega}$.

3. (a) Ainsi, $(\omega+\overline{\omega})^2+(\omega+\overline{\omega})-1=\omega^2+2\omega\overline{\omega}+\overline{\omega}^2+\omega+\overline{\omega}-1$
   $=\omega^2+2\,|\omega|^2+\omega^3+\omega+\omega^4-1=2\times 1^2-1-1=0$
   et $\omega+\overline{\omega}$ est solution de $\mathscr{E}$.

   (b) Ainsi, $\omega+\overline{\omega}=\frac{-1\pm\sqrt{5}}{2}\iff 2\mathfrak{Re}(\omega)=\frac{-1\pm\sqrt{5}}{2}$
   $\iff 2\cos(\frac{2\pi}{5})=\frac{-1\pm\sqrt{5}}{2}\overset{\cos>0}{\iff}\cos(\frac{2\pi}{5})=\frac{\sqrt{5}-1}{4}$ et puisque son sinus est positif, $\sin(\frac{2\pi}{5})=+\sqrt{1-(\frac{\sqrt{5}-1}{4})^2}=\sqrt{\frac{16-\sqrt{5}^2+2\sqrt{5}-1}{16}}=\frac{\sqrt{10+2\sqrt{5}}}{4}$.

4. (a) On cherche donc $z_W\in\mathbb{R}_+$ tel que
   $|z_V-z_A|=|z_W-z_A|\iff\left|i+\frac{1}{2}\right|=\left|z_W+\frac{1}{2}\right|$
   $\iff\sqrt{1^2+(\frac{1}{2})^2}=z_W+\frac{1}{2}\iff z_W=\frac{\sqrt{5}}{2}-\frac{1}{2}$.
   Le point B, milieu du segment $[OW]$, a donc pour affixe
   $z_B=\frac{\sqrt{5}-1}{4}=\cos(\frac{2\pi}{5})$, abscisse du « second » sommet du pentagone.

   (b) Pour tracer un pentagone régulier à la règle non graduée et au compas, on commence par tracer le cercle trigonométrique. Le cercle de centre $A_{-\frac{1}{2}}$ passant par V_i coupe la demi-droite $[OU_1)$ en W. On trace alors la médiatrice de $[OW]$. Elle coupe le cercle trigonométrique en Q et T. On reporte alors la longueur $QU=TU$ de part et d'autre de Q et de T sur le cercle trigonométrique et l'on obtient deux points R et S. Le polygone $QRSTU$ est alors un pentagone régulier.

Exercice 25 Transformée de Fourier discrète

La TDF de $(z_0;z_1;\ldots;z_{n-1})\in\mathbb{C}^n$ est $(Z_0;Z_1;\ldots;Z_{n-1})$ tels que

$$Z_p=\sum_{k=0}^{n-1}z_k\omega^{-kp}\quad\text{où}\quad\omega=e^{\frac{2i\pi}{n}}.$$

1. · Pour $(z_0;z_1)=(1\,,1)$, on a $n=2$, $\omega_2=e^{\frac{2i\pi}{2}}=e^{i\pi}=-1$ et

$$Z_0=\sum_{k=0}^{1}z_k(-1)^{-k\times 0}=z_0(-1)^{-0\times 0}+z_1(-1)^{-1\times 0}=z_0+z_1=2,$$

$$Z_1=\sum_{k=0}^{1}z_k(-1)^{-k\times 1}=z_0(-1)^{-0\times 1}+z_1(-1)^{-1\times 1}=z_0-z_1=0.$$

   La TDF de $(1\,,1)$ est donc $(2\,,0)$.

   · Pour $(z_0;z_1;z_2)=(0\,,1\,,1)$, on a $n=3$, $\omega_3=e^{\frac{2i\pi}{3}}=j$,
   $\omega_3^2=j^2=\overline{j}=\frac{1}{j}=\omega_3^{-1}$, $\omega_3^{-2}=j$

et $\quad Z_0 = \sum_{k=0}^{2} z_k j^{-k\times 0} = 0j^{-0\times 0} + 1j^{-1\times 0} + 1j^{-2\times 0} = 2$,

$Z_1 = \sum_{k=0}^{2} z_k j^{-k\times 1} = 0j^{-0\times 1} + 1j^{-1\times 1} + 1j^{-2\times 1} = \overline{j} + j = 2\mathfrak{Re}(j) = -1$,

$Z_2 = \sum_{k=0}^{2} z_k j^{-k\times 2} = 0j^{-0\times 2} + 1j^{-1\times 2} + 1j^{-2\times 2} = j + j^{-1} = j + \overline{j} = 2\mathfrak{Re}(j) = -1$.

La TDF de $(0, 1, 1)$ est donc $(2, -1, -1)$.

· Pour $\quad (z_0; z_1; z_2; z_3) = (0; 1; i; 0)$, on a $\quad n = 4$, $\quad \omega_4 = e^{\frac{2i\pi}{4}} = i$,
$\omega_4^2 = i^2 = -1$, $\quad \omega_4^3 = -i$, $\quad \omega_4^{-1} = \frac{1}{i} = -i$, $\quad \omega_4^{-2} = -1$, $\quad \omega_4^{-3} = i$, et

$Z_0 = \sum_{k=0}^{3} z_k i^{-k\times 0} = 0i^{-0\times 0} + 1i^{-1\times 0} + i.i^{-2\times 0} + 0i^{-3\times 0} = 1 + i$,

$Z_1 = \sum_{k=0}^{3} z_k i^{-k\times 1} = 0i^{-0} + 1i^{-1} + i.i^{-2} + 0i^{-3} = -2i$,

$Z_2 = \sum_{k=0}^{3} z_k i^{-k\times 2} = 0i^{-0} + 1i^{-2} + i.i^{-4} + 0i^{-6} = -1 + i$,

$Z_3 = \sum_{k=0}^{3} z_k i^{-k\times 3} = 0i^{-0} + 1i^{-3} + i.i^{-6} + 0i^{-9} = 0$.

La TDF de $(0; 1; i; 0)$ est donc $(1 + i; -2i; -1 + i; 0)$.

2. (a) On a $\quad Z_\ell = \sum_{k=0}^{n-1} z_k \omega^{-k\ell}$

et $\quad \sum_{\ell=0}^{n-1} Z_\ell \omega^{\ell p} = \sum_{\ell=0}^{n-1} \left(\sum_{k=0}^{n-1} z_k \omega^{-k\ell} \right) \omega^{\ell p} = \sum_{k=0}^{n-1} \left(z_k \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} \right)$.

(b) Si $\quad k = p$, $\quad$ on a $\quad \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} = \sum_{\ell=0}^{\ell-1} \omega^0 = \sum_{\ell=0}^{\ell-1} 1 = n$

et si $\quad k \neq p$, $\quad \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} = \sum_{\ell=0}^{\ell-1} \left(\omega^{p-k}\right)^\ell$

$$\sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} = \frac{1 - \left(\omega^{p-k}\right)^{n-1+1}}{1 - \left(\omega^{p-k}\right)} = \frac{1 - (\omega^n)^{p-k}}{1 - \omega^{p-k}} = \frac{1 - (1)^{p-k}}{1 - \omega^{p-k}} = 0.$$

(c) Ainsi, $\quad$ pour $k = p$, $\quad z_p \sum_{\ell=0}^{\ell-1} \omega^{(p-p)\ell} = z_p \times n$

et, pour $k \neq p$, $\quad z_k \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} = z_k \times 0 = 0$.

D'où, $\quad \frac{1}{n} \sum_{k=0}^{n-1} \left(z_k \sum_{\ell=0}^{\ell-1} \omega^{(p-k)\ell} \right) = \frac{1}{n}(z_p \times n) = z_p$, $\quad$ TDF inverse de (Z_k).

CORRIGÉS

(d) · Pour $(Z_0;Z_1)=(2\,,\,0)$, on a $n=2$, $\omega_2=-1$ et

$$z_0=\frac{1}{2}\sum_{k=0}^{1}Z_k(-1)^{k\times 0}=\tfrac{1}{2}(z_0(-1)^0+z_1(-1)^0)=\tfrac{1}{2}(z_0+z_1)=\tfrac{2}{2}=1,$$

$$z_1=\frac{1}{2}\sum_{k=0}^{1}Z_k(-1)^{k\times 1}=\tfrac{1}{2}(z_0(-1)^0+z_1(-1)^1)=\tfrac{1}{2}(z_0-z_1)=\tfrac{2}{2}=1.$$

La TDF inverse de $(2\,,\,0)$ est donc bien $(1\,,\,1)$.

· Pour $(Z_0;Z_1;Z_2)=(2\,,\,-1\,,\,-1)$, on a $n=3$, $\omega_3=e^{\frac{2i\pi}{3}}=j$, $\omega_3^2=j^2=\overline{j}$ et

$$z_0=\frac{1}{3}\sum_{k=0}^{2}Z_kj^{k\times 0}=\tfrac{1}{3}(2j^0-j^0-j^0)=0,$$

$$z_1=\frac{1}{3}\sum_{k=0}^{2}Z_kj^{k\times 1}=\tfrac{1}{3}(2j^0-1j^1-j^2)=\tfrac{1}{3}(2-j-\overline{j})=\tfrac{1}{3}(2-2\mathfrak{Re}(j))$$
$$=\tfrac{3}{3}=1,$$

$$z_2=\frac{1}{3}\sum_{k=0}^{2}Z_kj^{k\times 2}=\tfrac{1}{3}(2j^0-j^2-j^4)=\tfrac{1}{3}(2-\overline{j}-j)=\tfrac{1}{3}(2-2\mathfrak{Re}(j))$$
$$=\tfrac{3}{3}=1.$$

La TDF inverse de $(2\,,\,-1\,,\,-1)$ est donc bien $(0\,,\,1\,,\,1)$.

· Pour $(Z_0;Z_1;Z_2;Z_3)=(1+i;-2i;-1+i;0)$,
on a $n=4$, $\omega_4=e^{\frac{2i\pi}{4}}=i$ et

$$z_0=\frac{1}{4}\sum_{k=0}^{3}Z_ki^{k\times 0}=\tfrac{1}{4}((1+i)i^0-2i.i^0+(-1+i)i^0+0i^0)$$
$$=\tfrac{1}{4}(1+i-2i-1+i)=0,$$

$$z_1=\frac{1}{4}\sum_{k=0}^{3}Z_ki^{k\times 1}=\tfrac{1}{4}((1+i)i^0-2i.i^1+(-1+i)i^2+0i^3)$$
$$=\tfrac{1}{4}(1+i-2i^2-(-1+i))=\tfrac{4}{4}=1,$$

$$z_2=\frac{1}{4}\sum_{k=0}^{3}Z_ki^{k\times 2}=\tfrac{1}{4}((1+i)i^0-2i.i^2+(-1+i)i^4+0i^6)$$
$$=\tfrac{1}{4}(1+i+2i-1+i))=\tfrac{4i}{4}=i,$$

$$z_3=\frac{1}{4}\sum_{k=0}^{3}Z_ki^{k\times 3}=\tfrac{1}{4}((1+i)i^0-2i.i^3+(-1+i)i^6+0i^9)$$
$$=\tfrac{1}{4}(1+i-2-(-1+i))=0.$$

La TDF inverse de $(1+i;-2i;-1+i;0)$ est donc bien $(0;1;i;0)$.

Chapitre IX

NOMBRES PREMIERS

Sommaire

Les nombres premiers sont utiles, voire essentiels dans un nombre considérable de domaines, tant en mathématiques pures qu'appliquées mais ils nous sont encore bien mystérieux. La détermination de l'ensemble des nombres premiers est un immense problème des mathématiques. Quels sont-ils ? Peut-on trouver une formule explicite les donnant tous ou presque ? Comment sont-ils répartis ? La recherche autour des nombres premiers, multimillénaire, est encore très active et les conjectures sont nombreuses. Nous étudions ici leurs premières propriétés mais rien ne vous interdit d'investiguer un peu plus loin.

1 L'ensemble des nombres premiers

Définition 1
Un entier naturel est un nombre premier s'il admet exactement deux diviseurs positifs, 1 *et lui-même.*

Exemples : 3, 5, 11, 23 sont premiers, 6 n'est pas premier car il est divisible par $3 \in [\![2\,;5]\!]$, 1 n'est pas premier car il n'admet qu'un seul diviseur positif, 0 non plus car il en admet une infinité.
On se reportera à l'exercice *ad hoc* n° 2 en page 227 pour la liste des nombres premiers inférieurs à 100.

Remarques : • Trivialement, le seul nombre premier pair est 2.

• Un nombre est premier si ses seuls diviseurs sont ses diviseurs *triviaux* (1 et lui-même), autrement dit, s'il n'admet pas de diviseurs *propres* c.-à-d. non triviaux. Par exemple, 9 admet un seul diviseur propre ou non trivial, 3, et deux diviseurs stricts, 1 et 3.

• Nous pourrons noter $\mathfrak{P}$ l'ensemble des nombres premiers.

Théorème 1 *Soient a, b et n trois entiers non nuls et p un nombre premier.*
On a $p \big| ab \iff p \big| a$ *ou* $p \big| b$ *et* $p \big| a^n \iff p \big| a$.

Démonstration : Seuls les sens directs sont à démontrer, les réciproques étant évidentes.
On sait depuis le cours sur le PGCD (cf. 141) que
$\mathrm{PGCD}(p, a) = 1$ et $\mathrm{PGCD}(p, b) = 1 \iff \mathrm{PGCD}(p, ab) = 1$
et $\mathrm{PGCD}(a^n, p) = 1 \iff \mathrm{PGCD}(a, p) = 1$.
De plus, pour tout entier c, $\mathrm{PGCD}(c, p) = 1$ ou p puisque p est premier.
D'où, si $p|ab$, alors $ab \wedge p \geqslant p > 1$ donc $a \wedge p \neq 1$ ou $b \wedge p \neq 1$.
Ainsi, $a \wedge p = p$ ou $b \wedge p = p$ et $p|a$ ou $p|b$.
Si $p|a^n = a.a^{n-1}$, alors $p|a$ ou $p|a^{n-1}$... □

Propriété 1
Tout nombre entier supérieur ou égal à deux est divisible par un nombre premier.

Démonstration : Elle s'effectue par *récurrence forte.*
Soit, pour $n \geqslant 2$, la propriété $\mathscr{P}_n$: « Il existe un nombre premier p divisant n. »
· On a $2|2$ et 2 est premier donc $\mathscr{P}_2$ est vraie.
· Soit $n \geqslant 2$. Supposons, par récurrence forte, que $\mathscr{P}_k$ soit vraie pour tous les entiers $k \in [\![2 ; n]\!]$ (pour tous les termes précédents et pas seulement le précédent).
Si $n+1$ est premier, $n+1|n+1$ et $\mathscr{P}_{n+1}$ est vraie.
Sinon, $n+1$ n'est pas premier et admet donc un diviseur propre, un diviseur positif a différent de 1 et de $n+1$. Il existe alors deux entiers a, $b \in [\![2 ; n]\!]$ tels que $n+1 = ab$. Puisque $\mathscr{P}_a$ est vraie par hypothèse de récurrence, il existe un nombre premier p qui divise a et l'on peut écrire $a = pq$. Ainsi, $n+1 = ab = (pq)b = p(qb)$ et p est un nombre premier qui divise $n+1$: $\mathscr{P}_{n+1}$ est vraie.
· $\mathscr{P}_n$ est vraie pour tout $n \geqslant 2$. □

Propriété 2 *Tout entier $n \geqslant 2$ non premier est divisible par un nombre premier compris entre 2 et $\sqrt{n}$.*

Démonstration : Puisque n n'est pas premier, il admet des diviseurs propres : il existe deux entiers a, $b \in [\![2 ; n-1]\!]$ tels que $n = ab$.
Supposons, par l'absurde, que a et b sont tous deux strictement supérieurs à $\sqrt{n}$. On a alors, par produit de positifs, $ab > \sqrt{n}^2 = n$ $\lightning$ Ainsi, il existe un diviseur propre de n inférieur ou égal à $\sqrt{n}$, disons a. Puisque $a \geqslant 2$, il existe un nombre premier p qui divise a (d'après la propriété 1 précédente). On a alors $p|a|n$ et $p \leqslant a \leqslant \sqrt{n}$. □

Pour démontrer qu'un entier est premier, il suffit donc de vérifier qu'il n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée.

Exemple : 139 est-il premier ? On a $n = 139 < 144$ donc $\sqrt{n} < 12$. Puisque 139 n'est pas divisible par 2, 3, 5, 7 ou 11, il est premier : $139 \in \mathfrak{P}$.

L'élégante démonstration de la propriété suivante est due au remarquable Euclide.

Propriété 3 *Il existe une infinité de nombres premiers.*

Démonstration : Supposons par l'absurde que l'ensemble des nombres premiers est fini. On peut alors écrire $\mathfrak{P} = \{p_1; p_2; \ldots; p_n\}$.
Soit l'entier $N = p_1 \times p_2 \times \ldots \times p_n + 1$. Puisque trivialement $N \geqslant 2$, la propriété 1 permet d'affirmer qu'il existe $p_i \in \mathfrak{P}$ qui divise N. Or p_i divise $p_1 \times p_2 \times \ldots \times p_n$.
Donc, p_i divise la différence $N - p_1 p_2 \ldots p_n = 1$ ce qui est absurde car $p_i > 1$. $\square$

Remarque : Cette démonstration ne nous permet malheureusement pas de construire de nouveaux nombres premiers. En effet, le produit des premiers premiers plus un n'est pas nécessairement premier. Par exemple, $2 \times 3 \times 5 + 1 = 31$ est premier, tout comme $2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$, ce qui est moins évident.
En revanche, $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$
et $2 \times 3 \times 5 \times \ldots \times 17 + 1 = 510\,511 = 19 \times 26869$ ne le sont pas.

2 Décomposition en facteurs premiers

Écrivons tout d'abord les nombres suivants sous forme de produit de facteurs premiers : $12 = 2^2 \times 3^1$, $18 = 2^1 \times 3^2$, $100 = 2^2 \times 5^2$. Une telle décomposition est possible pour tous les nombres entiers.

Théorème 2 ***Décomposition en facteurs premiers***
Tout entier naturel $n \geqslant 2$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de nombres premiers :
Si $n \geqslant 2$, il existe des nombres premiers p_1, p_2,..., $p_k \in \mathfrak{P}$ et des entiers non nuls α_1, α_2,..., $\alpha_k \in \mathbb{N}^*$ tels que $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$, écriture unique à l'ordre près.

Exemples : On déterminera un telle décomposition par divisions successives et on l'écrira généralement par ordre croissant (*p.o.c.*) des facteurs premiers. ◦ $31 = 31^1$
◦ $132 = 2^2.3^1.11^1$ ◦ $252 = 2^2.3^2.7^1$ ◦ $27\,225 = 3^2.5^2.11^2$ ◦ $1\,090\,397 = 7^3.11^1.17^2$

Démonstration : • Existence :
Soit, pour $n \geqslant 2$, la proposition $\mathscr{P}_n$: « n se décompose en produit de facteurs premiers. »
· On a $2 \in \mathfrak{P}$ donc $\mathscr{P}_2$ est vraie.
· Soit $n \geqslant 2$ et supposons, par récurrence forte, que $\mathscr{P}_k$ est vraie pour tout $k \in [\![2\,; n]\!]$.
Si $n + 1$ est premier, alors $\mathscr{P}_{n+1}$ est vraie.
Sinon, $n+1$ admet des diviseurs propres et il existe a et $b \in [\![2\,; n]\!]$ tels que $n+1 = ab$.

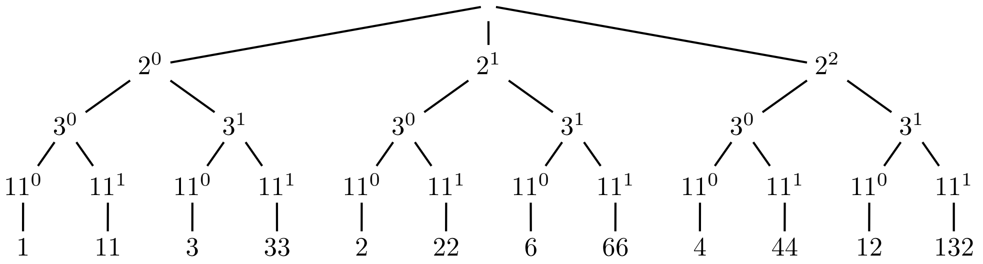
On peut alors écrire, par hypothèse de récurrence, a et b comme produits de facteurs premiers et donc $n+1$ aussi : $\mathscr{P}_{n+1}$ est vraie.
· $\mathscr{P}_n$ est vraie pour tout $n \geqslant 2$.
• Unicité :
Soit $n \geqslant 2$ et supposons que $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et $q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ soient deux décompositions de n en facteurs premiers rangés dans l'ordre croissant. On a alors $p_1^{\alpha_1}(p_2^{\alpha_2} \dots p_r^{\alpha_r}) = q_1^{\beta_1}(q_2^{\beta_2} \dots q_s^{\beta_s})$. Si $p_1 < q_1$ alors p_1 et q_1 sont premiers entre eux, tout comme $p_1^{\alpha_1}$ et $q_1^{\beta_1}$. Le théorème de Gauss permet d'affirmer que $p_1^{\alpha_1}$ divise $q_2^{\beta_2} \dots q_s^{\beta_s}$ donc p_1 divise $q_2^{\beta_2} \dots q_s^{\beta_s}$ ce qui est impossible car p_1 est premier avec chacun des q_i (il est strictement inférieur à ceux-ci et ils sont tous premiers). De même, $q_1 < p_1$ mène à la contradiction q_1 divise $p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et l'on a nécessairement $p_1 = q_1$.
Si maintenant $\alpha_1 < \beta_1$, on peut simplifier la décomposition :
$p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1 - \alpha_1}(q_2^{\beta_2} \dots q_s^{\beta_s})$ ce qui est impossible car $q_1 = p_1$ est premier avec p_2,..., p_r. De même, $\beta_1 < \alpha_1$ mène à une contradiction et l'on a nécessairement $\alpha_1 = \beta_1$.
On a donc montré que le premier terme $p_1^{\alpha_1}$ d'une décomposition en facteurs premiers par ordre croissant est unique. Il suffit alors de simplifier la décomposition par ce terme pour montrer que le deuxième est unique, ainsi que les suivants. □

Remarques : • La démonstration de l'existence ressemble fortement à celle de l'existence d'un diviseur premier (prop. 1). On peut en effet faire un raisonnement l'utilisant : Soit q_1 le plus petit diviseur premier de n (qui existe d'après cette proposition justement). On a $n = q_1 a_1$. Soit q_2 le plus petit diviseur de a_1... Les a_i sont strictement décroissants jusqu'à $a_r = 1$ et l'on a obtenu la décomposition $n = q_1 q_2 ... q_r$.
• Voici une version simplifiée de la démonstration de l'unicité.
On pose $n = p^{\alpha} a = p^{\beta} b$ avec a, b produits de premiers distincts de p et α, $\beta \geqslant 0$. On montre alors que l'on a nécessairement $\alpha = \beta$ grâce au théorème de Gauss. Ainsi, le terme en p d'une décomposition en facteurs premiers est unique.

Propriété 4 *Soit* $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ *la décomposition en facteurs premiers p.o.c. d'un entier* $n \geqslant 2$.
Les diviseurs de n *sont exactement les nombres de la forme* $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$ *où* $0 \leqslant \beta_i \leqslant \alpha_i$ *et il y a* $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ *diviseurs de* n.

Démonstration : · On a $\dfrac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}} = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k} \in \mathbb{N}$ car $\alpha_i - \beta_i \geqslant 0$ donc $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ divise $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
· Soit d un diviseur de $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (*p.o.c.*) et soit $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ sa décomposition en facteurs premiers *p.o.c.* On a alors $q_1^{\beta_1} | n$ et un raisonnement analogue à celui de la démonstration de l'unicité de la décomposition en facteurs premiers mène à $q_1 = p_1$ et $\beta_1 \leqslant \alpha_1$.
· Puisqu'il existe $\alpha_i + 1$ entiers dans $[\![0 ; \alpha_i]\!]$, les diviseurs de n sont bien au nombre de $\displaystyle\prod_{i=1}^{k} (\alpha_i + 1)$. □

Exemples : ◦ $31 = 31^1$ donc les diviseurs de 31 sont $31^0 = 1$ et $31^1 = 31$. Il y en a bien $(1+1) = 2$.
◦ $132 = 2^2.3.11$ donc les diviseurs de 132 sont
$\{2^0.3^0.11^0; 2^1.3^0.11^0; 2^2.3^0.11^0; 2^0.3^1.11^0; 2^1.3^1.11^0; 2^2.3^1.11^0;$
$2^0.3^0.11^1; 2^1.3^0.11^1; 2^2.3^0.11^1; 2^0.3^1.11^1; 2^1.3^1.11^1; 2^2.3^1.11^1\}$.
Il y en a bien $(2+1)(1+1)(1+1) = 12$ et il est certainement préférable de les présenter dans un arbre de choix.



Avant d'étudier la proposition suivante, on pourra se reporter à l'exercice n° 28 en page 146 pour une définition et un premier travail sur le PPCM, le *plus petit commun multiple*.

Propriété 5 *Soient m et n deux entiers supérieurs ou égaux à 2. En s'autorisant des exposants nuls, on peut supposer qu'ils peuvent s'écrire en produits de facteurs premiers de la manière suivante :*
$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$ *et* $n = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$.
On a $\mathrm{PGCD}\,(m\,,\,n) = m \wedge n = p_1^{min(\alpha_1\,,\,\beta_1)} \times p_2^{min(\alpha_2\,,\,\beta_2)} \times \ldots \times p_k^{min(\alpha_k\,,\,\beta_k)}$
et $\mathrm{PPCM}\,(m\,,\,n) = m \vee n = p_1^{max(\alpha_1\,,\,\beta_1)} \times p_2^{max(\alpha_2\,,\,\beta_2)} \times \ldots \times p_k^{max(\alpha_k\,,\,\beta_k)}$.

Démonstration : • PGCD :
· Puisque $min\,(\alpha_i\,,\,\beta_i) \leqslant \alpha_i$ pour tout $i \in [\![\,1\,;k\,]\!]$, on a $p_i^{min(\alpha_i\,,\,\beta_i)} | p_i^{\alpha_i}$ et de même pour l'entier β_i : $p_1^{min(\alpha_1\,,\,\beta_1)} p_2^{min(\alpha_2\,,\,\beta_2)} \ldots p_k^{min(\alpha_k\,,\,\beta_k)}$ est donc un diviseur de m et de n.
· Soit d un diviseur commun à m et n.
D'après la propriété 4, d peut s'écrire $p_1^{\gamma_1}.p_2^{\gamma_2} \ldots p_k^{\gamma_k}$ avec $\gamma_i \leqslant \alpha_i$ car il divise m et $\gamma_i \leqslant \beta_i$ car il divise n. On a donc $\gamma_i \leqslant min\,(\alpha_i\,,\,\beta_i)$ pour tout $i \in [\![\,1\,;k\,]\!]$ et $d \leqslant p_1^{min(\alpha_1\,,\,\beta_1)} p_2^{min(\alpha_2\,,\,\beta_2)} \ldots p_k^{min(\alpha_k\,,\,\beta_k)}$, ce dernier étant donc le $\mathrm{PGCD}\,(m\,,\,n)$.
• PPCM :
· Puisque $max\,(\alpha_i\,,\,\beta_i) \geqslant \alpha_i$ pour tout $i \in [\![\,1\,;k\,]\!]$, $p_i^{max(\alpha_i\,,\,\beta_i)}$ est multiple de $p_i^{\alpha_i}$ et de même pour β_i : $p_1^{max(\alpha_1\,,\,\beta_1)} p_2^{max(\alpha_2\,,\,\beta_2)} \ldots p_k^{max(\alpha_k\,,\,\beta_k)}$ est donc un multiple de m et de n.
· Soit $C = p_1^{\gamma_1}.p_2^{\gamma_2} \ldots p_r^{\gamma_r}$ un multiple commun à m et n. On a donc $m|C$ et d'après la propriété 4, m s'écrit $p_1^{\delta_1}.p_2^{\delta_2} \ldots p_r^{\delta_r}$ avec $\delta_i \leqslant \gamma_i$. Puisque la décomposition de m en facteurs premiers *p.o.c.* est unique, on a $\alpha_i = \delta_i \leqslant \gamma_i$. De même avec n, $\beta_i \leqslant \gamma_i$. D'où $\gamma_i \geqslant max\,(\alpha_i\,,\,\beta_i)$ pour

tout i et $C \geqslant p_1^{max(\alpha_1, \beta_1)} p_2^{max(\alpha_2, \beta_2)} \dots p_k^{max(\alpha_k, \beta_k)}$, ce dernier étant donc le PPCM (m, n). $\square$

Exemples : ◦ $132 = 2^2.3^1.7^0.11^1$ et $252 = 2^2.3^2.7^1.11^0$
donc PGCD $(132, 252) = 2^2.3^1.7^0.11^0 = 12$
et PPCM $(132, 252) = 2^2.3^2.7.11 = 2772$.
◦ $27\,225 = 3^2.5^2.11^2$ et $1\,090\,397 = 7^3.11.17^2$
donc PGCD $(27225, 1\,090\,397) = 3^0.5^0.7^0.11^1.17^0 = 11$
et PPCM $(27225, 1\,090\,397) = 3^2.5^2.7^3.11^2.17^2$.

Remarques : • Toutefois, l'algorithme d'Euclide est souvent plus rapide pour déterminer le PGCD.

• Nous retrouvons alors très rapidement le résultat de l'exercice n° 28 en page 146 :

$\boldsymbol{m \times n = \mathbf{PGCD}\,(m, n) \times \mathbf{PPCM}\,(m, n)}$.

En effet, on a toujours $min(\alpha_i, \beta_i) + max(\alpha_i, \beta_i) = \alpha_i + \beta_i$.

3 Le petit théorème de Fermat

Énoncé par Fermat en 1640, il n'en publie aucune démonstration, comme à son habitude. Leibniz puis Euler seront ensuite plus précis et Gauss en fera la renommée au XIXᵉ s.

Commençons par quelques calculs introductifs.

$\binom{7}{4} = 35 = 7 \times 5$ et $7 \mid \binom{7}{4}$, $\binom{13}{10} = 286 = 13 \times 22$ et $13 \mid \binom{13}{10}$,
$5^2 = 25 = 5 + 2 \times 10 \equiv 5\,[2]$, $3^5 = 243 = 3 + 5 \times 48 \equiv 3\,[5]$,
$4^3 = 64 = 4 + 3 \times 20 \equiv 4\,[3]$,
$4^2 = 16 = 1 + 3 \times 5 \equiv 1\,[3]$, $6^4 = 1296 = 1 + 5 \times 259 \equiv 1\,[5]$,
$4^6 = 4096 = 1 + 7 \times 585 \equiv 1\,[7]$.

Sous certaines conditions, ceci peut être généralisé.

Lemme 1 *Soit p un nombre premier.*
Pour tout entier $k \in [\![1 ; p-1]\!]$, p divise $\binom{p}{k}$.

Démonstration : En effet, pour tout $k \in [\![1 ; p-1]\!]$,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \times (p-1)!}{k \times (k-1)! \times ((p-1)-(k-1))!} = \frac{p}{k}\binom{p-1}{k-1} \quad \text{donc} \quad k\binom{p}{k} = p\binom{p-1}{k-1}$$

et puisque p et k sont premiers entre eux, il divise $\binom{p}{k}$. $\square$

Théorème 3 ***Petit théorème de Fermat***
Soient un entier n et un nombre premier p. On a $n^p \equiv n\,[p]$.

Démonstration : Soit $p \in \mathfrak{P}$. Pour $n \in \mathbb{N}$, on nomme $\mathscr{P}_n$ la proposition « $n^p \equiv n\,[p]$ ».
· On a $0^p = 0 \equiv 0\,[p]$: $\mathscr{P}_0$ est vraie.
· Supposons $\mathscr{P}_n$ vraie pour $n \in \mathbb{N}$. La formule du binôme de Newton donne alors $(n+1)^p = \displaystyle\sum_{k=0}^{p} \binom{p}{k} n^k.1^{p-k}$ où p divise tous les coefficients binomiaux sauf éven-

tuellement le premier et le dernier d'après le lemme 1.
Ainsi, $(n+1)^p \equiv \binom{p}{0} n^0.1^p + 0 + \binom{p}{p} n^p.1^0\,[p] \equiv 1 + n^p\,[p]$. Par hypothèse de récurrence, $n^p \equiv n\,[p]$ donc $(n+1)^p \equiv n+1\,[p]$ et $\mathscr{P}_{n+1}$ est vraie.
· $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$. □

Remarque : La réciproque est fausse : $1^4 \equiv 1\,[4]$ mais 4 n'est pas premier. Plus difficile, $2^{341} \equiv 2\,[341]$ et pourtant $341 = 11 \times 31$ n'est pas premier. Il est même prouvé que $n^{561} \equiv n\,[561]$ pour tout entier n alors que $561 = 3 \times 11 \times 17$ n'est pas premier : de tels nombres sont appelés *nombres de Carmichael*, mathématicien états-unien du XX^e s.

Exemple : Puisque $5 \in \mathfrak{P}$, $12^5 \equiv 12\,[5] \equiv 2\,[5]$.

Théorème 4 ***Petit théorème de Fermat (bis)***
Soit n un entier. Si p est un nombre premier ne divisant pas n, alors $n^{p-1} \equiv 1\,[p]$.

Démonstration : On a $n^p \equiv n\,[p]$ donc $n^p - n = n(n^{p-1} - 1) \equiv 0\,[p]$ et $p\,|\,n(n^{p-1}-1)$. Si p ne divise pas n, le théorème de Gauss permet d'affirmer que $p\,|\,n^{p-1} - 1$ c.-à-d. $n^{p-1} \equiv 1\,[p]$. □

Exemple : 9 n'est pas divisible par $5 \in \mathfrak{P}$ donc $9^4 \equiv 1\,[5]$.

Remarques : • Les deux petits théorèmes de Fermat sont en fait équivalents :
Si p divise n, alors p divise n^p donc $n^p - n$ et l'on a $n^p - n \equiv 0\,[p]$.
Si p ne divise pas n, alors le petit Fermat (bis) affirme que $n^{p-1} \equiv 1\,[p]$ donc $n \times n^{p-1} \equiv n \times 1\,[p]$.
• La réciproque est fausse. Par exemple, pour $p = 15$ et $n = 4$, on a $4^{14} - 1 = 268\,435\,455 = 15 \times 17\,895\,697 \equiv 0\,[15]$ et pourtant, 15 n'est pas premier.
En revanche, il est intéressant de regarder le cas de tous les entiers n inférieurs à p :
Par contraposition, si p n'est pas premier, il existe un diviseur non trivial d de p. On a $1 < d < p$ et pour tout $k \in \mathbb{Z}$, $d^{p-1} - kp \neq 1$ car divisible par d. D'où l'existence d'un entier d inférieur à p tel que $d^{p-1} \not\equiv 1\,[p]$.
Nous obtenons alors un test peu efficace de *primalité* en n'étudiant que les entiers inférieurs à p :

p est premier si, et seulement si, pour tout $1 \leqslant n < p$, $n^{p-1} \equiv 1\,[p]$.

Il existe bien d'autres théorèmes dus à Fermat dans des domaines très divers. Citons le dernier et le plus fameux théorème de Fermat, énoncé par celui-ci au XVII^e s. sans démonstration connue et démontré en 1994 par Andrew Wiles :

Pour tout $n \geqslant 3$, il n'existe pas de nombres entiers positifs non nuls x, y et z tels que $x^n + y^n = z^n$.

4 Problèmes ouverts

Quels sont donc les nombres premiers ? Certaines fonctions usuelles peuvent nous en donner : Euler, encore lui, a démontré que les images des entiers de $[\![\,0\,;39\,]\!]$ par

$n^2 + n + 41$ sont toutes des nombres premiers. En 2018, le plus grand connu était le nombre de Mersenne (cf. exercice n° 18 p.228) $2^{82\,589\,933} - 1$ mais on est très loin de tous les connaître. On ne connaît pas non plus leur répartition même si un théorème démontré en 2004 assure que pour tout entier k, il existe une infinité de suites de k nombres premiers en progression arithmétique, c'est-à-dire de la forme : a, $a + b$, $a + 2b$, $\dots$, $a + (k - 1)b$.

Il reste une multitude de questions ouvertes sur les nombres premiers. En voici quelques-unes.

- La conjecture de Goldbach : tout nombre pair strictement supérieur à 2 peut-il vraiment s'écrire comme somme de deux nombres premiers ?
- Existe-t-il une infinité de jumeaux premiers ? Un couple de nombres premiers jumeaux est une paire de nombres premiers dont la différence est égale à 2, comme 11 et 13.
- La conjecture de De Polignac : tout entier naturel pair peut-il vraiment s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières ?
- Toute suite de Fibonacci dont les deux termes initiaux sont premiers entre eux contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ou de Mersenne (cf. exercices n° 13 p.235 et n° 18 p.228) ?
- Existe-t-il une infinité de nombres premiers de la forme $n^2 + 1$?
- Existe-t-il une infinité de nombres premiers factoriels (de la forme $n! \pm 1$) ?
- Existe-t-il une infinité de nombres premiers primoriels (du type $p_1.p_2 \dots p_n \pm 1$) ?
- Legendre affirme qu'il existe toujours au moins un nombre premier entre n^2 et $(n + 1)^2$. Cette conjecture est liée à l'hypothèse de Riemann et, comme cette dernière, elle n'est pas démontrée.

Vous voilà paré pour une grande carrière de mathématicien, tout du moins, pour un grand oral !

Exercices

Nombres Premiers

Exercice 1 Soit n un entier supérieur ou égal à 2.
Le nombre n^2-1 peut-il être premier ?

Exercice 2 Crible d'Érathosthène.
Lister tous les entiers de 1 à 100. Barrer successivement 1, puis tous les multiples de 2 sauf 2, puis tous les multiples non déjà barrés de 3 sauf 3, puis tous les multiples non déjà barrés de 5 sauf 5, puis enfin tous les multiples non déjà barrés de 7 sauf 7. Que peut-on dire des nombres non barrés ?

Exercice 3 Un bon début
Pour tout entier $n \in \mathbb{N}$, on pose $P_n = n^2+n+17$.
Montrer que $P_k \in \mathfrak{P}$ pour tout $k \in [\![0\,;15]\!]$ mais que $P_{16} \notin \mathfrak{P}$.

Exercice 4 Les nombres 117, 383, 143 et 337 sont-ils premiers ?

Exercice 5 Nombres premiers jumeaux
Des nombres premiers sont dits jumeaux lorsque leur différence égale 2. Par exemple, 3 et 5 le sont. L'existence d'une infinité de premiers jumeaux n'est encore qu'une conjecture. Les plus grands nombres premiers jumeaux connus (en 2016) sont
$2\,996\,863\,034\,895 \times 2^{1\,290\,000} \pm 1$; ils possèdent $388\,342$ chiffres en écriture décimale.

1. Donner cinq autres exemples de couples de premiers jumeaux.
2. Montrer que 1619 et 1621 sont des premiers jumeaux.

Exercice 6 Pour quels entiers premiers p, l'entier $7p+1$ est-il un carré parfait ?

Exercice 7 Soit $n \geqslant 3$. Existe-t-il des valeurs de l'entier naturel n telles que $a = n^2-2n-3$ soit un nombre premier ? Et pour $b = n^2+2n+1$?

Exercice 8 Soit $n \geqslant 3$. Montrer que si n^2-2n+3 est premier, alors $n \equiv 4\,[6]$.
La réciproque est-elle vraie ?

Exercice 9 Montrer que si la somme de deux entiers non nuls est un nombre premier, alors ils sont premiers entre eux.

Exercice 10 Existe-t-il un nombre premier p tel que $\mathrm{PGCD}\,(\,p\,,\,3\,) = 3$? Si oui, combien en existe-t-il ?

Exercice 11

1. Montrer que si p est un nombre premier strictement supérieur à 3, alors il est de la forme $3k \pm 1$ où $k \in \mathbb{N}^*$.
2. Montrer que tout nombre premier supérieur ou égal à 3 est congru à ± 1 modulo 4.
3. Les réciproques sont-elles vraies ?

Exercice 12 On souhaite déterminer tous les entiers naturels n tels que $n+1$, $n+3$, $n+7$, $n+9$, $n+13$ et $n+15$ soient premiers.

1. Quels sont les entiers n de $[\![0\,;5]\!]$ qui conviennent ?
2. Montrer qu'aucun nombre n strictement supérieur à 5 ne convient.

Exercice 13 Les nombres de Fermat
Pour $n \in \mathbb{N}^*$, on définit le n^{e} nombre de Fermat par $F_n = 2^{2^n} + 1$. Ce grand mathématicien pensait que ces nombres étaient tous premiers.

1. Vérifier que $F_k \in \mathfrak{P}$ pour tout $k \in [\![1\,;4]\!]$.
2. Calculer le PGCD de F_5 et de 641 puis conclure.

Exercice 14

1. Montrer qu'un premier strictement supérieur à 3 est congru à ± 1 modulo 6.
2. Colette dit à Agathe : « Choisis un nombre premier différent de 2 et de 3, élève-le au carré, ajoute 17 puis calcule le résidu (le reste) modulo 12. »
   Agathe : « Ça y est. »
   Colette : « C'est 6, n'est-ce pas ? »
   Agathe : « Incroyable ! Comment as-tu fait ? Ah oui, je vois. »
   Et toi, vois-tu ?

Exercice 15 Pierre de Fermat : « Un nombre premier autre que 2 peut toujours s'écrire de manière unique comme différence de deux carrés parfaits. »

1. Vérifier ce résultat pour les premiers nombres premiers.
2. Démontrons donc cette propriété.
   (a) Supposons qu'un nombre premier p peut s'écrire comme différence de deux carrés : $p = a^2 - b^2$. Exprimer a et b en fonction de p.
   (b) Montrer la réciproque puis conclure.

Exercice 16 Soient p et q deux nombres premiers consécutifs impairs.

1. Montrer que $n = \frac{p+q}{2}$ n'est pas premier.
2. En déduire que $p+q$ est le produit d'au moins trois nombres premiers.

Exercice 17 Les nombres $29! + 17$ et $45! + 38$ sont-ils premiers ?
Déterminer un intervalle d'amplitude $n \in \mathbb{N}^*$ ne contenant pas de nombres premiers.

Exercice 18 Nombres de Mersenne
Soit un entier $n \geqslant 2$. Le n^{e} nombre de Mersenne, scientifique français du XVII$^{\text{e}}$ s. qui les a étudiés, est défini par $M_n = 2^n - 1$. Ces nombres sont utilisés dans la recherche de grands nombres premiers, le plus grand de tous connu à ce jour en étant d'ailleurs un.

1. Vérifier que M_2, M_3 et M_5 sont premiers.
2. On suppose ici que n n'est pas premier et que $n = kp$ avec $p \in \mathfrak{P}$ et $k \geqslant 2$. Factoriser M_n par $2^p - 1$.
3. En déduire que si M_n est premier, alors n est premier.
4. Montrer que la réciproque est fausse.

Exercice 19 Égalité de Sophie Germain
Sophie Germain (1776-1831) est une mathématicienne, physicienne et philosophe française. Elle est connue pour le théorème d'arithmétique qui porte son nom, pour ses échanges avec le mathématicien Carl Friedrich Gauss et pour ses travaux sur l'élasticité des corps. Pour pouvoir se consacrer aux mathématiques, alors réservées aux hommes, elle utilisa un nom d'emprunt de 1794 à 1807 : Antoine Auguste Le Blanc.

1. Montrer l'égalité $n^4 + 4m^4 = (n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn)$.
2. Pour quelles valeurs de l'entier naturel n, $n^4 + 4$ est-il premier ?
3. Montrer que $4^{545} + 545^4$ n'est pas premier.

Exercice 20 Décomposer les nombres suivants en produit de facteurs premiers.

$a = 125$	$c = 21^3 \times 170$	$e = 100000$
$b = 64 \times 81$	$d = 1080$	$f = 12^6 \times 14^5$

Exercice 21 a est-il un diviseur de b ?

1. $a = 5^3.7^2.11^7.13, \quad b = 5^5.7^2.11^9.13^7$
2. $a = 3^5.5^2.11^2.17, \quad b = 3^5.11^6.17^7$
3. $a = 13^5, \quad b = 2^7.7^3.13^5.19$

Exercice 22 Calculer, simplifier, réduire,...

$a = \text{PGCD}(24, 80)$	$c = \text{PGCD}(3757, 2873)$	$e = \frac{375}{1089}$
$b = \text{PGCD}(179, 181)$	$d = \sqrt{1764}$	$f = \frac{1960}{1120}$

Exercice 23 Combien y a-t-il de nombres entiers naturels inférieurs à 2000 dont l'écriture décimale se termine par deux zéros et ne comportant que 2 et 5 comme diviseurs premiers ?

Exercice 24 Déterminer dans $\mathbb{N}$ les solutions des équations $(n+1)(n+3) = 255$, $3u^2 + 6u - 24 = 255$ et $x^3 - y^3 = 469$.

Exercice 25 L'indicatrice d'Euler
Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre de nombres strictement positifs qui sont premiers avec n et inférieurs ou égaux à n : $\varphi(n) = \text{Card}(\{k \ / \ k \in [\![1 ; n]\!] \text{ et } k \wedge n = 1\})$.

1. Déterminer $\varphi(k)$ pour tout $k \in [\![1 ; 9]\!]$.
2. Calculer $\varphi(p)$ pour $p \in \mathfrak{P}$.
3. Calculer $\varphi(p^2)$ pour $p \in \mathfrak{P}$.

Exercice 26 Soit $n \in \mathbb{N}^*$ et k le nombre de diviseurs premiers de n.
Prouver que $\ln(n) \geqslant k \ln(2)$.

Exercice 27
Démontrer que pour tout $n \in \mathbb{N}$ et tout $p \in \mathfrak{P}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

Exercice 28 Montrer que 33 divise $n^{11} - n$ pour tout $n \in \mathbb{N}$.

Exercice 29 Soit $n \in \mathbb{N}^*$.

1. Montrer que $n^{13} - n$ est pair.
2. Montrer que 13 et 7 divisent $n^{13} - n$.
3. En déduire que $n^{13} - n$ est divisible par 182.

Exercice 30 Soient a, $b \in \mathbb{Z}$ et $p \in \mathfrak{P}$. Montrer que $(a+b)^p \equiv a^p + b^p \, [p]$.

Exercice 31 Soient $p \in \mathfrak{P}$ et a, $b \in \mathbb{N}$.

1. Montrer que $a^p - b^p \equiv (a-b)^p \, [p]$.
2. (a) Justifier que si p n'est pas premier avec $a^p - b^p$, alors $a^p \equiv b^p \, [p]$.
   (b) En déduire que dans ce cas, p divise $a - b$ et $a^p \equiv b^p \, [p^2]$

Exercice 32 Soit p un entier supérieur ou égal à 2.
Montrer que si $(p-1)! + 1$ est un multiple de p, alors p est un nombre premier.

Exercice 33 Un carré s'écrit aussi sous la forme $17n + 1$ où $n \in \mathbb{N}$.
Sous quelle forme s'écrit n ? Quelles sont les valeurs possibles pour $n \in \mathfrak{P}$?

Exercice 34 Les repunits
Les entiers qui ne s'écrivent qu'avec des chiffres 1, comme 1, 11, 111,... sont appelés des repunits.
Pour $k \in \mathbb{N}^*$, on note N_k le repunit à k chiffres.

1. Décomposer N_k en produit de facteurs premiers pour tout $k \in [\![2 ; 5]\!]$.
2. Soit n un entier supérieur ou égal à 2 tel que le chiffre des unités de n^2 est 1.
   (a) Montrer que $n \equiv 1 \, [10]$ ou $n \equiv 9 \, [10]$.
   (b) En déduire que $n^2 \equiv 1 \, [20]$.
3. (a) Soit k un entier supérieur ou égal à 2.
   Déterminer le reste de la division euclidienne de N_k par 20.
   (b) En déduire qu'un repunit distinct de 1 n'est pas un carré.

Exercice 35 Puissances croisées
On cherche les couples d'entiers naturels $(a\,,\,b)$ tels que $a > b \geqslant 2$ et $a^b = b^a$.

1. (a) Montrer que $2^n > n^2$ pour tout $n \geqslant 5$.
   (b) Étudier le cas $b = 2$.
2. On suppose désormais que $b \geqslant 3$.
   (a) Montrer que a et b ont les mêmes facteurs premiers dans leur décomposition.
   (b) Soit p un diviseur premier de ces décompositions présent avec l'exposant α dans a et avec β dans b. Montrer que $a\beta = b\alpha$.
   (c) En déduire qu'il existe un entier $c \geqslant 2$ tel que $a = bc$.
   (d) Montrer que $b^{c-1} = c$.
   (e) Conclure en montrant que cette dernière égalité est impossible.

Exercice 36 Nombres puissants
On dit qu'un entier naturel n est un nombre puissant si, pour tout diviseur premier p de n, p^2 est aussi un diviseur de n. Le but de l'exercice est de montrer qu'il existe un infinité de couples d'entiers naturels consécutifs puissants.

Soient l'équation d'inconnues dans $\mathbb{N}$ $\quad (E)\colon x^2 - 8y^2 = 1$, la matrice $A = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$
et deux suites $(x_n)_{\mathbb{N}}$, $(y_n)_{\mathbb{N}}$ définies par $\quad x_0 = 3$, $y_0 = 1$ et $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

1. Pour tout $n \in \mathbb{N}$, montrer que x_n et $y_n \in \mathbb{N}^*$ et que le couple (x_n, y_n) est une solution de (E).
2. Démontrer que la suite $(x_n)_{\mathbb{N}}$ est strictement croissante et en déduire que l'équation (E) admet une infinité de solutions.
3. Montrer que a^2b^3 est un nombre puissant pour tout a, $b \in \mathbb{N}$.
4. Montrer que si le couple (x, y) est solution de (E), alors $x^2 - 1$ et x^2 sont deux entiers consécutifs puissants.
5. Conclure.
6. $\int$ Écrire une fonction Python puissant(N) qui détermine un couple d'entiers consécutifs puissants supérieurs ou égaux à N.

Exercice 37 Déterminer le plus petit entier possédant 28 diviseurs.

Exercice 38

1. Soit n un entier supérieur ou égal à 1.
   Montrer qu'il y a au plus un nombre premier entre $n!$ et $n! + n$.
2. Montrer que l'on peut trouver deux nombres premiers consécutifs dont la différence est supérieure à 10^6.

Exercice 39 Par combien de zéros se termine le nombre $31!$?

Exercice 40 Déterminer le reste de la division euclidienne de n par p.

(a) $n = 3^{52}$, $p = 23$. | (b) $n = 4^{89}$, $p = 29$. | (c) $n = 15^{100}$, $p = 97$.

Exercice 41

1. On pose $\quad n = 3^{4\times 6}$.
   (a) Justifier que $\quad n \equiv 1\,[5] \quad$ et $\quad n \equiv 1\,[7] \quad$ puis en déduire que $\quad n \equiv 1\,[35]$.
   (b) Calculer $\quad 3^{75}$ modulo 35.
2. Montrer que $\quad 3^{72} \equiv 1\,[95] \quad$ puis calculer 3^{75} modulo 95.
3. Calculer 4^{207} modulo 55.

Exercice 42 Puissance de 4

1. Démontrer que, pour tout entier naturel n, $\quad 4^n \equiv 1\,[3]$.
2. Montrer que $4^{28} - 1$ est divisible par 29.
3. (a) Déterminer le reste de la division de 4^n par 17 pour $n \in [\![1\,;4]\!]$.

EXERCICES

(b) En déduire que $4^{4k} - 1$ est divisible par 17 pour tout entier k.

4. Pour quels entiers naturels n, $4^n - 1$ est-il divisible par 5 ?
5. Déterminer alors quatre diviseurs premiers de $4^{28} - 1$.

Exercice 43 Triplets pythagoriciens

Cet exercice a pour but d'étudier l'équation $(E)\colon x^2 + y^2 = p^2$ où p est premier et x, $y \in \mathbb{N}^*$. Vous voyez certainement pourquoi les solutions d'une telle équation sont appelées des triplets pythagoriciens.

1. Montrer que (E) n'admet pas de solution lorsque $p = 2$.
2. On suppose désormais que $p \neq 2$ et que le couple $(\,x\,,\,y\,)$ est solution de (E).
   (a) Montrer que x et y n'ont pas même parité.
   (b) Montrer que p ne divise ni x, ni y.
   (c) En déduire que x et y sont premiers entre eux.
3. On suppose désormais que p est la somme de deux carrés : $p = u^2 + v^2$ où u et $v \in \mathbb{N}^*$.
   (a) Montrer que le couple $\left(\left|u^2 - v^2\right|\,,\,2uv\right)$ est solution de (E).
   (b) Donner une solution de (E) pour $p = 5$ puis une solution pour $p = 13$.
4. On illustre maintenant le fait que (E) n'admet pas de solution lorsque p n'est pas somme de deux carrés.
   (a) $p = 3$ et $p = 7$ peuvent-ils s'écrire comme somme de deux carrés ?
   (b) Montrer que les équations $x^2 + y^2 = 9$ et $x^2 + y^2 = 49$ n'admettent pas de solutions.
   (c) Le théorème des deux carrés de Fermat affirme qu'un nombre premier est somme de deux carrés, et ce de façon unique, si, et seulement si, il est congru à 1 modulo 4.
   Vérifier ce résultat sur les exemples précédents.

Comptez jusqu'à 321 afin de réaliser le devoir n° 14.

Corrigé des exercices

NOMBRES PREMIERS

Exercice 1 Si $n = 2$, alors $n^2 - 1 = 3$ est premier. Si $n > 2$, alors $n - 1 > 1$ et $n^2 - 1 = (n-1)(n+1)$ admet un diviseur propre (non trivial) qui est $n-1$ donc $n^2 - 1$ n'est pas premier.

Exercice 2 Avec la méthode empirique du crible d'Érathosthène, nous obtenons la liste des nombres premiers inférieurs à 100.

Exercice 3 Un bon début
On a $P_0 = 17$, $P_1 = 19$, $P_2 = 23$, $P_3 = 29$, $P_4 = 37$, $P_5 = 47$, $P_6 = 59$, $P_7 = 73$, $P_8 = 89$, $P_9 = 107$, $P_{10} = 127$, $P_{11} = 149$, $P_{12} = 173$, $P_{13} = 199$, $P_{14} = 227$, $P_{15} = 257$, tous premiers. En revanche, $P_{16} = 289 = 17^2$ ne l'est pas.

Exercice 4 • $1+1+7 = 9$ donc $9 \mid 117$ et $117 \notin \mathfrak{P}$.
- 383 n'est pas divisible par 2, 3, 5, 7, 11, 13, 17 ou 19 et $\sqrt{383} \leqslant 20$ donc $383 \in \mathfrak{P}$.
- $1 + 3 = 4$ donc $11 \mid 143$ et $143 \notin \mathfrak{P}$.
- 337 n'est pas divisible par 2, 3, 5, 7, 11, 13 ou 17 et $\sqrt{337} < 19$ donc $337 \in \mathfrak{P}$.

Exercice 5 Nombres premiers jumeaux

1. $(5\,,7)$, $(11\,,13)$, $(17\,,19)$, $(29\,,31)$ et $(41\,,43)$ sont des couples de premiers jumeaux.
2. Il suffit de vérifier que 1619 et 1621 ne sont pas divisibles par des nombres premiers inférieurs ou égaux à leur racine carrée (c.-à-d. 40) et la liste est relativement brève.

Exercice 6 Soit $p \in \mathfrak{P}$ et $n \in \mathbb{N}$.
On a $7p + 1 = n^2 \iff 7p = n^2 - 1 = (n+1)(n-1)$ donc p divise $n+1$ ou $n-1$.
• Si $n+1 = kp$, alors $7p = kp(n-1) \iff 7 = k(n-1)$ et puisque $7 \in \mathfrak{P}$, on a $k = 7, n-1 = 1$ ou $k = 1, n-1 = 1$.
Si $k = 7$ et $n - 1 = 1$, alors $n = 2$ et $n + 1 = 3 = 7p$ ce qui est impossible.
Si $k = 1$ et $n - 1 = 7$, alors $n = 8$ et $n + 1 = 9 = 1p$ qui ne serait pas premier.
• Si $n-1 = kp$, alors $7p = kp(n+1) \iff 7 = k(n+1)$ et puisque $7 \in \mathfrak{P}$, on a $k = 7, n+1 = 1$ ou $k = 1, n+1 = 7$.
Si $k = 7$ et $n + 1 = 1$, alors $n = 0$ et $n - 1 = -1 = 7p$ ce qui est impossible.
Si $k = 1$ et $n + 1 = 7$, alors $n = 6$ et $n - 1 = 5 = 1p \in \mathfrak{P}$.
En effet, $7p + 1 = 7 \times 5 + 1 = 36 = 6^2$ marche.

Exercice 7 • On a $a = n^2 - 2n - 3 = (n+1)(n-3)$ qui ne peut être premier que si $n - 3 = 1$ (puisque $n + 1 > n - 3 \geqslant 0$) et l'on a bien, pour $n = 4$, $a = 5 \in \mathfrak{P}$.
• On a $b = n^2 + 2n + 1 = (n+1)^2$ qui ne peut être premier que si $n + 1 = 1$ mais pour $n = 0$, $b = 1 \notin \mathfrak{P}$.

Exercice 8 Dressons un tableau de congruence modulo 6.

$n\,[6]$	0	1	2	3	4	5
$n^2\,[6]$	0	1	4	3	4	3
$2n\,[6]$	0	2	4	0	2	4
$n^2-2n+3\,[6]$	3	2	3	0	5	2

Si $n \geqslant 3$, $n^2-2n+3 \geqslant 6$ et d'après le tableau précédent, pour $n \equiv 0\,[6]$ ou $2\,[6]$ ou $3\,[6]$, n^2-2n+3 est un multiple de 3 (différent de 3) et pour $n \equiv 1\,[6]$ ou $5\,[6]$, n^2-2n+3 est un multiple de 2 (différent de 2).
Ainsi, n^2-2n+3 ne peut être premier que si $n \equiv 4\,[6]$.
Par exemple, pour $n=4$, $4^2-2\times 4+3 = 11 \in \mathfrak{P}$
et pour $n=10$, $10^2-2\times 10+3 = 83 \in \mathfrak{P}$.
En revanche, pour $n=28$, $28^2-2\times 28+3 = 731 = 17\times 43 \notin \mathfrak{P}$: la réciproque est donc fausse.

Exercice 9 Soient $a,\, b \in \mathbb{N}^*$ tels que $a+b \in \mathfrak{P}$ et soit $d = \mathrm{PGCD}\,(a\,,\,b)$. On a $d|a$ et $d|b$ donc $d|a+b$. Puisque $a+b$ est premier, $d \in \{1; a+b\}$. Or, $d \leqslant a < a+b$. D'où, $\mathrm{PGCD}\,(a\,,\,b) = d = 1$.

Exercice 10 Si $\mathrm{PGCD}\,(p\,,\,3) = 3$, alors $3|p$. Puisque p est premier, on a $p = 3 \in \mathfrak{P}$, unique possibilité.

Exercice 11

1. Si $p \in \mathfrak{P}$ et $p > 3$, alors p n'est pas un multiple de 3 c.-à-d.
   $p \not\equiv 0\,[3] \iff p \equiv 1\,[3]$ ou $p \equiv 2\,[3] \iff p \equiv \pm 1\,[3]$:
   p s'écrit donc sous la forme $3k \pm 1$ avec $k \in \mathbb{N}^*$ car $p > 3$.
2. Tout nombre premier supérieur ou égal à 3 est impair et ne peut être congru à 0 ou à 2 modulo 4. Il est donc congru à 1 ou à 3, c.-à-d. -1, modulo 4.
3. Les réciproques sont fausses, cela serait trop facile autrement.
   Par exemple, $4 = 3\times 1+1$ et $9 = 1+4\times 2$ ne sont pas premiers.

Exercice 12 $n \in \mathbb{N}$ tel que $n+1$, $n+3$, $n+7$, $n+9$, $n+13$ et $n+15$ soient premiers.

1. Trivialement, pour $n=0$, $n+1 \notin \mathfrak{P}$, pour $n=1$, $n+3 \notin \mathfrak{P}$, pour $n=2$, $n+7 \notin \mathfrak{P}$, pour $n=3$, $n+1 \notin \mathfrak{P}$, pour $n=5$, $n+1 \notin \mathfrak{P}$ mais pour $n=4$, $n+1$, $n+3$, $n+7$, $n+9$, $n+13$ et $n+15$ sont premiers.
2. Dressons un tableau de congruence modulo 5.

$n\,[5]$	0	1	2	3	4
$n+1\,[5]$	1	2	3	4	0
$n+3\,[5]$	3	4	0	1	2
$n+7\,[5]$	2	3	4	0	1
$n+9\,[5]$	4	0	1	2	3
$n+13\,[5]$	3	4	0	1	2
$n+15\,[5]$	0	1	2	3	4

D'après ce tableau, il y a nécessairement un multiple de 5 parmi les six nombres imposés et puisque 5 ne convient pas, aucun entier $n \geqslant 5$ ne peut convenir. Le seul entier possible est donc $n = 4$.

Exercice 13 Les nombres de Fermat : $F_n = 2^{2^n} + 1$.

1. $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$ et $F_4 = 2^{2^4} + 1 = 65537$ sont premiers.
2. $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417 + 0$
donc $\text{PGCD}\,(F_5\,,\,641\,) = 641$ et $F_5 \notin \mathfrak{P}$.
Les nombres de Fermat ne sont donc pas tous premiers. C'était bien la seule conjecture fausse de cet immense mathématicien.

Exercice 14

1. Soit p un nombre premier strictement supérieur à 3. Il est donc impair et non multiple de 3 et ne peut ainsi être congru à 0, 2, 4 modulo 6 ni à 3 modulo 6. p est donc congru à 1 ou 5, c.-à-d. -1, modulo 6.
2. Soit p un nombre premier strictement supérieur à 3. On a donc $p \equiv \pm 1\,[6]$ et il existe $k \in \mathbb{N}^*$ tel que $p = 6k \pm 1$ donc
$p^2 + 17 = (6k \pm 1)^2 + 17 = 36k^2 \pm 12k + 1 + 17 = 12(3k^2 \pm k + 1) + 6 \equiv 6\,[12]$.

Exercice 15 Fermat : « Un premier impair est différence de deux carrés parfaits. »

1. On a bien $3 = 2^2 - 1^2$, $5 = 3^2 - 2^2$, $7 = 4^2 - 3^2$, $11 = 6^2 - 5^2$, $13 = 7^2 - 6^2$, $17 = 9^2 - 8^2$, $19 = 10^2 - 9^2$, $23 = 12^2 - 11^2$, $29 = 15^2 - 14^2$, $31 = 16^2 - 15^2$, $37 = 19^2 - 18^2$,...
2. Démontrons donc cette propriété.
   (a) On a $p = a^2 - b^2 = (a+b)(a-b)$ et si p est premier, il n'admet que des diviseurs triviaux et l'on a $a - b = 1$ et $a + b = p$ d'où $b = a - 1$ et $2a - 1 = p$. Ainsi, $a = \frac{p+1}{2}$ et $b = \frac{p-1}{2}$, ce qui implique que p est impair.
   (b) Soit p un nombre premier différent de 2. Posons $a = \frac{p+1}{2}$ et $b = \frac{p-1}{2}$.
   On a $a, b \in \mathbb{N}^*$ et $a^2 - b^2 = (a+b)(a-b) = \frac{p+1+p-1}{2}\,\frac{p+1-(p-1)}{2} = p \times 1 = p$.
   Ainsi, tout nombre premier différent de 2 est différence de deux carrés parfaits.

Exercice 16 Soient p et q deux nombres premiers consécutifs impairs.

1. On a $p \neq q$ donc $p < \frac{p+q}{2} < q$ et puisque p et q sont des premiers consécutifs, $n = \frac{p+q}{2}$ ne peut être premier.
2. Puisque n n'est pas premier, il admet au moins deux diviseurs premiers, éventuellement confondus et donc $p + q = 2n$ en admet au moins trois, éventuellement confondus. Par exemple, $3 + 5 = 2.2.2$, $5 + 7 = 2.2.3$ et $7 + 11 = 2.3.3$.

Exercice 17 Trivialement, $17 | 29!$ et $17 | 17$ donc $17 | 29! + 17$ et $29! + 17 \notin \mathfrak{P}$.
De même, $38 | 45!$ donc $45! + 38 \notin \mathfrak{P}$.
Soit $n \in \mathbb{N}^*$. On a $2 | (n+1)! + 2$, $3 | (n+1)! + 3$, $\ldots$, $(n+1) | (n+1)! + (n+1)$ donc l'intervalle $[\![\,(n+1)! + 2\,;(n+1)! + (n+1)\,]\!]$, d'amplitude $n + 1 - 1 = n$, ne contient aucun nombre premier.

Exercice 18 Nombres de Mersenne : $M_n = 2^n - 1$

1. On a $M_2 = 2^2 - 1 = 3 \in \mathfrak{P}$, $M_3 = 2^3 - 1 = 7 \in \mathfrak{P}$ et $M_5 = 2^5 - 1 = 31 \in \mathfrak{P}$.

CORRIGÉS

2. Si $n = kp$ pour $k \geqslant 2$, on a $\quad M_n = 2^n - 1 = (2^p)^k - 1^k$
$$M_n = (2^p - 1).\sum_{i=0}^{k-1}(2^p)^i.1^{k-1-i} = (2^p-1)(1 + 2^p + 2^{2p} + \ldots + 2^{(k-1)p}).$$
3. Si n n'est pas premier, alors $n = kp$ pour $k \geqslant 2$ et $\quad 1+2^p+2^{2p}+\ldots+2^{(k-1)p} > 1$ donc M_n admet un diviseur propre (différent de 1 et de lui-même) : $M_n \notin \mathfrak{P}$.
Par contraposition, si $M_n \in \mathfrak{P}$, alors $n \in \mathfrak{P}$.
4. Pour $n = 11 \in \mathfrak{P}$, on a $\quad M_{11} = 2^{11} - 1 = 2047 = 23 \times 89 \notin \mathfrak{P}$: la réciproque est fausse.

Exercice 19 Égalité de Sophie Germain

1. On a $\quad (n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn)$
$$= n^4 + 2n^2m^2 - 2mn^3 + 2m^2n^2 + 4m^4 - 4m^3n + 2mn^3 + 4m^3n - 4m^2n^2$$
$$= n^4 + 4m^4.$$
2. Pour $m = 1$, $\quad n^4 + 4 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$ ne peut être premier que lorsque $n^2 + 2 - 2n = 1$ (l'autre facteur lui étant supérieur ou égal), c.-à-d.
$$n^2 - 2n + 1 = 0 \iff (n-1)^2 = 0 \iff n = 1.$$
Pour $n = 1$, on a bien $n^4 + 4 = 5 \in \mathfrak{P}$.
3. On a $\quad 545 = 1 + 136 \times 4$ et pour $n = 545$ et $m = 4^{136}$, on a
$$4^{545} + 545^4 = 545^4 + 4 \times (4^{136})^4$$
$$= (545^2 + 2(4^{136})^2 + 2.4^{136}.545)(545^2 + 2(4^{136})^2 - 2.4^{136}.545) \notin \mathfrak{P}.$$

Exercice 20

$a = 125 = 5^3$

$b = 64 \times 81 = 2^6.3^4$

$c = 21^3 \times 170 = 2.3^3.5.7^3.17$

$d = 1080 = 2^3.3^3.5$

$e = 100000 = 10^5 = 2^5.5^5$

$f = 12^6.14^5 = (2^2)^6.3^6.2^5.7^5 = 2^{17}.3^6.7^5$

Exercice 21 a est-il un diviseur de b ?

1. $b = 5^5.7^2.11^9.13^7 = 5^2.11^2.13^6 \times 5^3.7^2.11^7.13 = ka$: $\quad a \mid b$.
2. $b = 3^5.11^6.17^7 = 5^{-2}.11^4.17^6 \times 3^5.5^2.11^2.17 = 5^{-2}.11^4.17^6 a$: $\quad a \nmid b$.
3. $b = 2^7.7^3.13^5.19 = 2^7.7^3.19 \times 13^5 = 2^7.7^3.19 \times a$: $\quad a \mid b$.

Exercice 22

$a =$ PGCD (24 , 80) : $\quad 24 = 2^3.3$ et $80 = 2^4.5$ donc $a = 24 \wedge 80 = 2^3$.

$b =$ PGCD (179 , 181) : $\quad 179 \in \mathfrak{P}$ et $179 \nmid 181$ donc $b = 179 \wedge 181 = 1$.
Sinon, $d \mid 179$ et $d \mid 181$ donc $d \mid 181 - 179 = 2$. Puisque $2 \nmid 179$, on a $d = 1$.

$c =$ PGCD (3757 , 2873) : $\quad 3757 = 13.17^2$, $\quad 2873 = 13^2.17$
donc $c = 3757 \wedge 2873 = 13.17 = 221$.

$d = \sqrt{1764} = \sqrt{2^2.3^2.7^2} = 2.3.7 = 42$.

$e = \frac{375}{1089} = \frac{3.5^3}{3^2.11^2} = \frac{5^3}{3.11^2} = \frac{125}{363}$ irréductible.

$f = \frac{1960}{1120} = \frac{14^2 \times 10}{10 \times 28 \times 4} = \frac{2^3.5.7^2}{2^5.5.7} = \frac{7}{2^2} = \frac{7}{4}$ irréductible.

Exercice 23 Soit n un entier naturel inférieur à 2000 dont l'écriture décimale se termine par deux zéros et ne comportant que 2 et 5 comme diviseurs premiers. On a donc $n = 2^p.5^q$. Puisque $100 = 2^2.5^2 \,|\, n$, on a $p \geqslant 2$ et $q \geqslant 2$. Puisque $1000 \not| n$, on a $p < 3$ ou $q < 3$. En éliminant les nombres supérieurs à 2000, il reste $2^2.5^2 = 100$, $2^2.5^3 = 500$, $2^3.5^2 = 200$, $2^4.5^2 = 400$, $2^5.5^2 = 800$ et $2^6.5^2 = 1600$: il y a donc 6 entiers possibles.

Exercice 24 • On a $255 = 3.5.17$ et $n+1 < (n+1)+2 = n+3$ donc $(n+1)(n+3) = 255$ admet pour seule solution $n+1 = 15$ et $n+3 = 17$, c.-à-d. $n = 14$.

• $3u^2 + 6u - 24 = 255 \iff 3(u-2)(u+4) = 3.5.17$
$\iff (u-2)(u+4) = 5 \times 17$
$\iff$ $(u-2 = 5$ et $u+4 = 17)$ ou $(u-2 = 1$ et $u+4 = 5 \times 17)$ par unicité de la décomposition. Cette équation n'admet donc aucune solution.

• En utilisant la factorisation classique (cf. prop.1 p.47),
$x^3 - y^3 = 469 \iff (x-y)(x^2+xy+y^2) = 7 \times 67$
$\iff$ $(x-y = 1$ et $x^2+xy+y^2 = 7 \times 67)$ ou $(x-y = 7$ et $x^2+xy+y^2 = 67)$ car $x - y < x^2+xy+y^2$.
Le premier cas donne $x = 1+y$ et $(1+y)^2 + (1+y)y + y^2 = 7 \times 67$
$\iff 3y^2+y-468 = 0 \iff y^2+y-156 = 0 \iff y = \frac{-1\pm\sqrt{625}}{2} \iff y = 12 \in \mathbb{N}$
et $x = 1+y = 13$. On a bien $13^3 - 12^3 = 469$.
Le second cas donne $x = 7+y$ et $(7+y)^2 + (7+y)y + y^2 = 67$
$\iff 3y^2 + 21y - 18 = 0 \iff y^2 + 7y - 6 = 0 \iff y = \frac{-1\pm\sqrt{85}}{2} \notin \mathbb{N}$.
Le seul couple solution est donc $(13\,,\,12)$.

Exercice 25 L'indicatrice d'Euler :
$\varphi(n) = Card\{k \in \mathbb{N}^*/k \leqslant n \text{ et } \mathrm{PGCD}\,(k\,,\,n) = 1\}$

1. On a $\varphi(1) = Card\{1\} = 1$, $\varphi(2) = Card\{1\} = 1$, $\varphi(3) = Card\{1;2\} = 2$, $\varphi(4) = Card\{1;3\} = 2$, $\varphi(5) = Card\{1;2;3;4\} = 4$, $\varphi(6) = Card\{1;5\} = 2$, $\varphi(7) = Card\{1;2;3;4;5;6\} = 6$, $\varphi(8) = Card\{1;3;5;7\} = 4$ et $\varphi(9) = Card\{1;2;4;5;7;8\} = 6$.
2. Puisque $p \in \mathfrak{P}$ est premier avec tout entier sauf ses multiples,
$\varphi(p) = Card\{1;2;\,\dots;p-1\} = p-1$.
3. Puisqu'il existe $p-1$ multiples de p dans $[\![\,1\,;p^2-1\,]\!]$, ceux de la forme kp pour $k \in [\![\,1\,;p-1\,]\!]$, on a $\varphi(p^2) = (p^2-1) - (p-1) = p(p-1)$.
On peut aussi compter p intervalles d'entiers premiers avec p du type $[\![\,k \times 1\,;k \times (p-1)\,]\!]$ pour $k \in [\![\,1\,;p\,]\!]$.

Exercice 26 Si k est le nombre de diviseurs premiers de $n \in \mathbb{N}^*$, alors la décomposition *p.o.c.* en facteurs premiers de n s'écrit $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ où $p_i \in \mathfrak{P}$ et $\alpha_i \in \mathbb{N}^*$.
Ainsi, $p_i \geqslant 2$ et $\alpha_i \geqslant 1$. D'où,

$$\ln(n) = \ln(p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}) = \sum_{i=1}^{k}\ln(p_i^{\alpha_i}) = \sum_{i=1}^{k}\alpha_i\ln(p_i) \geqslant \sum_{i=1}^{k}1.\ln(2) = k\ln(2).$$

Exercice 27 Soient $n \in \mathbb{N}$ et $p \in \mathfrak{P}$. On a $3^p \equiv 3\,[p]$ donc $3^p - 3 \equiv 0\,[p]$ et $3^n(3^p-3) = 3^{n+p} - 3^{n+1} \equiv 3^n \times 0\,[p] \equiv 0\,[p]$: $3^{n+p} - 3^{n+1}$ est divisible par p.

Exercice 28 Soit $n \in \mathbb{N}$. Puisque 3 et 11 sont premiers, le petit théorème de Fermat permet d'affirmer que $n^3 \equiv n\,[3]$ et $n^{11} \equiv n\,[11]$ d'où $n^{11} - n \equiv 0\,[11]$ et $11 \big| n^{11} - n$. De plus, $n^{11} = n^2(n^3)^3 \equiv n^2(n)^3\,[3] \equiv n^2.n\,[3] \equiv n\,[3]$ donc $n^{11} - n \equiv 0\,[3]$ et $3 \big| n^{11} - n$. Ainsi, 3 et 11 étant premiers entre eux, $3 \times 11 = 33$ divise $n^{11} - n$.

Exercice 29 Soit $n \in \mathbb{N}^*$.

1. Puisque n^{13} et n ont même parité, leur différence est nécessairement paire.
2. Puisque 7 et 13 sont premiers, le petit théorème de Fermat donne $n^{13} - n \equiv 0\,[13]$ et $n^7 \equiv n\,[7]$ donc $n^{13} = n^6.n^7 \equiv n^6.n\,[7] = n\,[7]$. Ainsi, 7 divise $n^{13} - n$.
3. Puisque 2, 7 et 13 divisent $n^{13} - n$ et sont premiers entre eux, leur produit 182 divise aussi $n^{13} - n$.

Exercice 30 Soient a, $b \in \mathbb{Z}$ et $p \in \mathfrak{P}$. Puisque $p \,|\, \binom{p}{k}$ pour tout $k \in [\![\, 1\,; p-1 \,]\!]$,

$$(a+b)^p = \sum_{k=0}^{p} \binom{k}{p} a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} \binom{k}{p} a^{p-k} b^k + b^p = a^p + pS + b^p \equiv a^p + b^p\,[p].$$

Exercice 31 Soient $p \in \mathfrak{P}$ et a, $b \in \mathbb{N}$.

1. Pour $p = 2$, on a $(a-b)^2 - (a^2 - b^2) = 2(b^2 - ab) \equiv 0\,[2]$.
   Pour $p \geqslant 3$, on a p impair donc $(-1)^p = -1$ et
   $$\begin{aligned}(a-b)^p = \sum_{k=0}^{p} \binom{k}{p} (-1)^k a^{p-k} b^k (a-b)^p &= a^p + \sum_{k=1}^{p-1} \binom{k}{p} (-1)^k a^{p-k} b^k + (-1)^p b^p \\ &= a^p + pS - b^p \equiv a^p - b^p\,[p] \quad \text{car } p \,|\, \tbinom{p}{k} \text{ pour } k \in [\![\, 1\,; p-1 \,]\!].\end{aligned}$$
2. (a) Si p n'est pas premier avec $a^p - b^p$, alors $\mathrm{PGCD}\,(\,p\,,\, a^p - b^p\,) > 1$ donc $\mathrm{PGCD}\,(\,p\,,\, a^p - b^p\,) = p$, seul autre diviseur de p, et p divise $a^p - b^p$:
   $a^p - b^p \equiv 0\,[p]$.

   (b) Le petit théorème de Fermat donne $a^p \equiv a\,[p]$ et $b^p \equiv b\,[p]$ donc $a - b \equiv a^p - b^p\,[p] \equiv 0\,[p]$ d'après la question précédente et p divise $a - b$.
   On a $a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \,\ldots\, + ab^{p-2} + b^{p-1})$.
   Or, $a \equiv b\,[p]$ donc $a^k \equiv b^k\,[p]$ et
   $a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv b^{p-1} + b^{p-1} + \ldots + b^{p-1}\,[p] \equiv pb^{p-1} \equiv 0\,[p]$.
   Ainsi, p divise le deuxième facteur. Puisque p divise aussi le premier, ce produit est divisible par p^2.

Exercice 32 Soit p un entier supérieur ou égal à 2 tel que $(p-1)!+1$ est un multiple de p. Il existe donc un entier k tel que $(p-1)!+1 = kp \iff kp-(p-1)! = 1$ et, d'après le théorème de Bézout, p et $(p-1)!$ sont premiers entre eux : $\mathrm{PGCD}\,(\,(p-1)!\,,\, p\,) = 1$. Par construction de $(p-1)!$, p n'est donc divisible par aucun entier de $[\![\, 2\,; p-1 \,]\!]$ c.-à-d. $p \in \mathfrak{P}$.

Exercice 33 Soient m, $n \in \mathbb{N}$ tels que $m^2 = 17n + 1$.
On a alors $17n = m^2 - 1 = (m-1)(m+1)$ et d'après le théorème de Gauss, 17 divise $m-1$ ou $m+1$ car $17 \in \mathfrak{P}$. Si $m-1 = 17k$, alors $m+1 = 17k+2$ et $17n = 17k(17k+2)$ donne la forme $n = k(17k+2)$ où $k \in \mathbb{N}$, l'écriture étant similaire pour $17\,|\,(m+1)$. Un tel n ne peut être premier que pour $k = 0$: $n = 0$, $m = 1$ et pour $k = 1$: $n = 19$ et $m = 17(17+2)+1 = 18^2$.

Exercice 34 Les repunits

1. On a $N_2 = 11 \in \mathfrak{P}$, $N_3 = 111 = 3 \times 37$, $N_4 = 1111 = 7 \times 101$ et $N_5 = 11111 = 41 \times 271$.
2. Soit n un entier supérieur ou égal à 2 tel que le chiffre des unités de n^2 est 1.
   (a) Un tableau de congruence modulo 10 montre rapidement que $n^1 \equiv 1\,[10]$ $\iff n \equiv 1\,[10]$ ou $n \equiv 9\,[10]$. En effet, 2^2, 3^2,... 8^2 ne se terminent pas par 1.
   (b) Puisque $9 \equiv -1\,[10]$, $n = 10p \pm 1$ et
   $$n^2 = (10p \pm 1)^2 = 100p^2 \pm 20p + 1 = 20(5p^2 \pm p) + 1 \equiv 1\,[20].$$
3. (a) Soit $k \geqslant 2$. On a $N_k = 11...1 = 11...100 + 11 \equiv 11\,[20]$.
   (b) Ainsi, N_k est un entier dont le chiffre des unités est 1 et tel que $N_k \equiv 11\,[20] \not\equiv 1\,[20]$ pour $k \geqslant 2$ donc N_k ne peut être un carré.

Exercice 35 Puissances croisées : $a > b \geqslant 2$ et $a^b = b^a$.

1. (a) On a $2^5 = 32 > 5^2 = 25$ et supposons par récurrence que $2^n > n^2$. On a alors
   $$2^{n+1} - (n+1)^2 = 2.2^n - (n+1)^2 > 2n^2 - (n+1)^2 = n^2 - 2n - 1 > 0$$
   pour tout $n \geqslant 5$ ($x_{1,2} = 1 \pm \frac{\sqrt{5}}{2} < 5$).
   (b) Pour $b = 2$, on ne peut avoir $a^2 = 2^a$ que pour $2 < a < 5$. Pour $a = 3$, $3^2 \neq 2^3$ mais pour $a = 4$, on a bien $2^4 = 4^2$. Le couple $(4, 2)$ est donc la seule solution de cette équation pour $b = 2$.
2. (a) Soit $b \geqslant 3$ et soient les décompositions en facteurs premiers *p.o.c.* $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{\ell} q_i^{\beta_i}$. On a $a^b = b^a \iff \prod_{i=1}^{k} p_i^{b\alpha_i} = \prod_{i=1}^{\ell} q_i^{a\beta_i}$ et l'unicité de la décomposition *p.o.c.* permet d'affirmer que $k = \ell$ et $p_i = q_i$ pour tout $i \in [\![1\,;k]\!]$.
   (b) De plus, on a nécessairement les mêmes exposants : $b\alpha_i = a\beta_i$ pour tout $i \in [\![1\,;k]\!]$.
   (c) Ainsi, pour tout $i \in [\![1\,;k]\!]$, $\frac{\alpha_i}{\beta_i} = \frac{a}{b} > 1$ donc $\alpha_i > \beta_i$ d'où $\frac{a}{b} = \prod_{i=1}^{k} p_i^{\alpha_i - \beta_i} = c \in \mathbb{N}$ c.-à-d. $a = bc$. De plus, $a > b$ implique $c \geqslant 2$.
   (d) Alors, $a^b = b^a \iff (bc)^b = b^{bc} \iff b^b c^b = (b^b)^c$
   $\iff c^b = (b^b)^{c-1} = (b^{c-1})^b \iff c = b^{c-1}$.
   (e) Or, par une récurrence facile, $b^{n-1} > n$ pour tous $b \geqslant 3$ et $n \geqslant 2$. En effet, $b^{2-1} = b > 2$ et si $b^{n-1} > n$, alors $b^n = b.b^{n-1} > 3n \geqslant n+1$.
   Ainsi, on ne peut avoir $b^{c-1} = c$ pour $c \geqslant 2$ donc il n'existe pas de couple (a, b) tels que $3 \leqslant b < a$ et $a^b = b^a$. La seule solution d'une telle équation est donc $2^4 = 4^2$.

On aurait aussi pu résoudre cette équation en étudiant la fonction $f(x) = \frac{\ln(x)}{x}$. En effet, $a^b = b^a \iff e^{a\ln(b)} = e^{b\ln(a)} \iff \frac{\ln(a)}{a} = \frac{\ln(b)}{b}$. f admet un maximum en $x = e$ et son tableau de variations complet permet de montrer que seul $(4, 2)$ est solution dans $\mathbb{N}^*$.

CORRIGÉS

Exercice 36 Nombres puissants

Un entier naturel n est un nombre puissant si, pour tout diviseur premier p de n, p^2 est aussi un diviseur de n.

1. On a $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 3x_n + 8y_n \\ x_n + 3y_n \end{pmatrix}$ donc $x_{n+1} = 3x_n + 8y_n$ et $y_{n+1} = x_n + 3y_n$. Une récurrence triviale prouve que x_{n+1} et y_{n+1} sont dans $\mathbb{N}^*$ car x_0 et y_0 le sont.
   Par ailleurs, $x_0^2 - 8y_0^2 = 9 - 8 = 1$: $(\,x_0\,,\,y_0\,)$ est solution de (E) et supposons, par récurrence, que $(\,x_n\,,\,y_n\,)$ est solution de (E). On a
   $$\begin{aligned} x_{n+1}^2 - 8y_{n+1}^2 &= (3x_n + 8y_n)^2 - 8(x_n + 3y_n)^2 \\ &= 9x_n^2 + 48x_ny_n + 64y_n^2 - 8x_n^2 - 48x_ny_n - 72y_n^2 = x_n^2 - 8y_n^2 = 1 : \end{aligned}$$
   $(\,x_{n+1}\,,\,y_{n+1}\,)$ est aussi solution de (E).
2. On a $x_{n+1} = 3x_n + 8y_n = x_n + (2x_n + 3y_n) > x_n$ car x_n et $y_n > 0$ donc $(x_n)_{\mathbb{N}}$ est strictement croissante. Puisque $x_n \in \mathbb{N}$, cette suite prend une infinité de valeurs entières correspondant à une infinité de solutions différentes de (E).
3. Soient a, $b \in \mathbb{N}$ et soit p un diviseur premier de a^2b^3. D'après la propriété 1 en page 220, on sait que p divise alors l'un des facteurs a ou b et donc p^2 divise a^2 ou b^2 : $p^2 \big| a^2b^3$.
4. Soit $(\,x\,,\,y\,)$ solution de (E). x^2 est trivialement puissant, comme tout carré, car les exposants de sa décomposition en nombres premiers sont tous pairs. Par ailleurs, $x^2 - 1 = 8y^2$: y^2 est puissant en tant que carré et le seul premier divisant 8 est 2 et son carré le divise aussi. Tout premier divisant un produit devant diviser l'un des facteurs, $8y^2$ est puissant. Ainsi, $x^2 - 1$ et x^2 sont deux entiers consécutifs puissants.
5. Puisqu'il existe un infinité de solutions à (E) et qu'à chaque solution correspond un couple d'entiers consécutifs puissants, il existe une infinité d'entiers consécutifs puissants.
6. Voici une fonction Python qui détermine un couple d'entiers consécutifs puissants supérieurs ou égaux à N puis sa variante avec l'utilisation d'une liste.

```
def puissant(N) :
    x=3
    y=1
    while x**2<N+1 :
        z=x
        x=3*z+8*y
        y=z+3*y
    return (x**2-1,x**2)

def puissantliste(N) :
    X=[3,1]
```

```
    while X[0]**2<N+1 :
        X=[3*X[0]+8*X[1],X[0]+3*X[1]]
    return [X[0]**2-1,X[0]**2]
```

Exercice 37 Soit $n \in \mathbb{N}$ ayant 28 diviseurs et soit une décomposition en facteurs premiers $n = \prod_{1}^{k} p_i^{\alpha_i}$. On sait que le nombre de diviseurs de n est alors $\prod_{1}^{k}(\alpha_i+1)$.
Puisque $28 = 2 \times 2 \times 7 = 2 \times 14 = 4 \times 7$ uniquement et $\alpha_i + 1 \geqslant 2$, on a nécessairement $k = 3$ et $(\alpha_1; \alpha_2; \alpha_3) = (1; 1; 6)$

ou $k = 2$ et $(\alpha_1 , \alpha_2) \in \{(1 , 13) ; (3 , 6)\}$ ou $k = 1$ et $\alpha_1 = 27$.
Les plus petits entiers possibles sont alors parmi $2^6.3.5$, $2^{13}.3$, $2^6.3^3$, 2^{27}.
Le plus petit entier ayant 28 diviseurs est donc $2^6.3.5 = 960$.

Exercice 38

1. Soit $n \in \mathbb{N}^*$ et $p \in \mathfrak{P} \cap [\, n! \,; n! + n\,]$. Il existe donc $k \in [\![\, 0 \,; n \,]\!]$ tel que $p = n! + k = k(\frac{n!}{k} + 1)$ où $\frac{n!}{k} + 1 \in \mathbb{N} \setminus \{0; 1\}$. Puisque p est premier, il n'admet que des diviseurs triviaux et l'on a nécessairement $\frac{n!}{k} + 1 = p$ et $k = 1$: le seul nombre premier éventuel de l'intervalle $[\, n! \,; n! + n\,]$ ne peut être que $p = n!+1$.
2. On désigne par m le plus grand nombre premier tel que $m \leqslant (10^7)! - 1$ et par M le plus petit nombre premier tel que $(10^7)! + 10^7 + 1 \leqslant M$. Les nombres premiers étant en nombre infini et commençant à 2, l'existence de m et M est garantie. D'après la question précédente avec $n = 10^7$, il existe au plus un nombre premier dans l'intervalle $I = [\![\,(10^7)! \,; (10^7)! + 10^7\,]\!]$. S'il n'existe pas de nombre premier dans I, alors m et M sont deux nombres premiers consécutifs de différence $M - n \geqslant 10^7 + 2 > 10^6$. S'il existe un nombre premier $p \in I$, alors m, p et M sont trois premiers consécutifs. De plus, l'une des différences entre p et les extrémités de I est supérieure ou égale à la moitié de l'amplitude de I. On a donc $p - m \geqslant \frac{10^7}{2} > 10^6$ ou $M - p \geqslant \frac{10^7}{2} > 10^6$.

Exercice 39 On a $31! = 2\times4\times5\times10\times15\times20\times25\times30\times K = 2^7\times5^7\times K' = K'\times10^7$ où la décomposition de K' ne comporte pas de 5. Le nombre $31!$ se termine donc par sept 0.

Exercice 40

(a) 23 est un nombre premier ne divisant pas 3 donc, d'après le petit théorème de Fermat, $3^{22} \equiv 1\,[23]$.
De plus, $3^{52} = (3^{22})^2 \times 3^8$ et $3^8 = 6561 = 285 \times 23 + 6$, d'où $3^8 \equiv 6\,[23]$.
Ainsi, $3^{52} \equiv 1^2 \times 6\,[23] \equiv 6\,[23]$ et le reste de la division euclidienne de 3^{52} par 23 est 6.

(b) 29 est un nombre premier ne divisant pas 4 donc, d'après le petit théorème de Fermat, $4^{28} \equiv 1\,[29]$.
De plus, $4^{89} = (4^{28})^3 \times 4^5$ et $4^5 = 1024 = 35 \times 29 + 9$, d'où $4^5 \equiv 9\,[29]$.
Ainsi, $4^{89} \equiv 1^3 \times 9\,[29] \equiv 9\,[29]$ et le reste de la division euclidienne de 4^{89} par 29 est 9.

(c) 97 est un nombre premier ne divisant pas 15 donc, d'après le petit théorème de Fermat, $15^{96} \equiv 1\,[97]$.
De plus, $15^{100} = 4^{96} \times 15^4$ et $15^4 = 50625 = 521 \times 97 + 88$, d'où $15^4 \equiv 88\,[97]$. Ainsi, $15^{100} \equiv 1 \times 88\,[97] \equiv 88\,[97]$ et le reste de la division euclidienne de 15^{100} par 97 est 88.

Exercice 41

1. On pose $n = 3^{4\times 6}$.
   (a) $5 \in \mathfrak{P}$, 3 n'est pas divisible par 5 donc, d'après le petit théorème de Fermat, $3^4 \equiv 1\,[5]$. Ainsi $3^{4\times 6} \equiv (3^4)^6\,[5] \equiv 1^6\,[5] \equiv 1\,[5]$.
   De même, d'après le petit théorème de Fermat, $3^6 \equiv 1\,[7]$
   d'où $3^{4\times 6} \equiv (3^4)^4\,[7] \equiv 1^4\,[7] \equiv 1\,[7]$.
   Puisque $n \equiv 1\,[5]$, 5 divise $n-1$. De même, puisque $n \equiv 1\,[7]$, 7 divise $n-1$. De plus, 5 et 7 sont premiers entre eux donc, d'après un corollaire du théorème de Gauss, $5 \times 7 = 35$ divise $n-1$ et donc $n \equiv 1\,[35]$.
   (b) D'après la question précédente, $3^{24} \equiv 1\,[35]$
   d'où $3^{75} \equiv \left(3^{24}\right)^3 \times 3^3 \equiv 3^3 \equiv 27\,[35]$.
2. On a $3^{72} = 3^{4\times 18}$. D'après le petit Fermat, $3^4 \equiv 1\,[5]$ donc $3^{4\times 18} \equiv (3^4)^{18}\,[5] \equiv 1^{18}\,[5] \equiv 1\,[5]$. D'autre part, toujours d'après le petit Fermat, $3^{18} \equiv 1\,[19]$ et $3^{4\times 18} \equiv (3^{18})^4\,[19] \equiv 1^4\,[19] \equiv 1\,[19]$.
   Or, $5 \wedge 19 = 1$, donc $3^{72} \equiv 3^{18\times 4}\,[5 \times 19] \equiv 1\,[95]$.
   On en déduit que $3^{72} \times 3^3 \equiv 1 \times 3^3\,[95]$ et donc que $3^{75} \equiv 27\,[95]$.
3. On a $4^{40} = 4^{4\times 10}$. D'après le petit Fermat, $4^4 \equiv 1\,[5]$, d'où $4^{4\times 10} \equiv (4^4)^{10}\,[5] \equiv 1^{10}\,[5] \equiv 1\,[5]$. De même, d'après le petit Fermat, $4^{10} \equiv 1\,[11]$, d'où $4^{4\times 10} \equiv (4^{10})^4\,[11] \equiv 1^4\,[11] \equiv 1\,[11]$.
   De plus, $5 \wedge 11 = 1$ donc $4^{40} \equiv 4^{4\times 10}\,[5 \times 11] \equiv 1\,[55]$.
   Ainsi, $4^{207} \equiv (4^{40})^5 \times 4^7\,[55] \equiv 1^5 \times 4^7\,[55] \equiv 16384\,[55]$.
   Or, $16384 = 297 \times 55 + 49$ donc $4^{207} \equiv 49\,[55]$.

Exercice 42 Puissance de 4

1. On a $4 \equiv 1\,[3]$ donc, pour tout $n \in \mathbb{N}$, $4^n \equiv 1^n\,[3] \equiv 1\,[3]$.
2. 29 est un nombre premier qui ne divise pas 4 donc, d'après le petit théorème de Fermat, $4^{28} \equiv 1\,[29]$ d'où $4^{28} - 1 \equiv 0\,[29]$ et 29 divise $4^{28} - 1$.
3. (a) On a $4^1 \equiv 4\,[17]$, $4^2 \equiv 16\,[17]$, $4^3 \equiv 13\,[17]$ et $4^4 \equiv 256\,[17] \equiv 1\,[17]$.
   (b) Ainsi, pour tout $k \in \mathbb{N}$, $4^{4k}\,[17] \equiv (4^4)^k\,[17] \equiv 1^k\,[17] \equiv 1\,[17]$ et $4^{4k} - 1$ est divisible par 17.
4. Soit $k \in \mathbb{N}$. On a $4^{2k} \equiv (4^2)^k\,[5] \equiv 16\,[5] \equiv 1\,[5]$
   et $4^{2k+1} \equiv (4^2)^n \times 4\,[5] \equiv 1 \times 4\,[5] \equiv 4\,[5]$. Ainsi, $4^n \equiv 1\,[5]$ si, et seulement si, n est pair : $4^n - 1$ est divisible par $5 \iff n$ est pair.
5. D'après la question 1., $4^{28} - 1$ est divisible par 3. D'après la question 2., $4^{28} - 1$ est divisible par 29. D'après la question 3., $4^{28} - 1$ est divisible par 17 car $28 = 4 \times 7$. Enfin, d'après la question 4., $4^{28} - 1$ est divisible par 5 car 28 est un nombre pair. Donc 3, 29, 17 et 5 sont quatre diviseurs premiers de $4^{28} - 1$.

Exercice 43 Triplets pythagoriciens : $(E) : x^2+y^2 = p^2$ pour $p \in \mathfrak{P}$ et $x,\ y \in \mathbb{N}^*$.

1. Si $p = 2$, l'équation devient $x^2 + y^2 = 4$ qui n'admet trivialement pas de solutions entières non nulles car $1^2 + 1^2 = 2 < 4$ et $1^2 + 2^2 = 5 > 4$.
2. Supposons que $p \neq 2$ et que le couple $(\,x\,,\,y\,)$ est solution de (E).
   (a) On sait que z et z^2 ont même parité. La somme de deux impairs ainsi que la somme de deux pairs étant paire, $x^2 + y^2$ est pair lorsque x^2 et y^2 ont même parité c.-à-d. lorsque x et y ont même parité. Puisque p est un premier impair, p^2 est impair et ne peut ainsi être égal à la somme de nombre de même parité. Donc, si $(\,x\,,\,y\,)$ est solution de (E), x et y sont de parité différente.
   (b) Si $p|x \neq 0$, alors il existe $k \in \mathbb{N}^*$ tel que $x = kp$.
   On a alors $x^2 + y^2 = p^2 \iff y^2 = p^2 - (kp)^2 = p^2(1-k^2) \leqslant 0$ ce qui contredit $y \neq 0$.
   (c) Soit $d = \mathrm{PGCD}\,(\,x\,,\,y\,)$. On a $x^2 + y^2 = p^2 \iff (dx')^2 + (dy')^2 = p^2$ $\iff d^2(x'^2 + y'^2) = p^2$ donc $d|p^2$.
   Ainsi, $d \in D(p^2) = \{1\,;\,p\,;\,p^2\}$. Puisque $p \not|\, x$, $d \notin \{p\,;\,p^2\}$ et $d = 1$: x et y sont premiers entre eux.
3. Supposons que p est la somme de deux carrés : $p = u^2 + v^2$ où u et $v \in \mathbb{N}^*$.
   (a) On a $\left|u^2 - v^2\right|^2 + (2uv)^2 = (u^2 - v^2)^2 + 4u^2v^2$
   $$\begin{aligned}\left|u^2 - v^2\right|^2 + (2uv)^2 &= u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = u^4 + 2u^2v^2 + v^4\\ &= (u^2+v^2)^2 = p^2\end{aligned}$$
   et le couple $\left(\left|u^2 - v^2\right|\,,\,2uv\right)$ est solution de (E).
   (b) Pour $p = 5 = 1^2 + 2^2$, le couple $\left(\left|u^2 - v^2\right|\,,\,2uv\right) = (\,3\,,\,4\,)$ est solution de (E) : $3^2 + 4^2 = 5^2$.
   Pour $p = 13 = 3^2 + 2^2$, le couple $\left(\left|u^2 - v^2\right|\,,\,2uv\right) = (\,5\,,\,12\,)$ est solution de (E) : $5^2 + 12^2 = 13^2$.
4. (a) $1^2 + 1^2 = 2 < 3$ et $1^2 + 2^2 = 5 > 3$ donc $p = 3$ ne peut s'écrire comme somme de deux carrés.
   $1^2 + 2^2 = 5 < 7$ et $2^2 + 2^2 = 8 > 7$ donc $p = 7$ ne peut s'écrire comme somme de deux carrés.
   (b) $x^2 + y^2 = 9 \iff y^2 = 9 - x^2 = (3-x)(3+x) > 0 \Longrightarrow x \in \{1\,;\,2\}$
   $\Longrightarrow y^2 \in \{9-1\,;\,9-2^2\} = \{5\,;\,8\}$ qui ne sont pas des carrés donc $x^2 + y^2 = 9$ n'admet pas de solutions entières.
   $x^2 + y^2 = 49 \iff y^2 = 49 - x^2 = (7-x)(7+x) > 0 \Longrightarrow x \in \{1\,;\,2\,;\,\ldots\,;\,6\}$
   $\Longrightarrow y^2 \in \{49-1\,;\,\ldots\,;\,49-6^2\} = \{13\,;\,24\,;\,33\,;\,40\,;\,45\,;\,48\}$ qui ne sont pas des carrés donc $x^2 + y^2 = 49$ n'admet pas de solutions entières.
   (c) On a $5 = 4\times1+1 \equiv 1\,[4]$, $13 = 4\times3+1 \equiv 1\,[4]$ et $3 = 4\times0+3 \not\equiv 1\,[4]$, $7 = 4\times1+3 \not\equiv 1\,[4]$.

Chapitre X

SUITES & MATRICES

Sommaire

Dernier chapitre de l'année, nous nous devons de parcourir tout le programme et de le mettre en lien avec d'autres domaines mathématiques : matrices à coefficients réels ou complexes, suites, graphes, probabilités et peut-être même arithmétique. Dans la première partie, nous confortons ce que nous avons pu observer sur les suites de matrices. Ensuite, nous appliquons tout ceci en probabilités en étudiant les chaînes d'Andreï Markov (1852-1922), mathématicien russe disciple de Tchebychev ayant publié les premiers résultats en 1906. Les systèmes markoviens sont très importants en probabilités mais aussi en physique, dans l'étude du mouvement brownien (mouvement aléatoire), dans la théorie des files d'attente, en bio-informatique, etc.

1 Suites de matrices

L'exemple principal de ce paragraphe est basé sur la situation « prédateurs-proies » suivante.

$\boxed{\text{Forêt}}$ Dans la forêt lointaine, on entend le coucou mais aussi des lapins qui tentent d'échapper aux renards. On sait bien que plus il y a de lapins, mieux les renards s'en portent ce qui fait que chaque année, la population de renards augmente à raison de 1 % de la population de lapins même si, concomitamment, 10 % des renards périssent de mort naturelle, ainsi va la vie. Quant aux lapins, leur population s'accroît de 1 % par an, même si elle est diminuée d'autant de lapins que de renards présents. Au début de l'année 2020, le coucou avait dénombré 10 renards et 10 000 lapins dans sa forêt.

Si l'on appelle r_n et ℓ_n les populations de renards et de lapins l'année $2020+n$, on a $\left\{\begin{array}{l} r_0 = 10 \\ \ell_0 = 10\,000 \end{array}\right.$ et, pour tout $n \in \mathbb{N}$, $\left\{\begin{array}{l} r_{n+1} = 0,9r_n + 0,01\ell_n \\ \ell_{n+1} = -r_n + 1,01\ell_n. \end{array}\right.$

Définition 1 *Soit $k \in \mathbb{N}^*$. On appelle suite de matrices colonnes de taille $k \times 1$, toute fonction qui, à tout entier naturel n, associe une matrice colonne de taille $k \times 1$. Une telle suite est généralement notée $(U_n)_{\mathbb{N}}$. Ses éléments sont donc k suites numériques.*

Remarque : On peut définir de manière analogue les suites de matrices lignes et celles de taille $p \times q$. Dans ce paragraphe, nous travaillons surtout avec les suites de matrices colonnes : il y a de nombreuses applications de ce cas de figure. En revanche, nous travaillerons avec des suites de matrices lignes dans le dernier paragraphe avec des résultats et des techniques similaires.

Exemples : La suite $(U_n)_{\mathbb{N}}$ définie par $U_n = \begin{pmatrix} n^2 \\ 7 - \frac{2}{n+1} \end{pmatrix}$ est une suite de matrices colonnes et la suite $(V_n)_{\mathbb{N}^*}$ définie par $V_n = \begin{pmatrix} e^{-n} & 7 & 2 - \frac{1}{n} \end{pmatrix}$ est une suite de matrices lignes.

$\boxed{\text{Forêt}}$ Afin de modéliser cette situation, on peut définir une suite de matrices $(F_n)_{\mathbb{N}}$ par $F_n = \begin{pmatrix} r_n \\ \ell_n \end{pmatrix}$.

Définition 2 *On dit qu'une suite de matrices (U_n) converge lorsque tous ses éléments, qui sont des suites, convergent. La limite U de cette suite est alors la matrice ayant pour éléments, la limite de chacun des éléments.*
Une suite de matrices qui ne converge pas est dite divergente.

Exemples : Clairement, la suite $U_n = \begin{pmatrix} n^2 \\ 7 - \frac{2}{n+1} \end{pmatrix}$ diverge tandis que la suite $V_n = \begin{pmatrix} e^{-n} & 7 & 2 - \frac{1}{n} \end{pmatrix}$ converge vers $V = \begin{pmatrix} 0 & 7 & 2 \end{pmatrix}$, mais quid de l'évolution de la suite (F_n) ?

Propriété 1 *Soient $k \in \mathbb{N}^*$, A une matrice carrée d'ordre k et $(U_n)_{\mathbb{N}}$ la suite de matrices colonnes de taille $k \times 1$ définie par $\left\{\begin{array}{l} U_0 \\ U_{n+1} = AU_n. \end{array}\right.$*
On a alors, pour tout $n \in \mathbb{N}$, $U_n = A^n U_0$.

Remarque : Et l'on pense évidemment à $u_{n+1} = au_n$...

Démonstration : Par récurrence triviale : On a $U_0 = I_k U_0 = A^0 U_0$.
Supposons que $U_n = A^n U_0$. On a alors $U_{n+1} = AU_n = A.A^n U_0 = A^{n+1} U_0$. □

Exemple : $\boxed{\text{Forêt}}$ On a vu que $F_0 = \begin{pmatrix} r_0 \\ \ell_0 \end{pmatrix}$ et $F_{n+1} = \begin{pmatrix} r_{n+1} \\ \ell_{n+1} \end{pmatrix} = \begin{pmatrix} 0,9r_n + 0,01\ell_n \\ -r_n + 1,01\ell_n \end{pmatrix}$. La suite $(F_n)_{\mathbb{N}}$ est donc définie par récurrence. Posons $A = \begin{pmatrix} 0,9 & 0,01 \\ -1 & 1,01 \end{pmatrix}$.
On a, pour tout n, $F_{n+1} = AF_n$ donc $F_n = A^n F_0$.
Puisque $F_3 = A^3 F_0 \simeq \begin{pmatrix} 280 \\ 9984 \end{pmatrix}$, le coucou devrait dénombrer environ 280 renards et 10 000 lapins dans la forêt au début de l'année $2020 + 3 = 2023$.

Puisque $F_{200} = A^{200}F_0 \simeq \begin{pmatrix}0\\0\end{pmatrix}$, il ne devrait plus rester de renards ni de lapins d'ici deux siècles.

Propriété 2 *Soient $k \in \mathbb{N}^*$, A une matrice carrée d'ordre k, B une matrice colonne de taille $k\times 1$ et $(U_n)_{\mathbb{N}}$ la suite de matrices colonnes de taille $k\times 1$ définie par* $\begin{cases} U_0 \\ U_{n+1} = AU_n + B. \end{cases}$
Si la suite (U_n) converge, alors sa limite est une matrice colonne U vérifiant
$U = AU + B.$
La matrice U est alors appelée état stable de la suite (U_n).

Démonstration : Posons $A = (a_{i,j})_{k\times k}$, $B = (b_i)_{k\times 1}$, $U_n = (u_i^{(n)})_{i\in[\![1\,;k]\!]}$ et, par hypothèse, $U = \lim\limits_{n\to\infty} U_n = (\lim\limits_{n\to\infty} u_i^{(n)})_{i\in[\![1\,;k]\!]\times 1} = (u_i)_{i\in[\![1\,;k]\!]\times 1}$.

On a $U_{n+1} = AU_n + B$ donc, d'après la règle du produit matriciel, pour tout $i \in [\![1\,;k]\!]$, $u_i^{(n+1)} = \sum\limits_{j=1}^{k} a_{i,j}u_j^{(n)} + b_i$ et en passant à la limite lorsque $n \to +\infty$,

$u_i = \sum\limits_{j=1}^{k} a_{i,j}u_j + b_i.$ D'où $U = AU + B.$ □

Exemple : $\boxed{\text{Forêt}}$ Afin de réguler la population de prédateurs et de proies, l'Office national des forêts relâche 1 000 lapins et abat 10 renards de cette forêt chaque année. Posons alors $B = \begin{pmatrix}-10\\1000\end{pmatrix}$ et l'on obtient la nouvelle relation de récurrence $F_{n+1} = AF_n + B$.
Ainsi, $F_1 = AF_0 + B = \begin{pmatrix}99\\11090\end{pmatrix}$, $F_2 = AF_1 + B = \begin{pmatrix}190\\12102\end{pmatrix}$ et $F_3 = AF_2 + B = \begin{pmatrix}282\\13032\end{pmatrix}$: avec l'action de l'ONF, le coucou devrait dénombrer environ 280 renards et 13 000 lapins dans la forêt au début de l'année 2020+3 = 2023.
Cherchons donc une matrice colonne stable $F = \begin{pmatrix}r\\\ell\end{pmatrix}$. L'équation $F = AF + B$ se traduit par le système
$\begin{cases} r = 0,9r + 0,01\ell - 10 \\ \ell = -r + 1,01\ell - 1000 \end{cases} \iff \begin{cases} r \simeq 1122 \\ \ell \simeq 12222. \end{cases}$ D'où $F \simeq \begin{pmatrix}1122\\12222\end{pmatrix}$.
Si les populations se stabilisent, le coucou devrait alors dénombrer environ 1 100 renards et 12 200 lapins dans sa forêt.

Avec la propriété suivante, nous obtenons une expression plus explicite d'un état stable et de U_n.

Propriété 3 *Soit* $(U_n)_{\mathbb{N}} : \begin{cases} U_0 \\ U_{n+1} = AU_n + B. \end{cases}$ *On suppose de plus que la matrice $A - I_k$ est inversible.*
On pose alors $C = -(A - I_k)^{-1}B$ et l'on définit la suite de matrices colonnes (V_n) par $V_n = U_n - C$.
Alors la suite (V_n) vérifie $\begin{cases} V_0 = U_0 - C \\ V_{n+1} = AV_n. \end{cases}$ *et donc* $V_n = A^nV_0$.
Ainsi, pour tout entier n, $U_n = A^n(U_0 - C) + C$.

Démonstration : On remarque premièrement que C est bien une matrice colonne puisque $A - I_k$ est carrée d'ordre k et B colonne de taille $k \times 1$. On a alors

$$\begin{aligned} V_{n+1} - V_n &= U_{n+1} - U_n = AU_n + B - U_n = (A - I_k)U_n + (A - I_k)(A - I_k)^{-1}B \\ &= (A - I_k)(U_n + (A - I_k)^{-1}B) = (A - I_k)(U_n - C) \\ &= (A - I_k)V_n = AV_n - V_n \quad \text{d'où} \quad V_{n+1} = AV_n. \end{aligned}$$

La relation $V_n = A^n V_0$ découle alors de la propriété 1 et $V_n = U_n - C$ donne

$$U_n = A^n(U_0 - C) + C. \qquad \square$$

<u>*Remarques :*</u> • Si $A - I_k$ n'est pas inversible et $B \neq O_k$, alors la suite (U_n) se comporte comme une suite arithmétique. Penser à $u_{n+1} = 1u_n + b$...

• Sous les conditions de la propriété, $C = AC + B \iff (A - I_k)C = -B$ $\iff C = -(A - I_k)^{-1}B$: la matrice C est un état stable de la suite (U_n). De plus, si $\lim\limits_{n\to\infty} A^n = O_k$, alors $U = \lim\limits_{n\to\infty} U_n = C$.

• En revanche, nous n'avons pas de condition nécessaire et suffisante pour que la suite des puissances d'une matrices converge. En effet, ce problème dépasse largement notre domaine de compétences et vous ne l'étudierez que dans quelques années. Nous pouvons tout de même remarquer que si l'on a diagonalisé cette matrice par D : $A = QDQ^{-1}$, il suffit que les termes diagonaux de D soient tous de module strictement inférieur à 1 pour que D^n et donc A^n converge vers O_k.

Exemple : $\boxed{\text{Forêt}}$ On a $\det(A - I_2) = \det\begin{pmatrix} -0,1 & 0,01 \\ -1 & 0,01 \end{pmatrix}$

$\det(A - I_2) = -0,1 \times 0,01 - (-1) \times 0,01 = 0,009 \neq 0$ donc $A - I_2$ est inversible et $(A - I_k)^{-1} = \frac{1}{0,009}\begin{pmatrix} 0,01 & -0,01 \\ 1 & -0,1 \end{pmatrix}$.

Posons $C = -\frac{1000}{9}\begin{pmatrix} 1/100 & -1/100 \\ 1 & -1/10 \end{pmatrix}\begin{pmatrix} -10 \\ 1000 \end{pmatrix} \simeq \begin{pmatrix} 1122 \\ 12222 \end{pmatrix} = F$. On a alors

$F_n = A^n(F_0 - C) + C$ et l'on retrouve bien $A^3(F_0 - C) + C \simeq \begin{pmatrix} 282 \\ 13032 \end{pmatrix} = F_3$.

2 Chaînes de Markov

On notera $\mathbb{P}_{(A)}(B) = \frac{\mathbb{P}(B\cap A)}{\mathbb{P}(A)}$ la probabilité conditionnelle de B sachant A, probabilités que l'on considérera dans ce paragraphe comme toutes définies c.-à-d. $\mathbb{P}(A) \neq 0$.

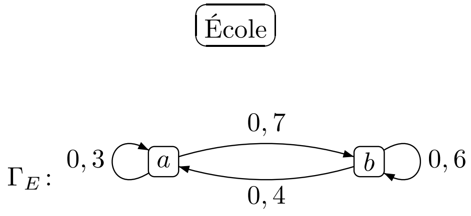
Les exemples du cours se baseront sur les deux situations suivantes.

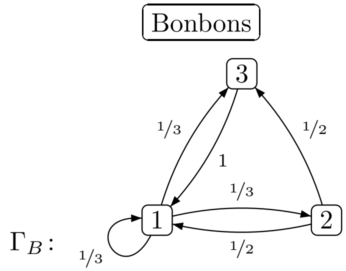
$\boxed{\text{École}}$ Pour se rendre à l'école, Agathe peut prendre l'autobus azur ou monter sa bicyclette bleue. Elle prend l'autobus trois fois sur dix lorsqu'elle l'a pris la veille, quatre fois sur dix sinon. Le jour de la rentrée, elle utilise l'autobus avec une probabilité p.

$\boxed{\text{Bonbons}}$ Colette dispose d'un immense sachet remplis de délicieuses friandises dans lequel elle puise une à trois confiseries chaque jour. Si, un jour donné, elle en a mangé une, elle en prend aléatoirement une, deux ou trois le jour suivant. Si elle en a dégusté deux, elle en savoure une ou trois aléatoirement le lendemain. En revanche, si elle en a englouti trois, elle n'en goûte qu'une seule ensuite. Le premier jour, elle en s'en délecte aléatoirement d'une, de deux ou de trois.

Définition 3 *Un graphe pondéré est un graphe dans lequel chaque arête est affectée d'un nombre réel positif, appelé poids de cette arête.*
Un graphe probabiliste est un graphe orienté pondéré par des réels de $[\,0\,;1\,]$ *tels que la somme des poids des arêtes issues de chaque sommet égale* 1.
Les sommets d'un graphe probabiliste sont appelés des états.

Exemples : Les graphes Γ_E et Γ_B ci-dessous sont des graphes probabilistes à deux et à trois états modélisant nos deux situations.





Définition 4 *La matrice de transition d'un graphe probabiliste à k états ordonnés est la matrice carrée d'ordre k où le terme de la i^e ligne et j^e colonne est égal au poids de l'arête reliant le sommet numéro i au sommet numéro j si elle existe,* 0 *sinon.*

Exemples : Matrices de transition des graphes probabilistes Γ_E et Γ_B précédents :

$\boxed{\text{École}}$ $P_E = \begin{pmatrix} 0,3 & 0,7 \\ 0,4 & 0,6 \end{pmatrix}$ et $\boxed{\text{Bonbons}}$ $P_B = \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/2 & 0 & 1/2 \\ 1 & 0 & 0 \end{pmatrix}$.

Remarques : • Il est nécessaire d'avoir préalablement numéroté les sommets, les états, généralement dans l'ordre croissant ou alphabétique.

• La somme des termes d'une même ligne d'une matrice de transition d'un graphe probabiliste égale 1. De plus, chaque terme d'une matrice de transition appartient à l'intervalle $[\,0\,;1\,]$. De telles matrices sont dites stochastiques.

• Si un graphe probabiliste permet de visualiser une situation, sa matrice de transition permet, elle, d'effectuer des calculs et d'obtenir des résultats précis.

Définition 5 *Soit (X_m) une suite de variables aléatoires modélisant l'évolution par étapes successives d'un système aléatoire comportant k états. On désigne par* $\Omega = \{e_1; e_2; \ldots; e_k\} \simeq \{1; 2; \ldots; k\}$ *l'univers, l'espace des états, de chaque variable aléatoire X_m.*
On dit que la suite (X_m) est une chaîne de Markov à k états lorsque la probabilité de passer de l'état i à l'état j de l'étape n à l'étape $n+1$ ne dépend que de l'état à l'étape n, et non des états précédents : $\forall n \in \mathbb{N}$ *et* $\forall (i_0; i_1; \ldots; i_{n-1}; i; j) \in \Omega^{n+2}$,

$$\mathbb{P}_{(X_0=i_0\,,\,X_1=i_1\,,\,\ldots\,,\,X_{n-1}=i_{n-1}\,,\;X_n=i)}(X_{n+1}=j) = \mathbb{P}_{(X_n=i)}(X_{n+1}=j).$$

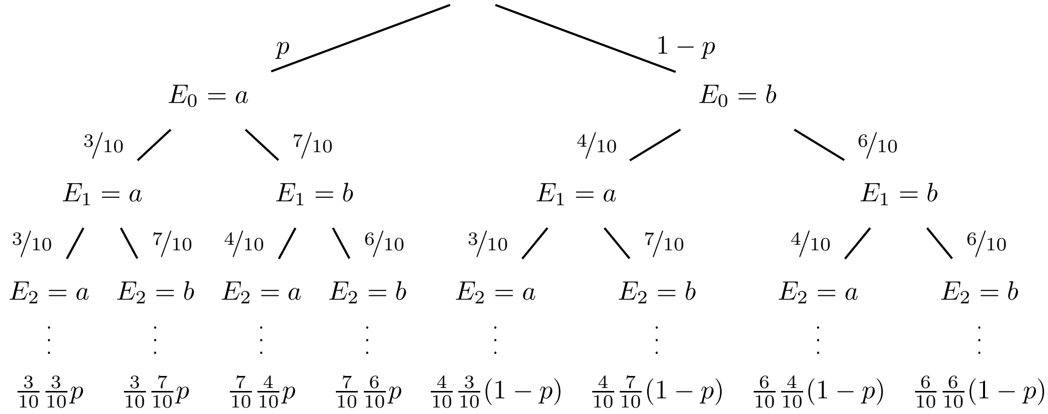
On dit qu'une chaîne de Markov à k états (X_m) est homogène lorsque la probabilité de transition d'un état à un autre entre l'étape n et l'étape $n+1$ ne dépend pas de n et l'on a alors, pour tout n, $\mathbb{P}_{(X_n=i)}(X_{n+1}=j) = \mathbb{P}_{(X_0=i)}(X_1=j) = p_{i,j}$, *probabilité de transition de l'état i à l'état j.*

Remarques : • Rassurez-vous, nous n'étudierons que des chaînes de Markov homogènes à deux ou à trois états : $k \in \{2; 3\}$.

• Dans une chaîne de Markov, les états passés n'ont aucune influence sur les états futurs, seul l'état présent importe et ce de manière homogène, indépendamment de l'étape.

• À toute chaîne de Markov homogène, on peut donc associer un graphe probabiliste Γ où les sommets sont les k états du système aléatoire et le poids de chaque arête est égal à la probabilité de transition d'un état à un autre $p_{i,j}$, ainsi qu'une matrice de transition $P = (p_{i,j})_{k\times k}$ de ce graphe probabiliste. Γ et P sont alors communs à toutes les transitions d'une étape à sa suivante puisque les probabilités celles-ci ne dépendent pas de n.

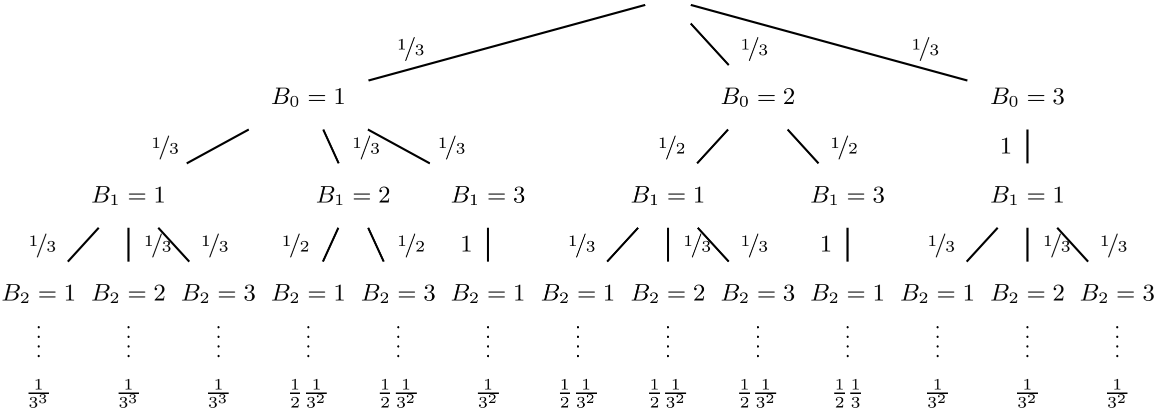
Exemples : École Soit E_n la variable aléatoire donnant le mode de locomotion utilisé par Agathe pour se rendre à l'école le $(n+1)$-ième jour de classe. L'espace des états est donc $\Omega_E = \{a; b\}$.
D'après l'énoncé de la situation, la probabilité de prendre l'un ou l'autre des moyens de locomotion ne dépend que de la situation de la veille. De plus, ces probabilités sont constantes et ne dépendent donc pas de n. Ainsi, la suite (E_n) est une chaîne de Markov à deux états.
Les probabilités de transitions sont $p_{a,a} = \mathbb{P}_{(E_0=a)}(E_1 = a) = 0,3$, $p_{a,b} = \mathbb{P}_{(E_0=a)}(E_1 = b) = 0,7$, $p_{b,a} = \mathbb{P}_{(E_0=b)}(E_1 = a) = 0,4$ et $p_{b,b} = \mathbb{P}_{(E_0=b)}(E_1 = b) = 0,6$.
Au jour de la rentrée, on a $\mathbb{P}(E_0 = a) = p$ et $\mathbb{P}(E_0 = b) = 1 - p$.
Dressons donc un arbre de probabilité afin de déterminer la loi de probabilité de E_2, correspondant au 3e jour de classe.



Ainsi, on a $\mathbb{P}(E_2 = a) = \frac{1}{100}(9p + 28p + 12(1-p) + 24(1-p)) = \frac{36+p}{100}$
et $\mathbb{P}(E_2 = b) = \frac{1}{100}(21p + 42p + 28(1-p) + 36(1-p)) = \frac{64-p}{100}$.
D'où la loi de E_2 suivante.

État e	a	b
$P(E_2 = e)$	$\frac{36+p}{100}$	$\frac{64-p}{100}$

$\boxed{\text{Bonbons}}$ Soit B_n la variable aléatoire donnant le nombre de friandises savourées par Colette le $(n+1)$-ième jour. L'espace des états est donc $\Omega_B = \{1; 2; 3\}$.
D'après l'énoncé de la situation, la probabilité d'ingérer une, deux ou trois confiseries ne dépend que du nombre de douceurs absorbées la veille. De plus, ces probabilités sont constantes et ne dépendent donc pas de n. Ainsi, la suite (B_n) est une chaîne de Markov à trois états.
Les probabilités de transitions sont $p_{1,1} = \mathbb{P}_{(B_0=1)}(B_1 = 1) = \frac{1}{3}$,
$p_{1,2} = \mathbb{P}_{(B_0=1)}(B_1 = 2) = \frac{1}{3}$, $p_{1,3} = \mathbb{P}_{(B_0=1)}(B_1 = 3) = \frac{1}{3}$,
$p_{2,1} = \mathbb{P}_{(B_0=2)}(B_1 = 1) = \frac{1}{2}$, $p_{2,2} = \mathbb{P}_{(B_0=2)}(B_1 = 2) = 0$,
$p_{2,3} = \mathbb{P}_{(B_0=2)}(B_1 = 3) = \frac{1}{2}$, $p_{3,1} = \mathbb{P}_{(B_0=3)}(B_1 = 1) = 1$,
$p_{3,2} = \mathbb{P}_{(B_0=3)}(B_1 = 2) = 0$ et $p_{3,3} = \mathbb{P}_{(B_0=3)}(B_1 = 3) = 0$.
On a au premier jour $\mathbb{P}(B_0 = 1) = \mathbb{P}(B_0 = 2) = \mathbb{P}(B_0 = 3) = \frac{1}{3}$.
Dressons donc un arbre de probabilité afin de déterminer la loi de probabilité de B_2, correspondant au 3ᵉ jour de dégustation.



Ainsi, on a $\mathbb{P}(B_2 = 1) = \frac{1}{3^3} + \frac{1}{2}\frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{2}\frac{1}{3^2} + \frac{1}{2}\frac{1}{3} + \frac{1}{3^2} = \frac{29}{54}$,
$\mathbb{P}(B_2 = 2) = \frac{1}{3^3} + \frac{1}{2}\frac{1}{3^2} + \frac{1}{3^2} = \frac{11}{54}$ et $\mathbb{P}(B_2 = 3) = \frac{1}{3^3} + \frac{1}{2}\frac{1}{3^2} + \frac{1}{2}\frac{1}{3^2}\frac{1}{3^2} = \frac{14}{54}$.
D'où la loi de B_2 suivante.

État e	1	2	3
$P(B_2 = e)$	$29/54$	$11/54$	$14/54$

3 Évolution d'une chaîne de Markov

Propriété 4 *Avec les notations précédentes, la probabilité de passer de l'état i à l'état j après n transitions est égal au terme de la i^e ligne et de la j^e colonne de la matrice P^n.*

Démonstration : On se place dans le cas $k = 2$, similaire au cas général, et l'on démontre par récurrence la propriété $\begin{pmatrix} \mathbb{P}_{(X_0=1)}(X_n = 1) & \mathbb{P}_{(X_0=1)}(X_n = 2) \\ \mathbb{P}_{(X_0=2)}(X_n = 1) & \mathbb{P}_{(X_0=2)}(X_n = 2) \end{pmatrix} = P^n$ pour tout entier $n \in \mathbb{N}$.

· On a, par définition de la matrice de transition P,
$P^1 = P = \begin{pmatrix} p_{1,1} & p_{1,2} \\ p_{2,1} & p_{2,2} \end{pmatrix} = \begin{pmatrix} \mathbb{P}_{(X_0=1)}(X_1=1) & \mathbb{P}_{(X_0=1)}(X_1=2) \\ \mathbb{P}_{(X_0=2)}(X_1=1) & \mathbb{P}_{(X_0=2)}(X_1=2) \end{pmatrix}$ et la propriété est vraie au rang 1.
Elle est trivialement vraie au rang 0 mais ceci est moins élégant.

· Supposons que la propriété soit vraie pour un certain rang n.
Pour $(i\,,\,j) \in \{1;2\}^2$, notons $t_{i,j}^{(n)} = \mathbb{P}_{(X_0=i)}(X_n=j)$ la probabilité de passer de l'état i à l'état j après n transitions. Par hypothèse de récurrence, $(t_{i,j}^{(n)})_{i,j} = P^n$.
D'après la formule des probabilités totales, la relation $\mathbb{P}_B(A\cap B) = \mathbb{P}_B(A)\times\mathbb{P}_{C\cap A}(B)$ et la non dépendance des états passés, on a

$$\begin{aligned} t_{i,j}^{(n+1)} &= \mathbb{P}_{(X_0=i)}(X_{n+1}=j) \\ &= \mathbb{P}_{(X_0=i)}(X_n=1\cap X_{n+1}=j) + \mathbb{P}_{(X_0=i)}(X_n=2\cap X_{n+1}=j) \\ &= \mathbb{P}_{(X_0=i)}(X_n=1)\times\mathbb{P}_{(X_0=i\,\cap\,X_n=1)}(X_{n+1}=j) \\ &\qquad + \mathbb{P}_{(X_0=i)}(X_n=2)\times\mathbb{P}_{(X_0=i\,\cap\,X_n=2)}(X_{n+1}=j) \\ &= \mathbb{P}_{(X_0=i)}(X_n=1)\times\mathbb{P}_{(X_n=1)}(X_{n+1}=j) \\ &\qquad + \mathbb{P}_{(X_0=i)}(X_n=2)\times\mathbb{P}_{(X_n=2)}(X_{n+1}=j) \\ &= t_{i,1}^{(n)}\times p_{1,j} + t_{i,2}^{(n)}\times p_{2,j} \end{aligned}$$

$t_{i,j}^{(n+1)} = \sum_{\ell=1}^{2} t_{i,\ell}^{(n)}\times p_{\ell,j}$ qui est précisément le coefficient i,j de la matrice $P^n.P = P^{n+1}$ par hypothèse de récurrence sur P^n.

· La propriété est donc vraie pour tout $n\in\mathbb{N}$. □

Exemples : $\boxed{\text{École}}$ On a $P_E = \begin{pmatrix} 0,3 & 0,7 \\ 0,4 & 0,6 \end{pmatrix}$ donc $P_E^2 = \begin{pmatrix} 0,37 & 0,63 \\ 0,36 & 0,64 \end{pmatrix}$.
Ainsi, Agathe a 36 % de chances de prendre l'autobus deux jours après avoir monté sa bicyclette, 63 % de chances de monter sa bicyclette deux jours après avoir pris l'autobus, 37 % de chances de prendre l'autobus deux jours après l'avoir pris et 64 % de chances de monter sa bicyclette deux jours après l'avoir montée.

$\boxed{\text{Bonbons}}$ On a $P_B = \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/2 & 0 & 1/2 \\ 1 & 0 & 0 \end{pmatrix}$ donc $P_B^2 = \begin{pmatrix} 11/18 & 1/9 & 5/18 \\ 2/3 & 1/6 & 1/6 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$.
Ainsi, Colette a 1 chance sur 6 d'ingurgiter trois sucreries deux jours après en avoir avalé deux, 1 chance sur 3 de grignoter une gâterie deux jours après en avoir consommé trois, 5 chances sur 18 d'apprécier trois gourmandises deux jours après en avoir picoré une et 2 chances sur 3 de se sustenter d'un bonbon deux jours après s'en être régalé de deux.

Définition 6 *Soit (X_n) une chaîne de Markov.*
La loi de probabilité de X_0 est appelée la distribution initiale du système et la loi de probabilité de X_n est appelée la distribution après n transitions.
On note π_n la matrice ligne de taille $1\times k$ dont le j^e terme est la probabilité qu'à l'étape n, la variable aléatoire X_n égale e_j (ou j). La matrice π_n représente donc la distribution de X_n :
$\pi_n = (\mathbb{P}(X_n=e_1) \quad \mathbb{P}(X_n=e_2) \quad \dots \quad \mathbb{P}(X_n=e_k))_{1\times k}$.

Exemples : $\boxed{\text{École}}$ La distribution initiale est $\pi_0 = (p \quad 1-p)$ et, d'après la loi de E_2 donnée par l'arbre précédent, $\pi_2 = \left(\frac{36+p}{100} \quad \frac{64-p}{100}\right)$.

$\boxed{\text{Bonbons}}$ La distribution initiale est $\pi_0 = \left(\frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{3}\right)$ et, d'après la loi de B_2 donnée par l'arbre précédent, $\pi_2 = \left(\frac{29}{54} \quad \frac{11}{54} \quad \frac{14}{54}\right)$.

Propriété 5 *Pour tout entier naturel n,* $\pi_{n+1} = \pi_n P$ *et* $\pi_n = \pi_0 P^n$.

Démonstration : Elle est similaire à la précédente, en plus simple. On se place encore dans le cas où $k = 2$.

$$\begin{aligned}\mathbb{P}(X_{n+1} = j) &= \mathbb{P}(X_n = 1 \cap X_{n+1} = j) + \mathbb{P}(X_n = 2 \cap X_{n+1} = j)\\ &= \mathbb{P}(X_n = 1) \times \mathbb{P}_{(X_n=1)}(X_{n+1} = j) + \mathbb{P}(X_n = 2) \times \mathbb{P}_{(X_n=2)}(X_{n+1} = j)\\ &= \mathbb{P}(X_n = 1) \times p_{1,j} + \mathbb{P}(X_n = 2) \times p_{2,j}\end{aligned}$$

d'où $\pi_{n+1} = (\mathbb{P}(X_{n+1} = 1) \quad \mathbb{P}(X_{n+1} = 2))$

$$\pi_{n+1} = (\mathbb{P}(X_n = 1) \quad \mathbb{P}(X_n = 2)) \, . \begin{pmatrix} p_{1,1} & p_{1,2} \\ p_{2,1} & p_{2,2} \end{pmatrix} = \pi_n \, P.$$

La relation $\pi_n = \pi_0 P^n$ s'obtient alors par récurrence triviale. □

Exemples : $\boxed{\text{École}}$ On a $\pi_2 = \pi_0 P_E^2 = (p \quad 1-p) \begin{pmatrix} 0,37 & 0,63 \\ 0,36 & 0,64 \end{pmatrix}$

$\pi_2 = (0,37p + 0,36(1-p) \quad 0,63p + 0,64(1-p)) = (0,36 - 0,01p \quad 0,64 - 0,01p)$.

$\boxed{\text{Bonbons}}$ On a $\pi_2 = \pi_0 P_B^2 = \left(\frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{3}\right) \begin{pmatrix} 11/18 & 1/9 & 5/18 \\ 2/3 & 1/6 & 1/6 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$

$\pi_2 = \frac{1}{3}\left(\frac{11}{18} + \frac{2}{3} + \frac{1}{3} \quad \frac{1}{9} + \frac{1}{6} + \frac{1}{3} \quad \frac{5}{18} + \frac{1}{6} + \frac{1}{3}\right) = \left(\frac{29}{54} \quad \frac{11}{54} \quad \frac{14}{54}\right)$.

Remarque : Nous retrouvons bien les résultats précédents, obtenus au moyen d'arbres de probabilités, et ce de manière beaucoup plus rapide. Et nous ne sommes qu'à la deuxième étape...

Théorème 1 *Soit (X_n) une chaîne de Markov à k états de matrice de transition P et de distributions π_n.*

- *Il existe au moins une distribution π, appelée distribution invariante ou état stable, telle que* $\pi = \pi P$.
- *S'il existe un entier m tel que P^m ne contient pas de 0, alors cette distribution invariante π est unique et, pour toute distribution initiale π_0, la suite π_n converge vers π.*

Remarques : • Ce théorème, non optimal, est admis.

• Si X_0 admet une distribution invariante π comme distribution initiale π_0, alors il en est de même pour toutes les variables X_n de cette chaîne :

$\pi_n = \pi P^n = (\pi P).P^{n-1} = \pi P^{n-1} = \pi_{n-1} = \ldots = \pi_0 = \pi$.

• Si $\pi P = \pi$, alors toute matrice multiple de π (*i.e.* $\lambda\pi$) vérifie cette équation mais une seule est une distribution, celle dont la somme des termes vaut 1.

• Dire que P^m ne contient pas de 0 signifie que l'on peut passer de n'importe quel état à n'importe quel autre en m transitions : cela peut s'anticiper en regardant les chemins sur le graphe. Dans l'exemple Bonbons, on remarque aisément que l'état 3 peut-être atteint par chacun des états 1, 2 ou 3 en deux transitions.

Exemples : $\boxed{\text{École}}$ La matrice P_E ne contient pas de 0 : tout état peut être atteint à partir d'un autre en une transition. Il existe donc une unique distribution invariante $\pi_E = (x \quad y)$.
On doit donc avoir $\pi_E P_E = \pi_E$ où π_E représente une loi de probabilité.
Résolvons donc le système :

$$\begin{cases} 0,3x + 0,4y = x \\ 0,7x + 0,6y = y \\ x + y = 1 \end{cases} \iff \begin{cases} y = \frac{7}{4}x \\ 0 = 0 \\ x + \frac{7}{4}x = 1 \end{cases} \iff \begin{cases} x = {}^4/_{11} \\ y = {}^7/_{11}. \end{cases}$$

On voit bien que toute matrice de la forme $\begin{pmatrix} x & \frac{7}{4}x \end{pmatrix}$ est invariante mais une seule est une distribution. L'unique état stable de la chaîne de Markov d'Agathe est $\pi_E = \begin{pmatrix} \frac{4}{11} & \frac{7}{11} \end{pmatrix}$ et, quelle que soit la probabilité initiale de prendre l'autobus le jour de la rentrée, elle aura une probabilité proche de $\frac{4}{11}$ de le prendre le dernier jour de l'année.

$\boxed{\text{Bonbons}}$ La matrice P_B^2 ne contient pas de 0 : tout état peut être atteint à partir d'un autre en deux transitions. Il existe donc une unique distribution invariante $\pi_B = (x \quad y \quad z)$.
On doit donc avoir $\pi_B P_B = \pi_B$ où π_B représente une loi de probabilité.
Résolvons donc le système :

$$\begin{cases} \frac{1}{3}x + \frac{1}{2}y + 1z = x \\ \frac{1}{3}x = y \\ \frac{1}{3}x + \frac{1}{2}y = z \\ x + y + z = 1 \end{cases} \iff \begin{cases} y = \frac{1}{3}x \\ z = \frac{1}{2}x \\ 0 = 0 \\ x + \frac{1}{3}x + \frac{1}{2}x = 1 \end{cases} \iff \begin{cases} x = {}^6/_{11} \\ y = {}^2/_{11} \\ z = {}^3/_{11}. \end{cases}$$

On voit bien que toute matrice de la forme $\begin{pmatrix} x & \frac{1}{3}x & \frac{1}{2}x \end{pmatrix}$ est invariante mais une seule est une distribution. L'unique état stable de la chaîne de Markov de Colette est donc $\pi_B = ({}^6/_{11} \quad {}^2/_{11} \quad {}^3/_{11})$ et, après plusieurs mois, elle aura une probabilité proche de $\frac{3}{11}$ de dévorer trois friandises un jour donné et ce, même si ses parents lui en ont imposé une seule le premier jour.

Exercices

SUITES & MATRICES

Exercice 1 Suite de Fibonacci

La suite de Fibonacci est définie sur $\mathbb{N}$ par $\begin{cases} u_0 = u_1 = 1, \\ u_{n+2} = u_{n+1} + u_n. \end{cases}$

Pour tout entier $n \in \mathbb{N}$, on pose $U_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$.

1. Déterminer U_0, U_1 et U_2.
2. Déterminer une matrice A telle que, pour tout $n \in \mathbb{N}$, $U_{n+1} = AU_n$.
3. En déduire l'expression de U_n en fonction de A et de n.
4. À l'aide de la calculatrice, déterminer u_{20} et u_{21}.

Exercice 2 Soient les matrices $A = \begin{pmatrix} 0,2 & 0,1 \\ 0 & 0,1 \end{pmatrix}$, $B = \begin{pmatrix} 0,4 \\ 0,4 \end{pmatrix}$ et $U_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et soit la suite de matrices $(U_n)_{\mathbb{N}}$ telles que, pour tout entier n, $U_{n+1} = AU_n + B$.

1. Déterminer une matrice colonne U, état stable de la suite $(U_n)_{\mathbb{N}}$.
2. On pose $V_n = U_n - U$. Montrer que, pour tout entier n, $V_{n+1} = AV_n$.
3. En déduire l'expression de V_n puis celle de U_n en fonction de A et n.
4. Montrer que $A = PDP^{-1}$ où $P = \begin{pmatrix} 1 & -1/\sqrt{2} \\ 0 & 1/\sqrt{2} \end{pmatrix}$ et $D = Diag(0,2\,;\,0,1)$.
5. Étudier la convergence de la suite $(U_n)_{\mathbb{N}}$.

Exercice 3 Soient $U_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $A = \begin{pmatrix} 1/2 & 0 \\ -1/2 & 1/2 \end{pmatrix}$ et $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

On définit la suite $(U_n)_{\mathbb{N}}$ de matrices colonnes par $U_{n+1} = AU_n + B$.
Montrer que la suite $(U_N)_{\mathbb{N}}$ converge vers une matrice L à déterminer.
On pourra conjecturer puis démontrer l'expression de A^n à l'aide de la calculatrice.

Exercice 4 Dans un jardin public, un artiste doit installer une œuvre aquatique commandée par la mairie. Cette œuvre sera constituée de deux bassins A et B ainsi que d'une réserve filtrante R. Au départ, les deux bassins contiennent chacun 100 litres d'eau. Un système de canalisations devra alors permettre de réaliser, toutes les heures et dans cet ordre, les transferts d'eau suivants :

- dans un premier temps, la moitié du bassin A se vide dans la réserve R ;
- ensuite, les trois quarts du bassin B se vident dans le bassin A ;
- enfin, on rajoute 200 litres d'eau dans le bassin A et 300 litres d'eau dans le bassin B.

Une étude de faisabilité du projet amène à étudier la contenance des deux bassins A et B qui est à prévoir pour éviter tout débordement. On modélise les quantités d'eau des

EXERCICES

deux bassins A et B à l'aide de deux suites (a_n) et (b_n) : plus précisément pour tout entier naturel n, on note a_n et b_n les quantités d'eau en centaines de litres qui seront respectivement contenues dans les bassins A et B au bout de n heures. On suppose pour cette étude mathématique que les bassins sont *a priori* suffisamment grands pour qu'il n'y ait pas de débordement.

Pour tout entier naturel n, on note U_n la matrice colonne $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. Ainsi $U_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

1. Justifier que, pour tout entier naturel n, $\quad U_{n+1} = MU_n + C \quad$ où
   $M = \begin{pmatrix} 0,5 & 0,75 \\ 0 & 0,25 \end{pmatrix}$ et $C = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.
2. On considère la matrice $P = \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$.
   (a) Calculer P^2. En déduire que la matrice P est inversible et préciser son inverse.
   (b) Montrer que PMP est une matrice diagonale D que l'on précisera.
   (c) Calculer PDP.
   (d) Démontrer par récurrence que, pour tout entier naturel n, $M^n = PD^nP$.

On admet par la suite que pour tout $n \in \mathbb{N}$, $\quad M^n = \begin{pmatrix} 0,5^n & 3 \times 0,5^n - 3 \times 0,25^n \\ 0 & 0,25^n \end{pmatrix}$.

3. Montrer que la matrice $X = \begin{pmatrix} 10 \\ 4 \end{pmatrix}$ vérifie $\quad X = MX + C$.
4. Pour tout entier naturel n, on définit la matrice V_n par $\quad V_n = U_n - X$.
   (a) Montrer que tout entier naturel n, $\quad V_{n+1} = MV_n$.
   (b) On admet que, pour tout entier naturel non nul n, $\quad V_n = M^nV_0$.
   Montrer que pour tout $n \in \mathbb{N}^*$, $\quad U_n = \begin{pmatrix} -18 \times 0,5^n + 9 \times 0,25^n + 10 \\ -3 \times 0,25^n + 4 \end{pmatrix}$.
5. (a) Montrer que la suite (b_n) est croissante et majorée. Déterminer sa limite.
   (b) Déterminer la limite de la suite (a_n).
   (c) On admet que la suite (a_n) est croissante. En déduire la contenance des deux bassins A et B qui est à prévoir pour la faisabilité du projet, c'est-à-dire pour éviter tout débordement.

Exercice 5 Suites complexes et matrices

On considèrent deux suites de nombres complexes (z_n) et (z'_n) définies par $\quad z_0 = 1$, $z'_0 = i \quad$ et, pour tout entier $n \in \mathbb{N}$, $\quad \begin{cases} z_{n+1} &= (9-4i)z_n + (-3+2i)z'_n \\ z'_{n+1} &= (18-12i)z_n + (-6+6i)z'_n. \end{cases}$

1. Calculer z_1 et z'_1.
2. Écrire ce système sous forme matricielle $\quad Z_n = A.Z_n$.
3. Montrer par récurrence que, pour tout entier $n \in \mathbb{N}$, $\quad Z_{n+1} = A^n.Z_n$.
4. Détermination de A^n.
   (a) Soit $\quad P = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. $\quad$ Justifier que P est inversible puis déterminer P^{-1}.

(b) Montrer que $A = PDP^{-1}$ où $D = \begin{pmatrix} 2i & 0 \\ 0 & 3 \end{pmatrix}$.

(c) Montrer par récurrence que, pour tout $n \in \mathbb{N}$, $A^n = PD^nP^{-1}$.

(d) En déduire les coefficients de la matrice A^n.

5. Exprimer, pour tout $n \in \mathbb{N}$, z_n et z'_n en fonction de n.

Exercice 6 Compléter les matrices de transition suivantes où $p \in \left[0\,;\frac{1}{3}\right]$ puis représenter des graphes probabilistes leur correspondant.

$A = \begin{pmatrix} 0,2 & \dots \\ \dots & 0,4 \end{pmatrix}$ | $B = \begin{pmatrix} 0,35 & \dots & 0,25 \\ 0 & 0,1 & \dots \\ \dots & 0,5 & 0,2 \end{pmatrix}$ | $C = \begin{pmatrix} p & 0,4 & \dots \\ 0,7-p & \dots & 0,1 \\ \dots & 2p & p \end{pmatrix}$

Exercice 7 La matrice $P = \begin{pmatrix} 0,5 & 0,5 & 0 \\ 0 & 0,5 & 0,5 \\ 1 & 0 & 0 \end{pmatrix}$ est la matrice de transition associée à une chaîne de Markov dont la distribution initiale est donnée par $\pi_0 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$.

1. Représenter cette chaîne par un graphe pondéré.
2. Calculer la distribution après trois transitions.
3. À l'aide la calculatrice, conjecturer le comportement asymptotique de cette chaîne de Markov.
4. Justifier que la suite des distributions converge et en donner sa limite.

Exercice 8 Un mobile se déplace aléatoirement sur les sommets d'un triangle ABC. Il se situe sur le sommet A au début de l'expérience puis, à chaque seconde, soit il reste sur le sommet sur lequel il est situé avec une probabilité de $0,5$, soit il se déplace sur l'un des autres sommets avec une probabilité identique.

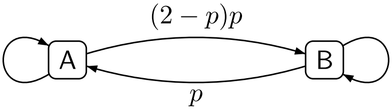
1. Représenter le déplacement du mobile par un graphe pondéré et donner la matrice de transition P associée.
2. Calculer P^3 et donner une interprétation du terme situé sur la 3e ligne et la 1re colonne.
3. Déterminer la probabilité que, 10 secondes après le début de l'expérience, le mobile soit sur le sommet A.
4. Justifier que la suite des distributions (π_n) converge et déterminer sa limite.

Exercice 9 Tous les matins, M.Fartezdekrié mange soit un kiwi, soit une mandarine. Pour choisir ce fruit, il lance un dé cubique bien équilibré, contrairement à lui, et s'il obtient un six, il savoure le même fruit que la veille, sinon, il en déguste un différent. Lundi, il a apprécié son kiwi. Quelle est la probabilité qu'il en avale un autre le lundi suivant ? Et que dire de l'an prochain ?

Exercice 10 On considère la matrice de transition $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ associée à une chaîne de Markov.

Peut-on trouver une chaîne invariante ? La suite des distributions après n transitions est-elle convergente ?

Exercice 11 Soit $p \in [0\,;1]$. On considère une chaîne de Markov associée au graphe probabiliste suivant.



1. Vérifier que $0 \leqslant (2-p)p \leqslant 1$.
2. Montrer que $\mathbb{P}_A(A) = (\mathbb{P}_B(B))^2$.
3. La distribution initiale de cette chaîne est $\begin{pmatrix} 0,3 & 0,7 \end{pmatrix}$.
   (a) Déterminer les valeurs de p correspondant aux extremums de la deuxième composante de la distribution de probabilité après une transition.
   (b) Que vaut alors la première composante de cette distribution de probabilité après une transition ?
   (c) Dresser les graphes probabilistes correspondants.

Exercice 12 On considère une chaîne de Markov (X_n) ayant π pour distribution invariante et l'on définit la chaîne de Markov (Z_n) par $Z_n = X_{2n}$.
Montrer que π est également une chaîne de Markov pour (Z_n).

Exercice 13 File d'attente

On modélise l'attente dans une certaine file par la situation suivante. À son arrivée, l'usager est en A. Quand il avance, il va tout d'abord en B puis en C où il reste et il est pris en charge. Chaque minute, il a une probabilité égale à $0,8$ de rester en A ou en B. On cherche à estimer le temps d'attente, c.-à-d. le nombre de minutes avant d'atteindre le point C. Pour tout entier n, la matrice $\pi_n = \begin{pmatrix} a_n & b_n & c_n \end{pmatrix}$ représente l'état probabiliste au bout de n minutes d'attente, où a_n, b_n et c_n désignent les probabilités d'être respectivement en A, B ou C à ce même moment.

1. Dresser un arbre probabiliste représentant la situation.
2. Déterminer la matrice de transition P de ce graphe probabiliste, l'état initial π_0 ainsi qu'une distribution invariante évidente π.
3. Quelle est l'attente minimale d'un usager.
4. Décomposer la matrice P en somme de deux matrices D et N où D est diagonale et N est strictement triangulaire et vérifier que $DN = ND$.
5. Calculer D^k et N^k pour tout entier k.
6. En déduire, en utilisant la formule du binôme de Newton pour les matrices commutantes(cf. ex. 21 p.77), que pour tout entier n non nul,
$$P^n = \begin{pmatrix} 0,8^n & 0,2 \times 0,8^{n-1} \times n & 0,02 \times 0,8^{n-2} \times n(n-1) \\ 0 & 0,8^n & 0,2 \times 0,8^{n-1} \times n \\ 0 & 0 & 1 \end{pmatrix}.$$
7. Montrer que π_n converge vers π.
8. Soit X la variable aléatoire correspondant au nombre de minutes d'attente.
   (a) Montrer que, pour tout entier naturel non nul k, on a $\mathbb{P}(X = k) = c_k - c_{k-1}$.

(b) Exprimer alors l'espérance $\mathbb{E}(X)$ de X en fonction des c_k.

(c) En déduire que $\quad \mathbb{E}(X) = 0,04 \lim\limits_{m\to+\infty} \sum\limits_{k=2}^{m} k(k-1)0,8^{k-2}$.

(d) On définit la fonction f sur $\mathbb{R}\setminus\{1\}$ par $\quad f_m(x) = \frac{1-x^{m+1}}{1-x}$.

Montrer que $\quad \displaystyle\sum_{k=2}^{m} k(k-1)x^{k-2} = f_m''(x)$.

(e) Déterminer alors $\mathbb{E}(X)$ puis interpréter le résultat obtenu dans le cadre de cet exercice.

Exercice 14 Les urnes d'Ehrenfest

On considère deux urnes A et B et un entier naturel non nul N. Au début de l'expérience, N boules numérotées de 0 à $N-1$ sont placées dans l'urne A et l'on répète ensuite n fois les actions suivantes : on choisit au hasard un nombre k entre 0 et $N-1$ et l'on déplace la boule numérotée k dans l'urne dans laquelle elle ne se trouve pas. On s'intéresse ici au cas $N=2$ et l'on désigne par X_j la variable aléatoire correspondant au nombre de boules contenues dans l'urne A à la j^{e} étape de l'expérience.

1. Quelles sont les valeurs que peut prendre X_j ?
   Afin de représenter cette situation, on dressera un graphe que l'on complètera au fur et à mesure des questions.
2. Déterminer $\quad \mathbb{P}_{X_j=i}(X_{j+1}=i) \quad$ pour tout $j \in [\![\,0\,;n-1\,]\!]$ et tout $i \in [\![\,1\,;2\,]\!]$.
3. Déterminer $\mathbb{P}_{X_j=0}(X_{j+1}=2)$ et $\mathbb{P}_{X_j=2}(X_{j+1}=0)$ pour tout $j \in [\![\,0\,;n-1\,]\!]$.
4. En déduire $\mathbb{P}_{X_j=0}(X_{j+1}=1)$ et $\mathbb{P}_{X_j=2}(X_{j+1}=1)$ pour tout $j \in [\![\,0\,;n-1\,]\!]$.
5. Déterminer $\mathbb{P}_{X_j=1}(X_{j+1}=0)$ et $\mathbb{P}_{X_j=1}(X_{j+1}=2)$ pour tout $j \in [\![\,0\,;n-1\,]\!]$ puis en déduire la matrice de transition M associée à cette chaîne de Markov.
6. Montrer que pour tout $j\in\mathbb{N}$, $\quad M^j = \begin{pmatrix} 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \end{pmatrix}$ si j est pair $\quad$ et
   $M^j = M$ si j est impair.
7. Déterminer la distribution de probabilité initiale de cette chaîne de Markov et en déduire la distribution de probabilité π_j à la j^{e} étape pour tout $j \in [\![\,0\,;n\,]\!]$.
8. En déduire, pour tout $j \in [\![\,0\,;n\,]\!]$, le nombre moyen de boules dans l'urne A à la j^{e} étape.

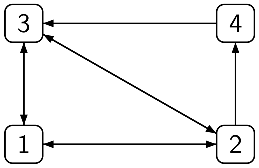
Exercice 15 Algorithme PageRank

Le PageRank est un algorithme d'analyse des liens hypertextes qui est utilisé par les moteurs de recherche pour le classement des pages web par ordre de pertinence et qui met en œuvre une méthode probabiliste.

Prenons un internaute lambda naviguant sur internet. Lorsqu'il est sur une page donnée, soit, avec une probabilité p, il choisit une page au hasard sur l'ensemble du réseau y compris celle sur laquelle il se trouve, soit, avec une probabilité $1-p$, il clique au hasard sur un des liens disponibles depuis la page sur laquelle il se trouve.

On considère le graphe suivant représentant les liens hypertextes entre les pages d'un mini-web à quatre pages.

EXERCICES



On note X_n la page sur laquelle se trouve l'internaute au bout de n étapes : $X_n \in \{1; 2; 3; 4\}$, et π_n la distribution de X_n à l'étape n :
$\pi_n = \big(\mathbb{P}(X_n = 1) \quad \mathbb{P}(X_n = 2) \quad \mathbb{P}(X_n = 3) \quad \mathbb{P}(X_n = 4)\big)$.

1. (a) Montrer, par disjonction des cas, que pour tout entier n,
$$\mathbb{P}(X_{n+1} = 1) = (1-p)\left(\tfrac{1}{3}\mathbb{P}(X_n = 2) + \tfrac{1}{2}\mathbb{P}(X_n = 3)\right) + \tfrac{p}{4}.$$
   (b) Exprimer de même $\mathbb{P}(X_{n+1} = 2)$, $\mathbb{P}(X_{n+1} = 3)$ et $\mathbb{P}(X_{n+1} = 4)$.
2. Déterminer alors deux matrices A et B telles que, pour tout entier n,
$\pi_{n+1} = (1-p)\pi_n A + \frac{p}{4}B$.
3. On pose $A' = (1-p)A$ et $B' = pB$ et l'on suppose qu'il existe une distribution invariante π.
Justifier que l'on a $\pi = B'(I_4 - A')^{-1}$ sous réserve d'existence.
4. (a) On pose $V_n = \pi_n - \pi$. Vérifier que $V_{n+1} = (1-p)V_n A$ et en déduire que $V_n = (1-p)^n V_0 A^n$.
   (b) On suppose que la suite de matrices (A^n) converge vers une matrice L. Quelle est alors la limite de la suite (π_n) ?
5. (a) À l'aide de la calculatrice, émettre une conjecture sur A^n, conjecture que l'on supposera vraie.
   (b) On suppose que $p = \frac{1}{4}$. Calculer la matrice π à l'aide de la calculatrice puis classer les pages par fréquence décroissante.

Hasardez-vous à présent en page 327 afin de réaliser le devoir n° 15.

Corrigé des exercices

SUITES & MATRICES

Exercice 1 Suite de Fibonacci $\begin{cases} u_0 = u_1 = 1, \\ u_{n+2} = u_{n+1} + u_n. \end{cases}$

1. On a $u_0 = u_1 = 1$, $u_2 = u_1 + u_0 = 2$ et $u_3 = u_2 + u_1 = 3$ donc $U_0 = \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $U_1 = \begin{pmatrix} u_2 \\ u_1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ et $U_2 = \begin{pmatrix} u_3 \\ u_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$.
2. On a $U_{n+1} = \begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} + u_n \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = AU_n$.
3. Ainsi, pour tout $n \in \mathbb{N}$ et par récurrence triviale ($AA^n = A^{n+1}$), on a $U_n = A^n U_0$.
4. D'où $\begin{pmatrix} u_{21} \\ u_{20} \end{pmatrix} = U_{20} = A^{20} U_0 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{20} \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = \begin{pmatrix} 10946 & 6765 \\ 6765 & 4181 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
   $\begin{pmatrix} u_{21} \\ u_{20} \end{pmatrix} = \begin{pmatrix} 17711 \\ 10946 \end{pmatrix}$: $u_{20} = 10\,946$ et $u_{21} = 17\,711$.

Exercice 2 $A = \begin{pmatrix} 0,2 & 0,1 \\ 0 & 0,1 \end{pmatrix}$, $B = \begin{pmatrix} 0,4 \\ 0,4 \end{pmatrix}$ et $U_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $U_{n+1} = AU_n + B$.

1. On cherche $U = \begin{pmatrix} a \\ b \end{pmatrix}$ telle que $U = AU + B$. On a $U = AU + B$
   $\iff \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0,2 & 0,1 \\ 0 & 0,1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 0,4 \\ 0,4 \end{pmatrix} \iff \begin{cases} a & = & 0,2a + 0,1b + 0,4 \\ b & = & 0a + 0,1b + 0,4 \end{cases}$
   $\iff \begin{cases} 0,9b & = & 0,4 \\ 0,8a & = & 0,1b + 0,4 \end{cases} \iff \begin{cases} b & = & \frac{4}{9} \\ a & = & \frac{0,1 \times \frac{4}{9} + 0,4}{0,8} = \frac{5}{9} \end{cases}$
   $\iff U = \frac{1}{9} \begin{pmatrix} 5 \\ 4 \end{pmatrix}. = \begin{pmatrix} 5/9 \\ 4/9 \end{pmatrix}$, unique état stable de (U_n).
2. $V_{n+1} = U_{n+1} - U = (AU_n + B) - (AU + B) = AU_n - AU = A(U_n - U) = AV_n$.
3. Ainsi, $V_n = A^n V_0 = A^n (U_0 - U) = A^n \begin{pmatrix} 4/9 \\ -4/9 \end{pmatrix} = \frac{4}{9} A^n \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
   et $U_n = V_n + U = \frac{4}{9} A^n \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \frac{1}{9} \begin{pmatrix} 5 \\ 4 \end{pmatrix}$.
4. On a $\det(P) = 1/\sqrt{2} \neq 0$ donc P est inversible et $P^{-1} = \frac{1}{1/\sqrt{2}} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix}$
   d'où $PDP^{-1} = \begin{pmatrix} 1 & -1/\sqrt{2} \\ 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 0,2 & 0 \\ 0 & 0,1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} 0,2 & 0,1 \\ 0 & 0,1 \end{pmatrix} = A$.
5. On a alors $A^n = (PDP^{-1})^n = PD^nP^{-1}$ et puisque les coefficients diagonaux de D sont tous dans $]-1\,;1[$, D^n et donc A^n convergent vers la matrice nulle O_2. Ainsi, la suite de matrices (U_n) converge vers la matrice
   $\frac{4}{9} O_2^n \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \frac{1}{9} \begin{pmatrix} 5 \\ 4 \end{pmatrix} = \frac{1}{9} \begin{pmatrix} 5 \\ 4 \end{pmatrix} = U$, son état stable.

Exercice 3 $U_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $A = \begin{pmatrix} 1/2 & 0 \\ -1/2 & 1/2 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $U_{n+1} = AU_n + B$.

Cherchons un éventuel état stable $L = \begin{pmatrix} a \\ b \end{pmatrix}$.

On a $L = AL + B \iff \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ -1/2 & 1/2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$$\iff \begin{cases} a = \frac{1}{2}a + 1 \\ b = -\frac{1}{2}a + \frac{1}{2}b + 1 \end{cases} \iff \begin{cases} a = 2 \\ \frac{1}{2}b = -\frac{1}{2} \times 2 + 1 = 0 \end{cases} \iff L = \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Si l'on pose $V_n = U_n - L$, on a

$V_{n+1} = U_{n+1} - L = (AU_n + B) - (AL + B) = A(U_n - L) = AV_n$ donc $V_n = A^n V_0$

et $U_n = V_n + L = A^n V_0 + L = A^n (U_0 - L) + L = A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix}$.

À l'aide de la calculatrice, on conjecture que $A^n = \frac{1}{2^n} \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$ et, par récurrence,

on a bien $A^{n+1} = A^n A = \frac{1}{2^n} \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix} = \frac{1}{2^{n+1}} \begin{pmatrix} 1 & 0 \\ -n-1 & 1 \end{pmatrix}$

$A^{n+1} = \frac{1}{2^{n+1}} \begin{pmatrix} 1 & 0 \\ -(n+1) & 1 \end{pmatrix}$.

Puisque $\frac{n+1}{2^{n+1}} \xrightarrow[n \to \infty]{} 0$ par croissances comparées, la suite de matrices A^n converge vers O_2 et la suite de matrices (U_n) converge vers $O_2^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = L$.

Exercice 4

1. D'après l'énoncé, on a $\begin{cases} a_{n+1} = \frac{1}{2}a_n + \frac{3}{4}b_n + 2 \\ b_{n+1} = \frac{1}{4}b_n + 3 \end{cases} \iff \begin{cases} a_{n+1} = 0,5a_n + 0,75b_n + 2 \\ b_{n+1} = 0,25b_n + 3. \end{cases}$

   Ce système s'écrit $U_{n+1} = MU_n + C$ où $M = \begin{pmatrix} 0,5 & 0,75 \\ 0 & 0,25 \end{pmatrix}$ et $C = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

2. (a) On a $P^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ donc P est inversible et $P^{-1} = P$.

   (b) On a $PMP = \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0,5 & 0,75 \\ 0 & 0,25 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$

   $PMP = \begin{pmatrix} 0,5 & 1,5 \\ 0 & -0,25 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0,5 & 0 \\ 0 & 0,25 \end{pmatrix}$.

   Donc $PMP = D$ avec la matrice diagonale $D = \begin{pmatrix} 0,5 & 0 \\ 0 & 0,25 \end{pmatrix}$.

   (c) On a $P^{-1} = P$ et $PMP = D$
   donc $PDP = P(PMP)P = P^{-1}PMPP^{-1} = M$.

   (d) Pour tout entier naturel n, posons $\mathscr{P}_n$: « $M^n = PD^nP$ ».
   • Initialisation : $M^0 = I_2$ et $PD^0P = PI_2P = P^2 = P$ d'après 2(a).
   • Hérédité : Soit n un entier naturel tel que $\mathscr{P}_n$: $M^n = PD^nP$ soit vraie.
   $M^{n+1} = PD^nP \times M$ d'après l'hypothèse de récurrence
   $= PD^nP \times PDP$ d'après la question précédente
   $= PD^nI_2DP$ d'après la question 2(a).

$M^{n+1} = PD^{n+1}P$ et $\mathscr{P}_{n+1}$ est vraie.
• Conclusion : $\forall n \in \mathbb{N}, \quad M^n = PD^nP.$

3. On a $\quad MX + C = \begin{pmatrix} 0,5 & 0,75 \\ 0 & 0,25 \end{pmatrix} \times \begin{pmatrix} 10 \\ 4 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 8 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 10 \\ 4 \end{pmatrix} = X.$

4. (a) $\forall n \in \mathbb{N}$, on a $\quad V_{n+1} = U_{n+1} - X = MU_n + C - X = MU_n - MX$
$V_{n+1} = M(U_n - X) = MV_n.$

(b) On a $\quad V_0 = U_0 - X = \begin{pmatrix} -9 \\ -3 \end{pmatrix}$ et puisque $\quad V_n = U_n - X,$ pour tout $n \in \mathbb{N}$, $\begin{pmatrix} a_n \\ b_n \end{pmatrix} = U_n = V_n + X = M^nV_0 + X$

$$U_n = \begin{pmatrix} 0,5^n & 3.0,5^n - 3.0,25^n \\ 0 & 0,25^n \end{pmatrix} \begin{pmatrix} -9 \\ -3 \end{pmatrix} + \begin{pmatrix} 10 \\ 4 \end{pmatrix}$$
$$= \begin{pmatrix} -18 \times 0,5^n + 9 \times 0,25^n + 10 \\ -3 \times 0,25^n + 4 \end{pmatrix}.$$

5. (a) $\forall n \in \mathbb{N}$, on a $\quad b_n = -3 \times 0,25^n + 4 \quad$ donc
$$b_{n+1} - b_n = -3 \times 0,25^{n+1} + 3 \times 0,25^n = 3 \times 0,25^n(1 - 0,25)$$
$$= 9 \times 0,25^{n+1} > 0 \text{ et } (b_n) \text{ est croissante.}$$
De plus, $\forall n \in \mathbb{N}, \quad b_n = 4 - 3 \times 0,25^n < 4 \quad$ donc (b_n) est majorée par 4. Ainsi, le théorème de convergence monotone permet d'affirmer que (b_n) est convergente. Puisque $\quad |0,25| < 1, \quad \lim\limits_{n\to\infty} 0,25^n = 0 \quad$ et par opération sur les limites, $\quad \lim\limits_{n\to\infty} b_n = 4.$

(b) Puisque $\quad |0,25| < |0,5| < 1, \quad \lim\limits_{n\to\infty} 0,25^n = \lim\limits_{n\to\infty} 0,5^n = 0 \quad$ et par opération sur les limites, $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} -18 \times 0,5^n + 9 \times 0,25^n + 10 = 10.$

(c) On a $\quad \lim\limits_{n\to\infty} a_n = 10 \quad$ et (a_n) est croissante donc (a_n) est majorée par 10. On sait d'autre part que (b_n) est majorée par 4. Il suffit donc de prévoir une contenance de 1 000 litres pour le bassin A et de 400 litres pour le bassin B.

Exercice 5 Suites complexes et matrices

$$z_0 = 1, \quad z'_0 = i \quad \text{et} \quad \begin{cases} z_{n+1} &= (9-4i)z_n + (-3+2i)z'_n \\ z'_{n+1} &= (18-12i)z_n + (-6+6i)z'_n. \end{cases}$$

1. On a $\quad z_1 = (9-4i) + (-3+2i)i = 7 - 7i$
et $\quad z'_1 = (18 - 12i) + (-6+6i)i = 12 - 18i.$

2. En posant, pour tout $n \in \mathbb{N}, \quad Z_n = \begin{pmatrix} z_n \\ z'_n \end{pmatrix} \quad$ et $\quad A = \begin{pmatrix} 9-4i & -3+2i \\ 18-12i & -6+6i \end{pmatrix},$
ce système s'écrit sous la forme $\quad Z_{n+1} = A \times Z_n.$

3. Pour tout $n \in \mathbb{N}$, posons $\quad \mathscr{P}_n$: « $Z_n = A^n \times Z_0$ ».
• Initialisation : pour $n = 0$, on a bien $\quad A^0 \times Z_0 = I_2 \times Z_0 = Z_0 \quad$ donc $\mathscr{P}_0$ est vraie.
• Hérédité : Supposons qu'il existe $k \in \mathbb{N}$ tel que $\mathscr{P}_k$ est vraie. Montrons que $\mathscr{P}_{k+1}$ est aussi vraie.
On a $\quad Z_{k+1} = A \times Z_k = A \times A^kZ_0 = A^{k+1}Z_0, \quad$ par hypothèse de récurrence, d'où $\quad \mathscr{P}_{k+1}$ est vraie.
• Conclusion : pour tout $n \in \mathbb{N}, \quad \mathscr{P}_n$: $Z_n = A^n \times Z_0$ est vraie.

CORRIGÉS

4. (a) On a $\det(P) = 1 \times 4 - 3 \times 2 = -2 \neq 0$ donc P est inversible, et $P^{-1} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$.

(b) On a $PDP^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2i & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix} = \begin{pmatrix} 2i & 6 \\ 6i & 12 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$

$$PDP^{-1} = \begin{pmatrix} 9-4i & -3+2i \\ 18-12i & -6+6i \end{pmatrix} = A.$$

(c) Pour tout $n \in \mathbb{N}$, posons $\mathscr{Q}_n$: « $A^n = PD^nP^{-1}$ ».

· Initialisation : pour $n = 0$, $PD^0P^{-1} = PP^{-1} = I_2 = A^0$ donc $\mathscr{Q}_0$ est vraie.

· Hérédité : Supposons qu'il existe $k \in \mathbb{N}$ tel que $\mathscr{Q}_k$ est vraie.
Montrons que $\mathscr{Q}_{k+1}$ est aussi vraie.
On a $A^{k+1} = A \times A^k = PDP^{-1} \times PD^kP^{-1} = PDD^kP^{-1} = PD^{k+1}P^{-1}$ et $\mathscr{Q}_{k+1}$ est vraie.

· Conclusion : pour tout $n \in \mathbb{N}$, $\mathscr{Q}_n$: $A^n = PD^nP^{-1}$ est vraie.

(d) Pour tout $n \in \mathbb{N}$, posons $\mathcal{R}_n$: « $D^n = \begin{pmatrix} (2i)^n & 0 \\ 0 & 3^n \end{pmatrix}$ ».

· Initialisation : pour $n = 0$, on a $\begin{pmatrix} (2i)^0 & 0 \\ 0 & 3^0 \end{pmatrix} = I_2 = D^0$ donc $\mathcal{R}_0$ est vraie.

· Hérédité : Supposons qu'il existe $k \in \mathbb{N}$ tel que $\mathcal{R}_k$ est vraie.
Montrons que $\mathcal{R}_{k+1}$ est aussi vraie.
On a $D^{k+1} = D \times D^k = \begin{pmatrix} 2i & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} (2i)^k & 0 \\ 0 & 3^k \end{pmatrix} = \begin{pmatrix} (2i)^{k+1} & 0 \\ 0 & 3^{k+1} \end{pmatrix}$ et $\mathcal{R}_{k+1}$ est vraie.

· Conclusion : pour tout $n \in \mathbb{N}$, $\mathcal{R}_n$: $D^n = \begin{pmatrix} (2i)^n & 0 \\ 0 & 3^n \end{pmatrix}$ est vraie.

On en déduit que, pour tout $n \in \mathbb{N}$,

$$A^n = PD^nP^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} (2i)^n & 0 \\ 0 & 3^n \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$$

$$A^n = \begin{pmatrix} -2(2i^n) + 3^{n+1} & (2i)^n - 3^n \\ -6(2i)^n + 2 \times 3^{n+1} & 3(2i)^n - 2 \times 3^n \end{pmatrix}.$$

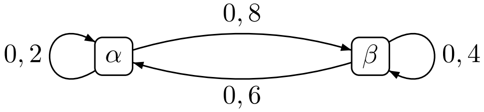
5. Ainsi, pour tout $n \in \mathbb{N}$, $\begin{pmatrix} z_n \\ z'_n \end{pmatrix} = Z_n = A^n Z_0$

$$\begin{pmatrix} z_n \\ z'_n \end{pmatrix} = \begin{pmatrix} -2(2i)^n + 3^{n+1} & (2i)^n - 3^n \\ -6(2i)^n + 2 \times 3^{n+1} & 3(2i)^n - 2 \times 3^n \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

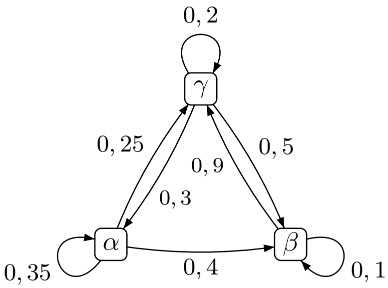
$$= \begin{pmatrix} (-2+i)(2i)^n + 3^n(3-i) \\ (-6+3i)(2i)^n + 3^n(6-2i) \end{pmatrix}.$$

Exercice 6 Les matrices de transition sont stochastiques : leurs coefficients doivent être positifs et leur somme lignes par lignes doit être égale 1.

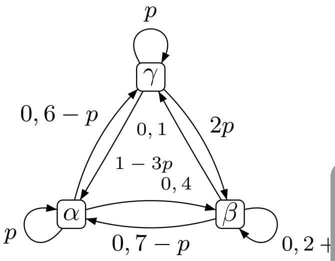
$A = \begin{pmatrix} 0,2 & 0,8 \\ 0,6 & 0,4 \end{pmatrix}$ de graphe probabiliste



$$B = \begin{pmatrix} 0,35 & 0,4 & 0,25 \\ 0 & 0,1 & 0,9 \\ 0,3 & 0,5 & 0,2 \end{pmatrix}$$ de graphe probabiliste

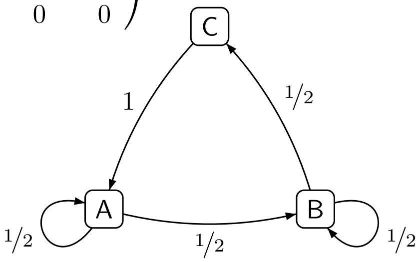


$$C = \begin{pmatrix} p & 0,4 & 0,6-p \\ 0,7-p & 0,2+p & 0,1 \\ 1-3p & 2p & p \end{pmatrix}$$ de graphe probabiliste



Exercice 7

1. La matrice $P = \begin{pmatrix} 0,5 & 0,5 & 0 \\ 0 & 0,5 & 0,5 \\ 1 & 0 & 0 \end{pmatrix}$ est associée au graphe pondéré suivant.



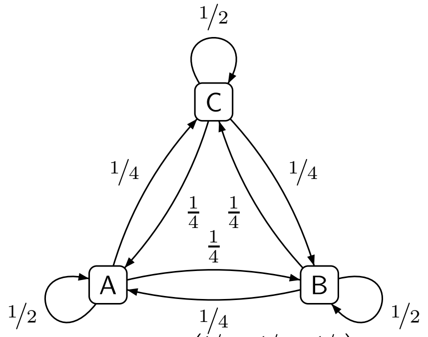
2. On a $\pi_3 = \pi_0 P^3 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} . \frac{1}{8} \begin{pmatrix} 3 & 3 & 2 \\ 4 & 3 & 1 \\ 2 & 4 & 2 \end{pmatrix} = \begin{pmatrix} \frac{3}{8} & \frac{3}{8} & \frac{1}{4} \end{pmatrix}$.

3. À l'aide la calculatrice, il semble que la suite de matrices (P^n) converge vers $\Pi = \begin{pmatrix} 0,4 & 0,4 & 0,2 \\ 0,4 & 0,4 & 0,2 \\ 0,4 & 0,4 & 0,2 \end{pmatrix}$ et donc la suite (π_n) devrait converger vers $\pi = \pi_0 \Pi = \begin{pmatrix} 0,4 & 0,4 & 0,2 \end{pmatrix}$ qui est bien une distribution invariante de cette chaîne puisque il est clair que $\pi P = \pi$.

4. Puisqu'il existe un entier $n = 3$ tel que P^n ne contienne pas de 0, la distribution invariante π précédente est unique et la suite des distributions π_n converge bien vers π.

Exercice 8

1. D'après l'énoncé, le déplacement du mobile peut être représenté par le graphe pondéré suivant.



Sa matrice de transition est alors $P = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}$.

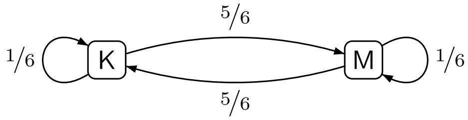
2. On a $P^3 = \dfrac{1}{64}\begin{pmatrix} 22 & 21 & 21 \\ 21 & 22 & 21 \\ 21 & 21 & 22 \end{pmatrix}$ donc la probabilité que le mobile soit sur le sommet A trois secondes après avoir été sur le sommet C est de $\mathbb{P}_{(C_k)}(A_{k+3}) = \frac{21}{64}$.
3. Le mobile est au sommet A au début de l'expérience dont la distribution initiale est $\pi_0 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$. La distribution après dix secondes est alors $\pi_{10} = \pi_0 P^{10}$ et la calculatrice donne comme première composante $\mathbb{P}(A_{10}) = \frac{174763}{524288}$.
Le mobile a donc une probabilité très proche d'un tiers d'être sur le sommet A dix secondes après le début de l'expérience.
4. Puisque $P^1 = P$ ne contient pas de 0, il existe une unique distribution invariante π qui est la limite des distributions (π_n) pour toute distribution initiale π_0.
Cherchons $(\,a\,,\,b\,)\,c \in [\,0\,;1\,]^3$ tels que $a+b+c=1$ et $\pi = \begin{pmatrix} a & b & c \end{pmatrix}$ soit invariante. On a $\pi = \pi P \iff \begin{pmatrix} a & b & c \end{pmatrix} = \begin{pmatrix} a & b & c \end{pmatrix}\begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}$

$$\iff \begin{cases} a+b+c=1 \\ a = \frac{1}{2}a + \frac{1}{4}b + \frac{1}{4}c \\ b = \frac{1}{4}a + \frac{1}{2}b + \frac{1}{4}c \\ c = \frac{1}{4}a + \frac{1}{4}b + \frac{1}{2}c. \end{cases}$$ (L2)-(L3)-(L4) donne $a = \frac{1}{2}b + \frac{1}{2}c$ d'où

(L3) : $b(1 - \frac{1}{2} - \frac{1}{8}) = \frac{1}{4}c + \frac{1}{8}c$ et $b = c$.
Ainsi, $a = \frac{1}{2}b + \frac{1}{2}b = b = c$ et la condition de distribution donne $3a = 1$.
On a donc $\pi = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$, qui est bien une distribution invariante et donc la limite de la suite des distributions (π_n).

Exercice 9 Kiwi ou mandarine ?

La situation peut être modélisée par le graphe probabiliste suivant.



La matrice de transition est alors $F = \begin{pmatrix} 1/6 & 5/6 \\ 5/6 & 1/6 \end{pmatrix}$.

La distribution initiale étant $\pi_0 = \begin{pmatrix} 1 & 0 \end{pmatrix}$, celle après 7 jours jours est

$$\pi_7 = \pi_0 F^7 = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \tfrac{1}{4379} \begin{pmatrix} 2059 & 2315 \\ 2315 & 2059 \end{pmatrix} = \tfrac{1}{4379} \begin{pmatrix} 2059 & 2315 \end{pmatrix}.$$

La probabilité que M.Fartezdekrié prenne un kiwi sept jours après en avoir mangé un est donc de $\frac{2059}{4379} \simeq 0,47$.

Il semble que la suite de matrices (F^n) converge vers $\Pi = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ donc la suite des distributions devraient converger vers $\pi = \pi_0 \Pi = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix}$, distribution effectivement invariante de cette chaîne de Markov.

Puisque F^1 ne contient aucun 0, la distribution invariante $\pi = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ est unique et toute suite de distribution converge vers celle-ci. M.Fartezdekrié aurait donc quasiment autant de chances de déguster un kiwi ou une mandarine un matin donné de l'an prochain.

Exercice 10 Cherchons une distribution invariante $\pi = \begin{pmatrix} a & b \end{pmatrix}$.

On a $\pi P = \pi \iff \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \iff \begin{pmatrix} b & a \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \iff a = b$.

De plus, π étant une distribution, on doit avoir $a + b = 1$.

La seule distribution invariante est donc $\pi = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

On a $P^2 = I_2$ donc, pour tout entier naturel n, $P^{2k} = I_2$ et $P^{2k+1} = P$.

Ainsi, pour toute distribution initiale $\pi_0 = \begin{pmatrix} \alpha & \beta \end{pmatrix}$, la suite des distributions $\pi_n = \pi_0 P^n$ vérifie $\pi_{2k} = \pi_0 I_2 = \begin{pmatrix} \alpha & \beta \end{pmatrix}$ et $\pi_{2k+1} = \pi_0 P = \begin{pmatrix} \beta & \alpha \end{pmatrix}$. Elle ne peut donc converger que si $\alpha = \beta = \frac{1}{2}$ et donc si $\pi_0 = \pi$, seule distribution invariante.

Exercice 11

1. La fonction $p \longmapsto (2-p)p$ est un polynôme du second degré. Elle admet donc un extremum en 1, la moyenne entre ses deux racines 0 et 2. Elle est donc monotone sur $[\,0\,;1\,]$ et ses bornes sont atteintes en 0 et en 1 et valent 0 et 1. Ainsi, pour tout $p \in [\,0\,;1\,]$, $0 \leqslant (2-p)p \leqslant 1$.
2. D'après le graphe, $\mathbb{P}_A(A) = 1 - \mathbb{P}_A(B) = 1 - (2-p)p = p^2 - 2p + 1 = (p-1)^2$ et $\mathbb{P}_B(B) = 1 - \mathbb{P}_B(A) = 1 - p$ d'où $(\mathbb{P}_B(B))^2 = (1-p)^2 = \mathbb{P}_A(A)$.
3. (a) La matrice de transition de ce graphe est donc $G = \begin{pmatrix} (1-p)^2 & (2-p)p \\ p & 1-p \end{pmatrix}$ et la distribution après une transition est

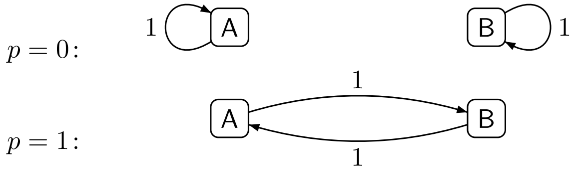
$$\begin{aligned} \pi_1 = \pi_0 G &= \begin{pmatrix} 0,3 & 0,7 \end{pmatrix} \begin{pmatrix} (1-p)^2 & (2-p)p \\ p & 1-p \end{pmatrix} \\ &= \begin{pmatrix} 0,3(1-p)^2 + 0,7p & 0,3(2-p)p + 0,7(1-p) \end{pmatrix} \\ &= \begin{pmatrix} 0,3 + 0,1p + 0,3p^2 & 0,7 - 0,1p - 0,3p^2 \end{pmatrix}. \end{aligned}$$

   Puisque $p \in [\,0\,;1\,]$, la deuxième composante $0,7 - 0,1p - 0,3p^2$ est trivialement minimale pour $p = 1$ et vaut $0,7 - 0,1 - 0,3 = 0,3$ et elle est maximale pour $p = 0$ et elle vaut $0,7 - 0 = 0,7$.

   (b) La première composante vaut alors au maximum $0,7$ en $p = 1$ et $0,3$ en $p = 0$.

CORRIGÉS

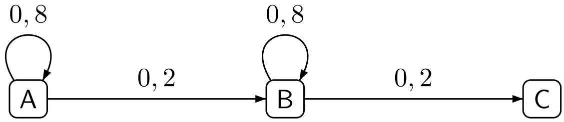
(c) Ces situations correspondent aux graphes anecdotiques suivants :



Exercice 12 Si l'on note P la matrice de transition de la chaîne de Markov X_n, alors P^2 est la matrice de transition de la chaîne de Markov Z_n. En effet, si $\widetilde{\pi}_n$ est la distribution de (Z_n), on a $\widetilde{\pi}_n = \pi_{2n} = \pi_0 P^{2n} = \pi_0 (P^2)^n$. D'où, si π est une distribution invariante de X_n, on a $\pi P = \pi$ et donc $\pi P^2 = (\pi P)P = \pi P = \pi$: π est invariante pour P^2 donc π est une distribution invariante de Z_n.

Exercice 13

1. La situation peut être modélisée par le graphe probabiliste suivant.



2. On obtient, par ordre alphabétique des sommets, la matrice de transition $P = \begin{pmatrix} 0,8 & 0,2 & 0 \\ 0 & 0,8 & 0,2 \\ 0 & 0 & 1 \end{pmatrix}$.
   Au début, le client est en A donc $a_0 = 1$. L'état initial est donc $\pi_0 = (1 \quad 0 \quad 0)$.
   De manière évidente, on a $(0 \quad 0 \quad 1) \times \begin{pmatrix} 0,8 & 0,2 & 0 \\ 0 & 0,8 & 0,2 \\ 0 & 0 & 1 \end{pmatrix} = (0 \quad 0 \quad 1)$ donc $\pi = (0 \quad 0 \quad 1)$ est une distribution invariante : une fois en C, le client y reste.
3. L'attente minimale d'un client est égale à 2 minutes : cela arrive lorsque le client passe dès la première transition en B et dès la suivante en C.
4. On a $P = \begin{pmatrix} 0,8 & 0,2 & 0 \\ 0 & 0,8 & 0,2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0,8 & 0 & 0 \\ 0 & 0,8 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0,2 & 0 \\ 0 & 0 & 0,2 \\ 0 & 0 & 0 \end{pmatrix} = D + N$
   où $D = \begin{pmatrix} 0,8 & 0 & 0 \\ 0 & 0,8 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est diagonale et $N = \begin{pmatrix} 0 & 0,2 & 0 \\ 0 & 0 & 0,2 \\ 0 & 0 & 0 \end{pmatrix}$ est strictement triangulaire.
   On a $DN = \begin{pmatrix} 0,8 & 0 & 0 \\ 0 & 0,8 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0,2 & 0 \\ 0 & 0 & 0,2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0,16 & 0 \\ 0 & 0 & 0,16 \\ 0 & 0 & 0 \end{pmatrix}$
   et $ND = \begin{pmatrix} 0 & 0,2 & 0 \\ 0 & 0 & 0,2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0,8 & 0 & 0 \\ 0 & 0,8 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0,16 & 0 \\ 0 & 0 & 0,16 \\ 0 & 0 & 0 \end{pmatrix}$
   donc $DN + ND$.
5. D est une matrice diagonale donc, pour tout $k \in \mathbb{N}$, $D^k = \begin{pmatrix} 0,8^k & 0 & 0 \\ 0 & 0,8^k & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
   On a $N^2 = \begin{pmatrix} 0 & 0 & 0,04 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et $N^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ donc $N^k = O_3$ pour tout $k \geqslant 3$.
   On dit que la matrice N est nilpotente d'ordre 3.

6. Puisque $P = D + N$ et $DN = ND$, la formule du binôme de Newton pour les matrices commutantes s'applique et l'on a, pour tout $n \in \mathbb{N}$,
$$P^n = (D+N)^n = \sum_{k=0} n \binom{n}{k} N^k D^{n-k}.$$
Pour $n \geqslant 3$, $P^n = \binom{n}{0} N^0 D^n + \binom{n}{1} N^1 D^{n-1} + \binom{n}{2} N^2 D^{n-2} + O_3$
$$P^n = 1D^n + nND^{n-1} + \tfrac{n(n-1}{2} N^2 D^{n-2}$$
$$= \begin{pmatrix} 0,8^n & 0 & 0 \\ 0 & 0,8^n & 0 \\ 0 & 0 & 1 \end{pmatrix} + n \begin{pmatrix} 0 & 0,2 & 0 \\ 0 & 0 & 0,2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0,8^{n-1} & 0 & 0 \\ 0 & 0,8^{n-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$+ \tfrac{n(n-1)}{2} \begin{pmatrix} 0 & 0 & 0,04 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0,8^{n-2} & 0 & 0 \\ 0 & 0,8^{n-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$P^n = \begin{pmatrix} 0,8^n & 0,2 \times 0,8^{n-1} \times n & 1-(0,8+0,2n) \times 0,8^{n-1} \\ 0 & 0,8^n & 1-0,8^n \\ 0 & 0 & 1 \end{pmatrix}.$$

7. La distribution au bout de n minutes est donnée par $\pi_n = \pi_0 \times P^n$
$$\pi_n = (1 \quad 0 \quad 0) \begin{pmatrix} 0,8^n & 0,2 \times 0,8^{n-1} \times n & 1-(0,8+0,2n) \times 0,8^{n-1} \\ 0 & 0,8^n & 1-0,8^n \\ 0 & 0 & 1 \end{pmatrix}$$
$$\pi_n = (0,8^n \quad 0,2 \times 0,8^{n-1} \times n \quad 1-(0,8+0,2n) \times 0,8^{n-1}).$$
Puisque $|0,8| < 1$, $\lim\limits_{n \to \infty} 0,8^n = 0$ et, par croissances comparées, $\lim\limits_{n \to \infty} n0,8^{n-1} = 0$ La suite des distributions π_n converge donc vers la matrice $\pi = (0 \quad 0 \quad 1)$, distribution invariante obtenue précédemment.

8. Soit X la variable aléatoire correspondant au nombre de minutes d'attente. On a vu que $X \geqslant 2$.

   (a) Une attente de k minutes signifie qu'à $k-1$ minutes, le client était encore en B et qu'il arrive en C à la k^{e} minute. La probabilité de $X = k$ est donc égale à la différence $\mathbb{P}(C_k) - \mathbb{P}(C_{k-1}) = c_k - c_{k-1}$.

   (b) Puisque $X \in [\![2\,;+\infty]\!]$, on a
$$\mathbb{E}(X) = \lim_{m \to +\infty} \sum_{k=2}^{m} k\mathbb{P}(X=k) = \lim_{m \to +\infty} \sum_{k=2}^{m} k(c_k - c_{k-1}).$$

   (c) Pour tout $k \geqslant 1$, on a $c_k = 1-(0,8+0,2k) \times 0,8^{k-1}$ et
$$\begin{aligned} \mathbb{P}(X=k) &= c_k - c_{k-1} \\ &= (1-(0,8+0,2k) \times 0,8^{k-1}) \\ &\quad - ((1-(0,8+0,2(k-1)) \times 0,8^{k-2})) \\ &= (-0,64+0,6+0,04k)0,8^{k-2} = 0,04(k-1)0,8^{k-2}. \end{aligned}$$
D'où $\mathbb{E}(X) = \lim\limits_{m \to +\infty} \sum\limits_{k=2}^{m} k(0,04(k-1)0,8^{k-2})$
$$\mathbb{E}(X) = 0,04 \lim_{m \to +\infty} \sum_{k=2}^{m} k(k-1)0,8^{k-2}.$$

   (d) On sait que $f_m(x) = \frac{1-x^{m+1}}{1-x} = \sum\limits_{k=0}^{m} x^k$.

   Ainsi, $f'_m(x) = \sum\limits_{k=0}^{m} (x^k)' = \sum\limits_{k=0}^{m} kx^{k-1} = \sum\limits_{k=1}^{m} kx^{k-1}$

   et $f''_m(x) = \sum\limits_{k=1}^{m} (kx^{k-1})' = \sum\limits_{k=1}^{m} k(k-1)x^{k-2} = \sum\limits_{k=2}^{m} k(k-1)x^{k-2}$.

CORRIGÉS

(e) Par ailleurs, $f_m'(x) = \left(\frac{1-x^{m+1}}{1-x}\right)' = \frac{(1-x^{m+1})'(1-x)-(1-x)'(1-x^{m+1})}{(1-x)^2}$

$$f_m'(x) = \frac{-(m+1)x^m(1-x)+(1-x^{m+1})}{(1-x)^2} = \frac{mx^{m+1}-(m+1)x^m+1}{(1-x)^2} \quad \text{et}$$

$$f_m''(x) = \left(\frac{mx^{m+1}-(m+1)x^m+1}{(1-x)^2}\right)'$$

$$= \frac{(mx^{m+1}-(m+1)x^m+1)'(1-x)^2-(mx^{m+1}-(m+1)x^m+1)[(1-x)^2]'}{[(1-x)^2]^2}$$

$$= \frac{(m(m+1)x^m-m(m+1)x^{m-1})(1-x)^2-(mx^{m+1}-(m+1)x^m+1)(-2)(1-x)}{(1-x)^4}$$

$$f_m''(x) = \frac{-m(m+1)x^{m+1}+2(m-1)(m+1)x^m-m(m+1)x^{m-1}+2}{(1-x)^3}.$$

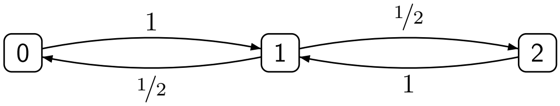
On a donc $\mathbb{E}(X) = 0,04 \lim\limits_{m\to+\infty} \sum\limits_{k=2}^{m} k(k-1)0,8^{k-2}$

$$\mathbb{E}(X) = 0,04 \lim_{m\to+\infty} f_m''(0,8) = 0,04 \times \frac{0+0+0+2}{(1-0,8)^3} = 10.$$

Le temps d'attente moyen est égal à 10 minutes.

Exercice 14 Les urnes d'Ehrenfest

1. Puisqu'il y a deux boules, l'urne A peut en contenir 0, 1 ou 2 et $X_j \in \{0;1;2\}$. Le graphe probabiliste complet associé suit.
2. Pour tout $i \in \{0;1;2\}$, on a $\mathbb{P}_{X_j=i}(X_{j+1}=i)=0$ car le nombre de boules dans l'urne A change à chaque étape : une boule change nécessairement d'urne et donc rentre dans A ou sort de A.
3. On a, pour tout $j \in [\![\, 0\,;n-1\,]\!]$, $\mathbb{P}_{X_j=0}(X_{j+1}=2)=0$ et $\mathbb{P}_{X_j=2}(X_{j+1}=0)=0$ car une seule boule, et non deux, change d'urne à chaque étape.
4. On a $\mathbb{P}_{X_j=0}(X_{j+1}=1) = 1-\mathbb{P}_{X_j=0}(X_{j+1}=0)-\mathbb{P}_{X_j=0}(X_{j+1}=2)$
   $\mathbb{P}_{X_j=0}(X_{j+1}=1)=1-0-0=1$ et
   $\mathbb{P}_{X_j=2}(X_{j+1}=1) = 1-\mathbb{P}_{X_j=2}(X_{j+1}=1)-\mathbb{P}_{X_j=2}(X_{j+1}=1) = 1-0-0=1.$
   En effet, si A ne contient pas de boule ou en contient deux, elle en contient nécessairement une seule à l'étape suivante.
5. Lorsque A contient une seule boule, il y a une chance sur deux que le numéro de celle-ci soit choisi, et autant qu'il ne le soit pas.
   On a donc $\mathbb{P}_{X_j=1}(X_{j+1}=0)=\mathbb{P}_{X_j=1}(X_{j+1}=2)=\frac{1}{2}$.
   La matrice de transition associée à cette chaîne de Markov, les sommets étant rangés dans l'ordre croissant du nombre de boules, est alors $M = \begin{pmatrix} 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \end{pmatrix}$ et le graphe probabiliste associé est le suivant.



6. On remarque que $M^2 = \begin{pmatrix} 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \end{pmatrix}$ et $M^3 = M$.

Donc $M^4 = M^3 M = M^2$ et une récurrence triviale montre que, pour tout $j \in \mathbb{N}$, $M^j = M^2 = \begin{pmatrix} 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \end{pmatrix}$ si j est pair et $M^j = M$ si j est impair.

7. Toutes les boules étant placées initialement dans l'urne A, on a $X_0 = 2$ et la distribution initiale est $\pi_0 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$.
   Si j est impair, la distribution au bout de j étapes est
   $$\pi_j = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} M^j = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}.$$
   Si j est pair, la distribution au bout de j étapes est
   $$\pi_j = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} M^j = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \\ 0,5 & 0 & 0,5 \end{pmatrix} = \begin{pmatrix} 0,5 & 0 & 0,5 \end{pmatrix}.$$

8. On a $\mathbb{E}(X_j) = \sum_{i=0}^{2} iP(X_j = i)$ donc $\mathbb{E}(X) = 0 \times 0 + 1 \times 1 + 0 \times 0 = 1$ si j est impair et $\mathbb{E}(X) = 0,5 \times 0 + 0 \times 1 + 0,5 \times 2 = 1$ si j est pair.
   Il y a donc en moyenne une boule dans l'urne A à la $j$ème étape.

Exercice 15 Algorithme PageRank

1. (a) Pour arriver sur la page 1 à l'étape $n+1$, c'est qu'à l'étape n,
   - soit il est sur la page 1 et il la choisit à nouveau parmi les quatre au choix lorsqu'il utilise cette méthode avec une probabilité p : $p \times \frac{1}{4}$.
   - soit il choisit avec une probabilité $1-p$ de changer de page et il est
     - soit sur la page 2 et choisit la page 1 avec une probabilité $\frac{1}{3}$: $(1-p)\frac{1}{3}\mathbb{P}(X_n = 2)$,
     - soit sur la page 3 et il choisit la page 1 avec une probabilité $\frac{1}{2}$: $(1-p)\frac{1}{2}\mathbb{P}(X_n = 3)$.

   Ainsi, pour tout entier n,
   $$\mathbb{P}(X_{n+1} = 1) = (1-p)\left(\tfrac{1}{3}\mathbb{P}(X_n = 2) + \tfrac{1}{2}\mathbb{P}(X_n = 3)\right) + \tfrac{p}{4}.$$

   (b) En procédant de même, on obtient
   $$\mathbb{P}(X_{n+1} = 2) = (1-p)\left(\tfrac{1}{2}\mathbb{P}(X_n = 1) + \tfrac{1}{2}\mathbb{P}(X_n = 3)\right) + \tfrac{p}{4},$$
   $$\mathbb{P}(X_{n+1} = 3) = (1-p)\left(\tfrac{1}{2}\mathbb{P}(X_n = 1) + \tfrac{1}{3}\mathbb{P}(X_n = 2) + \mathbb{P}(X_n = 4)\right) + \tfrac{p}{4},$$
   $$\mathbb{P}(X_{n+1} = 4) = (1-p)\left(\tfrac{1}{3}\mathbb{P}(X_n = 2)\right) + \tfrac{p}{4}.$$

2. Posons $A = \begin{pmatrix} 0 & 1/2 & 1/2 & 0 \\ 1/3 & 0 & 1/3 & 1/3 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$.

CORRIGÉS

On a alors, pour tout entier $n \in \mathbb{N}$, $\quad (1-p)\pi_n A + \frac{p}{4}B$

$$= (1-p)\begin{pmatrix}\mathbb{P}(X_n=1) & \mathbb{P}(X_n=2) & \mathbb{P}(X_n=3) & \mathbb{P}(X_n=4)\end{pmatrix}\begin{pmatrix} 0 & 1/2 & 1/2 & 0 \\ 1/3 & 0 & 1/3 & 1/3 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$+ \frac{p}{4}\begin{pmatrix}1 & 1 & 1 & 1\end{pmatrix}$$

$$(1-p)\pi_n A + \frac{p}{4}B = \begin{pmatrix}\mathbb{P}(X_n=1) & \mathbb{P}(X_n=2) & \mathbb{P}(X_n=3) & \mathbb{P}(X_n=4)\end{pmatrix} = \pi_{n+1}.$$

3. Si $I_4 - A'$ est inversible, alors π est invariante si, et seulement si,
$$\pi = \pi A' + B' \iff \pi - \pi A' = B' \iff \pi(I_4 - A') = B'$$
$$\iff \pi(I_4 - A')(I_4 - A')^{-1} = B'(I_4 - A')^{-1} \iff \pi = B'(I_4 - A')^{-1}.$$

4. (a) On a $\quad V_{n+1} = \pi_{n+1} - \pi = ((1-p)\pi_n A + \frac{p}{4}B) - ((1-p)\pi A + \frac{p}{4}B)$
$$V_{n+1} = ((1-p)\pi_n - (1-p)\pi)A = (1-p)(\pi_n - \pi)A = (1-p)V_n A.$$
Ainsi, par récurrence immédiate, $\quad (1-p)^0 V_0 A^0 = V_0$
et $\quad V_{n+1} = (1-p)V_n A = (1-p)[(1-p)^n V_0 A^n]A = (1-p)^{n+1}V_0 A^{n+1}$.

(b) Si $A^n \xrightarrow[n\to\infty]{} L$ alors les coefficients de A^n sont bornés, tout comme ceux de $V_0 A^n$. Puisque $\quad 0 \leqslant 1-p \leqslant 1, \quad (1-p)^n \xrightarrow[n\to\infty]{} 0 \quad$ et les coefficients de V_n tendent vers 0 : $\quad V_n \xrightarrow[n\to\infty]{} O_4 \quad$ et donc $\quad \pi_n = V_n + \pi$ converge vers π.

5. (a) La calculatrice montre que $\quad A^{99} \simeq L = \begin{pmatrix} 4/15 & 3/10 & 1/3 & 1/10 \\ 4/15 & 3/10 & 1/3 & 1/10 \\ 4/15 & 3/10 & 1/3 & 1/10 \end{pmatrix} \quad$ et l'on peut conjecturer que $\quad A^n \xrightarrow[n\to\infty]{} L, \quad$ ce que l'on admettra.
On a alors $\quad \pi_n \xrightarrow[n\to\infty]{} \pi$.

(b) On a $\quad A' = (1-p)A = \frac{3}{4}A = \begin{pmatrix} 0 & 3/8 & 3/8 & 0 \\ 1/4 & 0 & 1/4 & 1/4 \\ 3/8 & 3/8 & 0 & 0 \\ 0 & 0 & 3/4 & 0 \end{pmatrix}$,
$B' = pB = \frac{1}{4}\begin{pmatrix}1 & 1 & 1 & 1\end{pmatrix}$ donc, avec l'aide de la calculatrice, $\pi = B'(I_4 - A')^{-1} = \frac{1}{2068}\begin{pmatrix}530 & 583 & 680 & 275\end{pmatrix}$
et $\pi \simeq \begin{pmatrix}0,2563 & 0,2819 & 0,3288 & 0,1333\end{pmatrix}$ qui est bien une distribution (somme des coefficients égale 1). Peu importe la page sur laquelle se trouve l'internaute au départ c.-à-d. la distribution initiale, la suite π_n converge vers π. Le classement des pages par fréquence décroissante est donc 3, 2, 1, 4 ce qui semble cohérent avec le graphe mais on ne pouvait *a priori* pas trouver l'ordre entre les pages 1 et 2.

Devoirs corrigés

Devoir n° 1

Somme de deux carrés

Ce devoir est associé au chapitre I, *Nombres complexes : algèbre.*

Exercice

On dit que $n \in \mathbb{N}$ est somme de deux carrés s'il existe a et $b \in \mathbb{N}$ tels que $n = a^2 + b^2$.

1. Écrire un programme Python permettant de déterminer si un nombre est somme de deux carrés et en donner la décomposition le cas échéant.
2. Montrer que si deux entiers sont chacun somme de deux carrés alors leur produit l'est aussi.
3. En déduire que toute puissance entière d'une somme de deux carrés l'est aussi.

Bonus

Comme cadeau de rentrée, plutôt qu'une trousse azur, saumon ou citron, se faire offrir *Le Goût des Mathématiques*, ouvrage collectif de 128 toutes petites pages chez (Petit) Mercure de France. Tous y trouveront leur compte : vos parents puisque la somme dépensée est modique et vous puisque, même si l'on ne peut y mettre de crayons de couleur, c'est très divertissant.

Corrigé du devoir n^{o} 1

SOMME DE DEUX CARRÉS

On dit que $n \in \mathbb{N}$ est somme de deux carrés s'il existe a et $b \in \mathbb{N}$ tels que $n = a^2 + b^2$.

1. Le programme suivant permet de déterminer si un nombre est somme de deux carrés et en donner toutes les décompositions le cas échéant.

```
def SommeDeuxCarres(n) :
   T=0
   for a in range(n+1) :
      for b in range(n+1) :
         if a**2+b**2==n :
            print("Oui,", n,"=",x,"^2+",y,"^2")
            T=1
   if T==0 :
      print("Non,", n, "n'est pas somme de deux carrés")
```

2. Soient $m = a^2 + b^2$ et $n = c^2 + d^2$ où m, n, a, b, c, $d \in \mathbb{N}$.
   Posons $z_m = a + ib$ et $z_n = c + id$. On a $m = z_m\overline{z_m}$ et $n = z_n\overline{z_n}$ donc $mn = z_m\overline{z_m}z_n\overline{z_n} = z_m z_n\overline{z_m z_n} = (z_m z_n)\overline{(z_m z_n)} = \alpha^2 + \beta^2$ où $z_m z_n = \alpha + i\beta$.
   Comme $z_m z_n = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$, les nombres $\alpha = ac - bd$ et $\beta = ad + bc$ sont des entiers et mn est bien somme de deux carrés.

3. Soient k un entier naturel et n un entier non nul somme de deux carrés.
   Soit $\mathscr{P}_k$ la proposition « n^k est somme de deux carrés ».
   · Pour $k = 0$ $(n \neq 0)$, $n^0 = 1 = 1^2 + 0^2$ est somme de deux carrés.
   · Supposons que n^k est somme de deux carrés. On a $n^{k+1} = n.n^k$ produit de deux sommes de deux carrés par hypothèse de récurrence donc, d'après la question précédente, c'est aussi une somme de deux carrés et la proposition est héréditaire.
   · La proposition « n^k est somme de deux carrés » est donc vraie pour tout $k \in \mathbb{N}$.
   Le cas $n = 0$ n'a pas été traité mais est-ce vraiment utile ?

Devoir n^{o} 2

Base numb'

Ce devoir est associé au chapitre II, *Divisibilité dans* $\mathbb{Z}$.

La numération désigne le mode de représentation des nombres. Ces représentations ne sont pas toujours chiffrées ni même écrites. Un galet ou un bâton peut très bien représenter un animal du troupeau, une encoche sur une branche peut comptabiliser des événements... En revanche, dès que les nombres deviennent grands, il devient nécessaire de faire des regroupements par paquets homogènes, à partir d'un nombre précis, la base du système de numération. Les différents systèmes sont classés en trois groupes : les numérations additives (système romain), les numérations hybrides et les numérations de position comme dans les systèmes babylonien (base 60), chinois, maya (base 20), indo-arabes (base 10) ou en informatique (base 2 et 16).

Nous utilisons actuellement un système de numération de position décimal, en base 10 : les nombres sont découpés en paquets de puissances de 10. Par exemple, $2\,064 = 2.10^3 + 0.10^2 + 6.10^1 + 4.10^0$.
Dans un système de numération en base 2, le nombre vingt-et-un s'écrit $\overline{10101}^{2}$. En effet, $\quad 21 = 1.2^4 + 0.2^3 + 1.2^2 + 0.2^1 + 1.2^0$.
En base 3, ce même vingt-et-un s'écrit $\overline{210}^{3}$ car $\quad 21 = 2.3^2 + 1.3^1 + 0.3^0$.
Dans un système hexadécimal, en base 16, on a besoin de seize chiffres : on prend 0,..., 9 et A, B,..., F. Par exemple, $\quad \overline{13}^{10} = \overline{D}^{16}$, $\quad \overline{26}^{10} = \overline{1A}^{16}$ $(16 + 10)$ et $\quad \overline{206}^{10} = \overline{CE}^{16}$ $(12 \times 16 + 14)$.

1. Écriture en différentes bases.

(a) $\overline{87}^{10} = \overline{\qquad\qquad}^{3}$

(b) $\overline{341}^{10} = \overline{\qquad\qquad}^{3}$

(c) $\overline{255}^{10} = \overline{\qquad\qquad}^{2}$

(d) $\overline{3561}^{10} = \overline{\qquad\qquad}^{2}$

(e) $\overline{45255}^{10} = \overline{\qquad\qquad}^{16}$

(f) $\overline{100100101}^{2} = \overline{\qquad\qquad}^{10}$

(g) $\overline{22012}^{3} = \overline{\qquad\qquad}^{10}$

(h) $\overline{BAC21}^{16} = \overline{\qquad\qquad}^{10}$

(i) $\overline{10000}^{2} = \overline{\qquad\qquad}^{16}$

(j) $\overline{110110101}^{2} = \overline{\qquad\qquad}^{16}$

(k) $\overline{BAC21}^{16} = \overline{\qquad\qquad}^{2}$

(l) $\overline{111111}^{2} = \overline{2100}^{\cdots}$

(m) $\overline{657}^{10} = \overline{\qquad\qquad}^{5}$

(n) $\overline{12012}^{3} = \overline{\qquad\qquad}^{2}$

(o) $\overline{34102}^{5} = \overline{\qquad\qquad}^{10}$

(p) $\overline{24}^{10} = \overline{\qquad\qquad}^{12}$

(q) $\overline{111}^{60} = \overline{\qquad\qquad}^{10}$

(r) $\overline{20\,067}^{10} = \overline{\qquad\qquad}^{60}$

(s) $\overline{72}^{10} = \overline{\qquad\qquad}^{24}$

(t) $\overline{9999}^{10} = \overline{\qquad\qquad}^{11}$

(u) $\overline{263}^{7} = \overline{\qquad\qquad}^{10}$

(v) $\overline{1202}^{5} = \overline{342}^{\cdots}$

(w) $\overline{2}^{10} = \overline{\qquad\qquad}^{2}$

(x) $\overline{100}^{10} = \overline{\qquad\qquad}^{100}$

(y) $\overline{100}^{2} = \overline{\qquad\qquad}^{10}$

(z) $\overline{100}^{\cdots} = \overline{10000}^{\cdots}$

2. Vous avez donc remarqué que pour déterminer l'écriture en base b d'un nombre n, on effectue la division euclidienne de n par b, $\quad n = bq_0 + r_0, \quad$ puis celle du quotient $\quad q_0 = bq_1 + r_1, \quad$ et ainsi de suite. On construit ainsi deux suites d'entiers $(q_n)_{\mathbb{N}}$ et $(r_n)_{\mathbb{N}}$.
   (a) Montrer que la suite $(q_n)_{\mathbb{N}}$ est décroissante.
   (b) Montrer que la suite $(q_n)_{\mathbb{N}}$ est nulle à.p.c.r.
   (c) En déduire l'écriture du nombre n en base b et justifier son unicité.
3. Zoom hexadécimal
   (a) Combien de nombres distincts à p chiffres peut-on écrire en binaire ? Et en hexadécimal ?
   (b) Compléter $\quad \overline{7}^{16} = \overline{\qquad\qquad}^{2}, \quad \overline{D}^{16} = \overline{\qquad\qquad}^{2}$ et $\quad \overline{5}^{16} = \overline{\qquad\qquad}^{2}$.
   (c) Écrire $\overline{7D5}^{16}$ en base 2. Que remarque-t-on ?
   (d) Justifier cette méthode puis l'utiliser pour écrire $\overline{A2C}^{16}$ et $\overline{BE7D}^{16}$ en base 2 puis $\overline{1111\,1010\,0010}^{2}$ et $\overline{1001\,1101\,0101\,1110}^{2}$ en base 16.

Bonus

Puisqu'il est plus que temps d'émettre vos souhaits, je vous conseille de rajouter une ligne au texto que vous allez envoyer au Père Noël : *Théorème vivant* de Cédric Villani. Vous pouvez aussi le trouver en bibliothèque, faire un 50-50 en le partageant avec votre voisine, l'emprunter à un ami, faire un appel sur les réseaux sociaux ou user de tout autre moyen caritatif et légal mais vous devez impérativement lire ce chef-d'œuvre au moins une fois dans votre vie.

Corrigé du devoir n° 2

BASE NUMB'

1. (a) $\overline{87}^{10} = 81 + 6 = 1.3^4 + 2.3^1 = \overline{10020}^3$

   (b) $\overline{341}^{10} = 243 + 81 + 9 + 6 + 2 = 1.3^5 + 1.3^4 + 1.3^2 + 2.3^1 + 2 = \overline{110122}^3$

   (c) $\overline{255}^{10} = 128+64+32+16+8+4+2+1 = 2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$
   $= \overline{1111\,1111}^2$

   (d) $\overline{3561}^{10} = 2048 + 1024 + 256 + 128 + 64 + 32 + 8 + 1$
   $= 2^{11} + 2^{10} + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 + 2^0 = \overline{110\,1111\,0101}^2$

   (e) $\overline{45255}^{10} = 45056 + 192 + 7 = 11 \times 4096 + 12 \times 16 + 711.16^3 + 12.16 + 7$
   $= \overline{B0C7}^{16}$

   (f) $\overline{1\,0010\,0101}^2 = 2^8 + 2^5 + 2^2 + 2^0 = 256 + 32 + 4 + 1 = \overline{293}^{10}$

   (g) $\overline{22012}^3 = 2.3^4 + 2.3^3 + 1.3^1 + 2.3^0 = 2 \times 81 + 2 \times 27 + 3 + 2 = \overline{221}^{10}$

   (h) $\overline{BAC21}^{16} = 11.16^4 + 10.16^3 + 12.16^2 + 2.16^1 + 1.16^0 = \overline{764\,961}^{10}$

   (i) $\overline{1\,0000}^2 = 2^4 = 16^1 = \overline{10}^{16}$

   (j) $\overline{1\,1011\,0101}^2 = 2^8+2^7+2^5+2^4+2^2+2^0 = (2^4)^2+2^3.2^4+2^1.2^4+2^4+4+1$
   $= 16^2 + (8+2+1).2^4 + 5 = 16^2 + 11.16^1 + 5 = \overline{1B5}^{16}$

   (k) $\overline{BAC21}^{16} = 11.16^4 + 10.16^3 + 12.16^2 + 2.16^1 + 1.16^0$
   $= (8+2+1)(2^4)^4 + (8+2)(2^4)^3 + (8+4)(2^4)^2 + 2.2^4 + 1$
   $= 2^3.2^{16} + 2.2^{16} + 2^{16} + 2^3.2^{12} + 2.2^{12} + 2^3.2^8 + 2^2.2^8 + 2.2^4 + 1$
   $= 2^{19} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{11} + 2^{10} + 2^5 + 2^0$
   $= \overline{1011\,1010\,1100\,0010\,0001}^2$

   (l) $\overline{11\,1111}^2 = 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 63 = 54 + 9 = 2 \times 27 + 1 \times 9$
   $= 2.3^3 + 1.3^2 = \overline{2100}^3$

   (m) $\overline{657}^{10} = 625 + 25 + 5 + 2 = 5^4 + 5^2 + 2 = \overline{10102}^5$

   (n) $\overline{12012}^3 = 3^4+2.3^3+3^1+2 = 140 = 128+8+4 = 2^7+2^3+2^2 = \overline{1000\,1100}^2$

   (o) $\overline{34102}^5 = 3.5^4 + 4.5^3 + 1.5^2 + 2.5^0 = \overline{2402}^{10}$

   (p) $\overline{24}^{10} = 2 \times 12^1 + 0.12^0 = \overline{20}^{12}$: 24 h = 2 demi-journées.

   (q) $\overline{111}^{60} = 1.60^2 + 1.60^1 + 1.60^0 = \overline{3661}^{10}$: 1 h, 1 min, 1 s = 3661 s

   (r) $\overline{20\,067}^{10} = 5.60^2 + 34.60^1 + 27 = \overline{(5)(34)(27)}^{60}$: il nous manque des caractères.

   (s) $\overline{72}^{10} = 3 \times 24 = \overline{30}^{24}$: 72 h = 3 jours

   (t) $\overline{9999}^{10} = 7\times1331+5\times121+7\times11 = 7.11^3+5.11^2+7.11^1+0.11^0 = \overline{7570}^{11}$

   (u) $\overline{263}^7 = 2.7^2 + 6.7^1 + 3.7^0 = 2 \times 49 + 6 \times 7 + 3 \times 1 = \overline{143}^{10}$

(v) $\overline{1202}^{5} = 1.5^3 + 2.5^2 + 2 = 177 = 147 + 28 + 2 = 3.7^2 + 4.7^1 + 2.7^0 = \overline{342}^{7}$

(w) $\overline{2}^{10} = 1.2^1 + 0.2^0 = \overline{10}^{2}$

(x) $\overline{100}^{10} = 1.100^1 + 0.100^0 = \overline{10}^{100}$

(y) $\overline{100}^{2} = 1.2^2 + 0.2^1 + 0.2^0 = \overline{4}^{10}$

(z) $\overline{100}^{n^2} = 1.(n^2)^2 + 0.(n^2)^1 + 0.(n^2)^0 = n^4 = 1.n^4 + 0.n^3 + 0.n^2 + 0.n^1 + 0.n^0$
$= \overline{10000}^{n}$

2. $n = bq_0 + r_0$ puis $q_0 = bq_1 + r_1$, et ainsi de suite. On construit ainsi deux suites d'entiers $(q_n)_{\mathbb{N}}$ et $(r_n)_{\mathbb{N}}$.

(a) Soit $k \in \mathbb{N}$. Par définition, q_{k+1} est la partie entière du quotient de q_k par b : $q_k = bq_{k+1} + r_{k+1}$ d'où $q_{k+1} = \frac{q_k - r_{k+1}}{b}$ et $q_{k+1} \leqslant q_k$: la suite $(q_n)_{\mathbb{N}}$ est bien décroissante.

(b) La suite $(q_n)_{\mathbb{N}}$ est donc décroisante et minorée par 0 car $q_n \in \mathbb{N}$. Le théorème de convergence monotone permet d'affirmer qu'elle converge. Étant à valeurs entières, elle ne peut qu'être constante à.p.c.r., sinon elle serait très « loin » de sa limite. On a alors $q_{k+1} = bq_{k+1} + r_{k+1}$ donc $r_{k+1} = (1-b)q_{k+1} \leqslant 0$ ce qui n'est possible que si $q_{k+1} = r_{k+1} = 0$.

(c) Soit p le premier indice tel que $q_p = 0$.

$$\begin{aligned}
n &= bq_0 + r_0 \\
&= b(bq_1 + r_1) + r_0 \\
&= b^2 q_1 + br_1 + r_0 \\
&= b^2(bq_2 + r_2) + br_1 + r_0 \\
&= b^3 q_3 + b^2 r_2 + br_1 + r_0 = \dots \\
&= b^p q_{p-1} + b^{p-1} r_{p-1} + \dots + br_1 + r_0 \\
&= b^p(bq_p + r_p) + b^{p-1} r_{p-1} + \dots + br_1 + r_0 \\
&= b^p r_p + b^{p-1} r_{p-1} + \dots + br_1 + r_0 \\
&= \overline{r_p r_{p-1} \dots r_1 r_0}^{b}
\end{aligned}$$

3. (a) On peut écrire 2^p nombres distincts à p chiffres en écriture binaire et $16^p = 2^{4p}$ en base hexadécimale.

(b) On a $\overline{7}^{16} = 7 = 4 + 2 + 1 = \overline{111}^{2}$, $\overline{D}^{16} = 13 = 8 + 4 + 1 = \overline{1101}^{2}$ et $\overline{5}^{16} = 5 = 4 + 1 = \overline{101}^{2}$.

(c) $\overline{7D5}^{16} = 7.16^2 + 13.16^1 + 5 = 2005 = 1024 + 512 + 256 + 128 + 64 + 16 + 4 + 1$
$= 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^2 + 2^0 = \overline{111\,1101\,0101}^{2}$.

On remarque que $\overline{7}^{16} = \overline{111}^{2}$, trois premiers chiffres de l'écriture en base deux de $\overline{7D5}^{16}$, $\overline{D}^{16} = 13 = \overline{1101}^{2}$, quatre chiffres suivants, et $\overline{5}^{16} = \overline{101}^{2}$, quatre derniers chiffres.

(d) Pour transformer une écriture hexadécimale en binaire, il suffit de transcrire en base deux chacun des chiffres hexadécimaux puis de les écrire successivement. Pour passer du binaire à l'hexadécimal, on regroupe par paquets de quatre chiffres pour obtenir le chiffre en base 16. En effet, $16 = 2^4$ donc augmenter d'une puissance de 16 c'est augmenter de quatre puissances de 2 et la « barrière » entre les paquet reste « infranchissable ».

On a $\overline{1}^{16} = 1 = \overline{0001}^{2}$, $\overline{2}^{16} = 2 = \overline{0010}^{2}$, $\overline{3}^{16} = 3 = 2 + 1 = \overline{0011}^{2}$, $\overline{4}^{16} = 4 = \overline{0100}^{2}$, $\overline{5}^{16} = 5 = 4 + 1 = \overline{0101}^{2}$, $\overline{6}^{16} = 6 = 4 + 2 = \overline{0110}^{2}$, $\overline{7}^{16} = 7 = 4 + 2 + 1 = \overline{0111}^{2}$, $\overline{8}^{16} = 8 = \overline{1000}^{2}$, $\overline{9}^{16} = 9 = 8 + 1 = \overline{1001}^{2}$, $\overline{A}^{16} = 10 = 8 + 2 = \overline{1010}^{2}$, $\overline{B}^{16} = 11 = 8 + 2 + 1 = \overline{1011}^{2}$, $\overline{C}^{16} = 12 = 8 + 4 = \overline{1100}^{2}$, $\overline{D}^{16} = 13 = 8 + 4 + 1 = \overline{1101}^{2}$, $\overline{E}^{16} = 14 = 8 + 4 + 2 = \overline{1110}^{2}$ et $\overline{F}^{16} = 15 = 8 + 4 + 2 + 1 = \overline{1111}^{2}$.
D'où, $\overline{A2C}^{16} = \overline{1010\,0010\,1100}^{2}$
et $\overline{BE7D}^{16} = \overline{1011\,1110\,0111\,1101}^{2}$.
Réciproquement, $\overline{1111\,1010\,0010}^{2} = \overline{FA2}^{16}$
et $\overline{1001\,1101\,0101\,1110}^{2} = \overline{9D5E}^{16}$.

CORRIGÉS

Devoir n° 3

Arithmétique complexe

Ce devoir est associé au chapitre III, *Nombres complexes : équations polynomiales.*

Exercice Racines entières.

1. Soit P un polynôme dont tous les coefficients sont des entiers.
   (a) Démontrer que toute racine entière de P est un diviseur de $P(0)$ (cf. page 18).
   (b) Que dire si $P(0)$ est un nombre premier (cf. page 219) ?
2. Déterminer toutes les racines dans $\mathbb{C}$ du polynôme P défini par
   $P(z) = z^3 + 6z^2 + 10z + 3$.
3. Factoriser entièrement le polynôme Q défini par
   $Q(z) = z^4 + 6z^3 - 44z^2 - 294z - 245$
   en utilisant des divisions potences par exemple.
4. Le polynôme R défini par
   $R(z) = z^8 + 3z^7 + 2z^5 + 3z^3 + 2z^2 + 6$
   admet-il des racines entières ?

Bonus

Le 13 novembre 2014 décédait Alexandre Grothendieck, unanimement reconnu comme un des plus grands génies des mathématiques, après une disparition de 25 ans de la sphère publique et privée.

Apposer une souris et la faire cliquer sur le lien suivant, vous aurez un article approfondi sur son parcours, hébergé par le site toujours intéressant *Images des mathématiques* :

http ://images.math.cnrs.fr/Alexandre-Grothendieck.html

Ses écrits de réflexions et de témoignages d'un passé de mathématicien, *Récoltes et Semailles*, ont enfin été publiés chez Gallimard en 2022.

Corrigé du devoir n° 3

Arithmétique complexe

Exercice Racines entières.

1. Soit P un polynôme dont tous les coefficients sont des entiers.

   (a) On peut écrire $P(z) = \sum\limits_{k=0}^{n} a_k z^k$ où $n \in \mathbb{N}$, $a_k \in \mathbb{Z}$ et $k \in [\![0\,; n]\!]$.
   Soit $\alpha \in \mathbb{Z}$ une racine de P.
   On a $P(\alpha) = 0$ et $P(0) = a_0$.
   Ainsi, $\sum\limits_{k=0}^{n} a_k \alpha^k = 0 \iff a_0 + \sum\limits_{k=1}^{n} a_k \alpha^k = 0 \iff a_0 = -\sum\limits_{k=1}^{n} a_k \alpha^k$
   $\iff P(0) = -\alpha \sum\limits_{k=1}^{n} a_k \alpha^{k-1}$.
   Puisque $N = -\sum\limits_{k=1}^{n} a_k \alpha^{k-1}$ est un entier (somme et produit d'entiers), $P(0) = N\alpha$ et α divise $P(0)$.

   (b) Si $P(0)$ est un nombre premier, les seules racines entières de P ne peuvent être que ± 1 et $\pm P(0)$.

2. Le polynôme $P(z) = z^3 + 6z^2 + 10z + 3$ est de degré 3 et à coefficients entiers.
   $P(0) = 3$ est premier. Testons les différentes valeurs entières possibles.
   On a $P(1) = 1 + 6 + 10 + 3 \neq 0$, $P(-1) = -1 + 6 - 10 + 3 \neq 0$,
   $P(3) = 27 + 6 \times 9 + 30 + 3 \neq 0$: $P(-3) = -27 + 6 \times 9 - 30 + 3 = 0$ et -3 est la seule racine entière de P qui se factorise donc par $z + 3$.
   On a alors $P(z) = (z+3)(z^2 + bz + 1)$ en observant les termes extrêmes.
   Un développement permet d'identifier les coefficients ($b + 3 = 6$, $3b + 1 = 10$) et l'on obtient $P(z) = (z+3)(z^2 + 3z + 1)$. On aurait pu aussi réaliser une division polynomiale.
   Le trinôme $z^2 + 3z + 1$ n'admet pas de racine entière ni de factorisation évidente donc applique l'algorithme du discriminant : $\Delta = 3^2 - 4 = 5 > 0$ et il admet deux racines réelles $\frac{-3 \pm \sqrt{5}}{2}$.
   L'ensemble des racines de P est donc $\{-3; \frac{-3-\sqrt{5}}{2}; \frac{-3-\sqrt{5}}{2}\}$.

3. Après avoir remarqué successivement que -1 puis -5 sont des racines et avoir effectué les divisions potences correspondantes, on obtient
   $Q(z) = z^4 + 6z^3 - 44z^2 - 294z - 245 = (z+1)(z+5)(z-7)(z+7)$.

4. Les racines entières de $R(z) = z^8 + 3z^7 + 2z^5 + 3z^3 + 2z^2 + 6$ sont des diviseurs de $R(0) = 6$. Testons-les. On a $R(1) = 17 \neq 0$, $R(-1) = 1 \neq 0$, $R(2) = 742 \neq 0$, $R(-2) = -202 \neq 0$, $R(3) = 13713 \neq 0$, $R(-3) = -543 \neq 0$, $R(6) > 0$ et $R(-6) > 0$.
   Le polynôme R n'admet donc pas de racines entières.

Devoir n° 4

MATRIX

Ce devoir est associé au chapitre IV, *Matrices*.

On souhaite coder puis décoder des messages ultra-secrets à l'aide de la matrice $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.

Procédure de codage :

- À chaque lettre de l'alphabet, on associe son numéro dans l'ordre alphabétique en commençant par 0.
- On associe à un mot de deux lettres à coder, la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 est le code de la première lettre du mot et x_2, celui de la seconde.
- On calcule alors la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que $Y = QX$.
- On obtient alors la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ où r_i est le reste de la division euclidienne de y_i par 26.
- On associe enfin à la matrice R un mot de deux lettres en utilisant la même correspondance entre lettres et numéros. Le mot obtenu est le message que l'on peut alors communiquer à son interlocuteur.

1. Coder le mot MATH.
2. L'interlocuteur ayant reçu le message doit pouvoir le décoder bien-sûr.
   (a) Pour cela, calculer la matrice inverse Q^{-1} de Q.
   (b) Montrer que $3X = 3Q^{-1}Y$ puis que $\begin{cases} 3x_1 & \equiv & 3r_1 - 3r_2\,[26] \\ 3x_2 & \equiv & -5r_1 + 6r_2\,[26]. \end{cases}$
   (c) Déterminer l'inverse de 3 modulo 26 puis en déduire que $\begin{cases} x_1 & \equiv & r_1 - r_2\,[26] \\ x_2 & \equiv & 7r_1 + 2r_2\,[26]. \end{cases}$
   (d) En déduire la matrice Q' de déchiffrement et décoder le mot UIZC.
   Que remarque-t-on ?

Toute la sécurité de la transmission tient dans la confidentialité des matrices de chiffrement et/ou déchiffrement, matrices que l'on ne doit donc divulguer sous aucun prétexte.

Bonus Let's play Jeopardy : $\boxed{\text{Flatland}}$
Indice : C'est un livre, pas une chanson.

EXERCICES

Corrigé du devoir n° 4

Matrix

1. Le mot MATH est associé aux numéros 12 ;0 ;19 ;7. On a alors $X_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$,
$Y_1 = QX_1 = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 72 \\ 60 \end{pmatrix} = \begin{pmatrix} 20+2\times 26 \\ 8+2\times 26 \end{pmatrix}$, $R_1 = \begin{pmatrix} 20 \\ 8 \end{pmatrix}$ qui donne les lettres UI.
Puis, $X_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$, $Y_2 = QX_2 = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 135 \\ 116 \end{pmatrix} = \begin{pmatrix} 5+5\times 26 \\ 12+4\times 26 \end{pmatrix}$,
$R_2 = \begin{pmatrix} 5 \\ 12 \end{pmatrix}$ qui donne les lettres FM.
Ainsi, MATH est codé en UIFM.

2. (a) On a $\det(Q) = 6\times 3 - 5\times 3 = 3 \neq 0$ donc Q est inversible et
$Q^{-1} = \frac{1}{3}\begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}$.

   (b) On a $Y = QX \iff Q^{-1}QX = Q^{-1}Y \iff 3X = 3Q^{-1}Y$
$$\iff 3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 3\times\frac{1}{3}\begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \iff \begin{pmatrix} 3x_1 \\ 3x_2 \end{pmatrix} = \begin{pmatrix} 3y_1 - 3y_2 \\ -5y_1 + 6y_2 \end{pmatrix}$$
$$\iff \left\{\begin{array}{lllll} 3x_1 & = & 3y_1 - 3y_2 & \equiv & 3r_1 - 3r_2\,[26] \\ 3x_2 & = & -5y_1 + 6y_2 & \equiv & -5r_1 + 6r_2\,[26]. \end{array}\right.$$

   (c) On a $3\times 9 = 27 \equiv 1[26]$ donc 9 est l'inverse de 3 modulo 26. Ainsi,
$$\left\{\begin{array}{lll} 9\times 3x_1 & \equiv & 9\times(3r_1 - 3r_2)\,[26] \\ 9\times 3x_2 & \equiv & 9\times(-5r_1 + 6r_2)\,[26]. \end{array}\right.$$
$$\iff \left\{\begin{array}{lll} 27x_1 & \equiv & 27r_1 - 27r_2\,[26] \\ 27x_2 & \equiv & -45r_1 + 54r_2\,[26]. \end{array}\right.$$
$$\iff \left\{\begin{array}{lll} 1x_1 & \equiv & 1r_1 - 1r_2\,[26] \\ 1x_2 & \equiv & (7-2\times 26)r_1 + (2+2\times 26)r_2\,[26]. \end{array}\right.$$
$$\iff \left\{\begin{array}{lll} x_1 & \equiv & r_1 - r_2\,[26] \\ x_2 & \equiv & 7r_1 + 2r_2\,[26]. \end{array}\right.$$

   (d) La matrice de déchiffrement est donc $Q' = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}$.

   Le mot UIZC est associé aux numéros 20 ;8 ;25 ;2. On a alors $R'_1 = \begin{pmatrix} 20 \\ 8 \end{pmatrix}$,
$Y'_1 = Q'R'_1 = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}\begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 12 \\ 156 \end{pmatrix} = \begin{pmatrix} 12+0\times 26 \\ 0+6\times 26 \end{pmatrix}$,
et enfin, $X'_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$ qui donne les lettres MA.

Puis, $R'_2 = \begin{pmatrix} 25 \\ 2 \end{pmatrix}$, $Y'_2 = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} 25 \\ 2 \end{pmatrix} = \begin{pmatrix} 23 \\ 179 \end{pmatrix} = \begin{pmatrix} 23 + 0 \times 26 \\ 23 + 6 \times 26 \end{pmatrix}$,

$X'_2 = \begin{pmatrix} 23 \\ 23 \end{pmatrix}$ qui donne les lettres XX.

Ainsi, UIZC se déchiffre en MAXX.

On remarque qu'il est nécessaire d'avoir un nombre pair de lettres dans le message à coder. Si ce n'est pas cas, il suffit de doubler la dernière pour que celui-ci reste lisible. Par ailleurs, le couple MA se code en UI et réciproquement. En revanche, un X en première position se code en Z alors qu'un X en seconde position se code en C. Le codage d'une lettre dépend donc de sa position.

Bonus $\boxed{\text{Flatland}}$

Quel est le titre du livre publié en 1884 par Edwin Abbott Abbott dans lequel les personnages sont des figures géométriques – triangles isocèles, carrés, polygones, cercles... – qui, dans leur monde plat, en deux dimensions, sont très hiérarchisées et ont des coutumes et des croyances bien ancrées et où l'on crie à l'hérésie lorsqu'un modeste carré doté d'une conscience découvre la troisième dimension lors de l'apparition soudaine et invraisemblable d'une sphère, et qui, on l'aura compris, est tout à la fois critique de la rigidité de la société victorienne et texte fondateur de la science-fiction et aborde la question troublante de la possibilité d'une quatrième dimension spatiale et qui, bien que n'ayant pas de rapport avec un texte de Jacques Brel, vous est néanmoins conseillé avec insistance par le rédacteur, d'autant plus qu'il ne coûte pas même trois euros ?

Devoir n° 5

Les Quaternions

Ce devoir est associé au chapitre IV, *Matrices*.

On pose $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathrm{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{K} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$.

Attention à la notation : $\mathrm{I} \neq I_2 = \mathbb{1}$.

1. Calculer $\mathbb{1}^2$, I^2, J^2, K^2 et IJK.
2. En déduire IJ, JK, IK, JI, KJ et KI.
3. Compléter alors la table de multiplication suivante.

$\times$ ↬	$\mathbb{1}$	I	J	K
$\mathbb{1}$				
I				
J				
K				

   Que remarque-t-on ?

4. L'ensemble des quaternions est défini par
   $\mathbb{H} = \left\{Q = a\mathbb{1} + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \;/\; a,\ b,\ c,\ d \in \mathbb{R}\right\}$.
   $\mathbb{H}$ est donc l'ensemble des matrices qui peuvent s'écrire comme combinaison linéaire réelle de $\mathbb{1}$, I, J et K.
   (a) On donne $Q_1 = 2.\mathbb{1} - 3\mathrm{K}$, $Q_2 = 4\mathrm{I} - 3\mathrm{J} + \mathrm{K}$ et $Q_3 = 3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K}$.
   Calculer $Q_1 + Q_2$, $2Q_3 - 4Q_1$, Q_1Q_2, Q_2Q_1, Q_2Q_3 et Q_3Q_2.
   (b) Justifier que $\mathbb{H}$ est stable par addition, par multiplication par un réel et par produit.
   (c) On pose $\overline{Q_1} = 2.\mathbb{1} + 3\mathrm{K}$, $\overline{Q_2} = -4\mathrm{I} + 3\mathrm{J} - \mathrm{K}$ et $\overline{Q_3} = 3.\mathbb{1} - 2\mathrm{I} + \mathrm{J} - 4\mathrm{K}$.
   Calculer $Q_1\overline{Q_1}$, $\overline{Q_3}Q_2$ et $Q_3\overline{Q_3}$. Que remarque-t-on ?
   (d) Compléter :
   Si $Q = a\mathbb{1} + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \in \mathbb{H}$, on pose $\overline{Q} = \ldots \in \mathbb{H}$
   et $\|Q\| = \sqrt{\ldots\qquad\qquad} \in \mathbb{R}$.
   On a toujours $Q\overline{Q} = \ldots \qquad \overline{Q}Q$.
   Tout quaternion Q ... admet donc un ... , le quaternion ... .

5. Soit E le sous-ensemble de $\mathbb{H}$ dans lequel les éléments s'écrivent sous la forme $Z = a\mathbb{1} + b\mathrm{I}$ (autrement dit, $c = d = 0$).
   (a) Quelle matrice est associée à un tel $Z \in E$?
   (b) Soient $Z, Z' \in E$. Calculer $Z + Z'$, ZZ', $Z'Z$, $\overline{Z}$, $\|Z\|$ et $Z\overline{Z}$.
   (c) Quel est donc l'ensemble E ?

EXERCICES

L'ensemble $\mathbb{H}$ des quaternions généralise l'ensemble des nombres complexes. En contrepartie, la multiplication de ces nombres n'est plus commutative. Introduits par le mathématicien irlandais W. R. Hamilton en 1843, ils trouvent aujourd'hui des applications en mathématiques, en physique, en informatique et en sciences de l'ingénieur.

Bonus

Puisqu'il est temps d'émettre vos souhaits, je vous conseille de rajouter une ligne au texto que vous allez envoyer au Père Noël : *Le Théorème du perroquet* de Denis Guedj. Vous pouvez aussi le trouver en bibliothèque, faire un 50-50 en le partageant avec votre voisine, l'emprunter à un ami, faire un appel sur les réseaux sociaux ou user de tout autre moyen caritatif et légal mais vous ne pourrez qu'apprécier ce roman policier qui retrace avec talent, humour et suspense l'avènement des plus grandes avancées dans l'histoire des mathématiques.

Corrigé du devoir n° 5

Les Quaternions

On pose $\quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathrm{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad$ et $\quad \mathrm{K} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$

1. On a $\quad \mathbb{1}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}, \quad \mathrm{I}^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = -\mathbb{1},$

   $\mathrm{J}^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbb{1},$

   $\mathrm{K}^2 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}^2 = \begin{pmatrix} (-i)^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = -\mathbb{1}$

   et $\quad \mathrm{IJK} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -\mathbb{1}.$

2. $\mathrm{IJK} = -\mathbb{1} \Longrightarrow \mathrm{IJK}^2 = -\mathrm{K} \Longrightarrow -\mathrm{IJ}\mathbb{1} = -\mathrm{K} \Longrightarrow \mathrm{IJ} = \mathrm{K},$
   $\mathrm{IJK} = -\mathbb{1} \Longrightarrow \mathrm{I}^2\mathrm{JK} = -\mathrm{I} \Longrightarrow -\mathrm{JK} = -\mathrm{I} \Longrightarrow \mathrm{JK} = \mathrm{I},$
   $\mathrm{IK} = (\mathrm{JK})\mathrm{K} = \mathrm{JK}^2 = -\mathrm{J}, \qquad \mathrm{JI} = \mathrm{J}(\mathrm{JK}) = \mathrm{J}^2\mathrm{K} = -\mathrm{K},$
   $\mathrm{KJ} = (\mathrm{IJ})\mathrm{J} = \mathrm{IJ}^2 = -\mathrm{I}, \quad$ et $\quad \mathrm{KI} = (-\mathrm{JI})\mathrm{I} = -\mathrm{JI}^2 = \mathrm{J}.$

3.

$\times \looparrowright$	$\mathbb{1}$	I	J	K
$\mathbb{1}$	$\mathbb{1}$	I	J	K
I	I	$-\mathbb{1}$	K	$-$J
J	J	$-$K	$-\mathbb{1}$	I
K	K	J	$-$I	$-\mathbb{1}$

   Ce tableau n'est pas symétrique : cette multiplication n'est pas commutative.

4. (a) On donne $\quad Q_1 = 2.\mathbb{1} - 3\mathrm{K}, \quad Q_2 = 4\mathrm{I} - 3\mathrm{J} + \mathrm{K} \quad$ et $\quad Q_3 = 3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K}.$

   On a $\quad Q_1 + Q_2 = (2.\mathbb{1} - 3\mathrm{K}) + (4\mathrm{I} - 3\mathrm{J} + \mathrm{K}) = 2.\mathbb{1} + 4\mathrm{I} - 3\mathrm{J} - 2\mathrm{K},$

$$2Q_3 - 4Q_1 = 2(3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K}) - 4(2.\mathbb{1} - 3\mathrm{K}) = -2.\mathbb{1} + 4\mathrm{I} - 2\mathrm{J} + 20\mathrm{K},$$

$$\begin{aligned} Q_1Q_2 &= (2.\mathbb{1} - 3\mathrm{K})(4\mathrm{I} - 3\mathrm{J} + \mathrm{K}) = 8.\mathbb{1}.\mathrm{I} - 6.\mathbb{1}.\mathrm{J} + 2.\mathbb{1}.\mathrm{K} - 12\mathrm{KI} + 9\mathrm{KJ} - 3\mathrm{K}^2 \\ &= 8\mathrm{I} - 6\mathrm{J} + 2\mathrm{K} - 12\mathrm{J} + 9(-\mathrm{I}) - 3(-\mathbb{1}) = 3.\mathbb{1} - \mathrm{I} - 18\mathrm{J} + 2\mathrm{K}, \\ Q_2Q_1 &= (4\mathrm{I} - 3\mathrm{J} + \mathrm{K})(2.\mathbb{1} - 3\mathrm{K}) = 8\mathrm{I}.\mathbb{1} - 12\mathrm{IK} - 6\mathrm{J}.\mathbb{1} + 9\mathrm{JK} + 2\mathrm{K}.\mathbb{1} - 3\mathrm{K}^2 \\ &= 8\mathrm{I} - 12(-\mathrm{J}) - 6\mathrm{J} + 9\mathrm{I} + 2\mathrm{K} - 3(-\mathbb{1}) = 3.\mathbb{1} + 17\mathrm{I} + 6\mathrm{J} + 2\mathrm{K}, \\ Q_2Q_3 &= (4\mathrm{I} - 3\mathrm{J} + \mathrm{K})(3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K}) \\ &= 12\mathrm{I}.\mathbb{1} + 8\mathrm{I}^2 - 4\mathrm{IJ} + 16\mathrm{IK} - 9\mathrm{J}.\mathbb{1} - 6\mathrm{JI} + 3\mathrm{J}^2 - 12\mathrm{JK} + 3\mathrm{K}.\mathbb{1} \\ &\qquad + 2\mathrm{KI} - \mathrm{KJ} + 4\mathrm{K}^2 \\ &= 12\mathrm{I} + 8(-\mathbb{1}) - 4\mathrm{K} + 16(-\mathrm{J}) - 9\mathrm{J} - 6(-\mathrm{K}) - 3(-\mathbb{1}) - 12\mathrm{I} + 3\mathrm{K} \\ &\qquad + 2\mathrm{J} - (-\mathrm{I}) + 4(-\mathbb{1}) \\ &= -9.\mathbb{1} + \mathrm{I} - 23\mathrm{J} + 5\mathrm{K}, \\ Q_3Q_2 &= (3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K})(4\mathrm{I} - 3\mathrm{J} + \mathrm{K}) \end{aligned}$$

$$\begin{aligned} Q_3Q_2 &= 12.\mathbb{1}.\mathrm{I} - 9.\mathbb{1}.\mathrm{J} + 3.\mathbb{1}.\mathrm{K} + 8\mathrm{I}^2 - 6\mathrm{IJ} + 2\mathrm{IK} - 4\mathrm{JI} + 3\mathrm{J}^2 - \mathrm{JK} \\ &\qquad + 16\mathrm{KI} - 12\mathrm{KJ} + 4\mathrm{K}^2 \\ &= 12\mathrm{I} - 9\mathrm{J} + 3\mathrm{K} + 8(-\mathbb{1}) - 6\mathrm{K} + 2(-\mathrm{J}) - 4(-\mathrm{K}) + 3(-\mathbb{1}) - \mathrm{I} \\ &\qquad + 16\mathrm{J} - 12(-\mathrm{I}) + 4(-\mathbb{1}) \\ &= -15.\mathbb{1} + 23\mathrm{I} + 5\mathrm{J} + \mathrm{K}. \end{aligned}$$

: la multiplication n'est pas commutative.

(b) Les règles de la somme de matrices et du produit d'une matrice par un réel impliquent que $\mathbb{H}$ est stable par addition et par multiplication par un réel. La table de multiplication précédente implique que $\mathbb{H}$ est stable par produit.

(c) On pose $\overline{Q_1} = 2.\mathbb{1} + 3\mathrm{K}$, $\overline{Q_2} = -4\mathrm{I} + 3\mathrm{J} - \mathrm{K}$ et $\overline{Q_3} = 3.\mathbb{1} - 2\mathrm{I} + \mathrm{J} - 4\mathrm{K}$. On a

$$\begin{aligned} Q_1\overline{Q_1} &= (2.\mathbb{1} - 3\mathrm{K})(2.\mathbb{1} + 3\mathrm{K}) = 4.\mathbb{1}^2 + 6.\mathbb{1}.\mathrm{K} - 6\mathrm{K}.\mathbb{1} - 9\mathrm{K}^2 \\ Q_1\overline{Q_1} &= 4\mathbb{1} + 6\mathrm{K} - 6\mathrm{K} - 9(-\mathbb{1}) = 13.\mathbb{1} = (2^2 + 3^2).\mathbb{1}, \\ \overline{Q_2}Q_2 &= (-4\mathrm{I} + 3\mathrm{J} - \mathrm{K})(4\mathrm{I} - 3\mathrm{J} + \mathrm{K}) \\ &= -16\mathrm{I}^2 + 12\mathrm{IJ} - 4\mathrm{IK} + 12\mathrm{JI} - 9\mathrm{J}^2 + 3\mathrm{JK} - 4\mathrm{KI} + 3\mathrm{KJ} - \mathrm{K}^2 \\ &= -16(-\mathbb{1}) + 12\mathrm{K} - 4(-\mathrm{J}) + 12(-\mathrm{K}) - 9(-\mathbb{1}) + 3\mathrm{I} - 4\mathrm{J} + 3(-\mathrm{I}) - (-\mathbb{1}) \\ \overline{Q_2}Q_2 &= 26.\mathbb{1} = ((-4)^2) + 3^3 + (-1)^2).\mathbb{1}, \\ Q_3\overline{Q_3} &= (3.\mathbb{1} + 2\mathrm{I} - \mathrm{J} + 4\mathrm{K})(3.\mathbb{1} - 2\mathrm{I} + \mathrm{J} - 4\mathrm{K}) \\ &= 9.\mathbb{1}^2 - 6.\mathbb{1}.\mathrm{I} + 3.\mathbb{1}.\mathrm{J} - 12.\mathbb{1}.\mathrm{K} + 6\mathrm{I}.\mathbb{1} - 4\mathrm{I}^2 + 2\mathrm{IJ} - 8\mathrm{IK} - 3\mathrm{J}.\mathbb{1} \\ &\qquad + 2\mathrm{JI} - \mathrm{J}^2 + 4\mathrm{JK} + 12\mathrm{K}.\mathbb{1} - 8\mathrm{KI} + 4\mathrm{KJ} - 16\mathrm{K}^2 \\ &= 9.\mathbb{1} - 6\mathrm{I} + 3\mathrm{J} - 12\mathrm{K} + 6\mathrm{I} - 4(-\mathbb{1}) + 2\mathrm{K} - 8(-\mathrm{J}) \\ &\qquad - 3\mathrm{J} + 2(-\mathrm{K}) - (-\mathbb{1}) + 4\mathrm{I} + 12\mathrm{K} - 8\mathrm{J} + 4(-\mathrm{I}) - 16(-\mathbb{1}) \\ Q_3\overline{Q_3} &= 30.\mathbb{1} = (3^2 + 2^2 + (-1)^2 + 4^2).\mathbb{1}. \end{aligned}$$

(d) Si $Q = a\mathbb{1} + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \in \mathbb{H}$, on pose $\overline{Q} = a\mathbb{1} - b\mathrm{I} - c\mathrm{J} - d\mathrm{K} \in \mathbb{H}$ et $\|Q\| = \sqrt{a^2 + b^2 + c^2 + d^2} \in \mathbb{R}$.
On a toujours $Q\overline{Q} = \|Q\|^2.\mathbb{1} = \overline{Q}Q$. Tout quaternion Q non nul admet donc un inverse, le quaternion $Q^{-1} = \frac{1}{\|Q\|^2}\overline{Q}$.

5. Soit E le sous-ensemble de $\mathbb{H}$ dans lequel les éléments s'écrivent sous la forme $Z = a\mathbb{1} + b\mathrm{I}$ (autrement dit, $c = d = 0$).

(a) On a $Z = a\mathbb{1} + b\mathrm{I} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix}$.

(b) Soient $Z = a\mathbb{1} + b\mathrm{I}$ et $Z' = a'\mathbb{1} + b'\mathrm{I} \in E$. On a

$$\begin{aligned} Z + Z' &= a\mathbb{1} + b\mathrm{I} + a'\mathbb{1} + b'\mathrm{I} = (a + a')\mathbb{1} + (b + b')\mathrm{I} \in E, \\ ZZ' &= (a\mathbb{1} + b\mathrm{I})(a'\mathbb{1} + b'\mathrm{I}) = aa'\mathbb{1} + ab'\mathbb{1}\mathrm{I} + a'b\mathrm{I}\mathbb{1} + bb'\mathrm{I}^2 \\ &= (aa' - bb')\mathbb{1} + (a'b - ab')\mathrm{I} \in E, \end{aligned}$$

$Z'Z = ZZ'$, $\overline{Z} = a\mathbb{1} - b\mathrm{I}$, $\|Z\| = \sqrt{a^2 + b^2}$ et $Z\overline{Z} = \|Z\|^2.\mathbb{1}$.

(c) L'ensemble E est précisément l'ensemble des nombres complexes $\mathbb{C}$.

L'ensemble $\mathbb{H}$ des quaternions généralise l'ensemble des nombres complexes. En contrepartie, la multiplication de ces nombres n'est plus commutative. Introduits par le mathématicien irlandais W. R. Hamilton en 1843, ils trouvent aujourd'hui des applications en mathématiques, en physique, en informatique et en sciences de l'ingénieur.

Devoir n° 6

Hi Hi Hi !

Ce devoir est associé au chapitre V, *Nombres complexes : géométrie.*

Exercice 1 VouF

Pour chaque proposition, indiquer si elle est vraie ou fausse. Justifer. Le plan complexe est rapporté à un repère orthonormé direct $(O\,;\,\overrightarrow{u},\,\overrightarrow{v})$.

İ. f est l'application qui à tout nombre complexe z non nul associe le nombre complexe $z' = f(z) = \left(\dfrac{z}{|z|}\right)^2$.

On note M le point d'affixe $z = x+iy$ $(z \neq 0)$ et M' celui d'affixe $z' = x'+iy'$.

(i) $x' = \dfrac{x^2-y^2}{x^2+y^2}$ et $y' = \dfrac{2xy}{x^2+y^2}$.

(ii) « $z' \in \mathbb{R}$ » équivaut à « M appartient à l'axe des ordonnées ».

(iii) $f\left([1+i]^8\right)$ est un réel.

(iiii) Il existe un unique point M tel que M et M' soient confondus.

İİ. Même exercice pour $z' = f(z) = \left(\dfrac{z}{\overline{z}}\right)^2$.

Exercice 2

Soient n un entier naturel et z un nombre complexe de module 1 tels que z^{2n} soit différent de -1.

Montrer que $\dfrac{z^n}{1+z^{2n}}$ est un nombre réel.

Exercice 3 Déterminer l'ensemble les points M d'affixe z tels que les points $A(i)$, $B(iz)$ et M soient alignés.

Exercice 4 Les questions suivantes sont indépendantes.

Toute trace de recherche, même incomplète, ou d'initiative, même infructueuse, sera prise en compte dans l'évaluation.

(i) Trouver une formule (vraie) liant la base du logarithme népérien, les éléments neutres des opérations usuelles, la quadrature du cercle et l'imaginaire.

(ii) Si les personnages étaient des nombres, lesquels seraient Quasimodo et Esmeralda ? Argumenter.

(iii) Qu'égale Icare ?

(iiii) L'Éléphant sait-il conjuguer ?

(iiiii) Que transcrit le titre de ce devoir ?

Corrigé du devoir n° 6

HI HI HI !

Exercice 1 :

İ. Pour la fonction $\boldsymbol{z' = f(z) = \left(\dfrac{z}{|z|}\right)^2}$.

(i) Pour $z \neq 0$,

$$x' + iy' = f(z) = \frac{z^2}{|z|^2} = \tfrac{(x+iy)^2}{x^2+y^2} = \tfrac{(x^2-y^2)+i(2xy)}{x^2+y^2} = \tfrac{x^2-y^2}{x^2+y^2} + i\tfrac{2xy}{x^2+y^2} \ : \ \text{Vrai.}$$

(ii) Pour $z \neq 0$, $z' \in \mathbb{R} \iff y' = 0 \iff 2xy = 0 \iff x = 0$ ou $y = 0$
$\iff M$ appartient à l'axe des ordonnées ou celui des abscisses donc Faux.

(iii) $1 + i = \sqrt{2}\,\mathrm{e}^{i\frac{\pi}{4}}$ donc $(1+i)^8 = \sqrt{2}^8\,\mathrm{e}^{8i\frac{\pi}{4}} = 16\,\mathrm{e}^{2i\pi} = 16$ et
$f[(1+i)^8] = \left(\frac{16}{16}\right)^2 = 1 \in \mathbb{R}$: Vrai.

(iiii) Pour $z \neq 0$, $z' = z \iff \left(\dfrac{z}{|z|}\right)^2 = z \iff \frac{z^2}{z\overline{z}} = z \iff \frac{z^2}{z^2} = \overline{z} \iff z = 1$
donc Vrai.

İI. Pour la fonction $\boldsymbol{z' = f(z) = \left(\dfrac{z}{\overline{z}}\right)^2}$.

(i) Faux. Contre-exemple $z = i$: facile et beaucoup plus efficace que
$\frac{x^2-y^2}{x^2+y^2} + i\frac{2xy}{x^2+y^2} \neq (\frac{x^2-y^2}{x^2+y^2} + i\frac{2xy}{x^2+y^2})^2$.

(ii) Pour $z = \rho e^{i\theta}$, $f(z) = \left(\frac{\rho e^{i\theta}}{\rho e^{-i\theta}}\right)^2 = \left(e^{2i\theta}\right)^2 = e^{4i\theta}$ et
$z' \in \mathbb{R} \Leftrightarrow 4\theta \equiv 0[\pi] \Leftrightarrow \theta \equiv 0[\frac{\pi}{4}]$: Faux.
Beaucoup mieux que le propos « $z' \in \mathbb{R} \Leftrightarrow ... \Leftrightarrow z' = 1$ impossible » car vous ne montrez pas que z' peut prendre des valeurs réelles autres que 1.

(iii) Idem et $f(16) = \left(\frac{16}{16}\right)^2 = 1^2 = 1$: Vrai

(iiii) Faux. Pour $z \neq 0$, $z' = z \iff e^{4i\theta} = \rho e^{i\theta} \iff \rho = 1$ et $4\theta \equiv \theta\,[2\pi]$
$\iff \rho = 1$ et $\theta \equiv 0\,[\frac{2\pi}{3}]$.

Exercice 2

$$\left(\frac{z^n}{1+z^{2n}}\right) - \overline{\left(\frac{z^n}{1+z^{2n}}\right)} = \frac{z^n}{1+z^{2n}} - \frac{\overline{z^n}}{\overline{1+z^{2n}}}$$

$$= \frac{z^n\left(\overline{1} + \overline{z^{2n}}\right) - \overline{z^n}(1+z^{2n})}{(1+z^{2n})\overline{(1+z^{2n})}} = \frac{z^n + z^n\overline{z^n}\,\overline{z^n} - \overline{z^n} - \overline{z^n}z^n z^n}{|1+z^{2n}|^2}$$

$$= \frac{z^n + (z\overline{z})^n\overline{z^n} - \overline{z^n} - (\overline{z}z)^n z^n}{|1+z^{2n}|^2} = \frac{z^n + 1\times\overline{z^n} - \overline{z^n} - 1\times z^n}{|1+z^{2n}|^2} = 0$$

donc $\dfrac{z^n}{1+z^{2n}}$ égale son conjugué et $\dfrac{z^n}{1+z^{2n}} \in \mathbb{R}$.

Sinon, $\frac{z^n}{1+z^{2n}} = \frac{e^{in\theta}}{1+(e^{i\theta})^{2n}} = \frac{1}{e^{-in\theta}(1+e^{2ni\theta})} = \frac{1}{e^{-in\theta}+e^{ni\theta}} = \frac{1}{2\,\frac{e^{ni\theta}+e^{-ni\theta}}{2}} = \frac{1}{2\cos(n\theta)} \in \mathbb{R}$.

Exercice 3 $A(i)$, $B(iz)$ et $M(z)$ alignés

Posons $z = x+iy$. On a $iz = -y+ix$ donc $z-i = x+i(y-1)$ et $iz-i = -y+i(x-1)$.

Les points $A(i)$, $B(iz)$ et $M(z)$ sont alignés

$\iff$ les vecteurs $\overrightarrow{AM}_{z-i}\begin{pmatrix} x \\ y-1 \end{pmatrix}$ et $\overrightarrow{AB}_{iz-i}\begin{pmatrix} -y \\ x-1 \end{pmatrix}$ sont colinéaires

$\iff$ $x(x-1)-(-y)(y-1)=0$

$\iff$ $x^2-x+\frac{1}{4}+y^2-y+\frac{1}{4}-\frac{1}{2}=0$

$\iff$ $(x-\frac{1}{2})^2+(y-\frac{1}{2})^2 = \sqrt{\frac{1}{2}}^{\,2}$

$\iff$ M appartient au cercle de centre $\left(\frac{1}{2}, \frac{1}{2}\right)$ et de rayon $\frac{\sqrt{2}}{2}$.

On peut d'ailleurs vérifier que les points d'affixe 0, 1, i et $1+i$ satisfont cette propriété.

Exercice 4

(i) La plus belle d'entre toutes : $\boldsymbol{e^{i\pi}+1=0}$.

(ii) D'un premier abord repoussant mais néanmoins astucieux, serviable et bon, le personnage de Quasimodo ne pourrait être qu'$\boldsymbol{i^2}$ (et non $-i$). Esmeralda serait alors $\boldsymbol{-1}$ pour que leur produit ne fasse plus qu'un.

(iii) Chacun sait bien qu'Icare égale -1.

(iiii) Bien sûr, même s'il se trompe et conjugue parfois dans un ordre différent. Par exemple, il est bien connu qu'en cas de coup $\overline{de}$, $\overline{Ba}$ $\underline{i}$ pour des $\overline{Caram}$.

(iiiii) Le titre de ce devoir est bien la transcription d'un rire complexe.

CORRIGÉS

Devoir n° 7

Mandelbrot et Julia

Ce devoir est associé au chapitre V, *Nombres complexes : géométrie.*

Exercice

Partie A : Ensemble de Mandelbrot

Dans le plan complexe, on considère un point C d'affixe c. On construit alors la suite de point M_n dont les affixes z_n sont définies par $\begin{cases} z_0 &= 0 \\ z_{n+1} &= z_n^2 + c. \end{cases}$

Il est démontré que :

- soit $OM_n = |z_n|$ est bornée, et l'on dit alors que le point C appartient à l'ensemble de Mandelbrot $\mathcal{M}$,
- soit $OM_n = |z_n|$ tend vers $+\infty$, et dans ce cas, le point $C \notin \mathcal{M}$.

1. Justifier que cette double propriété est généralement fausse.
2. Justifier que O appartient à l'ensemble de Mandelbrot $\mathcal{M}$.
3. Démontrer que le point d'affixe -1 appartient à l'ensemble de Mandelbrot $\mathcal{M}$.
4. Dans cette question, on pose $c = i$.
   (a) Montrer que les points M_2 et M_4 sont alors confondus.
   (b) Montrer que $C_i \in \mathcal{M}$.
5. Montrer que $C_{-i} \in \mathcal{M}$.
6. Démontrer que le point d'affixe 2 n'appartient pas à $\mathcal{M}$.
7. On pose $c = a + ib$ et $z_n = x_n + iy_n$.
   Déterminer une expression de x_{n+1} et y_{n+1}.

Cet ensemble $\mathcal{M}$ a été découvert par Gaston Julia (1893-1978) et Pierre Fatou (1878-1929) avant la Première Guerre mondiale. Le mathématicien franco-américain Benoit Mandelbrot (1924-2010) est le premier à en avoir obtenu une visualisation par ordinateur, en 1980. Il est considéré comme le père des magnifiques objets que sont les fractales et dont l'ensemble nommé en son honneur est un exemple extraordinaire. Vous en trouverez de magnifiques explorations sur l'internet.

Partie B : Ensembles de Julia

On définit l'ensemble de Julia rempli $\mathcal{J}_c$ d'un nombre complexe c comme l'ensemble des complexes ω tels que la suite (z_n) définie par $\begin{cases} z_0 &= \omega \\ z_{n+1} &= z_n^2 + c. \end{cases}$ soit bornée.

1. En utilisant la partie A, que dire de $\mathcal{J}_0$, $\mathcal{J}_{-1}$, $\mathcal{J}_i$, $\mathcal{J}_{-i}$ et $\mathcal{J}_2$?
2. Plus généralement, quel lien peut-on définir entre $\mathcal{J}_c$ et $\mathcal{M}$?
3. Quel est précisément l'ensemble $\mathcal{J}_0$?

Un théorème fondamental affirme que si c appartient à l'ensemble de Mandelbrot $\mathcal{M}$ alors l'ensemble de Julia rempli correspondant J_c est connexe, c.-à-d. en « un seul morceau ». Lorsque le point c est hors de l'ensemble de Mandelbrot, l'ensemble de Julia « se brise » en une poussière de Cantor formée de points non connectés mais dont tout voisinage contient un autre point de l'ensemble. Les ensembles de Julia sont aussi fractals. Il est possible de trouver (ou créer) de remarquables applications pour téléphone ou tablettes vous permettant de voyager dans ces mondes fractals et observer les différentes composantes de l'ensemble de Mandelbrot correspondants aux différentes allures des Julias.

Partie C : Tracé

Soit C un point du plan d'affixe $c = a + ib$. Il est démontré que s'il existe $n_0 \in \mathbb{N}$ tel que $|z_{n_0}| \geqslant 2$ alors cette suite tend vers l'infini, c.-à-d. $C \notin \mathcal{M}$. Ceci constitue un test sommaire mais relativement rapide d'appartenance à l'ensemble de Mandelbrot.

Compléter l'algorithme suivant afin d'obtenir une superbe image approchée en noir sur fond blanc de l'ensemble de Mandelbrot.

```
IterationMax = 50
Pour chaque pixel C de coordonnées (a;b)
   d2 = a**2+b**2
   x = a
   y = b
   Tant Que (d2 < ...) ... (n < ...)
      x = ...
      y = ...
      d2 = ...
      n = ...
   Fin Tant Que
   Si (n == IterationMax) Alors
      Colorier le pixel en ...
   Sinon
      Colorier le pixel en ...
   Fin Si
Fin Pour
```

Bonus Compléter le texte suivant.

Half of what I say is ... But I say it just to reach you, ... , Julia, Julia ... calls me So I ... the song of love Julia, Julia, seashell eyes Windy smile ... So I sing the song of ... Julia Her hair of floating ... is shimmering Glimmering in the ... Julia, Julia Morning ... touch me So I sing the ... ... When I cannot sing my ... I can only ... my mind Julia ... , sleeping sand, silent cloud ... So I sing a ... Julia Hmm ... hmm Calls me So I ... for Julia, ... , Julia

Corrigé du devoir n° 7

MANDELBROT ET JULIA

Exercice

Partie A : Ensemble de Mandelbrot

$\begin{cases} z_0 &= 0 \\ z_{n+1} &= z_n^2 + c. \end{cases}$ Si $|z_n|$ est bornée, alors $C \in \mathcal{M}$. Sinon, $|z_n| \xrightarrow[n\to\infty]{} +\infty$ et $C \notin \mathcal{M}$.

1. La suite (u_n) définie par $u_{2k} = 1 + ik^2$, $u_{2k+1} = \frac{i}{k-i}$ n'est pas bornée ($|u_{2k}| > k^2 \xrightarrow[n\to\infty]{} +\infty$) et ne tend pas vers $+\infty$ ($|u_{2k+1}| \leqslant 1$). Cette propriété de la suite (z_n) est donc bien exceptionnelle.

2. Si $c = 0$, on a $z_1 = z_0^2 + 0 = 0^2 + 0 = 0 = z_0$ et $z_n = 0\ \forall n \in \mathbb{N}$: $(z_n)_0$ est bornée donc $O \in \mathcal{M}$.

3. Pour $c = -1$, $z_1 = z_0^2 + c = 0^2 - 1 = -1$, $z_2 = z_1^2 - 1 = 1 - 1 = 0 = z_0$, $z_3 = z_2^2 - 1 = 0 - 1 = z_1$: $z_{2k} = z_0 = 0$ et $z_{2k+1} = z_1 = -1$.
La suite $(z_n)_{-1}$ est bornée donc le point d'affixe -1 appartient à l'ensemble de Mandelbrot $\mathcal{M}$.

4. (a) Pour $c = i$, on a $z_1 = z_0^2 + i = i$, $z_2 = z_1^2 + i = i - 1$,
$z_3 = z_2^2 + i = (i-1)^2 + i = i^2 - 2i + 1 + i = -i$
et $z_4 = z_3^2 + i = (-i)^2 + i = i - 1 = z_2$.
Ainsi, les points M_2 et M_4 sont confondus.

   (b) On a alors $z_5 = z_4^2 + i = (i-1)^2 + i = z_3$ et $z_6 = z_4$: $z_{2k} = z_2$ et $z_{2k+1} = z_3$: la suite $(z_n)_i$ est bornée donc le point d'affixe i appartient à l'ensemble de Mandelbrot $\mathcal{M}$.

5. Pour $c = -i$, on a $z_1 = z_0^2 - i = -i$, $z_2 = z_1^2 - i = -1 - i$,
$z_3 = z_2^2 - i = (-1-i)^2 - i = 1 + 2i + i^2 - i = i$,
$z_4 = z_3^2 - i = i^2 - i = -1 - i = z_2$,
$z_5 = z_4^2 - i = (-1-i)^2 - i = z_3$ et $z_6 = z_4$: $z_{2k} = z_2$ et $z_{2k+1} = z_3$:
la suite $(z_n)_{-i}$ est bornée donc le point d'affixe $-i$ appartient à l'ensemble de Mandelbrot $\mathcal{M}$.

6. Pour $c = 2$, on a $z_1 = z_0^2 + c = 2 \geqslant 2^1$, $z_2 = z_1^2 + c = 2^2 + 2 = 6 \geqslant 2^2$ et $z_3 = z_2^2 + c = 6^2 + 2 = 38 \geqslant 2^3$.
Supposons par récurrence que $z_n \in \mathbb{R}$ et $z_n \geqslant 2^n$ pour un certain $n \geqslant 1$.
On a $2n - 1 \geqslant n$, $z_{n+1} = z_n^2 + 2 \in \mathbb{R}$
et $z_{n+1} = z_n^2 + 2 \geqslant (2^n)^2 + 2 = 2^{2n} + 2 = 2(2^{2n-1} + 1) \geqslant 2.2^n = 2^{n+1}$.
Ainsi, $\forall n \in \mathbb{N}^*$, $z_n \geqslant 2^n$ donc $z_n \xrightarrow[n\to\infty]{} +\infty$ et le point d'affixe 2 n'appartient pas à $\mathcal{M}$.

7. On pose $c = a + ib$ et $z_n = x_n + iy_n$.
On a $z_{n+1} = x_{n+1} + iy_{n+1} = z_n^2 + c = (x_n + iy_n)^2 + a + ib$
$z_{n+1} = x_n^2 + 2ix_ny_n + (iy_n)^2 + a + ib = (x_n^2 - y_n^2 + a) + i(2x_ny_n + b)$
d'où l'expression $\begin{cases} x_0 = y_0 = 0 \\ x_{n+1} = x_n^2 - y_n^2 + a \\ y_{n+1} = 2x_ny_n + b. \end{cases}$

Partie B : Ensembles de Julia $\mathcal{J}_c = \{\omega \in \mathbb{C} / (z_n) \colon z_0 = \omega,\ z_{n+1} = z_n^2 + c \text{ est borné}\}$.

1. On a vu que $O \in \mathcal{M}$ *i.e.* la suite $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 + 0 \end{cases}$ est bornée donc $\omega = 0 \in \mathcal{J}_0$.
On a vu que le point d'abscisse -1 appartient à $\mathcal{M}$ *i.e.* la suite $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 - 1 \end{cases}$ est bornée donc $\omega = 0 \in \mathcal{J}_{-1}$.
On a vu que le point d'abscisse i appartient à $\mathcal{M}$ *i.e.* $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 + i \end{cases}$ est bornée donc $\omega = 0 \in \mathcal{J}_i$.
On a vu que le point d'abscisse $-i$ appartient à $\mathcal{M}$ *i.e.* $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 - i \end{cases}$ est bornée donc $\omega = 0 \in \mathcal{J}_{-i}$.
On a vu que le point d'abscisse 2 n'appartient pas à $\mathcal{M}$ *i.e.* la suite $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 + 2 \end{cases}$ n'est pas bornée donc $\omega = 0 \notin \mathcal{J}_2$.

2. Plus généralement, $C(c) \in \mathcal{M} \iff$ la suite $\begin{cases} z_0 = \omega = 0 \\ z_{n+1} = z_n^2 + c \end{cases}$ est bornée $\iff \omega = 0 \in \mathcal{J}_c$.

3. Pour $c = 0$, la suite $\begin{cases} z_0 = \omega \\ z_{n+1} = z_n^2 \end{cases}$ s'écrit $z_0 = \omega = \omega^{2^0}$, $z_1 = z_0^2 = \omega^2 = \omega^{2^1}$,
$z_2 = z_1^2 = (\omega^2)^2 = \omega^4 = \omega^{2^2}$, $z_3 = z_2^2 = (\omega^4)^2 = \omega^8 = \omega^{2^3}$,
$z_4 = z_3^2 = (\omega^8)^2 = \omega^{16} = \omega^{2^4}$ et, par récurrence, $z_n = \omega^{2^n}$.
Trivialement, si $|\omega| < 1$, alors $|z_n| \xrightarrow[n\to\infty]{} 0$, si $|\omega| > 1$, alors $|z_n| \xrightarrow[n\to\infty]{} +\infty$ et si $|\omega| = 1$ alors $|z_n| = 1$.
Ainsi, $\mathcal{J}_0$ est le disque fermé de centre O et de rayon 1 : $\mathcal{J}_0 = \{\omega \in \mathbb{C} / |\omega| \leqslant 1\}$.

Partie C : Tracé Si $\exists n_0 \in \mathbb{N}$ tel que $|z_{n_0}| \geqslant 2$ alors $C \notin \mathcal{M}$.
L'algorithme suivant permet d'obtenir une superbe image approchée en noir sur fond blanc de l'ensemble de Mandelbrot.

```
IterationMax = 50
Pour chaque pixel C de coordonnées (a;b)
   d2 = a**2+b**2
   x = a
   y = b
   Tant Que (d2 < 4) et (n < IterationMax)
      x = x**2-y**2+a
      y = 2xy+b
      d2 = x**2 + y**2
```

```
      n = n+1
   Fin Tant Que
   Si (n == IterationMax) Alors
      Colorier le pixel en noir
   Sinon
      Colorier le pixel en blanc
   Fin Si
Fin Pour
```

Bonus Vous aurez reconnu l'inoubliable *Julia* des Beatles, sur le magistral Double Blanc, sorti en 1968.

Half of what I say is meaningless
But I say it just to reach you, Julia
Julia, Julia
Oceanchild calls me
So I sing the song of love
Julia
Julia, seashell eyes
Windy smile calls me
So I sing the song of love
Julia
Her hair of floating sky is shimmering
Glimmering in the Sun
Julia, Julia
Morning moon touch me
So I sing the song of love
Julia
When I cannot sing my heart
I can only speak my mind
Julia
Julia, sleeping sand, silent cloud
Touch me
So I sing a song of love
Julia
Hmm hmm hmm
Calls me
So I sing the song of love for
Julia, Julia, Julia

Devoir n° 8

Le plein de Bézout

Ce devoir est associé au chapitre VI, *PGCD et applications*.

Soit a et b deux entiers naturels.
Existe-t-il deux entiers consécutifs tels que le premier soit divisible par a et le second par b ?

Déterminer maintenant trois entiers consécutifs tels que le premier est divisible par 13, le deuxième par 17 et le troisième par 23.

Bonus

Au cours des prochaines vacances, vous allez certainement avoir besoin de vous détendre. Alors je vous conseille la lecture de la trilogie d'Hortense de Jacques Roubaud, en commençant par *La belle Hortense*. Bien que mathématicien, Jacques Roubaud est un individu très amusant. Membre de l'Oulipo et donc adepte de l'écriture avec contraintes, il nous donne à lire un roman plein de trouvailles, intelligemment écrit et très divertissant.

Corrigé du devoir n° 8

LE PLEIN DE BÉZOUT

Soient a, $b \in \mathbb{N}$ et supposons qu'il existe $n \in \mathbb{Z}$ tel que $a \mid n$ et $b \mid n+1$. Il existe alors p et $q \in \mathbb{Z}$ tels que $n = pa$ et $n+1 = qb$ donc $qb - pa = n + 1 - n = 1$. Le théorème de Bézout dit qu'alors a et b sont premiers entre eux.
Réciproquement, si $\mathrm{PGCD}\,(a\,,\,b) = 1$, il existe, d'après Bézout, p et $q \in \mathbb{Z}$ tels que $qb - pa = 1$ et en posant $n = pa$, on a $n+1 = pa+1 = qb$ et l'on a bien $a \mid n$ et $b \mid n+1$.
Ainsi, il existe deux entiers consécutifs tels que le premier soit divisible par a et le second par b si , et seulement si, a et b sont premiers entre eux.

13, 17 et 23 sont premiers entre eux donc le problème semble résoluble et l'on cherche des entiers relatifs p, q et r tels que si $13p = n$, alors $n+1 = 17q$ et $n+2 = 23r$.
On a alors $17q - 13p = n + 1 - 1 = 1$ (Bézout nous avait prévenu) et puisque $-3 \times 17 + 4 \times 13 = 1$ (en remontant l'algorithme d'Euclide de 17 et 13), $(p\,,\,q) = (-4\,,\,-3)$ est une solution particulière de $(E_1)\colon 17q - 13p = 1$.
D'après le théorème de Gauss, après soustraction des équations, on obtient les solutions de (E_1) :

$\mathscr{S}_{(E_1)} = \{(17k-4\,,\,13k-3)\,/k \in \mathbb{Z}\}$.

· De même, on a $23r - 17q = (n+2) - (n+1) = 1$ (Bézout nous avait prévenu) et puisque $3 \times 23 - 4 \times 17 = 1$ (en remontant l'algorithme d'Euclide de 23 et 17), $(q\,,\,r) = (3\,,\,4)$ est une solution particulière de $(E_2)\colon 23r - 17q = 1$.
D'après le théorème de Gauss, après soustraction des équations, on obtient les solutions de de (E_2) :

$\mathscr{S}_{(E_2)} = \{(23k'+4\,,\,17k'+3)\,/k' \in \mathbb{Z}\}$.

· On cherche donc k et $k' \in \mathbb{Z}$ tels que $q_1 = q_2$ c.-à-d. $13k - 3 = 23k' + 4$ $\iff$ $(E_3)\colon 13k - 23k' = 7$ qui admet des solutions car $\mathrm{PGCD}\,(13\,,\,23) = 1 \mid 7$ (merci Bézout). Puisque $4 \times 23 - 7 \times 13 = 1$ (en remontant l'algorithme d'Euclide de 23 et 13), $(k\,,\,k') = (-7\,,\,-4)$ est une solution particulière de $(E_3')\colon 13k - 23k' = 1$ et $(k\,,\,k') = (-49\,,\,-28)$ est une solution particulière de $(E_3)\colon 13k - 23k' = 7$.
· On a alors $q = 13(-49) - 3 = 23(-28) + 4 = -640$
donc $n+1 = 17(-640) = -10\,880$, $n = -10\,881 = 13(-837)$ et $n+2 = -10\,879 = 23(-473)$ sont des solutions du problème.

Devoir n° 9

Les œufs de Nasr Eddin Hodja

Ce devoir est associé au chapitre VI, *PGCD et applications*.

Nasr Eddin Hodja s'en allait au marché sur son âne vendre les œufs de ses poules lorsqu'il rencontra une jeune fille. Il lui fit une proposition qu'elle refusa catégoriquement et, de rage, en cassa tous ses œufs. Celui-ci, fort courroucé, porta l'affaire devant le cadi. Le juge demanda naturellement à Nasr Eddin combien d'œufs avaient été brisés. Nasr Eddin Hodja prétendit ne pas les avoir comptés mais qu'en essayant de les ranger par 2, il en restait un, en les rangeant par 3, il en restait encore un, tout comme par 4, 5 et 6 alors qu'en les rangeant par 7, il n'en restait plus.

1. Traduire cet énoncé par un système de congruence.
2. En déduire que le nombre d'œufs n vérifie $\quad n \equiv 1\,[60] \quad$ et $\quad n \equiv 0\,[7]$.
3. Déterminer l'ensemble des entiers a et b tels que $\quad 7a = 60b + 1$.
4. En déduire le plus petit nombre d'œufs possibles que possédait Nasr Eddin Hodja.

Cependant, la jeune fille exposa la teneur de la proposition que Naser Eddin lui avait faite et le cadi condamna Nasr Eddin, sur le champ et à ses frais, à gober autant d'œufs que ce dont la plainte faisait l'objet.

Corrigé du devoir n° 9

LES ŒUFS DE NASR EDDIN HODJA

1. Soit n le nombre d'oeufs. Ce problème se traduit par le système d'équations de congruence suivant :
   $n \equiv 1\,[2]\,, \quad n \equiv 1\,[3]\,, \quad n \equiv 1\,[4]\,, \quad n \equiv 1\,[5]\,, \quad n \equiv 1\,[6]\,, \quad n \equiv 0\,[7].$
2. On en déduit que $n-1$ est divisible par 2, 3, 4, 5 et 6. En particulier, $n-1$ est divisible par 3, 4 et 5, qui sont premiers entre eux, donc aussi, d'après le corollaire du théorème de Gauss, par leur produit. D'où $n \equiv 1\,[60]$. Et l'on a toujours $n \equiv 0\,[7]$.
3. Cherchons tout d'abord une solution particulière de l'équation $7a = 60b + 1$, équivalente à $7a - 60b = 1$. L'algorithme d'Euclide pour les entiers 60 et 7 donne $60 = 7\times 8+4$, $7 = 4\times 1+3$, $4 = 3\times 1+1$. Puis, on remonte cet algorithme : $1 = 4-3 = 4-(7-4) = 4\times 2-7 = (60-7\times 8)\times 2-7 = 60\times 2-7\times 17$. Le couple $(-17;-2)$ est donc solution de cette équation.
   Soit $(a;b)$ une autre solution de cette équation. Alors on a $7a - 60b = -17\times 7 + 2\times 60$, donc $7\,(a+17) = 60\,(b+2)$. Or 7 et 60 sont premiers entre eux donc, d'après le théorème de Gauss, 7 divise $b+2$.
   Soit c l'entier tel que $b+2 = 7c$. On a alors $7\,(a+17) = 60\times 7c$ et donc $a = 60c - 17$. On en déduit que l'ensemble des solutions est inclus dans $\mathscr{S} = \left\{ \left(60c-17/7c-2\right) ; c \in \mathbb{Z} \right\}$.
   Réciproquement, on vérifie que tout élément de $\mathscr{S}$ est solution.
4. Puisque $n \equiv 0\,[7]$, il existe $a \in \mathbb{Z}$ tel que $n = 7a$. De même, $n \equiv 1[60]$, donc il existe $b \in \mathbb{Z}$ tel que $n = 60b+1$. De tels entiers a et b vérifient donc $n = 7a = 60b+1$. D'après la question précédente, il existe un entier $c \in \mathbb{Z}$ tel que $a = 60c - 17$. La première valeur positive de a étant 43, le plus petit nombre d'oeufs possible de Nasr Eddin Hodja est $n = 7\times 43 = 301$.

Devoir n° 10

Indicatrice chinoise

Ce devoir est associé au chapitre VI, *PGCD et applications.*

<u>Partie A</u> : Théorème des restes chinois

Soient m et n deux entiers naturels premiers entre eux.

On souhaite résoudre le système $\quad (S) : \begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases} \quad$ où a et b sont deux entiers.

1. Démontrer qu'il existe des entiers u et v tels que $\quad \begin{cases} um \equiv 1\,[n] \\ nv \equiv 1\,[m]. \end{cases}$
2. Montrer que $\quad x_0 = bum + van \quad$ est solution de (S).
3. Soit x une solution de (S). Que dire de $x - x_0$? Justifier alors que mn divise $x - x_0$.
4. En déduire les solutions du système (S).
5. Justifier que le système (S) admet une unique solution modulo mn puis énoncer le théorème des restes chinois ainsi démontré.
6. Résoudre le système $\quad (S_1) : \begin{cases} x \equiv 3\,[8] \\ x \equiv 5\,[11]. \end{cases}$
7. Que dire du système $\quad (S_2) : \begin{cases} x \equiv 3\,[9] \\ x \equiv 5\,[6] \end{cases}$?

<u>Partie B</u> : Indicatrice d'Euler

L'indicatrice d'Euler $\varphi(p)$ d'un entier naturel non nul p est le nombre d'entiers naturels non nuls inférieurs ou égaux à p et premiers avec p.

On note $\quad \mathscr{E}_p = \{k \;/\; k \in [\![1\,;p]\!] \text{ et } k \wedge p = 1\}$

et $\quad \mathcal{I}_p = \{k \;/\; k \in [\![1\,;p]\!] \text{ et } k \text{ est inversible modulo } p\}$.

1. Quel est le lien entre $\varphi(p)$, $\mathscr{E}_p$ et $\mathcal{I}_p$?
2. (a) Déterminer $\varphi(9)$ et vérifier que les entiers comptabilisés sont tous inversibles modulo 9.

   (b) Même consigne pour $p = 10$.
3. (a) Rappeler quels sont les entiers inversibles modulo pq pour p, $q \in \mathbb{N}^*$.

   (b) Soient m et n deux entiers naturels premiers entre eux.
   En utilisant le théorème des restes chinois, montrer que l'on peut établir une correspondance, une bijection, entre les ensembles $\mathcal{I}_m \times \mathcal{I}_n$ et $\mathcal{I}_{mn}$.

   (c) Que dire alors de $\varphi(mn)$ lorsque m et n sont deux entiers naturels premiers entre eux ?

Corrigé du devoir n° 10

INDICATRICE CHINOISE

Partie A : Théorème des restes chinois

Soient m et n deux entiers naturels premiers entre eux et $(S): \begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$ où a et b sont deux entiers.

1. Puisque m et n sont premiers entre eux, le théorème de Bézout permet d'affirmer qu'il existe deux entiers u et v tels que $um + nv = 1$.
   Ainsi, $um = 1 - vn \equiv 1\,[n]$ et $nv = 1 - um \equiv 1\,[m]$.
2. Soit $x_0 = bum + van$.
   On a $x_0 = a(vn) + (bu)m \equiv a \times (vn)\,[m] \equiv a \times 1\,[m] \equiv a\,[m]$
   et $x_0 = b(um) + (av)n \equiv b \times (um)\,[n] \equiv b \times 1\,[n] \equiv b\,[n]$.
3. Si x et x_0 sont solutions de $(S): \begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n], \end{cases}$

   alors $\begin{cases} x - x_0 \equiv a - a\,[m] \equiv 0\,[m] \\ x - x_0 \equiv b - b\,[n] \equiv 0\,[n] \end{cases}$ donc m divise $x - x_0$ et n divise $x - x_0$.
   Puisque m et n sont premiers entre eux, la propriété 10 p.140 du cours permet d'affirmer que mn divise $x - x_0$.
4. Ainsi, il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kmn$
   et $x = x_0 + kmn = bum + van + kmn$.
   Réciproquement, un tel $x = bum + van + kmn$ vérifie
   $x = a(vn) + (bu + kn)m \equiv a \times (vn)\,[m] \equiv a \times 1\,[m] \equiv a\,[m]$
   et $x = b(um) + (va + km)n \equiv b \times (um)\,[n] \equiv b \times 1\,[n] \equiv b\,[n]$ donc x est solution de (S).
   Les solutions de (S) sont donc les nombres de la forme $bum + van + kmn$ où $k \in \mathbb{Z}$ et $um + nv = 1$.
5. Soient x et x' deux solution de (S). On sait qu'il existe alors deux entiers k et k' tels que $x - x_0 = kmn$ et $x' - x_0 = k'mn$.
   Ainsi, $x - x' = (k - k')mn \equiv 0\,[mn]$ et $x' \equiv x\,[mn]$: les solutions de (S) sont bien uniques modulo mn.
   On a donc démontré le théorème des restes chinois suivants :
   Si m et n sont deux entiers naturels premiers entre eux, alors, pour tous entiers a et b, le système $\begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$ admet toujours des solutions. De plus, ces solutions sont uniques modulo mn.
6. Pour $a = 3$, $b = 5$, $m = 8$ et $n = 11$, le système (S_1) s'écrit $\begin{cases} x \equiv 3\,[8] \\ x \equiv 5\,[11]. \end{cases}$
   Puisque $m \wedge n = 8 \wedge 11 = 1$, (S_1) admet une unique solution modulo $mn = 8 \times 11 = 88$.

Cherchons x_0 c.-à-d. u et v. On a $11 = 8 \times 1 + 3$, $8 = 3 \times 2 + 2$ et $3 = 2 \times 1 + 1$
donc $1 = 3 - 2 = 3 - (8 - 3 \times 2) = 3 \times 3 - 8 = 3(11 - 8) - 8 = -4 \times 8 + 3 \times 11$: $u = -4$, $v = 3$.
D'où $x_0 = bum + van = 5 \times (-4) \times 8 + 3 \times 3 \times 11 = -61$ et l'on a $x_0 = -61 = 3 - 8 \times 8 \equiv 3\,[8]$ et $x_0 = -61 = 5 - 6 \times 11 \equiv 5\,[11]$: $x_0 = -61$ est bien une solution de (S).
Les solutions de (S_1) sont donc les entiers congrus à -61 modulo 88 :
$\mathscr{S}_1 = \{88k - 61 \;/\; k \in \mathbb{Z}\}$.

7. Pour $a = 3$, $b = 5$, $m = 9$ et $n = 6$, le système (S_2) s'écrit $\begin{cases} x \equiv 3\,[9] \\ x \equiv 5\,[6]. \end{cases}$
   Puisque $m \wedge n = 9 \wedge 6 = 3 \neq 1$, (S_2) n'admet pas de solution. En effet, si $x = 3 + 9k = 5 + 6k'$, alors $5 = 3 + 9k - 6k' = 3(1 + 3k - 2k')$ et 3 divise 5, ce qui est absurde. $\mathscr{S}_2 = \varnothing$.

Partie B : Indicatrice d'Euler
$\mathscr{E}_p = \{k \;/\; k \in [\![1 ; p]\!] \text{ et } k \wedge p = 1\}$, $\mathcal{I}_p = \{k \;/\; k \in [\![1 ; p]\!] \text{ et } k \text{ inversible modulo } p\}$.

1. Par définition de l'indicatrice d'Euler φ, on a, pour $p \in \mathbb{N}^*$, $\varphi(p) = \mathrm{Card}(\mathscr{E}_p)$.
   D'après la propriété 8 du cours, on sait que $k \in \mathbb{Z}$ est inversible modulo $p \in \mathbb{N}^*$ si, et seulement si, k et p sont premiers entre eux donc $\mathscr{E}_p = \mathcal{I}_p$.
   On a donc aussi $\varphi(p) = \mathrm{Card}(\mathcal{I}_p)$.
2. (a) On a $\mathscr{E}_9 = \{1 ; 2 ; 4 ; 5 ; 7 ; 8\}$ donc $\varphi(9) = \mathrm{Card}(\mathscr{E}_9) = 6$.
   Par ailleurs, $2 \times 5\,[9] \equiv 4 \times 7\,[9] \equiv 8 \times 8\,[9] \equiv 1\,[9]$ et ni 3 ni 6 ne sont inversibles modulo 9 : les entiers de $\mathscr{E}_9$ sont bien les inversibles modulo 9.
   (b) On a $\mathscr{E}_{10} = \{1 ; 3 ; 7 ; 9\}$ donc $\varphi(10) = \mathrm{Card}(\mathscr{E}_{10}) = 4$. Par ailleurs, $3 \times 7\,[10] \equiv 9 \times 9\,[10] \equiv 1\,[10]$ et 2, 4, 5, 6, 8 ne sont inversibles pas modulo 10 : les entiers de $\mathscr{E}_{10}$ sont bien les inversibles modulo 10.
3. (a) D'après la propriété 13 du cours, les entiers inversibles modulo pq sont exactement ceux inversibles modulo p et modulo q.
   (b) Soit $c \in [\![0 ; mn - 1]\!]$.
   Par définition, c est inversible modulo $m \iff \exists a \in \mathcal{I}_m$ tel que $c \equiv a\,[m]$
   et c est inversible modulo $n \iff \exists b \in \mathcal{I}_n$ tel que $c \equiv b\,[n]$.
   D'après 3a, $c \in \mathcal{I}_{mn} \iff \exists\,(a, b) \in \mathcal{I}_m \times \mathcal{I}_n$ tel que $\begin{cases} c \equiv a\,[m] \\ c \equiv b\,[n]. \end{cases}$
   Il est clair que pour chaque c, il existe un unique a tel que $c \equiv a\,[m]$: $a \equiv c\,[m]$. De même pour l'unicité de b.
   Par ailleurs, d'après le théorème des restes chinois, pour chaque (a, b), il existe un unique entier modulo mn vérifiant ce système et donc un unique $c \in [\![0 ; mn - 1]\!]$.
   À chaque entier c de $\mathcal{I}_{mn}$ correspond donc un unique couple (a, b) de $\mathcal{I}_m \times \mathcal{I}_n$ et réciproquement. On dit que les ensembles $\mathcal{I}_{mn}$ et $\mathcal{I}_m \times \mathcal{I}_n$ sont équipotents : ils sont en bijection, en correspondance, l'un avec l'autre.
   (c) $\varphi(mn) = \mathrm{Card}(\mathcal{I}_{mn}) = \mathrm{Card}(\mathcal{I}_m \times \mathcal{I}_n) = \mathrm{Card}(\mathcal{I}_m)\,\mathrm{Card}(\mathcal{I}_n) = \varphi(m)\varphi(n)$.

Devoir n° 11

DES FOURMIS ET DES HOMMES

Ce devoir est associé au chapitre VII, *Graphes*.

Exercice 1 Alpinisme myrmicéen

Deux téméraires fourmis se promènent sur les arêtes effilées d'un octaèdre régulier. Chaque fois qu'elles atteignent un sommet, elles admirent le paysage, comme il se doit, puis enchaînent par une des arêtes adjacentes, au hasard de leurs envies et des conditions climatiques. Quelle est la probabilité que notre aventureuse cordée soit revenue au sommet de départ après un épique trajet long de huit arêtes ?

Exercice 2 Feux interdits

Ton professeur de mathématiques te lance un défi : le battre au jeu des allumettes dont la règle est la suivante.

On dispose des tas de trois allumettes. À tour de rôle, les joueurs retirent au choix une ou deux allumettes de l'un des tas. Celui qui retire la dernière allumette a perdu. Étant manifestement le plus jeune, ton professeur te laisse commencer.

1. Que dois-tu jouer pour être certain de gagner si vous disposez d'un seul tas de trois allumettes ?
2. Que dois-tu jouer pour être certain de gagner si vous disposez de deux tas de trois allumettes ?
3. Que dois-tu jouer pour être certain de gagner si vous disposez de trois tas de trois allumettes ?
4. Que dois-tu jouer pour être certain de gagner si vous disposez de $n \geqslant 1$ tas de trois allumettes ?

Bonus

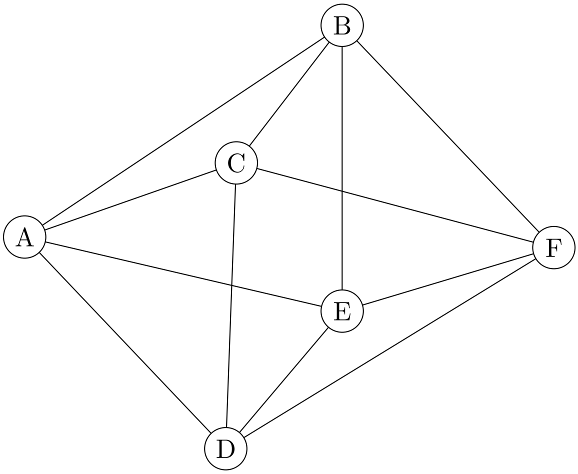
Voyagez donc avec *Le Mont Analogue*, brillant roman inachevé d'aventures alpines, non euclidiennes et symboliquement authentiques de René Daumal.

Corrigé du devoir n$^{\text{o}}$ 11

Des fourmis et des hommes

Exercice 1 Alpinisme myrmicéen

L'octaèdre régulier peut être modélisé par le graphe suivant :



La matrice de ce graphe est alors $M = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

et l'on a $M^8 = \begin{pmatrix} 11008 & 10880 & 10880 & 10880 & 10880 & 11008 \\ 10880 & 11008 & 10880 & 11008 & 10880 & 10880 \\ 10880 & 10880 & 11008 & 10880 & 11008 & 10880 \\ 10880 & 11008 & 10880 & 11008 & 10880 & 10880 \\ 10880 & 10880 & 11008 & 10880 & 11008 & 10880 \\ 11008 & 10880 & 10880 & 10880 & 10880 & 11008 \end{pmatrix}$.

D'après les éléments diagonaux de M^8, il y a 11 008 chaînes de longueur 8 partant d'un des sommets et revenant sur lui-même.

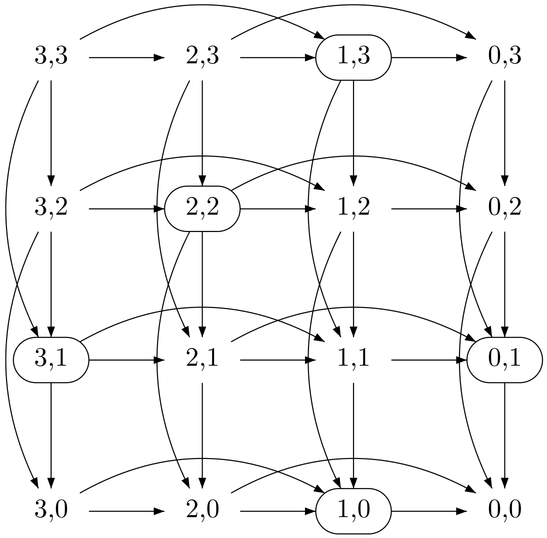
En sommant les termes d'une ligne (ou d'une colonne) quelconque, on obtient un total de $4 \times 10\,880 + 2 \times 11008 = 65\,536$ chaînes de longueur 8 partant d'un sommet quelconque de l'octaèdre.

Il y a donc une probabilité de $\frac{11008}{65536} = \frac{43}{256}$ pour que notre cordée de téméraires fourmis revienne au sommet de départ après son ascension de huit arêtes.

On peut remarquer que cette probabilité est légèrement supérieure à $\frac{1}{6}$.

Exercice 2 Feux interdits

1. Si vous disposez d'un seul tas de trois allumettes, il te suffit de retirer 2 allumettes pour que ton professeur soit obligé de retirer la dernière.
2. Si vous disposez de deux tas de trois allumettes, tu peux dresser le graphe des différentes combinaisons.



   Après analyse de ce graphe, tu remarques que si tu arrives te déplacer sur les positions entourées, tu es certain de gagner car quoi qu'il joue alors, tu pourras rejoindre la position 1,0 ou 0,1. Tu vas donc astucieusement retirer 2 allumettes lors de ton premier coup !

3. Si vous disposez de trois tas de trois allumettes, tu peux imaginer le graphe précédent surmonté de trois niveaux similaires pour les quatre états distincts du nouveau tas. Tu remarques qu'en retirant encore deux allumettes, tu pourras, au coup d'après, rejoindre une position gagnante connue. En effet, il peut jouer ton 133 en 033 (qui est comme le 33 précédent : tu sais quoi faire) ou en 113 (et tu le ramènes à alors 013) ou en 123 (et tu peux aussi revenir à 103).
4. Si vous disposez de $n \geqslant 1$ tas de trois allumettes, tu retires deux allumettes et tu le ramènes à la situation précédente avec plus de 3 : il te suffit de garder le cap et de revenir à 3...3 ou 13...3 à chacun de tes coups. Tu es donc certain de terrasser ton professeur.

CORRIGÉS

Devoir n° 12

Napoléon Van Aubel

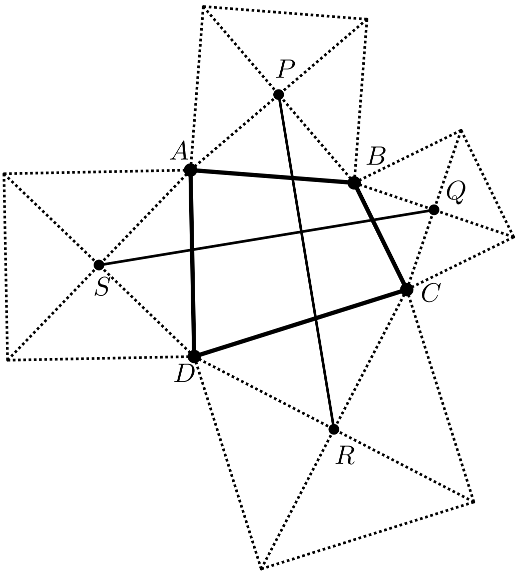
Ce devoir est associé au chapitre VIII, *Nombres complexes : compléments*.

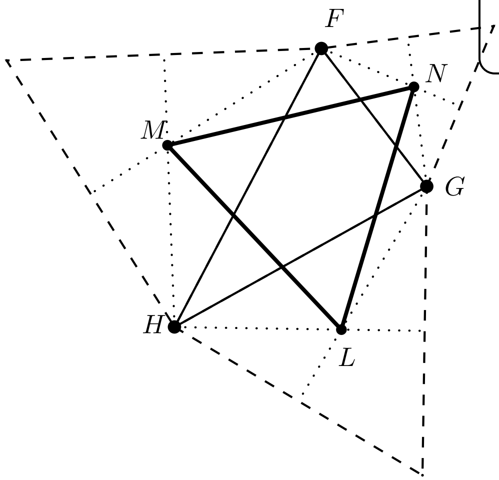
Exercice 1 Théorème de Van Aubel

Soient A, B, C et D quatre points quelconques distincts du plan complexe.
On construit, à l'extérieur du quadrilatère $ABCD$ et en tournant autour, quatre carrés portés par les côtés de $ABCD$, carrés de centres P, Q, R et S comme sur la figure suivantes.
Démontrer que $PR = QS$ et $(PR)\perp(QS)$.
Indications : on pourra déterminer l'affixe de P en fonction de celles de A et B puis calculer $i.z_{\overrightarrow{PR}}$.

Exercice 2 Théorème de Napoléon

Soient F, G et H trois points quelconques distincts du plan complexe.
On construit, à l'extérieur du triangle FGH, trois triangles équilatéraux portés par les côtés de FGH, triangles de centres L, M et N comme sur la figure suivante.
Démontrer que le triangle LMN est équilatéral.





EXERCICES

Corrigé du devoir n° 12
Napoléon Van Aubel

Exercice 1 Théorème de Van Aubel

On nomme a, b, c, d, p, q, r et s les affixes des points éponymes.
Puisque $PA = PB$ et $(PA)\perp(PB)$,
on a $\frac{b-p}{a-p} = 1e^{i\frac{\pi}{2}} = i \iff b-p = i(a-p) \iff (i-1)p = ia - b$.
De même, $(i-1)q = ib - c$, $(i-1)r = ic - d$ et $(i-1)s = id - a$.
Ainsi, $(i-1)(q-s) = (ib-c) - (id-a) = i(b-d) - (c-a)$
et $(i-1)(r-p)\times i = ((ic-d)-(ia-b))\times i = i^2(c-a) - i(d-b) = i(b-d) - (c-a)$
$= (i-1)(q-s)$.
D'où, $\frac{q-s}{r-p} = i = 1e^{i\frac{\pi}{2}}$ c.-à-d. $z_{\overrightarrow{SQ}} = i.z_{\overrightarrow{PR}}$
et l'on a bien $(SQ)\perp(PR)$ et $SQ = PR$.

On peut remarquer que si le quadrilatère $ABCD$ est direct, il suffit de changer $\frac{\pi}{2}$ en $-\frac{\pi}{2}$ c.-à-d. i en $-i$ dans les premières identités et l'on obtient le même résultat. De même si le quadrilatère est croisé mais il faut bien faire attention à construire les carrés du bon côtés.

Exercice 2 Théorème de Napoléon

On nomme f, g, h, ℓ, m et n les affixes des points éponymes et l'on définit $j = e^{i\frac{2\pi}{3}}$.
On a $e^{i\frac{\pi}{3}} = j+1$ et $j^2 = -j-1$.
Par construction, G est l'image de F par la rotation de centre N et d'angle $\frac{2\pi}{3}$ donc
$g - n = 1e^{i\frac{2\pi}{3}}(f-n) = j(f-n) \iff (j-1)n = jf - g$.
De même, $(j-1)\ell = jg - h$ et $(j-1)m = jh - f$.
Ainsi, $(j-1)(\ell - n) = (jg-h) - (jf-g) = j(g-f) - (h-g)$
et
$$\begin{aligned}(j-1)(m-n)\times e^{i\frac{\pi}{3}} &= ((jh-f)-(jf-g))\times(j+1)\\
&= (j+1)j(h-f) - (j+1)(f-g)\\
&= j^2(h-f) + j(h-f) - j(f-g) - (f-g)\\
&= (-j-1)(h-f) + j(h-f-f+g) - (f-g)\\
&= j(-h+f+h-2f+g) - (h-f+f-g)\\
&= j(g-f) - (h-g)\\
&= (j-1)(\ell-n).\end{aligned}$$
D'où, $\frac{\ell-n}{m-n} = e^{i\frac{\pi}{3}}$ c.-à-d. $z_{\overrightarrow{NL}} = e^{i\frac{\pi}{3}}.z_{\overrightarrow{NM}}$ et L est l'image de M par la rotation de centre N et d'angle $\frac{\pi}{3}$: le triangle LMN est bien équilatéral.

On peut remarquer que si le triangle FGH est direct, il suffit de changer $\frac{2\pi}{3}$ et $-\frac{2\pi}{3}$ c.-à-d. j en $\overline{j}$ et l'on obtient le même résultat. De même, on peut construire les triangles à l'intérieur sans changer le résultat.

Devoir n° 13

Génération $\mathbb{U}_n$

Ce devoir est associé au chapitre VIII, *Nombres complexes : compléments*.

Exercice

1. Soit $n \geqslant 2$ un entier naturel.
   (a) Soit ω une racine n-ième de l'unité.
   Démontrer que pour tout $k \in \mathbb{N}$, ω^k est une racine n-ième de l'unité.
   (b) Montrer que, plus généralement, $\mathbb{U}_n$ est stable par produit et par passage à l'inverse.
2. (a) Soit la racine troisième de l'unité $\omega = j^2 = e^{-i\frac{2\pi}{3}}$.
   Déterminer ω^k pour $k \in [\![0\,;2]\!]$. Que remarque-t-on ?
   On dit que les puissances de j^2 génèrent $\mathbb{U}_3$.
   (b) Soit la racine cinquième de l'unité $\omega = e^{i\frac{4\pi}{5}}$.
   Déterminer ω^k pour $k \in [\![0\,;4]\!]$. Que remarque-t-on ?
   (c) Faire de même avec la racine cinquième de l'unité $\omega' = e^{-i\frac{2\pi}{5}}$.
   (d) Que dire dans $\mathbb{U}_4$? Et dans $\mathbb{U}_6$?
3. (a) Soit $n \geqslant 2$ un entier naturel. On pose $\omega_1 = e^{i\frac{2\pi}{n}}$. Justifier que les puissances de ω_1 génèrent $\mathbb{U}_n$.
   (b) Pour tout $k \in \mathbb{N}$, on pose $\quad \omega_k = (\omega_1)^k = e^{i\frac{2k\pi}{n}}$.
   Montrer que $\quad \omega_k = \omega_{k'} \iff k \equiv k'\,[n]$.
   (c) On suppose que k et n sont premiers entre eux : $\quad k \wedge n = 1$.
   Montrer que, pour tous entiers p, q tels que $0 \leqslant q \leqslant p \leqslant n-1$,
   $\omega_k^p = \omega_k^q \iff p = q$.
   (d) En déduire que, si $k \wedge n = 1$, les puissances de ω_k génèrent $\mathbb{U}_n$.
4. (a) Réciproquement, on suppose que $\quad k \wedge n = d \geqslant 2. \quad$ Calculer $\quad (\omega_k)^{\frac{n}{d}}$.
   (b) En déduire que les puissances de ω_k ne génèrent pas $\mathbb{U}_n$.
5. Conclure.

Bonus

Je me dois de vous conseiller *L'Anomalie* d'Hervé Le Tellier, prix Goncourt 2020. Président de l'Oulipo, d'une formation mathématique, il signe ici un roman de romans jubilatoire inspiré par une science-fiction postmoderne, tendance cyberpunk. Le Tellier lui-même décrit son roman comme un « scoubidou » et pose, *in fine*, plusieurs questions sur la réalité du monde et la fiction. À lire et à relire.

Corrigé du devoir nº 13

GÉNÉRATION $\mathbb{U}_n$

Exercice

1. (a) Soit $n \geqslant 2$, $k \in \mathbb{N}$ et $\omega \in \mathbb{U}_n$. On a $(\omega^k)^n = (\omega^n)^k = 1^k = 1$ donc $\omega^k \in \mathbb{U}_n$.

   (b) Soit ω, $\omega' \in \mathbb{U}_n$. On a $\quad (\frac{1}{\omega})^n = \frac{1}{\omega^n} = \frac{1}{1} = 1 \quad$ donc $\quad \frac{1}{\omega} \in \mathbb{U}_n$
   et $\quad (\omega\omega')^n = \omega^n(\omega')^n = 1 \times 1 = 1 \quad$ donc $\quad \omega\omega' \in \mathbb{U}_n$.
   $\mathbb{U}_n$ est donc stable par produit et par passage à l'inverse.

2. (a) On a $\quad \omega = j^2 = e^{-i\frac{2\pi}{3}} \quad$ donc $\quad \omega^0 = 1, \quad \omega^1 = \omega = j^2 \quad$ et
   $\omega^2 = (j^2)^2 = j^4 = j^3.j = 1j = j \quad$ et l'on remarque que
   $\{\omega^k \ / \ k \in [\![\, 0\,;2\,]\!]\} = \{1; j; j^2\} = \mathbb{U}_3$: $\quad$ les puissances de j^2 génèrent $\mathbb{U}_3$.

   (b) On a $\quad \omega = e^{i\frac{4\pi}{5}} \quad$ donc $\omega^0 = 1$, $\omega^1 = \omega = e^{i\frac{4\pi}{5}}$, $\omega^2 = (e^{i\frac{4\pi}{5}})^2 = e^{i\frac{8\pi}{5}}$, $\omega^3 = (e^{i\frac{4\pi}{5}})^3 = e^{i\frac{12\pi}{5}} = e^{i\frac{2\pi}{5}}$ et $\omega^4 = (e^{i\frac{4\pi}{5}})^4 = e^{i\frac{16\pi}{5}} = e^{i\frac{6\pi}{5}}$.
   On remarque que $\quad \{\omega^k \ / \ k \in [\![\, 0\,;4\,]\!]\} = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![\, 0\,;4\,]\!]\} = \mathbb{U}_5$: $\quad$ les puissances de ω génèrent $\mathbb{U}_5$.

   (c) On a $\quad \omega' = e^{-i\frac{2\pi}{5}} \quad$ donc $\quad (\omega')^0 = 1, \quad (\omega')^1 = \omega' = e^{-i\frac{2\pi}{5}} = e^{i\frac{8\pi}{5}}$, $(\omega')^2 = (e^{-i\frac{2\pi}{5}})^2 = e^{-i\frac{4\pi}{5}} = e^{i\frac{6\pi}{5}}$, $\quad (\omega')^3 = (e^{-i\frac{2\pi}{5}})^3 = e^{-i\frac{6\pi}{5}} = e^{i\frac{4\pi}{5}} \quad$ et $(\omega')^4 = (e^{-i\frac{2\pi}{5}})^4 = e^{-i\frac{8\pi}{5}} = e^{i\frac{2\pi}{5}}$.
   On remarque que $\quad \{(\omega')^k \ / \ k \in [\![\, 0\,;4\,]\!]\} = \{e^{i\frac{2k\pi}{5}} \ / \ k \in [\![\, 0\,;4\,]\!]\} = \mathbb{U}_5$: les puissances de ω génèrent $\mathbb{U}_5$.

   (d) Dans $\quad \mathbb{U}_4 = \{1; i; -1; -i\}$, $\quad$ si $\quad e^{i\frac{2\pi}{4}} = e^{i\frac{\pi}{2}} = i \quad$ et $\quad e^{i\frac{6\pi}{4}} = e^{-i\frac{\pi}{2}} = -i$ génèrent bien $\mathbb{U}_4$, il n'en est pas de même pour $\quad e^{i\frac{4\pi}{4}} = e^{i\pi} = -1$:
   $$\{(-1)^k \ / \ k \in [\![\, 0\,;3\,]\!]\} = \{1; -1\} \neq \mathbb{U}_4.$$
   Dans $\quad \mathbb{U}_6 = \{1; e^{i\frac{\pi}{3}}; e^{i\frac{2\pi}{3}}; -1; e^{i\frac{4\pi}{3}}; e^{i\frac{5\pi}{3}}\}$, $\quad$ si $\quad e^{i\frac{\pi}{3}} \quad$ et $\quad e^{i\frac{5\pi}{3}} \quad$ génèrent bien $\mathbb{U}_6$, il n'en est pas de même pour les autres. En effet,
   $$\begin{aligned}\{e^{i\frac{5\pi}{3}} \ / \ k \in [\![\, 0\,;5\,]\!]\} &= \{e^{i\frac{0\pi}{3}}; e^{i\frac{5\pi}{3}}; e^{i\frac{10\pi}{3}}; e^{i\frac{15\pi}{3}}; e^{i\frac{20\pi}{3}}; e^{i\frac{25\pi}{3}}\} \\ &= \{1; e^{i\frac{5\pi}{3}}; e^{i\frac{4\pi}{3}}; -1; e^{i\frac{2\pi}{3}}; e^{i\frac{\pi}{3}}\} = \mathbb{U}_6, \\ \{e^{i\frac{4\pi}{3}} \ / \ k \in [\![\, 0\,;5\,]\!]\} &= \{e^{i\frac{0\pi}{3}}; e^{i\frac{4\pi}{3}}; e^{i\frac{8\pi}{3}}; e^{i\frac{12\pi}{3}}; e^{i\frac{16\pi}{3}}; e^{i\frac{20\pi}{3}}\} \\ &= \{1; e^{i\frac{4\pi}{3}}; e^{i\frac{2\pi}{3}}; 1; e^{i\frac{4\pi}{3}}; e^{i\frac{2\pi}{3}}\} \neq \mathbb{U}_6.\end{aligned}$$

3. (a) Pour $n \geqslant 2$ et $\omega_1 = e^{i\frac{2\pi}{n}}$, on a trivialement
   $$\{\omega_1^k \ / \ k \in [\![\, 0\,;n-1\,]\!]\} = \{e^{i\frac{2k\pi}{n}} \ / \ k \in [\![\, 0\,;n-1\,]\!]\} = \mathbb{U}_n.$$

   (b) Soient k, $k' \in \mathbb{N}$. On a $\quad \omega_k = \omega_{k'} \iff e^{i\frac{2k\pi}{n}} = e^{i\frac{2k'\pi}{n}} \iff \dfrac{e^{i\frac{2k\pi}{n}}}{e^{i\frac{2k'\pi}{n}}} = 1$
   $$\iff e^{i\frac{2(k-k')\pi}{n}} = e^{i0} \iff \frac{2(k-k')\pi}{n} \equiv 0\,[2\pi] \iff \frac{k-k'}{n} \equiv 0\,[1]$$
   $$\iff k - k' \equiv 0\,[n] \iff k \equiv k'\,[n].$$

   (c) Soient k, p, $q \in \mathbb{N}$ tels que $\quad k \wedge n = 1 \quad$ et $\quad 0 \leqslant q \leqslant p \leqslant n-1$.
   On a $\quad \omega_k^p = \omega_k^q \iff (e^{i\frac{2k\pi}{n}})^p = (e^{i\frac{2k\pi}{n}})^q \iff e^{i\frac{2k\pi}{n}(p-q)} = e^{i0}$

$$\begin{aligned}\omega_k^p = \omega_k^q &\iff \tfrac{2k\pi}{n}(p-q) \equiv 0\,[2\pi] \iff \tfrac{(p-q)k}{n} \equiv 0\,[1]\\ &\iff (p-q)k \equiv 0\,[n] \iff n\,|\,(p-q)k\\ &\overset{Gauss}{\iff} n\,|\,p-q \overset{0\leqslant p-q\leqslant n-1}{\iff} p-q=0 \iff p=q.\end{aligned}$$

(d) Ainsi, les puissances entre 0 et $n-1$ de ω_k sont toutes distinctes. D'où, $\{(\omega_k)^p \ / \ p \in [\![\,0\,;n-1\,]\!]\}$ est inclus dans $\mathbb{U}_n$ et de même cardinal n (nombre d'éléments). C'est donc exactement $\mathbb{U}_n$: les puissances de ω_k génèrent bien $\mathbb{U}_n$.

4. (a) Si $k \wedge n = d \geqslant 2$, il existe p et $q \in \mathbb{N}^*$ tels que $n = dp$, $k = dq$.
On a $\frac{n}{d} = p \in [\![\,1\,;n-1\,]\!]$
et $(\omega_k)^{\frac{n}{d}} = (e^{i\frac{2k\pi}{n}})^{\frac{dp}{d}} = e^{i\frac{2dq\pi}{dp}.p} = e^{i.2\pi q} = e^{i0} = 1.$

(b) Ainsi, $(\omega_k)^{p+1} = (\omega_k)^p.\omega_k = (\omega_k)^1$, $(\omega_k)^{p+2} = (\omega_k)^p.(\omega_k)^2 = (\omega_k)^2$,... $(\omega_k)^{p+p} = (\omega_k)^p.(\omega_k)^p = 1$.
D'où, $\{(\omega_k)^\ell \ / \ \ell \in [\![\,0\,;n-1\,]\!]\} = \{(\omega_k)^\ell \ / \ \ell \in [\![\,0\,;p-1\,]\!]\}$ est de cardinal inférieur ou égal à p donc strictement inférieur à n : il existe donc une racine n-ième de l'unité (ω_k) dont les puissances ne génèrent pas $\mathbb{U}_n$.

5. Les puissances de $\omega_k = e^{i\frac{2k\pi}{n}}$ génèrent $\mathbb{U}_n$ si, et seulement si, k et n sont premiers entre eux.

Devoir n° 14

Chiffrement RSA

Ce devoir est associé au chapitre IX, *Nombres Premiers*.

Le but de ce problème est d'étudier une méthode de cryptage à clé publique d'une information numérique, méthode appelée système RSA en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman qui ont inventé cet outil de cryptage en 1977 et l'ont publié en 1978.
La partie A introduit la méthode sur des exemples : les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage et la question 4, le décryptage. La partie B la justifie.

Partie A :

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.
   (a) Vérifier que $8^7 \equiv 2\,[55]$. En déduire le reste dans la division euclidienne par 55 du nombre 8^{21}.
   (b) Vérifier que $8^2 \equiv 9\,[55]$ puis déduire de la question (a) le reste dans la division euclidienne par 55 de 8^{23}.
2. Dans cette question, on considère l'équation $(E) : 23x - 40y = 1$, dont les solutions sont des couples $(x\ ;\ y)$ d'entiers relatifs.
   (a) Justifier que l'équation (E) admet au moins un couple solution.
   (b) Donner un couple, solution particulière de l'équation (E).
   (c) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).
   (d) En déduire qu'il existe un unique entier d vérifiant les conditions
   $0 \leqslant d < 40$ et $23d \equiv 1\,[40]$.
3. Cryptage dans le système RSA
   Alice choisit deux nombres premiers distincts p et q, puis calcule $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n.
   Alice publie le couple $(N\ ;\ c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$. Pour crypter un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c et le nombre crypté est l'entier b.
   Dans la pratique, cette méthode est sûre si Alice choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres. On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$. Alice choisit également $c = 23$.

(a) Calculer les nombres N et n, puis justifier que la valeur de c vérifie la condition voulue.

(b) Bob souhaite envoyer à Alice le nombre $a = 8$. Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA

Alice calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1\,[n]$. Elle garde secret ce nombre d qui lui permet, à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique. Pour décrypter un nombre crypté b, Alice calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a. On admet pour l'instant l'existence et l'unicité de l'entier d et le fait que le décryptage fonctionne. Les nombres choisis par Alice sont encore $p = 5$, $q = 11$ et $c = 23$.

(a) Quelle est la valeur de d ?

(b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.

Partie B :

p et q sont deux nombres premiers distincts, $N = pq$, $n = (p-1)(q-1)$ et $c < n$ est premier avec n.

La clef publique est $(N\,,\,c)$. Le principe est donc le suivant : pour transmettre l'entier a, on envoie b tel que $a^c \equiv b\,[N]$. Pour déchiffrer b, on calcule a tel que $b^d \equiv a\,[N]$, où d est la clef privée.

1. Petit théorème de Fermat

(a) Soit a un entier naturel premier avec p et q.
Montrer que $a^{(p-1)(q-1)} \equiv 1\,[p]$ et $a^{(p-1)(q-1)} \equiv 1\,[q]$.

(b) En déduire que $a^{(p-1)(q-1)} \equiv 1\,[N]$.

(c) Démontrer que pour tout entier naturel a,
si $k \equiv 1\,[n]$, alors $a^k \equiv a\,[N]$.

2. Détermination de d

(a) Justifier que l'équation $(E)\colon cx - ny = 1$ admet des solutions entières.

(b) Soit $(x_0\,,\,y_0)$ une solution particulière de (E).
Montrer que le couple d'entiers $(x\,,\,y)$ est solution de (E) si, et seulement si, $x = x_0 + kn$ et $y = y_0 + kc$ où $k \in \mathbb{Z}$.

(c) En déduire qu'il existe un unique entier naturel $d < n$ tel que $dc \equiv 1\,[n]$.

3. Conclusion

Montrer que, quels que soient les entiers naturels a et b, on a
$b \equiv a^c\,[N] \Longrightarrow b^d \equiv a\,[N]$.

La sécurité de cette méthode tient pour l'essentiel dans la difficulté de trouver n et donc d lorsque l'on connaît N. En effet, il n'existe pas encore de méthode vraiment efficace pour déterminer la factorisation $N = pq$ lorsque p et q sont très grands. Heureusement car la plupart de nos échanges et transactions sont cryptés au moyen du système RSA, mais que se passera-t-il lorsque cela sera possible ?

Corrigé du devoir n° 14

CHIFFREMENT RSA

Partie A :

1. (a) • $8^3 = 512 = 9 \times 55 + 17$ donc $8^3 \equiv 17\,[55]$.
   • $8^6 = \left(8^3\right)^2 \equiv 17^2\,[55]$, $17^2 = 289 = 5 \times 55 + 14 \equiv 14\,[55]$ donc $8^6 \equiv 14\,[55]$.
   • $8^7 = 8^6 \times 8 \equiv 14 \times 8\,[55]$. Puisque $14 \times 8 = 112 = 2 \times 55 + 2 \equiv 2\,[55]$, $8^7 \equiv 2\,[55]$.

   Ainsi, $8^{21} = \left(8^7\right)^3 \equiv 2^3\,[55]$ donc $8^{21} \equiv 8\,[55]$.

   (b) $8^2 = 64 = 1 \times 55 + 9 \equiv 9\,[55]$, $8^{23} = 8^{21} \times 8^2 \equiv 8 \times 9\,[55]$
   et $8 \times 9 = 72 = 1 \times 55 + 17 \equiv 17\,[55]$ donc $8^{23} \equiv 17\,[55]$.
   Or $0 \leqslant 17 < 55$ donc 17 est le reste de la division de 8^{23} par 55.

2. (a) 23 est un nombre premier et 40 n'est pas un multiple de 23 donc les nombres 23 et 40 sont premiers entre eux et, d'après le théorème de Bézout, l'équation $(E)\colon 23x - 40y = 1$ admet au moins un couple solution.

   (b) On détermine une solution particulière de l'équation (E) par divisions euclidiennes successives :

$40 = 1 \times 23 + 17$	$23 \times (-1) + 40 \times 1 = 17$
$23 = 1 \times 17 + 6$	$23 \times 1 + 17 \times (-1) = 6$
	$23 \times 1 + (23 \times (-1) + 40 \times 1) \times (-1) = 6$
	$23 \times 2 + 40 \times (-1) = 6$
$17 = 2 \times 6 + 5$	$17 \times 1 + 6 \times (-2) = 5$
	$(23 \times (-1) + 40 \times 1) \times 1 + (23 \times 2 + 40 \times (-1)) \times (-2) = 5$
	$23 \times (-5) + 40 \times 3 = 5$
$6 = 5 \times 1 + 1$	$6 \times 1 + 5 \times (-1) = 1$
	$(23 \times 2 + 40 \times (-1)) \times 1 + (23 \times (-5) + 40 \times 3) \times (-1) = 1$
	$23 \times 7 + 40 \times (-4) = 1$

   On arrive à $23 \times 7 + 40 \times (-4) = 1$ donc $23 \times 7 - 40 \times 4 = 1$.
   Le couple $(7, 4)$ est solution de l'équation (E).

   (c) • Le couple (x, y) est solution de (E) : $23 \times x - 40 \times y = 1$
   Le couple $(7, 4)$ est solution de (E) : $23 \times 7 - 40 \times 4 = 1$
   Par soustraction membre à membre : $23\,(x - 7) - 40\,(y - 4) = 0$
   On déduit donc que $23\,(x - 7) = 40\,(y - 4)$ donc 23 divise $40\,(y - 4)$.
   Or 23 et 40 sont premiers entre eux donc, d'après le théorème de Gauss, 23 divise $y - 4$.
   On a donc $y - 4 = 23k$ avec $k \in \mathbb{Z}$, c'est-à-dire $y = 4 + 23k$.

CORRIGÉS

$23\,(x-7) = 40\,(y-4)$ et $y-4 = 23k$ donc
$23\,(x-7) = 40 \times 23k$ et $x-7 = 40k$, c'est-à-dire $x = 7+40k$.

- Réciproquement, si $x = 7+40k$ et $y = 4+23k$ avec $k \in \mathbb{Z}$,
$$\begin{aligned}23x - 40y &= 23\,(7+40k) - 40\,(4+23k) = 161 + 23 \times 40 \times k - 160 \\ &= 40 \times 23 \times k = 1.\end{aligned}$$
Le couple $(7+40k\ ,\ 4+23k)_{k\in\mathbb{Z}}$ est donc solution de (E).

L'ensemble des solutions de l'équation (E) est donc
$\big\{(7+40k\ ,\ 4+23k)\big\}_{k\in\mathbb{Z}}$.

(d) $23d \equiv 1\,[40] \iff 23d = 1+40y$ avec $y \in \mathbb{Z} \iff 23d-40y = 1$ avec $y \in \mathbb{Z}$ ce qui équivaut à « le couple (d, y) est solution de (E) » . Donc d s'écrit $7+40k$ avec $k \in \mathbb{Z}$. Pour satisfaire à la condition $0 \leqslant d < 40$, il faut $0 \leqslant 7+40k < 40$, ce qui n'est possible que si $k = 0$, ce qui donne $d = 7$.
Il existe donc un unique entier $d = 7$ vérifiant les conditions
$0 \leqslant d < 40$ et $23d \equiv 1\,[40]$.

3. Cryptage dans le système RSA
   (a) On a $N = pq = 5 \times 11 = 55$ et $n = (p-1)\,(q-1) = 4 \times 10 = 40$. On a déjà vu que 23 et 40 étaient premiers entre eux donc l'entier naturel $c = 23$ vérifie la condition voulue.
   (b) Bob souhaite envoyer à la personne A le nombre $a = 8$. Le nombre crypté b est le reste dans la division par N du nombre a^c donc b est le reste dans la division par 55 du nombre 8^{23}. D'après la question 1.b, le nombre crypté b vaut 17.
4. Décryptage dans le système RSA
   (a) Le nombre d est l'unique entier tel que $0 \leqslant d < n$ et $cd \equiv 1\,[n]$, c'est-à-dire $0 \leqslant d < 40$ et $23d \equiv 1\,[40]$. D'après la question 2.d on peut dire que $d = 7$.
   (b) Le nombre crypté étant $b = 17$, le nombre en clair est le nombre a, reste de la division de b^d par N, c'est-à-dire le reste de la division de 17^7 par 55.
   - $17^3 = 4\,913 = 89 \times 55 + 18$ donc $17^3 \equiv 18\,[55]$
   - $17^6 = \left(17^3\right)^2 \equiv 18^2\,[55]$, $18^2 = 324 = 4 \times 55 + 49$ donc $17^6 \equiv 18^2\,[55] \equiv 49\,[55]$.
   - $17^7 = 17^6 \times 17 \equiv 49 \times 17\,[55]$, $49 \times 17 = 833 = 15 \times 55 + 8$ donc $17^7 \equiv 49 \times 17\,[55] \equiv 8\,[55]$. Comme $0 \leqslant 8 < 55$, on peut dire que 8 est le reste de la division de 17^7 par 55.

   Le nombre qui se crypte en 17 est donc 8.

Partie B :
p et q sont deux nombres premiers distincts, $N = pq$, $n = (p-1)(q-1)$ et $c < n$ est premier avec n.
La clef publique est $(\,N\ ,\ c\,)$. Le principe est donc le suivant : pour transmettre l'entier a, on envoie b tel que $a^c \equiv b\,[N]$. Pour déchiffrer b, on calcule a tel que $b^d \equiv a\,[N]$, où d est la clef privée.

1. Petit théorème de Fermat

   (a) Si a est premier avec p, on a $a^{p-1} \equiv 1\,[p]$
   donc $a^{(p-1)(q-1)} = (a^{p-1})^{q-1} \equiv 1^{q-1}\,[p] \equiv 1\,[p]$.
   De même, si $a \wedge q = 1$, on a $a^{q-1} \equiv 1\,[q]$
   et $a^{(p-1)(q-1)} = (a^{q-1})^{p-1} \equiv 1^{p-1}\,[q] \equiv 1\,[q]$.

   (b) Ainsi, p et q divisent $a^{(p-1)(q-1)} - 1$. D'après la propriété 10 p.140 du cours P.G.C.D., le produit $N = pq$ divise $a^{(p-1)(q-1)} - 1$.
   D'où, $a^{(p-1)(q-1)} \equiv 1\,[N]$.

   (c) Soit $k \equiv 1\,[n]$. On a $k = 1 + rn = 1 + r(p-1)(q-1)$ et
   $a^k = a^{1+r(p-1)(q-1)} = a.a^{r(p-1)(q-1)} = a.(a^{(p-1)(q-1)})^r \equiv a.1^r\,[N] \equiv a\,[N]$.

2. Détermination de d

   (a) Puisque c et n sont premiers entre eux, le théorème de Bézout permet d'affirmer que l'équation $(E)\colon cx - ny = 1$ admet des solutions entières.

   (b) Soit (x_0, y_0) une solution particulière de (E). Si (x, y) est solution de (E), on a $c(x - x_0) - n(y - y_0) = 1 - 1 = 0$ donc $c(x - x_0) = n(y - y_0)$.
   Puisque $c \wedge n = 1$, le théorème de Gauss affirme que $c \,|\, (y - y_0)$ et il existe $k \in \mathbb{Z}$ tel que $y = y_0 + kc$. Alors, $c(x - x_0) = nkc$ et $x = x_0 + kn$.
   Réciproquement, si $x = x_0 + kn$ et $y = y_0 + kc$, alors (x, y) est trivialement une solution de (E).

   (c) Ainsi, $dc \equiv 1\,[n] \iff \exists\,(n, y),\ dc - ny = 1 \iff \exists k,\quad d = x_0 + kn$, unique dans $[\![\, 0\,;n-1 \,]\!]$.

3. Conclusion
   Soient a et $b \in \mathbb{N}$ et soit d l'unique entier de $[\![\, 0\,;n-1 \,]\!]$ tel que $dc \equiv 1\,[n]$.
   On a alors $b \equiv a^c\,[N] \Longrightarrow b^d \equiv a^{cd}\,[N] \equiv a\,[N]$ d'après la question 1c.

CORRIGÉS

Devoir n° 15

La crème de la crème

Ce devoir est associé au chapitre X, *Suites & Matrices*.

Quelque part, un peu en haut :
– Elle n'a pas l'air facile cette longueur : un véritable Écrin de nei*j*e glacée.
– T'es perdu ? Faut pas regarder l'Envers du Plan, pardi ! Ça va, ne boude pas. Tu fais La Tête ?
– Tré(s). File moi des dégaines.
– Il n'en reste plus beaucoup, ça ne pas fait de Profit. La Verte ou les Rouges ? Ou alors je te mets aussi la Blanche, ça te ferait un Trio laid ?... Qui ne Mot dit, consent : tiens.
– Au fait, tu crois que j'ai pas vu ta chute sur le (Ta)cul tout à l'heure ? Ça va ? Tu t'es pas félé le Pelvoux ? Talèfre est enflée et Dorée mais ça n'a pas l'air trop Grave.
– Sur le coup, j'ai cru voir un Mi(r)age : un Géant avec une dent de Requin poursuivant un Chardonnet, tout Tondu par la Bér(an)gère !
– C'est vraiment Co(s)mique comme situation. Quand j'vais raconter ça à Laurence.
– Arête ! Pas un mot. T'as qu'une envie, c'est de me la prendre. Tu crois que je te vois pas venir ? Tu vas lui faire le coup d'Allalin et la lampe magique.
– Il est vrai qu'Entrève et moi, il y a un coup de mou et je ne suis pas Moine mais je ne te ferais quand même pas ça.
– Mouais, bon, Bossons si on veut finir notre petit Tour avant la nuit.
– Ho ! Regarde qui est dans Lafaillle, en face.
– Qu'il est Beau, Anselme ! Et plus il Court, meilleur il est.
Juste en dessous se Pointe Isabelle d'Argentière, Montée(ts) sur ses Grands Mulets.
– Faut dire qu'il Vise haut avec cette voie mais elle l'aiMe son Ogre, la Jungfraü de Rochefort.
– Avec un temps pareil, j'aurais plutôt voté pour la République. Voilà qu'il pleut Dru, t'as pas froid ?
– Non, mais il commence à faire faim, non ?
– À Midi ? On n'attend pas l'heure du Goûter ? Tu n'y penses pas. Moi, je te laisse en Plan.
– C'est vrai, mon Dos lent retarde un peu notre course. Faut dire que j'ai Mal aux ris.
– Bon, bon. Un peu de remontant ? Du Leschaud ? Sinon, j'ai ma fiole de Walker ?
– Non, merci mais je prendrais bien un Chamonix. J'ai faim et puis, Grépon de Dieu ! Le Bio, (n)assez ! comme disait le grand homme.
– Qui donc ?
– Jean Jorasses, je crois.

– Je trouve pas les Chamomoux. De toutes façons, ils seraient aMers et de glace mais y'a ça.
Il lui tend un pot bleu fade.
– Génial, rien de tel que la crème Mon Banc !

Exercice

L'entreprise *Saint-Gervais* fabrique la fameuse crème *Mon Banc*. Une enquête effectuée auprès d'un grand nombre de malheureux consommateurs de crèmes montre que 30 % d'entre eux achètent la crème *Mon Banc*. Pour faire un poil plus vendeur et afin de compenser les lacunes gustatives de sa crème, l'entreprise décide de les conditionner dans un emballage recyclable, décomposable et surtout peu onéreux et elle lance alors une grande campagne publicitaire afin d'en faire la réclame. Un nouveau sondage est réalisé après une semaine et montre que si 10 % des acheteurs de crème *Mon Banc* sont partis vers la concurrence, 20 % des acheteurs de marques concurrentes consomment désormais de la crème *Mon Banc*. L'opération publicitaire se poursuit et il s'avère que l'évolution des pratiques de consommation reste identique.

1. Dresser un graphe probabiliste montrant l'évolution des pratiques d'achat d'une semaine à l'autre.
2. (a) Donner la distribution initiale π_0.
   (b) Écrire la matrice de transition A associée à ce graphe.
   (c) Déterminer la probabilité qu'un acheteur de crème choisi au hasard après deux semaines d'opération publicitaire achète la crème *Mon Banc*.
3. Déterminer un lien matriciel entre A, P et D où
   $P = \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} 0,7 & 0 \\ 0 & 1 \end{pmatrix}$.
4. Exprimer π_n, la distribution au bout de n semaines de réclame, en fonction de A et de n.
5. Justifier que la suite (π_n) converge et déterminer sa limite.
6. Quelle part de marché l'entreprise *Saint-Gervais* peut-elle espérer atteindre ?

Bonus Cette fois-ci, je vous conseille fortement d'écouter les émissions d'Étienne Klein, les samedis après-midi sur France Culture :

https ://www.radiofrance.fr/franceculture/podcasts/la-conversation-scientifique

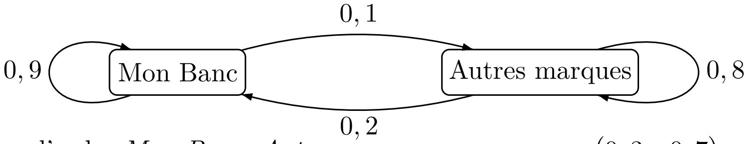
Science en question est un moment de débats et d'échanges autour de la science mais aussi de la philosophie, la culture et les arts, l'histoire, la géographie, la nature,... et tout ceci est curieux, amusant, passionnant,... Bref, intelligent.
En effet, bien que physicien, Étienne Klein est quelqu'un de très bien : il pratique l'alpinisme.

Corrigé du devoir n^{o} 15

LA CRÈME DE LA CRÈME

Exercice

1. La situation peut être modélisée par le graphe probabiliste suivant.



2. (a) Dans l'ordre *Mon Banc*, *Autre marques*, on a $\pi_0 = \begin{pmatrix} 0,3 & 0,7 \end{pmatrix}$.

   (b) La matrice de transition associée à ce graphe est $A = \begin{pmatrix} 0,9 & 0,1 \\ 0,2 & 0,8 \end{pmatrix}$.

   (c) On a $\pi_2 = \pi_0 A^2 = \begin{pmatrix} 0,3 & 0,7 \end{pmatrix} \begin{pmatrix} 0,83 & 0,17 \\ 0,34 & 0,66 \end{pmatrix} = \begin{pmatrix} 0,487 & 0,513 \end{pmatrix}$.
   La probabilité qu'un acheteur de crème choisi au hasard après deux semaines d'opération publicitaire achète la crème est de $0,487$.

3. $\det(P) = \det \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix} = 1 \times 1 - (-2) \times 1 = 3 \neq 0$ donc P est inversible et

   $P^{-1} = \frac{1}{3} \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}$. Ainsi, $PDP^{-1} = \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 0,7 & 0 \\ 0 & 1 \end{pmatrix} \cdot \frac{1}{3} \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}$

   $PDP^{-1} = \frac{1}{3} \begin{pmatrix} 2,7 & 0,3 \\ 0,6 & 2,4 \end{pmatrix} = \begin{pmatrix} 0,9 & 0,1 \\ 0,2 & 0,8 \end{pmatrix} = A$.

4. Par récurrence, on a $\pi_0 A^0 = \pi_0$ et si $\pi_n = \pi_0 A^n$, alors
   $\pi_{n+1} = \pi_n A = \pi_0 A^n A = \pi_0 A^{n+1}$: pour tout entier $n \in \mathbb{N}$, $\pi_n = \pi_0 A^n$.

5. Puisque $A^1 = A$ ne contient pas de 0, il existe une unique distribution invariante π qui est la limite des distributions (π_n) pour toute distribution initiale π_0. Cherchons $(\, a \,,\, b \,) \in [\,0\,;1\,]^2$ tels que $a + b = 1$ et $\pi = \begin{pmatrix} a & b \end{pmatrix}$ soit invariante.

   On a $\pi = \pi A \iff \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0,9 & 0,1 \\ 0,2 & 0,8 \end{pmatrix}$

   $$\iff \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} 0,9a + 0,2b & 0,1a + 0,8b \end{pmatrix}$$

   $$\iff \left\{ \begin{array}{l} a + b = 1 \\ a = 0,9a + 0,2b \\ b = 0,1a + 0,8b \end{array} \right. \iff \left\{ \begin{array}{l} b = 1 - a \\ a - 0,9a + 0,2a = 0,2 \\ 1 - a = 0,1a + 0,8(1 - a) \end{array} \right.$$

   $$\iff \left\{ \begin{array}{l} a = \frac{0,2}{0,3} = \frac{2}{3} \\ b = 1 - \frac{2}{3} = \frac{1}{3} \\ 1 - 0,8 = 0,1a + a - 0,8a \end{array} \right. \iff \pi = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \end{pmatrix}, \quad \text{limite de } (\pi_n)_{\mathbb{N}}.$$

6. Ainsi, l'entreprise *Saint Gervais* peut espérer atteindre une part de marché d'environ 67 %.

Devoir n^{o} 16

Devoir parental

Échangeons les rôles pour une fois : ce devoir doit être fait par les parents, aidés de leur enfant.

Cet exercice est un Q.C.M. Pour chaque question, une seule réponse est juste et aucune justification n'est demandée.

1. Du point de vue des mathématiques, l'enjeu de cette année scolaire est
   - S. nul et non avenu.
   - A. majeur et vacciné.
   - V. multiple, riche et enthousiasmant.
2. Le travail demandé est
   - A. une simple répétition hebdomadaire de la formule apprise en septembre.
   - U. inutile et ennuyeux.
   - I. nécessaire, formateur et passionnant.
3. Il y aura un devoir
   - N. par an.
   - C. par hasard.
   - V. par thème, ou quasiment.
4. Les énoncés fantasques
   - S. n'ont aucun rapport avec les mathématiques.
   - U. n'existent pas, ou alors, je n'ai pas compris.
   - E. changent de l'ordinaire et apprennent à se focaliser sur l'essentiel.
5. Le rédacteur de cet ouvrage tape bien
   - S. sur les nerfs.
   - N. sur ses élèves.
   - L. sur ordinateur.
6. Les documents distribués seront
   - C. peu nombreux, confus, dans le désordre.
   - R. en couleur, écrits à la main et enluminés à l'or fin.
   - E. nombreux, trop peut-être, et seront notre outil de travail. Les élèves devront apprendre à travailler avec, quitte à en recopier une partie ou faire des fiches afin de se les approprier et de les mémoriser.

7. Le manuel numérique
   - R. est une pièce indispensable et doit être en permanence à portée de main.
   - A. est joli, coloré, et bien mieux que ce qui est fourni en classe.
   - S. une aide utile et riche, en complément de ce qui est fait en classe.
8. Le matériel est
   - U. imposé : un classeur petit format, des feuilles de teintes diverses à gros carreaux, un cahier de brouillon, un stylo vert clair, deux crayons HB gras, un compas de précision, un double décimètre, quelques feuilles de papier Canson, un stylo plume, pas d'effaceur, un taille crayon sans réserve. Équerre interdite.
   - P. inutile : tout se passe dans la tête.
   - M. conseillé : un classeur grand format, des feuilles doubles et simples à petits carreaux, une calculatrice (cf. question 9) et une perforatrice (si, si).
9. La calculatrice exigée est
   - P. un simple convertisseur francs nouveaux - euros.
   - P′. la même que celle demandée en eps.
   - A. scientifique, de type lycée, mode examen.
10. Parti comme cela, au fil de l'année, votre enfant
    - U. aura perdu beaucoup de temps.
    - O. aura déjà un an de plus.
    - T. apprendra des concepts fascinants, tout en se faisant plaisir.
11. Parti comme cela, au fil de l'année, le professeur de mathématiques de votre enfant
    - L. aura perdu beaucoup de temps.
    - R. aura encore un an de plus.
    - H. enseignera des concepts fascinants, tout en se faisant plaisir.
12. Le rédacteur de cet ouvrage s'estime satisfait lorsque ses lecteurs
    - E. ne l'ont pas molesté.
    - T. ne l'ont pas vilipendé sur les réseaux sociaux.
    - S. ont pris du plaisir et se sentent plus intelligents après leur lecture.
13. Pour réussir, le plus important c'est
    - :-(le travail.
    - :-| le travail.
    - :-) le travail.

Cahiers transversaux

Cahier α

ALGO À GOGO

Sommaire

Ce cahier est essentiel pour toute votre scolarité.

Le mot algorithme vient du nom d'un mathématicien perse du IX^{e} s., Al-Khwarizmi. On trouve trace de méthodes algorithmiques dès le début des mathématiques et ce, dans toutes les cultures. L'algorithme d'Archimède donne une approximation du nombre π. Ératosthène, lui, a défini une procédure pour retrouver les nombres premiers en procédant par l'élimination des multiples successifs. Euclide trouve rapidement le *pgcd* de deux entiers. Dans son *Discours de la méthode*, René Descartes propose en 1637 de diviser chacune des difficultés qu'il examine, en autant de parcelles qu'il se peut et qui sont requises afin de mieux les résoudre. Au XIX^{e} s., Ada Lovelace, fille de Lord Byron, est considérée comme la pionnière de la science informatique. Elle a réalisé le premier véritable programme informatique lors de son travail sur un ancêtre de l'ordinateur. En effet, on trouve dans ses notes le premier programme destiné à être exécuté par une machine. Elle a également entrevu et décrit certaines possibilités offertes par les calculateurs universels, allant bien au-delà du calcul numérique qu'imaginaient ses contemporains. Le langage informatique Ada a été nommé en son honneur.

Un algorithme est un enchaînement fini d'étapes ou d'instructions à effectuer dans un certain ordre et dont la réalisation permet la résolution en un temps fini d'un problème donné. Les structures que nous étudierons ici seront plutôt simples mais pourront tout de même user de tests (Sialors) et autres boucles (Pour et Tantque) et mettront en œuvre des fonctions, peut-être même des listes. Nos algorithmes seront ici écrits en langage *naturel* ou en langage Python, qui lui est très proche. Ceux-ci ont l'avantage de rester lisibles car, outre les problèmes de syntaxe, les mauvaises constructions sont sources de nombreuses erreurs et autres bugs et l'on sait qu'en informatique, on a rapidement la rage envers la machine.

1 Installer Python

Il faut au préalable installer une distribution Python. Rassurez-vous, c'est très facile, il suffit de visiter le site http ://www.python.org/ et de la télécharger. Des applications EduPython sur PC, Idle sur Mac ou Pydroid 3 sur tablette par exemple fonctionnent bien.

Le principe est toujours le même : on dispose d'une console Python, une fenêtre dans laquelle on peut effectuer des calculs, appliquer des fonctions et observer les résultats de sortie des programmes, ainsi que d'un éditeur de programmes, une fenêtre où l'on saisit les programmes.

Par exemple, dans la console :

```
>>> from math import *
      # permet d'utiliser les commandes mathématiques
>>> from random import *
      # permet d'utiliser les commandes de probabilité
>>> 2**3   # ** signifie puissance
8
>>> sqrt(3)
1.732050808
>>> 13%8   # reste de la division euclidienne
5
>>> b=3
>>> h=4
>>> Aire_Triangle=b*h/2
>>> print(Aire_Triangle)
6
```

Dorénavant, nous considérons que les modules `math` et `random` sont importés dès que nécessaire.

Dans l'éditeur, nous pouvons écrire un programme comme le suivant puis lancer son exécution dans la console.

```
Nom=input("Quel est ton prénom ?")
Accueil="Bonjour "+Nom+". Bienvenue sur Python !"
print(Accueil)
```

L'éditeur permet de sauvegarder ses programmes dans un fichier « .py » ce qui est essentiel car la console oublie tout une fois qu'elle est fermée.

2 Les variables

Dans un programme, une variable est repérée par son nom et possède une valeur qui peut changer au fur et à mesure de l'exécution. On peut schématiser une variable par une boîte portant une étiquette, son nom, et ayant un contenu, sa valeur. C'est une différence fondamentale par rapport à ce qui est d'usage en mathématiques où l'on peut effectuer des calculs sans jamais connaître la valeur de la variable et si celle-ci est connue, elle ne peut changer.

On distingue plusieurs types de variables : les entiers (`int`), les décimaux (`float`), les chaînes de caractères (`str` pour string), les booléens (`bool`) : vrai et faux (ils ont aussi une valeur numérique : 1 et 0).
Une instruction d'affectation permet de donner une valeur à une variable, de remplir la boîte. En langage naturel, on écrit X$\longleftarrow$2 et en Python, « `X=2` ».
La demande d'une saisie de valeur s'écrit `X=float(input())` en Python. On remarque que l'on précise en même temps le type de la variable saisie. Pour l'afficher, `print(X)` fonctionne bien.

En mathématiques, le symbole = peut signifier une égalité ($3+5=8$), peut servir à définir un objet ($A=\pi R^2$) ou écrire une équation ($2x+3=5-x$) qui n'est pas toujours vérifiée et que l'on peut parfois résoudre. En Langage Python, `=` ne sert qu'à définir une variable. Pour tester une égalité, on utilisera `==`.

Exercice 1 Écrire un programme en langage Python appliquant l'algorithme suivant : saisir un nombre, l'élever au carré, en prendre le triple, retrancher 5 puis afficher le résultat.

3 Instructions conditionnelles

Une condition est un énoncé qui peut être vrai ou faux. Dans un programme, on peut tester si cette condition est vrai ou fausse et effectuer un traitement différent selon les cas.

Voici l'architecture d'un test :

```
Si condition Alors
    Traitement 1
Sinon
    Traitement 2
Fin Si
```

En Python, la fin de l'indentation (le décalage) marque la fin du traitement :

```
if condition :
    Traitement 1
else :
    Traitement 2
```

On peut ne pas effectuer de traitement dans le cas où la condition est fausse et l'on omet alors le « sinon/else ».
On peut aussi imbriquer plusieurs tests conditionnels et la commande « elif » combine un else suivi d'un if : cela permet de ne pas avoir un niveau d'indentation supplémentaire. Nous verrons cela en exercice.

Exercice 2 Agathe souhaite s'inscrire au club de mathématique de sa ville et on lui propose deux formules :

Formule α : une cotisation annuelle de 8 francs et chaque séance coûte 1,50 franc ;
Formule β : la séance coûte 1,70 franc.

Voici le programme incomplet qu'elle a écrit. Le compléter puis le saisir et l'exécuter.
À partir de combien de séances le programme α semble-t-il plus avantageux ?

```
n=int(input("Entrer n : "))
a=8+1,5*n
...............
if .......... :
```

```
    print("Le tarif .... est plus avantageux.")
................
    print("Le tarif beta est plus avantageux.")
```

Exercice 3 Saisir et exécuter le programme suivant. Que fait-il ?

```
x=int(input("Combien vois-tu de lignes ? |||||||||| "))
if x==10 :
    print("Bravo !")
elif x<=9 :
    print("Tu devrais consulter un ophtalmologue.")
else :
    print("Arrête de loucher !")
```

Exercice 4 Écrire un programme demandant à une personne si elle est majeure et le cas échéant, si elle a obtenu le permis de conduire. La féliciter si cela est le cas, l'encourager sinon.

4 Boucle bornée

Une boucle permet de répéter plusieurs fois de suite un même traitement. Lorsque le nombre n de répétition est connu à l'avance, on dit que la boucle est bornée et l'on utilise un compteur i qui s'incrémente à chaque itération : à chaque fois que le traitement est effectué, le compteur i augmente de 1. Lorsque i atteint la valeur n, on effectue une dernière fois le traitement puis on sort de la boucle.

Voici l'architecture d'une boucle bornée :

```
Pour i allant de 1 à n
    Traitement
Fin Pour
```

En Python, on utilise la commande range où la borne de droite est exclue et cela donne :

```
for i in range(1,n+1) :
    Traitement
```

Exercice 5 Ce programme affiche les puissances de 1 à n du nombre x. Le compléter.

```
x=....(input("De quel nombre souhaites-tu connaître les
puissances ? "))
n=...(input("Quelle puissance maximale souhaites-tu obtenir ? "))
p=1
for i in range(0,...) :
    p=x*p
    print(...)
```

Que cela change-t-il si l'on omet l'indentation de la dernière ligne ?

Exercice 6 Soit la fonction $f : x \longmapsto 3x^2 - 5$.

(a) Écrire un programme donnant les images par f de tous les entiers compris entre 0 et l'entier N.

(b) Le modifier afin qu'il donne les images de tous les multiples de $\frac{1}{2}$ compris entre 0 et l'entier N.

Exercice 7 Au cours de chaque semaine, tu doubles ton nombre de suiveurs sur ton compte Amstramgram mais tu en perds 7 le dimanche. Tu avais 9 suiveurs à l'aube du premier jour.

(a) Écris un programme donnant le nombre de suiveurs après n semaines et exécute-le.

(b) Que se passe-t-il si tu en avais seulement 6 au premier jour ? Et si tu en avais 7 ?

5 Boucle non bornée

Dans un boucle, le nombre de répétitions, d'itération n'est pas nécessairement connu à l'avance, il peut dépendre d'une condition et le traitement est alors répété tant que la condition est vérifiée puis on sort de la boucle. On parle de boucle non bornée (*a priori*) mais attention à ce que cette condition soit bien fausse après un certain nombre de répétitions, sinon le programme tournera *en boucle* sans jamais s'arrêter...

Voici l'architecture d'une boucle non bornée :

```
Tant que Condition
    Traitement
Fin Tant que
```

En Python, on utilise la commande while et cela donne :

```python
while Condition :
    Traitement
```

Exercice 8 Écrire un programme affichant tous les entiers naturels compris entre 0 et un décimal positif D.

Exercice 9 Colette est un peu lassée de lancer son dé alors elle a écrit le programme suivant. À quoi peut-il donc bien servir ?

```python
from random import *   # pour utiliser des fonctions de probabilités
f=randint(1,6)   # entier choisi au hasard
l=1
while f != 6 :   # différent de
    f=randint(1,6)
    l=l+1
print("Nombre de lancers : ", l)
```

Exercice 10 Ta capacité de concentration diminue de 16 % pour chaque heure passée quotidiennement devant un écran. Écris un programme donnant le nombre d'heures quotidiennes passées devant un écran à partir duquel ta capacité de concentration diminue de moitié.

Exercice 11 Il est bien connu que si l'on place un grain de riz sur la première case d'un échiquier, deux grains sur la deuxième case, quatre sur la troisième, huit sur la quatrième et ainsi de suite, on dépasse rapidement le nombre total de grains de riz disponibles. Complète le programme qu'a écrit Agathe afin qu'il détermine le nombre de cases que l'on peut complètement remplir avec un nombre R de grains de riz à disposition.

```
R=int(input("Nombre de grains de riz disponibles : "))
S=1
n=0
while S<=R :
    n=.......
    S=S+.....
print("Nombre de cases remplies : ", .... )
```

Exercice 12 On reprend la fonction $f\colon x \longmapsto 3x^2 - 5$ de l'exercice 6.

(a) Créer un programme donnant le premier entier naturel d'image strictement supérieure à un décimal M.

(b) Le modifier afin d'obtenir le premier multiple de $\frac{1}{2}$ vérifiant cette même condition.

6 Fonction

Une fonction d'un ou plusieurs arguments réalise un traitement et renvoie un résultat. Elle peut être appelée plusieurs fois par le programme principal et permet de mieux structurer celui-ci.

Voici l'architecture d'une fonction :

```
Fonction mafonction(a,b)
    Traitement
Résultat c
```

En Python, on utilise la commande def et cela donne :

```
def mafonction(a,b) :
    Traitement
    return c
```

Exercice 13 Écrire une fonction `airect` donnant l'aire d'un rectangle en fonction de la longueur de ses côtés.

Exercice 14

(a) Que calcule la fonction `so` suivante ?

```
def so(N) :
    S=0
    for i in range(1,N+1) :
        S=S+i
    return S
```

(b) Écrire une fonction `pr` calculant le produit de tous les entiers de 1 à N.

Exercice 15 Cette fonction nbfois détermine le nombre d'apparition d'un caractère dans un texte, une chaîne de caractères. Le compléter. Que signifient les lignes 2 et 5 ?

```
1| def nbfois(caractere,chaine) :   # doivent être mis entre " et "
2|    l=len(chaine)
3|    n=0
4|    for i in range(0,l) :   # ou range(l)
5|       if chaine[i]== caractere :
6|          n=......
7|    .........
```

Exercice 16 Écrire

(a) une fonction opposé donnant l'opposé d'un nombre,

(b) une fonction valabs donnant la valeur absolue d'un nombre,

(c) une fonction max2 donnant le plus grand de deux nombres,

(d) une fonctions max5 donnant le maximum de cinq nombres en utilisant la précédente,

(e) une fonction puissmin donnant le plus petit entier tel qu'un nombre donné élevé cette puissance soit supérieur ou égal à un autre nombre donné.

Quant l'architecture commence à être complexe, il ne faut pas hésiter à créer plusieurs fonctions et faire appel aux unes dans les autres. On peut très bien utiliser une fonction qui est écrite après dans l'éditeur mais il faut faire attention à ne pas les définir en boucle. Par exemple, si `mafonction1` fait appel à `mafonction2` et si `mafontion2` à `mafonction1`, vous risquez bien de tourner en rond. En revanche, dans une architecture correctement construite, une fonction peut très bien s'appeler elle-même sans problème. C'est ce qui s'appelle un algorithme récursif.

Exercice 17 Soit la fonction $f : x \longmapsto 3x^2 - 2x - 4$. Écrire un programme donnant le maximum entre la valeur absolue d'un nombre et l'image par f de ce nombre en précisant duquel il s'agit.

Exercice 18 Tel Euclide, créez une fonction donnant le plus grand commun diviseur de deux entiers naturels. Vous pourrez utiliser une version récursive.

7 Liste

Cette partie n'est pas au programme de seconde mais simplement à partir de la classe de première. Elle peut néanmoins être utile à tous.

Lorsque l'on a besoin de garder et d'utiliser plusieurs variables au cours d'un programme, on utilise des listes pour les stocker. Une liste est une collection d'objets de différents types (nombres, chaînes de caractères, booléens, listes...). On peut ensuite la manipuler, faire appel à l'un de ses termes, l'utiliser dans une boucle, etc. Un exemple typique d'utilisation est la collecte des premiers termes d'un suite. Voici quelques commandes utiles en langage Python.

Un exemple de liste	`L=[2,"mai",7,True]`
Une liste vide	`L=[]`
Premier objet de la liste (rang 0)	`L[0]`
$(k+1)^e$ objet de la liste (rang k)	`L[k]`
Dernier objet de la liste	`L[-1]`
Longueur de la liste	`len(L)`
Ajouter un `objet` en fin de liste	`L.append(objet)`
Insérer un `objet` au rang k	`L.insert(k,objet)`
Supprimer l'objet de rang k	`del L[k]`
Supprimer l'objet `element`	`L.remove(element)`
Compte le nombre d'objets `element` dans la liste	`L.count(element)`
Trouve l'index de l'objet `element` dans la liste	`L.index(element)`
Concaténer (rassembler) deux listes	`L1+L2`
Inverser l'ordre des valeurs	`L.reverse()`
Afficher les objets par ordre croissant (si possible)	`sorted(L)`
Réarranger la liste par ordre croissant (si possible)	`L.sort()`

Exercice 19 On considère la fonction suivante.

```
def cettefonction(valeur,liste) :
   nombre=0
   for v in liste :
      if v>=valeur :
         nombre=nombre+1
return nombre
```

Pour `L=[1,2,4,2,1]`, `cettefonction(2,L)` donne 3, `cettefonction(3,L)` donne 1 et `cettefonction(6,L)` donne 0. Que fait cette fonction ?

Exercice 20

A. La ligne `L=[i**2 for i in range(6)]` donne la liste [0, 1, 4, 9, 16, 25]. Que fait cette instruction ?

B. Créer une liste des cubes des entiers naturels inférieurs ou égaux à douze.

C. Saisir les instructions suivantes. Que font-elles ?

   (a) `L=[9-k for k in range(7)]`

   (b) `M=[6]*5`

   (c) `N=[randint(1,6) for i in range(8)]`

   (d) `M[2]=1`

   (e) `P=M+N`
   `P.sort()`

   (f) `X=[0.5*i for i in range(-5,5)]`
   `Y=[3*x**2-5 for x in X]`

Exercice 21 Écrire une fonction calculant la somme des objets d'une liste de nombres.

Exercice 22 Écrire une fonction donnant la liste des diviseurs d'un entier naturel.

Exercice 23 Écrire un programme échangeant la place de deux objets d'une liste.

Exercice 24 Les notes de Colette en mathématiques augmentent de 2 % à chaque devoir jusqu'à ce qu'elle obtienne la note maximale. Écrire une fonction créant la liste de ses notes jusqu'à 20 en fonction de la note non nulle qu'elle a obtenue au premier devoir rendu.

8 Foire de l'algo

Les algorithmes seront rédigés ici en langage naturel mais je vous encourage à les saisir en Python afin de vérifier que vous maîtrisez bien ce que vous avez appris précédemment. Ils sont d'un niveau varié et peuvent parfois utiliser des résultats et notions mathématiques que vous ne connaissez pas encore mais vous pourrez tout de même comprendre leur architecture.

1. (a) Que contient la variable Z après exécution de l'algorithme (A) pour $Z = 0$, $Z = 1$ puis $Z = 3$?

(b) Quel est le rôle de cet algorithme ?

> **Algo (A)**
> $Z \longleftarrow 2 - Z^2$

2. (a) Que contient la variable T après exécution de l'algorithme (B) pour $S = 0$, $S = 1$ puis $S = -2$?

(b) Quel est le rôle de cet algorithme ?

(c) Le simplifier.

> **Algo (B)**
> $R \longleftarrow 2$
> $T \longleftarrow -\pi$
> $R \longleftarrow 2S + 3$
> $R \longleftarrow 4R - 1$
> $T \longleftarrow 3R^2 - 4$

3. (a) Que contient la variable U après exécution de l'algorithme (C) pour $N = 3$?

(b) Quel est le rôle de cet algorithme ?

> **Algo (C)**
> $U \longleftarrow 7$
> Pour I allant de 1 à N
> $U \longleftarrow \frac{3}{4} \times U$
> Fin Pour
> Afficher U

4. (a) Quelles valeurs affiche l'algorithme (D) pour $P = 5$ et $V = -3$?

(b) Quel est le rôle de cet algorithme ?

> **Algo (D)**
> Pour K allant de 2 à P
>   Affecter $V \longleftarrow 4 + V$
>   Afficher V
> Fin Pour

5. (a) Exécuter les algorithmes (E) pour $N = 3$, (F) pour $A = 4$ puis $A = 10$ et (G) pour $N = 4$.

(b) Quel est le rôle de chacun de ces algorithmes ?

Algo (**E**)
$U \longleftarrow 4$
$I \longleftarrow 0$
Tant que $I < N$
  $I \longleftarrow I + 1$
  $U \longleftarrow \frac{2}{5}U + 2$
Fin Tant que
Afficher U

Algo (**F**)
$X \longleftarrow 0$
$F \longleftarrow 2$
Tant que $F < A$
  $X \longleftarrow X + \frac{1}{2}$
  $F \longleftarrow X^2 + 2$
Fin Tant que
Afficher X

Algo (**G**)
$P \longleftarrow \pi$
Pour I allant de 0 à N
  $D \longleftarrow Ent(P)$
  $P \longleftarrow 10(P - D)$
  Afficher D
Fin Pour

6. (a) À quoi correspond la modification « Pour K allant de 1 à P » dans le (D) ?

(b) À quoi correspond la modification « $I \longleftarrow 1$ » dans l'algorithme (E) ?

7. Évariste est gallois et son cousin est Germain. Le premier raffole des boucles *Tant que* tandis que le second affectionne les boucles *Pour*.

(a) Aide Germain à transformer la boucle *Tant que* du (E) en boucle *Pour*.

(b) Peut-il transformer la boucle *Tant que* de l'algorithme (F) en boucle *Pour* ?

(c) Tel Évariste, transforme les boucles *Pour* des (C) et (D) en boucles *Tant que*.

8. (a) Observer et analyser l'algorithme (H).

(b) Le compléter afin qu'il réponde au problème donné dans $\mathbb{R}$.

Algo (**H**)
Saisir $A \neq 0$, B et C
$D \longleftarrow$ ...
Si D..., Alors
  $U \longleftarrow \frac{-B-\sqrt{D}}{2A}$
  $V \longleftarrow$ ...
  Afficher ....
Sinon
....
Fin Si

9. (a) Observer, analyser, compléter, modifier, exécuter pour différentes valeurs les algorithmes (I), (J), (K), (L) et (M).

(b) Quel est le rôle de chacun de ces algorithmes ?

Algo (**I**)
$K \longleftarrow 0$
$B \longleftarrow 2$
Saisir N
Pour K allant de 1 à N
  $B \longleftarrow A + 1$
  $A \longleftarrow B - 1$
Fin Pour
Afficher $A - B$

Algo (**J**)
$B \longleftarrow 3$
Saisir N
Tant que $K < N$
  $K \longleftarrow K + 1$
  $A \longleftarrow 3B$
  $C \longleftarrow A - 2$
  $A \longleftarrow \frac{C+2}{3}$
Fin Tant que
Afficher $A - B$

Algo (K)
$F \longleftarrow 1$
$U \longleftarrow 0$
Pour K allant de 1 à N
  Afficher F
  $V \longleftarrow F$
  $F \longleftarrow U + F$
  $U \longleftarrow V$
Fin Pour

Algo (L)
$U \longleftarrow 4$
$V \longleftarrow 1$
$I \longleftarrow 0$
Saisir M
Tant que $I < M$
  $W \longleftarrow V$
  $V \longleftarrow \frac{U+V}{2}$
  $U \longleftarrow W$
  Afficher U
Fin Tant que

Algo (M)
$X \longleftarrow 0$
Saisir A
$F \longleftarrow 1 - X^3$
Tant que $F < A$
  $X \longleftarrow X + 1$ à X
  $F \longleftarrow 1 - X^3$
Fin Tant que
Afficher X

10. (a) Observer, analyser, compléter, exécuter, au moyen de tableaux et pour différentes valeurs, l'algorithme (N) pour les fonctions $f(x) = 2x + 1$, $f(x) = x^2 - 1$, $f(x) = \sin(x)$ puis $f(x) = 1 - x^2$.

(b) Quel est le rôle de cet algorithme ?

(c) Le test « Si $f(A) \times f(B) > 0$ » est-il nécessaire ?

Algo (N)
f est une fonction ....ante et ...
Saisir A, B et E
$I \longleftarrow A$
Si $f(A) \times f(B) > 0$, Alors
  Afficher "Non mais ça ne va pas ?"
Sinon
  Tant que $|f(I)| > E$
    $I \longleftarrow \frac{A+B}{2}$
    Si $f(I) > 0$, Alors
      ... $\longleftarrow I$
    Sinon
      ... $\longleftarrow I$
    Fin Si
  Fin Tant que
  Afficher I
Fin Si

11. Rédiger puis exécuter pour différentes valeurs des algorithmes répondant aux problèmes suivants :

(a) Afficher l'image d'un réel x_0 à saisir par la fonction $f(x) = 3x^2 - 5\cos(x) + 7$.

(b) Afficher les coordonnées du milieu d'un segment dont on saisit les coordonnées des extrémités.

(c) Afficher tous les termes jusqu'au rang p de la suite $u_n = n^2 - 3n + 4$, $n \in \mathbb{N}$.

(d) Afficher le $(n + 1)$-ième terme de la suite $v_0 = 5$, $v_{n+1} = 2v_n - 3$.

(e) Afficher le terme numéro n de la suite $w_0 = 4$, $w_1 = 5$, $w_{n+2} = 3w_{n+1} - 2w_n$.

(f) Calculer le produit scalaire de deux vecteurs dont on saisit les coordonnées dans un repère orthonormé, l'afficher puis déterminer leur éventuelle orthogonalité.

(g) Faire choisir un nombre entier entre 0 et 100 à la machine (*Aléat*) puis saisir des entiers jusqu'à ce qu'il soit trouvé. La machine doit préciser si la saisie est supérieure ou inférieure à la solution et féliciter chaleureusement le joueur lorsqu'il réussit enfin.

12. Implémenter le cas réel de l'algorithme du discriminant (H) dans votre calculatrice, cela pourra vous servir...

13. ($\int$) Implémenter ses algorithmes préférés en langage Python et les exécuter pour différentes valeurs.

9 Solutions

Exercice 1 Dans la console, cela donne :

```
>>> x=float(input("Saisir un nombre : "))
>>> x=x**2   # On utilise la même variable
>>> x=3*x
   # Cela prend moins de « place » mais on perd l'information de départ
>>> x=x-5
>>> print(x)
```

Exercice 2 Avec ce programme, Agathe s'aperçoit qu'à partir de 40 séances, le tarif α est plus avantageux.

```
n=int(input("Entrer n : "))
a=8+1,5*n
b=1,7*n
if a<=b :
   print("Le tarif alpha est plus avantageux.")
else :
   print("Le tarif beta est plus avantageux.")
```

Exercice 3 Ce programme teste sommairement la vue du joueur. S'il voit 10 lignes, on le félicite, s'il en voit moins c'est qu'il devrait certainement porter des lunettes et s'il en voit plus, c'est qu'il louche.

Exercice 4

```
n=int(input("Quel âge as-tu ? "))
if n>=18 :
   p=str(input("Tu es donc majeur(e). As-tu le permis de conduire ? "))
   if p=="oui" :   # chaîne de caractères
      print("Bravo !")
   else :
      print("Rien n'est perdu.")
else :
   print("Tu es mineur(e) et tu ne peux pas encore avoir le permis de conduire.")
```

Exercice 5 Le programme suivant affiche les puissances de 1 à n du nombre x.

```
x=float(input("De quel nombre souhaites-tu connaître les puissances ? "))
```

```
n=int(input("Quelle puissance maximale souhaites-tu obtenir? "))
p=1
for i in range(0,n) :
    # i va prendre n valeurs différentes, de 0 à n-1
    p=x*p
    print(p)
```

Si l'on omet l'indentation de la dernière ligne, seule la dernière puissance est affichée.

Exercice 6 Soit la fonction $f\colon x \longmapsto 3x^2 - 5$.

(a) Voici un programme donnant les images par f de tous les entiers compris entre 0 et l'entier N.

```
N=int(input("Antécédent max : "))
for i in range(0,N+1) :
    y=3*i**2-5
    print(y)
```

(b) En voici un donnant les images de tous les multiples de $\frac{1}{2}$ compris entre 0 et N.

```
N=int(input("Antécédent max : "))
for i in range(0,N) :
    y1=3*i**2-5
    y2=3*(i+0.5)**2-5
    print(y1)
    print(y2)
print(3*N**2-5)   # Pour calculer et afficher l'image de N
```

Exercice 7 Compte Amstramgram

(a)

```
n=int(input("Depuis combien de semaines as-tu ton compte
Amstramgram?"))
S=9
for i in range(n) :
    # On a omis la borne gauche, c'est alors 0 par défaut
    S=2*S-7
print("Tu as désormais ",S," suiveurs.")
```

(b) Si tu avais 6 suiveurs au premier jour, on s'aperçoit que tu n'en as plus dès la troisième semaine.
Et si tu en avais 7 à l'aube du premier jour, cela restera ainsi jusqu'à la fin des temps.

Exercice 8 Celui-ci affiche tous les entiers naturels entre 0 et un décimal positif D.

```
D=float(input("Quel nombre positif, je te prie?"))
k=0
```

```
while k<=D :
    print(k)
    k=k+1
```

Exercice 9 Le programme de Colette simule des lancers d'un dé cubique jusqu'à l'obtention d'un six et affiche le nombre de lancers qui ont été nécessaires.

Exercice 10 Grâce au programme suivant, tu sais que ta capacité de concentration aura diminuée de moitié si tu passes plus de 4 heures par jour devant un écran.

```
c=1   # Capacité initiale
h=0
while c>0.5 :
    c=0.84*c   # diminution de 16 % : multiplication par 1 - 16/100
    h=h+1
print("Nombre d'heures quotidiennes devant un écran: ", h)
```

Exercice 11 Grains de riz

```
R=int(input("Nombre de grains de riz disponibles : "))
S=1
n=0
while S<=R :
    n= n+1
    S=S+2**n
print("Nombre de cases remplies : ", n )
```

Exercice 12 $f : x \longmapsto 3x^2 - 5$

(a)
```
1| M=float(input("Borne à dépasser : "))
2| f=-5
3| n=0
4| while f<=M :
5|     n=n+1
6|     f=3*n**2-5
7| print("L'image de ",n," par f est strictement plus grande que ",M)
```

(b) Afin d'obtenir le premier multiple de $\frac{1}{2}$, il suffit de remplacer la ligne 5 par `n=n+0.5`.

Exercice 13 La fonction `airect` suivante donne l'aire d'un rectangle en fonction de la longueur de ses côtés.

```
def airect(l,L) :
```

```
    a=l*L
    return a
```

Exercice 14

(a) La fonction so calcule la somme des entiers entre 0 et N.

(b) La fonction pr suivante calcule le produit des entiers entre 1 et N.

```
def pr(N) :
    P=1
    for i in range(1,N+1) :
        P=P*i
    return P
```

Exercice 15 La fonction `nbfois` détermine le nombre d'apparition d'un caractère dans une chaîne de caractères.

```
def nbfois(caract,chain) :   # doivent être mis entre " et "
    l=len(chain)   # nombre de caractères dans la chaîne
    n=0
    for i in range(0,l) :   # ou range(l)
        if chain[i]== caract :   # si le caractère de rang i est caract
# Rq : le premier caractère d'une chaîne est de rang 0 et le dernier, de rang len−1
            n=n+1
    return n
```

Exercice 16

(a)
```
def opposé(x) :
    return -x
```

(b)
```
def valabs(x):
    if x<0 :
        return -x
    else :
        return x
```

(c)
```
def max2(a,b) :
    if a<b :
        return b
    else :
        return a
```

(d)
```
def max5(a,b,c,d,e) :
    M=max2(a,max2(b,
        max2(c,max2(d,e))))
    return M
```

(e)
```
def puissmin(a,A) :
    n=0
    while a**n<A :
        n=n+1
    return(n)
```

Exercice 17 On va utiliser les fonctions `max2` et `valabs` de l'exercice précédent.

```
def monmaxf(x) :
```

```
    f=3*x**2-2*x-4
    m=max2(f,valabs(x))
    if m==f :
        return print("Le maximum est l'image ",m)
    else :
        return print("Le maximum est l'antécédent ", m)
```

Exercice 18 Algorithme d'Euclide

```
def EuclideClassique(a,b) :
  # algorithme classique du pgcd de a et b
    while a%b != 0 :
    # le % donne le reste de la division euclidienne, != teste si différent
        a, b = b, a%b
    # on change les valeurs de a et b en même temps, cela évite de sauver l'ancien a pour l'utiliser dans le nouveau b
    return b
```

```
def EuclideRécursif(a,b) : # algorithme récursif du pgcd de a et b
    if (b==0) :
        return(a)
    else :
        r=a%b
        return EuclideRécursif(b,r)
```

Exercice 19 Cette fonction donne le nombre d'objets numériques ou bouléens (True valant 1 et False valant 0) de la liste ayant une valeur supérieure ou égale à la valeur en argument.

Exercice 20

A. `L=[i**2 for i in range(6)]` crée la liste des carrés des six premiers entiers (de 0 à 5).

B. `L=[i**3 for i in range(13)]` crée la liste des cubes des entiers jusqu'à douze.

C. (a) `L=[9-k for k in range(7)]` donne la liste `[9,8,7,6,5,4,3]`.

   (b) `M=[6]*5` donne la liste `[6,6,6,6,6]`.

   (c) `N=[randint(1,6) for i in range(8)]` donne une liste aléatoire de huit entiers entre 1 et 6.

   (d) `M[2]=1` remplace l'objet de rang 2 (le troisième) par un 1 dans la liste `M`.

   (e) `P=M+N` puis `P.sort()` crée la liste concaténée de `M` suivie de `N` puis la réorganise par ordre croissant.
   La liste `P` est ici `[1, 1, 1, 2, 3, 4, 4, 5, 6, 6, 6, 6, 6]`.

(f) `X=[0.5*i for i in range(-5,5)]` crée la liste des multiples de $\frac{1}{2}$ dans $\left[-\frac{5}{2}\,;\frac{5}{2}\right[$.
`Y=[3*x**2-5 for x in X]` crée la liste des images de ces mêmes multiples par $f(x) = 3x^2 - 5$.

Exercice 21 La fonction suivante calcule la somme des objets d'une liste de nombres. Remarquons que la fonction intégrée `sum()` aurait donné le même résultat.

```
def sommeliste(L) :
    s=0
    for v in L :
        s=s+v
    return s
```

Exercice 22 Cette fonction affiche la liste des diviseurs d'un entier naturel.

```
def listediv(n) :
    div=[]
    for i in range(1,n+1) :
        if n
            div.append(i)
    print(div)
```

Exercice 23 Le programme suivant échange la place de deux objets d'une liste.

```
def echange(i,j,L) :
    if i>len(L) or j>=len(L) :
   # afin de ne pas dépasser les dimensions de la liste
        print("Liste trop courte")
    else :
        L[i],L[j]=L[j],L[i]   # échange simultané, c'est pratique
    return L
```

Exercice 24 Les notes de Colette en mathématiques sont données par ce programme.

```
def notesaugementées(n) :
    L=[]
    d=n
    while d<20 :
        L.append(d)
        d=1.02*d
    L.append(20)
    return L
```

Foire de l'algo

1. On obtient 2, 1 puis -7. L'algorithme (A) affiche l'image de Z par la fonction $f(x) = 2 - x^2$.

2. On obtient 359, 1079 puis 71. L'algorithme (B) affiche l'image de S par la fonction $192x^2 + 528x + 359$. Il est bien plus simple de reprendre alors l'algorithme (A) avec cette fonction f.

3. L'algorithme (C) affiche u_N pour $u_n = 7 \times (\frac{3}{4})^n$, $\forall n \in \mathbb{N}$.

$U \longleftarrow 7$
$N \longleftarrow 3$
Début Pour
  $I \longleftarrow 1$
    $U \longleftarrow \frac{3}{4} \times 7$
  $I \longleftarrow 2$
    $U \longleftarrow \frac{3}{4} \times \frac{3}{4} \times 7$
  $I \longleftarrow 3$
    $U \longleftarrow 7(\frac{3}{4})^3$
Fin Pour
"$\frac{189}{64}$"

4. L'algorithme (D) affiche v_2, v_3,...v_P pour $v_1 = -3$, $v_{n+1} = v_n + 4$, $\forall n \geqslant 1$.

$P \longleftarrow 5$
$V \longleftarrow -3$
Début Pour
  $K \longleftarrow 2$
    $V \longleftarrow 4 - 3 = 1$
    "1"
  $K \longleftarrow 3$
    $V \longleftarrow 4 + 1 = 5$
    "5"
  $K \longleftarrow 4$
    $V \longleftarrow 4 + 5 = 9$
    "9"
  $K \longleftarrow 5$
    $V \longleftarrow 4 + 9 = 13$
    "13"
FinPour

5. • L'algorithme (E) affiche u_N pour $u_0 = 4$, $u_{n+1} = \frac{2}{5}u_n + 2$, $\forall n \geqslant 0$.

$U \longleftarrow 4$
$I \longleftarrow 0$
$N \longleftarrow 3$
Début Tantque
  $0 < 3$
    $I \longleftarrow 0 + 1 = 1$
    $U \longleftarrow \frac{2}{5} \times 4 + 2 = \frac{18}{5}$
  $1 < 3$
    $I \longleftarrow 1 + 1 = 2$
    $U \longleftarrow \frac{2}{5} \times \frac{18}{5} + 2 = \frac{86}{25}$
  $2 < 3$
    $I \longleftarrow 2 + 1 = 3$
    $U \longleftarrow \frac{2}{5} \times \frac{86}{25} + 2 = \frac{422}{125}$
  $3 \geqslant 3$
FinTantque
"$\frac{422}{125}$"

• L'algorithme (F) affiche le premier multiple positif de $\frac{1}{2}$ tel que $f(X) = X^2 + 2 \geqslant A$.

$X \longleftarrow 0$
$F \longleftarrow 2$
$A \longleftarrow 4$
Début Tantque
  $2 < 4$
    $X \longleftarrow 0 + \frac{1}{2} = \frac{1}{2}$
    $F \longleftarrow (\frac{1}{2})^2 + 2 = \frac{9}{4}$
  $\frac{9}{4} < 4$
    $X \longleftarrow \frac{1}{2} + \frac{1}{2} = 1$
    $F \longleftarrow 1^2 + 2 = 3$
  $3 < 4$
    $X \longleftarrow 1 + \frac{1}{2} = \frac{3}{2}$
    $F \longleftarrow (\frac{3}{2})^2 + 2 = \frac{17}{4}$
  $\frac{17}{4} \geqslant 4$
FinTantque (pour $A = 4$)
"$\frac{3}{2}$"

Pour $A = 10$, on continue jusqu'à $X = 3$.

• L'algorithme (G) affiche les $N + 1$ premières décimales de π (pour peu qu'on les connaisse auparavant).

$P \longleftarrow \pi = 3,14159...$
$N \longleftarrow 4$
Début Pour
  $I \longleftarrow 0$
    $D \longleftarrow Ent(\pi) = 3$
    $P \longleftarrow 10(\pi - 3) = 1,4159...$
    "3"
  $I \longleftarrow 1$

$D \longleftarrow Ent(1,4159...) = 1$
$P \longleftarrow 10(1,4159... - 1) = 4,159...$
"1"
$I \longleftarrow 2$
$D \longleftarrow Ent(4,159...) = 4$
$P \longleftarrow 10(4,159... - 4) = 1,59...$
"4"
$I \longleftarrow 3$
$D \longleftarrow Ent(1,59...) = 1$
$P \longleftarrow 10(1,59... - 1) = 5,9...$
"1"
$I \longleftarrow 4$
$D \longleftarrow Ent(5,9...) = 5$
$P \longleftarrow 10(5,9... - 5) = 9,...$
"5"
FinPour

6. (a) Si K va de 1 à P alors, D affiche v_1, v_2,...v_P pour $v_0 = -3$, $v_{n+1} = v_n + 4$.

(b) Si on affecte 1 à I, alors E affiche u_N pour $u_1 = 4$, $u_{n+1} = \frac{2}{5}u_n + 2, \forall n \geqslant 1$.

7. (a) La boucle *Tantque* de E devient « Pour I allant de 1 à N, $U \longleftarrow \frac{2}{5}U + 2$, Fin Pour », sans initialisation de I.

(b) Dans l'algorithme F, on ne peut transformer la boucle *Tant que* en boucle *Pour* car on ne sait pas à l'avance à partir de quel multiple de $\frac{1}{2}$ la fonction f « dépasse » la borne A que l'on saisit.

(c) C : $I \in \mathbb{N}$, Init. : $I \longleftarrow 0$, Boucle : Tant que $I < N$, $I \longleftarrow I + 1$, $U \longleftarrow \frac{3}{4}U$, Fin Tantque.
D : $K \geqslant 1$, Init. : $K \longleftarrow 1$, Boucle : Tant que $K < P$, $K \longleftarrow K + 1$, $V \longleftarrow 4 + V$, Fin Tantque.

8. L'algorithme H est celui du discriminant d'un trinôme du second degré dans $\mathbb{R}$, $f(x) = ax^2 + bx + c$.

Algo H
Saisir $A \neq 0$, B et C
$D \longleftarrow B^2 - 4AC$ à D
Si $D > 0$, Alors
  $U \longleftarrow \frac{-B-\sqrt{D}}{2A}$ et $V \longleftarrow \frac{-B+\sqrt{D}}{2A}$
  Afficher "Deux racines réelles :" U "et" V "."
Sinon
  Si $D = 0$, Alors
    $U \longleftarrow \frac{-B}{2A}$
    Afficher "Une racine réelle double :" U "."
  Sinon
    Afficher "Pas de racine réelle."
  Fin Si
Fin Si

9. I : A n'est pas initialisé alors que B l'est sans que ce soit nécessaire. On peut donc « Affecter 2 à A » plutôt qu'à B. Par ailleurs, N ne doit pas être nul et l'initialisation de K est inutile tout comme cet algorithme qui affichera toujours $3 - 2 = 1$.
J : C n'est pas déclaré et K n'est pas initialisé à 0. Cet algorithme affichera toujours 0 ce qui est extrêmement inutile.
K : Il faut « Saisir N ($\geqslant 1$) » et la variable s'appelle K et non I. Cet algorithme affiche alors les termes f_1, f_2, ..., f_N de l'historique suite de Fibonacci : $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_{n+1} + f_n$.

CORRIGÉS

(L) : Il manque l'incrémentation « $I \longleftarrow I+1$ » dans la boucle. Cet algorithme affiche les valeurs successives de la suite $u_0 = 1,\ u_1 = 4,\ u_{n+2} = \dfrac{u_{n+1}+u_n}{2}$.

(M) donne le premier entier naturel pour lequel la fonction $f(x) = 1 - x^3$ dépasse A. Le problème est que f est décroissante et ceci n'est donc pas pertinent du tout : cela donne généralement 0 ou pire, l'algorithme tourne à l'infini si $A > 1$. Il faut donc mieux imposer A négatif et faire un test « Tant que $F > A$ » pour voir quand elle passe en dessous.

10. L'algorithme (N) affiche une valeur approchée d'une racine de la fonction f sur l'intervalle $[\,A\,;B\,]$ par la *méthode de dichotomie.* Le réel strictement positif E donne la précision de l'approximation.
La fonction f doit être continue et monotone (théorème des valeurs intermédiaires !). Pour f croissante, on affecte I à B lorsque $f(I)$ est positif et I à A lorsque $f(I)$ est négatif. On inverse B et A lorsque f est décroissante.
Si $f(A) \times f(B) < 0$, f change de signe entre A et B et s'annule donc : ce test est nécessaire.
Il est à noter que f n'admet pas nécessairement une unique racine et l'algorithme ne donne pas le même résultat selon les valeurs de A et de B saisies.
Vous avez peut-être besoin des explications de votre professeur alors, n'hésitez pas.

11. Voici des algorithmes répondant aux problèmes posés.

Algo (a)
Saisir X
$X \longleftarrow 3X^2 - 5\cos(X) + 7$
Afficher X

Algo (b)
Saisir xA, yA, xB et yB
$xA \longleftarrow \frac{xA+xB}{2}$
$yA \longleftarrow \frac{yA+yB}{2}$
Afficher xA et yA

Algo (c)
Saisir P
Pour I allant de 0 à P
  $U \longleftarrow I^2 - 3I + 4$
  Afficher U
Fin Pour

Algo (d)
$V \longleftarrow 5$
Saisir N ($\geqslant 1$)
Pour K allant de 1 à N
  $V \longleftarrow 2V - 3$
Fin Pour
Afficher V

Algo (e)
$W \longleftarrow 5$
$U \longleftarrow 4$
Saisir N ($\geqslant 2$)
Pour K allant de 1 à $N-1$
  $V \longleftarrow W$
  $W \longleftarrow 3U - 2W$
  $U \longleftarrow V$
Fin Pour
Afficher W

Algo (f)
Saisir Xu, Yu, Xv et Yv
$S \longleftarrow Xu \times Xv + Yu \times Yv$
Afficher "Leur produit scalaire est" S
Si $S = 0$, Alors
  Afficher "et ils sont orthogonaux"
Fin Si

Algo **g**

$N \longleftarrow Aléat(0; 100)$
$I \longleftarrow 0$
Tant que $I < 101$
  $I \longleftarrow I + 1$
  Saisir E
  Si $E = N$, Alors
    Afficher "Bravo !"
  Sinon
    Si $E > N$, Alors
      Si $E \geqslant 101$, Alors
        Afficher "Tu n'as rien compris !"
      Sinon
        Afficher "Trop grand !"
      Fin Si
    Sinon
      Afficher "Trop petit !"
    Fin Si
  Fin Si
Fin Tant que
Si $I \geqslant 101$, Alors
  Afficher "Tu n'es vraiment pas très doué !"
Fin Si

12. Voici le programme du « discriminant réel » sur une T.I.

Commentaires	**T.I.**
Écriture du programme	PROGRAM :DEGRE2
Initialisation	
Commencer par effacer l'écran	`: ClrHome`
Entrées	
Demander la valeur de a	`: Prompt A`
Demander la valeur de b	`: Prompt B`
Demander la valeur de c	`: Prompt C`
Traitement	
Calculer Δ *et Affecter la valeur à D*	: B^2-4×A×C → D
Afficher D	`: Disp D`
Si Δ *est strictement négatif*	`: If D < 0`
Alors	`: Then`
Afficher "Pas de solution réelle"	`: Disp "Pas de solution réelle"`
Fin de si	`: End`
Si Δ *est nul*	`: If D = 0`
Alors	`: Then`
Afficher "1 solution double"	`: Disp "1 solution double"`
Calculer la solution et affecter la valeur à X	: -B/(2A)→ X
Afficher la valeur de X	`: Disp X`
Fin de si	`: End`
Si Δ *est strictement positif*	`: If D > 0`
Alors	`: Then`
Afficher "2 solutions réelles"	`: Disp "2 solutions réelles"`
Calculer la première solution et affecter la valeur à X	: (-B - $\sqrt{D}$)/(2A) → X
Afficher la valeur de X	`: Disp X`
Calculer la deuxième solution et affecter la valeur à X	: (-B - $\sqrt{D}$)/(2A) → X
Afficher la valeur de X	`: Disp X`
Fin de si	`: End`

13. Après tout ceci, vous avez certainement réussi à faire tourner vos préférés.

CORRIGÉS

Cahier β

En toute logique

Sommaire

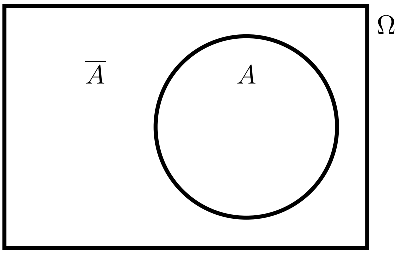
Ce cahier est fondamental pour votre scolarité et votre vie.

1 Diagrammes de Venn

Les diagrammes de Venn, ou diagrammes *en patates*, sont des représentations graphiques des relations entre plusieurs ensembles. Chaque ensemble est représenté par une forme géométrique simple comme un cercle, une ellipse ou un rectangle.

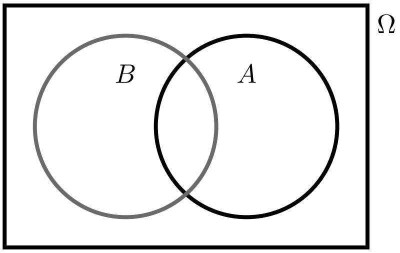
Un ensemble dans l'univers

Dans ce premier exemple, nous voyons Ω (l'intérieur du rectangle) et A, un *sous-ensemble* de Ω (l'intérieur du cercle). Le *complémentaire* de A, noté $\overline{A}$, est la partie du rectangle qui n'est pas dans le cercle.



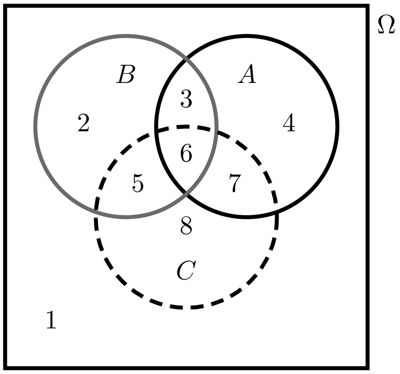
Deux ensembles dans l'univers

Dans ce second exemple, nous voyons l'univers Ω et deux sous-ensembles de Ω, A et B. L'*intersection* $A \cap B$ des deux ensembles est leur partie commune, ce qui est dans les deux cercles en même temps. L'*union* $A \cup B$ des deux ensembles est ce qui se situe dans au moins un des deux cercles, intersection incluse donc.



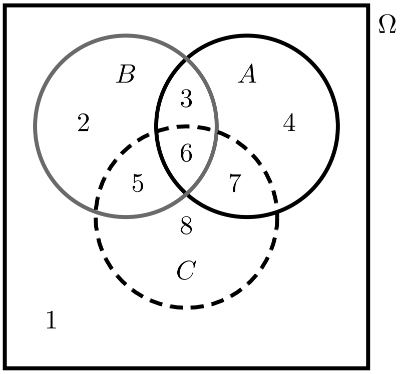
Trois ensembles dans l'univers

Dans ce troisième exemple, nous voyons l'univers Ω et trois sous-ensembles de Ω, A, B et C. Toutes les intersections et unions de deux ou trois de ces ensembles ainsi que leur complémentaire, y sont représentées.
Par exemple, la region 3 est $(A \cap B) \cap \overline{C}$, tandis que $(\overline{A} \cup B) \cap C$ est constitué des régions 5, 6 et 8.



Exercice 1

Décrire les différentes régions au moyen d'unions et d'intersections des ensembles A, B, C ainsi que leur complémentaire, et réciproquement.



(a) 1.
(b) 2.
(c) 3.
(d) 4.
(e) 5.
(f) 6.
(g) 7.
(h) 8.
(i) 3 et 6.
(j) 8 et 3.
(k) 5 et 7.
(l) 6 et 8.
(m) 1 et 7.
(n) $\overline{A \cap C}$.
(o) $\overline{A} \cup \overline{C}$.
(p) $\overline{B \cup C}$.
(q) $\overline{B} \cap \overline{C}$.
(r) $(B \cap C) \cup A$.
(s) $B \cap (C \cup A)$.
(t) $(B \cup A) \cap (C \cup A)$.
(u) $(B \cup C) \cap A$.
(v) $B \cup (C \cap A)$.
(w) $(B \cap A) \cup (C \cap A)$.
(x) $(\overline{A} \cup B) \cap C$.
(y) $\overline{B \cup C} \cap \overline{A}$.
(z) $\overline{\overline{A \cap C} \cup B}$.

Vous aurez donc remarqué que l'on a toujours $\overline{\overline{A}} = A$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$ et $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.

Exercice 2

Faire correspondre à chacun de ces ensembles, son diagramme de Venn parmi ceux des pages suivantes. Les décrire ensuite en termes d'unions et d'intersections.

A. Fonctions affines et fonctions trigonométriques telles que $f(0) = 0$.

B. Triangles isocèles non équilatéraux.

C. Parmi les réels, les entiers naturels et les nombres irrationnels.

D. Les entiers naturels qui ne sont ni multiples de 2 ni de 3.

E. Parallélogrammes dont les diagonales n'ont pas même longueur et ne sont pas perpendiculaires.

F. Parallélogrammes dont les diagonales ont même longueur et sont perpendiculaires ou ni l'un, ni l'autre.

G. Entiers multiples de 7 ou de 2 mais pas de 14.

H. Parallélogrammes dont les diagonales ont même longueur ou sont perpendiculaires ou ni l'un, ni l'autre mais pas les deux.

I. Les réels n'étant pas décimaux.

J. Les fonctions telles que $f(0) \neq 0$ qui ne sont ni affines, ni trigonométriques.

K. Les nombres réels étant décimaux.

L. Parallélogrammes ayant leurs diagonales de même longueur ou perpendiculaires.

M. Les réels irrationnels ou décimaux.

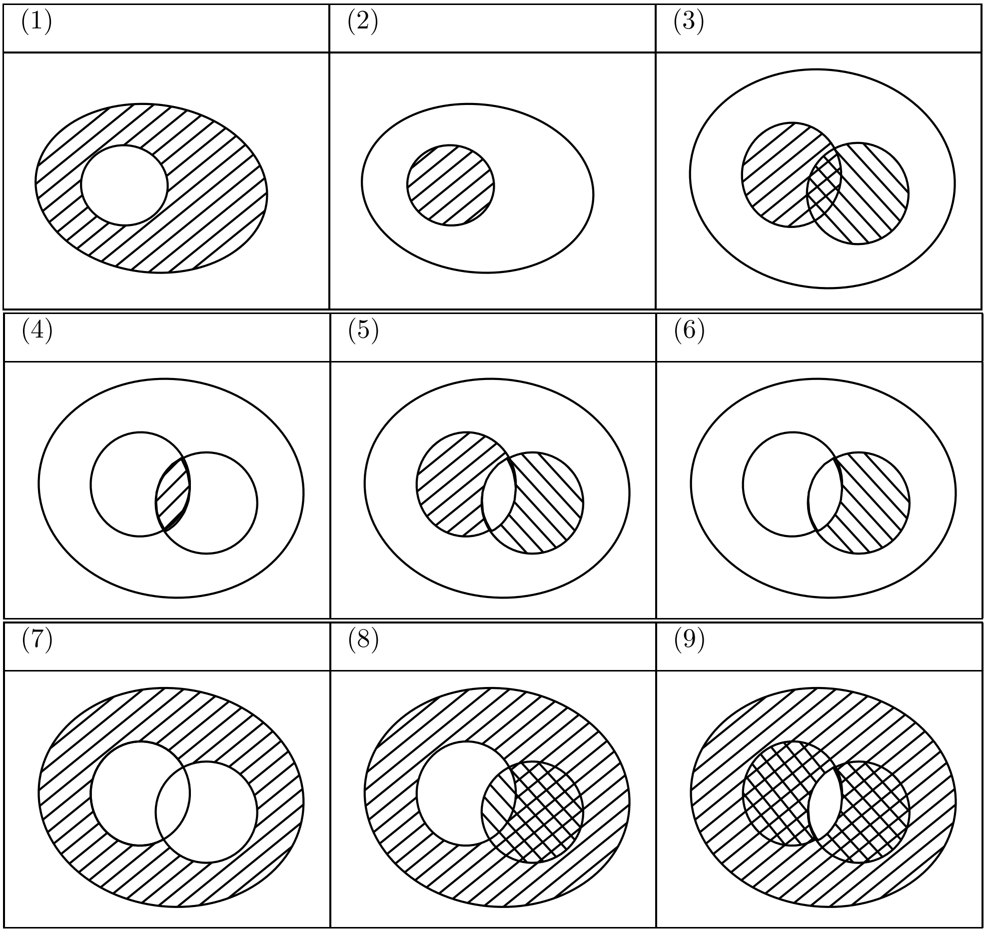
N. Les réels ni irrationnels, ni naturels.

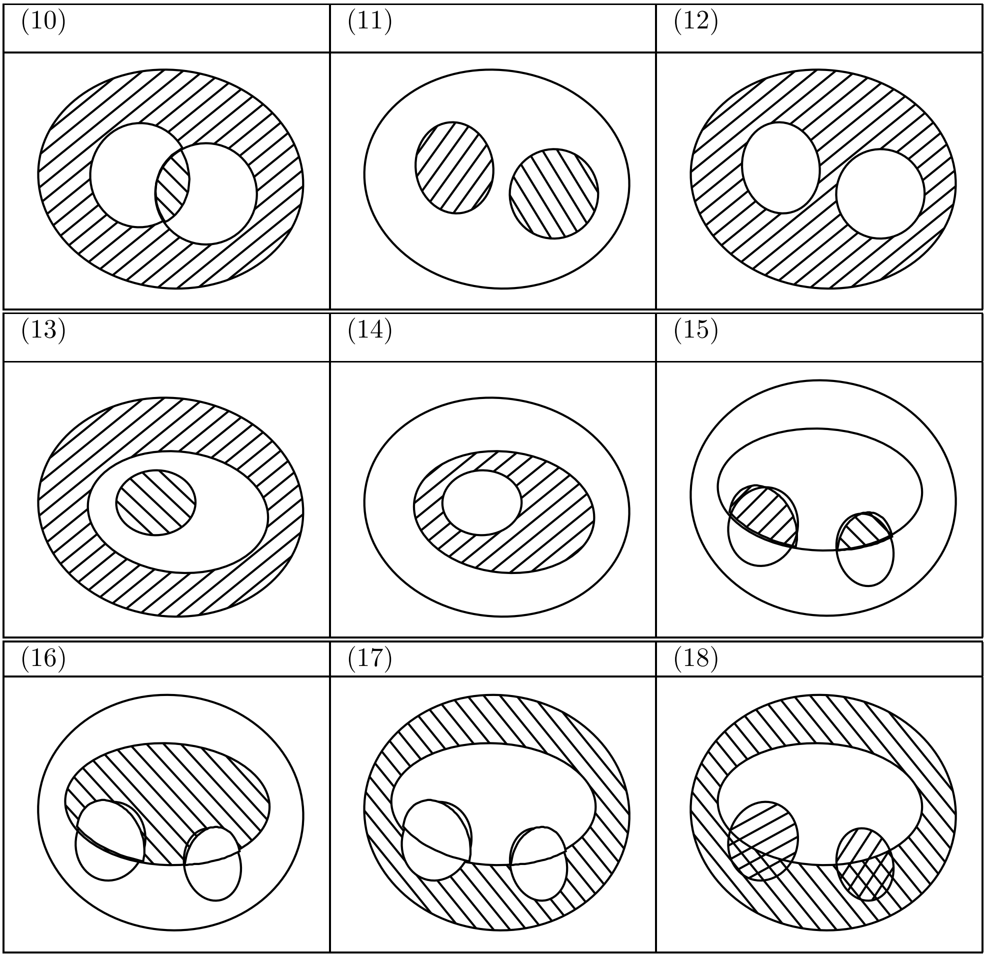
O. Parallélogrammes de diagonales de même longueur et perpendiculaires.

P. Les fonctions telles que $f(0) = 0$ qui ne sont ni affines, ni trigonométriques.

Q. Les fonctions affines, trigonométriques ou les fonctions telles que $f(0) \neq 0$.

R. Les entiers multiples de 7 qui ne sont pas pairs.





2 Ensembles

Vocabulaire

Notations ensemblistes

$\{\ldots\}$: un ensemble.

: ou | ou / : "tel que" (tq.).

$\setminus$: "privé de", $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Ensembles de nombres

$\mathbb{N}$: les entiers naturels.

$\mathbb{Z}$: les entiers relatifs

$\mathbb{D}$: les nombre décimaux.

$\mathbb{Q}$: les nombres rationnels.

$\mathbb{R}$: les nombres réels.

$\mathbb{R}^*$: les réels non nuls.

$\mathbb{R}^+$ ou $\mathbb{R}_+$: les réels positifs.

$\mathbb{R}^-$ ou $\mathbb{R}_-$: les réels négatifs.

$\mathbb{R}_+^*$: les réels strictement positifs.

Ensemble, sous-ensembles, éléments

$\cap$: l'intersection de deux ensembles.

$\cup$: l'union de deux ensembles.

$\in$: “appartient à” ou “est un élément de”.

$\subset$: “est un sous-ensemble de”.

Opérateurs logiques

$\neg$: la négation d'une proposition, “non”.

$\wedge$: la conjonction de deux propositions, “et”.

$\vee$: la disjonction de deux propositions, “ou”.

$\forall$: “pour tout”.

$\exists$: “il existe”.

$\exists!$: “il existe un unique”.

$\nexists$: “il n'existe pas”.

Un ensemble E est défini si, et seulement si, l'assertion $(x \in E) \wedge \neg(x \in E)$ est fausse.

Exercice 3 Faire correspondre chaque liste de nombres (à droite) avec l'ensemble qui la contient (à gauche).

$\{2k+1 \ : \ k \in \mathbb{Z}\} \ \ldots A$

$\left\{n \ : \ n \in \mathbb{Z} \wedge \dfrac{12}{n} \in \mathbb{Z}\right\} \ \ldots B$

$\{n^2 \ : \ n \in \mathbb{N} \cap [0\,;5]\} \ \ldots C$

$\{3k \ : \ k \in \mathbb{N}\} \ \ldots D$

$\{x \in \mathbb{R} \ : \ 3x \in \mathbb{Z}\} \ \ldots E$

$\{a + bi \ : \ a \in \mathbb{R} \wedge b \in \mathbb{R}\} \ \ldots F$

$\{7k+1 \ : \ k \in \mathbb{Z}\} \ \ldots G$

$\{n \in \mathbb{N} \ : \ \exists m \in \mathbb{Z}, m^2 = n\} \ \ldots H$

$\{x \in \mathbb{R} \ : \ x^2 = x\} \ \ldots I$

$\{x \in \mathbb{R} : \exists p, q \in \mathbb{Z}, q \neq 0 \wedge xq = p\} \ \ldots J$

$\{r \in \mathbb{R} \ : \ \exists k \in \mathbb{Z}, r^2 = k\} \ \ldots K$

$\{n \in \mathbb{Z} \ : \ |n| \leqslant 5\} \ \ldots L$

$\{x \in \mathbb{R} \ : \ |x| \leqslant 5\} \ \ldots M$

$\{x \in \mathbb{R} \ : \ \forall y \in \mathbb{N}, x \leqslant y\} \ \ldots N$

$\{(x;y) : x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge \ x + y = 7\} \ \ldots O$

$\{x \in \mathbb{R} \ : \ x \leqslant -3 \vee \ x \geqslant 5\} \ \ldots P$

$\{n \in \mathbb{Z} \ : \ \forall m \in \mathbb{Z}, n > m\} \ \ldots Q$

$\left\{n \in \mathbb{N} : \nexists m \in \mathbb{N} \setminus \{1;n\}, \dfrac{n}{m} \in \mathbb{N}\right\} \ \ldots R$

$\{(x;y) : x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge \ xy \leqslant 6\} \ \ldots S$

$\{(x;y) : x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge \ y = 2x\} \ \ldots T$

$a \ldots$ 6, 21, 336, 4272

$b \ldots$ $3 + 5i$, $\sqrt{2} - i$, 17, $-1 + \pi i$

$c \ldots$ -5, -2π, $-\frac{4}{7}$, -0.0001

$d \ldots$ 0, 1, 9, 16

$e \ldots$ -5, $-\sqrt{19}$, 17.25, 5

$f \ldots$ 0, 9, 81, 196

$g \ldots$ $\frac{12}{7}$, $-\frac{2}{3}$, 42, $\frac{-28}{2}$

$h \ldots$ 3, 6, -12, 1

$i \ldots$ 17, 2, 5, 43, 199

$j \ldots$ 5, $\sqrt{2}$, -13, $\sqrt{13}$

$k \ldots$ $(2;2)$; $(1;5)$; $(3;1)$; $(1;1)$

$l \ldots$ -4, -2, 0, 3

$m \ldots$ $\frac{7}{3}$, -17, $-\frac{52}{3}$, 0

$n \ldots$ 0, 1

$o \ldots$ -7, -3, 5, 17

$p \ldots$ $(3;6)$; $(12;24)$; $(5;10)$; $(131;262)$

$q \ldots$ $(2;5)$; $(1;6)$; $(4;3)$; $(3;4)$

$r \ldots$ $\sqrt{2}$, $-\pi$, 2.256, -4.99

$s \ldots$ -20, 1, 50, 778

$t \ldots$ $\varnothing$

Paradoxe de Russell †

L'ensemble des ensembles n'appartenant pas à eux-mêmes appartient-il à lui-même ?

Si l'on répond oui, alors, comme par définition les membres de cet ensemble n'appartiennent pas à eux-mêmes, il n'appartient pas à lui-même : contradiction. Mais si l'on répond non, alors il a la propriété requise pour appartenir à lui-même : contradiction de nouveau. On a donc une contradiction dans les deux cas, ce qui rend l'existence d'un tel ensemble paradoxale.

Plus formellement, si l'on pose $y = \{x \mid x \notin x\}$, on a immédiatement que $y \in y \iff y \notin y$ donc chacune des deux possibilités, $y \in y$ et $y \notin y$, mène à une contradiction.

Et de façon plus imagée : *Un barbier se propose de raser tous les hommes qui ne se rasent pas eux-mêmes, et seulement ceux-là. Le barbier doit-il se raser lui-même ?*

3 Logique

3.1 Propositions

Définition 1 *Une proposition est une affirmation qui peut être vraie ou fausse, mais qui ne peut être les deux en même temps ou ni l'un ni l'autre.*

Exemples : Considérons les trois propositions suivantes :

- $\mathscr{P}_1$: « $x + 2 = 2 + x$ ».
- $\mathscr{P}_2$: « $2 \times 3 = 7$ ».
- $\mathscr{P}_3$: « $x^2 = 9$ ».

∗ La proposition $\mathscr{P}_1$ est toujours vraie.

∗ La proposition $\mathscr{P}_2$ est toujours fausse.

∗ La proposition $\mathscr{P}_3$ peut être vraie ou fausse suivant les valeurs de x : si $x = 3$, elle est vraie, si $x = -3$, elle est vraie et elle est fausse dans tous les autres cas.

Exercice 4 Les trois propositions suivantes sont-elles toujours vraies ?

- $\mathscr{P}_4$: « $x - 2$ est strictement plus grand que x ».
- $\mathscr{P}_5$: « $2x$ est plus grand ou égal à x ».
- $\mathscr{P}_6$: « le carré d'un nombre pair est pair ».

Exercice 5 Énoncer une affirmation qui n'est pas une proposition.

Définition 2 *La négation d'une proposition, notée « non $\mathscr{P}$ » ou « $\neg\mathscr{P}$ », est une proposition qui est fausse lorsque $\mathscr{P}$ est vraie et qui est vraie lorsque $\mathscr{P}$ est fausse.*

Remarque : La proposition $\neg(\neg\mathscr{P})$ est précisément $\mathscr{P}$.

Exercice 6 Établir la négation des propositions $\mathscr{P}_1$ à $\mathscr{P}_6$. Sont-elles toujours vraies ?

†. Publié en 1903 par Bertrand Russell (1872–1970), troisième comte du nom. Mathématicien, logicien, épistémologue, écrivain (Nobel 1950), homme politique (membre du Parlement britannique) et moraliste gallois, Russell est considéré comme l'un des plus importants philosophes du XXe s.

Exercice 7 Établir la négation des propositions suivantes. Lesquelles sont vraies ?

- $\mathscr{P}_7$: $\forall a \in \mathbb{R},\ a^2 > 0.$
- $\mathscr{P}_8$: $\exists b \in \mathbb{R}^+$ tq. $b - 3 < 0.$
- $\mathscr{P}_9$: $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}$ tq. $x \leqslant y.$
- $\mathscr{P}_{10}$: $\exists \alpha \in \mathbb{R}^+$ tq. $\forall \beta \in \mathbb{R},\ \beta^2 - \alpha < 0.$

Toutefois, il existe des propositions *indécidables*, dont on ne peut affirmer si elles sont vraies ou fausses. C'est un fameux résultat du mathématicien Kurt Gödel (1906-1978) et je ne peux que vous conseiller de lire *La Déesse des petites victoires*, brillant roman de Yannick Grannec autour de ce personnage.

3.2 Implication

Définition 3 *Pour affirmer que « si $\mathscr{P}$ (est vraie), alors $\mathscr{Q}$ (est vraie) », les mathématiciens disent que « $\mathscr{P}$ implique $\mathscr{Q}$ » et écrivent $\mathscr{P} \Longrightarrow \mathscr{Q}$. $\mathscr{P}$ est la condition suffisante (l'hypothèse) et $\mathscr{Q}$ est la condition nécessaire (la conclusion).*

Exemples :

- Si $\underbrace{x = 3}_{\mathscr{P}}$, alors $\underbrace{x^2 = 9}_{\mathscr{Q}}$.
- Si $\underbrace{\overrightarrow{AB} = \overrightarrow{CD}}_{\mathscr{P}}$, alors $\underbrace{ABDC \text{ est un parallélogramme}}_{\mathscr{Q}}$.

Remarque : Attention, l'implication n'est pas une relation de causalité. Par exemple, l'assertion « les oiseaux volent donc la neige est blanche » est fausse mais l'implication « si les oiseaux volent alors la neige est blanche » est vraie. N'allons pas plus loin, nous risquerions d'être déconcertés.

Définition 4
L'implication $\mathscr{Q} \Longrightarrow \mathscr{P}$ est appelée l'implication réciproque de $\mathscr{P} \Longrightarrow \mathscr{Q}$.
L'implication non $\mathscr{Q} \Longrightarrow$ non $\mathscr{P}$ est appelée la contraposée de $\mathscr{P} \Longrightarrow \mathscr{Q}$.

Exercice 8 VouF ?

$\mathscr{P}$	$\mathscr{Q}$	$\mathscr{P} \Rightarrow \mathscr{Q}$	$\mathscr{Q} \Rightarrow \mathscr{P}$	$\neg\mathscr{Q} \Rightarrow \neg\mathscr{P}$	$\neg\mathscr{P} \Rightarrow \neg\mathscr{Q}$
n est premier	$n = 3$				
$x \in \mathbb{D}$	$x \in \mathbb{Q}$				
$ab = 9$	$a = 3$ et $b = 3$				
$x \geqslant 2$	$x \geqslant 3$				
$x > 0$	$x \geqslant 0$				
$x < 0$	$x^3 < 0$				

Propriété 1
Si l'implication $(\mathscr{P} \Longrightarrow \mathscr{Q})$ est vraie,
alors sa contraposée (non $\mathscr{Q} \Rightarrow$ non $\mathscr{P}$) est vraie.

Exercice 9 Quelle est la contraposée de l'implication (*non* $\mathscr{Q} \Rightarrow$ *non* $\mathscr{P}$) ?

EXERCICES

3.3 Équivalence

Définition 5
Deux propositions $\mathscr{P}$ et $\mathscr{Q}$ sont dites équivalentes si $\mathscr{P} \Longrightarrow \mathscr{Q}$ *et* $\mathscr{Q} \Longrightarrow \mathscr{P}$.
Si $\mathscr{P} \Longleftrightarrow \mathscr{Q}$, *alors* $\mathscr{P}$ *est vraie si, et seulement si,* $\mathscr{Q}$ *est vraie.*

Exemples : • $\underbrace{x = 3}_{\mathscr{P}} \Longleftrightarrow \underbrace{2x = 6}_{\mathscr{Q}}$.

• Soit $\mathscr{C}$ un cercle de diamètre $[AB]$.
$\underbrace{M \text{ est un point de } \mathscr{C} \text{ différent de } A \text{ et } B}_{\mathscr{P}}$ si, et seulement si, $\underbrace{\widehat{AMB} = 90°}_{\mathscr{Q}}$.

Exercice 10 Donner un exemple d'implication qui n'est pas une équivalence.

3.4 Exercices

Exercice 11 Très facile

A. La phrase suivante est supposée vraie :
« Si la télé est allumée, alors il y a nécessairement quelqu'un qui la regarde. »
Choisir la réponse correcte pour chaque question.

1. La télé est allumée. Quelqu'un la regarde-t-il ?
A. Oui. B. Non. C. On ne peut savoir.
2. Personne ne regarde la télé. Est-elle allumée ?
A. Oui. B. Non. C. On ne peut savoir.
3. La télé est éteinte. Quelqu'un la regarde-t-il ?
A. Oui. B. Non. C. On ne peut savoir.
4. Quelqu'un regarde la télé. Est-elle allumée ?
A. Oui. B. Non. C. On ne peut savoir.

B. Même consigne pour la phrase : « L'équation (E) n'a pas de solution négative. »

1. Est-ce que -2 est une solution de (E) ?
A. Oui. B. Non. C. On ne peut savoir.
2. a est une solution de (E). Est-ce que a est négatif ?
A. Oui. B. Non. C. On ne peut savoir.
3. 3 est-il une solution de (E) ?
A. Oui. B. Non. C. On ne peut savoir.
4. b n'est pas une solution de (E). Est-ce que b est négatif ?
A. Oui. B. Non. C. On ne peut savoir.

Exercice 12 Facile
Compléter par « donc » ou « car ».

1. J'ai eu un accident ... j'ai grillé un feu rouge.
2. Il est malade ... il ne viendra pas.
3. J'ai eu un cadeau ... c'est mon anniversaire.

4. Je ne suis pas européen ... je ne suis pas allemand.
5. Jean est triste ... c'est la fin des vacances.
6. Il pleut ... la fête est annulée.
7. (AB) et (CD) sont parallèles ... $ABCD$ est un parallélogramme.
8. $ABCD$ possède deux angles droits ... c'est un rectangle.
9. Le triangle ABC est équilatéral ... il est isocèle.
10. $y^2 = 25 \ \ldots \ y = 5$.
11. $x \in [-1\,;4] \ \ldots \ x \in [-2\,;5]$.
12. $u^2 \geqslant 49 \ \ldots \ u \geqslant 7$.
13. $\sqrt{x} \leqslant 6 \ \ldots \ x \leqslant 36$.

Exercice 13 Pas si facile

Préciser si les implications et équivalences suivantes sont vraies ou fausses.

A	B	$A \Longrightarrow B$	$B \Longrightarrow A$	$A \Longleftrightarrow B$
Je vis en France	Je vis en Europe			
Je suis un adolescent	J'ai 16 ans			
$CDEF$ parallélogramme	$CDEF$ carré			
MNP rectangle en M	$MP^2 + MN^2 = NP^2$			
$x \in \mathbb{N}$	$x \in \mathbb{Z}$			
$a + b = 5$	$a = 2$ et $b = 3$			
$4x - (x - 5) = 11$	$x = 2$			
$(ax + b)(cx + d) = 0$	$ax + b = 0$ et $cx + d = 0$			
$(ax + b)(cx + d) = 0$	$ax + b = 0$ ou $cx + d = 0$			

Exercice 14 Peu difficile

Pour chacune des affirmations suivantes, déterminer si elle est vraie ou fausse.

- Pour prouver qu'elle est fausse, il suffit de trouver un contre-exemple.
- Pour prouver qu'elle est vraie, il est nécessaire de trouver une démonstration.

1. Si $x^2 \geqslant 4$ alors $x \geqslant 2$.
2. Pour tous réels x et y, $(x + y)^3 = x^3 + y^3$.
3. Pour tout réel x, le réel $-10x$ est négatif.
4. Il existe une équation n'ayant aucune solution réelle.
5. Il existe une équation ayant cinq solutions réelles distinctes.
6. Si a et b sont deux entiers naturels, alors $\frac{(a+b)^2-(a-b)^2}{4}$ est un entier naturel.

Exercice 15 Assez difficile

Soient a et b deux entiers naturels tels que $a > b$.
Démontrer que, si $(a^2 - b^2)$ est premier, alors a et b sont consécutifs.
La réciproque est-elle vraie ?

Bonus Très plaisant

Faites-vous donc offrir puis lisez le petit *Éloge des mathématiques* d'Alain Badiou qui nous explique avec ravissement pourquoi l'on se passionne logiquement pour cette discipline.

4 Solutions

Exercice 1

Ces solutions ne sont pas toujours uniques et vous pouvez en avoir trouvé d'autres.

(a) 1 : $\overline{A \cup B \cup C}$.

(b) 2 : $B \cap \overline{A \cup C}$.

(c) 3 : $A \cap B \cap \overline{C}$.

(d) 4 : $A \cap \overline{B} \cap \overline{C}$.

(e) 5 : $B \cap C \cap \overline{A}$.

(f) 6 : $A \cap B \cap C$.

(g) 7 : $A \cap C \cap \overline{B}$.

(h) 8 : $C \cap \overline{A \cup B}$.

(i) 3 et 6 : $A \cap B$.

(j) 8 et 3 : $(C \cap \overline{B} \cap \overline{A}) \cup (A \cap B \cap \overline{C})$.

(k) 5 et 7 : $[(C \cap A) \cup (C \cap B)] \cap (\overline{A \cap B})$.

(l) 6 et 8 : $(C \cap \overline{A \cup B}) \cup (A \cap B \cap C)$.

(m) 1 et 7 : $(\overline{A \cup B \cup C}) \cup (A \cap C \cap \overline{B})$.

(n) $\overline{A \cap C}$: 1, 2, 3, 4, 5 et 8.

(o) $\overline{A} \cup \overline{C}$: 1, 2, 3, 4, 5 et 8.

(p) $\overline{B \cup C}$: 1 et 4.

(q) $\overline{B} \cap \overline{C}$: 1 et 4.

(r) $(B \cap C) \cup A$: 3, 4, 5, 6 et 7.

(s) $B \cap (C \cup A)$: 3, 5, 6.

(t) $(B \cup A) \cap (C \cup A)$: 3, 4, 5, 6, 7.

(u) $(B \cup C) \cap A$: 3, 6, 7.

(v) $B \cup (C \cap A)$: 2, 3, 5, 6, 7.

(w) $(B \cap A) \cup (C \cap A)$: 3, 6, 7.

(x) $(\overline{A} \cup B) \cap C$: 5, 6 et 8.

(y) $\overline{B \cup C} \cap \overline{A}$: 1.

(z) $\overline{\overline{A \cap C} \cup B}$: 7.

Ainsi, on a toujours, $\overline{\overline{A}} = A$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$,
$(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$ et $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.

Exercice 2 Ce qui suit est écrit de manière informelle.

(1) : (I). $\mathbb{R} \setminus \mathbb{D}$.

(2) : (K). $\mathbb{D} \subset \mathbb{R}$.

(3) : (L). $Diag.\text{É}gal. \cup Diag.Perp. \subset Parall\text{é}logrammes.$

(4) : (O). $Diag.\text{É}gal. \cap Diag.Perp. \subset Parall\text{é}logrammes.$

(5) : (G). $\{Multiples(7) \cup Multiples(2)\} \setminus Multiples(14) \subset \mathbb{Z}$.

(6) : (R). $Multiples(7) \setminus Multiples(14) \subset \mathbb{Z}$.

(7) : (D). $\mathbb{N} \setminus \{Multiples(2) \cup Multiples(3)\}$.

(8) : (E). $\overline{Rectangles} \cup Losanges \subset Parall\text{é}logrammes.$

(9) : (H). $\overline{Carr\text{é}s} \subset Parall\text{é}logrammes.$

(10) : (F). $\overline{Rectangle \cup Losanges} \cup Carr\text{é}s \subset Parall\text{é}logrammes.$

(11) : (C). $\mathbb{N} \cup Irrationnels \subset \mathbb{R}$ ou (M). $\mathbb{D} \cup Irrationnels \subset \mathbb{R}$.

(12) : (N). $\overline{\mathbb{N}} \cap \overline{Irrationnels} \subset \mathbb{R}$.

(13) : (M). $\mathbb{D} \cup Irrationnels \subset \mathbb{R}$ ou (C). $\mathbb{N} \cup Irrationnels \subset \mathbb{R}$.

(14) : (B). $Isoc\text{è}les \setminus \text{É}quilat\text{é}raux \subset Triangles.$

(15) : (A). $(Trigos \cup Affines) \cap (0 \mapsto 0)$.

(16) : (P). $\overline{Trigos \cup Affines} \cap (0 \mapsto 0)$

(17) : (J). $\overline{Trigos \cup Affines} \cap \overline{0 \mapsto 0}$

(18) : (Q). $Trigos \cup Affines \cup \overline{0 \mapsto 0}$.

Exercice 3

A - o	D - a	G - s	J - g	M - r	P - e	S - k
B - h	E - m	H - f	K - j	N - c	Q - t	T - p
C - d	F - b	I - n	L - l	O - q	R - i	

Exercice 4

- $\mathscr{P}_4$ « $x-2$ est strictement plus grand que x » : toujours faux puisque $x-2 \leqslant x$, $\forall x \in \mathbb{R}$.
- $\mathscr{P}_5$ « $2x$ est plus grand ou égal à x » : vrai pour $x \geqslant 0$, faux pour $x < 0$.
- $\mathscr{P}_6$ « le carré d'un nombre pair est pair » : toujours vrai car $(2n)^2 = 4n^2$ pair.

Exercice 5 La phrase « Il fait beau et chaud. » n'est pas une proposition mathématique car elle peut être à la fois vraie et fausse selon les préférences de chacun.
En revanche, c'est une contrepèterie amusante et facile.

Exercice 6

- $\neg\mathscr{P}_1$: « $x+2 \neq 2+x$ » : toujours faux puisque $\mathscr{P}_1$ est toujours vrai.
- $\neg\mathscr{P}_2$: « $2 \times 3 \neq 7$ » : toujours vraie puisque $\mathscr{P}_2$ est toujours fausse.
- $\neg\mathscr{P}_3$: « $x^2 \neq 9$ » : vraie pour $x \neq \pm 3$, fausse si $x = \pm 3$.
- $\neg\mathscr{P}_4$ « $x-2 < x$ » : toujours vraie car $\mathscr{P}_4$ toujours fausse.
- $\neg\mathscr{P}_5$ « $2x$ est strictement plus petit que x » : vrai pour $x < 0$, faux pour $x \geqslant 0$.
- $\neg\mathscr{P}_6$ « le carré d'un pair n'est pas pair » : toujours faux car $\mathscr{P}_6$ toujours vraie.

Exercice 7

- $\neg\mathscr{P}_7$: $\exists a \in \mathbb{R},\ a^2 \leqslant 0$ est vraie : $a = 0$ et $a^2 = 0 \leqslant 0$ donc $\mathscr{P}_7$ est fausse.
- $\mathscr{P}_8$: $\exists b \in \mathbb{R}^+$ tq. $b - 3 < 0$ est vraie : $b = 1 \in \mathbb{R}^+$ et $b - 3 = -2 < 0$
donc $\neg\mathscr{P}_8$: $\forall b \in \mathbb{R}^+,\ b - 3 \geqslant 0$ est fausse.
- $\mathscr{P}_9$: $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ tq. $x < y$ est vraie : $y = x + 1 > x$
donc $\neg\mathscr{P}_9$: $\exists x \in \mathbb{R}$ tq. $\forall y \in \mathbb{R},\ x \geqslant y$ est fausse.
- $\neg\mathscr{P}_{10}$: $\forall \alpha \in \mathbb{R}^+$, $\exists \beta \in \mathbb{R}$ tq. $\beta^2 - \alpha \geqslant 0$ est vraie : $\beta = \sqrt{\alpha}$ et $\beta^2 - \alpha = 0 \geqslant 0$
donc $\mathscr{P}_{10}$ est fausse.

Exercice 8

$\mathscr{P}$	$\mathscr{Q}$	$\mathscr{P} \Rightarrow \mathscr{Q}$	$\mathscr{Q} \Rightarrow \mathscr{P}$	$\neg\mathscr{Q} \Rightarrow \neg\mathscr{P}$	$\neg\mathscr{P} \Rightarrow \neg\mathscr{Q}$
n est premier	$n = 3$	F	V	F	V
$x \in \mathbb{D}$	$x \in \mathbb{Q}$	V	F	V	F
$ab = 9$	$a = 3$ et $b = 3$	F	V	F	V
$x \geqslant 2$	$x \geqslant 3$	F	V	F	V
$x > 0$	$x \geqslant 0$	V	F	V	F
$x < 0$	$x^3 < 0$	V	V	V	V

Exercice 9 La contraposée de $\neg\mathscr{Q} \Rightarrow \neg\mathscr{P}$ est $\neg\neg\mathscr{P} \Rightarrow \neg\neg\mathscr{Q}$ *i.e.* $\mathscr{P} \Rightarrow \mathscr{Q}$.

Exercice 10 Dans l'exercice 8, seul le dernier item concerne une implication qui est aussi une équivalence.

Exercice 11 Très facile

A. 1 - Oui. 2 - Non. 3 - On ne peut savoir. 4 - On ne peut savoir.

B. 1 - Non. 2 - Non. 3 - On ne peut savoir. 4 - On ne peut savoir.

Exercice 12 Facile

1. car	3. car	5. car	7. car	9. donc	11. donc	13. donc
2. donc	4. donc	6. donc	8. car	10. car	12. car	

Exercice 13 Pas si facile

A	B	$A \Longrightarrow B$	$B \Longrightarrow A$	$A \Longleftrightarrow B$
Je vis en France	Je vis en Europe	Vrai	Faux	Faux
Je suis un adolescent	J'ai 16 ans	Faux	Vrai	Faux
$CDEF$ parallélogramme	$CDEF$ carré	Faux	Vrai	Faux
MNP rectangle en M	$MP^2 + MN^2 = NP^2$	Vrai	Vrai	Vrai
$x \in \mathbb{N}$	$x \in \mathbb{Z}$	Vrai	Faux	Faux
$a + b = 5$	$a = 2$ et $b = 3$	Faux	Vrai	Faux
$4x - (x - 5) = 11$	$x = 2$	Vrai	Vrai	Vrai
$(ax + b)(cx + d) = 0$	$ax + b = 0$ et $cx + d = 0$	Faux	Vrai	Faux
$(ax + b)(cx + d) = 0$	$ax + b = 0$ ou $cx + d = 0$	Vrai	Vrai	Vrai

Exercice 14 Peu difficile

1. Si $x^2 \geqslant 4$ alors $x \geqslant 2$ Faux. $x = -3$ par exemple.
2. Pour tous réels x et y, $(x + y)^3 = x^3 + y^3$: Faux. $x = y = 1$ par exemple.
3. Pour tout réel x, le réel $-10x$ est négatif : Faux. $x = -1$ par exemple.
4. Il existe une équation n'ayant aucune solution réelle : Vrai, $x^2 + 1 = 0$ par exemple.
5. Il existe une équation ayant cinq solutions réelles distinctes : Vrai.
   $x(x - 1)(x + 1)(x - 2)(x + 2) = 0$ par exemple.
6. Si a et b sont deux entiers naturels, alors $\frac{(a+b)^2-(a-b)^2}{4}$ est un entier naturel :
   Vrai car $\frac{(a+b)^2-(a-b)^2}{4} = \frac{[(a+b)+(a-b)][(a+b)-(a-b)]}{4} = \frac{(2a)(2b)}{4} = ab \in \mathbb{N}$.

Exercice 15 Assez difficile

Soient a et b deux entiers naturels tels que $a > b$.

Si $(a^2 - b^2) = (a + b)(a - b)$ est premier alors il a exactement deux diviseurs et donc l'un des deux termes est égal à 1, le plus petit des deux nécessairement. Ainsi, $a - b = 1$: a et b sont consécutifs.

Réciproquement, si a et b sont consécutifs, $a^2 - b^2$ n'est pas toujours premier. Par exemple, $5^2 - 4^2 = 9$ est dans la table de 3.

Cahier γ

FAUTE DE PREUVES

Sommaire

Cet extra est capital pour l'argumentation.

Associer chacun des types de « preuve » suivants avec son explication en pages suivantes puis préciser leur validité.

Types de preuve

- ❐ Preuve visuelle
- ❐ Preuve par identité multiplicative
- ❐ Preuve par restriction
- ❐ Preuve par présupposition
- ❐ Preuve par croyance
- ❐ Preuve par construction
- ❐ Preuve capitale
- ❐ Preuve complexe
- ❐ Preuve faible
- ❐ Preuve par large consensus
- ❐ Preuve d'août
- ❐ Preuve par défaut
- ❐ Preuve forte
- ❐ Preuve par transposition
- ❐ Preuve enfantine
- ❐ Preuve par délégation
- ❐ Preuve directe
- ❐ Preuve par Darth Vader
- ❐ Preuve par le chocolat
- ❐ Preuve par désaccord
- ❐ Preuve par distraction
- ❐ Preuve par disjonction des cas
- ❐ Preuve de l'ingénieur
- ❐ Preuve par analyse-synthèse
- ❐ Preuve par diagramme
- ❐ Preuve par récurrence
- ❐ Preuve par six fois sept
- ❐ Preuve par la peur
- ❐ Preuve par répétition
- ❐ Preuve par l'absurde
- ❐ Preuve stupide

1	Type de preuve		Valide	Non valide

Il suffit de multiplier chaque expression par zéro afin d'obtenir l'égalité voulue. Par exemple, prouvons que $1 = 2$:

$$1 = 2 \quad \Longleftrightarrow \quad 1 \times 0 = 2 \times 0 \quad \Longleftrightarrow \quad 0 = 0.$$

Puisque la dernière égalité est vraie, la première l'est aussi.

2	Type de preuve		Valide	Non valide

Puisqu'août est une période si agréable, personne ne sera en désaccord avec ce qui est publié à ce moment-là, ce qui en atteste la véracité. Bien sûr, l'inverse est vraie : janvier est triste et aucune logique ne prouvera vos affirmations.

3	Type de preuve		Valide	Non valide

UN ARGUMENTAIRE ÉCRIT EN LETTRES CAPITALES EST CORRECT. AINSI, ÉCRIVEZ LA PROPOSITION QUE VOUS ESSAYEZ DE PROUVER EN LETTRES MAJUSCULES : ELLE SERA ALORS JUSTE !!! VOUS POUVEZ AUSSI ABUSER DES POINTS D'EXCLAMATION, EN PARTICULIER POUR LES PREUVES DIFFICILES.

4	Type de preuve		Valide	Non valide

En écrivant ce qui semble être une démonstration complète puis en étalant du chocolat fondu sur les parties les plus délicates, le lecteur supposera avec délectation que la preuve est correcte afin de ne pas paraître idiot.

5	Type de preuve		Valide	Non valide

Dans ce type de démonstration, on arrive à la conclusion en divisant le problème en un nombre fini de cas et en les démontrant chacun séparément. Le nombre de cas peut parfois être démesuré. Par exemple, la première démonstration du théorème des quatre couleurs comportait 1 936 cas. Cette démonstration est controversée car la majorité d'entre eux furent vérifiés par ordinateur, pas à la main. Aujourd'hui, la démonstration comporte encore plus de 600 cas.

6	Type de preuve		Valide	Non valide

Souvenez-vous, une affirmation est fausse si sa preuve a été vérifiée et elle est vraie si elle n'a pas été contredite. Ainsi, la meilleure stratégie est de réduire le plus possible le nombre de personnes capables de comprendre votre démonstration.
N'hésitez pas à y mettre des éléments très compliqués comme des dimensions multiples ou même infinies, des nombres hypercomplexes, des formes indéterminées, des graphes, des références à des livres épuisés, des films disparus, des chants inconnus, de la physique quantique, de la musique modale... Faites des citations en latin, grec, sanskrit et inventez des langues.
Encore une fois, le but est que personne n'y comprenne rien et ne puisse donc vous contredire.

7	Type de preuve		Valide	Non valide

S'il y a un nombre conséquent de personnes qui pensent qu'un résultat est juste, alors il l'est certainement. Pour une preuve plus emphatique, on peut user de phrases comme “De nombreux scientifiques s'accordent sur...” aux moments opportuns.

8	Type de preuve		Valide	Non valide

Commencez par démontrer un premier cas, l'initialisation, puis montrez l'hérédité de votre propriété : si un cas quelconque est vrai, alors le suivant l'est aussi. Alors, tous sont vrais à partir du cas initial, même si, séparément, chacun n'a pas été démontré. Soit $P(n)$ une proposition mathématique impliquant l'entier naturel n telle que :

(i) $P(0)$ est vraie, i.e. $P(n)$ est vraie pour $n = 0$;

(ii) $P(n+1)$ est vraie si $P(n)$ est vraie, i.e. $P(n)$ vraie implique $P(n+1)$ vraie.

Alors $P(n)$ est vraie pour tout entier naturel n.

9	Type de preuve		Valide	Non valide

J'ai raison, na !

10	Type de preuve		Valide	Non valide

La proposition est vraie par manque de contre-exemple. De toutes façons, vous savez que vous avez raison et peu vous importe ce que peuvent penser les autres.

11	Type de preuve		Valide	Non valide

Bien que non formelle, une démonstration visuelle d'un théorème. Ce type de preuve est souvent utilisé pour démontrer le théorème de Pythagore.

12	Type de preuve		Valide	Non valide

J'ai raison parce que je suis ton père.

13	Type de preuve		Valide	Non valide

Facilitez-vous la vie en laissant la démonstration au lecteur. Après tout, si vous savez la faire, il le peut certainement lui aussi. Encouragez-le :

- "Le lecteur pourra facilement effectuer ces menus calculs."
- "Les 253 autres cas sont similaires."
- "La preuve est laissée en exercice pour le lecteur".
- "La preuve est laissée en exercice pour le correcteur" (succès garanti en examen).

14	Type de preuve		Valide	Non valide

Aussi appelée preuve par l'exemple, il suffit d'exhiber un exemple concret ayant toutes les propriétés voulues pour démontrer l'existence de tels objets. Par exemple, Joseph Liouville a prouvé l'existence des nombres transcendants en en construisant un explicitement.

15	Type de preuve		Valide	Non valide

S'il y a consensus sur un sujet que vous n'acceptez pas, alors vous avez certainement raison puisque les autres sont stupides.
Pensez aux climato-sceptiques, aux créationnistes, à Donald... pour une application de ce type de preuve.

16	Type de preuve		Valide	Non valide

« Je crois en cette affirmation donc elle est vraie, cqfd. »

17	Type de preuve		Valide	Non valide

Réduire le problème à des diagrammes contenant de nombreuses flèches, simples et doubles. Ceci est lié à la preuve par complexité.

18	Type de preuve		Valide	Non valide

Dans ce type de preuve, aussi appelé par *contradiction*, on montre que si une certaine proposition est vraie, alors une contradiction (flagrante) apparaît, donc cette proposition est fausse. On louvoie donc dans le *faux*, en toute connaissance de cause, afin de prouver le *vrai*. C'est un type de preuve absolument sublime.
Voici un exemple montrant l'irrationalité de $\sqrt{2}$:

> Supposons que $\sqrt{2}$ est rationnel *i.e.* $\sqrt{2} = \frac{a}{b}$ où a et b sont des entiers non nuls premiers entre eux (la fraction est réduite). Ainsi, $b\sqrt{2} = a$. Élevant au carré, $2b^2 = a^2$. Puisque 2 divise le membre de gauche, il divise celui de droite et a^2 est pair, ce qui implique que a doit aussi être pair. On a alors $a = 2c$, où c est un entier. La première équation s'écrit alors $2b^2 = (2c)^2 = 4c^2$. Divisant par 2, $b^2 = 2c^2$. Ainsi, par le même argument que précédemment, 2 doit diviser b^2, et b doit être pair. Mais, si a et b sont tous deux pairs, ils ne peuvent être premiers entre eux ce qui contredit l'hypothèse de départ. Force est donc d'affirmer que $\sqrt{2}$ est un nombre irrationnel.

19	Type de preuve		Valide	Non valide

Soit $P(n)$ une proposition.

1° Prouvez que $P(0)$ est vraie.

2° Prouvez que $P(1)$ est vraie.

3° Prouvez que $P(2)$ est vraie.

Alors, $P(n)$ est vraie pour tout n.

20	Type de preuve		Valide	Non valide

On prouve la proposition “si p alors q” en démontrant sa contraposée “si *non* q alors *non* p”.

21	Type de preuve		Valide	Non valide

Si Khaleesi affirme quelque chose, alors c'est vrai. Pas de *si*, *mais* ni *or*. Fin de la discussion. Cela peut aussi marcher avec Voldemort, Kim Jong-un ou votre professeur de mathématiques bien-aimé.

22	Type de preuve		Valide	Non valide

Vous êtes fatigués, c'est l'heure de la sieste, vous vous sentez las, las, las. Tout affaibli, vous ne pouvez qu'accepter la preuve que l'on vous apporte.

23	Type de preuve		Valide	Non valide

Dans ce type de preuve, on arrive à la conclusion en combinant de façon logique les axiomes, définitions et les résultats précédents. Par exemple, on peut ainsi établir que la somme de deux entiers pairs est toujours paire :

> Soient x et y deux entiers pairs. il peuvent donc s'écrire $x = 2a$ et $y = 2b$ où a et b sont entiers. Alors, leur somme vaut $x + y = 2a + 2b = 2(a + b)$. Il est alors clair que $x + y$ est divisible par 2 et il est donc pair.

Cette preuve n'utilise que la définition des nombres pairs ainsi que la distributivité.

24	Type de preuve		Valide	Non valide

Puisque quarante-deux est bien la réponse universelle, tout argument impliquant le produit de six par sept est véridique.

25	Type de preuve		Valide	Non valide

N'hésitez pas à distraire l'attention des auditeurs lors de votre exposé. Un complice peut tirer la sonnette d'alarme, annoncer la fin du monde, attirer l'attention sur le mur du fond... pendant que vous effacez le tableau et déclarez la démonstration finie.

Vous pouvez aussi tirer avantage d'une distraction plus longue que prévue en démontrant par là-même le résultat suivant. Par exemple :

1. "Regardez derrière vous !"
2. ... ce qui prouve l'existence d'une réponse à $2 + 2$.
3. "Là, un singe à trois têtes !"
4. ... ce qui donne 5 comme seul résultat possible à $2 + 2$.
5. Ainsi, $2 + 2 = 5$, cqfd.

26	Type de preuve		Valide	Non valide

Si l'on dit qu'une affirmation est vraie un grand nombre de fois, alors elle est vraie. Si l'on dit qu'une affirmation est vraie un grand nombre de fois, alors elle est vraie. Si l'on dit qu'une affirmation est vraie un grand nombre de fois, alors...

Le nombre de fois qu'il faut le dire exactement pour que cela soit vérifié fait l'objet d'intenses débats académiques. Généralement, on s'arrête lorsque l'audience est littéralement morte d'ennui.

Par exemple : Soient A et B. On a $A = B \iff B = A \iff A = B$
$\iff B = A \iff A = B \iff B = A \iff A = B \iff B = A$
$\iff A = B \iff B = A \iff A = B \iff B = A$ donc $A = B$.

27	Type de preuve		Valide	Non valide

Dans un raccourci de la preuve par récurrence, on fait l'hypothèse que le résultat est vrai. Ainsi, le résultat est vrai.

28	Type de preuve		Valide	Non valide

Si vous prouvez votre affirmation pour un cas et vous restreignez à celui-ci seulement, vous évitez alors tous les autres. Vous pouvez alors espérer que personne ne remarquera votre omission.

Par exemple, montrez le théorème des quatre couleurs en se contentant des cartes à une seule région. Une seule couleur est alors nécessaire et $1 \leqslant 4$.

Si jamais on vous parle d'une certaine incomplétude de votre preuve, rabattez-vous sur une méthode précédente.

29	Type de preuve		Valide	Non valide

Ce que je dis est vrai car je suis plus fort que toi.

30	Type de preuve		Valide	Non valide

Un tel raisonnement se déroule en deux étapes :

- on raisonne sur une hypothétique solution au problème et l'on accumule des déductions de propriétés qu'elle doit vérifier, du seul fait qu'elle est solution ;
- on examine tous les objets vérifiant les conditions nécessaires précédemment accumulées (ce sont les seuls candidats pouvant être des solutions) et l'on détermine, parmi eux, lesquels sont réellement des solutions.

Il arrive souvent que la première phase, l'analyse, produise des conditions nécessaires si restrictives qu'il ne reste plus qu'un “candidat” qui les vérifie. Dans ce cas, cette première phase prouve l'unicité de la solution, et la seconde phase, la synthèse, permet de montrer soit l'existence d'une solution (si ce candidat répond au problème), soit qu'il n'y a aucune solution (sinon).

La recherche des minima et maxima d'une fonction se fait souvent ainsi : on détermine d'abord la liste des points qui auraient le droit d'être des extrema en utilisant des conditions nécessaires d'optimalité (dérivée, extrema liés…). Ensuite, on regarde lesquels parmi eux le sont vraiment en comparant leurs valeurs.

La limite d'une suite récurrente se détermine parfois par analyse synthèse : on montre qu'elle converge, car croissante et majorée par exemple, on cherche ensuite les points fixes de la fonction de récurrence qui est continue puis on détermine ceux qui peuvent être la limite de la suite : il n'y en a souvent plus qu'un possible et c'est donc lui.

31	Type de preuve		Valide	Non valide

Je n'y comprends rien, c'est donc vrai.

Solutions

Preuve visuelle : 11 **Valide**
Preuve par identité multiplicative : 1
Preuve par restriction : 28
Preuve par présupposition : 27
Preuve par croyance : 16
Preuve par construction : 14 **Valide**
Preuve capitale : 3
Preuve complexe : 6
Preuve faible : 22
Preuve par large consensus : 7
Preuve d'août : 2
Preuve par défaut : 10
Preuve forte : 29
Preuve par transposition : 20 **Valide**
Preuve enfantine : 9
Preuve par délégation : 13
Preuve directe : 23 **Valide**
Preuve par Darth Vader : 12
Preuve par le chocolat : 4
Preuve par désaccord : 15
Preuve par distraction : 25
Preuve par disjonction des cas : 5 **Valide**
Preuve de l'ingénieur : 19
Preuve par analyse-synthèse : 30 **Valide**
Preuve par diagramme : 17
Preuve par récurrence : 8 **Valide**
Preuve par six fois sept : 24
Preuve par la peur : 21
Preuve par répétition : 26
Preuve par l'absurde : 18 **Valide**
Preuve stupide : 31

Si vous avez validé à tort plus de deux « preuves », vous commencez malheureusement à maîtriser *l'art d'avoir toujours raison*.

Extras

Extra A

TROP GRAND ÉCART

Cet extra est sensationnel pour redécouvrir la valeur absolue.

Exercices

Exercice 1 On cherche à déterminer l'ensemble $\mathcal{I}$ des fonctions f vérifiant les propriétés suivantes :

- f est définie sur $[0;1]$,
- f est à valeurs dans $[0;1]$: $\forall x \in [0;1],\ f(x) \in [0;1]$,
- Pour tout $a, b \in [0;1]$, on a l'inégalité $(I) : \quad |f(a) - f(b)| \geqslant |a - b|$.

1. (a) Justifier que, pour tout μ et $\nu \in [0;1]$, $\quad |\mu - \nu| \leqslant 1$.

   (b) En déduire que, pour $f \in \mathcal{I}$, on a
   soit $(i) : f(0) = 0$ et $f(1) = 1$, soit $(ii) : f(0) = 1$ et $f(1) = 0$.

2. (a) Déterminer les deux fonctions affines u et v vérifiant l'une (i), l'autre (ii).

   (b) Vérifier que u et v appartiennent à $\mathcal{I}$.

3. Soit $f \in \mathcal{I}$ vérifiant (i).

   (a) Montrer que, pour tout $x \in [0;1]$, $\quad f(x) \geqslant u(x)$.

   (b) Montrer que, pour tout $x \in [0;1]$, $\quad f(x) \leqslant u(x)$.

   (c) Qu'en déduire pour f ?

4. Soit $f \in \mathcal{I}$ vérifiant (ii).
   De façon analogue, montrer que pour tout $x \in [0;1]$, $\quad f(x) = v(x)$.

5. Conclure sur $\mathcal{I}$ puis tenter d'expliquer le titre de ce devoir.

Exercice 2 Soient les fonctions f et g définies sur $\mathbb{R}$ par
$f(x) = \sqrt{x^2+1} \quad$ et $\quad g(x) = |x|$.

1. Tracer leur représentation graphique $\mathscr{C}_f$ et $\mathscr{C}_g$ dans un repère adapté sur GeoGebra. À première vue, $\mathscr{C}_f$ va-t-elle passer au-dessous de $\mathscr{C}_g$?
2. Démontrer que pour réel x non nul, on a $\quad f(x) = |x|\sqrt{1 + \dfrac{1}{x^2}}$.
3. Montrer que pour tout réel x, on a $\quad f(x) - g(x) > 0$.
4. En déduire les positions relatives de $\mathscr{C}_f$ et $\mathscr{C}_g$.

EXERCICES

Solutions

Exercice 1

1. (a) Puisque $0 \leqslant \mu \leqslant 1$ et $-1 \leqslant -\nu \leqslant -0$, on a $0-1 \leqslant \mu-\nu \leqslant 1-0$ *i.e.* $|\mu-\nu| \leqslant 1$.

   (b) Ainsi, comme $f(0)$ et $f(1) \in [\,0\,;1\,]$, $|f(1)-f(0)| \leqslant 1$.
   Par ailleurs, $f \in \mathcal{I}$ donc $|f(1)-f(0)| \geqslant |1-0| = 1$.
   On a donc $|f(1)-f(0)| = 1$ qui ne peuvent alors être que les valeurs « extrêmes » 0 et 1.
   En effet, on a soit $f(1)-f(0)=1$ et $1+0 \leqslant 1+f(0) = f(1) \leqslant 1$, soit $f(0)-f(1)=1$ et $1+0 \leqslant 1+f(1) = f(0) \leqslant 1$.

2. (a) On cherche des fonctions sous la forme "$mx+p$".

   (i) Puisque l'on doit avoir $m+p=1$ et $p=0$, la seule fonction affine vérifiant (i) est $u(x)=x$.

   (ii) Et puisque l'on doit avoir $m+p=0$ et $p=1$, la seule fonction affine vérifiant (ii) est $v(x)=1-x$.

   (b) Soient a, $b \in [\,0\,;1\,]$.
   On a $0 \leqslant u(a) = a \leqslant 1$ et $|u(a)-u(b)| = |a-b| \geqslant |a-b|$.
   De même, $1-0 \geqslant v(a) = 1-a \geqslant 1-1$
   et $|v(a)-v(b)| = |1-a-1+b| = |b-a| \geqslant |a-b|$.

3. Soit $f \in \mathcal{I}$ vérifiant (i) et soit $x \in [\,0\,;1\,]$.

   (a) On a $u(x) = x = |x| = |x-0| \leqslant |f(x)-f(0)| = |f(x)-0| = |f(x)| = f(x)$.

   (b) On a $1-u(x) = 1-x = |1-x| \leqslant |f(1)-f(x)| = |1-f(x)| = 1-f(x)$ d'où $f(x) \leqslant u(x)$.

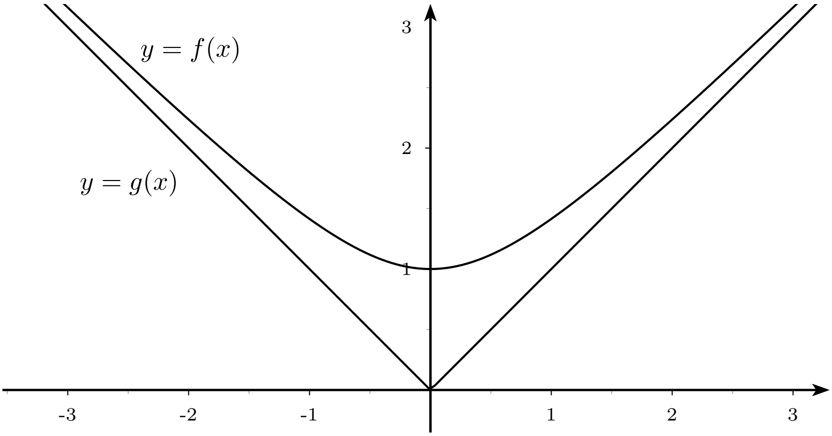
   (c) Ainsi, $f(x)=u(x)$ sur $[\,0\,;1\,]$.

4. Soit $f \in \mathcal{I}$ vérifiant (ii) et soit $x \in [\,0\,;1\,]$.
   On a $v(x) = 1-x = |x-1| \leqslant |f(x)-f(1)| = |f(x)-0| = |f(x)| = f(x)$
   et $1-v(x) = x = |0-x| \leqslant |f(0)-f(x)| = |1-f(x)| = 1-f(x)$
   d'où $f(x) \leqslant v(x)$.
   Ainsi, $f(x) = v(x)$ sur $[\,0\,;1\,]$.

5. L'ensemble $\mathcal{I}$ est donc uniquement constitué des deux fonctions $x \longmapsto x$ et $x \longmapsto 1-x$ qui vérifient en fait une relation plus précise sur $[\,0\,;1\,]$:
   $|f(a)-f(b)| = |a-b|$.
   Ainsi, une fonction de $[\,0\,;1\,]$ sur $[\,0\,;1\,]$ ne peut pas « toujours » dépasser la pente 1 en valeur absolue. En effet, (I) peut s'écrire, pour $a \neq b$, $\left|\frac{f(a)-f(b)}{a-b}\right| \geqslant 1$ qui correspond à la « pente » de f entre a et b.

Exercice 2

f et g sont définies sur $\mathbb{R}$ par $f(x) = \sqrt{x^2+1}$ et $g(x) = |x|$.

1. 

   Il ne semble pas que la courbe $\mathscr{C}_f$ passe au-dessous de la courbe $\mathscr{C}_g$.

2. On a, $\forall x \neq 0$,
$$f(x) = \sqrt{x^2+1} = \sqrt{x^2\left(1+\frac{1}{x^2}\right)} = \sqrt{x^2}\sqrt{1+\frac{1}{x^2}} = |x|\sqrt{1+\frac{1}{x^2}}.$$

3. Ainsi, $\forall x \neq 0$, on a $f(x) - g(x) = |x|\sqrt{1+\frac{1}{x^2}} - |x| = |x|\left(\sqrt{1+\frac{1}{x^2}} - 1\right)$ du signe de $\sqrt{1+\frac{1}{x^2}} - \sqrt{1}$. Or, $1 + \frac{1}{x^2} > 1$ donc, la fonction racine étant croissante, $\sqrt{1+\frac{1}{x^2}} > \sqrt{1}$ et $f(x) - g(x) > 0$.
   Si $x = 0$, $f(0) = \sqrt{1} > 0 = g(0)$.

4. La courbe $\mathscr{C}_f$ est donc située au-dessus de la courbe $\mathscr{C}_g$ sur $\mathbb{R}$.

CORRIGÉS

Extra B

EINSTEIN VAUT MIEUX QUE DEUX TU L'AURAS

Cet extra est récréatif.

Énigme

Il y a cinq maisons de cinq couleurs différentes, alignées le long d'une route. Dans chacune de ces maisons vit une personne de nationalité différente. Chacune de ces personnes boit une boisson différente, pratique un sport différent et possède un animal domestique différent.

1. Le Qatari séjourne dans la maison grenat.
2. L'Uruguayen dresse des manchots.
3. Le Wallon s'abreuve de thé.
4. La maison violette est directement à gauche de la maison beige.
5. Le kayakiste élève des rhinocéros.
6. On apprécie le café dans la maison violette.
7. Le propriétaire de la maison indigo joue au jokari.
8. La personne qui occupe la maison du centre sirote du lait.
9. Le Fidjien habite dans la première maison.
10. Le nageur loge à côté de celui qui possède des yacks.
11. Le hockeyeur ingurgite du soda.
12. Celui qui prend soin de ses zèbres est voisin de celui qui pratique le jokari.
13. L'Ouzbek vole en deltaplane.
14. Le Fidjien réside juste à côté de la maison azur.
15. Celui qui pratique la natation a un voisin qui ne boit que de l'eau.

Question : Qui a un poisson ?

Cette énigme est attribuée à Albert Einstein selon qui, seulement 2 % des individus seraient capable de résoudre cette énigme sans papier ni crayon, de tête. Et vous ?

Aide

Moi, j'ai listé les initiales, dressé un tableau et mis les maisons sur la première ligne, de gauche à droite. J'ai rempli plutôt facilement quelques cases puis j'ai fait les associations imposées et les ai testées dans mon tableau. Ainsi, j'ai trouvé... avec un papier et un stylo.

Solution

La première maison est indigo. Son propriétaire est le Fidjien, qui boit de l'eau, joue au jokari et a des yacks.

La seconde maison est azur. Son propriétaire est le Wallon, qui boit du thé, pratique la natation et a des zèbres.

La troisième maison est grenat. Son propriétaire est le Qatari, qui boit du lait, fait du kayak et a des rhinocéros.

La quatrième maison est violette. Son propriétaire est l'Ouzbek, qui boit du café, vole en deltaplane et a un poisson.

La dernière maison est beige. Son propriétaire est l'Uruguayen, qui boit du soda, pratique le hockey et a des manchots.

C'est donc l'Ouzbek qui possède un poisson.

If

Cet extra est instructif.

Si tu lis une première fois l'énoncé afin de comprendre la structure du problème,

Si tu rédiges correctement et montres comment les résultats sont obtenus et ne te contentes pas de la réponse ; sache que le correcteur la connaît déjà et qu'il juge seulement ton travail,

Si tu prends le temps de te relire avant de sortir comme si ce n'était pas ta copie et corriges ainsi maintes fautes de français et de mathématiques,

Si tu fais des phrases de conclusions, sans faute d'orthographe, un tableau ne concluant rien tout seul par exemple,

Si tu évites les tirets, qui sont des signes $-$ et préfères les étoiles, d'autant que c'est plus joli,

Si tu n'abrèges pas les barres de fractions car le signe $-$ s'applique alors sur tout le numérateur le cas échéant,

Si tu prends soin de ta calligraphie : p, P, $\mathscr{P}$, $\mathcal{P}$, ρ... désignant des objets différents,

Si tu réponds à toutes les questions, dans l'ordre, surtout si tu sais y répondre,

Si tu utilises des résultats précédents mais ne te sers point d'une question suivante,

Si tu remarques qu'il n'est pas anodin qu'une consigne commençe par « en déduire » et qu'il ne faut alors pas faire autrement,

Si tu vérifies et contre-vérifies tes résultats avec l'énoncé, les résultats obtenus précédemment, les résultats attendus, les résultats théoriques... tout ce que tu peux excepté la copie d'un tiers,

Si tu ne confonds pas $=$ et $\iff$: deux nombres, vecteurs, expressions algébriques, fonctions... peuvent être égaux mais des équations, des propositions... sont équivalentes,

Si tu n'effectues pas trois calculs en un passage de ligne car tu fais souvent faux comme, par exemple, la factorisation par a et l'identité remarquable en même temps pour la forme canonique,

Si tu sais calculer avec les fractions de manière infaillible, Si tu simplifies systématiquement les fractions et, en particulier, ne laisses pas un dénominateur négatif : cela t'évite le ridicule et les erreurs,

Si tu ne confonds pas « racines d'un polynôme » et « solutions d'une équation algébrique »,

Si tu ne t'encombres pas l'esprit et utilises des formules le moins possible : celle de la forme canonique est souvent mal appliquée, celles de Δ et $x_{1,2}$ en première sont bien suffisantes et tu auras bientôt de nombreuses formules de dérivation autrement plus importantes et plus difficiles à retrouver,

Si tu résous une équation en trouvant la valeur de l'inconnue, généralement x, et non une valeur d'un X, d'un t ou de $\frac{2}{x+3}$; lors d'un changement de variable, change d'abord x en X puis trouve des solutions X_1 et X_2 et repasse ensuite vers x_1 et x_2 par exemple,

Si tu n'oublies pas de tester tes solutions,

Si tu es méticuleux et ne confonds pas $1 - x$ et $x - 1$ par exemple au lieu de passer en force ; de même, $b \neq -b$ donc si $b = -56$, $-b = 56$; $c = -3$ et $c^2 = 9$ mais $a^2 = 4 \Rightarrow a = \pm 2$,

Si tu fais attention aux couples : le sommet d'une parabole est un point du plan et possède ainsi deux coordonnées : $\frac{-b}{2a}$ et son image, l'extremum,

Si tu sais dresser un tableau de signes et ne remplis pas des cases sous les nombres mais bien entre les nombres ; la première ligne correspond aux « x » et les suivantes aux « y », alors ne mélange pas tout ; les doubles barres sont réservées aux valeurs interdites et surtout pas aux racines,

Si tu n'hésites pas, dans un tableau de variations, à faire une haute ligne de variations pour pouvoir distinguer le sens des flèches,

Si tu regardes au final à quoi ressemble ton ouvrage et que tu n'y comprends pas grand-chose, pense que cela sera pire pour le correcteur,

Si tu écris des choses vraies car il est infiniment mieux d'écrire peu et juste que des pages entières mais fausses,

Si surtout, les mathématiques te passionnent,

Tu seras bon, mon élève.

ANNEXES

Notations & Abréviations

Cette partie n'a pas un but exhaustif mais simplement indicatif pour ceux qui aurait un doute, d'autant que l'on use dans cet ouvrage de certaines abréviations non conventionnelles, par commodité généralement. Après leur description, il y aura souvent la référence de la page de leur première utilisation.

Commençons par lister quelques notations et abréviations classiques et usuelles dans le petit monde des mathématiques.

- $\forall$: « pour tout », le quantificateur universel (cf. page 361).
- $\exists$: « il existe (au moins un) », le quantificateur existentiel (cf. page 361).
- ! : « un unique » lorsque précédé de $\exists$. Exemple : $\exists! x \in \mathbb{R}^- \cap \mathbb{R}^+$ (cf. p.361).
- ! : « factorielle » lorsque suivi d'un nombre entier.
  Par exemple, $4! = 1 \times 2 \times 3 \times 4 = 24$ (cf. page 21).
- $\setminus$: « privé de ». Exemple, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ (cf. page 361).
- $\pm$ et $\mp$: « plus ou moins » et « moins ou plus ». Signifie « soit $+$, soit $-$ » (et surtout pas « environ », attention).
- $\subset$: « inclus dans ». Se dit d'un sous-ensemble (cf. page 361).
- c.q.f.d. et $\square$: « ce qu'il fallait démontrer ».
- *Ent* : « partie entière ». Est parfois notée $[x]$ (cf. page 19).
- *i.e.* : « id est », c'est-à-dire mais en latin.
- $\circ$: « rond », la composition de fonctions.
- $\mathbb{R}^-$ et $\mathbb{R}^+$: $]-\infty\,;0]$ et $[0\,;+\infty[$, les réels positifs / négatifs ou nuls.
- $\mathbb{R}^* =]-\infty\,;0[\,\cup\,]0\,;+\infty[$: les réels non nuls.
- *ssi* et $\iff$: « si, et seulement si » et « équivaut ». À la fois $\Longleftarrow$ et $\Longrightarrow$ (cf. page 364).
- $[\![1\,;n]\!]$: l'ensemble des entiers compris entre 1 et n c.-à-d. $\mathbb{N} \cap [1\,;n]$.

Voici ensuite des notations et abréviations moins classiques mais bien pratiques.

- $\nearrow$, $\searrow$: croissante, décroissante, à propos d'une fonction.
- $\nearrow\nearrow$ ou $\nearrow^{\text{nt}}$, $\searrow\searrow$ ou $\searrow^{\text{nt}}$: strictement (dé)croissante, pour une fonction.
- $\lightning$: « contradiction ». Étape finale d'une démonstration par l'absurde. (cf. page 369).
- à.p.c.r. : « à partir d'un certain rang ». Se dit d'une suite dont les tous termes vérifient une certaine propriété, sauf un nombre fini d'entre eux.
- coeff. dir. : « coefficient directeur » d'une droite ou d'une fonction affine.
- colin. : « colinéaires ». Se dit de deux vecteurs.
- CV et DV : « converge(nte) » et « diverge(nte) ».
  Se dit d'une suite ayant / n'ayant pas une limite finie.
- $\mathbb{E}$: « espérance » d'une variable aléatoire.
- $\mathfrak{P}$: ensemble des nombres premiers (cf. page 219).
- $\mathbb{P}$: « probabilité » d'un événement.
- p.o.c. : « par ordre croissant ».
- r.o.n. : « repère orthonormé ».
- th. : « théorème ».
- tq. : « tel que ».
- VouF : « Vrai ou faux ». Type d'exercice très prisé des élèves.

Bibliographie & Références

Commençons par des manuels de terminale experte. Les suivants sont ceux que je parcours régulièrement :

[BZ] *T^{le} Exp., coll. Barbazo*, É. Barbazo (dir.), éd. Hachette, 2020.

[LS1] *Le Livre scolaire T^{le} Exp.*, manuel collaboratif, éd. Livre scolaire, 2020.

Puis, quelques ouvrages pour réviser ou aller un peu plus loin :

[CR] M. Colonval et A. Roumadni, *Les Mathématiques au quotidien*, éd. Ellipses, 2010.

[Th] François Thirioux, *Mathématiques $T^{le}S$ pour réussir en prépa*, éd. Ellipses, 2015.

[LS1] *Le Livre scolaire 1^{re} Spé*, manuel collaboratif, éd. Livre scolaire, 2019.

[LST] *Le Livre scolaire T^{le} Spé*, manuel collaboratif, éd. Livre scolaire, 2020.

[K2] Sébastien Krief-Détraz, *Math Max 2^{de}*, éd. Ellipses, 2020.

[K1] Sébastien Krief-Détraz, *Math Max 1^{re} Spé.*, éd. Ellipses, 2020.

[KS] Sébastien Krief-Détraz, *Math Max T^{le} Spé.*, éd. Ellipses, 2022.

Poursuivons par des références sur la toile, très utiles lorsqu'utilisées à bon escient :

[WK] *Wikipedia* : toujours utile, même si très vite technique.

[KA] *Khan Academy* : https ://fr.khanacademy.org. Tous les cours, en vidéo.

[MN] *Les Mathématiques.net* : http ://www.les-mathematiques.net. Pour le supérieur plutôt mais cela permet déjà de voir plus loin. Le forum est réactif.

[IM] *Images des mathématiques* : http ://images.math.cnrs.fr. Des actualités, des articles, des énigmes, des images... de mathématiques.

[AP] *APMEP : Association des Professeurs de Mathématiques de l'Enseignement Public* : http ://www.apmep.fr. Vous pouvez y trouver toutes les annales corrigées du baccalauréat depuis le siècle dernier mais aussi des jeux mathématiques.

[JC] *J'ai compris* : jaicompris.com. Des vidéos pour tout comprendre... aux mathématiques.

[MP] *Math en poche* : http ://mathenpoche.sesamath.net. Pour réviser en ligne (plutôt les « petites » classes toutefois).

Ensuite, des ouvrages et références autour des mathématiques et des sciences dont je conseille fortement la lecture. Ils sont parfois cités dans cet ouvrage, à vous de retrouver en quel endroit (les solutions suivent).

[AG] Alexandre Grothendieck, *Récoltes et Semailles*, éd. Gallimard, 2022.

[AH] Alain Badiou avec Gilles Haéri, *Éloge des mathématiques*, éd. Flammarion, 2015.

[AS] Arthur Schopenhauer, *L'Art d'avoir toujours raison*, écrit vers 1830.

[BK] Yoram Bauman et Grady Klein, *Les Mathématiques en bande dessinée - L'Analyse*, éd. Eyrolles, 2019.

[CV] Cédric Villani, *Théorème vivant*, éd. Grasset, 2012.

[Dé] François-Henri Désérable, *Évariste*, éd. Gallimard, 2015.

[DG] Denis Guedj, *Le Théorème du perroquet*, éd. du Seuil, 1998.

[EA] Edwin Abbot Abbot, *Flatland*, 1884.

[EK] Étienne Klein, *Science en question*, émission radiodiffusée sur France Culture.

[Eu] Euclide, *Éléments*, $\sim$ 300 av. J.-C.

[GM] *Le Goût des Mathématiques*, ouvrage collectif, éd. Mercure de France, 2013.

[HL] Hervé Le Tellier, *L'Anomalie*, éd. Gallimard, 1920.

[JD] Jacqueline Détraz, *Sofia Kovalesvskaïa, l'aventure d'une mathématicienne*, éd. Belin, 1993.

[MS] *La Marche des Sciences*, émission radiodiffusée sur France Culture.

[RH] *Un Homme d'exception*, réal. Ron Howard, prod. Universal, 2001. Film retraçant la vie de John Forbes Nash (1928-2015), remarquable mathématicien (prix Abel 2015, prix Nobel d'économie 1994).

[RQ] Raymond Queneau, *Cent mille milliards de poèmes*, 1961.

[YG] Yannick Grannec, *La Déesse des petites victoires*, éd. Anne Carrière, 2012.

Enfin, voilà les références des allusions qui ont guidé, inspiré ou simplement connoté certains énoncés que l'on pourrait parfois qualifier de décalés. À vous de les retrouver dans le corps du texte (les solutions suivent).

[AD] Alexandre Dumas, *Les Trois Mousquetaires*, éd. Baudry, 1844.

[Be] The Beatles, *Discographie complète*, label Parlophone, 1962-1970.

[CK] *Le Péril jeune*, réal. Cédric Klapisch, prod. La Sept-Arte, 1994.

[Da] René Daumal, *Le Mont analogue*, éd. Gallimard, 1952.

[DF] *Fight Club*, réal. David Fincher, prod. Fox 2000 Pictures, 1999.

[GE] Gustave Eiffel, *La Tour*, Paris, 1889.

[GS] R. Goscinny et J.-J. Sempé, *Le Petit Nicolas*, journal Pilote, 1956-1965.

[GT] *Game of Thrones*, série nord-américaine (HBO) inspirée de l'œuvre de George R. R. Martin, 2011-2018.

[GU] R. Goscinny et A. Uderzo, *Astérix : La Serpe d'or* et tous les autres albums, éd. Dargaud, 1959-1977.

[HM] Henri Matisse, Rideau pour l'*Étrange farandole*, 1938.

[HS] Henri Salvador, *Syracuse*, label Phillips, 1963.

[Ic] Icare, mythologie grecque.

[JF] Jean Ferrat, *La Montagne*, label Barclay, 1964.

[JI] *Jeux interdits*, musique du film de René Clément, arrangée par Narciso Yepes, label Musicales Transatlantiques, 1952.

[JJ] Joseph Joffo, *Un sac de billes*, éd. J.-C. Lattès, 1973.

[JR] Jacques Roubaud, *La Trilogie d'Hortense*, éd. Ramsay, 1985-1990.

[JS] John Steinbeck, *Des souris et des hommes*, éd. Gallimard, 1937.

[MM] *Mad Max*, réal. George Miller, prod. Kennedy Miller, 1979-2015.

[MX] *Matrix*, réal. L. et L. Wachowski, prod. Warner Bros., 1999.

[NH] *Sublimes paroles et idioties de Nasr Eddin Hodja*, éd. Phébus, 2002.

[Ra] RATM, *Rage against the machine*, label EPIC, 1992.

[RK] Rudyard Kipling, *Tu seras un homme, mon fils*, 1910.

[SW] *Star Wars*, réal. George Lucas, prod. Lucasfilm, 1977-2019.

[VH] Victor Hugo, *Notre-Dame de Paris*, éd. C. Gosselin, 1831.

[VM] *Vertical Magazine*, revue trimestrielle, éd. Nivéales.

Crédits images : Mark Howison (page 110).

Solutions

Remerciements

Contrairement à ce que l'on pourrait parfois penser à la lecture de cet ouvrage, je suis bien un professeur de mathématiques. Je n'ai donc aucun scrupule à effectuer des remerciements sous forme de liste et dans un ordre quasi aléatoire. L'important est qu'ils soient sincères, non ?

Ainsi,

· à mes élèves, pour leurs questions, pertinentes ou non, leur insistance pour avoir des devoirs ou non, leur souhait d'avoir des corrections d'exercices tapées (comme si leur professeur avait une écriture illisible), leur curiosité et leur soif d'apprendre et de découvrir et pour le sourire dans leurs yeux lorsqu'ils ont compris ce que l'on étudie,
· à ma compagne qui m'a encouragé, m'a supporté et a prodigué de précieux conseils,
· à mes filles, qui ne me voient généralement que derrière un écran et qui, dès le plus jeune âge, ont appris à envoyer un courriel afin de communiquer avec moi,
· à ma mère, ma première lectrice, au sens mathématique littéral,
· à mes collègues, de mathématiques ou d'autres disciplines, qui m'ont donné de nombreuses idées, à leur insu parfois,
· au corps d'inspection pour les remarques judicieuses,
· à mes stagiaires qui me poussent à une réflexion approfondie sur mes pratiques,
· aux nombreux auteurs d'ouvrages et contributeurs de sites personnels ou académiques comme les IREM, qui m'ont inspiré et dont je n'ai plus la référence, qu'ils veuillent bien me pardonner,
· à Donald Knuth (1938-), à l'origine du LaTeX, sans qui rien de ceci n'aurait pu être écrit (sous TeXShop),
· aux éditions Ellipses, et en particulier Corinne Baud qui a immédiatement accepté et soutenu ce projet,
· et finalement, à mes lecteurs, qui voudront bien excuser les coquilles et erreurs subsistantes et qui pourront envoyer leurs remarques aux éditions Ellipses ou même m'écrire : mathmax@yahoo.com,

je dis merci !

Table des matières

MATH MAX

MATHS EXPERTES

NOUVEAUX PROGRAMMES

MATH MAX, parce que les mathématiques sont très sérieuses… mais pas uniquement.

Cette seconde édition, conforme aux nouveaux programmes, contient :

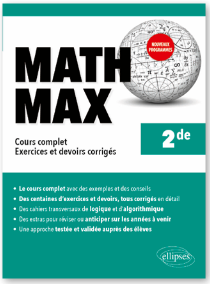
- un cours complet avec des exemples, des remarques et des conseils,
- des centaines d'exercices et devoirs, tous corrigés en détail, de difficulté croissante, couvrant tout le programme et même plus,
- des cahiers transversaux de logique et d'algorithmique,
- des activités d'approche, de révision et de synthèse,
- des extras pour anticiper sur les années à venir,
- des exercices en anglais pour enrichir la langue,
- des corrections rédigées comme l'exigent les enseignants,
- une approche testée et validée auprès des élèves.

Tout ce qui est nécessaire pour asseoir ses bases, réussir son année et bien préparer la suivante.

Mais **MATH MAX**, c'est aussi des données historiques, des conseils de lectures, des touches culturelles, des exercices décalés, des énoncés fantasques, des contextes farfelus, des jeux de mots (presque) amusants.

Voici bien de quoi égayer votre réflexion.

Et aussi dans la même série



www.editions-ellipses.fr

9 782340 074651