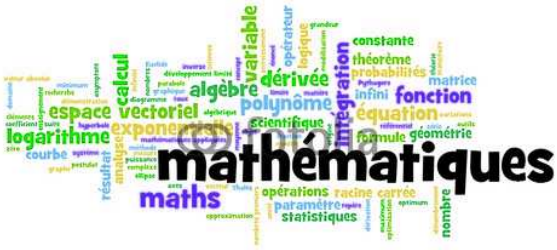
Fomesoutra.com
ça soutra!

Wallis et Futuna

Cours de
MATHÉMATIQUES

— Fabien PUCCI —

Classe de Terminale S



Enseignement de SpÃ©cialitÃ©

Année 2015

Table des matières

Chapitre

1

Division euclidienne

L'arithmétique concerne l'étude des entiers naturels $\mathbb{N}$ ou relatifs $\mathbb{Z}$.

Avant-propos

ATTENTION

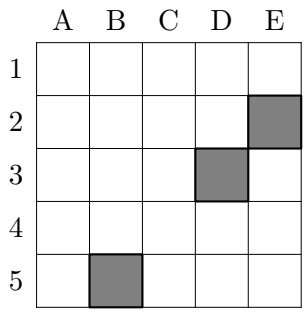
- Il est important de remarquer si la résolution se fait dans $\mathbb{N}$ ou dans $\mathbb{Z}$.
- Le mode de résolution dans les ensembles $\mathbb{N}$ ou $\mathbb{Z}$ est différent de celui dans l'ensemble des réels $\mathbb{R}$.

Théorème 1 (Admis)

- Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
- Toute suite dans $\mathbb{N}$ strictement décroissante est stationnaire au bout d'un certain rang.

Sommaire

Remplir la grille de nombres croisés ci-dessous sachant que tous les nombres y figurant sont des entiers naturels non nuls.



Horizontalement

1/ Carré parfait dont le produit des chiffres est 756.

2/ Le nombre formé de ses deux premiers chiffres est le même que celui formé de ses deux derniers chiffres.

3/ Multiple de 139.
Reste de la division euclidienne de 2001 par 9.

4/ Permutation de 23444.

5/ Carré parfait.
Le produit de ses chiffres est 392.

Verticalement

A/ La somme de ses chiffres est 35.

B/ Entier divisible par 11.

C/ Nombre palindrome (qui se lit aussi bien à l'endroit qu'à l'envers).

D/ Nombre premier. Cube parfait.

E/ Entier naturel admettant un seul diviseur positif. Le produit de ses chiffres est 72 et seul son dernier chiffe est pair.

I Divisibilité dans $\mathbb{Z}$

Rappels 1

On note $\mathbb{N} = \{0;\ 1;\ 2;\ 3;\ \ldots\}$ l'ensemble des entiers naturels et $\mathbb{Z} = \{\ldots;\ -3;\ -3;\ -1;\ 0;\ 1;\ 2;\ 3;\ \ldots\}$ l'ensemble des entiers relatifs.

Définition 1

Soient a et b deux entiers ($a \neq 0$). On dit que a **divise** b et on note $a|b$ si, et seulement s'il existe un entier k tel que $b = ka$. On dit aussi que a est un **diviseur** de b. On dit encore que b est un **multiple** de a.

Exemple 1: 7 divise 56 car $56 = 7 \times 8$ avec 8 entier. 7 est un diviseur de 56 et 56 est un multiple de 7. On peut écrire $7|56$.

Remarques:

1/ 0 est multiple de tout entier.

2/ Tout entier non nul n a (au moins) pour diviseurs dans $\mathbb{Z}$ 1, n, -1 et $-n$.

3/ 1 a seulement deux diviseurs dans $\mathbb{Z}$, -1 et lui-même (donc 1 a pour seul diviseur 1 dans $\mathbb{N}$).

Comme a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$, on se restreint à l'étude de la divisibilité dans $\mathbb{N}$.

Proposition 1

1/ Tout diviseur positif d'un naturel non nul n vérifie : $1 \leqslant d \leqslant n$.

2/ Tout naturel non nul a un nombre fini de diviseurs.

Preuve:

1/ Soit n un naturel non nul. L'entier d divise n s'il existe un entier k tel que $n = kd$. Si $d > 0$, alors $k > 0$ (car n est positif) et ainsi $k \geqslant 1$.
Par conséquent : $kd \geqslant d \Leftrightarrow n \geqslant d$ et $1 \leqslant d \leqslant n$.

2/ Il est clair qu'un entier n a au plus n diviseurs dans $\mathbb{N}$ donc au plus $2n$ dans $\mathbb{Z}$. Un entier n admet donc un nombre fini de diviseurs.

Remarque: 0 a une infinité de diviseurs.

Pour simplifier les écritures, on notera souvent $\mathscr{D}(n)$, l'ensemble des diviseurs de n dans $\mathbb{N}$.

Exemple 2:

- Les diviseurs de 24 dans $\mathbb{N}$ sont : $\mathscr{D}(24) = 1; 2; 3; 4; 6; 12; 24$.
- Les diviseurs de 24 dans $\mathbb{Z}$ sont : $-24; -12; 6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12; 24$.

Définition 2

Un nombre premier est un nombre entier strictement plus grand que 1 dont les seuls diviseurs sont 1 et lui-même dans $\mathbb{N}$.

Exemple 3: 2, 3, 5, 7, 11, 13, ...sont des nombres premiers.

Remarque: Si n est un nombre premiers alors $\mathscr{D}(n) = \{1, n\}$.

Définition 3

Deux entiers relatifs sont premiers entre eux si, et seulement, leurs seuls diviseurs communs sont -1 et 1.
Si a et b sont deux entiers premiers entre eux, on note $a \wedge b = 1$.

Si a est un nombre premier alors tout nombre entier b différent de a est premier avec a.

Exemple 4:

$$\left.\begin{array}{l}\mathscr{D}(15) = \{-15;\ -5;\ -3;\ -1;\ 1;\ 3;\ 5;\ 15\} \\ \mathscr{D}(14) = \{-14;\ -7;\ -2;\ -1;\ 1;\ 2;\ 7;\ 14\}\end{array}\right\} \quad \Longrightarrow \quad 14 \wedge 15 = 1.$$

Proposition 2

1/ 1 divise a pour tout entier relatif a.

2/ a divise a pour tout entier relatif a.

3/ Si a divise b et si b divise c, alors, a divise c : on dit que la relation de divisibilité est **transitive**.

Énoncé équivalent : Si b est un multiple de a et si c est un multiple de b, alors c est un multiple de a.

4/ Si a divise b et si m est un entier, alors a divise mb.

5/ Si a divise b et si a divise c, alors a divise $b + c$ et plus généralement, a divise $mb + nc$ où m et n sont des entiers quelconques. [1]

1. $mb + nc$ est une combinaison linéaire de b et c.

Preuve:

1/ $a = a \times 1$, donc 1 divise a.

2/ $a = a \times 1$, donc a divise a.

3/ Si a divise b, alors il existe k entier tel que $b = ka$.
Si b divise c, alors il existe k' entier tel que $c = k'b$.
Alors $c = k'b = k'(ka) = (k'k)a$ où $k'k \in \mathbb{Z}$, donc a divise c.

4/ Démonstration analogue.

Exemple 5: Si $a \in \mathbb{Z}$ divise $3n+2$ et $n-3$ alors $a|11$. En effet, a divise alors $(3n+2) - 3(n-3) = 11$.

1 **Exercice** Déterminer les entiers n tels que 7 divise $n+3$.

Correction: 7 divise $n+3$ si, et seulement si, il existe un entier k tel que $n+3 = 7k$, soit $n = 7k+3$.
L'ensemble des solutions est : $\mathscr{S} = \{7k-3,\ k \in \mathbb{Z}\}$

2 **Exercice** Déterminer les entiers n tels que $2n-5$ divise 6.

Correction: Les diviseurs de 6 sont -6, -3, -2, -1, 1, 2, 3 et 6.

On résout les différentes équations sous la condition $2n-5 \leqslant 6$ et on trouve comme solutions : $\mathscr{S} = \{1\ ;\ 2\ ;\ 3\ ;\ 4\}$.

3 **Exercice** Trouver les entiers n pour lesquels $\dfrac{n+15}{n+2}$ est entier.

Correction: On simplifie d'abord un peu et on isole la variable n :

$n+15 = n+2+13$ donc $\dfrac{n+15}{n+2} = \dfrac{(n+2)+13}{n+2} = 1 + \dfrac{13}{n+2}$.

Le problème s'énonce alors de façon plus simple :

$$\frac{n+15}{n+2} \in \mathbb{Z} \iff \frac{13}{n+2} \in \mathbb{Z},$$

c'est-à-dire si, et seulement si $n+2$ est un diviseur de 13.

Les diviseurs de 13 sont -13, -1, 1 et 13. Il y a donc 4 équations à résoudre ($n+2 = -13$, $n+2 = \ldots$).

On obtient : $\mathscr{S} = \{-15;\ -3;\ -1;\ 11\}$.

D'une manière générale,

Méthode 1

Pour résoudre un problème du type $f(n)|g(n)$, on se ramène à un problème du type $h(n)|A$ où A est un entier **indépendant** de n.[2]

4 **Exercice** Déterminer les entiers n tels que $2n-3$ divise $n+5$.

Correction: Si n un entier tel que $2n-3$ divise $n+5$ alors $2n-3$ divise aussi $2n+10$ et aussi la différence $(2n+10)-(2n-3)=13$.

Les diviseurs de 13 sont -13, -1, 1 et 13. On en déduit que n vaut -5, 1, 2 ou 8.

Réciproquement, ces nombres sont tels que $2n-3|n+5$.

On obtient : $\mathscr{S}=\{-5,\,1,\,2\,8\}$.

5 **Exercice (Équations diophantiennes[3])** Déterminer les entiers x et y tels que $x^2-y^2=9$.

Méthode 2

Pour les problèmes donnés sous forme additive, on essaiera de se ramener à une forme multiplicative du type $A\times B=C$, où on connaît les diviseurs de C.

Correction: Simplifions d'abord le champ de recherche en remarquant que si $(x;\ y)$ est solution, alors $(x;\ -y)$, $(-x;\ y)$ et $(-x;\ -y)$ sont aussi solutions. On peut alors se restreindre à x et y naturels (positifs).

Il est naturel de factoriser : $x^2-y^2=(x-y)(x+y)$.

Ainsi, $x-y$ et $x+y$ sont nécessairement des diviseurs de 9.

Or, l'ensemble des diviseurs de 9 sont -9, -3, -1, 1, 3, 9.

On réduit encore le champ d'investigation en remarquant que comme x^2-y^2 est positif, avec x et y positifs alors nécessairement $x>y$. On en déduit alors que $x-y$ et $x+y$ sont positifs, et $x-y\leqslant x+y$.

Il ne reste plus qu'à étudier les différentes possibilités :

- Si $x-y=1$ alors $x+y=9$, d'où $x=5$ et $y=4$.
- Si $x-y=3$ alors $x=y=3$ d'où $x=3$ et $y=0$.

Finalement, il ne reste que six couples solutions possibles : $(5;4)$, $(5;-4)$, $(-5;4)$, $(-5;-4)$, $(3;0)$ et $(-3;0)$.

Comme on a raisonné par condition nécessaire, on vérifie que ces couples sont solutions du problème.

Conclusion : $\mathscr{S}=\big\{(5;4);\,(5;-4),\,(-5;4),\,(-5;-4),\,(3;0),\,(-3;0)\big\}$.

2. En d'autres termes, on isole la variable.
3. Diophante : mathématicien, III^{e} siècle après J.C.)

Corollaire 1

Les nombres impairs sont exactement les entiers de la forme $2p+1$ où $p \in \mathbb{Z}$.

Preuve: Il y a deux choses à prouver.

1/ Tout nombre de la forme $2p+1$ où $p \in \mathbb{Z}$ est impair.

En effet, $2|2p$ mais 2 ne divise pas 1, donc $2p+1$ n'est pas divisible par 2, donc est impair.

2/ Tout nombre impair s'écrit sous la forme $2p+1$ où $p \in \mathbb{Z}$.

Par l'absurde, supposons qu'il existe un nombre impair positif m tel que $m-1$ n'est pas pair. On note encore m le plus petit entier vérifiant cette propriété et on va prouver qu'en fait $m?1$ vérifie aussi cette propriété.

Comme $2|(-2)$ alors $2|m \iff 2|(m-2)$.

Or 2 ne divise pas m c'est-à-dire que m est impair de même que $m-2$ qui est impair.

Mais, par définition de m, $m-1$ est nombre impair à qui, si on retranche 1, donne un nombre impair $m-2$.

Ceci contredit que m est le plus petit impair vérifiant cette propriété.

Ainsi tout nombre impair positif q est tel que $q-1$ soit pair (i.e) $q-1=2p$, c'est-à-dire $q=2p+1$.

De même avec les négatifs.

6 **Exercice** Prouver que la somme de 3 entiers consécutifs est divisible par 3.

II Division euclidienne

On étudie de façon approfondie la division des nombres entiers vue dans les petites classes.

Théorème 11 (Division euclidienne dans $\mathbb{N}$)

Soit a un entier et soit b un entier naturel non nul. Il existe un **unique** entier q et un unique entier r tels que

$$a = bq + r \quad \text{et } 0 \leqslant r < b. \tag{1.1}$$

On dit qu'on a effectué la division euclidienne de a par b.
q s'appelle le quotient et r le reste.

Preuve: On admet d'abord la propriété suivante : toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Il y a deux parties à démontrer dans ce théorème : **l'existence** du couple $(q;\ r)$, puis son **unicité**.

Existence de q et r :

1/ Premier cas : Si $0 \leqslant a < b$ alors le couple $(q;\ r) = (0;\ a)$ convient.

2/ Second cas : Si $a = b$ alors le couple $(1;\ a)$ convient.

3/ Troisième cas : Supposons que $a > b$. En particulier, a et b sont donc tous deux strictement positifs.

On note $\mathscr{M}(b)$ l'ensemble des multiples de b inférieurs ou égaux à a :

$$\mathscr{M}(b) = \{kb,\ \forall\, k \in \mathbb{Z},\ kb \leqslant a\}.$$

$b \in \mathscr{M}(b)$ donc $\mathscr{M}(b)$ est non vide et majorée par a.
D'après la propriété admise, $\mathscr{M}(b)$ admet donc un plus petit grand élément que l'on note q.

Par définition de q, on a donc $qb \leqslant a < (q+1)b$ [4].

Posons alors $r = a - bq$. r est un entier puisque a, b et q le sont et on a :

$$qb \leqslant a \Rightarrow r \geqslant 0.$$

Donc $r \in \mathbb{N}$.
Comme $a < (q+1)b$ alors $a - bq < b$, c'est-à-dire $r < b$.

On a donc bien $0 \leqslant r < b$.

Conclusion, dans tous les cas, il existe un couple $(q;\ r)$ vérifiant la relation (1.1).

Unicité de q et r Cette partie va donner toute son importance à l'inégalité stricte $r < b$ de la relation (1.1).

Supposons qu'il existe deux couples $(q;\ r)$ et $(q';\ r')$ tels que $a = bq + r$ et $a = bq' + r'$, avec $0 \leqslant r < b$ et $0 \leqslant r' < b$.

- Comme $a = bq + r = bq' + r'$ alors $b(q - q') = r - r'$ avec $q - q'$ entier : $r - r'$ est multiple de b.
- Comme $0 \leqslant r < b$ alors $-b < -r \leqslant 0$ et, en additionnant avec la relation $0 \leqslant r' < b$, on obtient :
$$-b < r' - r < b.$$
Or $r' - r$ est aussi multiple de b. Le seul multiple de b compris strictement entre $-b$ et b est 0.
Par conséquent : $r' - r = 0$ et $r = r'$.
En reportant dans $a = bq + r = bq' + r'$, on obtient alors $bq + r = bq' + r$ puis $bq = bq'$, d'où $q = q'$ car $b \neq 0$.

Conclusion, le couple $(q;\ r)$ est unique.

Exemple 6: $123 = 37 \times 3 + 12$; 12 est le reste de la division euclidienne de 123 par 37.

7 **Exercice** Calculer $\sin\left(2015 \times \dfrac{\pi}{3}\right)$.

Proposition 3 (Division euclidienne dans $\mathbb{Z}$)

1/ b divise a si, et seulement si, le reste de la division de a par b est nul.

2/ On peut étendre le théorème au cas où a est entier (relatif) et b entier non nul : $a = bq + r$, avec $0 \leqslant r < |b|$.

4. Par définition de q!

Exemple 7: $-35 = 4 \times (-9) + 1$.

8 **Exercice** Montrer que tout entier n non divisible par 5 a un carré de la forme $5p+1$ ou $5p-1$ (raisonner par disjonction des cas).

9 **Exercice** Soit $n \in \mathbb{N}$. Quel est le reste de la division euclidienne de $(n+2)^2$ par $n+3$?

Même question avec $(n+5)^2$ et $n+3$.

Diviseurs

1 **Exercice** Dresser la listes des diviseurs de 150 et 230.

2 **Exercice** Déterminer les couples $(x,\ y)$ d'entiers naturels qui vérifient $x^2 = y^2 + 21$.

3 **Exercice** Déterminer les entiers relatifs n qui vérifient :

1/ $n^2 + n = 20$. **2/** $n^2 + 2n = 35$.

4 **Exercice** Déterminer les entiers relatifs n tel que :

1/ $n + 1$ divise $3n - 4$ **2/** $n + 3 | n + 10$.

5 **Exercice** Soit n un entier naturel.

1/ Montrer que 2 divise $n(n + 1)$.

2/ Montrer que 3 divise $n(n + 1)(n + 2)$.

6 **Exercice** Montrer que pour tout entier relatif a, 6 divise $a(a^2 - 1)$.

On pourra se servir de l'exercice précédent.

7 **Exercice** Soit l'équation (E) dans $\mathbb{N}$: $xy - 5x - 5y - 7 = 0$.

1/ Montrer que : $xy - 5x - 5y - 7 = 0 \iff (x - 5)(y - 5) = 32$.

2/ Résoudre alors l'équation (E).

8 **Exercice** Soit n un entier naturel. Démontrer que quel que soit n, $3n^4 + 5n + 1$ est impair et en déduire que ce nombre n'est jamais divisible par $n(n + 1)$.

Division euclidienne

1 **Exercice** Écrire la division euclidienne de -5000 par 17.

2 **Exercice** La différence entre deux naturels est 538. Si l'on divise l'un par l'autre le quotient est 13 et le reste 34. Quels sont ces deux entiers naturels ?

3 **Exercice** Trouver les entiers naturels n qui, divisés par 4, donnent un quotient égal au reste.

4 **Exercice** Trouver un naturel qui, divisé par 23, donne pour reste 1 et, divisé par 17, donne le même quotient et pour reste 13.

5 **Exercice** Le quotient d'un entier relatif x par 3 est 7. Quels sont les restes possibles ?

En déduire quelles sont les valeurs de x possibles.

6 **Exercice** Si l'on divise un entier a par 18, le reste est 13. Quel est le reste de la division de a par 6 ?

7 **Exercice** Si l'on divise un entier a par 6, le reste est 4. Quels sont les restes possibles de la division de a par 18 ?

8 **Exercice** La division euclidienne de a par b donne $a = 625b + 8634$. De quels naturels peut-on augmenter à la fois a et b sans changer de quotient ?

Chapitre

2 Congruences dans $\mathbb{Z}$

Sommaire

I Congruences

Définition 1

Soit n un entier naturel non nul.
On dit que a et b sont congrus modulo n si, et seulement si, a et b ont même reste dans la division euclidienne par n.
On dit aussi que a est égal à b modulo n.

Notation : $a \equiv b(n)$ ou $a \equiv b$ (modulo n) ou $a \equiv b\ [n]$.

Une conséquence importante de cette définition est que :

$a \equiv r\ [n]$ avec $0 \leqslant r < n$ si, et seulement si r est le reste de la division euclidienne de a par n.

Exemple 1:

- $25 = 11 \times 1 + \mathbf{14}$ donc $25 \equiv 14\ [11]$.
- On a aussi $25 = 11 \times 2 + \mathbf{3}$ donc $25 \equiv 3\ [11]$.
- $10 \equiv 1$ [9]car $10 = 9 \times 1 + \mathbf{1}$ et $1 = 9 \times 0 + \mathbf{1}$.

Théorème 1

Soient a et b deux entiers relatifs et n un entier naturel. a et b ont même reste dans la division euclidienne par n si, et seulement si $a - b$ est divisible par n.

Preuve:

Condition nécessaire : Supposons que a et b aient même reste dans la division par n, c'est-à-dire qu'il existe q et q' tels que : $a = nq + r$ et $b = nq' = r$ avec q et q' entiers et $0 \leqslant r < n$.

En soustrayant les deux égalités, on obtient $a-b=n(q-q')$ avec $q-q'$ entier, donc $a-b$ est divisible par n.

Condition suffisante : Supposons que $a-b$ soit divisible par n. Alors, $\exists k \in \mathbb{Z}$ tel que $a-b=kn$.

Soit r le reste de la division euclidienne de b par n. On a : $b=nq+r$, avec q entier et $0 \leqslant r < n$.

D'où $a=b+kn=nq+r+kn=(k+q)n+r$ avec $0 \leqslant r < n$. Le reste de la division de a par n est donc aussi r et le résultat.

Ce théorème nous permet alors d'obtenir une caractérisation de la congruence par le corollaire ci-dessous :

Corollaire 1

a et b sont congrus modulo n si, et seulement si $a-b$ est divisible par n.

$$a \equiv b\ [n] \qquad \Longleftrightarrow \qquad n|a-b.$$

A l'aide de ce dernier, on obtient alors aisément toutes les propriétés ci-dessous :

Proposition 1

1/ a est divisible par $n \Leftrightarrow a \equiv 0\ [n]$.

2/ $n \equiv 0\ [n]$

3/ $a \equiv a\ [n]$ (la relation de congruence est réflexive)

4/ Si $a \equiv b\ [n]$ et si $b \equiv c\ [n]$, alors $a \equiv c\ [n]$ (la relation de congruence est transitive).

5/ Si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$ (la relation de congruence est symétrique)

6/ Si $a \equiv a'\ [n]$ et si $b \equiv b'\ [n]$, alors $a+b \equiv a'+b'\ [n]$. (la relation de congruence est compatible avec l'addition).

7/ Si $a \equiv a'\ [n]$ et si $b \equiv b'\ [n]$, alors $a \times b \equiv a' \times b'\ [n]$. (la relation de congruence est compatible avec la multiplication).

8/ Si $a \equiv b\ [n]$ et si p appartient à $\mathbb{N}$, alors $a^p \equiv b^p\ [n]$.

Pour plus tard mais il n'est jamais trop tôt pour apprendre, le fait que la relation de congruence soit réflexive, symétrique et transitive fait de celle-ci une relation d'équivalence. De plus, la compatibilité avec les deux lois de $\mathbb{Z}$ permet de donner à l'ensemble des classes de $\mathbb{Z}$ une structure d'anneau. Vous verrez ça plus tard. Patience !

Preuve:

1/ Évident d'après le corollaire précédent.

2/ n a pour reste 0 dans la division par n, donc $n \equiv 0\ [n]$.

3/ $n|(a-a)$ donc $a \equiv a\ \ [n]$

4/ Si a et b ont même reste dans la division euclidienne par n et si b et c aussi, alors a et c aussi.

5/ Si $a \equiv b\ [n]$, alors $n|a-b$; on déduit que $n|b-a$ (dans $\mathbb{Z}$) et donc $b \equiv a\ [n]$

6/ Si $a-b=qn$ et $a'-b'=q'n$, alors $a+a'-(b+b')=(q+q')n$ donc $a+a'-(b+b')$ est divisible par n, d'où le résultat.

7/ On a les mêmes hypothèses, donc $a-b=qn$ et $a'-b'=q'n$ et on peut écrire :

$$\begin{aligned} ab-a'b' &= ab-ab'+ab'-a'b' = a(b-b')+b'(a-a') \\ &= aq'n+b'qn = n(aq'+b'q). \end{aligned}$$

Il est clair que $aq'+b'q \in \mathbb{Z}$ (somme et produit d'entiers). Par conséquent : $n|(ab-a'b')$ donc $ab \equiv a'b'\ \ [n]$.

8/ Se montre par récurrence sur p. [1]

Exemple 2 (Une application au CE2 : la preuve par 9): Comment vérifier que l'on ne s'est pas trompé en effectuant une addition, une différence, une multiplication ou une division ?

Réponse : Il suffit de refaire les calculs modulo 9 par exemple et de vérifier que les calculs correspondent.

Comme $10 \equiv 1\ [9]$, grâce à la proposition précédente, on en déduit que $\forall\, p \in \mathbb{N}$, $10^p \equiv 1\ [9]$.

Considérons un entier $m = \overline{a_n a_{n-1} \dots a_1 a_0} = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0 \times 1$. Modulo 9, on obtient :

$$\begin{aligned} m &\equiv a_n \times 1 + a_{n-1} \times 1 + \dots + a_1 \times 1 + a_0 \times 1\ [9]\ [9] \\ &\equiv a_n + a_{n-1} + \dots + a_1 + a_0 \end{aligned} \iff m \text{ est égal à la somme de ses chiffres modulo } n.$$

Vérifions les opérations suivantes :

Une addition :

$$\begin{array}{cccccc} & 7 & 5 & 8 & 0 & 6 \\ + & & & 4 & 5 & 7 \\ + & 3 & 5 & 2 & 3 & 5 \\ \hline 1 & 1 & 1 & 4 & 9 & 8 \end{array}$$

Comme $\left\{ \begin{array}{rcl} 75806 & \equiv & 8\ [9] \\ 457 & \equiv & 7\ [9] \\ 35235 & \equiv & 0\ [9] \end{array} \right.$, l'addition modulo 9 devient :

$$\begin{array}{rcl} & & 8 \\ + & & 7 \\ + & & 0 \\ \hline \equiv & & 6 \end{array}$$

Il ne reste plus qu'à vérifier que 111498 est bien égal à 6 modulo 9... C'est bien le cas !

Une multiplication :

$$\begin{array}{cccccc} & & 6 & 8 & 2 & 5 \\ \times & & & & 4 & 7 \\ \hline 3 & 2 & 0 & 7 & 7 & 5 \end{array}$$

De la même manière, $\left\{ \begin{array}{rcl} 6825 & \equiv & 3\ [9] \\ 47 & \equiv & 2\ [9] \end{array} \right.$ donne, modulo 9,

$$\begin{array}{rcl} & & 3 \\ \times & & 2 \\ \hline \equiv & & 6 \end{array}$$

Comme $320775 \equiv 6\ [9]$, on peut espérer ne pas s'être trompé... modulo 9 !

1. Un bon exercice !

Exercice Quel est le reste de 50^{100} par la division par 7 ? celui de 100^{100} ? de $50^{100} + 100^{100}$?

2 **Exercice** Déterminer l'ensemble des entiers x tels que : $x + 4 \equiv 2\ [8]$

Correction: $x + 4 \equiv 2\ [8] \Leftrightarrow x \equiv -2\ [8] \Leftrightarrow x \equiv 6\ [8]$ car -2 est congru à 6 modulo 8.

3 **Exercice** Déterminer l'ensemble des x entiers tels que $5x \equiv 3\ [7]$.

Correction: On remplit un tableau des valeurs prises modulo [7] par $5x$ lorsque x prend les 7 valeurs des restes possibles modulo 7.

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

On en déduit que les solutions sont les nombres x congrus à 2 modulo 7, c'est-à-dire les éléments de l'ensemble $\mathscr{S} = \{2 + 7k,\ k \in \mathbb{Z}\}$

4 **Exercice**

1/ Déterminer le reste de la division par 7 de 2^n.

2/ En déduire le reste de la division euclidienne de 2^{134589} par 7.

Correction:

1/ Par définition, chercher le reste de la division par 7 de 2^n revient à chercher l'ensemble des valeurs prises par 2^n modulo 7 [2].

Pour se donner une idée de la démonstration, on teste sur les premières valeurs de n :

$2^0 = 1\ [7]$; $2^1 = 2\ [7]$; $2^2 = 4\ [7]$; $2^3 = 8 \equiv 1\ [7]$. On remarque que l'on va avoir un cycle modulo 3.

- Si $n \equiv 0\ [3]$, alors $n = 3p$ d'où $2^n = 2^{3p} = (2^3)^p \equiv 1^p\ [7] \equiv 1\ [7]$.
- Si $n \equiv 1\ [7]$, alors $n = 3p + 1$ d'où $2^n = 2^{3p+1} = 2^{3p} \times 2 \equiv 2\ [7]$.
- Si $n \equiv 2\ [7]$, alors $n = 3p + 2$ d'où $2^n = 2^{3p+2} = 2^{3p} \times 4 \equiv 4\ [7]$.

2/ D'après la question précédente, il suffit de calculer le reste de la division de 13459 par 3 pour conclure suivant les cas.

Comme $13459 = 4486 \times 3 + 1$, on a : $13459 \equiv 1\ [3]$.

D'où $2^{13458} \equiv 2\ [7]$. Le reste de la division euclidienne de 2^{134589} par 7 est 2.

5 **Exercice** Montrer que $\forall\, n \in\ N$, $3^{n+3} - 4^{4n+2}$ est divisible par 11.

Correction: On a : $3^{n+3} = 3^n \times 3^3 = 27 \times 3^n$

Or, $27 \equiv 5\ [11]$, donc d'après la compatibilité avec la multiplication, on a :

$$\forall\, n \in \mathbb{N},\ 3^{n+3} \equiv 5 \times 3^n\ [11].$$

De la même manière, on a : $4^{4n+2} = \left(4^4\right)^n \times 4^2$.

2. ou encore de déterminer la classe de 2^n modulo 7.

Or, $4^2 \equiv 5\ [11]$. Donc $4^4 \equiv 5^2 \equiv 3\ [11]$.

Finalement, $\forall\, n \in \mathbb{N}$, $4^{4n+2} \equiv 3^n \times 5\ [11]$.

On en déduit donc :

$$3^{n+3} - 4^{4n+2} \equiv 0\ [11].$$

$\forall\, n \in \mathbb{N}$, $3^{n+3} - 4^{4n+2}$ est divisible par 11.

II Critères de divisibilité

Un critère de divisibilité par n où $n \in \mathbb{N}$ $(n \geqslant 2)$ est un moyen de savoir « rapidement » si un nombre est divisible par n.

Rappels !

n est divisible par k si et seulement si $n \equiv 0\ [k]$.

Un certain nombre de critères de divisibilité ont été vus dans les petites classes, souvent sans justification.

Donnons-les et justifions-les !

Proposition 2 (Divisibilité par 2)

Un nombre est divisible par 2 si, et seulement si, son chiffre des unités est lui-même divisible par 2.

Preuve: Commençons par écrire $n = a_0 + 10a_1 + \ldots + 10^m a_m$, c'est-à-dire que a_0 est le chiffre des unités, a_1 celui des dizaines, ...

Comme $2|10^k$ pour tout $k \geqslant 1$, $n \equiv a_0\ [2]$.

Donc, $n \equiv 0\ [2]$ si et seulement si $a_0 \equiv 0\ [2]$.

Proposition 3 (Divisibilité par 5)

Un nombre est divisible par 5 si, et seulement si, son chiffre des unités est lui-même divisible par 5.

Preuve: Même type de démonstration.

Proposition 4 (Divisibilité par 4)

Un nombre A est divisible par 4 si, et seulement si, le nombre formé par le chiffre des dizaines et celui des unités est lui-même divisible par 4.

Preuve: Comme $4|100$, $4|10^k$ pour tout $k \geqslant 2$. Ainsi $n \equiv a_0 + 10a_1$ [4].

Donc, $n \equiv 0$ [4] si et seulement si le nombre a_1a_0 est divisible par 4.

Proposition 5 (Divisibilité par 3)

Un nombre est divisible par 3 si la somme des chiffres qui le composent est divisible par 3.

Preuve: Supposons $A \geqslant 10$ (sinon, c'est évident !).
$A = \overline{a_n a_{n-1} \cdots a_k \cdots a_1 a_0}$ en écriture décimale ; par conséquent :

$$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_k \times 10^k + \cdots + a_1 \times 10 + a_0 = \sum_{i=0}^{i=n} a_i \times 10^i.$$

Raisonnons modulo 3

Comme $10 \equiv 1$ [3] alors, pour tout n, $10^n \equiv 1^n$ [3] $\equiv 1$ [3].

D'où $A \equiv a_n + a_{n-1} + \cdots + a_0 \equiv \sum_{i=0}^{n} a_i$ [3] et le résultat.

Proposition 6 (Divisibilité par 9)

Un nombre A est divisible par 9 si la somme des chiffres qui le composent est divisible par 9.

Preuve: Même type de démonstration car $10 \equiv 1$ [9].

Proposition 7 (Divisibilité par 11)

Un nombre A est divisible par 11 si la somme alternée de ses chiffres est elle-même divisible par 11.

$A = \overline{a_n a_{n-1} \ldots a_k \ldots a_1 a_0}$ en notation décimale, la somme alternée de ses chiffres est

$$a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^k a_k + \ldots + (-1)^n a_n.$$

Preuve: Pour tout $k \in \mathbb{N}$, $10 \equiv -1$ [11].
On en déduit : $A \equiv a_0 \times (-1)^0 + a_1 \times (-1)^1 + a_k \times \cdots + (-1)^k + a_n \times \cdots + (-1)^n$ [11] $\equiv a_0 - a_1 \cdots$.

Nous avons vu les principaux critères (les plus faciles). Rien n'empêche d'en trouver d'autres.

Exemple 3 (Divisibilité par 7): Regardons les restes successifs dans la division euclidienne par 7 des puissances successives de 10.

10^k	1	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8
Reste de la division de 10^kpar 7	1	3	2	6	4	5	1	3	2

On remarque un cycle (**à justifier**), donc il est facile de déterminer tous les restes de 10^n modulo 7.

Dans l'écriture décimale avec les puissances de 10, on remplace chaque puissance de 10 par son reste modulo 7.

$$\begin{aligned} 689243157 &= 6\times 10^8 + 8\times 10^7 + 9\times 10^6 + 2\times 10^5 + 4\times 10^4 + 3\times 10^3 + 1\times 10^2 + 5\times 10 + 7 \\ &\equiv (6\times 2) + (9\times 3) + (8\times 1) + (2\times 5) + (4\times 4) + (3\times 6) + (1\times 2) + (5\times 3) + 7 \ \ [7] \\ &\equiv 115 \ \ [7] \equiv 3 \ \ [7]. \end{aligned}$$

Ce nombre n'est donc pas divisible par 7.

En remarquant que $6 \equiv -1$ [7], $5 \equiv -2$ [7] et $4 \equiv -3$ [7], on pourrait améliorer ce critère peu utilisé car peu pratique.

6

Exercice **(Autre critère de divisibilité par 7)** Soit n un nombre d'au moins trois chiffres et dont l'écriture décimale est $\overline{a_n a_{n-1}\cdots a_k \cdots a_1 a_0}$.

On note d le nombre dont l'écriture décimale est $= \overline{a_n a_{n-1}\cdots a_k \cdots a_1}$ (nombre formé à partir de N en supprimant son chiffre des unités).

On pose $n_1 = d - 2a_0$.

1/ Que vaut $n - 10n_1$?

2/ Montrons que n est divisible par 7 si, et seulement si n_1 est divisible par 7.

3/ Montrer que $n_1 < n$.

4/ Si n_1 a au moins trois chiffres, on itère le procédé ; on définit ainsi une suite de nombres n_k. À quelle condition sur n_k n est-il divisible par 7 ?

5/ Le nombre 881909 est-il divisible par 7 ?

Correction:

1/ On a $n = 10d + a_0$ donc $n - 10n_1 = 10d + a_0 - 10(d - 2a_0) = 21a_0$.

2/ Supposons que $n \equiv 0$ [7] ; on a $n - 10n_1 \equiv 21a_0$ [7] $\equiv 0$ [7] donc $10n_1 \equiv 0$ [7].
Résolvons l'équation $10x \equiv 0$ [7]. Pour cela, on renseigne un tableau.
$10 \equiv 3$ [7] et soit r le reste de la division euclidienne de x par 7. Alors $10x \equiv 3r$ [7].

r	0	1	2	3	4	5	6
$10x$ [7]	0	3	6	2	5	1	4

On en déduit que $10x \equiv 0$ [7] $\Leftrightarrow x \equiv 0$ [7].
Par conséquent : $n \equiv 0$ [7] $\Rightarrow n_1 \equiv 0$ [7].
Réciproquement : si $n_1 \equiv 0$ [7], alors $n \equiv 0$ [7].

3/ $n - n_1 = 10d + a_0 - (d - 2a_0) = 9d + 3a_0 > 0$ donc $n > n_1$

4/ n est divisible par 7 si, et seulement si, n_k l'est.

5/ Pour $n = 881909$, on trouve $n_1 = 88172$, $n_2 = 8813$ puis $n_3 = 875$ qui est divisible par 7, donc $n = 881909$ est divisible par 7.

Congruences

1 **Exercice** Pour chaque valeur de a donnée, trouver un relatif x tel que : $a \equiv x\ [9]$ et $-4 \leqslant x < 5$.

1/ $a = 11$ **3/** $a = 62$ **5/** $a = -12$

2/ $a = 24$ **4/** $a = 85$ **6/** $a = 32$

2 **Exercice** Démontrer que pour tout naturel k, $5^{4k} - 1$ est divisible par 13.

3 **Exercice** Trouver les restes de la division euclidienne par 7 des nombres $351^{12} \times 85^{15}$ et $16^{12} - 23^{12}$.

4 **Exercice** Trouver les restes de la division euclidienne par 11 des nombres 12^{15}, 10^{7}, 78^{15}, 13^{12} et $(-2)^{19}$.

5 **Exercice**

1/ Vérifier que $2^4 \equiv -1\ [17]$ et $6^2 \equiv 2\ [[]17]$.

2/ Quel est le reste de la division par 17 des nombres 1532^{20} et 346^{12}.

6 **Exercice** Résoudre dans $\mathbb{Z}$ les système suivants :

1/ $\begin{cases} x+2 & \equiv & -1\ [7] \\ x & > & 0 \end{cases}$. **2/** $\begin{cases} x & \equiv & -2\ [5] \\ 100 \leqslant & x & < 125 \end{cases}$.

7 **Exercice** Le nombre n désigne un naturel.

1/ Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisible par $n + 1$.

2/ Déterminer l'ensemble de valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$.

3/ En déduire que, quel que soit $n \in \mathbb{Z}$, $3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$.

8 **Exercice** Démontrer que pour tout entier naturel n, $5^{2n} - 14^n$ est divisible par 11.

9

Exercice

1/ Démontrer que pour tout entier n est congru soit à 0, 1 ou 4 modulo 8.

2/ Résoudre alors dans $\mathbb{Z}$ l'équation : $(n+3)^2 - 1 \equiv 0\ [8]$.

10

Exercice

1/ Quels sont les restes possibles de la division de 3^n par 11 ?

2/ En déduire les entier n pour lesquels $3^n + 7$ est divisible par 11.

11

Exercice Déterminer les entiers n tels que $2^n - 1$ est divisible par 9.

12

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

1/ Déterminer les restes de la division euclidienne de x^3 par 9 selon les valeurs de x.

2/ En déduire que pour tout relatif x :

- $x^3 \equiv 0\ [9]$ équivaut à $x \equiv 0\ [3]$.
- $x^3 \equiv 1\ [9]$ équivaut à $x \equiv 1\ [3]$.
- $x^3 \equiv 8\ [9]$ équivaut à $x \equiv 2\ [3]$.

3/ x, y, z sont des relatifs tels que : $x^3 + y^3 + z^3$ est divisible par 9.
Démontrer que l'un des nombres x, y, z est divisible par 3.

13

Exercice

1/ Déterminer l'ensemble $\mathscr{E}_1$, des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 7.

2/ Déterminer l'ensemble $\mathscr{E}_2$ des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 3.

3/ Soit $k \in \mathbb{N}$. Vérifier que si $x = 1 + 21k$ ou $x = -2 + 21k$ alors $n = x^2 + x - 2$ est divisible par 42.

14

Exercice *Pour chacune des propositions suivantes indiquer si elle est vraie ou fausse et donner une justification de la réponse choisie.*

Proposition 1 : Le reste de la division euclidienne de 2011^{2011} par 7 est 2.

Proposition 2 : 11^{2011} est congru à 4 modulo 7.

Proposition 3 : $x^2 + x + 3 \equiv 0\ [5]$ si et seulement si $x \equiv 1\ [5]$.

15

Exercice On considère l'équation $(\mathscr{F})$: $11x^2 - 7y^2 = 5$, où x et y sont des entiers relatifs.

1/ Démontrer que si le couple $(x;\ y)$ est solution de $(\mathscr{F})$, alors $x^2 \equiv 2y^2\ [5]$.

2/ Soient x et y des entiers relatifs. Recopier et compléter les deux tableaux suivants :

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à					

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à					

Quelles sont les valeurs possibles du reste de la division euclidienne de x^2 et de $2y^2$ par 5 ?

3/ En déduire que si le couple $(x;\ y)$ est solution de $(\mathscr{F})$, alors x et y sont des multiples de 5.

16

Exercice Pour tout entier naturel n supérieur ou égal à 2, on pose $A(n) = n^4 + 1$.

1/ Étudier la parité de l'entier $A(n)$.

2/ Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.

3/ Montrer que, pour tout entier d diviseur de $A(n)$, $n^8 \equiv 1\ [d]$.

17

Exercice On considère l'équation notée $(\mathscr{G})$:

$$3x^2 + 7y^2 = 10^{2n}, \quad \text{où } x \text{ et } y \text{ sont des entiers relatifs.}$$

1/ Montrer que $100 \equiv 2\ [7]$.
Démontrer que si $(x;\ y)$ est solution de $(\mathscr{G})$ alors $3x^2 \equiv 2^n\ [7]$.

2/ Reproduire et compléter le tableau suivant :

Reste de la division euclidienne de x par 7	0	1	2	3	4	5	6
Reste de la division euclidienne de $3x^2$ par 7							

3/ Démontrer que 2^n est congru à 1, 2 ou 4 modulo 7.
En déduire que l'équation $(\mathscr{G})$ n'admet pas de solution.

18

Exercice On considère la suite $(u_n)_{n\in\mathbb{N}}$ d'entiers naturels définie par :

$$\begin{cases} u_o &= 14 \\ u_{n+1} &= 5u_n - 6 \end{cases}, \quad \text{pour tout entier naturel } n.$$

1/ Calculer u_1, u_2, u_3 et u_4.
Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?

2/ Montrer que, pour tout entier naturel n, $u_{n+2} \equiv u_n$ [4].
En déduire que pour tout entier naturel k, $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4].

3/ (a) Montrer par récurrence que, pour tout entier naturel n, $2u_n = 5^{n+2} + 3$.

(b) En déduire que, pour tout entier naturel n, $2u_n \equiv 28$ [1]00.

4/ Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

19

Exercice Soit a et b deux entiers naturels non nuls.

On appelle « réseau » associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthogonal, dont les coordonnées $(x;\ y)$ sont des entiers vérifiant les conditions : $0 \leqslant x \leqslant a$ et $0 \leqslant y \leqslant b$.

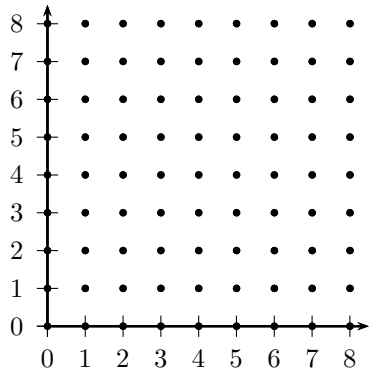
On note $R_{a,b}$ ce réseau. Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriétés géométriques des points correspondants du réseau.

Représentation graphique de quelques ensembles

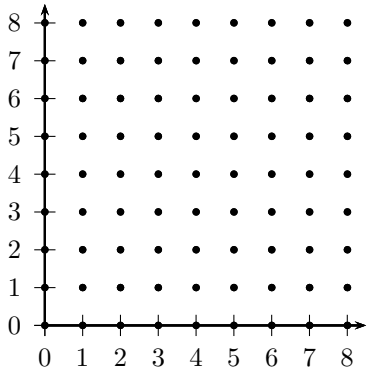
Dans cette question, les réponses sont attendues sans explication, sous la forme d'un graphique qui sera dûment complété sur la feuille ci-dessous.

Représenter graphiquement les points $M(x;\ y)$ du réseau $R_{8,8}$ vérifiant :

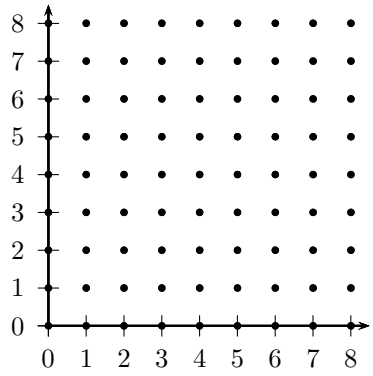
1/ $x \equiv 2$ [3] et $y \equiv 1$ [3].



2/ $x + y \equiv 1$ [3].



3/ $x \equiv y$ [3].



Chapitre

3

PGCD et PPCM

On continue notre voyage avec les entiers et la divisibilité en rajoutant une condition qualitative :« plus grand » diviseur et « plus petit » multiple.

Ce chapitre est un prélude nécessaire à deux théorème centraux en arithmétique : les théorèmes de Gauss et de Bézout.

Sommaire

I Plus Grand Commun Diviseur

I.1 Généralités

Définition 1

Soit a et b deux entiers relatifs non nuls.
Le plus grand diviseur commun à a et à b est appelé le PGCD de a et b.
On le note $\text{pgcd}(a,b)$ ou encore $a \wedge b$.

Remarque: Comme 1 divise tous nombres entiers a et b alors $\text{pgcd}(a,b) \geqslant 1$.

Preuve: Avant de donner un nom à quelque chose, il faut montrer que ce quelque chose existe et avant de l'appeler « le », il faut montrer qu'il est unique.

Existence : L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ des diviseurs communs à a et b est un ensemble fini car intersection de deux ensembles finis.

De plus 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.

Or, tout ensemble fini non vide admet un plus grand élément que l'on peut appeler $\text{pgcd}(a,b)$.

Unicité : Le fait que $\text{pgcd}(a,b)$ ait été choisi comme le plus grand élément d'un ensemble fini impose son unicité. . . s'il en existait un plus grand, on prendrait celui-là.

Dans la pratique, on se bornera souvent au cas où a et b sont dans $\mathbb{N}^*$ et tels que $a > b$. Cette condition n'est pas restrictive car les diviseurs d'un nombre et de son opposé sont les mêmes, donc $\text{pgcd}(a,b) = \text{pgcd}(|a|,|b|)$ pour a et b dans $\mathbb{Z}$. Et, par ailleurs, parmi deux entiers naturels a et b, il y en a un qui est plus grand que l'autre. Il suffira donc de commencer par diviser le plus grand par le plus petit.

Exemple 1:

- $\text{pgcd}(24,18) = 6$.
- $\text{pgcd}(60,84) = 12$.
- $\text{pgcd}(150,240) = 30$.
- $\text{pgcd}(27,140) = 1$.
- $\text{pgcd}(6,72) = 6$.
- $\text{pgcd}(31,45) = 1$.
- $\text{pgcd}(5,7) = 1$.

[Exercices 105 à 107 page 464 , **Maths Repère**, *Hachette*]

Proposition 1

- $\text{pgcd}(a,a) = a$ et $\text{pgcd}(1,a) = 1$.
- Si $b|a$ alors $\text{pgcd}(a,b) = |b|$.

Preuve: Évident !

Théorème 1 (Fondamental)

Soit a et b deux entiers non nuls tels et un couple d'entiers $(q\,;r\,)$tels que $a = bq + r$.

$$\text{pgcd}(a,b) = \text{pgcd}(b,r).$$

[Lemme d'Euclide page 439 , **Maths Repère**, *Hachette*]

Preuve: Posons $D = \text{pgcd}(a,b)$ et $d = \text{pgcd}(a,b)$.

- Comme D divise a et b, il divise aussi $a - bq = r$. Donc D est un diviseur de a et r et $D \leqslant d$.
- De la même manière, d divise b et r donc divise $bq + r = a$ et $d \leqslant D$.
- On conclue aisément à $D = d$.

[Exercices 108, 112 à 114 page 464
Exercices 118 et 121 pages 464-465 , **Maths Repère**, *Hachette*]

Méthode 1 (Égalité entre deux nombres)

Soit d et D, deux quantités. Pour montrer que $d = D$, il suffit :

- de montrer successivement que $d \leqslant D$ puis $D \leqslant d$.
- dans le cas de nombres entiers positifs, on pourra aussi montrer que $d|D$ puis $D|d$.

Remarque: Même si cela ressemble fortement à la division euclidienne, il n'est nullement besoin que ce le soit pour que ce théorème soit vrai.

Ce théorème est fondamental par ses applications et notamment dans l'algorithme d'Euclide ci-dessous.

[Vrai ou faux 11 page 454 , **Maths Repère**, *Hachette*]

I.2 Algorithme d'Euclide

Théorème 11

Soit a et b deux naturels non nuls tels que b ne divise pas a. La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le pgcd(a, b).

$$\begin{array}{lll} a \text{ par } b & a = bq_0 + r_0 & \text{avec} \quad b > r_0 \geqslant 0 \\ b \text{ par } r_0 & b = r_0q_1 + r_1 & \text{avec} \quad r_0 > r_1 \geqslant 0 \\ r_0 \text{ par } r_1 & r_0 = r_1q_2 + r_2 & \text{avec} \quad r_1 > r_2 \geqslant 0 \\ \vdots & \vdots & \vdots \quad \vdots \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}q_n + r_n & \text{avec} \quad r_{n-1} > r_n \geqslant 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_nq_{n-1} + 0 & \end{array}$$

On a alors pgcd$(a, b) = r_n$.

Preuve:

- La suite des restes r_0, r_1, r_2, …, r_n est une suite strictement décroissante dans $\mathbb{N}$. Elle est donc nécessairement finie. Il existe, de plus, un certain rang n tel que $r_{n+1} = 0$.
- En appliquant le **théorème** (I) de proche en proche, on obtient alors :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1) = \ldots = \text{pgcd}(r_{n-1}, r_n).$$

- Or, $r_{n-1} = r_nq_{n-1} + 0$ (*ie*) r_n divise r_{n-1}.
  Donc pgcd$(r_{n-1}, r_n) = r_n$.
- Conclusion : pgcd$(a, b) = r_n$. Le dernier reste non nul est le PGCD.

Exemple 2: Calculer le pgcd$(4539, 1958)$. On effectue les divisions euclidiennes suivantes :

$$\begin{aligned} 4539 &= 1958 \times 2 + 623 \\ 1958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

Conclusion : pgcd$(4539, 1958) = 89$.

Remarque: Le petit nombre d'étapes montre la performance de cet algorithme. Celui-ci porte le nom d'un père des mathématiques car il était effectivement connu d'Euclide six siècles avant notre ère!!!

Algorithme

Voici un algorithme d'Euclide que l'on peut proposer pour trouver le PGCD de deux nombres. On utilise la partie entière pour trouver le quotient.

```
1:  VARIABLES
2:  a, b, q, r SONT_DU_TYPE ENTIER NATUREL
3:  DEBUT_ALGORITHME
4:      Lire a, b
5:      q PREND_LA_VALEUR E(a/b)
6:      r PREND_LA_VALEUR a − bq
7:      TANT_QUE r <> 0 FAIRE
8:          DEBUT_TANT_QUE
9:          a PREND_LA_VALEUR b
10:         b PREND_LA_VALEUR r
11:         q PREND_LA_VALEUR E(a/b)
12:         r PREND_LA_VALEUR a − bq
13:         FIN_TANT_QUE
14:     Afficher b
15: FIN_ALGORITHME
```

[Exercice 117 page 464 , **Maths Repère**, *Hachette*]

Théorème III

Soient a et b deux entiers non nuls. Les diviseurs communs de a et b sont **exactement** les diviseurs de pgcd(a, b) :

$$\begin{cases} d|a \\ d|b \end{cases} \iff d|\operatorname{pgcd}(a, b).$$

Preuve: On démontre les deux implications séparément :

Condition nécessaire : Si $d|\operatorname{pgcd}(a, b)$ alors $d|a$ et $d|b$ par transitivité.

Condition suffisante : Soit d divisant a et b. Appliquons l'algorithme d'Euclide à a et b et considérons la suite finie des r_n apparaissant dans celui-ci.

A la première étape, $r_0 = a - bq$ (ie) $d|r_0$. On déroule alors en appliquant le **théorème** (I) fondamental :

$$\begin{cases} d|a \\ d|b \end{cases} \implies \begin{cases} d|b \\ d|r_0 \end{cases} \implies \begin{cases} d|r_0 \\ d|r_1 \end{cases} \implies \dots \implies \begin{cases} d|r_{n-1} \\ d|r_n \end{cases}.$$

Or, $r_n = \text{pgcd}(a, b)$.
Donc $d | \text{pgcd}(a, b)$.

Dans le cas de deux nombres a et b pas trop grands, on pourra ainsi réviser ses tables de multiplication et décomposer les deux nombres a et b en facteurs premiers et trouver, « à la main », le plus grand diviseur commun. [1]

1 **Exercice** Déterminer le PGCD de 1960 et de 34300.

Correction: On a : $1960 = 2^3 \times 5^1 \times 7^2$ et $34300 = 2^2 \times 5^2 \times 7^3$.

On en déduit que $\text{pgcd}(1960, 34300) = 2^2 \times 5^1 \times 7^2 = 980$.

Proposition 2

Pour tout entier naturel k non nul, $\text{pgcd}(ka, kb) = k \times \text{pgcd}(a, b)$.

[Démonstration page 439 , **Maths Repère**, *Hachette*]

Preuve: Ici aussi, on applique l'algorithme d'Euclide à a et b. Partant de $a = b \times q + r_0$ avec $0 \leqslant r_0 < b$, on a

$$ka = kb \times q + kr_0, \quad \text{avec } 0 \leqslant kr_0 < kb \tag{3.1}$$

(*ie*) (3.1) est bien l'expression de la division euclidienne de ka par kb et, dans l'algorithme d'Euclide appliqué à ka et kb, la suite des restes est formée des kr_n. Le dernier reste non nul sera donc $kr_n = k\,\text{pgcd}(a, b)$.

Donc $\text{pgcd}(ka, kb) = k \times \text{pgcd}(a, b)$.

Exemple 3: $\text{pgcd}(800, 500) = 100$ et $\text{pgcd}(36, 24 = \text{pgcd}(12 \times 3, 12 \times 2) = \text{pgcd}(3, 2)$.

2 **Exercice** Déterminer le PGCD de 8870 et de 3120.

I.3 Exercices classiques

3 **Exercice (Déterminer le PGCD de deux entiers dépendant de n)**

Déterminer, selon les valeurs de n, le pgcd de $A = 2n + 1$ et de $B = n - 5$.

1. Cette décomposition en facteurs premiers proprement dite est, en fait, un problème extrêmement difficile pour des nombres élevés. Pour trouver le pgcd de tels nombres nous aurons besoin d'un algorithme plus puissant (*cf* plus loin).

Méthode 2

On essaie de se débarrasser de n par des combinaisons linéaires afin d'utiliser le **théorème** (I).

Correction: On remarque tout d'abord que $A - 2B = 2n + 1 - 2(n-5) = 11$ (ie) $A = 2B + 11$.

D'après le **théorème** (I), on a donc $\text{pgcd}(A;B) = \text{pgcd}(B, 11)$. Comme 11 est un nombre premier, celui-ci ne peut valoir que 1 ou 11.

Or, $\text{pgcd}(B, 11) = 11$ si et seulement si 11 divise B.

Et, $\text{pgcd}(B, 11) = 11 \iff B \equiv 0\ [11] \iff n - 5 \equiv 0\ [11] \iff n \equiv 5\ [11]$.

On en conclut que $\text{pgcd}(A, B) = 11$ lorsque n est congru à 5 modulo 11 et à $\text{pgcd}(A, B) = 1$ dans tous les autres cas.

[Exercice résolu 7 page 446
Exercices 112 à 116 page 464 , **Maths Repère**, *Hachette*]

4 **Exercice (Égalité de deux PGCD)**

Soient a et b deux entiers naturels non nuls. Soient $x = 7a + 5b$ et $y = 4a + 3b$.

Montrer que $\text{pgcd}(x, y) = \text{pgcd}(a, b)$.

Correction:

Première méthode : On applique le même raisonnement qu'à l'exercice précédent avec des combinaisons linéaires judicieusement choisies afin d'utiliser le **théorème** (I).

$$7a + 5b = (4a + 3b) + (3a + 2b) \implies \text{pgcd}(7a + 5b, 4a + 3b) = \text{pgcd}(4a + 3b, 3a + 2b).$$

$$3a + 2b = 2(a + b) + a \implies \text{pgcd}(4a + 3b, 3a + 2b) = \text{pgcd}(a + b, a) = \text{pgcd}(a, b) = \text{pgcd}(a, b).$$

On en déduit que : $\text{pgcd}(x, y) = \text{pgcd}(a, b)$.

Deuxième méthode : On revient à la définition du PGCD en montrant, en deux temps, que $\text{pgcd}(x, y) | \text{pgcd}(a, b)$ puis $\text{pgcd}(a, b) | \text{pgcd}(x, y)$.

Pour se simplifier les notations, on pose $d = \text{pgcd}(a, b)$ et $d' = \text{pgcd}(x, y)$.

- d divise a et b, donc d divise aussi $x = 7a + 5b$ et $y = 4a + 3b$. On en déduit que $d|d'$.
- De même, si d' divise $7a + 5b$ et $4a + 3b$ alors d' divise aussi $7(4a + 3b) - 4(7a + 5b) = b$ et $3(7a + 5b) - 5(4a + 3b) = a$. Donc $d'|d$.

Comme d divise d' et d' divise d, on a donc $d = d'$.

II Nombres premiers entre eux

Définition 2 (Nombres premiers entre eux)

On dit que a et b sont premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$.

Exemple 4: $\text{pgcd}(15, 8) = 1$ donc 15 et 8 sont premiers entre eux.

Remarques:

- Cela revient aussi à dire que leurs seuls diviseurs sont -1 et 1.
- Une autre conséquence est que deux entiers consécutifs n et $n + 1$ sont nécessairement premiers entre eux puisque tout diviseur des deux diviserait 1.
- Cette notion s'étend facilement à un nombre quelconque d'entiers :

  Dire que 3 entiers sont premiers entre eux signifie que le plus grand nombre les divisant est 1.

  Exemple 5: 6, 10 et 15 sont premiers entre eux sans qu'ils le soient deux à deux.

ATTENTION Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers : 15 et 8 sont premiers entre eux sans pour autant être premiers.

Bien sûr, deux nombres premiers distincts sont nécessairement premiers entre eux.

Tout d'abord une propriété simple mais utile :

Proposition 3

Un nombre premier est premier avec tous les nombres qu'il ne divise pas.

Preuve: Soient p un nombre premier, a un entier non divisible par p et $d = \text{pgcd}(a, p)$.

Par définition, d vaut 1 ou p, puisque p est premier.

d ne peut pas être égal à p, sinon p diviserait a. Par conséquent : $d = 1$.

Proposition 4

Soient a et b des naturels non nuls et d un diviseur commun de a et b. On pose $a = da'$ et $b = db'$.
Le PGCD de a et b est d si et seulement si a' et b' sont premiers entre eux.

$$\text{pgcd}(a, b) = d \iff \text{pgcd}(a', b') = 1.$$

Preuve: Tout repose sur la **proposition** (2) : $\text{pgcd}(da', db') = d \times \text{pgcd}(a', b')$.

- Si d est le PGCD de a et b alors $d = \text{pgcd}(da', db') = d\,\text{pgcd}(a', b') \implies \text{pgcd}(a', b') = 1$ après simplification par $d \neq 0$. Donc a' et b' sont premiers entre eux.
- Réciproquement, si $\text{pgcd}(a', b') = 1$, alors $\text{pgcd}(a, b) = d\,\text{pgcd}(a', b') = d$.

[Vrai ou faux 12 page 454 , **Maths Repère**, *Hachette*]

On utilisera, en général, cette proposition sous la forme du corollaire ci-dessous :

Corollaire 1

Soient a et b deux entiers non nul et $d = \text{pgcd}(a, b)$.
Alors il existe un unique couple d'entier $(a' ; b')$ premiers entre eux tels que $a = da'$ et $b = db'$.

On utilisait déjà ce corollaire au collège lorsque l'on simplifier les fractions par exemple :

$$\frac{a}{b} = \frac{\cancel{d} \times a'}{\cancel{d} \times b'} = \frac{a'}{b'}.$$

Comme $\text{pgcd}(a', b') = 1$, la fraction $\dfrac{a'}{b'}$ est irréductible.

[Exercices 109 et 110 page 464 , **Maths Repère**, *Hachette*]

5 **Exercice** Déterminer les entiers naturels dont la somme est 600 et dont le PGCD est 50.

Correction: On cherche a et b tels que : $a + b = 600$ et $\text{pgcd}(a; b) = 50$.

D'après le **corollaire** (1), il existe deux entiers a' et b' premiers entre eux tels que $a = 50a'$ et $b = 50b'$.

Il n'y a plus qu'à dérouler et simplifier :

$$a + b = 600 \implies 50(a' + b') = 600 \implies a' + b' = 12.$$

On cherche donc tous les couples d'entiers naturels vérifiant cette relation et on ne garde que les couples d'entiers premiers entre eux. $(1; 11)$, $(5; 7)$, $(7; 5)$ et $(11; 1)$.

Les couples solutions sont alors $(50; 550)$, $(250; 350)$, $(350; 250)$ et $(550; 50)$.

Réciproquement, on vérifiera bien que ces couples conviennent. [2]

[Exercice résolu 8 page 447
Exercices 124 à 126 page 465 , **Maths Repère**, *Hachette*]

2. On l'écrira dans tous les cas.

[Exercices 127 à 135 pages 465-466 , **Maths Repère**, *Hachette*]

[Problème 218 page 481 , **Maths Repère**, *Hachette*]

III Plus Petit Commun Multiple

III.1 Généralités

Définition 3

Soit a et b deux entiers relatifs non nuls.
L'ensemble des multiples strictement positifs communs à a et à b admet un plus petit élément appelé plus petit commun multiple.
On le note $\text{ppcm}(a,b)$ ou $a \vee b$.

Preuve: La démonstration est identique à celle du pgcd :

- L'ensemble des multiples strictement positifs à a et à b n'est pas vide puisqu'il contient au moins $|ab|$.

  Comme toute partie non vide de $\mathbb{N}$ admet un plus petit élément, $\text{ppcm}(a,b)$ existe.

- Comme on a pris le plus petit des candidats par définition, $\text{ppcm}(a,b)$ est unique.

Au collège[3], pour additionner deux fractions, on recherchait le dénominateur commun le plus petit qui n'était rien d'autre que $\text{ppcm}(a,b)$.

Exemple 6:

- $\text{ppcm}(18,12) = 36$.
- $\text{ppcm}(24,40) = 120$.
- $\text{ppcm}(11,17) = 11 \times 17 = 187$.
- $\text{ppcm}(19,5) = 19 \times 5 = 195$.

Remarque: Le seul multiple de 0 est 0 donc, pur tout entier a, $\text{ppcm}(a,0) = 0$.

3. Encore !

Proposition 5

Soient a et b deux entiers non nuls.

- Le PPCM de deux entiers naturels non nuls est un entier au moins égal à 1.
- $\text{ppcm}(a,a) = a$ et $\text{ppcm}(1,a) = a$.
- Si $b|a$ alors $\text{ppcm}(a,b) = |a|$.
- Si a et b sont premiers entre eux alors $\text{ppcm}(a,b) = |ab|$.
- $|ab| = \text{ppcm}(a,b) \times \text{pgcd}(a,b)$.

Preuve: Les premières assertions sont claires.

Pour la dernière, il nous manque encore un théorème qui arrive bientôt : le théorème de Gauss.

Exemple 7: Le PGCD de 42 et 60 est 6. Si on note m leur PPCM, alors $6m = 42 \times 60$ d'où $m = 420$.

6 **Exercice** Déterminer $m = 44100 \vee 36036$.

Correction: On commence par déterminer $44100 \wedge 36036$ l'algorithme d'Euclide :

$$44100 \wedge 36036 = 36036 \wedge 8064 = 8064 \wedge 3780 = 3780 \wedge 504 = 504 \wedge 252 = 252.$$

D'après la relation (5), on a alors $252 \times m = 44100 \times 36036$.

D'où $m = \dfrac{44100 \times 36036}{252} = 6306300$.

Corollaire 2

Si k est un entier naturel : $\text{ppcm}(ka, kb) = k \times \text{ppcm}(a,b)$.

Preuve: Si k, a ou b est nul, c'est évident.

Sinon, supposons a, b et k non nuls.

Toujours d'après (5), $\text{ppcm}(ka,kb) \times \text{pgcd}(ka,kb) = ka \times kb$.

Or, $\text{pgcd}(ka,kb) = k \times \text{pgcd}(a,b)$.

Après simplification, on a le résultat escompté.

Théorème IV

Soient a et b deux entiers non nuls. Les multiples communs de a et b sont **exactement** les multiples $\text{ppcm}(a,b)$:

$$\begin{cases} a|m \\ b|m \end{cases} \iff \text{ppcm}(a,b)|m.$$

Preuve: On démontre les deux implications séparément :

Condition nécessaire : Si m est un multiple de $\text{ppcm}(a,b)$ alors m est un multiple de a et b par définition.

Condition suffisante : Soit m un multiple de a et b. Posons $M = \text{ppcm}(a,b)$.

La division euclidienne de m par M s'écrit $m = Mq + r$ avec $0 \leqslant r < M$.

Or, $r = m - Mq$ est alors aussi un multiple de a et b et strictement plus petit que $M = \text{ppcm}(a,b)$. Ceci n'est possible qu'à la condition que $r = 0$ (ie) $m|M$. $\text{ppcm}(a,b)$ est donc un multiple de m.

Méthode 3 (Trouver un PPCM)

Pour des entiers a et b pas « trop grands », une méthode enfantine mais souvent suffisante est de décomposer a et b en facteurs premiers.
Le PPCM de a et b est alors égal au produit de tous les facteurs premiers de a et b pris avec l'exposant le plus grand apparaissant dans les décompositions.

7 **Exercice** Déterminer le PPCM de 240 et de 756.

III.2 Exercices classiques

8 **Exercice** Déterminer deux entiers naturels a et b connaissant leur produit 1512 et leur PPCM 252.

Correction: Posons $d = a \wedge b$.

D'après (5), $252 \times d = ab$. Donc $d = 6$.

Posons $a = da'$ et $b = db'$ avec a' et b' premiers entre eux.

On a alors $35a'b' = 1512$ d'où $a'b' = 42$. Comme a' et b' sont premiers entre eux, le couple (a', b') ne peut être égal qu'à :

$$(1;42),\ (2;21),\ (3.14),\ (6.7),\ (7;6),\ (14,3),\ (21;2),\ \text{ou}\ (42;1).$$

On multiplie par 6 pour avoir tous les couples solutions.

9 **Exercice** Soient d et m le PGCD et le PPCM de deux naturels a et b? Déterminer a et b tels que $m - 2d = 11$.

Correction: Posons toujours $a = da'$ et $b = db'$ avec a' et b' premiers entre eux.

Comme $md = ab$, on a $md = d^2a'b'$ puis $m = da'b'$.

La relation donnée s'écrit ainsi $da'b' - 2d = 11$.

$$d(a'b' - 2) = 11$$

D'où d, positif, divise 11. Il ne peut être égal qu'à 11 ou 1.

- Si $d = 11$, alors $a'b' - 2 = 1$ et $a'b' = 3$. Donc $(a', b') = (1, 3)$ ou $(3, 1)$ et $(a, b) = (11, 33)$ ou $(33, 11)$.
- Si $d = 1$, alors $a'b' = 13$ et $(a', b') = (1, 13)$ ou $(13, 1)$. Alors $(a, b) = (13, 1)$ ou $(1, 13)$.

On trouve donc 4 couples solutions.

Arithmétique

1 **Exercice (Petite devinette)**

« Je suis un entier naturel. Quand on me divise par 4, le reste est 3, mais quand on me divise par 5, le reste est 1 et le quotient inchangé.

Qui suis-je ? »

2 **Exercice**

1/ Résoudre dans $\mathbb{R}_+$, l'inéquation $x^2 - 12x - 8 > 0$.

2/ Soit n un entier naturel.

(a) Montrer que $(n+2)^3 = n^2(n+6) + 12n + 8$.

(b) Sous quelle condition, cette écriture traduit-elle la division euclidienne de $(n+2)^3$ par n^2 ? Préciser le reste et le quotient.

3/ Déterminer les entiers naturels pour lesquels le reste de la division euclidienne de $(n+2)^3$ par n^2 est $12n + 8$.

3 **Exercice (Disjonction de cas)**

1/ Compléter la phrase suivante : « $a \equiv 0\ [7]$ signifie que ..... »

2/ Compléter le tableau suivant des restes dans la congruence modulo 7 :

n	0	1	2	3	4	5	6
n^2							
n^2+5							
$n(n^2+5)$							

3/ Déterminer les entiers n pour lesquels le nombre $a = n(n^2+5)$ est divisible par 7.

4 **Exercice (Questions diverses)**

1/ Quel est le reste de la division par 5 de 8^{2015} ?

2/ Soit n un entier naturel. Montrer que $3^{2n+1} + 2^{n+2} \equiv 0\ [7]$.

3/ Reprenons la fonction f du devoir précédent, c'est-à-dire, $f(x) = \dfrac{3x-1}{x+1}$ sur $\mathbb{R} \setminus \{-1\}$.

Quels sont les points de sa courbe représentative dont les coordonnées sont des entiers naturels ?

L'arithmétique, c'est être capable de compter jusqu'à vingt sans enlever ses chaussures.

W. Disney

Chapitre

4

Les Grands Théorèmes

Entrons dans le vif du sujet !

Sommaire

I Théorème de Bézout

I.1 Égalité de Bézout

Théorème 1

Soit a et b deux entiers non nuls et $d = \text{pgcd}(a, b)$.
Il existe alors un couple (u, v) d'entiers relatifs tels que :

$$au + bv = d.$$

[Démonstration page 440 , **Maths Repère**, *Hachette*]

ATTENTION Il n'y a pas unicité du couple (u, v).

Preuve: Considérons $\mathcal{G}$ l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs.

$\mathcal{G}$ est une partie de $\mathbb{N}$ non vide car il contient, par exemple $|a|$ en prenant $m = \pm 1$ et $n = 0$.

$\mathcal{G}$ admet donc un plus petit élément $d = au + bv$. Il ne reste plus qu'à montrer que $d = \text{pgcd}(a, b)$. On le fait par double inégalité.

- Posons $D = \text{pgcd}(a, b)$. Comme D divise a et b, il divise aussi $au + bv = d$. Donc $D \leqslant d$.

- Montrons que d divise a.
  La division euclidienne de a par d s'écrit $a = dq + r$ avec $0 \leqslant r < d$. D'où,

$$\begin{aligned} r &= a - dq \\ r &= a - (au + bv)q \\ r &= a(1 - uq) + b(-vq). \end{aligned}$$

  Donc $r \in \mathcal{G}$ et $r < d$. Cette condition ne peut être remplie sans contredire la définition de d que si $r = 0$ (ie) $d|a$.
  Par le même raisonnement, on montrerait que $d|b$.
  Le nombre d est donc un diviseur de a et b. Il est plus petit que D : $d \leqslant D$.

Conclusion : $d = D$.

Corollaire 1

Tout diviseur commun à a et b divise leur pgcd.

Remarque: On avait déjà démontré ce corollaire au chapitre précédent.

Ce corollaire permettra, par exemple, de montrer que deux entiers sont égaux en montrant qu'ils se divisent l'un l'autre.

I.2 Théorème de Bézout

ROC

Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que :

$$au + bv = 1.$$

Preuve:

- Si $a \wedge b = 1$, c'est immédiat grâce à l'égalité de Bézout.
- Réciproquement, supposons qu'il existe deux entiers u et v tels que : $au + bv = 1$.
  $\text{pgcd}(a, b)$ divise a et b par définition donc divise aussi $au + bv = 1$.
  Donc $\text{pgcd}(a, b) = 1$.

Remarque: (Un peu hors-programme)

$$au + bv = 1 \iff au \equiv 1\ [b]\ (ie) \text{ modulo } b,\ a \text{ est inversible d'inverse } u\ [b].$$

[Exercice 156 page 468 , **Maths Repère**, *Hachette*]

Exemples 1:

- 5 et 12 sont premiers entre eux car $7 \times (-5) + 3 \times 12 = 1$.
- $(n+1) - n = 1$ donc n et $n+1$ sont toujours premiers entre eux.
- Montrons que $2n+1$ et $3n+2$ sont premiers entre eux pour tout $n \in \mathbb{N}$.
  Il s'agit de trouver des coefficients u et v tels que $u(2n+1) + v(3n+2) = 1$.
  Or, $-3(2n+1) + 2(3n+2) = -6n - 3 + 6n + 4 = 1$, $\forall\, n \in \mathbb{N}$.
  Donc $2n+1$ et $3n+2$ sont premiers entre eux.

Reste un problème de taille : comment trouver un des couples (u, v) ? L'algorithme d'Euclide va, ici encore, venir à notre rescousse.

[Exercices 136 à 140 page 467 , **Maths Repère**, *Hachette*]

1 **Exercice (Fondamental)** Montrer que les nombres 3920 et 1089 sont premiers entre eux et déterminer des entiers u et v tels que :

$$3920u + 1089v = 1.$$

Méthode 1 (Trouver u et v tels que $au + bv = 1$)

On écrit toutes les divisions de l'algorithme d'Euclide.
On reporte alors chaque reste obtenu en partant de la fin.

Correction: On applique la méthode :

$$\begin{aligned}
3920 &= 1089 \times 3 + \boxed{653} \\
1089 &= 653 \times 1 + \boxed{436} \\
653 &= 436 \times 1 + \boxed{217} \\
436 &= 217 \times 2 + \boxed{2} \\
217 &= 2 \times 108 + \boxed{1} \\
2 &= 1 \times 2 + 0
\end{aligned}$$

Tout d'abord, le dernier reste non nul est bien 1, donc 3920 et 1089 sont bien premiers entre eux.

On remonte ensuite l'algorithme d'Euclide :

$$\begin{aligned}
217 - \boxed{2} \times 108 &= \boxed{1} \\
\boxed{2} &= 436 - 217 \times 2
\end{aligned} \quad \Longrightarrow \quad \begin{aligned}
\boxed{217} - (436 - \boxed{217} \times 2) \times 108 &= 1 \\
\boxed{217} \times (1 + 2 \times 108) - 436 \times 108 &= 1 \\
\boxed{217} \times 217 - 436 \times 108 &= 1.
\end{aligned}$$

Or, $\boxed{217} = 653 - 436 \times 1$. On remplace et on réitère :

$$(653 - \boxed{436} \times 1) \times 217 - \boxed{436} \times 108 = 1$$
$$653 \times 217 - \boxed{436} \times 325 = 1.$$

Or, $\boxed{436} = 1089 - 653$. On remplace encore :

$$\boxed{653} \times 217 - (1089 - \boxed{653}) \times 325 = 1$$
$$\boxed{653} \times 542 - 1089 \times 325 = 1$$

$$\boxed{653} = 3920 - 1089 \times 3 \implies (3920 - 1089 \times 3) \times 542 - 1089 \times 325 = 1$$
$$\mathbf{3920} \times 542 - \mathbf{1089} \times 1951 = 1.$$

2 **Exercice** Même exercice avec les entiers 59 et 27.

Correction: $59 \times 11 + 27 \times (-24) = 1$.

I.3 Algorithme de Bézout

Deux entiers aa et b donnés, il s'agit de déterminer un couple (u, v) d'entiers relatifs vérifiant $au+bv = \text{pgcd}(a, b)$. On va d'abord démontrer un lemme préliminaire en revenant à l'algorithme d'Euclide :

$$\begin{array}{ccccccccccccc}
a & \text{par} & b & & a & = & bq_0 + r_0 & \implies & r_0 & = & a - bq & = & au_0 + bv_0 \\
b & \text{par} & r_0 & & b & = & r_0q_1 + r_1 & \implies & r_1 & = & b - r_0q_1 & = & au_1 + bv_1 \\
r_0 & \text{par} & r_1 & & r_0 & = & r_1q_2 + r_2 & \implies & r_2 & = & r_0 - r_1q_1 & = & au_2 + bv_2 \\
 & \vdots & & & & \vdots & & \vdots & & \vdots & & \vdots & \\
r_{k-2} & \text{par} & r_{k-1} & & r_{k-2} & = & r_{k-1}q_k + r_k & \implies & r_k & = & r_{k-2} - r_{k-1}q_k & = & au_k + bv_k \\
 & \vdots & & & & \vdots & & \vdots & & \vdots & & \vdots & \\
r_{n-2} & \text{par} & r_{n-1} & & r_{n-2} & = & r_{n-1}q_n + d & \implies & d & = & r_{n-2} - r_{n-1}q_n & = & au_n + bv_n
\end{array}$$

Lemme II: Les suites $(r_n)_{n\in\mathbb{N}}$, $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ intervenant dans l'algorithme d'Euclide sont définies par la même relation de récurrence d'ordre 2 :

$$\forall\, n \in \mathbb{N},\ n \geqslant 2,\ \begin{cases} r_k = r_{k-2} - r_{k-1}q_k \\ u_k = u_{k-2} - u_{k-1}q_k \\ v_k = v_{k-2} - v_{k-1}q_k \end{cases} \quad \text{où } q_k \text{ est le quotient de } r_{k-2} \text{ par } r_{k-1}. \tag{4.1}$$

Preuve: Il suffit de reprendre la méthode à l'étape une étape k quelconque :

Par construction,

$$r_k = r_{k-2} - r_{k-1}q_k. \tag{4.2}$$

Or, $r_{k-2} = au_{k-2} + bv_{k-2}$ et $r_{k-1} = au_{k-1} + bv_{k-1}$. En remplaçant dans (4.2), on obtient :

$$r_{k-2} = a(\underbrace{u_{k-2} - u_{k-1}q_k}_{u_k}) + b(\underbrace{v_{k-2} - v_{k-1}q_k}_{v_k}).$$

D'où le résultat.

En empruntant une notation matricielle au chapitre suivant, la relation (4.1) s'écrit plus simplement :

$$\begin{pmatrix} r_k \\ u_k \\ v_k \end{pmatrix} = \begin{pmatrix} r_{k-2} \\ u_{k-2} \\ v_{k-2} \end{pmatrix} - \begin{pmatrix} r_{k-1} \\ u_{k-1} \\ v_{k-1} \end{pmatrix} \times q_k \qquad \Longleftrightarrow \qquad L_k = L_{k-2} - L_{k-1} \times q_k.$$

où L_k pourra être considérée, pour l'instant, comme une liste de trois entiers par l'algorithme.

Au premier passage de l'algorithme on a $u_0 = 1$, $v_0 = -q$ et $r_0 = a - bq$ donc on a :

$$\begin{pmatrix} u \\ v \\ r \end{pmatrix} = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix} \times q.$$

Il faudra donc initialiser le rang $k-2$ avec $\begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$ et le rang $k-1$ avec $\begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$.

```
1:  VARIABLES
2:  a, b SONT_DU_TYPE ENTIER NATUREL
3:  List1, List2 et List3 SONT DU TYPE LISTE
4:  DEBUT_ALGORITHME
5:      Lire a, b
6:      List1 PREND_LA_VALEUR {a, 1, 0}
7:      List2 PREND_LA_VALEUR {b, 0, 1}
8:      List3(1) PREND_LA_VALEUR a − b × E(a/b)
9:      TANT_QUE List3(1) <> 0 FAIRE
10:         DEBUT_TANT_QUE
11:         List3 PREND_LA_VALEUR List1 − E(List1(1)/List2(1)) × List2
12:         List1 PREND_LA_VALEUR List2
13:         List2 PREND_LA_VALEUR List3
14:         FIN_TANT_QUE
15:     Afficher List1
16: FIN_ALGORITHME
```

Le dernier triplet $\begin{pmatrix} r \\ u \\ v \end{pmatrix}$ dans la liste 1 correspond au PGCD d et aux coefficients de la relation de Bézout.

On a : $au + bv = d$.

[Exercice 159 page 468 , **Maths Repère**, *Hachette*]

Théorème III

L'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple du pgcd(a, b).

Dans $\mathbb{R}$, les solutions sont tous les points de la droite d'équation $ax + by = c$. Dans $\mathbb{Z}^2$, cela revient à chercher seulement ceux à coordonnées entières. Problème pas si évident qu'il n'y paraît.

[Exercice 21 page 455 , **Maths Repère**, *Hachette*]

Preuve: Posons $d = \text{pgcd}(a, b)$.

- Si $ax + by = c$ admet une solution (x_0, y_0) alors, d divisant a et b, il divise toute combinaison linéaire de ceux-ci.
  Donc $d|c$.
- Réciproquement, supposons que c soit multiple de d (ie) $\exists k \in \mathbb{Z}$ tel que $c = kd$.
  D'après l'égalité de Bézout, il existe aussi deux entiers relatifs u et v tels que :

$$au + bv = d.$$

  En multipliant par k, on obtient :

$$auk + bvk = kd \iff a(uk) + b(vk) = c.$$

  Le couple $(x_0, y_0) = (uk, vk)$ est donc bien solution.

[Exercice résolu 10 page 448
Exercice résolu 11 page 449 , **Maths Repère**, *Hachette*]

Exemples 2:

- L'équation $4x + 9y = 2$ admet des solutions car $\text{pgcd}(4, 9) = 1$ et 2 multiple de 1.
- L'équation $9x - 15y = 2$ n'admet pas de solution car $\text{pgcd}(9, 15) = 3$ et 2 non multiple de 3.

Si l'on sait, à ce stade, montrer qu'une telle équation a des solutions, on ne peut encore les trouver. Le théorème suivant va nous y aider.

II Le théorème de Gauss

Tout d'abord une première propriété, application du théorème de Bézout et dans l'esprit du théorème de Gauss :

Proposition 1

Si un entier est premier avec deux entiers alors il est premier avec leur produit.

Preuve: Soit a un entier premier avec b et c.

D'après le théorème de Bézout, il existe deux entiers u et v tels que $au+bv=1$ et des entiers u' et v' tels que $au'+cv'=1$.

On effectue le produit membre à membre. On obtient :

$$\begin{aligned} & (au+bv)(au'+cv')=1 \\ \iff & a^2uu'+acuv'+abvu'+bcvv'=1 \\ \iff & a(auu'+cuv'+bvu')+bc(vv')=1. \end{aligned}$$

D'après le théorème de Bézout, a et bc sont bien premiers entre eux.

Exemple 3:

1/ 4 est premier avec 9 et avec 35, donc 4 est premier avec 315.

2/ Pour tout n, n est premier avec $n+1$ et $n-1$, donc n est premier avec $(n+1)(n-1)=n^2-1$.

II.1 Le théorème

ROC (Théorème de Gauss)

Soit a, b et c trois entiers relatifs non nuls.
Si a divise le produit bc et si a et b sont premiers entre eux alors a divise c.

$$\left\{\begin{array}{l} a|bc \\ a\wedge b=1 \end{array}\right. \implies a|c.$$

[Démonstration page 440 , **Maths Repère**, *Hachette*]

[Exercice 176 page 471 , **Maths Repère**, *Hachette*]

Preuve: Avec le théorème de Bézout, la démonstration est simple. On traduit l'énoncé et on observe :

- Comme $a|bc$, il existe $k\in\mathbb{Z}$ tel que $bc=ka$.

- Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$.
- En multipliant par c, on a :

$$acu + (bc)v = c \iff a(cu + kv) = c.$$

Donc a divise c.

Exemple 4: Soient a et b deux entiers tels que $5a = 14b$. 14 divise le produit $5a$, les entiers 14 et 5 sont premiers entre eux, donc 14 divise a.

De même, 5 divise b.

3 **Exercice** Trouver les solutions dans $\mathbb{Z}^2$ de l'équation : $5(x-1) = 7y$.

Correction: Nécessairement, 5 divise $7y$.

Or, $\text{pgcd}(5, 7) = 1$

D'après le théorème de Gauss 5 divise donc y et on peut écrire $y = 5k$ pour $k \in \mathbb{Z}$.

En remplaçant dans l'équation, on a :

$$5(x-1) = 7 \times 5k \iff x - 1 = 7k \iff x = 7k + 1.$$

Les solutions sont donc de la forme : $\begin{cases} x = 7k+1 \\ y = 5k \end{cases}$, $k \in \mathbb{Z}$.

II.2 Conséquences du théorème de Gauss

ROC

1/ Si un entier c est divisible par des entiers a et b premiers entre eux, alors il est divisible par leur produit ab.

2/ Si un entier premier divise un produit de facteurs ab, alors il divise au moins un des facteurs a et b.

Preuve:

1/ Il suffit d'appliquer le théorème (II.1) de Gauss :
Comme a divise c, il existe un entier k tel que $c = ka$.
D'où b divise $ka(= c)$ et premier avec a.
Il divise donc k d'après (II.1) et ab divise c.

2/ Soit p un nombre premier divisant ab.
Si p divise a, alors la condition est vérifiée.
Sinon, a et p sont premiers entre eux puisque p est un nombre premier. On applique (II.1) : comme p divise ab, il divise b.

[Exercice 146 page 467 , **Maths Repère**, *Hachette*]

Exemple 5: Si 5 et 12 divisent a, comme 5 et 12 sont premiers entre eux, $5 \times 12 = 60$ divise a.

Mais ATTENTION 6 et 4 divisent 12 sans que $6 \times 4 = 24$ ne divise 12. La condition de primalité est essentielle.

Revenons maintenant sur une propriété du chapitre précédent que nous n'avions pas encore pu démontrer :

Proposition 2

Soient a et b deux entiers naturels.

$$\text{ppcm}(a,b) \times \text{pgcd}(a,b) = ab.$$

Preuve: Tout d'abord, si a est nul et b non nul, l'égalité est vérifiée car $d = b$ et $m = 0$. De même pour $b = 0$ et $a \neq 0$. Supposons maintenant que a et b soient non nuls, posons $d = \text{pgcd}(a,b)$ et soient a' et b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$.

Soit μ un multiple commun de a et b (ie) $\exists (k,k') \in \mathbb{Z}^2$ / $\mu = ka$ et $\mu = k'b$
$= kda'$ $= k'db'$.

D'où, $kda' = k'db'$ et par simplification par $d \neq 0$,

$$ka' = k'b'.$$

Conséquence, a' divise $k'b'$.

Or, a' et b' sont premiers entre eux.

D'après le théorème de Gauss, $a'|k'$. Il existe ainsi un entier q tel que $k' = qa'$ (ie) $\mu = qda'b'$.

Ainsi, tout multiple commun μ à a et b est un multiple de $da'b'$.

Or, par définition, le plus petit de ces multiples est $\text{ppcm}(a,b)$ et l'égalité est atteinte pour $q = 1$ (ie) $\text{ppcm}(a,b) = da'b'$.

On alors $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = (da'b') \times d = (da') \times (db') = ab$.

[Exercices 168 à 173 page 470 , **Maths Repère**, *Hachette*]

III Exercices classiques

Résoudre une équation du type $ax + by = 0$ dans $\mathbb{Z}^2$.

Exemple 6: Déterminer les entiers x et y tels que $7x + 5y = 0$.

Cette équation s'écrit $7x = -5y$. 7 et -5 sont premiers entre eux. 7 divise $-5y$ donc 7 divise y d'après le théorème de Gauss. Ainsi $y = 7k$ avec k entier.

En reportant : $7x = -5 \times 7k$ d'où $x = -5k$.

Les solutions sont les couples $\begin{cases} x &= -5k \\ y &= 7k \end{cases}$ où $k \in \mathbb{Z}$.

Résoudre une équation du type $ax + by = c$ dans $\mathbb{Z}^2$, avec a et b premiers entre eux.

[Exercices 147 et 148 page 467 , **Maths Repère**, *Hachette*]

1/ Exemple 7: Déterminer les entiers x et y tels que $5x + 7y = 1$.

Comme 5 et 7 sont premiers entre eux, il existe d'après le théorème de Bézout deux nombres u et v tels que : $5u + 7v = 1$.

Pour déterminer u et v, on peut utiliser l'algorithme d'Euclide ou remarquer que

$$5 \times 10 - 7 \times 7 = 1.$$

On pourra alors prendre $u = 10$ et $v = -7$. Le couple $(10; -7)$ est une **solution particulière** de cette équation.

On va alors se servir de cette solution particulière pour obtenir la solution générale[1]. On se ramène à l'équation précédente que l'on sait résoudre en écrivant 1 d'une manière particulière :

$$1 = 5 \times 10 + 7 \times (-7).$$

Puis on insère, observe, ...

$$5x + 7y = 1 \iff 5x + 7y = 5 \times 10 + 7 \times (-7) \iff 5\underbrace{(x - 10)}_{X} + 7\underbrace{(y + 7)}_{Y} = 0.$$

Équation d'un type connu. On déroule la méthode :

5 divise $7(y + 7)$, 5 et 7 sont premiers entre eux. Donc 5 divise $y + 7$. Par conséquent : $y = -7 + 5k$, $k \in \mathbb{Z}$ puis, en reportant, $5(x - 10) = 7 \times 5k$ et $x = 10 + 7k$.

Les solutions sont de la forme $\begin{cases} x &= 10 + 7k \\ y &= -7 + 5k \end{cases}$, $k \in \mathbb{Z}$.

Remarque: Les solutions générales sont donc les points à coordonnées entières de la droite vectorielle passant par le point $A\begin{pmatrix} 10 \\ -7 \end{pmatrix}$ et de vecteur directeur $\vec{u}\begin{pmatrix} 7 \\ 5 \end{pmatrix}$.

1. C'est un procédé courant.

2/ Exemple 8: Déterminer les entiers x et y tels que $5x + 7y = 3$.

Condition nécessaire, $\text{pgcd}(5, 7) = 1$ divise 3. On applique alors le théorème de Bézout puis la même méthode :

Comme $5 \times 10 - 7 \times 7 = 1$ alors $5 \times 30 - 7 \times 21 = 3$ et $(30, -21)$ est une solution particulière de cette équation.

Les couples solutions sont $\begin{cases} x = 30 + 7k \\ y = -21 - 5k \end{cases}$, $k \in \mathbb{Z}$.

[Exercices 149 à 152 page 468 , **Maths Repère**, *Hachette*]

Montrer la divisibilité par un produit d'entiers.

Exemple 9: Montrer que $A = n(n + 1)(n + 2)$ est divisible par 6 pour tout n entier.

On sait depuis le chapitre sur la divisibilité que $n(n+1)$ est divisible par 2 et que $n(n+1)(n+2)$ est divisible par 3.

A est divisible par 2 et par 3, premiers entre eux, donc divisible par leur produit 6.

[Exercices 178 à 180 pages 471-472 , **Maths Repère**, *Hachette*]

Chapitre

5

Les nombres Premiers

Alors que leur définition semble ne receler aucun mystère, on échoue à trouver une régularité quelconque dans leur succession. Connus dès les débuts de l'arithmétique, les nombres premiers ont excité la curiosité de milliers de mathématiciens.

Ils sont au cœur de la science des nombres, car tout entier se décompose de façon unique en un produit de facteurs premiers. Ils sont aussi à l'origine de certains des problèmes les plus difficiles des mathématiques et ont acquis, avec les progrès de la cryptographie, une importance économique considérable.

La reconnaissance des nombres premiers et des nombres composés avec leur décomposition en facteurs premiers est connue pour être des plus importants et utiles en arithmétique.

Il a tant impliqué le zèle et la sagesse des géomètres anciens comme modernes qu'il serait superflu d'en discuter plus avant...

En plus, la dignité des sciences mêmes semble exiger que tous les moyens possibles soient explorés pour trouver la solution d'un problème si élégant et si célébré.

Karl Friedrich Gauss,

Disquisitiones Arithmeticae, 1801

Découvert le 25 janvier 2013, le plus grand nombre premier connu est le nombre premier de Mersenne $2^{57885161} - 1$, qui comporte 17 425 170 chiffres en écriture décimale. On le doit à l'équipe de Curtis Cooper (en), à l'université du Missouri Central (en), dans le cadre du projet Great Internet Mersenne Prime Search (GIMPS). Écrits les uns à la suite des autres, ses chiffres occuperaient plus de 4 000 pages en police Times New Roman taille 12.

Sommaire

I Définition et propriétés immédiates

Définition 1

Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Exemples 1:

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur).
- Un nombre premier p est un naturel supérieur ou égal à 2 soit : $p \geqslant 2$.
- Les nombres premiers inférieurs à 100 sont : 2, 3, 5, 7,11,13,17,19, 23,29, 31, 37,41,43,47,53, 59, 61, 67, 71, 73, 79, 83, 89 et 97
- Pour la culture, deux nombres premiers consécutifs comme 11 et 13, 17 et 19 ou 41 et 43 sont appelés *nombres jumeaux*.
- Une curiosité et un jeu des siècles passés, le polynôme $P(n) = n^2 - n + 41$ associé à Euler donne des nombres premiers pour n prenant les valeurs 0 à 39 mais $P(40) = 1681 = 41^2$!

[Exercice 190 page 472 , **Maths Repère**, *Hachette*]

Théorème 1 (Critère d'arrêt)

- Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.
- Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

Preuve:

- Si n est premier, il admet donc un diviseur premier : lui-même.
- Sinon, l'ensemble des diviseurs d de n tel que : $2 \leqslant d < n$ n'est pas vide (il contient 1). Il admet donc un plus petit élément p. Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leqslant d' < p$ qui diviserait n. Ceci contredirait la définition de p. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leqslant q$. En multipliant cette inégalité par p, on obtient :

$$p^2 \leqslant pq \implies p^2 \leqslant n \iff p \leqslant \sqrt{n}.$$

[Démonstration page 441 , **Maths Repère**, *Hachette*]

Exemple 2 (Comment montrer que 109 est un nombre premier):

- On a $10 < \sqrt{109} < 11$.
  On teste donc tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.
- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- Soit, on se rappelle le critère de divisibilité par 7 [1], soit on effectue la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4 \implies 109 \text{ n'est pas divisible par } 7.$$

- Conclusion : comme 109 n'est pas divisible par 2, 3, 5, et 7, il est premier.

[Exercice résolu 13 page 452
Exercice 184 page 472 , **Maths Repère**, *Hachette*]

Algorithme

Un petit programme (pas le plus efficace) pour déterminer si un nombre N est premier. N'ayant pas à notre disposition la liste des nombres premiers, on teste si N est divisible par 2, puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieur $\sqrt{N}$.

On obtient alors :

- 527 est divisible par 17.
- 719 est premier.
- 11111 est divisible par 41.
- 37 589 est premier.

```
1:  VARIABLES
2:  N EST_DU_TYPE ENTIER
3:  I EST_DU_TYPE ENTIER
4:  DEBUT_ALGORITHME
5:      Lire N
6:      I ⟵ 2
7:      SI E(N/I) = N/I ALORS
8:          DEBUT_SI
9:          Afficher « N est divisible par
    I ».
10:         FIN_SI
11:     I ⟵ I+1
12:     TANT_QUE I ⩽ √N FAIRE
13:         DEBUT_TANT_QUE
14:         SI E(N/I) = N/I ALORS
15:             DEBUT_SI
16:             Afficher « N est divisible par
    I ».
17:             FIN_SI
18:         I ⟵ I+2
19:         FIN_TANT_QUE
20:     AFFICHER N est premier.
21: FIN_ALGORITHME
```

1. Moi pas. Il est inutile de se rappeler des critères peu pratiques.

I.1 Infinité des nombres premiers

Théorème 11

Il existe une infinité de nombres premiers.

ROC

Supposons le contraire (*ie*) qu'il existe un nombre fini de nombres premiers que l'on va noter p_1, p_2, ..., P_n et posons

$$N = p_1 \times p_2 \times \ldots \times p_n + 1.$$

L'objectif de la cette démonstration[2] est de prouver que N est premier. Comme il est strictement plus grand que les p_i, on aura notre contradiction.
Si N est premier, la contradiction est déjà toute trouvée. Sinon, d'après le critère d'arrêt, N admet un diviseur premier. Soit p_i ce diviseur premier.
Par définition p_i divise donc $p_1 \times p_2 \times \ldots \times p_n$ et N donc divise aussi $N - p_1 \times p_2 \times \ldots \times p_n = 1$.
Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.

[Démonstration page 441 , **Maths Repère**, *Hachette*]

I.2 Crible d'Ératosthène

Pour dresser la liste des nombres premiers entre 2 et 150, la méthode du crible d'Ératosthène[3] consiste à :

1/ Écrire la liste des nombres entiers de 2 à 150.

2/ Éliminer successivement les multiples propres de 2, de 3, ..., puis ceux de p, où p est le premier nombre non encore éliminé[4], etc...

2. Connue d'Euclide himself !

3. Ératosthène, mathématicien, géographe, astronome et poète grec serait né en 276 avant J.C. à Cyrène (aujourd'hui en Libye). Il étudie quelques années à Athènes puis devient l'élève du poète grec Callimaque qui dirige la grande Bibliothèque d'Alexandrie.

Ayant ainsi accès à toutes les connaissances de l'époque, Ératosthène se lance dans différents travaux qui le rendront célèbre :

- En observant la position du Soleil à Syène (Assouan aujourd'hui) puis à Alexandrie au moment du solstice d'été, il parvient à déduire avec une bonne précision la circonférence de la Terre.
- Inventeur du mot géographie, il étudie les différentes zones climatiques, les altitudes des montagnes, la répartition des continents et des océans.
- Passionné d'astronomie, il réalise un catalogue de plus de 600 étoiles et 44 constellations. Il parvient aussi à calculer l'obliquité de l'écliptique (l'inclinaison de l'axe de la Terre par rapport à son axe de rotation autour du Soleil) avec une bonne précision.
- En mathématiques il invente un procédé (le crible d'Ératosthène) permettant de trouver les nombres premiers.

Devenu aveugle, Eratosthène se laisse mourir de faim en l'an 194 av. J-C.

4. donc premier

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~

Les entiers barrés sont les entiers non premiers entre 2 et 150. Les entiers restant (en rouge) sont donc les nombres premiers inférieur à 150.

Remarques:

- Pour éliminer les multiples propre de 7, commencer à 7^2, car les multiples inférieurs ont déjà été éliminés.
- D'après la **proposition** (I), il est possible de savoir à l'avance « jusqu'où aller ». En effet, tout entier composé n admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$.

  Si $n \leqslant 150$, alors $12 < \sqrt{n} < 13$. Il suffira donc de tester au plus pour tous les multiples de 12 [5] et de les barrer, le cas échéant.

Algorithme

- Les entiers A correspondent aux nombres premiers de la liste des entiers de 2 à N.
- Les entiers M correspondent aux multiples de A inférieurs à N.
- Les entiers P correspondent aux rangs des nombres premiers A.
- Les entiers Q correspondent au nombre de multiples de A inférieurs à N.
- La liste L_1 correspond à la liste des entiers de 2 à N.
- La Liste L_2 correspond à la liste des nombres premiers inférieurs à N.

À chaque fois que l'on trouve un nombre premier A, on le met dans la liste L_2 et l'on remplace tous les multiples de A dans la liste L_1 par un 0 [6].

On trouve le nombre premier suivant A, en prenant dans la liste L_1 le nombre suivant non nul.

5. Plutôt 11 car les multiples de 12 seront déjà barrés en tant que multiples de 2 ou de 3.
6. Cela revient à rayer tous ces multiples.

```
1: VARIABLES
2: N, I, A, M, P, Q EST_DU_TYPE ENTIER
3: L_1, L_2 EST_DU_TYPE LISTE
4: DEBUT_ALGORITHME
5:     Lire N
6:     Effacer liste L_1
7:     Effacer liste L_2
8:     POUR I ALLANT_DE 2 A N
9:         DEBUT_POUR
10:        L_1(I) ⟵ I
11:        FIN_POUR
12:    A ⟵ 2
13:    P ⟵ 0
14:    TANT_QUE A ⩽ N FAIRE
15:        DEBUT_TANT_QUE
16:        TANT_QUE L_1(A) = 0 FAIRE
17:            DEBUT_TANT_QUE
18:            A ⟵ A + 1
19:            FIN_TANT_QUE
20:        SI A ⩽ N ALORS
21:            DEBUT_SI
22:            P ⟵ P + 1
23:            L_2(P) ⟵ L_1(A)
24:            Q ⟵ E(N/A)
25:            FIN_SI
26:        POUR I ALLANT_DE 1 A Q
27:            DEBUT_POUR
28:            M ⟵ A × I
29:            L_1(M) ⟵ 0
30:            FIN_POUR
31:        FIN_TANT_QUE
32:    AFFICHER P, L_2.
33: FIN_ALGORITHME
```

I.3 Nombres de Mersenne

Définition 2 (Nombre de Mersenne [7])

On appelle **nombres de Mersenne**, les nombres M_n de la forme :

$$\forall n \in \mathbb{N}^*,\ M_n = 2^n - 1.$$

On a :

$$M_1 = 2 - 1 = 1 \qquad M_2 = 4 - 1 = 3$$
$$M_3 = 8 - 1 = 7 \qquad M_4 = 16 - 1 = 15$$
$$M_5 = 32 - 1 = 31 \qquad M_6 = 64 - 1 = 63$$

On remarque que M_2, M_3 et M_5 sont premiers, M_1, M_4 et M_6 ne le sont pas. De cette observation est née une conjecture :

$$n\,est\,premier \iff M_n\,est\,premier.$$

7. Marin Mersenne, connu également sous son patronyme latinisé Marinus Mersenius, né le **8 septembre 1588** à Oizé, mort le **1er septembre 1648** à Paris, est un religieux français appartenant à l'ordre des Minimes, érudit, mathématicien et philosophe. On lui doit les premières lois de l'acoustique, qui portèrent longtemps son nom1. Il établit concomitamment avec Galilée la loi de la chute des corps dans le vide. De Waard dit de lui qu'il était le secrétaire de l'Europe savante de son temps. Ecclésiastique érudit, à la culture encyclopédique et aux centres d'intérêt multiples, Marin Mersenne est une des figures les plus marquantes parmi les érudits de son temps.

Si celle-ci était vraie, cela permettrait de connaître un nombre premier aussi grand que l'on souhaite :

$$2 \text{ premier} \implies M_2 \text{ premier} \implies M_{M_2} \text{ premier} \implies M_{M_{M_2}} \text{ premier} \implies \dots$$

Actuellement, le plus grand nombre premier trouvé (nombre de Mersenne) est : $2^{57885161} - 1$ qui possède 17 425 170 chiffres !

Malheureusement cette conjecture est fausse dans un sens.

En effet si $n = 11$, premier donc, alors $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

M_{11} n'est donc pas premier alors que 11 l'est.

On peut cependant prouver que le sens direct est vrai en prouvant sa contraposée :

« Si n n'est pas premier alors M_n ne l'est pas non plus ».

Rappels !

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1).$$

Il suffit de développer le second membre et de simplifier ou de reconnaître dans le second membre, la somme des n premiers termes de la suite géométrique de premier terme 1 et de raison x.

Si n n'est pas premier, alors il existe d, diviseur propre de n tel que $n = dq$ avec $q > 1$.

D'où,

$$\begin{aligned} M_n &= 2^n - 1 = (2^d)^q - 1 \\ &= (2^d - 1)\Big((2^d)^{q-1} + (2^d)^{q-2} + \dots + 2^d + 1\Big). \end{aligned}$$

Donc $2^d - 1$ est un diviseur propre de M_n qui n'est donc pas premier.

Conclusion : Si n n'est pas premier alors M_n non plus et la contraposée :

Si M_n est premier alors n l'est également.

[Exercice résolu 14 page 452 , **Maths Repère**, *Hachette*]

II Divisibilité et nombres premiers

II.1 Théorème de Gauss et nombres premiers

Les résultats qui suivent ne sont que des reformulations du théorème de Gauss et de ses conséquences dans le cas particulier des nombres premiers. Les démonstrations étant évidentes, elles sont laissées à l'entraînement du lecteur.

Théorème III

Un nombre premier divise un produit de facteurs si, et seulement si il divise l'un de ces facteurs.

$$p \text{ premier tel que } p|ab \implies p|a \text{ ou } p|b.$$

En particulier, si p premier divise une puissance a^k alors, nécessairement, p divise a puis $p^k|a^k$.

Corollaire 1

- Si un nombre premier p divise un produit de facteurs premiers, alors p est l'un de ces facteurs premiers.
- Soit p_1, p_2, …, p_k des nombres premiers distincts et α_1, α_2, …, a_k des entiers naturels non nuls.

  Si, pour tout $i \in \{1, 2, \ldots, k\}$, $p_i^{\alpha_i}$ divise un entier n alors le produit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ divise aussi l'entier n.

[Exercices 197 et 198 page 474 , **Maths Repère**, *Hachette*]

II.2 Décomposition, diviseurs d'un entier

Théorème IV (Théorème fondamental de l'arithmétique)

Tout entier n$\geqslant 2$, peut se décomposer de façon unique en produit de facteurs premiers.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}, \quad \text{où } p_i \text{ est premier et } \alpha_i \in \mathbb{N}.$$

[Exercice résolu 15 page 453
Exercices 185 à 188 page 472 , **Maths Repère**, *Hachette*]

Exemple 3: Décomposons 16 758 en produit de facteurs premiers :

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

On obtient :

$$16758 = 2 \times 3^2 \times 7^2 \times 19.$$

Algorithme

En suivant la même idée, on peut donc proposer l'algorithme suivant pour chercher les facteurs premiers d'un entier $N \geqslant 2$:

- On teste si D est un diviseur de N en commençant par 2 puis les nombres impairs dans l'ordre croissant en appliquant le critère d'arrêt $D \leqslant \sqrt{N}$.
- On réinitialise N à chaque étape en prenant le quotient $\dfrac{N}{D}$.
- Le dernier nombre qui ne vérifie par le critère d'arrêt est alors premier et on le rajoute à la liste des diviseurs.

On peut tester la programme avec :

- $L_1(16758) = \{2, 3, 3, 7, 7, 19\}$.
- $L_1(87616) = \{2, 2, 2, 2, 2, 37, 37\}$.
- $L_1(77986545) = \{3, 5, 7, 13, 19, 31, 97\}$.

Remarque: On pourrait accélérer l'algorithme en remplaçant les variables D et C par une liste des premiers nombres premiers dans laquelle on irait puiser les valeurs de D.

```
1:  VARIABLES
2:  N, D, I, C EST_DU_TYPE ENTIER
3:  L1 EST_DU_TYPE LISTE
4:  DEBUT_ALGORITHME
5:      Lire N
6:      D ⟵ 2
7:      I ⟵ 1
8:      C ⟵ 1
9:      TANT_QUE D ⩽ √N FAIRE
10:         DEBUT_TANT_QUE
11:         SI E(N/D) = N/D ALORS
12:             DEBUT_SI
13:             L1(I) ⟵ D
14:             I ⟵ I + 1
15:             N ⟵ N/D
16:             FIN_SI
17:         SINON
18:             DEBUT_SINON
19:             D ⟵ D + C
20:             C ⟵ 2
21:             FIN_SINON
22:     FIN_TANT_QUE
23:     L1(I) ⟵ N
24:     AFFICHER L1.
25: FIN_ALGORITHME
```

1 **Exercice** Calculer pgcd(126; 735) et ppcm(126; 735)

Correction:

1/ On commence par décomposer les deux nombres :

126	2
63	3
21	3
7	7
1	

735	3
245	5
49	7
7	7
1	

On a donc :

$$126 = 2 \times 3^2 \times 7.$$

$$735 = 3 \times 5 \times 7^2.$$

2/ Par définition de $126 \wedge 735$ et $126 \vee 735$, on obtient :

$$\text{pgcd}(126; 735) = 3 \times 7 = 21 \quad \text{et} \quad \text{ppcm}(126; 735) = 2 \times 3^2 \times 5 \times 7^2 = 4410.$$

II.3 Diviseurs d'un entier

Théorème V

Soit un nombre $n \geqslant 2$ dont la décomposition en facteurs premiers est :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}.$$

Alors tout diviseurs d de n a pour décomposition :

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}, \quad \text{avec} \quad 0 \leqslant \beta_i \leqslant \alpha_i, \quad \forall i \in \{1, 2, \dots, m\}.$$

Le nombre de diviseurs $\varphi(n)$ est alors :

$$\varphi(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1).$$

[Exercice 189 page 472 , **Maths Repère**, *Hachette*]

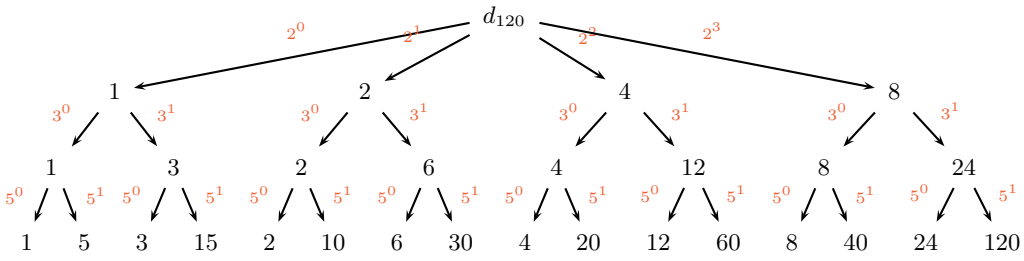
2 **Exercice** Trouver le nombre de diviseurs de 120 et déterminer tous ces diviseurs.

Correction:

- La décomposition de 120 en facteurs premiers est $120 = 2^3 \times 3 \times 5$.
  Donc $\varphi(120) = (3+1) \times (1+1) \times (1+1) = 4 \times 2 \times 2 = 16$.
  Il y a donc 16 diviseurs pour 120.
- Pour déterminer tous ces diviseurs, on peut utiliser un tableau double entrée en séparant les puissance de 2 et les puissance de 3 et 5.
  On obtient alors :

$\times$	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

- On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles :



- Les 16 diviseurs de 120 sont donc :

$$d_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}.$$

[Exercices 193 et 194 page 473 , **Maths Repère**, *Hachette*]

3 **Exercice** Un entier naturel n a 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Déterminer cet entier n.

Correction: On doit aborder ce genre d'exercice comme une chasse au trésor en lisant et utilisant **toutes** les informations de l'énoncé.

L'entier n a 15 diviseurs. D'après le **théorème** (V), il faut donc connaître toutes les décompositions de 15 en facteurs supérieurs à 1. Il n'y a que 2 décompositions soit en un seul facteur 15, soit en deux facteurs 3×5.

On sait que n est divisible par 6, il est donc divisible par 2 et par 3. Donc n admet 2 facteurs premiers. Comme 15 ne peut se décomposer en plus de 2 facteurs, alors n ne peut admettre que 2 facteurs premiers 2 et 3. On a donc :

$$n = 2^\alpha \times 3^\beta.$$

Comme $15 = 3 \times 5$, on a alors : $(1+\alpha)(1+\beta) = 3 \times 5$.

On trouve alors deux solutions : $\alpha = 2$ et $\beta = 4$ ou $\alpha = 4$ et $\beta = 2$.

On sait de plus que n n'est pas divisible par $8 = 2^3$, donc α est inférieur à 3.

Le nombre n cherché est donc :

$$n = 2^2 3^4 = 4 \times 81 = 324.$$

4 **Exercice** Déterminer le plus petit entier naturel possédant 28 diviseurs.

Correction: Posons n l'entier cherché.

Toujours d'après le **théorème** (V), on cherche d'abord toutes les décompositions de 28 en facteurs supérieurs à 1. On peut décomposer 28 en 1, 2 ou 3 facteurs :

$$28 \quad \text{ou} \quad 2 \times 14 \quad \text{ou} \quad 4 \times 7 \quad \text{ou} \quad 2 \times 2 \times 7.$$

1/ En 1 facteur :
Le plus petit entier n est alors $n = 2^\alpha$ avec $\alpha + 1 = 28$ soit $\alpha = 27$.
D'où, $n = 2^{27} = 134217728$.

2/ En deux facteurs : $28 = 2 \times 14$.
Le plus petit entier n est alors $n = 2^\alpha \times 3^\beta$ avec $\alpha + 1 = 14$ et $\beta + 1 = 2$.[8]
On a donc $\alpha = 13$ et $\beta = 1$.
D'où, $n = 2^{13} \times 3 = 24576$.

3/ En deux facteurs : $28 = 4 \times 7$.
Le plus petit entier n est alors $n = 2^\alpha \times 3^\beta$ avec $\alpha + 1 = 7$ et $\beta + 1 = 4$.
On trouve alors $\alpha = 6$ et $\beta = 3$.
D'où, $n = 2^6 \times 3^3 = 1728$.

4/ En trois facteurs : $28 = 2 \times 2 \times 7$.
Le plus petit entier n est alors $n = 2^\alpha \times 3^\beta \times 5^\gamma$ avec $\alpha + 1 = 7$, $\beta + 1 = 2$ et $\gamma + 1 = 2$.
On trouve alors $\alpha = 6$, $\beta = 1$ et $\gamma = 1$.
D'où $n = 2^6 \times 3 \times 5 = 960$.

Le plus petit entier naturel ayant 28 diviseurs est donc 960.

5

Exercice (Théorème d'Euclide)

Définition 3

On appelle **nombre parfait** un nombre dont la somme des diviseurs stricts est égal à lui-même.

1/ (Exemples) Euclide donne la règle suivante pour trouver des nombre parfait :

« Si un nombre a s'écrit $2^n(2^{n+1}-1)$ et si $2^{n+1}-1$ est premier, alors a est parfait ».

Trouver alors les quatre premiers nombres parfaits. (On ne demande pas de prouver la règle).

2/ (Démonstration) On pose $a = 2^n(2^{n+1}-1)$ et on suppose que $2^{n+1}-1$ est premier.

(a) Quelle est la décomposition de a en facteurs premiers ?

(b) En déduire la liste des diviseurs de a.

(c) Démontrer alors que la somme des diviseurs stricts de a est égale à ce nombre a.

Remarque: Le problème de savoir s'il existe des nombres parfaits impairs n'est toujours pas résolu.

[Exercices 220 et 221 page 483 , **Maths Repère**, *Hachette*]

III (Hors-programme) Petit théorème de Fermat

[Exercice 92 page 461 , **Maths Repère**, *Hachette*]

Théorème VI (Petit théorème de Fermat)

Soient p un nombre premier et $a \geqslant 2$ est un entier non multiple de p.
Alors $a^{p-1}-1$ est divisible par p (*ie*) $a^{p-1} \equiv 1\ [p]$.

Preuve: Remarquons tout d'abord que comme p est un nombre premier, p est donc premier avec 1, 2, ..., $p-1$ (sinon p admettrait un diviseur positif autre que 1). En particulier p est donc premier avec $(p-1)!$.

1/ Si k est un entier tel que $1 \leqslant k \leqslant p-1$, alors le reste r_k de la division de ka par p est non nul. En effet, d'après le théorème de Gauss, si p divise ka, alors p divise a car p est premier avec k ce qui contredit l'hypothèse initiale[9].

2/ Si k' est un entier distinct de k (par exemple $k < k'$) tel que $1 \leqslant k' \leqslant p-1$, alors les restes $r_{k'}$ et r_k des divisions respectives de $k'a$ et ka par p sont distincts.

En effet, si $r_{k'} = r_k$, alors p diviserait $k'a - ka = (k'-k)a$ avec $1 \leqslant k'-k \leqslant p-1$, ce qui est impossible toujours pour la même raison : a n'est pas divisible par p.

8. Le second cas avec $\alpha+1=2$ et $\beta+1=14$ donne un entier clairement plus grand d'après la stricte croissance des fonctions puissances $x \longmapsto x^\gamma$.

3/ Ainsi, les $p-1$ restes r_1, r_2,..., r_{p-1} des divisions respectives de a, $2a$, ..., $(p-1)a$ par p sont donc des entiers naturels non nuls, strictement inférieurs à p et tous distincts.

Nécessairement alors l'un de ces restes est égal à 1, l'autre à 2, ..., l'autre à $p-1$.

La multiplication étant compatible avec la relation de congruence, on a alors :

$$a \times 2a \times \ldots \times (p-1)a \equiv r_1 r_2 \ldots r_{p-1} \ [p].$$

(*ie*)

$$(p-1)! \times a^{p-1} \equiv (p-1)! \ [p].$$

Donc p divise $(p-1)!a^{p-1} - (p-1)! = (p-1)!\left(a^{p-1}-1\right)$.

Or, d'après le théorème de Gauss, comme p est premier avec $(p-1)!$, alors p divise $a^{p-1}-1$.

Exemple 4: 7 est premier et ne divise pas 3, donc $3^6 - 1$ est divisible par 7.

Mieux, par compatibilité de la relation de congruence avec les puissances, on obtient aussi :

$$\forall n \in \mathbb{N}, \quad 3^{6n} \equiv 1 \ [7]$$

Pour tout entier naturel n, $3^{6n}-1$ est divisible par 7.

Corollaire 1

Soient p un nombre premier, a est un entier supérieur ou égal à 2.
Alors $a^p - a$ est divisible par p (*ie*) $a^p \equiv a \ [p]$.

Preuve: On a $a^p - a = a(a^{p-1}-1)$.

Deux cas s'impose alors : soit a est divisible par p, soit pas.

1/ Si a est divisible par p, alors $a(a^{p-1}-1)$ est divisible par p.

2/ Si a n' est pas divisible par p, alors, d'après le **théorème** (VI), $a^{p-1}-1$ est divisible par p et donc $a(a^{p-l}-1)$ est divisible par p.

6 **Exercice (Nombre de Poulet)**

Définition 4

On appelle **nombre de Poulet** (**1886-1946**) [10], un entier n, non premier, tel que : $2^{n-1} \equiv 1 \ [n]$.

Soit un entier $n \geqslant 1$ un nombre impair tel que $2^{n-1} \not\equiv 1 \ [n]$.

9. a n'est pas un multiple de p.

1/ Montrer que n n'est pas premier.

2/ Prouver que $2^{340} \equiv 1\ [341]$, mais que 341 n'est pas premier.

3/ Conclure.

Correction:

1/ Montrons plutôt la contraposée de la proposition (*ie*)

$$\text{« Si } n \text{ est premier impair alors } 2^{n-1} \equiv 1\ [n]. \text{ »}$$

Cela devient alors très simple. Comme n est premier et impair, alors 2 n'est pas un multiple de n et d'après **théorème** (VI), on a :

$$2^{n-1} \equiv 1\ [n].$$

La contraposée est donc vérifiée.

2/ Tout d'abord $341 = 11 \times 31$ donc 341 n'est pas un nombre premier.
La suite est un peu plus subtile comme tous les problèmes d'arithmétique. On suit son instinct :

$$2^{340} = \left(2^{10}\right)^{34}.$$

On cherche alors un lien entre $2^{10} = 1024$ et 341 :

$$1024 = 341 \times 3 + 1.$$

Le reste égal à 1 nous sauve :

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1^{34} \equiv 1\ [341].$$

La conclusion de cette question est que la réciproque de la contraposée est fausse (*ie*) « On peut trouver des entiers n non premiers tels que $2^{n-1} \equiv 1\ [n]$. »

3/ Le nombre 341 est un nombre de Poulet.

[Exercices 206 à 217 pages 477 à 480 , **Maths Repère**, *Hachette*]

10. Un test de primalité courant pour un nombre impair n consiste à tester si n divise $2^{n-1} - 1$: dans le cas contraire, en vertu de la contraposée du petit théorème de Fermat, on conclut que n n'est pas premier.

Cependant il existe des nombres composés qui passent ce test avec succès : on les appelle **nombres de Sarrus** ou **nombres de Poulet**, en l'honneur de Paul Poulet qui en a listés en 1926.

Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

$\text{ppcm}(a,b)$ est le plus petit multiple de a et b.

Toute suite dans $\mathbb{N}$ strictement décroissante est stationnaire au bout d'un certain rang.

$$\forall (a\ ;\ b) \in \mathbb{Z}^* \times \mathbb{Z},\ b|a \iff \exists k \in \mathbb{Z}\ /\ a = kb$$
$$\iff \text{Le reste de la division de } a \text{ par } b \text{ est nul.}$$
$$\iff a \equiv 0\ [b].$$

$$d|n \implies 1 \leqslant d \leqslant n.$$

$$a|b \text{ et } a|c \implies a|mb+nc$$

Division euclidienne dans $\mathbb{Z}$:

$$\forall (a\ ;\ b) \in \mathbb{Z} \times \mathbb{N}^*,\ \exists !\,(q\ ;\ r) \in \mathbb{Z}^2\ /\ a = bq + r \quad \text{et } 0 \leqslant r < |b|.$$

$d = \text{pgcd}\,(a\ ;\ b)$ = le plus grand diviseur commun à a et à b.

$\|$ = le dernier reste non nul dans l'algorithme d'Euclide.

$a \wedge b$ $\iff \exists\,(u\ ;\ v) \in \mathbb{Z}^2\ /\ au + bv = d.$

$$\iff \exists\,(a'\ ;\ b') \text{ unique } /\ \begin{cases} a = da' \\ b = db' \end{cases} \text{ et } a' \wedge b' = 1.$$

$$a = bq + r \implies \text{pgcd}(a,b) = \text{pgcd}(b,r).$$

$$d|a \text{ et } d|b \iff d|\,\text{pgcd}(a,b).$$
$$a|m \text{ et } b|m \iff \text{ppcm}(a,b)|m.$$

$$\text{pgcd}(ka,kb) = k \times \text{pgcd}(a,b).$$
$$\text{ppcm}(ka,kb) = k \times \text{ppcm}(a,b).$$

$$\text{ppcm}(a,b) \times \text{pgcd}(a,b) = |ab|\,.$$

Congruences modulo n :

$a \equiv b\ [n] \iff a$ et b ont même reste dans la division euclidienne par n.
$\iff n|b-a$
$\iff$ si $0 \leqslant b < n$, b est le reste de la division euclidienne de a par n.
$\iff pa+q \equiv pb+q\ [n]$.

a et b sont premiers entre eux $\iff \mathcal{D}iv(a) \cap \mathcal{D}iv(b) = \{1\}.$
$\iff \text{pgcd}(a,b) = 1$

$au \equiv 1\ [b] (ie)$ modulo b, a est inversible d'inverse u modulo b. $\iff$ $\exists\,(u\ ;\ v) \in \mathbb{Z}^2\ /\ au + bv = 1.$ (Égalité de Bézout)

$$\begin{aligned} 3920 &= 1089 \times 3 + 653 \\ 1089 &= 653 \times 1 + 436 \\ 653 &= 436 \times 1 + 217 \\ 436 &= 217 \times 2 + 2 \\ 217 &= 2 \times 108 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= \mathbf{3920} \times 542 - \mathbf{1089} \times 1951 \\ 1 &= 653 \times 217 - (1089 - 653) \times 235 \\ 1 &= (653 - 436 \times 1) \times 217 - 436 \times 108 \\ 1 &= 217 - (436 - 217 \times 2) \times 108 \\ 1 &= 217 - 2 \times 108 \end{aligned}$$

Th. de Gauss : $a|bc$ et $a \wedge b = 1 \implies a|c.$

$$\begin{cases} a|c \text{ et } b|c \\ a \wedge b = 1 \end{cases} \implies ab|c.$$

$$p|ab \text{ et } p \text{ premier} \implies p|a \text{ ou } p|b.$$
$$a \wedge c = 1 \text{ et } b \wedge c = 1 \implies c \wedge ab = 1.$$

Équation diophantienne :

$ax + by = c$ admet des solutions entières $\iff \text{pgcd}(a, b)|c$

p premier $\iff$ p admet exactement deux diviseurs

p premier $\implies$ p premier avec tous les nombres qu'il ne divise pas.

Tout entier naturel $n \geqslant 2$, admet un diviseur premier.

n pas premier $\implies$ il existe un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

Il existe une infinité de nombres premiers.
(Crible d'Ératosthène pour les trouver)

Th. Fondamental : $\forall n \in \mathbb{Z},\ n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$
(p_i premier)

$d|n \implies p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$,
avec $0 \leqslant \beta_i \leqslant \alpha_i,\ \forall i \in \{1, 2, \dots, m\}$.

Nombre de diviseurs de n :

$\varphi(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$.

Un nombre $\overline{a_n a_{n-1} \dots a_k \dots a_1 a_0}$ est divisible par ...

2 ssi $2|\overline{a_0}$.

3 ssi $3|a_0 + a_1 + a_2 + \dots + a_n$.

4 ssi $4|\overline{a_1 a_0}$.

5 ssi $5|\overline{a_0}$.

9 ssi $9|a_0 + a_1 + a_2 + \dots + a_n$.

11 ssi $11|a_0 - a_1 + a_2 \pm \dots + (-1)^k a_k + \dots + (-1)^n a_n$.

Chapitre

6

Matrices

Le but de ce chapitre est de résoudre quelques problèmes liés à des variables discrète par l'intermédiaire d'un nouvel outil que constituent les **matrices**. Il s'agit de mettre en évidence la pertinence d'introduire des matrices pour résoudre quelques problèmes concrets.

Extrait du programme : *Il s'agit d'étudier des exemples de processus discrets, déterministes ou stochastiques, à l'aide de suites ou de matrices. On introduit le calcul matriciel sur des matrices d'ordre 2. Les calculs sur des matrices d'ordre 3 ou plus sont essentiellement effectués à l'aide d'une calculatrice ou d'un logiciel.*

Sommaire

I L'ensemble des matrices

I.1 Généralités et vocabulaire

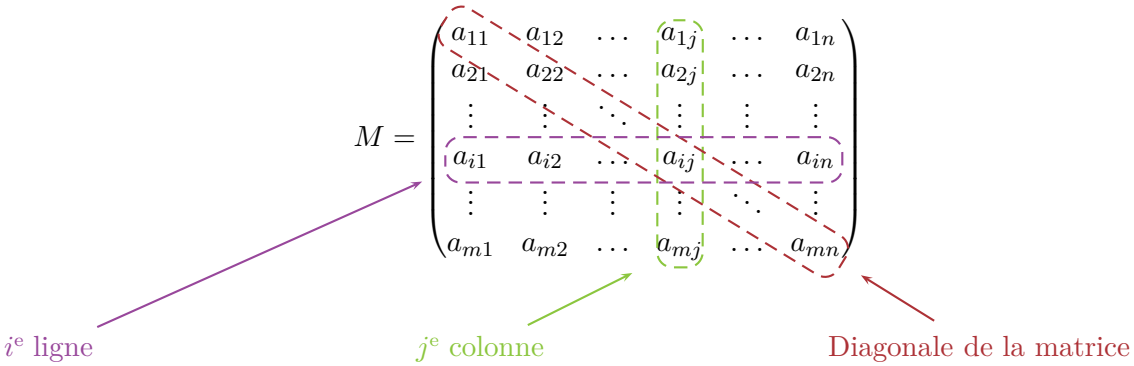
Définition 1

Une matrice M est un tableau de nombres possédant m lignes et n colonnes. On écrit alors :

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix}$$

- Les nombres a_{ij} sont les éléments ou coefficients de la matrice M.
- a_{ij} est situé à l'intersection de la i^{e} ligne et de la j^{e} colonne.

On notera souvent, en abrégé, $M = (a_{ij})$.



En mathématiques, l'ensemble des matrices est noté $\mathscr{M}_{mn}(\mathbb{R})$ où m et n sont, réciproquement, le nombre de lignes et de colonnes et $\mathbb{R}$ est le corps auquel appartiennent les coefficients.

Exemple 1: $A = \begin{pmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{pmatrix}$ est une matrice 2×3.

Par exemple, $a_{21} = 4$ et $a_{13} = 0$.

[Exercice 29 page 28 , **Maths Repère**, *Hachette*]

Une matrice M est donc entièrement déterminée par la donnée de $m \times n$ nombres réels qui la déterminent ce qui implique notamment que :

$$\boxed{A = 0 \iff \forall\, i, j,\ a_{ij} = 0 \quad \text{et} \quad \big(a_{ij}\big) = \big(b_{ij}\big) \iff \forall\, i, j,\ a_{ij} = b_{ij}.}$$

Une matrice est nulle si, et seulement si ses coefficients sont tous nuls et deux matrices sont égales si, et seulement si leurs coefficient sont égaux deux à deux.

Exemple 2: On peut regrouper les effectifs des classes de terminales de deux lycées pour l'année 2015 répartis suivant les filières.

	S	ES	L	STMG	ST2S
Lycée M	45	63	22	58	54
Lycée W	29	12	5	42	26

En supprimant les lignes et colonnes de titres et ne gardant que les valeurs numériques, on peut alors créer une matrice élève E dont les lignes correspondent aux lycée et les colonnes aux différentes filières. La matrice E est alors une matrice 2×5 :

$$E = \begin{pmatrix} 45 & 63 & 22 & 58 & 54 \\ 29 & 12 & 5 & 42 & 26 \end{pmatrix}$$

[Situation page 492 , **Maths Repère**, *Hachette*]

I.2 Quelques matrices particulières

- Si $m = 1$, la matrice M est appelée matrice ou vecteur ligne.
$$M = \begin{pmatrix} 1 & 5 & 8 \end{pmatrix} \in \mathscr{M}_{10}(\mathbb{R}).$$

- Si $n = 1$, la matrice M est appelée matrice ou vecteur colonne.
$$M = \begin{pmatrix} 1 \\ 3 \\ -4 \end{pmatrix} \in \mathscr{M}_{01}(\mathbb{R}).$$

- Si $m = n$, la matrice M est appelée **matrice carrée** d'ordre n.
$$M = \begin{pmatrix} 4 & 5 \\ 3 & -2 \end{pmatrix} \in \mathscr{M}_{2}(\mathbb{R}).$$

- Une matrice carrée est **symétrique** si, et seulement si $a_{ij} = a_{ji}$, $\forall\, i \neq j$.
$$M = \begin{pmatrix} 4 & -1 \\ -1 & 4 \end{pmatrix}$$

- On définit la **matrice unité** I_n d'ordre n par la matrice carrée d'ordre n qui ne possède que des « 1 » sur sa diagonale et des « 0 » ailleurs : $a_{ii} = 1$ et $a_{ij} = 0$, $\forall\, i \neq j$.
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- On définit une **matrice diagonale** d'ordre n par la matrice carrée d'ordre n qui ne possède des éléments non nuls que sur sa diagonale : $a_{ij} = 0, \forall\, i \neq j$.

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

- On définit une **matrice triangulaire** d'ordre n par une matrice carrée d'ordre n qui possède un triangle composé uniquement de « 0 » strictement sous la diagonale : $a_{ij} = 0$, $\forall i < j$ est une matrice triangulaire inférieure.

$$T_1 = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 5 & 0 \\ 2 & 5 & 7 \end{pmatrix}$$

Matrice triangulaire inférieure

$$T_2 = \begin{pmatrix} 1 & 4 & 5 \\ 0 & -5 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

Matrice triangulaire supérieure

$$T = \begin{pmatrix} 0 & 0 & 0 \\ 3 & 0 & 0 \\ 7 & -1 & 0 \end{pmatrix}$$

Matrice strictement triangulaire

I.3 Opérations sur les matrices

Comme pour les nombres complexes, un nouvelle ensemble créé, il est nécessaire, afin d'en faire quelque chose, de définir les lois qui régissent ses éléments. On dit que l'on dote l'ensemble $\mathscr{M}_{mn}(\mathbb{K})$ d'une structure de groupe, d'anneau ou de $\mathbb{K}$-algèbre suivant les cas.

I.4 Addition

Définition 2

Soient A et B deux matrices de **même** dimension.
La matrice $C = A + B$ est la matrice dont les coefficients sont les sommes des coefficients de A et B. On note :

$$C = A + B \iff (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}).$$

Difficile de faire plus simple !

De même que l'addition dans $\mathbb{R}$ [1], l'addition des matrices vérifient les mêmes lois : associativité, commutativité, élément neutre et opposé. On dit que l'ensemble $\left(\mathscr{M}_{mn}(\mathbb{K});+\right)$ est un groupe commutatif.

ATTENTION Les matrices doivent avoir les mêmes dimensions sinon leur addition n'est pas définie.

Exemples 3:

- $\begin{pmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{pmatrix} - \begin{pmatrix} -5 & 2 & 3 \\ 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 0 & -3 \\ 3 & 1 & -5 \end{pmatrix}$.

1. ou $\mathbb{C}$.

- $\begin{pmatrix} 1 & 2 \\ 4 & 3 \\ -5 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 4 & 3 \\ -5 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 4 & 3 \\ -5 & -1 \end{pmatrix}$.

  Remarque: On dit que la matrice nulle (0) est l'élément neutre pour l'addition.

- $\begin{pmatrix} 1 & 2 & -4 \\ 4 & 3 & -1 \\ 5 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 0 \\ 5 & 0 & -3 \end{pmatrix} + \begin{pmatrix} 0 & 2 & -4 \\ 0 & 1 & -1 \\ 0 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 2 & -4 \\ 0 & 1 & -1 \\ 0 & 0 & 5 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 0 \\ 5 & 0 & -3 \end{pmatrix}$.

  On peut décomposer une matrice carrée en deux matrices triangulaires.

I.5 Loi externe

Définition 3 (Multiplication par un scalaire)

Le produit de la matrice $A = (a_{ij})$ par un scalaire λ, est égal à la matrice dont chaque coefficient est obtenu en multipliant chaque coefficient de la matrice A par λ. On note :

$$\lambda.(a_{ij}) = (\lambda \times a_{ij}).$$

Remarque: Le terme de scalaire fait référence à un élément de $\mathbb{R}$ ou de $\mathbb{C}$ que l'on notera indistinctement $\mathbb{K}$.

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

Cette opération ne pose donc aucun problème. Les deux opérations précédentes sont identiques à celles utilisées dans l'ensemble des vecteurs. On dit que l'ensemble $\left(\mathscr{M}_{mn}(\mathbb{K});\ +;\ .\right)$, comme celui des vecteurs, est un $\mathbb{K}$-espace vectoriel.

I.6 Transposition d'une matrice

Définition 4

La transposée d'une matrice $M \in \mathscr{M}_{mn}$ est la matrice, notée ${}^tM$, obtenue en échangeant les lignes et les colonnes de la matrice M.

$${}^tM = (a_{ji}) \in \mathscr{M}_{nm}.$$

Exemple 5: Si $M = \begin{pmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{pmatrix}$ alors ${}^tM = \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 0 & -1 \end{pmatrix}$.

Remarques:

- La transposée d'un vecteur colonne est un vecteur ligne et réciproquement :

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

- Une matrice carré M est symétrique si, et seulement si ${}^tM = M$.

I.7 Produit de deux matrices

C'est là que les choses deviennent intéressantes. Comme je vous l'ai déjà dit, il est rare, voire exceptionnel qu'un objet se comporte bien avec nos deux opérations principales. Comme l'addition de deux matrices est simple ...

On commence doucement :

Définition 5 (Produit d'un vecteur ligne par un vecteur colonne)

Le produit d'un vecteur ligne par un vecteur colonne est égal au produit scalaire des deux vecteurs considérés comme deux vecteurs colonnes.

$$ \begin{pmatrix}a_1 & a_2 & \dots & a_n\end{pmatrix} \times \begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix} = a_1b_1 + a_2b_2 + \dots a_nb_n = \sum_{k=1}^{n} a_kb_k. $$

ATTENTION On ne parle pas (encore) du produit d'un vecteur colonne par un vecteur ligne.

On généralise cette opération à deux matrices quelconques A et B pourvu que le nombre de colonnes de la matrice A correspondent au nombre de lignes de la matrice B.

Définition 6

Le produit de la matrice $A \in \mathscr{M}_{mn}$ par la matrice $B \in \mathscr{M}_{np}$ est égal à la matrice $C = (c_{ij}) \in \mathscr{M}_{mp}$ dont chaque coefficient c_{ij} est égal au produit scalaire de la ligne i de la matrice A par la colonne j de la matrice B.

$$ c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}. $$

$$ \begin{pmatrix}a_{11} & a_{12} & \dots & a_{1n}\\a_{21} & a_{22} & \dots & a_{2n}\\\vdots & \vdots & \ddots & \vdots\\a_{i1} & a_{i2} & \dots & a_{in}\\\vdots & \vdots & \vdots & \vdots\\a_{m1} & a_{m2} & \dots & a_{mn}\end{pmatrix} \times \begin{pmatrix}b_{11} & b_{12} & \dots & b_{1j} & \dots & b_{1p}\\b_{21} & b_{22} & \dots & b_{2j} & \dots & b_{2p}\\\vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\b_{n1} & b_{n2} & \dots & b_{nj} & \dots & b_{np}\end{pmatrix} = \begin{pmatrix}c_{11} & c_{12} & \dots & c_{1j} & \dots & c_{1p}\\c_{21} & c_{22} & \dots & c_{2j} & \dots & c_{2p}\\\vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\c_{i1} & c_{i2} & \dots & c_{ij} & \dots & c_{ip}\\\vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\c_{m1} & c_{m2} & \dots & c_{mj} & \dots & c_{mp}\end{pmatrix} $$

[Exercice 66 page 517 , **Maths Repère**, *Hachette*]

Exemple 6: Reprenons la matrice élève E de l'**exemple** (2).

Si l'on regroupe les taux de réussite par filière dans une matrice colonne $R = \begin{pmatrix} 0,72 \\ 0,56 \\ 0,62 \\ 0,44 \\ 0,47 \end{pmatrix}$, le produit $E \times R$ est une matrice colonne 2×1 dont chaque ligne représente le nombre d'élèves qui ont réussi.

$$E = \begin{pmatrix} 45 & 63 & 22 & 58 & 54 \\ 29 & 12 & 5 & 42 & 26 \end{pmatrix} \times \begin{pmatrix} 0,72 \\ 0,56 \\ 0,62 \\ 0,44 \\ 0,47 \end{pmatrix} \simeq \begin{pmatrix} 132 \\ 61 \end{pmatrix}.$$

où, par exemple, $132 \simeq 45 \times 0,72 + 63 \times 0,56 + 22 \times 0,62 + 58 \times 0,44 + 54 \times 0,47$

[Situation page 494 , **Maths Repère**, *Hachette*]

ATTENTION Le produit de matrices n'est pas commutatif en général.

En effet, il se peut que AB soit défini mais pas BA, ou que AB et BA soient tous deux définis mais pas de la même taille.

Mais, même dans le cas où AB et BA sont définis et de la même taille, on a, en général, $AB \neq BA$. Les exemples suivants sont à retenir afin d'éviter d'écrire des bourdes.

Exemple 7 ($AB \neq BA$):

$$\begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 14 & 3 \\ 2 & -6 \end{pmatrix} \quad \text{mais} \quad \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 10 & 2 \\ 29 & -2 \end{pmatrix}.$$

Exemple 8 ($AB = 0$ n'implique pas $A = 0$ ou $B = 0$): Il peut arriver que le produit de deux matrices non nulles soit nul. En d'autres termes, on peut avoir $A \neq 0$ et $B \neq 0$ mais $AB = 0$. Les matrices A et B sont alors appelées des **diviseurs de zéros**.

$$A = \begin{pmatrix} 0 & -1 \\ 0 & 5 \end{pmatrix} \quad B = \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exemple 9 ($AB = AC$ n'implique pas $B = C$): On peut avoir $AB = AC$ et $B \neq C$.

$$A = \begin{pmatrix} 0 & -1 \\ 0 & 3 \end{pmatrix} \quad B = \begin{pmatrix} 4 & -1 \\ 5 & 4 \end{pmatrix} \quad C = \begin{pmatrix} 2 & 5 \\ 5 & 4 \end{pmatrix} \quad \text{et} \quad AB = AC = \begin{pmatrix} -5 & -4 \\ 15 & 12 \end{pmatrix}.$$

[Exercice 48 516 , **Maths Repère**, *Hachette*]

Vous verrez par la suite que nombre de ces difficultés n'existeraient pas si l'inverse d'une matrice non nulle pouvait toujours être défini.

Alors que reste-t-il au final ? Ce qui est indiqué dans la proposition est seulement cela :

Proposition 1 (Propriété algébrique de la multiplication)

Le produit de deux matrices est :

- associatif : $A \times (B \times C) = (A \times B) \times C = ABC$.
- distributif sur l'addition : $A \times (B + C) = A \times B + A \times C$.
- non commutatif : $A \times B \neq B \times A$ en général.
- Si A est une matrice carrée d'ordre n alors $A \times I_n = I_n \times A = A$.
  On dit que I_n est l'élément neutre pour la multiplication des matrices carrées.

1 **Exercice** Effectuer le produit des matrices :

1/ $\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$

2/ $\begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 4 \end{pmatrix} \times \begin{pmatrix} -1 & -1 & 0 \\ 1 & 4 & -1 \\ 2 & 1 & 2 \end{pmatrix}$

3/ $\begin{pmatrix} a & b & c \\ c & b & a \\ 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a & c \\ 1 & b & b \\ 1 & c & a \end{pmatrix}$

2 **Exercice** On considère les trois matrices suivantes :

$$A = \begin{pmatrix} 2 & -3 & 1 & 0 \\ 5 & 4 & 1 & 3 \\ 6 & -2 & -1 & 7 \end{pmatrix} \quad B = \begin{pmatrix} 7 & 2 \\ -5 & 2 \\ 3 & 1 \\ 6 & 0 \end{pmatrix} \text{ et } \quad C = \begin{pmatrix} -1 & 2 & 6 \\ 3 & 5 & 7 \end{pmatrix}.$$

1/ Calculer AB puis $(AB)C$. **2/** Calculer BC puid $A(BC)$. **3/** Que remarque-t-on ?

3 **Exercice** On considère les deux matrices suivantes :

$$A = \begin{pmatrix} 2 & 3 & -4 & 1 \\ 5 & 2 & 1 & 0 \\ 3 & 1 & -6 & 7 \\ 2 & 4 & 0 & 1 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 3 & -1 & -3 & 7 \\ 4 & 0 & 2 & 1 \\ 2 & 3 & 0 & -5 \\ 1 & 6 & 6 & 1 \end{pmatrix}.$$

1/ Calculer AB. **2/** Calculer BA. **3/** Que remarque-t-on ?

4 **Exercice** Trouver les matrices qui commutent avec $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$.

I.8 Puissance n-ième d'une matrice carrée

Définition 7

On appelle puissance n-ième d'une matrice carrée A, la matrice, notée A^n telle que :

$$A^n = \underbrace{A \times A \times \ldots \times A}_{n\ fois}.$$

Exemple 10: Soit $A = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$.

$$A^2 = A \times A = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 3 & 6 \end{pmatrix}.$$

$$A^3 = A \times (A \times A) = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \times \begin{pmatrix} 7 & 2 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 13 & 14 \\ 21 & 6 \end{pmatrix}.$$

Remarque: Vos calculatrices savent très bien faire tous ces calculs. Une fois la théorie comprise, il est bon de les laisser se charger des calculs. La matrice rentrée dans la calculatrice est vue par celle-ci comme un nombre quelconque et vous pourrez utiliser les touches « puissances » et « inverse » comme avec eux.

5 **Exercice** On considère la matrice suivante :

$$M = \begin{pmatrix} 0 & a & b & c \\ 0 & 0 & d & e \\ 0 & 0 & 0 & f \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Calculer M^2, M^3, M^4, M^5.

[Exercices 60 et 61 page 517 , **Maths Repère**, *Hachette*]

Théorème 1 (Binôme de Newton)

Soient A et B deux matrices carrées d'ordre p qui **commutent**. Pour tout entier $n \in \mathbb{N}$, on a :

$$\left(A + B\right)^n = \sum_{k=0}^{n} \binom{n}{k} A^k \times B^{n-k}.$$

ATTENTION Si A et B ne commutent pas (ie) $AB \neq BA$ alors

$$\begin{aligned} (A+B)^2 &= (A+B)(A+B) \\ &= A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2 ! \ldots \end{aligned}$$

Preuve: Montrons ce résultat par récurrence sur $n \in \mathbb{N}$.

- Pour $n = 1$, il n'y a rien à montrer.
- Supposons le résultat vérifié pour un certains $m \in \mathbb{N}$ (ie) $\left(A+B\right)^m = \sum_{k=0}^{m} \binom{m}{k} A^k \times B^{m-k}$.

  Alors :

$$\left(A+B\right)^{m+1} = \left(A+B\right)^m \left(A+B\right) = \left(\sum_{k=0}^{m} \binom{m}{k} A^k \times B^{m-k}\right)\left(A+B\right)$$
$$= \sum_{k=0}^{m} \binom{m}{k} A^k \times B^{m-k} A + \sum_{k=0}^{m} \binom{m}{k} A^k \times B^{m-k+1}$$

  Comme A et B commutent, $A^k \times B^{m-k} A = A^{k+1} \times B^{m-k}$

$$= \sum_{k=0}^{m} \binom{m}{k} A^{k+1} \times B^{m-k} + \sum_{k=0}^{m} \binom{m}{k} A^k \times B^{m-k+1}$$
$$= A^{m+1} + \sum_{k=0}^{m-1} \binom{m}{k} A^{k+1} \times B^{m-k} + \sum_{k=1}^{m} \binom{m}{k} A^k \times B^{m-k+1} + B^{m+1}$$
$$= A^{m+1} + \sum_{k=1}^{m} \binom{m}{k-1} A^k \times B^{m-k+1} + \sum_{k=1}^{m} \binom{m}{k} A^k \times B^{m-k+1} + B^{m+1}$$
$$= A^{m+1} + \sum_{k=1}^{m} \binom{m}{k-1} A^k \times B^{m-k+1} + \binom{m}{k} A^k \times B^{m-k+1} + B^{m+1}$$
$$= A^{m+1} + \sum_{k=1}^{m} \underbrace{\left[\binom{m}{k-1} + \binom{m}{k}\right]}_{\binom{m+1}{k}} A^k \times B^{m-k+1} + B^{m+1}$$
$$= \sum_{k=0}^{m+1} \binom{m+1}{k} A^k \times B^{(m+1)-k}.$$

  Le résultat est donc vrai à l'ordre $m+1$ (ie) la propriété est héréditaire.
- La propriété est donc vraie à l'ordre 1 et héréditaire. Elle est donc vraie pour tout $n \in \mathbb{N}$.

Ce théorème est particulièrement intéressant dans le cas des matrices N nilpotentes à partir d'un certain rang (ie) telles qu'il existe un entier n_0 vérifiant $N^{n_0} = 0_{\mathscr{M}_{mn}}$.

6

Exercice (Calcul de A^n par la formule du binôme) Soit $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

1/ On pose $J = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Calculer J^n, $n \in \mathbb{Z}$.

2/ En écrivant $A = I_3 + J$, calculer A^n, $n \in \mathbb{Z}$.

Exercice résolu 3 page 508
Exercices 108 et 109 page 524 , **Maths Repère**, *Hachette*

On peut effectuer les calculs avec une calculatrice pour des matrices de petite taille et des puissances raisonnables ou utiliser un logiciel dans le cas de matrices plus grosses mais on essaiera le plus souvent de trouver des relations de récurrence sur les coefficients afin d'obtenir des formules « closes », donnant l'expression des coefficients en fonction de l'exposant. Ce sera le cadre du paragraphe III.2 que nous allons d'abord motiver.

II Systèmes linéaires et matrices

[Situation page 496 , **Maths Repère**, *Hachette*]

II.1 Écriture matricielle d'un système linéaire

Définition 8 (Système linéaire)

On appelle système linéaire à m équations et n inconnues $x_1, x_2, \dots x_n$ tout système $(\mathcal{S})$ de la forme :

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \dots & + & \dots & + & \dots & + & \dots & = & \dots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{2m}x_n & = & b_m \end{cases}$$

On pose $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{2m} \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ et $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$.

Le système $(\mathcal{S})$ s'écrit alors sous la forme matricielle :

$$(\mathcal{S}) : \ AX = B.$$

Exemple 11: Le système $\begin{cases} 2x & - & 3y & = & 5 \\ 5x & - & 4y & = & 1 \end{cases}$ s'écrit sous la forme matricielle :

$$\begin{pmatrix} 2 & -3 \\ 5 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}.$$

[Exercice 70 page 519 , **Maths Repère**, *Hachette*]

Un système linéaire n'est donc qu'une grosse équation de la forme $ax = b$ que nous connaissons bien. Dans $\mathbb{R}$[2], il suffit de multiplier les deux membres par l'inverse de a noté $a^{-1} = \dfrac{1}{a}$ et le tour est joué : $x = a^{-1}b$.

Pourquoi ne pas faire pareil dans $\mathscr{M}_{mn}$ et considérer quelque chose que l'on nommerait A^{-1} ? Et bien tout simplement pour deux raisons :

1/ La première c'est que le produit n'est pas commutatif comme on l'a déjà vu. Alors devrait-on considérer $A^{-1}B$ ou BA^{-1} ? Deux produits, qui plus est, que l'on sait depuis l'**exemple** (7) ne pas forcément être égaux .

2. qui est un corps (*ie*) tout élément non nul est inversible.

2/ L'inverse d'une matrice, comme on va le voir, n'existe pas forcément et cela à cause de l'existence des diviseurs de zéros mis en évidence dans l'**exemple** (8).

On ne considérera à présent que des matrices carrées[3] qui sont les seules à pouvoir être inversibles.

II.2 Inversion d'une matrice

Définition 9 (Inverse d'une matrice)

Une matrice carrée A est dite **inversible** (ou régulière) si, et seulement si il existe une matrice carrée, appelée matrice inverse et notée A^{-1}, telle que :

$$A \times A^{-1} = A^{-1} \times A = I_n.$$

Si A^{-1} n'existe pas, on dit que la matrice A est non inversible ou singulière.

Remarque: Si elle existe, la matrice inverse est unique.

[Démonstration page 502 , **Maths Repère**, *Hachette*]

On retrouve donc bien la définition de l'inverse d'un réel x non nul (*ie*) le nombre, noté $\frac{1}{x} = x^{-1}$ tel que $x \times \frac{1}{x} = 1$. La matrice unité I_n joue ici le rôle du 1 dans $\mathbb{R}$.

7 **Exercice** Soit la matrice A carrée d'ordre 2, définie par : $\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$.

1/ Montrer que la matrice B définie par : $\begin{pmatrix} -0,5 & 1,5 \\ 1 & -2 \end{pmatrix}$ est la matrice inverse de la matrice A.

2/ Résoudre le système linéaire $(\mathcal{S})$: $\begin{cases} 4x + 3y = 2 \\ 2x + y = 3 \end{cases}$.

Correction:

1/ Il suffit de calculer AB et BA et montrer que ces deux produits donnent I_2.

$$A \times B = \begin{pmatrix} -2+3 & 6-6 \\ -1+1 & 3-2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

et

$$B \times A = \begin{pmatrix} -2+3 & -1,5+1,5 \\ 4-4 & 3-2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Donc $B = A^{-1}$.

2/ Le système $(\mathcal{S})$ s'écrit sous la forme matricielle :

$$\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \iff AX = B \quad \text{avec} \quad B = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

3. (*ie*) des systèmes avec autant d'inconnues que d'équations

Multipliant les deux membres à gauche par $A^{-1} = B$, on obtient :

$$\begin{aligned} A^{-1}(AX) = A^{-1}B &\iff (A^{-1}A)X = A^{-1}B && \text{(associativité de la multiplication)} \\ &\iff \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -0,5 & 1,5 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 2 \\ 3 \end{pmatrix} && \text{(définition de } A^{-1}\text{)} \\ &\iff \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3,5 \\ -4 \end{pmatrix} && \text{(produit des matrices).} \end{aligned}$$

[Exercice résolu 1 page 506
Exercices 74, 78 et 79 page 519 , **Maths Repère**, *Hachette*]

Inverser une matrice semble donc être la clé du problème. Si des conditions d'ordre n existent, en terminale, on se contentera souvent de matrices carrées d'ordre 2 voire 3 mais pas plus.

II.3 Condition pour qu'une matrice d'ordre 2 soit inversible

Définition 10

Soit A une matrice carrée d'ordre 2, on appelle déterminant de la matrice A, noté $\det A$, le nombre réel tel que :

$$\text{Si } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ alors } \det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Exemple 12: Si $A = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$ alors $\det A = \begin{vmatrix} 4 & 3 \\ 2 & 1 \end{vmatrix} = 4 \times 1 - 2 \times 3 = -2$.

Théorème 11 (Inverse d'une matrice d'ordre 2)

Une matrice carrée d'ordre deux est inversible si, et seulement si son déterminant est différent de 0.

$$A^{-1} \text{ existe} \iff \det A \neq 0.$$

On a alors :

$$\text{Si } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ alors } A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{6.1}$$

Preuve: Comme la dimension de la matrice est petite, on peut le faire à la main et chercher une matrice $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ telle que :

$$A \times B = B \times A = I_2.$$

On verra alors si l'on on peut résoudre ce problème à 4 inconnues et si des conditions nécessaires et suffisantes apparaissent.

$$\begin{aligned} A\times B = I_2 &\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &\iff \begin{pmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &\iff \begin{cases} ax+bz=1 \\ cx+dz=0 \end{cases} \quad \text{et} \quad \begin{cases} ay+bt=1 \\ cy+dt=0 \end{cases} \end{aligned}$$

Ces deux systèmes n'ont des solutions que si les vecteurs directeurs des droites qu'ils représentent ne sont pas colinéaires (*ie*)

$$ad-bc\neq 0 \iff \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0 \iff \det A \neq 0.$$

Cette condition vérifiée, des combinaisons linéaires élémentaires donnent les solutions :

$$x=\frac{d}{ad-bc}, \qquad z=\frac{-c}{ad-bc}, \qquad y=\frac{-b}{ad-bc} \quad et \quad t=\frac{a}{ad-bc}.$$

On obtient alors la matrice B suivante : $B=\dfrac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Réciproquement, il ne reste plus qu'à vérifier que $B\times A = I_2$. C'est le cas. !

[Démonstration page 502
Exercice 89 page 521 , **Maths Repère**, *Hachette*]

Ces formules, pratiques essentiellement en petites dimensions, sont connues sous le nom de « formule des Cramer [4] ».

Exemple 13 (Déterminer la matrice inverse de la matrice $A=\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$):

1/ On calcule : $\det(A)=4\times 1-2\times 3=-2\neq 0$ donc la matrice A es inversible.

2/ La condition d'inversibilité remplie, on applique la formule (6.1) :

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

8

Exercice Soit $A=\begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$.

1/ Calculer A^2 et montrer que $A^2=2I-A$.

2/ En déduire que A est inversible et calculer A^{-1}.

4. Gabriel Cramer, mathématicien suisse (**1704-1752**)

Remarque: Le polynôme $P(X) = X^2 + X - 2$ est appelé « polynôme annulateur » de la matrice A. Une matrice donnée, l'existence d'un polynôme annulateur dont le dernier coefficient est non nul assure qu'elle soit inversible :

S'il existe $P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ tel que $P(A) = 0$ alors A est inversible et

$$A^{-1} = -\frac{1}{a_0}\left(a_n A^{n-1} + a_{n-1}A^{n-2} + \ldots + a_1 I\right).$$

III Suites de matrices

[Situation page 498 , **Maths Repère**, *Hachette*]

III.1 Systèmes linéaires

Un exemple tiré du bac pour comprendre la motivation...

Exemple 14 (Métropole septembre 2014 Début): Dans le cadre d'une étude sur les interactions sociales entre des souris, des chercheurs enferment des souris de laboratoire dans une cage comportant deux compartiments A et B. La porte entre ces compartiments est ouverte pendant dix minutes tous les jours à midi.

On étudie la répartition des souris dans les deux compartiments. On estime que chaque jour :

- 20 % des souris présentes dans le compartiment A avant l'ouverture de la porte se trouvent dans le compartiment B après fermeture de la porte,
- 10 % des souris qui étaient dans le compartiment B avant l'ouverture de la porte se trouvent dans le compartiment A après fermeture de la porte.

On suppose qu'au départ, les deux compartiments A et B contiennent le même effectif de souris. On pose $a_0 = 0,5$ et $b_0 = 0,5$.

Pour tout entier naturel n supérieur ou égal à 1, on note a_n et b_n les proportions de souris présentes respectivement dans les compartiments A et B au bout de n jours, après fermeture de la porte. On désigne par U_n la matrice $\begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

1/ Soit n un entier naturel.

(a) Justifier que $U_1 = \begin{pmatrix} 0,45 \\ 0,55 \end{pmatrix}$.

(b) Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

(c) En déduire que $U_{n+1} = MU_n$ où M est une matrice que l'on précisera.

Définition II (Système linéaire de suites récurrentes avec second membre)

Soient les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ définies par leur premier terme respectif u_0 et v_0 et la relation de récurrence :

$$\forall n \in \mathbb{N}, \quad \begin{cases} u_{n+1} = au_n + bv_n + p \\ v_{n+1} = cu_n + dv_n + q \end{cases}, \qquad (a,b,c,d,p,q) \in \mathbb{R}^6.$$

On pose alors :

$$X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} p \\ q \end{pmatrix}.$$

Alors, l'écriture matricielle du système linéaire de suites récurrentes s'écrit :

$$\forall n \in \mathbb{N}, \quad X_{n+1} = AX_n + B.$$

L'objectif de ce paragraphe est de trouver une relation donnant directement la matrice X_n pour toutes valeurs de $n \in \mathbb{N}$ en fonction des conditions initiales.

Ce n'est pas sans rappeler les exercices que l'on a déjà vus où l'on étudiait des suites du genre

$$u_{n+1} = au_n + b,$$

où a et b étaient des réels quelconques.

La résolution est d'ailleurs quasi-identique à la non-commutativité du produit des matrices près.

Pour bien comprendre, on va mener les deux démonstrations de front.

Le théorème à démontrer tout d'abord :

Théorème III

On considère un système linéaire de suites récurrentes donné sous sa forme matricielle :

$$X_{n+1} = AX_n + B.$$

On note I la matrice unité.
Si la matrice $I - A$ est inversible alors $X_n = A^n(X_0 - C) + C$ où $C = (I - A)^{-1}B$.

N'ayez crainte, tout va s'éclairer lors du raisonnement.

Remarque: Dans le cas où $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, on dit que le système linéaire est sans second membre comme dans l'**exemple** (14), question (1c). Il est alors facile de montrer que l'on obtient, par récurrence :

$$\forall n \in \mathbb{N}, \quad X_{n+1} = A^n X_0.$$

Preuve:

Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres vérifiant

$$u_{n+1} = au_n + b \text{ avec } 1-a \neq 0.$$

1/ On résout l'équation $x = ax+b$ dont l'unique solution est

$$c = (1-a)^{-1}b.$$

2/ On introduit la suite auxiliaire $(v_n)_{n\in\mathbb{N}}$ définie par :

$$v_n = u_n - c.$$

(a) On prouve que la suite $(v_n)_{n\in\mathbb{N}}$ est géométrique de raison a.

(b) On en déduit :

$$\begin{aligned}\forall n\in\mathbb{N}, \quad v_n &= a^n v_0\\ &= a^n(u_0-c).\end{aligned}$$

3/ On revient à la suite initiale :

$$\forall n\in\mathbb{N}, \quad u_n = v_n + c.$$

Conclusion :

$$\boxed{\forall n\in\mathbb{N}, \quad u_n = a^n(u_0-c)+c.}$$

Soit $(X_n)_{n\in\mathbb{N}}$ une suite de matrices vérifiant

$$X_{n+1} = AX_n + B \text{ avec } A-I \text{ inversible.}$$

1/ On résout l'équation $X = AX + B$ dont l'unique solution est

$$C = (I-A)^{-1}B.$$

2/ On introduit la suite auxiliaire $(Y_n)_{n\in\mathbb{N}}$ définie par :

$$Y_n = X_n - C.$$

(a) On prouve que la suite $(Y_n)_{n\in\mathbb{N}}$ vérifie, pour tout $n\in\mathbb{N}$ la relation

$$Y_{n+1} = AY_n.$$

(b) On en déduit, par récurrence, que :

$$\begin{aligned}\forall n\in\mathbb{N}, \quad Y_n &= A^n Y_0\\ &= A^n(X_0-C).\end{aligned}$$

3/ On revient à la suite initiale :

$$\forall n\in\mathbb{N}, \quad X_n = Y_n + C.$$

Conclusion :

$$\boxed{\forall n\in\mathbb{N}, \quad X_n = A^n(X_0-C)+C.} \tag{6.2}$$

On remarquera bien le pendant matriciel $(I-A)$ inversible de $1-a\neq 0$ (ie) inversible dans $\mathbb{R}$.

Cette démonstration n'est pas exigible d'un élève de terminale, soit-il en spécialité. Cependant, nombre d'exercices de bac suivent le même raisonnement comme l'exercice ci-dessous.

C'est donc une bonne idée de l'avoir déjà vu...et compris.

9 **Exercice (Polynésie juin 2013)** Un opérateur téléphonique A souhaite prévoir l'évolution du nombre de ses abonnés dans une grande ville par rapport à son principal concurrent B à partir de 2013.

En 2013, les opérateurs A et B ont chacun 300 milliers d'abonnés.

Pour tout entier naturel n, on note a_n le nombre d'abonnés, en milliers, de l'opérateur A la n-ième année après 2013, et b_n le nombre d'abonnés, en milliers, de l'opérateur B la n-ième année après 2013.

Ainsi, $a_0 = 300$ et $b_0 = 300$.

Des observations réalisées les années précédentes conduisent à modéliser la situation par la relation suivante :

pour tout entier naturel n, $\begin{cases} a_{n+1} = 0,7a_n + 0,2b_n + 60 \\ b_{n+1} = 0,1a_n + 0,6b_n + 70 \end{cases}$.

On considère les matrices $M = \begin{pmatrix} 0,7 & 0,2 \\ 0,1 & 0,6 \end{pmatrix}$ et $P = \begin{pmatrix} 60 \\ 70 \end{pmatrix}$.

Pour tout entier naturel n, on note $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

1/ (a) Déterminer U_1.

(b) Vérifier que, pour tout entier naturel n, $U_{n+1} = M \times U_n + P$.

2/ On note I la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(a) Calculer $(I - M) \times \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$.

(b) En déduire que la matrice $I - M$ est inversible et préciser son inverse.

(c) Déterminer la matrice U telle que $U = M \times U + P$.

3/ Pour tout entier naturel, on pose $V_n = U_n - U$.

(a) Justifier que, pour tout entier naturel n, $V_{n+1} = M \times V_n$.

(b) En déduire que, pour tout entier naturel n, $V_n = M^n \times V_0$.

4/ On admet que, pour tout entier naturel n,

$$V_n = \begin{pmatrix} \dfrac{-100}{3} \times 0,8^n - \dfrac{140}{3} \times 0,5^n \\ \dfrac{-50}{3} \times 0,8^n + \dfrac{140}{3} \times 0,5^n \end{pmatrix}$$

(a) Pour tout entier naturel n, exprimer U_n en fonction de n et en déduire la limite de la suite (a_n).

(b) Estimer le nombre d'abonnés de l'opérateur A à long terme.

[2013, **Métropole** *(Juin)*]

III.2 Puissance n-ième d'une matrice carrée

L'expression de $X_n \begin{pmatrix} u_n \\ v_n \end{pmatrix}$ dans l'équation (6.2) dépend de A^n (*ie*) point de jolies expressions de u_n et v_n sans calculs explicites et rapides de A^n.

S'il était nécessaire de se motiver encore, il suffirait de poursuivre l'**exemple** (14) :

Exemple 15 (Métropole septembre 2014 Milieu):

1/ ...

On admet sans démonstration que $U_n = M^n U_0$.

(d) Déterminer la répartition des souris dans les compartiments A et B au bout de 3 jours.

Certaines matrices sont très bien adaptées au calcul de leur puissance n-ième. C'est le cas particulièrement des matrices diagonales :

$$D = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \quad \Longrightarrow \quad D^n = \begin{pmatrix} a^n & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & c^n \end{pmatrix}.$$

Celles-ci vont donc jouer un rôle primordial dans ce genre de problèmes. Le théorème suivant montre tout l'intérêt de pouvoir transformer (ou pas) une matrice quelconque en matrice diagonale.

Théorème IV

Soient A une matrice carrée d'ordre m, P une matrice carrée inversible d'ordre m et D une matrice diagonale d'ordre m telle que $A = PDP^{-1}$. Alors :

$$\forall n \in \mathbb{N}, \quad A^n = PD^nP^{-1}.$$

La matrice P s'appelle la matrice de passage.

Preuve: On démontre ce résultat par récurrence sur n :

- **Initialisation :** $A^2 = \left(PDP^{-1}\right)\left(PDP^{-1}\right) = PD\underbrace{\left(PP^{-1}\right)}_{I_m}DP^{-1}$

  $= PD^2P^{-1}.$

  La relation est vraie pour $n = 2$.

- **Hérédité :** Supposons qu'il existe un entier k tel que $A^k = PD^kP^{-1}$. Alors

  $$A^{k+1} = AA^k = \left(PDP^{-1}\right)\left(PD^kP^{-1}\right) = PD\underbrace{\left(PP^{-1}\right)}_{I_m}D^kP^{-1}$$

  $$= PD^{k+1}P^{-1}$$

  La relation est vraie à l'ordre $k+1$, elle est héréditaire.

La relation est initialisée et héréditaire donc elle est vraie pour tout entier $n \in \mathbb{N}$.

[Exercice résolu 2 page 507
Exercice [5]110 page 524 , **Maths Repère**, *Hachette*]

[Exercice 113 page 525 , **Maths Repère**, *Hachette*]

5. Et lire le commentaire « Méthode ».

Exemple 16 (Métropole septembre 2014 FiN): On reprend les notations de l'**exemple** (14).

2/ Soit la matrice $P = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}$.

(a) Calculer P^2. En déduire que P est inversible et $P^{-1} = \frac{1}{3}P$.

(b) Vérifier que $P^{-1}MP$ est une matrice diagonale D que l'on précisera.

(c) Démontrer que pour tout entier naturel n supérieur ou égal à 1, $M^n = PD^nP^{-1}$.
À l'aide d'un logiciel de calcul formel, on obtient

$$M^n = \begin{pmatrix} \dfrac{1+2\times 0,7^n}{3} & \dfrac{1-0,7^n}{3} \\ \dfrac{2-2\times 0,7^n}{3} & \dfrac{2+0,7^n}{3} \end{pmatrix}.$$

3/ En s'aidant des questions précédentes, que peut-on dire de la répartition à long terme des souris dans les compartiments A et B de la cage ?

Définition 12

On dit que la suite de matrices colonnes $(X_n)_{n\in\mathbb{N}}$ converge si, et seulement si chacune des suites composantes de X_n converge.
On pose alors $X = \lim\limits_{n\to+\infty} X_n$. La matrice colonne X décrit l'**état stable** du système.

La suite de matrices carrées $(A^n)_{n\in\mathbb{N}}$ converge si, et seulement si chacune des suites coefficients de A^n converge.

Remarque: Comme pour les suites récurrentes définies par des fonctions continues, la matrice colonne X est nécessairement solution de l'équation $X = AX$.

Théorème V

La suite de matrices colonnes $(X_n)_{n\in\mathbb{N}}$ converge si, et seulement si la suite de matrices carrées $(A^n)_{n\in\mathbb{N}}$ converge.

Exemple 17: Reprenons une dernière fois les notations de l'**exemple** (14) :

$$M = \lim_{n\to+\infty} M^n = \begin{pmatrix} \lim\limits_{n\to+\infty} \dfrac{1+2\times 0,7^n}{3} & \lim\limits_{n\to+\infty} \dfrac{1-0,7^n}{3} \\ \lim\limits_{n\to+\infty} \dfrac{2-2\times 0,7^n}{3} & \lim\limits_{n\to+\infty} \dfrac{2+0,7^n}{3} \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{2}{3} \end{pmatrix}.$$

Donc $\lim\limits_{n\to+\infty} U_n = \lim\limits_{n\to+\infty} \left(M^nU_0\right) = MU_0 = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$.

Les souris se répartiront donc dans les cages A et B dans les proportions respectives $\frac{1}{3}/\frac{2}{3}$.

[2014, **Antilles-Guyane** *(Septembre)*]

[Exercice 118 page 526
Exercice 121 page 528 , **Maths Repère**, *Hachette*]

III.3 Marches aléatoires

[Situation page 500
Exercice résolu 5 pages 510 et 511 , **Maths Repère**, *Hachette*]

Exemple 18: On estime que les patients admis dans un certain service d'un hôpital peuvent se trouver dans l'un des 3 états suivants :

1/ Soins réguliers. **2/** Soins intensif. **3/** Sortie.

Cette estimation est décrite par le tableau suivant, dans lequel sont indiquées les probabilités de passage d'un des états à un autre dans un intervalle de 24 heures (probabilités obtenues par modélisation des fréquences observées sur une longue période).

	Soins réguliers	Soins intensif	Sortie
Soins réguliers	0,6	0,1	0,3
Soins intensif	0,5	0,4	0,1
Sortie	0	0,1	0,9

Les informations chiffrées précédentes peuvent être stockées sous la forme d'une matrice $T \in \mathscr{M}_3(\mathbb{R})$ appelée **matrice de transition** :

$$T = \begin{pmatrix} 0,6 & 0,1 & 0,3 \\ 0,5 & 0,4 & 0,1 \\ 0 & 0,1 & 0,9 \end{pmatrix}$$

On pourrait aussi, à partir du tableau tracer un graphe probabiliste.

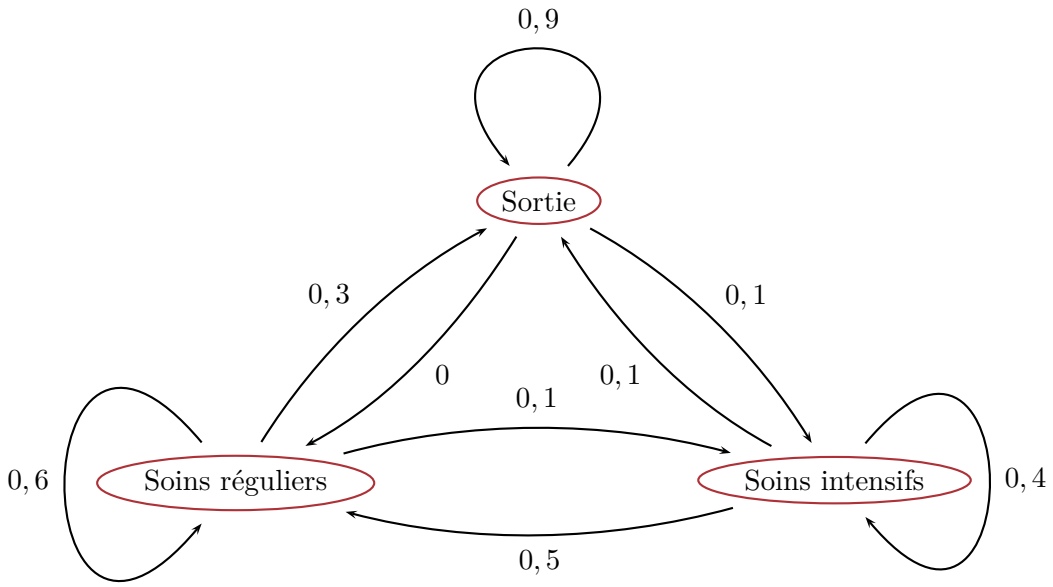
Définition 13 (Graphe probabiliste)

Quand on se déplace sur un graphe à p sommets et que l'on a, à chaque fois, une certaine probabilité d'aller d'un sommet à un autre, on parle de **marche aléatoire**.
La **matrice de transition** $T = (t_{ij})$ d'une telle marche aléatoire est la matrice carrée de taille p dont le coefficient t_{ij} est la probabilité p_{ij} d'aller du sommet i au sommet j.
Cette probabilité est appelée **probabilité de transition**.
Lorsqu'on effectue n pas dans ce graphe, on note X_n la matrice ligne dont le i-ième coefficient est la probabilité d'être au sommet i au bout de ces n pas.
Pour tout entier naturel n on a donc :

$$X_{n+1} = X_n T \quad \Longrightarrow \quad X_n = X_0 T^n.$$

[Démonstration page 505
Exercices 126 et 127 page 530 , **Maths Repère**, *Hachette*]

Remarque: De telles matrices où la somme des coefficients d'une même ligne est égale à 1 s'appellent des matrices **stochastiques**.



Supposons qu'un certain jour n, la distribution des patients suivant les trois états possibles s'écrive $X_n = \begin{pmatrix} 12 & 5 & 6 \end{pmatrix}$. Le lendemain $n+1$, la nouvelle distribution sera X_{n+1} telle que :

$$X_{n+1} = X_n \times T.$$

On retrouve alors le même type de problèmes que précédemment qui se résoudront exactement de la même manière si ce n'est que la matrice X_n est ici une matrice ligne. Cela ne change pas grand chose. [6]

La limite X, si elle existe, de cette suite représente l'état asymptotique ou **stable** du système.

Remarque: On peut compliquer un peu le problème en supposant que, chaque jour, sont admis des patients supplémentaires sous la forme d'une matrice $J = \begin{pmatrix} 5 & 3 & 0 \end{pmatrix}$. Le système se transformerait alors en :

$$X_{n+1} = X_n \times T + J.$$

Le **théorème** (III) s'applique encore.

C'est ainsi le même genre de problèmes que précédemment dans un contexte différent.

6. En admettant que ${}^t(X_nT) = {}^tT{}^tX_n$ par transposition, on obtient exactement le même système.

10 **Exercice (Métropole septembre 2013)** *Les parties A et B peuvent être traitées indépendamment l'une de l'autre*

Dans un village imaginaire isolé, une nouvelle maladie contagieuse mais non mortelle a fait son apparition.

Rapidement les scientifiques ont découvert qu'un individu pouvait être dans l'un des trois états suivants :

S : « l'individu est sain, c'est-à-dire non malade et non infecté »,

I : « l'individu est porteur sain, c'est-à-dire non malade mais infecté »,

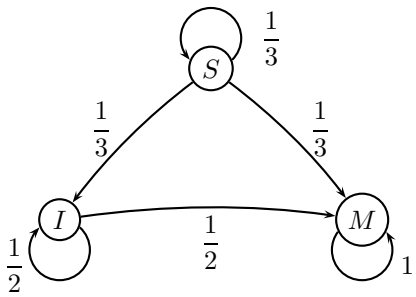
M : « l'individu est malade et infecté ».

Partie A

Les scientifiques estiment qu'un seul individu est à l'origine de la maladie sur les 100 personnes que compte la population et que, d'une semaine à la suivante, un individu change d'état suivant le processus suivant :

- parmi les individus sains, la proportion de ceux qui deviennent porteurs sains est égale à $\frac{1}{3}$ et la proportion de ceux qui deviennent malades est égale à $\frac{1}{3}$,
- parmi les individus porteurs sains, la proportion de ceux qui deviennent malades est égale à $\frac{1}{2}$.

La situation peut être représentée par un graphe probabiliste comme ci-dessous.



On note $P_n = (s_n \quad i_n \quad m_n)$ la matrice ligne donnant l'état probabiliste au bout de n semaines où s_n, i_n et $m_n$désignent respectivement la probabilité que l'individu soit sain, porteur sain ou malade la n-ième semaine.

On a alors $P_0 = (0,99 \quad 0 \quad 0,01)$ et pour tout entier naturel n,

$$\begin{cases} s_{n+1} &= \frac{1}{3}s_n \\ i_{n+1} &= \frac{1}{3}s_n + \frac{1}{2}i_n \\ m_{n+1} &= \frac{1}{3}s_n + \frac{1}{2}i_n + m_n \end{cases}$$

1/ Écrire la matrice A appelée *matrice de transition*, telle que pour tout entier naturel n, $P_{n+1} = P_n \times A$.

2/ Démontrer par récurrence que pour tout entier naturel n non nul, $P_n = P_0 \times A^n$.

3/ Déterminer l'état probabiliste P_4 au bout de quatre semaines. On pourra arrondir les valeurs à 10^{-2}.

Quelle est la probabilité qu'un individu soit sain au bout de quatre semaines ?

Partie B

La maladie n'évolue en réalité pas selon le modèle précédent puisqu'au bout de 4 semaines de recherche, les scientifiques découvrent un vaccin qui permet d'enrayer l'endémie et traitent immédiatement l'ensemble de la population.

L'évolution hebdomadaire de la maladie après vaccination est donnée par la matrice de transition :

$$B = \begin{pmatrix} \frac{5}{12} & \frac{1}{4} & \frac{1}{3} \\ \frac{5}{12} & \frac{1}{4} & \frac{1}{3} \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \end{pmatrix}.$$

On note Q_n la matrice ligne donnant l'état probabiliste au bout de n semaines après la mise en place de ces nouvelles mesures de vaccination. Ainsi, $Q_n = (S_n \quad I_n \quad M_n)$ où S_n, I_n et M_n désignent respectivement la probabilité que l'individu soit sain, porteur sain et malade la n-ième semaine après la vaccination.

Pour tout entier naturel n, on a alors $Q_{n+1} = Q_n \times B$.

D'après la partie A, $Q_0 = P_4$. Pour la suite, on prend $Q_0 = (0,01 \quad 0,10 \quad 0,89)$ où les coefficients ont été arrondis à 10^{-2}.

1/ Exprimer S_{n+1}, I_{n+1} et M_{n+1} en fonction de S_n, I_n et M_n.

2/ Déterminer la constante réelle k telle que $B^2 = kJ$ où J est la matrice carrée d'ordre 3 dont tous les coefficients sont égaux à 1.

On en déduit que pour tout entier n supérieur ou égal à 2, $B^n = B^2$.

3/ (a) Démontrer que pour tout entier n supérieur ou égal à 2, $Q_n = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$.

(b) Interpréter ce résultat en terme d'évolution de la maladie.
Peut-on espérer éradiquer la maladie grâce au vaccin ?

[2014, **Pondichéry** *(Avril)*]

[Exercice 135 page 534
Exercice 131 page 532 , **Maths Repère**, *Hachette*]

$$A = \left(a_{ij}\right) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix} \in \mathscr{M}_{mn}(\mathbb{R})$$

i^{e} ligne — j^{e} colonne — Diagonale de la matrice

$(a_{ij})+(b_{ij}) = (a_{ij}+b_{ij})$.

$\lambda.(a_{ij}) = (\lambda \times a_{ij})$.

${}^tM = (a_{ji}) \in \mathscr{M}_{nm}$.
${}^t\begin{pmatrix} Vecteur \\ ligne \end{pmatrix} = \begin{pmatrix} Vecteur \\ colonne \end{pmatrix}$

Si $C = A \times B$ alors $\left(c_{ij}\right) = \left(a_{ij}\right) \times \left(b_{ij}\right)$

$$c_{ij} = \begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix} \times \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix}.$$

$$= a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1j} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2j} & \dots & b_{2p} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nj} & \dots & b_{np} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1j} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2j} & \dots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{i1} & c_{i2} & \dots & c_{ij} & \dots & c_{ip} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mj} & \dots & c_{mp} \end{pmatrix}$$

$AB \neq BA$.

$AB = 0 \not\Longrightarrow A = 0$ ou $B = 0$.

$AB = AC \not\Longrightarrow B = C$.

$A \times (B + C) = A \times B + A \times C$.

$A \times I_n = I_n \times A = A$.

$A^n = \underbrace{A \times A \times \ldots \times A}_{n\ fois}$.

$AB = BA$ (A et B commutent) $\Longrightarrow \left(A+B\right)^n = \sum_{k=0}^{n} \binom{n}{k} A^k \times B^{n-k}$.

Système linéaire :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots + \ldots + \ldots + \ldots = \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{2m}x_n = b_m \end{cases} \iff \underbrace{\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{2m} \end{pmatrix}}_{A} \times \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}}_{B}$$

$$\iff AX = B \implies \boxed{X = A^{-1}B} \quad \text{(si } A \text{ est inversible)}$$

$$\begin{aligned} A \text{ inversible} &\iff \exists B \text{ telle que } A \times B = B \times A = I_n \\ &\iff \det A \neq 0 \end{aligned} \implies B = A^{-1}.$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

$$A \text{ inversible} \implies A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Système linéaire de suites récurrentes :

$$\begin{cases} u_{n+1} = au_n + bv_n + p \\ v_{n+1} = cu_n + dv_n + q \end{cases} \iff \underbrace{\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix}}_{X_{n+1}} = \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \times \underbrace{\begin{pmatrix} u_n \\ v_n \end{pmatrix}}_{X_n} + \underbrace{\begin{pmatrix} p \\ q \end{pmatrix}}_{B}$$

$$\iff X_{n+1} = AX_n + B$$

(Cas général) $I - A$ inversible $\implies X_n = A^n(X_0 - C) + C$ où $C = (I - A)^{-1}B$.

(Par récurrence) $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \implies X_n = A^n X_0.$

$$D = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \implies D^n = \begin{pmatrix} a^n & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & c^n \end{pmatrix}.$$

$A = PDP^{-1} \implies A^n = PD^nP^{-1}$.
P : matrice de passage.

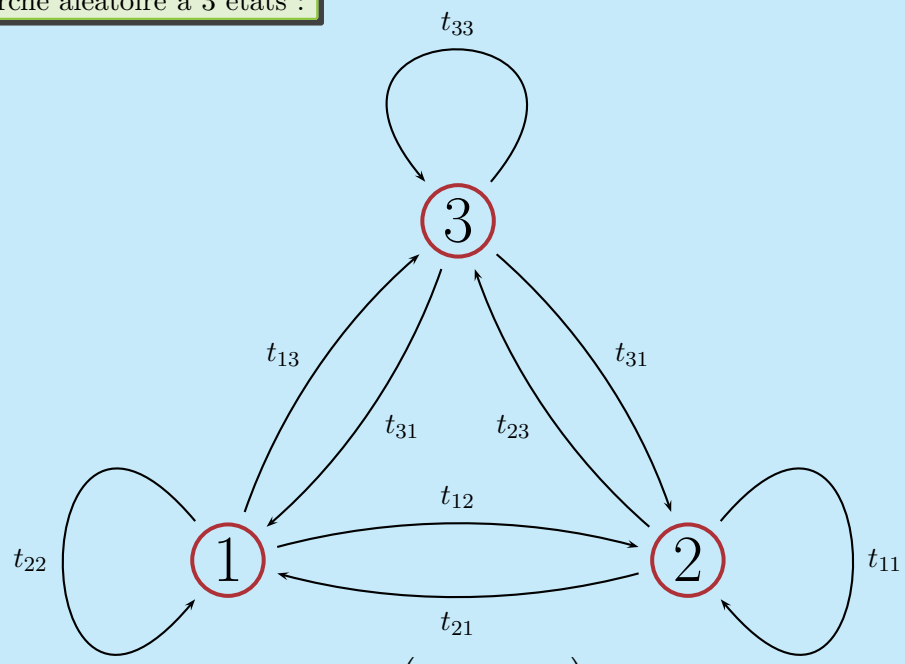
Si $X_n = \big((x_{ij})_n\big)$ alors $\lim\limits_{n\to+\infty} X_n = \big(\lim\limits_{n\to+\infty}(x_{ij})_n\big)$.
$X = \lim\limits_{n\to+\infty} X_n$ est l'état stable ou asymptotique du système.

Marche aléatoire et Graphe probabiliste :

$T = (t_{ij})$: matrice de transition $\iff$ t_{ij} = probabilité d'aller de l'état i à l'état j.
L_n : matrice **ligne** dont le i-ième coefficient est la probabilité d'être dans i au bout de n pas.

$$\implies \forall n \in \mathbb{N},\ L_{n+1} = L_nT \quad \implies \quad L_n = L_0T^n.$$

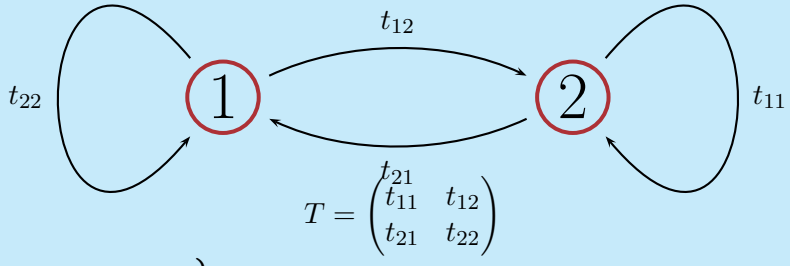
Marche aléatoire à 3 états :



$$T = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix}$$

$$\left.\begin{matrix} t_{11}+t_{12}+t_{13} \\ t_{21}+t_{22}+t_{23} \\ t_{31}+t_{32}+t_{33} \end{matrix}\right\} = 1 \implies T \text{ est une matrice stochastique.}$$

Marche aléatoire à 2 états :



$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$$

$$\left.\begin{matrix} t_{11}+t_{12} \\ t_{21}+t_{22} \end{matrix}\right\} = 1 \implies T \text{ est une matrice stochastique.}$$

Ne pas confondre avec les systèmes linéaires $X_{n+1} = AX_n$ où X_n est un vecteur **colonne**.
Les matrices A et T sont transposées l'une de l'autre.

$$\begin{cases} x_{n+1} = ax_n + by_n \\ y_{n+1} = cx_n + dy_n \end{cases} \iff \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

ou

$$\iff \begin{pmatrix} x_{n+1} & y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & y_n \end{pmatrix} \times \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Chapitre

7

Bac 2015 spécialité

1

Exercice (Pondichery) Les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés **nombres de Mersenne**.

1/ On désigne par a, b et c trois entiers naturels non nuls tels que $\text{pgcd}(b\ ;\ c) = 1$.
Prouver, à l'aide du théorème de Gauss, que :

si b divise a et c divise a alors le produit bc divise a.

2/ On considère le nombre de Mersenne $2^{33} - 1$.
Un élève utilise sa calculatrice et obtient les résultats ci-dessous.

$(2^{33} - 1) \div 3$	2863311530
$(2^{33} - 1) \div 4$	2147483648
$(2^{33} - 1) \div 12$	715827882,6

Il affirme que 3 divise $(2^{33} - 1)$ et 4 divise $(2^{33} - 1)$ et 12 ne divise pas $(2^{33} - 1)$.

(a) En quoi cette affirmation contredit-elle le résultat démontré à la question **1.** ?
(b) Justifier que, en réalité, 4 ne divise pas $(2^{33} - 1)$.
(c) En remarquant que $2 \equiv -1 \quad [3]$, montrer que, en réalité, 3 ne divise pas $2^{33} - 1$.
(d) Calculer la somme $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \cdots + (2^3)^{10}$.
(e) En déduire que 7 divise $2^{33} - 1$.

3/ On considère le nombre de Mersenne $2^7 - 1$. Est-il premier ? Justifier.

4/ On donne l'algorithme suivant où $\text{MOD}(N,\ k)$ représente le reste de la division euclidienne de N par k.

Variables :	n entier naturel supérieur ou égal à 3
	k entier naturel supérieur ou égal à 2
Initialisation :	Demander à l'utilisateur la valeur de n.
	Affecter à k la valeur 2.
Traitement :	Tant que $\text{MOD}(2^n - 1,\ k) \neq 0$ et $k \leqslant \sqrt{2^n - 1}$
	Affecter à k la valeur $k + 1$
	Fin de Tant que.
Sortie :	**Afficher** k.
	Si $k > \sqrt{2^n - 1}$
	Afficher « CAS 1 »
	Sinon
	Afficher « CAS 2 »
	Fin de Si

(a) Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?

(b) Que représente le CAS 2 pour le nombre de Mersenne étudié ? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié ?

(c) Que représente le CAS 1 pour le nombre de Mersenne étudié ?

2 **Exercice (Liban)** Un fumeur décide d'arrêter de fumer. On choisit d'utiliser la modélisation suivante :

- s'il ne fume pas un jour donné, il ne fume pas le jour suivant avec une probabilité de 0,9 ;
- s'il fume un jour donné, il fume le jour suivant avec une probabilité de 0,6.

On appelle p_n la probabilité de ne pas fumer le n-ième jour après sa décision d'arrêter de fumer et q_n, la probabilité de fumer le n-ième jour après sa décision d'arrêter de fumer.

On suppose que $p_0 = 0$ et $q_0 = 1$.

1/ Calculer p_1 et q_1.

2/ On utilise un tableur pour automatiser le calcul des termes successifs des suites (p_n) et (q_n). Une copie d'écran de cette feuille de calcul est fournie ci-dessous :

	A	B	C	D
1	n	p_n	q_n	
2	0	0	1	
3	1			
4	2			
5	3			

Dans la colonne A figurent les valeurs de l'entier naturel n.

Quelles formules peut-on écrire dans les cellules B3 et C3 de façon qu'en les recopiant vers le bas, on obtienne respectivement dans les colonnes B et C les termes successifs des suites (p_n) et (q_n) ?

3/ On définit les matrices M et, pour tout entier naturel n, X_n par :

$$M = \begin{pmatrix} 0,9 & 0,4 \\ 0,1 & 0,6 \end{pmatrix} \quad \text{et} \quad X_n = M^n \times X_0.$$

On admet que $X_{n+1} = M \times X_n$ et que, pour tout entier naturel n, $Xn = M^n \times X_0$.

On définit les matrices A et B par $A = \begin{pmatrix} 0,8 & 0,8 \\ 0,2 & 0,2 \end{pmatrix}$ et $B = \begin{pmatrix} 0,2 & -0,8 \\ -0,2 & 0,8 \end{pmatrix}$.

(a) Démontrer que $M = A + 0,5B$.

(b) Vérifier que $A^2 = A$, et que $A \times B = B \times A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

On admet dans la suite que, pour tout entier naturel n strictement positif, $A^n = A$ et $B^n = B$.

(c) Démontrer que, pour tout entier naturel n, $M^n = A + 0,5^n B$.

(d) En déduire que, pour tout entier naturel n, $p_n = 0,8 - 0,8 \times 0,5^n$.

(e) À long terme, peut-on affirmer avec certitude que le fumeur arrêtera de fumer ?

3

Exercice (Amérique du Nord) On donne les matrices $M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix}$ et $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Partie A

1/ Déterminer la matrice M^2. On donne $M^3 = \begin{pmatrix} 20 & 10 & 11 \\ 12 & 2 & 9 \\ 42 & 20 & 21 \end{pmatrix}$.

2/ Vérifier que $M^3 = M^2 + 8M + 6I$.

3/ En déduire que M est inversible et que $M^{-1} = \dfrac{1}{6}\left(M^2 - M - 8I\right)$.

Partie B Étude d'un cas particulier

On cherche à déterminer trois nombres entiers a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A$(1\,;\,1)$, B$(-1\,;\,-1)$ et C$(2\,;\,5)$.

1/ Démontrer que le problème revient à chercher trois entiers a, b et c tels que

$$M \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}.$$

2/ Calculer les nombres a, b et c et vérifier que ces nombres sont des entiers.

Partie C Retour au cas général

Les nombres a, b, c, p, q, r sont des entiers.

Dans un repère $(O;\,\vec{\imath};\,\vec{\jmath})$, on considère les points A$(1\,;\,p)$, B$(-1\,;\,q)$ et C$(2\,;\,r)$.

On cherche des valeurs de p, q et r pour qu'il existe une parabole d'équation $y = ax^2 + bx + c$ passant par A, B et C.

1/ Démontrer que si $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = M^{-1} \begin{pmatrix} p \\ q \\ r \end{pmatrix}$ avec a, b et c entiers, alors

$$\begin{cases} -3p + q + 2r & \equiv & 0\,[6] \\ 3p - 3q & \equiv & 0\,[6] \\ 6p + 2q - 2r & \equiv & 0\,[6] \end{cases}$$

2/ En déduire que $\begin{cases} q - r & \equiv & 0\,[3] \\ p - q & \equiv & 0\,[2] \end{cases}$.

3/ Réciproquement, on admet que si $\begin{cases} q - r & \equiv & 0\,[3] \\ p - q & \equiv & 0\,[2] \\ \text{A, B, C ne sont pas alignés} \end{cases}$

alors il existe trois entiers a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A, B et C.

(a) Montrer que les points A, B et C sont alignés si et seulement si $2r + q - 3p = 0$.

(b) On choisit $p = 7$. Déterminer des entiers q, r, a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A, B et C.

4

Exercice (Centres étrangers) Dans cet exercice, on s'intéresse aux triplets d'entiers naturels non nuls $(x,\ y,\ z)$ tels que :

$$x^2 + y^2 = z^2.$$

Ces triplets seront nommés « triplets pythagoriciens » en référence aux triangles rectangles dont ils mesurent les côtés, et notés en abrégé « TP ».

Ainsi $(3,\ 4,\ 5)$ est un TP car $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

Partie A : généralités

1/ Démontrer que, si $(x,\ y,\ z)$ est un TP, et p un entier naturel non nul, alors le triplet $(px,\ py,\ pz)$ est lui aussi un TP.

2/ Démontrer que, si $(x,\ y,\ z)$ est un TP, alors les entiers naturels x, y et z ne peuvent pas être tous les trois impairs.

3/ Pour cette question, on admet que tout entier naturel non nul n peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair :

$n = 2^\alpha \times k$ où α est un entier naturel (éventuellement nul) et k un entier naturel impair.

L'écriture $n = 2^\alpha \times k$ est nommée *décomposition* de n.

Voici par exemple les *décompositions* des entiers 9 et 120 : $9 = 2^0 \times 9$,

$120 = 2^3 \times 15$.

(a) Donner la décomposition de l'entier 192.

(b) Soient x et z deux entiers naturels non nuls, dont les décompositions sont $x = 2^\alpha \times k$ et $z = 2^\beta \times m$.

Écrire la *décomposition* des entiers naturels $2x^2$ et z^2.

(c) En examinant l'exposant de 2 dans la *décomposition* de $2x^2$ et dans celle de z^2 , montrer qu'il n'existe pas de couple d'entiers naturels non nuls $(x,\ z)$ tels que $2x^2 = z^2$.

On admet que la question **A - 3.** permet d'établir que les trois entiers naturels x, y et z sont deux à deux distincts. Comme de plus les entiers naturels $x,\ y$ jouent un rôle symétrique, dans la suite, pour tout TP $(x,\ y,\ z)$, les trois entiers naturels x, y et z seront rangés dans l'ordre suivant :

$$x < y < z.$$

Partie B : recherche de triplets pythagoriciens contenant l'entier 2015

1/ Décomposer en produit de facteurs premiers l'entier 2015 puis, en utilisant le TP donné dans le préambule, déterminer un TP de la forme $(x,\ y,\ 2015)$.

2/ On admet que, pour tout entier naturel n , $(2n+1)^2 + \left(2n^2+2n\right)^2 = \left(2n^2+2n+1\right)^2$.

Déterminer un TP de la forme $(2015,\ y,\ z)$.

3/ (a) En remarquant que $403^2 = 169 \times 961$, déterminer un couple d'entiers naturels non nuls $(x,\ z)$ tels que : $z^2 - x^2 = 403^2$, avec $x < 403$.

(b) En déduire un TP de la forme $(x,\ 2015,\ z)$.

5

Exercice (Polynésie) On considère la matrice $A = \begin{pmatrix} -4 & 6 \\ -3 & 5 \end{pmatrix}$.

1/ On appelle I la matrice identité d'ordre 2.
Vérifier que $A^2 = A + 2I$.

2/ En déduire une expression de A^3 et une expression de A^4 sous la forme $\alpha A + \beta I$ où α et β sont des réels.

3/ On considère les suites (r_n) et (s_n) définies par $r_0 = 0$ et $s_0 = 1$ et, pour tout entier naturel n,

$$\left\{ \begin{array}{rcl} r_{n+1} & = & r_n + s_n \\ s_{n+1} & = & 2r_n \end{array} \right\}$$

Démontrer que, pour tout entier naturel n, $A^n = r_n A + s_n I$.

4/ Démontrer que la suite (k_n) définie pour tout entier naturel n par $k_n = r_n - s_n$ est géométrique de raison -1.
En déduire, pour tout entier naturel n, une expression explicite de k_n en fonction de n.

5/ On admet que la suite (t_n) définie pour tout entier naturel n par $t_n = r_n + \dfrac{(-1)^n}{3}$ est géométrique de raison 2.
En déduire, pour tout entier naturel n, une expression explicite de t_n en fonction de n.

6/ Déduire des questions précédentes, pour tout entier naturel n, une expression explicite de r_n et s_n en fonction de n.

7/ En déduire alors, pour tout entier naturel n, une expression des coefficients de la matrice A^n.

6

Exercice (Asie) On dit qu'un entier naturel non nul N est un nombre triangulaire s'il existe un entier naturel n tel que : $N = 1 + 2 + \ldots + n$. Par exemple, 10 est un nombre triangulaire car $10 = 1 + 2 + 3 + 4$.

Le but de ce problème est de déterminer des nombres triangulaires qui sont les carrés d'un entier.

On rappelle que, pour tout entier naturel non nul n, on a :

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Partie A : nombres triangulaires et carrés d'entiers

1/ Montrer que 36 est un nombre triangulaire, et qu'il est aussi le carré d'un entier.

2/ (a) Montrer que le nombre $1 + 2 + \ldots + n$ est le carré d'un entier si et seulement s'il existe un entier naturel p tel que : $n^2 + n - 2p^2 = 0$.

(b) En déduire que le nombre $1 + 2 + \ldots + n$ est le carré d'un entier si et seulement s'il existe un entier naturel p tel que : $(2n+1)^2 - 8p^2 = 1$.

Partie B : étude de l'équation diophantienne associée

On considère (E) l'équation diophantienne :

$$x^2 - 8y^2 = 1,$$

où x et y désignent deux entiers relatifs.

1/ Donner deux couples d'entiers naturels inférieurs à 10 qui sont solution de (E).

2/ Démontrer que, si un couple d'entiers relatifs non nuls $(x\ ;\ y)$ est solution de (E), alors les entiers relatifs x et y sont premiers entre eux.

Partie C : lien avec le calcul matriciel

Soit x et y deux entiers relatifs. On considère la matrice $A = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$.

On définit les entiers relatifs x' et y' par l'égalité : $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$.

1/ Exprimer x' et y' en fonction de x et de y.

2/ Déterminer la matrice A^{-1}, puis exprimer x et y en fonction de x' et y'.

3/ Démontrer que $(x\ ;\ y)$ est solution de (E) si et seulement si $(x'\ ;\ y')$ est solution de (E).

4/ On considère les suites (x_n) et (y_n) définies par $x_0 = 3,\ y_0 = 1$ et, pour tout entier naturel n, $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix}$. On admet que, ainsi définis, les nombres x_n et y_n sont des entiers naturels pour toute valeur de l'entier n.

Démontrer par récurrence que, pour tout entier naturel n, le couple $(x_n\ ;\ y_n)$ est solution de (E).

Partie D : retour au problème initial

À l'aide des parties précédentes, déterminer un nombre triangulaire supérieur à 2015 qui est le carré d'un entier.

7 Exercice (Antilles-Guyane)

Les parties A et B peuvent être traitées de façon indépendante

Partie A

Pour deux entiers naturels non nuls a et b, on note $r(a,\ b)$ le reste dans la division euclidienne de a par b.

On considère l'algorithme suivant :

Variables :	c est un entier naturel
	a et b sont des entiers naturels non nuls
Entrées :	Demander a
	Demander b
Traitement :	Affecter à c le nombre $r(a,\ b)$
	Tant que $c \neq 0$
	Affecter à a le nombre b
	Affecter à b la valeur de c
	Affecter à c le nombre $r(a,\ b)$
	Fin Tant que
Sortie :	Afficher b

1/ Faire fonctionner cet algorithme avec $a = 26$ et $b = 9$ en indiquant les valeurs de a, b et c à chaque étape.

2/ Cet algorithme donne en sortie le PGCD des entiers naturels non nuls a et b.

Le modifier pour qu'il indique si deux entiers naturels non nuls a et b sont premiers entre eux ou non.

Partie B

À chaque lettre de l'alphabet on associe grâce au tableau ci-dessous un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :

Étape 1 : on choisit deux entiers naturels p et q compris entre 0 et 25.

Étape 2 : à la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau ci-dessus.

Étape 3 : on calcule l'entier x' défini par les relations :

$$x' \equiv px + q \quad [26] \quad \text{et} \quad 0 \leqslant x' \leqslant 25.$$

Étape 4 : à l'entier x', on associe la lettre correspondante dans le tableau.

1/ Dans cette question, on choisit $p = 9$ et $q = 2$.

(a) Démontrer que la lettre V est codée par la lettre J.

(b) Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que $9u + 26v = 1$. Donner sans justifier un couple $(u,\ v)$ qui convient.

(c) Démontrer que $x' \equiv 9x + 2 \quad [26]$ équivaut à $x \equiv 3x' + 20 \quad [26]$.

(d) Décoder la lettre R.

2/ Dans cette question, on choisit $q = 2$ et p est inconnu. On sait que J est codé par D.
Déterminer la valeur de p (on admettra que p est unique).

3/ Dans cette question, on choisit $p = 13$ et $q = 2$. Coder les lettres B et D. Que peut-on dire de ce codage ?

8 Exercice (Métropole)

1/ On considère l'équation (E) à résoudre dans $\mathbb{Z}$:

$$7x - 5y = 1.$$

(a) Vérifier que le couple $(3\,;\,4)$ est solution de (E).

(b) Montrer que le couple d'entiers $(x\ ;\ y)$ est solution de (E) si et seulement si $7(x-3) = 5(y-4)$.

(c) Montrer que les solutions entières de l'équation (E) sont exactement les couples $(x\ ;\ y)$ d'entiers relatifs tels que :

$$\begin{cases} x &= 5k+3 \\ y &= 7k+4 \end{cases} \quad \text{où } k \in \mathbb{Z}.$$

2/ Une boîte contient 25 jetons, des rouges, des verts et des blancs. Sur les 25 jetons il y a x jetons rouges et y jetons verts. Sachant que $7x - 5y = 1$, quels peuvent être les nombres de jetons rouges, verts et blancs ?

Dans la suite, on supposera qu'il y a 3 jetons rouges et 4 jetons verts.

3/ On considère la marche aléatoire suivante d'un pion sur un triangle ABC. À chaque étape, on tire au hasard un des jetons parmi les 25, puis on le remet dans la boîte.

- Lorsqu'on est en A :

Si le jeton tiré est rouge, le pion va en B. Si le jeton tiré est vert, le pion va en C. Si le jeton tiré est blanc, le pion reste en A.

- Lorsqu'on est en B :

Si le jeton tiré est rouge, le pion va en A. Si le jeton tiré est vert, le pion va en C. Si le jeton tiré est blanc, le pion reste en B.

- Lorsqu'on est en C :

Si le jeton tiré est rouge, le pion va en A. Si le jeton tiré est vert, le pion va en B. Si le jeton tiré est blanc, le pion reste en C.

Au départ, le pion est sur le sommet A.

Pour tout entier naturel n, on note a_n, b_n et c_n les probabilités que le pion soit respectivement sur les sommets A, B et C à l'étape n.

On note X_n la matrice ligne $\begin{pmatrix} a_n & b_n & c_n \end{pmatrix}$ et T la matrice $\begin{pmatrix} 0,72 & 0,12 & 0,16 \\ 0,12 & 0,72 & 0,16 \\ 0,12 & 0,16 & 0,72 \end{pmatrix}$.

Donner la matrice ligne X_0 et montrer que, pour tout entier naturel n, $X_{n+1} = X_n T$.

4/ On admet que $T = PDP^{-1}$ où $P^{-1} = \begin{pmatrix} \frac{3}{10} & \frac{37}{110} & \frac{4}{11} \\ \frac{1}{10} & -\frac{1}{10} & 0 \\ 0 & \frac{1}{11} & -\frac{1}{11} \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0,6 & 0 \\ 0 & 0 & 0,56 \end{pmatrix}$.

(a) À l'aide de la calculatrice, donner les coefficients de la matrice P. On pourra remarquer qu'ils sont entiers.

(b) Montrer que $T^n = PD^nP^{-1}$.

(c) Donner sans justification les coefficients de la matrice D^n.

On note α_n, β_n, γ_n les coefficients de la première ligne de la matrice T^n ainsi :

$$T^n = \begin{pmatrix} \alpha_n & \beta_n & \gamma_n \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}.$$

On admet que $\alpha_n = \dfrac{3}{10} + \dfrac{7}{10} \times 0,6^n$ et $\beta_n = \dfrac{37 - 77 \times 0,6^n + 40 \times 0,56^n}{110}$.

On ne cherchera pas à calculer les coefficients de la deuxième ligne ni ceux de la troisième ligne.

5/ On rappelle que, pour tout entier naturel n, $X_n = X_0 T^n$.

(a) Déterminer les nombres a_n, b_n, à l'aide des coefficients α_n et β_n. En déduire c_n.

(b) Déterminer les limites des suites (a_n), (b_n) et (c_n).

(c) Sur quel sommet a-t-on le plus de chance de se retrouver après un grand nombre d'itérations de cette marche aléatoire ?

Index