ODYSSÉE le Ts

MATHÉMATIQUES

ENSEIGNEMENT DE SPÉCIALITÉ

+ Site compagnon
www.odyssee-hatier.com

Hatier
www.editions-hatier.fr

NOMBRES PREMIERS INFÉRIEURS À 5000

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439
1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783
1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069
2081	2083	2087	2089	2099	2111	2113	2129	2131	2137	2141	2143
2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267
2269	2273	2281	2287	2293	2297	2309	2311	2333	2339	2341	2347
2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543
2549	2551	2557	2579	2591	2593	2609	2617	2621	2633	2647	2657
2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713
2719	2729	2731	2741	2749	2753	2767	2777	2789	2791	2797	2801
2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011
3019	3023	3037	3041	3049	3061	3067	3079	3083	3089	3109	3119
3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221
3229	3251	3253	3257	3259	3271	3299	3301	3307	3313	3319	3323
3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527
3529	3533	3539	3541	3547	3557	3559	3571	3581	3583	3593	3607
3613	3617	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697
3701	3709	3719	3727	3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989	4001	4003
4007	4013	4019	4021	4027	4049	4051	4057	4073	4079	4091	4093
4099	4111	4127	4129	4133	4139	4153	4157	4159	4177	4201	4211
4217	4219	4229	4231	4241	4243	4253	4259	4261	4271	4273	4283
4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493	4507	4513
4517	4519	4523	4547	4549	4561	4567	4583	4591	4597	4603	4621
4637	4639	4643	4649	4651	4657	4663	4673	4679	4691	4703	4721
4723	4729	4733	4751	4759	4783	4787	4789	4793	4799	4801	4813
4817	4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999			

COLLECTION ODYSSÉE

MATHÉMATIQUES Tle S

NOUVEAU PROGRAMME

Enseignement de spécialité

Sous la direction de

Éric SIGWARD

IA-IPR de mathématiques de l'académie de Strasbourg

Auteurs

François BRISOUX

Professeur de mathématiques au lycée Kirschleger de Munster

Christian BRUCKER

Professeur de mathématiques au lycée Théodore Deck de Guebwiller

Frédéric LÉON

Professeur de mathématiques au lycée Emily Brönte de Lognes

Nadine MEYER

Professeur de mathématiques au lycée Marguerite Yourcenar d'Erstein

Didier REGHEM

Professeur de mathématiques au lycée Marguerite de Flandre de Gondecourt

Christophe ROLAND

Professeur de mathématiques au lycée Pasteur de Hénin-Beaumont

Matthieu SCHAVSINSKI

Professeur de mathématiques au lycée Emilie du Châtelet de Serris

Hatier

AVANT-PROPOS

Ce manuel consacré à l'enseignement de spécialité de mathématiques des terminales scientifiques répond aux orientations des nouveaux programmes, qui mettent en avant la résolution de problèmes. Cette approche est mise en œuvre en particulier :

- Dans les Activités d'exploration, au cours desquelles le vocabulaire, les propriétés et certains théorèmes peuvent être introduits directement dans la situation étudiée. Le Cours qui suit ces activités reprend de façon plus formelle les notions qui sont alors illustrées par des exemples et souvent démontrées.
- Dans la rubrique Activités de recherche et résolution de problèmes : elle contient des problèmes qui mettent les élèves en situation de recherche sur les thèmes classiques d'arithmétique et d'algèbre linéaire. La résolution de ces problèmes suppose connue la théorie de base correspondante mais introduit également d'autres théorèmes dans des situations concrètes. On y retrouve, entre autres, les thèmes donnés à titre indicatif dans les programmes officiels. Ces différents problèmes font largement appel aux outils informatiques : tableurs, logiciel de géométrie dynamique, logiciel de calcul formel. La démarche algorithmique, enfin, est présente dans de nombreuses situations.

Les Savoir-faire aident les élèves à résoudre les Exercices d'application, pour ancrer quelques points de méthodes générales.

Enfin les pages OBJECTIF BAC qui terminent le chapitre permettent de s'entraîner à résoudre des exercices type Bac, un Sujets type BAC Exercice résolu détaillant la méthode de résolution attendue à l'examen.

Nous proposons ainsi aux élèves un manuel qui favorise un travail actif, méthodique dans lequel, avec l'aide de leur professeur, ils trouveront les éléments essentiels pour réussir l'épreuve du baccalauréat et les préparer à la poursuite d'études scientifiques.

Les auteurs

SOMMAIRE

PROGRAMME DE LA CLASSE DE T^le S ENSEIGNEMENT DE SPÉCIALITÉ (EXTRAITS)

Bulletin officiel spécial n° 8 du 13 octobre 2011.

Arithmétique

Exemples de problèmes	Contenus
Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee) Problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill). Questionnement sur les nombres premiers : infinitude, répartition, tests de primalité, nombres premiers particuliers (Fermat, Mersenne, Carmichaël). Sensibilisation au système cryptographique RSA.	• Divisibilité dans $\mathbb{Z}$ • Division euclidienne. • Congruences dans $\mathbb{Z}$. • PGCD de deux entiers. • Entiers premiers entre eux. • Théorème de Bézout. • Théorème de Gauss. • Nombres premiers. • Existence et unicité de la décomposition en produit de facteurs premiers.

Matrices et suites

Exemples de problèmes	Contenus
Marche aléatoire simple sur un graphe à deux ou trois sommets. Marche aléatoire sur un tétraèdre ou sur un graphe à N sommets avec saut direct possible d'un sommet à un autre : à chaque instant, le mobile peut suivre les arêtes du graphe probabiliste ou aller directement sur n'importe quel sommet avec une probabilité constante p . Étude du principe du calcul de la pertinence d'une page web. Modèle de diffusion d'Ehrenfest : N particules sont réparties dans deux récipients ; à chaque instant, une particule choisie au hasard change de récipient. Modèle proie prédateur discrétisé : – évolution couplée de deux suites récurrentes ; – étude du problème linéarisé au voisinage du point d'équilibre.	• Matrices carrées, matrices colonnes : opérations. • Matrice inverse d'une matrice carrée. • Exemples de calcul de la puissance n-ième d'une matrice carrée d'ordre 2 ou 3. • Écriture matricielle d'un système linéaire. • Suite de matrices colonnes (U_n) vérifiant une relation de récurrence du type $U_{n+1} = AU_n + C$: – recherche d'une suite constante vérifiant la relation de récurrence ; – étude de la convergence. • Étude asymptotique d'une marche aléatoire.

PARTIE A

ARITHMÉTIQUE

L'arithmétique – tapisserie vers 1520, Musée du Moyen Âge, Paris.

INTRODUCTION

« La Mathématique est la reine des sciences et l'Arithmétique est la reine des mathématiques. »
Carl Friedrich Gauss (1777-1855)

Arithmétique
Branche des mathématiques qui étudie les propriétés élémentaires des nombres entiers et rationnels.
Petit Larousse illustré 2011

L'arithmétique est certainement de loin la plus ancienne des sciences. Voilà près de 30 000 ans que l'homme a commencé à compter ses moutons, ses cueillettes, les fruits de sa pêche. Puis vint le temps de représenter ces nombres pour les communiquer, pour commercer, pour gérer ses stocks de nourriture.
De nombreux systèmes de numération ont vu le jour dans le monde entier : des Incas aux Babyloniens en passant par les Indiens ou les Égyptiens.
Des systèmes très différents et plus ou moins performants se sont succédés jusqu'au nôtre. Leur évolution, ou leur extinction, dépendait des invasions mais aussi de leur efficacité. En effet, compter ne suffit plus, il faut pouvoir additionner, multiplier, soustraire, ...et tous les systèmes de numération ne sont pas égaux.

Les os D'Ishango : probablement la plus ancienne trace de comptage retrouvée en Afrique (20 000 ans). Les encoches faites sur ces os ont de nombreuses propriétés arithmétiques laissant à penser qu'elles ne sont pas là par hasard.
Ces os sont probablement les vestiges d'une table de calcul ou de calendrier lunaire.

Mais quel que soit le système de représentation des nombres choisi, ces derniers ont des propriétés utilisées depuis des millénaires (pourrais-je léguer mon troupeau à mes trois fils équitablement?) et toujours incontournables de nos jours (le paiement par carte bancaire utilise le système de cryptage RSA qui dépend de deux nombres entiers secrets choisis pour leurs propriétés bien particulières...).

Axiome
1. Vérité non démontrable qui s'impose avec évidence.
2. En mathématiques et en logique : proposition première, vérité admise sans démonstration et sur laquelle se fonde une science, un raisonnement ; principe posé hypothétiquement à la base d'une théorie déductive.
Petit Larousse illustré 2011

« L'axiome est l'atome du raisonnement »
Victor Hugo (1802–1885)

L'étude de l'arithmétique repose donc sur la seule connaissance des nombres entiers mais aussi sur un élément de raisonnement nécessaire pour démontrer de nombreuses propriétés : **un axiome.**
Un axiome est donc un principe incontournable qu'on ne peut justifier que par le bon sens, et sur lequel on peut s'appuyer pour démontrer un résultat.
L'arithmétique est construite en admettant l'axiome suivant :

AXIOME DU PLUS PETIT ÉLÉMENT

Tout ensemble non vide d'entiers naturels admet un plus petit élément.

Ainsi l'ensemble des multiples communs de 4 et 6 possède un plus petit élément, 12.
Cet axiome n'est vrai que pour un ensemble d'entiers naturels.
L'ensemble des multiples de 2, par exemple, n'admet pas de plus petit élément car il contient aussi les nombres -2, -4, -6, etc. L'ensemble $]2\,;\,5[$ n'admet pas non plus de plus petit élément.
On peut énoncer en conséquence de cet axiome, la propriété suivante :

PRINCIPE DE DESCENTE INFINIE

Il n'existe pas de suite strictement décroissante d'entiers naturels.

Ce principe permet, entre autres, de garantir que des procédés algorithmiques (comme l'algorithme de recherche du PGCD de deux nombres) se terminent toujours.

1 Divisibilité dans $\mathbb{Z}$, division euclidienne, congruences

En coupant la pomme en deux, puis en quatre, puis en douze, on est assuré que les quartiers ont la même taille.
En fixant la taille des quartiers avant de couper, il se peut que le dernier quartier soit plus petit que les autres : c'est le reste.

Le chapitre en bref

Réinvestir

- La notion de diviseur
- La division euclidienne

Explorer

- Les propriétés des diviseurs
- La notion de congruence

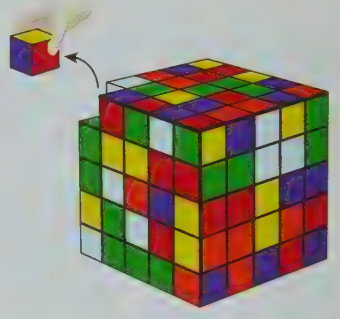
Activités de recherche p. 21

Activités d'exploration

1 Des paquets de cubes

Explorer : La notion de diviseur.

Un cube est constitué de n^3 petits cubes identiques, où n est un entier supérieur ou égal à 2.
On lui enlève un petit cube et on souhaite regrouper les petits cubes restants en plusieurs paquets identiques.



1. Vérifier qu'un tel regroupement n'est pas possible pour $n = 2$.
2. On suppose $n > 2$.
   a. Vérifier que $8^3 - 1$ est divisible par 7.
   b. Vérifier que $23^3 - 1$ est divisible par 22.
3. **a.** Conjecturer un diviseur de $n^3 - 1$ pour un entier n quelconque.
   b. Démontrer cette conjecture.
   c. En déduire en fonction de n deux nombres de paquets de petits cubes possibles.

COUP DE POUCE

Pour montrer que a divise b, il suffit de trouver une écriture de la forme $b = ka$ avec k un entier.

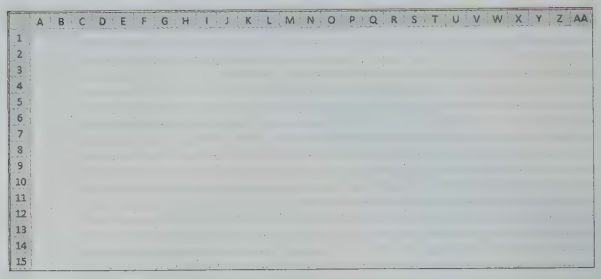
La propriété rencontrée dans l'activité

On dit que l'entier relatif a **divise** l'entier relatif b s'il existe un entier relatif k tel que $b = ka$.
On dit aussi que a est un **diviseur** de b ou que b est **divisible** par a.
b est alors un **multiple** de a.

2 Format de tableau

Réinvestir : Faire la liste des diviseurs d'un entier.

Sur un tableur, un tableau est composé de lignes et de colonnes.



1. Pour que ce tableau comporte 35 cases, déterminer les nombres de lignes possibles.
2. Pour que ce tableau comporte 48 cases, déterminer les nombres de lignes possibles.
3. On souhaite désormais construire un tableau de n cases.
   a. Proposer deux valeurs de n telles qu'il y ait exactement trois façons de construire le tableau, c'est-à-dire trois valeurs distinctes du nombre de lignes possibles.
   b. Quelle condition est nécessaire sur n pour qu'il y ait un nombre impair de façons de construire le tableau. Justifier.
   c. Proposer une valeur de n telle qu'il y ait exactement cinq façons de construire le tableau.

3 Un diviseur étonnant

Explorer : Les propriétés des diviseurs.

1. Montrer que les nombres suivants sont divisibles par 37 :
   - **a.** Les nombres formés de trois chiffres identiques.
   - **b.** Les nombres formés de six chiffres identiques.
   - **c.** Les nombres formés de six chiffres par duplication d'un nombre à deux chiffres (comme 474747).
2. En déduire que $333^{777} - 777^{333}$ est divisible par 37.

COUP DE POUCE

- Tester les propositions sur des exemples.
- Identifier un diviseur commun pour chaque famille de nombres proposée.
- Pour la question 2, on peut montrer que l'expression se factorise par 37.

Les propriétés rencontrées dans l'activité

- Soit a, b et c trois entiers relatifs. Si a divise b et b divise c, alors a divise c.
- Soit a et b deux entiers. Si d est un diviseur commun de a et b, alors d divise toute combinaison linéaire de a et b, c'est-à-dire tout nombre de la forme $au + bv$ où u et v sont des entiers.

VERS LE COURS
• Démonstrations proposées, p. 12.

4 Une division avec un reste

Réinvestir : La division euclidienne.

En athlétisme, le 3 000 mètres steeple se court sur une piste de 390 mètres de long passant par le saut d'une rivière.

1. À quelle distance avant la ligne d'arrivée doit-on positionner la ligne de départ ?
2. Lors d'un championnat de France, la vitesse moyenne du vainqueur était de 6 $m.s^{-1}$. Quel temps a-t-il réalisé, exprimé en minutes et secondes ?

La notion rencontrée dans l'activité

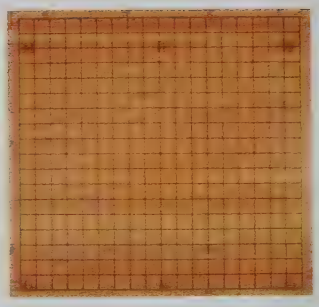
Soit a un entier relatif et b un entier naturel non nul.
Il existe un unique couple d'entiers $(q ; r)$ tels que $a = bq + r$ avec $0 \leqslant r < b$.
Cette écriture s'appelle la division euclidienne de a par b, q est le quotient et r le reste de cette division euclidienne.

VERS LE COURS
Démonstration proposée, p. 13.

5 Des restes impossibles

Réinvestir : Démonstration par disjonction de cas.

Un damier a autant de lignes que de colonnes.
Toutes les cases seront occupées par un et un seul jeton.
En distribuant autant de jetons à chacun des 5 joueurs, Mickaël se rend compte qu'il lui reste 3 jetons à distribuer.
« Impossible ! dit Laura, tu t'es forcément trompé en distribuant. »
Que penser de l'affirmation de Laura ?



1. Justifier qu'il existe un entier naturel n tel que le nombre total de jetons $N = n^2$.

2. Traduire la problématique de la question à l'aide d'une division euclidienne.

3. Avec la calculatrice, construire une table de valeurs des restes de n^2 dans la division euclidienne par 5 et conjecturer une réponse au problème.

4. Démontrer le résultat général.

COUP DE POUCE

3 Sur la calculatrice, le reste peut s'obtenir en calculant la partie décimale d'un quotient avec une fonction **partdéc**, puis en la multipliant par le diviseur (ex. : **partdéc**(38/5)×5 = 3).

4 On peut justifier que, pour tout entier n, il existe un entier p tel que :

$n = 5p$ ou $n = 5p + 1$ ou $n = 5p + 2$
ou $n = 5p + 3$ ou $n = 5p + 4$.

6 Mêmes restes

Explorer : La notion de congruences.

1. Déterminer le reste dans la division euclidienne par 11 de 608 et 487.

2. En déduire sans effectuer les calculs que 608 – 487 est divisible par 11. Vérifier ce résultat.

3. Plus généralement, soit a, b et n des entiers naturels, n étant non nul.
Montrer que si a et b ont même reste dans la division euclidienne par n, alors $a - b$ est divisible par n.

4. On admet que, réciproquement, si $a - b$ est divisible par n, alors a et b ont même reste dans la division euclidienne par n.
a. En déduire que 9^{22} et 9^{20} ont le même chiffre des unités.
b. Montrer de même que $7^{1\,004}$ et $7^{1\,000}$ ont le même chiffre des unités et des dizaines.

COUP DE POUCE

- Effectuer la différence et en chercher un diviseur.
- Le chiffre des unités est le reste dans la division euclidienne par 10.

VERS LE COURS
Démonstration proposée, p. 14.

Les notions rencontrées dans l'activité

- Soit n est un entier naturel non nul.
Deux entiers a et b sont dit **congrus modulo** n lorsque que $a - b$ est divisible par n.

- Soit n un entier naturel non nul. Deux entiers a et b sont congrus modulo n, si et seulement si, ils ont même reste dans la division euclidienne par n.
On le note $\boldsymbol{a \equiv b}$ $\boldsymbol{[n]}$. On lira « a est congru à b modulo n ».

7 De beaux restes

Explorer : Les opérations sur les restes.

Pour engazonner un stade rectangulaire, on le recouvre de plaques de gazon carrées livrées par paquets de 12 plaques. Le jardinier n'entame un paquet que lorsque le précédent est fini.

1 En réalisant une ligne en suivant la longueur du terrain, il lui reste 7 plaques sur le dernier paquet entamé.

a. Quel est le reste dans la division euclidienne par 12 du nombre L de plaques utilisées ?

b. Au bout de 2 lignes, combien reste-t-il de plaques sur le dernier paquet entamé ?

c. Au bout de 17 lignes, combien reste-t-il de plaques sur le dernier paquet entamé ?

COUP DE POUCE

• On peut écrire la division euclidienne par 12 de L et ℓ, puis exprimer les quantités $2L$, $17L$ et $L \times \ell$.

2 S'il avait suivi la largeur du terrain, en réalisant une ligne, il lui serait resté 2 plaques sur le dernier paquet entamé.

a. Quel est le reste dans la division euclidienne par 12 du nombre ℓ de plaques utilisées ?

b. Combien reste-t-il de plaques sur le dernier paquet entamé lorsque le terrain est entièrement engazonné ?

3 En utilisant les congruences, vérifier que l'on obtient les mêmes résultats en effectuant les calculs précédents uniquement sur les restes de L et ℓ dans la division euclidienne par 12.

COUP DE POUCE

• Avec les congruences :

si $L \equiv 5$ [12], alors $17L \equiv 17 \times 5$ [12],

on peut ensuite déterminer le reste de 17×5.

VERS LE COURS
Démonstrations proposées, p. 14.

Les notions rencontrées dans l'activité

Soit a et b deux entiers relatifs et n est un entier naturel non nul.

On note r et r' les restes respectifs de a et b dans la division euclidienne par n (en particulier $a \equiv r$ [n] et $b \equiv r'$ [n]).

On a alors les congruences suivantes :

- $a + b \equiv r + r'$ [n]
- $a - b \equiv r - r'$ [n]
- $a \times b \equiv r \times r'$ [n]
- $a^k \equiv r^k$ [n] quel que soit $k \in \mathbb{N}$

A. Divisibilité dans $\mathbb{Z}$

DÉFINITION

On dit que l'entier relatif a **divise** l'entier relatif b lorsqu'il existe un entier relatif k tel que $b = ka$.
On dit aussi que a est un **diviseur** de b ou que b est **divisible** par a.
b est alors un **multiple** de a.

REMARQUE

Tout entier relatif a possède au moins quatre diviseurs : 1, -1, a et $-a$. En outre, un entier relatif non nul possède un nombre fini de diviseurs compris entre $-a$ et a.
0 est un cas particulier car 0 possède une infinité de diviseurs : tous les entiers relatifs non nuls.

PROPRIÉTÉ

Soit a, b et c trois entiers relatifs.
Si a divise b et b divise c, alors a divise c.

▶ Savoir-faire 1
Déterminer la liste des diviseurs positifs d'un entier naturel, p. 15

DÉMONSTRATION

Si a divise b et b divise c, alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.
On en déduit que $c = k' \times (ka) = (k'k) \times a$.
c est donc un multiple de a, d'où a divise c. ■

EXEMPLES

a) 7 divise 63 et 63 divise 6 300, donc 7 divise 6 300.
b) 3 divise 6 et 6 divise 6^7, donc 3 divise 6^7.

REMARQUE

La contraposée de cette propriété sera bien utile pour établir la liste des diviseurs d'un entier (voir **Savoir-Faire 1**). En effet, si b ne divise pas a, aucun multiple de b ne peut diviser a car sinon, comme b divise kb, si kb divise a alors b diviserait a.
Par exemple, comme 2 ne divise pas 1 001, on est assuré qu'aucun nombre pair ne divise 1 001. En effet, si 4 divisait 1 001, alors 2 diviserait 1 001.
Cette remarque permet ici de limiter la recherche des diviseurs de 1 001 aux seuls nombres impairs.

PROPRIÉTÉ

Soit a, b et d trois entiers relatifs.
Si d divise a et b, alors d divise toute combinaison linéaire de a et b, de la forme $au + bv$ où u et v sont des entiers.

DÉMONSTRATION

Si d est un diviseur commun de a et b, il existe deux entiers relatifs k et k' tels que $a = kd$ et $b = k'd$.
$au + bv$ est une combinaison linéaire de a et b, avec u et v des entiers. On a :

$$au + bv = kdu + k'dv = (ku + k'v) \times d.$$

$au + dv$ est donc un multiple de d, d'où d divise $au + bv$. ■

▶ Savoir-faire 2
Justifier qu'un entier divise ou non une expression numérique, p. 15

EXEMPLE

Comme 3 divise 3^n et 21, alors 3 divise $3^n - 21$ pour tout entier naturel n.

B. Division euclidienne

PROPRIÉTÉ ET DÉFINITION

Soit a un entier relatif et b un entier naturel non nul. Il existe un unique couple d'entiers $(q\,;\,r)$ tels que $a = bq + r$ avec $0 \leqslant r < b$.

Cette écriture s'appelle la **division euclidienne de** a par b, q est le **quotient** et r le **reste** de cette division euclidienne.

DÉMONSTRATION

1. Existence

- **Cas où a est positif**

Soit $\mathscr{E}$ l'ensemble des entiers naturels m tels que $mb > a$. Comme $b \geqslant 1$, $(a+1) \times b \geqslant a+1 > a$ d'où $a+1$ appartient à $\mathscr{E}$ qui est donc un ensemble non vide.

D'après l'axiome du plus petit élément, il existe un entier m_0, plus petit élément de $\mathscr{E}$, tel que $(m_0 - 1) \times b \leqslant a < m_0 \times b$.

En notant $q = (m_0 - 1)$ et $r = a - bq$, on a bien $a = bq + r$ et $0 \leqslant r < b$.

En effet, comme $(m_0 - 1) \times b \leqslant a < m_0 \times b$, on a alors $(m_0 - 1) \times b - bq \leqslant a - bq < m_0 \times b - bq$, ce qui, en simplifiant, équivaut à $0 \leqslant r < b$.

- **Cas où a est négatif**

On considère le nombre $-a$ qui est positif. Il existe donc deux entiers naturels q et r tels que $-a = bq + r$ avec $0 \leqslant r < b$ d'après le cas étudié précédemment.

On en déduit que $a = b \times (-q) - r$.

Si $r = 0$, alors $a = b \times (-q)$, et $-q$ est le quotient.

Si $r > 0$, alors $a = b \times (-q) - r = b \times (-q - 1) + (b - r)$. Comme $0 < r < b$ alors, avec $0 < b - r < b$, et par extension $0 \leqslant b - r < b$.

En notant $q' = -q - 1$ et $r' = b - r$, on a bien $a = bq' + r'$ avec $0 \leqslant r' < b$.

2. Unicité

On suppose qu'il existe deux couples $(q\,;\,r)$ et $(q'\,;\,r')$ qui vérifient la propriété.

On a $a = bq + r = bq' + r'$, d'où $b \times (q - q') = r' - r$.

Comme $0 \leqslant r < b$, alors $-b < -r \leqslant 0$, et comme on sait que $0 \leqslant r' < b$, on obtient, par addition, l'encadrement $-b < r' - r < b$. Or $r' - r = b \times (q - q')$ est un multiple de b compris strictement entre $-b$ et b, il ne peut s'agir que de 0.

Par suite $r' - r = 0$ d'où $r = r'$. D'autre part, $b \times (q - q') = 0$, d'où $q = q'$.

En conclusion, le couple $(q\,;\,r)$ vérifiant la propriété est unique. ■

EXEMPLE

Dans la division euclidienne par 17, on a $328 = 17 \times 19 + 5$ et $-328 = 17 \times (-20) + 12$.

NOTE
Voir définition de l'axiome, p. 6.

▶ Savoir-faire 3
Déterminer le quotient et le reste d'une division euclidienne, p. 16

C. Congruences

DÉFINITION

Soit n un entier naturel non nul.
Deux entiers a et b sont dit **congrus modulo n** lorsque $a - b$ est divisible par n.

PROPRIÉTÉ

Soit n un entier naturel non nul.
Deux entiers a et b sont congrus modulo n si, et seulement si, ils ont **même reste** dans la division euclidienne par n. On note $a \equiv b\ [n]$ et on lit « a est congru à b modulo n ».

DÉMONSTRATION

On note $a = nq + r$ et $b = nq' + r'$ les divisions euclidiennes de a et b par n.

- **On suppose que $r = r'$.**

$a - b = nq + r - (nq' + r) = n \times (q - q')$ est un multiple de n , d'où a et b sont congrus modulo n.

- **On suppose que a et b soient congrus modulo n.**

$a - b = nq + r - (nq' + r') = n \times (q - q') + r - r'$. On en déduit que $r - r' = a - b - n \times (q - q')$.
Puisque a et b sont congrus modulo n, la différence $a - b$ est divisible par n et par suite :
$r - r' = a - b - n \times (q - q')$ est divisible par n.
Comme $0 \leqslant r < n$, alors $-n < -r \leqslant 0$, et comme $0 \leqslant r' < n$, on obtient, par addition, l'encadrement $-n < r' - r < n$.
Or $r' - r$ est un multiple de n compris strictement entre $-n$ et n, il ne peut s'agir que de 0.
D'où $r - r' = 0$, c'est-à-dire $r = r'$.

EXEMPLE

$19 \equiv 11\ [4]$ car $19 - 11 = 8$ est divisible par 4. On peut vérifier que 19 et 11 ont le même reste dans la division euclidienne par 4 : $19 = 4 \times 4 + 3$ et $11 = 4 \times 2 + 3$.

PROPRIÉTÉS

Soit n un entier naturel non nul.
Si a, b, r, et r' sont des entiers relatifs tels que $a \equiv r\ [n]$ et $b \equiv r'\ [n]$, on a les relations :

- $a + b \equiv r + r'\ [n]$
- $a - b \equiv r - r'\ [n]$
- $a \times b \equiv r \times r'\ [n]$
- $a^k \equiv r^k\ [n]$ quel que soit $k \in \mathbb{N}$

DÉMONSTRATIONS

$a \equiv r\ [n]$ et $b \equiv r'\ [n]$ équivaut à $a - r$ et $b - r'$ sont deux multiples de n.
On en déduit que toute combinaison linéaire de ces deux nombres est multiple de n, d'où :
$(a - r) + (b - r') = (a + b) - (r + r')$ est multiple de n, ce qui équivaut à $a + b \equiv r + r'\ [n]$;
$(a - r) - (b - r') = (a - b) - (r - r')$ est multiple de n, ce qui équivaut à $a - b \equiv r - r'\ [n]$;
$(a - r) \times b + (b - r') \times r = a \times b - b \times r + b \times r - r \times r' = a \times b - r \times r'$ est multiple de n, ce qui équivaut à $a \times b \equiv r \times r'\ [n]$.
k étant un entier naturel, on démontre le dernier résultat par récurrence sur k à l'aide de la propriété sur le produit : $a \times b \equiv r \times r'\ [n]$.
La propriété $a^k \equiv r^k\ [n]$ est vraie pour $k = 0$ et $k = 1$ de manière évidente. On suppose qu'elle soit vraie pour un entier $k > 0$. Comme $a^k \equiv r^k\ [n]$, alors $a^{k+1} \equiv a \times a^k \equiv r \times r^k \equiv r^{k+1}\ [n]$ et la propriété est vraie au rang $k + 1$.
En conclusion, on a montré par récurrence que $a^k \equiv r^k\ [n]$ pour tout $k \in \mathbb{N}$.

EXEMPLE

$59 \equiv 3\ [7]$ et $48 \equiv 6\ [7]$. On en déduit que $59 + 48 \equiv 3 + 6\ [7]$ et, par suite, que $59 + 48 \equiv 2\ [7]$.
De même, on a $59 \times 48 \equiv 3 \times 6\ [7]$ d'où $59 \times 48 \equiv 18 \equiv 4\ [7]$.

▶ Savoir-faire 4
Déterminer un reste dans une division euclidienne à l'aide des congruences, p. 16

▶ Savoir-faire 5
Justifier à l'aide des congruences qu'un entier divise une expression. p. 16

Savoir-faire

Savoir-faire 1 — Déterminer la liste des diviseurs positifs d'un entier naturel

ÉNONCÉ Déterminer la liste des diviseurs de 90.

SOLUTION

On teste les entiers dans l'ordre croissant pour déterminer les diviseurs entiers de 90 :

$90 \div 1 = 90$

$90 \div 2 = 45$

$90 \div 3 = 30$

$90 \div 4 = 22{,}5$

$90 \div 5 = 18$

$90 \div 6 = 15$

$90 \div 7 \approx 12{,}8$

Il est inutile de tester la divisibilité par 8.

$90 \div 9 = 10$

On a déterminé la liste des couples de diviseurs :

(1 ; 90), (2 ; 45), (3 ; 30), (5 ; 18), (6 ; 15), (9 ; 10),

d'où l'ensemble des diviseurs :

$\mathcal{D} = \{1 ; 2 ; 3 ; 5 ; 6 ; 9 ; 10 ; 15 ; 18 ; 30 ; 45 ; 90\}$.

MÉTHODE

On teste les entiers dans l'ordre croissant en commençant par 1.

Pour économiser le nombre de calcul, on peut s'appuyer sur la propriété que si k ne divise pas n, aucun multiple de k ne divise n. Ici 4 ne divisant pas 90, il est inutile de tester les multiples de 4.

De plus, lorsqu'on trouve un diviseur de n, on trouve aussi son diviseur associé $\frac{n}{k}$. Lorsque le diviseur testé k est supérieur au quotient $\frac{n}{k}$, on a alors la garantie d'avoir trouvé tous les diviseurs de n.

Exercices 1 à 4 p. 17

Savoir-faire 2 — Justifier qu'un entier divise ou non une expression numérique

ÉNONCÉ **a.** Montrer que $15p - 3q^2$ est divisible par 3 pour tout p et q entiers relatifs.

b. Montrer que $3n + 7$ n'est jamais divisible par 3 quel que soit l'entier naturel n.

c. L'entier $n^2 - n + 3$ est-il divisible par 3 pour tout entier naturel n ?

SOLUTION

a. $15p - 3q^2 = 3 \times (5p - q^2)$. Comme p et q sont des entiers, $5p - q^2$ l'est aussi et $15p - 3q^2$ est alors divisible par 3.

b. Si $3n + 7$ était divisible par 3, alors il existerait un entier relatif k tel que $3n + 7 = 3k$. On en déduirait que $7 = 3k - 3n = 3 \times (k - n)$, c'est-à-dire que 3 divise 7, ce qui absurde, donc 3 ne divise pas $3n + 7$.

c. Pour $n = 2$, l'expression $n^2 - n + 3 = 5$ n'est donc pas divisible par 3 pour tout entier naturel n.

MÉTHODE

a. Pour montrer qu'un nombre est divisible par 3, il suffit de montrer que l'on peut factoriser par 3.

b. On utilise un raisonnement par l'absurde pour montrer qu'une propriété est toujours fausse.

c. On utilise un contre-exemple.

Exercices 5 à 12 p. 17

Savoir-faire 3 — Déterminer le quotient et le reste d'une division euclidienne

ÉNONCÉ Déterminer le quotient et le reste dans la division euclidienne par 23 de 10 000 et de – 10 000.

SOLUTION

$10\,000 = 23 \times 434 - 18$.

Le quotient est 434 et le reste est 18.

On sait que $-10\,000 = 23 \times (-434) - 18$.

Pour que le reste soit positif, on écrit :

$-10\,000 = 23 \times (-434) - 23 + 23 - 18$

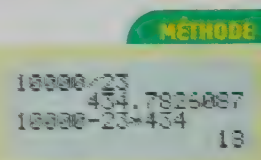
$= 23 \times (-435) + 5$

Le quotient est – 435 et le reste est 5.

→ Exercices 14 à 19 p. 17

MÉTHODE

Le quotient de l'entier naturel a par l'entier naturel b est donné par la partie entière de a/b.



Le reste peut alors se calculer à l'aide de la relation $r = a - bq$.

Lorsque a est négatif, on adaptera le calcul précédent selon la méthode décrite dans la démonstration vue dans le cours, p. 13.

Savoir-faire 4 — Déterminer à l'aide des congruences un reste dans une division euclidienne

ÉNONCÉ Déterminer le reste dans la division euclidienne par 7 de 25×2^{17}.

SOLUTION

$25 \times 2^{17} \equiv 4 \times 2^{17}$ [7]

$\equiv 4 \times 2^{3 \times 5 + 2}$ [7]

$\equiv 4 \times (2^3)^5 \times 2^2$ [7]

$\equiv 4 \times (8)^5 \times 4$ [7]

$\equiv 4 \times (1)^5 \times 4$ [7]

$\equiv 16$ [7]

$\equiv 2$ [7]

Le reste dans la division euclidienne par 7 de 25×2^{17} est 2.

→ Exercices 30 à 32 p. 18

MÉTHODE

Pour déterminer le reste, on utilise ici les congruences des produits et des puissances jusqu'à ce que le terme obtenu soit compris entre 0 et 6.

Pour déterminer une congruence d'une puissance de 2 modulo 7, il faut chercher la plus petite puissance de 2 supérieure à 7, ici $2^3 = 8$.

On effectue alors la division euclidienne de 17 par 3 pour faire apparaître les termes 2^3 qui seront congrus ici à 1 modulo 7.

Savoir-faire 5 — Justifier à l'aide des congruences qu'un entier divise une expression

ÉNONCÉ Montrer que, pour tout entier n, $7^n - 3^n - 2$ est divisible par 4.

SOLUTION

$7^n - 3^n - 2 \equiv (-1)^n + (-1)^n + 2$ [4]

$\equiv 2 \times (-1)^n + 2$ [4]

Si n est pair :

$7^n + 3^n + 2 \equiv 2 \times 1 + 2 \equiv 4 \equiv 0$ [4]

Si n est impair :

$7^n + 3^n + 2 \equiv 2 \times (-1) + 2 \equiv 0$ [4]

Dans tous les cas, $7^n + 3^n + 2$ est divisible par 4.

→ Exercices 33 à 36 p. 19

MÉTHODE

Pour montrer qu'un nombre est divisible par 4, il suffit de montrer que son reste est 0 dans la division euclidienne par 4, c'est-à-dire que ce nombre est congru à 0 modulo 4.

$7^n \equiv (3)^n$ [4] ; mais ce résultat n'est pas aussi exploitable que $7^n \equiv (-1)^n$ [4] qui donne directement les deux valeurs possibles du reste.

Il est ainsi toujours plus intéressant de se ramener à des nombres congrus à 1 ou à – 1 avant de les élever à une puissance car les résultats peuvent être déterminés quel que soit l'exposant.

Exercices d'application

Divisibilité dans $\mathbb{Z}$

1 Déterminer les diviseurs des nombres suivants :
a. 54 **b.** 144 **c.** 200

Savoir-faire 1, p. 15

2 **a.** Déterminer la liste des diviseurs de 100.
b. En déduire la liste des diviseurs de 700.

3 **a.** Déterminer les diviseurs de 21.
b. Montrer, sans la résoudre, que l'équation $n(n+2) = 21$ n'a pas de solution dans $\mathbb{N}$.
c. Résoudre dans $\mathbb{N}$ l'équation $(n^2-1)(n^3-1) = 21$.

4 Déterminer tous les couples d'entiers naturels a et b tels que $a^2 - b^2 = 28$.

5 a, b et c sont des entiers non nuls.
Montrer que si a divise b et c, alors a^2 divise bc.

Savoir-faire 2, p. 15

6 **1.** Montrer que si n est pair, alors n^2 est pair.
2. Montrer que si n est impair, alors n^2 est impair.
3. En déduire que $n^2 - n$ est divisible par 2 pour tout entier naturel n.

7 **1.** Montrer que la somme de trois entiers consécutifs est divisible par 3.

COUP DE POUCE

On pourra noter n le plus petit de ces entiers et écrire la somme en fonction de n.

2. Montrer de même que la somme de cinq entiers consécutifs est divisible par 5 et que la somme de sept entiers consécutifs est divisible par 7.
3. Montrer que la somme de six entiers consécutifs n'est jamais divisible par 6.
4. Plus généralement, on étudie la somme de k entiers consécutifs en notant n le plus petit d'entre eux.
a. Réduire cette somme à l'aide des suites arithmétiques.
b. Montrer que cette somme est divisible par k si et seulement si k est impair.

8 **1.** Montrer que pour tout entier n, $51n + 4$ n'est pas divisible par 17.
2. En déduire un nombre compris entre 3 000 et 3 100 non divisible par 17.

9 n est un entier naturel. On veut déterminer n tel que $n^2 + 18$ soit divisible par 19.
1. À l'aide de la **calculatrice**, construire une table de valeur permettant de conjecturer une réponse.
2. En factorisant $n^2 - 1$, montrer que si $n - 1$ est divisible par 19, $n^2 + 18$ le sera aussi.
3. Montrer de même que si $n + 1$ est divisible par 19, $n^2 + 18$ le sera aussi.
4. Retrouver les conjectures établies à la question **1**.

10 On veut montrer que le produit de trois entiers consécutifs est divisible par 6.
1. Justifier que l'un des termes est divisible par 3.
2. Montrer alors que si ce terme n'est pas divisible par 6, l'un des deux autres termes est divisible par 2.
3. Conclure en raisonnant par disjonction de cas.

11 On cherche l'ensemble des entiers relatifs non nuls n tels que $n + 1$ divise $n + 13$.
1. Déterminer une combinaison linéaire de $n + 1$ et $n + 13$ indépendante de n.
2. Montrer que $n + 1$ divise cette combinaison linéaire.
3. Déterminer les valeurs de n qui conviennent.

12 n est un entier naturel non nul.
1. À l'aide d'une factorisation, déterminer trois diviseurs de $n^4 - 1$.
2. En déduire trois diviseurs de 9 999.

Division euclidienne

13 L'écriture $434 = 23 \times 18 + 20$ est une division euclidienne.
Identifier le dividende, le diviseur, le quotient et le reste.

14 **a.** Déterminer le quotient et le reste dans la division euclidienne par 17 de 500.
b. En déduire le quotient et le reste dans la division euclidienne par 17 de -500.

Savoir-faire 3, p. 15

15 **1.** L'égalité $6\,489 = 72 \times 89 + 81$ peut-elle traduire une division euclidienne ? Préciser le diviseur.
2. Même question avec l'égalité $-6\,489 = (-72) \times 89 - 81$.

16 Déterminer le nombre de multiples de 13 compris entre -300 et 300.

17 b est un entier naturel non nul.
En divisant 250 par b, il reste 3 et en divisant -250 par b, il reste 10. Identifier b.

18 b est un entier naturel non nul.
En divisant 250 par b, il reste 7 et en divisant 500 par b, il reste 5. Identifier b.

19 **a.** Quels sont les entiers naturels qui divisés par 5 ont un quotient égal au reste ?
b. Quels sont les entiers naturels qui divisés par 5 ont un reste égal au dividende ?

20 a et b désignent deux entiers naturels avec $a > b$.
Dans la division euclidienne de a par b, le quotient est q et le reste r. On sait que $a + b = 86$ et que $r = 9$.
Déterminer les couples $(a ; b)$ possibles.

21 *Vrai/Faux.* Justifier.
On note q et r le quotient et le reste de la division euclidienne de a par b.
a. Le reste dans la division euclidienne de $2a$ par b est $2r$.
b. Le quotient dans la division euclidienne de $2a$ par b est $2q$.
c. Le reste dans la division euclidienne de a par q est r.
d. Le reste dans la division euclidienne de $-a$ par b est $b - r$.

22 La Terre tourne autour du Soleil en 31 556 952 secondes.

Donner ce temps en jours, heures, minutes et secondes.

23 Donner la mesure principale de l'angle donné en radian par :
a. $\frac{427\pi}{3}$ **b.** $\frac{1\,277\pi}{6}$
Rappel : La mesure principale d'un angle est celle appartenant à l'intervalle $]-\pi ; \pi]$.

24 Dans une classe de plus de 10 enfants, le maître distribue autant de gommettes rouges à chaque enfant.
Sa plaque contient 120 gommettes et il ne lui en reste qu'une à la fin de sa distribution.
Combien y a-t-il d'enfants ?

25 Déterminer suivant les valeurs de n le reste dans la division euclidienne par n de :
a. $5n + 3$ **b.** $n^2 + 3n + 4$

COUP DE POUCE
On pourra traiter le problème par disjonction de cas.

26 Déterminer suivant les valeurs de n le reste dans la division euclidienne de $7n + 5$ par $3n + 1$.

27 Déterminer pour tout entier naturel non nul n le reste dans la division euclidienne de $3^n - 1$ par 3^{n-1}.

Congruences

28 **1.** Montrer que 7 305 et 7 322 ont même reste dans la division euclidienne par 17.
2. En déduire que $7\,305^3$ et $7\,322^3$ ont même reste dans la division euclidienne par 17.

29 On donne $a \equiv 6$ [11] et $b \equiv 5$ [11].
1. Déterminer le reste dans la division par 11 de :
a. $2a + 3b$ **b.** $a^2 + b^2$ **c.** ab
2. Montrer que $a^2 - b^2$ est divisible par 11.

30 **a.** Déterminer le reste dans la division euclidienne par 9 de $11^4 + 2013$.
b. Déterminer le reste dans la division euclidienne par 9 de $11^4 \times 2013$.

▸ Savoir-faire 4, p. 16

31 **a.** Déterminer le reste dans la division euclidienne par 11 de 2014^{2014}.
b. Déterminer le reste dans la division euclidienne par 11 de 2012^{2012}.

32 **a.** Déterminer le reste dans la division euclidienne par 17 de 2^{2012}.
b. Déterminer le reste dans la division euclidienne par 15 de 2^{2015}.

33 **a.** Montrer que $2^{11} + 1$ est divisible par 3.
b. Montrer que $5^{10} + 1$ est divisible par 13.

▸ Savoir-faire 5, p. 16

34 **a.** Déterminer le chiffre des unités de $11^{1\,000}$.
b. Déterminer le chiffre des unités de $3^{1\,000}$.

35 **a.** Montrer que $2^9 \equiv 2$ [10].
b. En déduire le chiffre des unités de 2^{63}.
c. Déterminer de même le chiffre des unités de 2^{100}.

36 **a.** Déterminer le chiffre des unités de 7^{2013}.
b. Déterminer le chiffre des dizaines de 7^{2013}.

37 En étudiant les restes possibles de x dans la division par 7, résoudre les équations suivantes :

a. $3x \equiv 1$ [7] **b.** $5x \equiv 1$ [7]

38 En étudiant les restes possibles de x dans la division par 6, résoudre les équations suivantes :

a. $2x \equiv 4$ [6] **b.** $2x \equiv 5$ [6]

39 On veut étudier les restes dans la division euclidienne par 7 de 2^n pour tout entier naturel n.

1. Recopier et compléter le tableau des restes de 2^n dans la division par 7 pour $n \leqslant 10$.

n	0	1	2	3	4	5	6	7	8	9	10
Reste modulo 7 de 2^n											

2. Conjecturer un résultat général sur le reste de 2^n dans la division euclidienne par 7.

3. Montrer que, pour tout entier naturel n :

$$2^{n+3} \equiv 2^n \text{ [7]}$$

4. En déduire les restes dans la division euclidienne par 7 de 2^n pour tout entier naturel n.

40 Étudier en suivant la démarche de l'exercice **39**, le chiffre des unités de 2^n pour tout entier naturel n.

41 Soit n un entier naturel. Étudier les restes possibles de n^2 modulo 3.

On appelle **triplet pythagoricien**, les entiers naturels x, y et z vérifiant l'égalité $x^2 + y^2 = z^2$.

Montrer que pour un tel triplet, l'un des nombres x ou y est un multiple de 3.

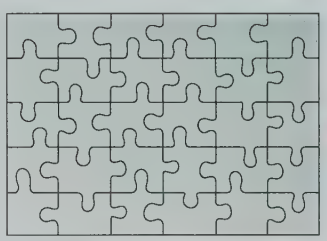
Exercices d'approfondissement

42 **La guerre des boutons**

On veut répartir 204 boutons dans des sachets en mettant autant de boutons dans chaque sachet et en les distribuant tous.

Quels sont les nombres possibles de boutons à mettre dans chaque sachet ?

43 **Puzzle**



Un puzzle affiche 350 pièces.

De plus, on sait que le nombre de pièces sur sa largeur dépasse la moitié du nombre de pièces sur la longueur.

1. Déterminer le nombre de pièces sur chaque ligne et chaque colonne.

2. Déterminer le nombre de pièces avec au moins un bord droit.

44 **Sans pioche**

Si les règles le permettaient, combien pourrait-on accepter de joueurs aux jeux suivants pour que toutes les cartes soient distribuées (on se limitera à 3 joueurs minimum et 10 joueurs maximum).

a. Belote (32 cartes) ; **b.** Bridge (52 cartes) ;

c. Tarot (78 cartes) .

45 **Trop gourmand ?**

Gilles prétend qu'en faisant des lots identiques des 240 bonbons qu'il compte distribuer comme cadeau, il doit en garder 19 qu'il ne peut répartir sur chaque lot.

Est-ce possible ? Expliquer.

46 **En retard**

En sortie scolaire, les élèves attendent que le professeur recompte les élèves dans le bus.

Les élèves occupent des rangées de 4 personnes et une rangée de 5 au fond, toutes complètes. Seuls les trois premières rangées sont entièrement libres.

Le professeur dit immédiatement au chauffeur : « Je devrais avoir 39 élèves, il m'en manque au moins deux ! »

A-t-il raison ? Expliquer.

47 **Au casino**

Dans le film *Ocean's eleven*, les onze braqueurs se partagent équitablement les 163 156 759 dollars du butin, au dollar près.

a. Combien de dollars n'ont pu être partagés ? Auraient-ils pu partager au cent près ?

b. Dans la suite du film, *Ocean's twelve*, malgré un braqueur supplémentaire, ils ne dérobent que 97 millions de dollars et le partage n'est toujours pas possible.

Combien aurait-il fallu de braqueurs supplémentaires au minimum pour que le partage soit exact ?

48 **Au lycée**

En répartissant les 414 élèves de classe de seconde, le proviseur adjoint du lycée veille à mettre autant d'élèves dans chaque classe. Lorsqu'il a terminé, il lui reste 11 élèves non affectés.

1. Combien peut-il y avoir de classes ?

2. Le rectorat décide de supprimer une classe.

En réaffectant les élèves, combien le proviseur adjoint aura-t-il d'élèves en trop pour que les classes aient le même effectif ?

49 Divisible par 11 ?

On souhaite déterminer les valeurs de l'entier naturel n telles que le nombre $4^n - 3^n$ soit divisible par 11.

a. Recopier et compléter le tableau suivant :

Valeurs de n	0	1	2	3	4	5	6	7
Congruence de 4^n mod 11								
Congruence de 3^n mod 11								

b. Déterminer une valeur de k telle que $4^{n+k} - 3^{n+k}$ et $4^n - 3^n$ aient le même reste dans la division par 11 quelque soit n.

c. Déterminer toutes les valeurs de n telles que $4^n - 3^n$ soit divisible par 11.

d. En déduire si $4^{2015} - 3^{2015}$ est divisible par 11.

50 Unités en puissance

1. Déterminer le chiffre des unités de 13^{13} et de $2\,023^{2\,023}$.

2. Soit n un entier dont le chiffre des unités est 3.
Déterminer suivant les valeurs de n le chiffre des unités de n^n.

51 Vrai ou falsifié ?

Ce billet est-il un faux ? Le numéro de série peut nous donner une première indication. Il est composé d'une lettre et de onze chiffres. La lettre correspond à un nombre de 1 à 26 en suivant l'ordre alphabétique (la lettre s correspond à 19). En remplaçant la lettre par le nombre correspondant, on constitue un nombre à 12 ou 13 chiffres. Ce nombre doit avoir 8 comme reste dans la division euclidienne par 9.

1. Montrer que la somme $\overline{\square}$ des chiffres (incluant ceux correspondants à la lettre) doit vérifier $\overline{\square} \equiv 8$ [9].

2. Vérifier alors sans calculatrice si ce billet est faux.

3. Déterminer le chiffre manquant d'un billet non falsifié, dont un chiffre du numéro u49834■82406 a été masqué.

52 Critère de divisibilité

Les nombres que nous utilisons usuellement sont écrits en base 10 (voir Activité de recherche 58, p. 28).
L'écriture du nombre 4 257 signifie :

$$4 \times 10^3 + 2 \times 10^2 + 5 \times 10^1 + 7 \times 10^0$$

1. À l'aide de cette décomposition, montrer que :
$4\,257 \equiv 4 + 2 + 5 + 7$ [3] et $4\,257 \equiv 4 + 2 + 5 + 7$ [9]

2. On généralise pour tout nombre dont l'écriture sera notée $\overline{x_n x_{n-1} x_{n-2} \ldots x_1 x_0}^{10}$ avec $0 \leqslant x_i < 10$ pour $0 \leqslant i \leqslant n$, et telle que :

$$\overline{x_n x_{n-1} x_{n-2} \ldots x_1 x_0}^{10} = x_n \times 10^n + x_{n-1} \times 10^{n-1} + \ldots + x_1 \times 10^1 + x_0 \times 10^0$$

a. Montrer que :
$\overline{x_n x_{n-1} x_{n-2} \ldots x_1 x_0}^{10} \equiv x_n + x_{n-1} + \ldots + x_1 + x_0$ [3]
et $\overline{x_n x_{n-1} x_{n-2} \ldots x_1 x_0}^{10} \equiv x_n + x_{n-1} + \ldots + x_1 + x_0$ [9].

b. En déduire l'énoncé d'un critère de divisibilité par 3 et par 9 faisant appel à la somme des chiffres composant le nombre.

c. En déduire si le nombre 127 392 est divisible par 3 ou par 9.

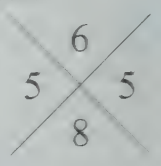
3. On énonce ainsi un critère de divisibilité par 11 :
« Un nombre est divisible par 11 si la somme alternée de ses chiffres est divisible par 11 ».
Par exemple, 917 092 est divisible par 11 car $9 - 1 + 7 - 0 + 9 - 2 = 22$ est divisible par 11.

a. Déterminer à l'aide de ce critère si 47 586, 14 572 et 124 153 sont divisibles par 11.

b. Démontrer ce critère dans le cas général.

53 Que prouve la preuve par 9 ?

La preuve par 9 est un mécanisme de vérification des opérations élémentaires. Il repose sur le critère de divisibilité par 9 démontré dans l'exercice précédent :
« Un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9. »
Exemple : $a = 42$ et $b = 71$. La somme vaut 113.
On représente les résultats dans une croix, en plaçant en haut la somme des chiffres de a, en bas celle de b, à gauche celle de $a + b$, à droite celle obtenue en ajoutant les nombres du haut et du bas de la croix (à gauche, $1 + 1 + 3 = 5$; à droite, $6 + 8 = 14$ d'où $1 + 4 = 5$).



La preuve est juste si la case de droite est identique à celle de gauche.

1. Montrer que si le calcul de $a + b$ est juste, la preuve est nécessairement juste.

2. Montrer que la réciproque est fausse.

3. Montrer que la preuve par 9 fonctionne aussi pour les produits.

4. Le petit frère de Léa lui demande de vérifier ses multiplications mais celle-ci a oublié sa calculatrice.
Il a trouvé :

a. $17 \times 142 = 2\,414$;

b. $75 \times 84 = 6\,320$;

c. $93 \times 52 = 4\,926$.

En s'aidant de la preuve par 9, que peut lui affirmer Léa dans chacun des cas ?

Activités de recherche et résolution de problèmes

Travaux pratiques avec l'outil informatique

Problèmes de recherche

54 Les triplets pythagoriciens

Un triplet pythagoricien est un triplet $(x\,;y\,;z)$ d'entiers naturels non nuls tels que $x^2+y^2=z^2$. Par exemple, le triplet $(3\,;4\,;5)$ est pythagoricien ; il permet notamment de construire un triangle rectangle avec des cotés de longueur entière.
Le but du problème est de savoir si, pour tout entier naturel non nul x donné, on peut trouver y et z tels que $(x\,;y\,;z)$ soit un triplet pythagoricien.

Partie 1

À l'aide d'un tableur, on a construit la feuille de calcul ci-dessous affichant pour x et y donnés la valeur de z correspondant si z est entier.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	x \ y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	1																									
3	2																									
4	3				5																					
5	4			5																						
6	5												13													
7	6								10																	
8	7																								25	
9	8						10									17										
10	9												15													
11	10																								26	
12	11																									
13	12					13				15							20									
14	13																									
15	14																									
16	15								17												25					
17	16												20													
18	17																									
19	18																								30	
20	19																									
21	20															25						29				
22	21																				29					
23	22																									
24	23																									
25	24							25			26								30							

1. Expliquer la symétrie observée dans le tableau.
2. Expliquer le lien entre les triplets coloriés. En déduire qu'il existe une infinité de triplets pythagoriciens.
3. On appelle triplet primitif, un triplet $(x\,;y\,;z)$ tels que x, y et z n'aient pas de diviseur commun. À l'aide du tableau, donner la liste des triplets primitifs pour x et y compris entre 1 et 24.

Partie 2

1. Construire cette feuille pour $1 \leqslant x \leqslant 21$ et $1 < y < 255$ à l'aide d'une fonction **SI**, affichant $z=\sqrt{x^2+y^2}$ si ce dernier est entier, rien sinon (pour afficher une case vide, on saisira des doubles guillemets dans la partie « sinon » de la formule).

2. Pour quelles valeurs de x ne semble-t-il pas exister de triplet ? Démontrer ce résultat en factorisant la différence $z^2 - y^2$.

3. Déterminer les triplets $(x\,;y\,;z)$ pour tout x impair supérieur à 1 et inférieur ou égal à 21.

4. Conjecturer dans ce cas une relation entre y et z.

Partie 3

1. On cherche à déterminer des triplets tels que $z = y + 1$.
   - **a.** Montrer que y et z n'ont pas de diviseur commun autre que 1.
   - **b.** Exprimer x^2 en fonction de y, puis y et z en fonction de x.
   - **c.** En déduire l'existence d'un triplet primitif pour tout x impair supérieur à 1.

2. x est désormais un entier naturel supérieur à 2 quelconque.
   - **a.** Si x n'est pas une puissance de 2, alors x peut s'écrire sous la forme $2^n \times x'$ avec x' impair différent de 1. En déduire un triplet $(x\,;y\,;z)$.
   - **b.** Si x est une puissance de 2 supérieure à 2, alors x est un multiple de 4.
     En déduire un triplet $(x\,;y\,;z)$.

3. Conclure quant à l'existence d'un triplet pythagoricien pour un entier naturel x quelconque.

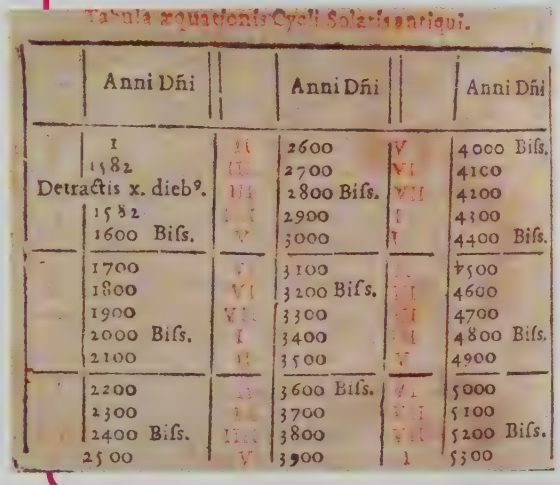
4. **Applications**
   - **a.** Déterminer un triplet pythagoricien $(x\,;y\,;z)$ avec $x = 2013$.
   - **b.** Déterminer un triplet pythagoricien $(x\,;y\,;z)$ avec $x = 2014$.

55 Le calendrier grégorien

Le calendrier grégorien est celui que nous utilisons dans la plus grande partie du monde depuis le 15 octobre 1582.

Le pape Grégoire XIII (1502-1585).

Les années bissextiles sont nées du fait de la durée réelle de l'année tropique (révolution de la Terre autour du Soleil). En effet, l'année tropique dure 365,24219 jours. Au bout de quatre ans avec des années à 365 jours, il manquerait 0,96876 jour. Au bout d'un siècle, Pâques se retrouverait en été, ce qui ne fut pas du goût des états pontificaux et qui motiva cette réforme. En rajoutant un jour tous les quatre ans, l'écart moyen avec l'année tropique serait alors de 0,00771 jour en trop par an, soit presque un jour tous les cent ans, d'où l'idée d'ôter les siècles de la liste des années bissextiles.
Par le même raisonnement, on ajouta une année tous les 400 ans, ce qui mène finalement à un décalage moyen de 18 secondes par an sur l'année tropique, soit une journée au bout d'environ 4 700 ans.



Tabula æquationis Cycli Solaris antiqui.

Anni Dñi		Anni Dñi		Anni Dñi
I		2600		4000 Biſs.
1582		2700		4100
Detractis x. dieb⁹.		2800 Biſs.		4200
1582		2900		4300
1600 Biſs.		3000		4400 Biſs.
1700		3100		4500
1800		3200 Biſs.		4600
1900		3300		4700
2000 Biſs.		3400		4800 Biſs.
2100		3500		4900
2200		3600 Biſs.		5000
2300		3700		5100
2400 Biſs.		3800		5200 Biſs.
2500		3900		5300

Ce document donne la liste des siècles bissextiles du nouveau calendrier grégorien. Pour rattraper le décalage de 10 jours déjà observé, ce calendrier fut adopté le jeudi 4 octobre 1582 et mis en place le lendemain, vendredi 15 octobre 1582.

Tableau des années bissextiles

On souhaite réaliser la feuille de calcul donnant le jour de la semaine correspondant à une date quelconque (saisie dans les cellules G2, H2 et I2) à partir du 1er janvier de l'an 1.
Le mois de février compte 28 ou 29 jours selon que l'année est bissextile ou non.
Une année est bissextile si elle est soit divisible par 400, soit divisible par 4 sans être divisible par 100.

	A	B	C	D	E	F	G	H	I
1		rang	nb jours	jours cumulés des mois précédents			jour	mois	annee
2	janvier	1	31				1	1	2013
3	février	2	28	31					
4	mars	3	31	59					
5	avril	4	30	90					
6	mai	5	31	120		nb jours écoulés année courante	1		
7	juin	6	30	151		nb années écoulées	2012		
8	juillet	7	31	181		nb années bissextiles écoulées	488		
9	août	8	31	212					mardi
10	septembre	9	30	243		reste mod 7	2		
11	octobre	10	31	273					
12	novembre	11	30	304					
13	décembre	12	31	334					

1 Pour calculer le nombre de jours écoulés en février l'année donnée, on a saisi dans la cellule C3 la formule suivante :

=SI(OU(ET(MOD(I2 ;4)=0 ;MOD(I2 ;100)<>0) ;MOD(I2 ;400)=0) ;29 ;28).

a. Expliquer la structure algorithmique de ce test conditionnel.
b. Saisir la date proposée en ligne 2, puis compléter les colonnes A à D.
c. Vérifier le nombre de jours écoulés en février en testant une année bissextile.

2 Le nombre J de jours écoulés de l'année courante comprend la date proposée (un jour écoulé le premier janvier).
À l'aide d'une fonction SOMME.SI et des colonnes B et D, compléter la cellule G6.

3 On note A le nombre d'années écoulées (cellule G7).
a. Montrer que le nombre d'années bissextiles écoulées est donné par :

$$B = E\left(\frac{A}{400}\right) + E\left(\frac{A}{4}\right) - E\left(\frac{A}{100}\right)$$ où E désigne la fonction partie entière.

b. Compléter les cellules G7 et G8.

4 **a.** Justifier que le nombre de jours écoulés entre le 1er janvier de l'an 1 et la date proposée vaut $J + 365A + B$.
b. Montrer que ce nombre est congru à $J + A + B$ modulo 7.
c. À l'aide de la fonction MOD, en déduire son reste R dans la division euclidienne par 7 (cellule G10).

5 À l'aide de la date proposée, déterminer le lien entre le reste R et le jour de la semaine et vérifier ce résultat à l'aide de la date d'aujourd'hui.
On pourra ensuite à l'aide d'une fonction conditionnelle afficher le jour correspondant au reste obtenu.

6 Vérifier que le centenaire de l'armistice de la Première Guerre mondiale aura lieu un dimanche.
Combien d'années faudra-t-il attendre pour que cela se reproduise ?

56 Déterminer le chiffre des unités de a^n

Partie 1 : Algorithme

Pour déterminer le chiffre des unités de a^n, on cherche son reste dans la division euclidienne par 10.

1 Le processus sur un exemple

Pour trouver le chiffre des unités de 17^{91}, on suit les étapes suivantes :

- on remplace 17 par son reste dans la division euclidienne par 10, soit $17^{91} \equiv 7^{91}$ [10] ;
- on effectue la division euclidienne de 91 par 2, soit $91 = 2 \times 45 + 1$;
- on en déduit $7^{91} \equiv 7^{2\times 45+1}$ [10] $\equiv (7^2)^{45} \times 7^1$ [10] $\equiv 49^{45} \times 7$ [10] ;
- on réitère le processus avec 49^{45}.

a. Montrer qu'après deux itérations du processus, on peut alors l'interrompre et obtenir $17^{91} \equiv 9 \times 7$ [10].

b. En déduire le chiffre des unités de 17^{91}.

c. En appliquant le même algorithme, déterminer le chiffre des unités de 2013^{2013}.

2 Une structure algorithmique

On propose l'algorithme suivant pour rechercher le chiffre des unités.

```
Entrées :      Entrer les valeurs A et N
Sortie :       Chiffre des unités de A^N
               Affecter à U la valeur 1
               Affecter à A son chiffre des unités
               Tant que N > 0 et A ≠ 1 faire
Traitement :   |  Affecter à Q le quotient de N dans la division
               |  euclidienne par 2
               |  Affecter à R le reste de N dans la division
               |  euclidienne par 2
               |  Si R = 1
               |  |  Affecter à U la valeur U × A
               |  fin si
               |  Affecter à A le chiffre des unités de A²
               |  Affecter à N la valeur Q
               fin tant que
               Affecter à U son chiffre des unités
               Afficher U
```

a. Reproduire et compléter le tableau suivant, donnant les valeurs successives des variables de l'algorithme pour $A = 12$ et $N = 5$.

Étapes / Variables	Q	R	U	A	N
Entrées				12	5
Initialisation			1	2	
1re boucle	2	1	2	4	2
2e boucle					
3e boucle					
Sortie					

b. Réaliser le même tableau pour exécuter l'algorithme avec $A = 17$ et $N = 91$.

c. Montrer que les valeurs de N successives forment une suite décroissante. En déduire que le processus se termine toujours.

d. Expliquer pourquoi la condition $A \neq 1$ a été ajoutée ?

e. L'algorithme fonctionnera-t-il si le chiffre des unités de A est 0 ?

Partie 2 : Programmation

1 Quotient et reste dans une division euclidienne

En notant **partEnt** la fonction donnant la partie entière d'un entier, partEnt $\left(\frac{X}{B}\right)$ donne le quotient dans la division euclidienne de X par B et $X - B \times$ partEnt $\left(\frac{X}{B}\right)$ donne le reste.

Pour le calcul du reste, on pourra aussi utiliser directement la fonction **partDéc** donnant la partie décimale d'un nombre.

a. Quel calcul permet de remplacer A par son chiffre des unités ?

b. Dans la boucle « Tant que » de l'algorithme, quels calculs permettent d'affecter les valeurs successives de Q, R, A, U et N ?

2 Programmer

a. Programmer l'algorithme précédent dans un langage, sur un logiciel ou sur une calculatrice.

b. Vérifier son bon fonctionnement en évaluant le chiffre des unités de 2013^{2013}, puis de 2010^{2010}.

c. Ajouter un compteur de boucle et évaluer le nombre de boucles nécessaire en exécutant le programme pour 2012^{2012}.
Pouvait-on prévoir le nombre de boucles en étudiant les valeurs successives de N ?

Partie 3 : Pour aller plus loin... Réduction du coût algorithmique

1 Avec une division euclidienne par 10

Les capacités des ordinateurs ou des calculatrices permettent de donner le chiffre des unités de nombres plus grands que A^2, avec $A < 10$. Par exemple, $9^{10} = 3\,486\,784\,401 \equiv 1 \ [10]$.
On décide de modifier l'algorithme en effectuant les divisions euclidiennes successives de l'exposant par 10.

a. Exécuter cet algorithme avec des congruences pour évaluer le chiffre des unités de 2^{2012}, cet algorithme commençant par $2^{2012} = 2^{10 \times 201 + 2} = (2^{10})^{201} \times 2^2 = 1\,024^{201} \times 2^2$.

$2^{2012} \equiv 4^{201} \times 4 \ [10]$.

b. Comparer le nombre de boucles à celui de la question **2 c.** de la **partie 2**.

c. Pour modifier l'algorithme de la **partie 2**, expliquer pourquoi on peut remplacer U dans la boucle par $U \times A \text{^} R$.

d. Modifier le programme de la **partie 2** afin de réaliser le nouvel algorithme.

2 Exceptions et améliorations

a. Ce programme ne fonctionne pas si le chiffre des unités vaut 0. Déterminer les raisons de cette erreur et corriger le programme.

b. Adapter cet algorithme pour déterminer aussi le chiffre des dizaines du nombre a^n.

57 Les clés de contrôle

L'informatisation de nombreux systèmes a progressivement donné une place centrale aux identifiants numériques. De nombreux numéros permettent d'identifier les personnes, les comptes bancaires, les objets manufacturés, etc.
Mais il est plus facile de commettre une faute en donnant un numéro à 21 chiffres qu'en donnant son nom. Pour fiabiliser ce système, on a inventé des clés de contrôles qui sont des chiffres supplémentaires obtenus par calcul à l'aide du numéro concerné et permettant de repérer d'éventuelles erreurs.

Partie 1. Numéros EAN-13 et ISBN-13

Ces deux numéros ont une structure identique. Le numéro EAN-13 (European Article Numbering) est le numéro indiqué sous les codes barres de produits manufacturés.
Le numéro ISBN-13 (International Standard Book Number) est propre aux livres. Ils sont facilement identifiables, car ils commencent par 978 ou 979.
Les 12 premiers chiffres donnent des informations sur le pays d'origine, l'entreprise et la série du produit. Le dernier chiffre est une clé de contrôle.
Le calcul de cette clé se fait en sommant les chiffres du numéro, pondérés alternativement par 1 ou 3 comme dans le tableau ci-dessous :

Numéro	9	7	8	1	2	3	4	5	6	7	8	9
Pondération	1	3	1	3	1	3	1	3	1	3	1	3
Produit	9	21	8	3	2	9	4	15	6	21	8	27

On calcule ensuite le reste R dans la division par 10 de la somme des nombres de la dernière ligne. Si ce reste est 0, c'est la clé de contrôle, sinon, la clé est $10 - R$.

1. Vérifier la valeur de la clé du numéro ISBN précédent.
2. Montrer qu'une erreur sur un chiffre pondéré par 1 donnera nécessairement une clé de contrôle différente.
3. Montrer qu'une erreur sur un chiffre pondéré par 3 donnera nécessairement une clé de contrôle différente.
4. Montrer que si deux chiffres consécutifs diffèrent de 5, la clé serait inchangée en les intervertissant.

Partie 2. Numéro d'INSEE

Le numéro d'INSEE est un identifiant individuel national. Ce numéro est demandé dans certaines démarches administratives et joue le rôle de numéro de sécurité sociale.
Ce numéro est composé de 15 chiffres, les deux derniers étant la clé de contrôle.
Le premier chiffre détermine le sexe (1 ou 2), les suivants l'année de naissance (2 chiffres), le mois de naissance (2 chiffres), le département de naissance (2 chiffres), le numéro de la commune (3 chiffres), le numéro d'inscription sur le registre de l'état civil (3 chiffres), ce qui garantit l'unicité du numéro à 13 chiffres.
Pour déterminer la clé de contrôle C d'un numéro d'INSEE N à 13 chiffres, on calcule le reste R dans la division euclidienne par 97 de N. La clé est donnée par $C = 97 - R$.

1 Quelques propriétés

a. Donner la liste des valeurs possibles de la clé de contrôle.

b. Montrer que si un numéro N a pour clé C, alors $N + C$ est divisible par 97.

c. Vérifier la clé de contrôle du numéro proposé sur la carte vitale ci-dessus.

2 Calculer une clé de contrôle avec un tableur

La fonction **MOD** du tableur ne permet pas de calculer un reste dans une division euclidienne pour des nombres à 13 chiffres, car ils dépassent sa capacité de calcul.

On décompose donc le numéro d'INSEE suivant la base 10 de son écriture. Le numéro précédent peut s'écrire $2 \times 10^{12} + 9 \times 10^{11} + \ldots + 8 \times 10^{1} + 5 \times 10^{0}$. On s'appuiera sur les restes des puissances de 10 successives pour calculer la clé à l'aide de la feuille de calcul suivante :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	n° insee	**2**	**9**	**4**	**0**	**1**	**6**	**8**	**0**	**6**	**5**	**2**	**8**	**5**
2	facteur 10^n	1E+12	1E+11	1E+10	1E+09	1E+08	1E+07	1E+06	100000	10000	1000	100	10	1
3	reste mod 97	50	5	49	34	81	76	27	90	9	30	3	10	1
4	produit mod 97	3	45	2	0	81	68	22	0	54	83	6	80	5
5	reste R	61												
6	clé	36												

Le numéro d'INSEE est saisi en ligne 1, les puissances de 10 en ligne 2, leur reste respectif en ligne 3.

a. En saisissant la valeur 1 dans les cellules N2 et N3, proposer des formules à saisir en M2 et M3 recopiables vers la gauche permettant de compléter les lignes 2 et 3.

b. On a saisi la formule =MOD(B1*B3;97) dans la cellule B4 avant de recopier cette formule vers la droite. Justifier que la somme des termes de la ligne 4 a même reste dans la division euclidienne par 97 que le numéro d'INSEE évalué.

c. Déterminer les formules à saisir dans les cellules B5 et B6.

3 Les erreurs repérées

a. Montrer que si un seul chiffre est erroné, le numéro d'INSEE augmente ou diminue de $A = k \times 10^n$, en précisant les valeurs possibles de k et de n.

b. On admet qu'un tel nombre A n'est pas divisible par 97 (cette propriété sera démontrée à l'aide du théorème de Gauss dans le **chapitre 2**, voir encadré).

Montrer que si un seul chiffre du numéro est erroné, la clé ne sera pas la même.

Montrer que si l'on intervertit deux chiffres consécutifs, la clé ne sera pas la même.

c. Trouver à l'aide de la feuille de calcul précédente, une erreur non détectée en modifiant deux chiffres du numéro proposé.

NOTE

Pourquoi 97 ?

C'est parce que 97 est le plus grand nombre premier inférieur à 100 qu'il a été choisi pour calculer les clés de contrôle à 2 chiffres.

Le fait qu'il soit premier assure qu'il ne peut diviser de nombre de la forme $A = k \times 10^n$, car sinon 97 serait un facteur de la décomposition en produit de nombres premiers de A. De fait, toute erreur concernant un seul chiffre est toujours détectée.

En outre, si le plus grand nombre premier inférieur à 100 a été choisi, c'est pour offrir le plus grand nombre possible de clé à deux chiffres.

Partie 3. Numéro de compte bancaire

Le mode de calcul de la clé de contrôle d'un numéro de compte bancaire N est basé sur un principe proche de celui d'un numéro d'INSEE.

Ce numéro N à 21 chiffres est constitué d'un code de banque (5 chiffres), d'un code guichet (5 chiffres) et du numéro du compte (11 chiffres).

La clé C à deux chiffres s'obtient en calculant le reste R de $100 \times N$ dans la division euclidienne par 97. On a alors $C = 97 - R$.

1 Le nombre constitué de 23 chiffres (le numéro N suivi de la clé C) est-il divisible par 97 ?

2 On peut décomposer le numéro par bloc comme sur ce relevé d'identité bancaire :

Code banque	Code guichet	Numéro de compte	Clé
17219	40550	76001018958	41

a. En notant B le code banque, G le code guichet et N_C le numéro de compte, montrer que :

$$C \equiv -(89B + 15G + 3N_C) \ [97].$$

b. Vérifier à la calculatrice la clé du relevé d'identité bancaire précédent.

58 Bases de numération

Les systèmes de numération

Tablette comptable en cunéiforme archaïque picto graphique. (3500-3100 av. J.-C.)

30 000 ans nous séparent des premiers systèmes de numération. Ces systèmes étaient additifs, utilisant quelques symboles. Le plus connu ayant résisté au temps est le **système romain**. En chiffres romains le nombre 38 s'écrit XXXVIII. La difficulté évidente étant le nombre de symboles répétés, qui pose de sérieux problèmes lorsqu'on veut écrire, par exemple, le nombre 7 548 223.

Le système que nous utilisons est basé sur la position des chiffres. En regroupant les objets par paquets de 10, puis les paquets de 10 eux-mêmes par paquets de 10, on a fabriqué les dizaines, puis les centaines et ainsi de suite. Écrire un nombre 274 signifie qu'il comprend 2 centaines, 7 dizaines et 4 unités.

Mais pourquoi avons nous regroupé les objets par paquet de 10 ? De nombreuses explications ont été proposées, la plus cohérente s'appuyant sur le nombre de doigts des deux mains pour compter. Nous comptons donc aujourd'hui en base 10.

Pourtant de nombreuses autres bases ont jalonné l'histoire de la numération. Les Mayas comptaient en base 20 (était-ce les mains et les pieds ?), les ancêtres des Babyloniens en base 12 (probablement par l'existence de 4 × 3 phalanges sur les doigts opposables au pouce d'une main). Ces mêmes Babyloniens établirent le système le plus abouti et proche du notre, en base 60, qui nous est resté pour mesurer le temps ou les angles (minutes et secondes).

Partie 1. Convertir l'écriture d'un nombre de base a en base 10

En base 10, on dispose de 10 chiffres (de 0 à 9) pour écrire les nombres. Pour écrire le nombre dix, on juxtapose le 1 et le 0, signifiant « une dizaine et zéro unité ».

a est un entier supérieur ou égal à 2. En base a, on dispose de a chiffres.

Le nombre a s'écrit alors $\overline{10}^a$, qui signifie 1 quantité de a (l'équivalent des dizaines en base 10) et 0 unité. La notation « $\overline{\ }^a$ » permet juste de préciser la base d'écriture du nombre lorsqu'il n'est pas en base 10.

1 **Système binaire**

En base 2, les nombres ne s'écrivent qu'avec les chiffres 0 et 1.

a. Recopier et compléter le tableau de correspondance suivant :

Système décimal	0	1	2	3	4	5	6	7	8	9	10	11	12
Système binaire	$\overline{0}^2$	$\overline{1}^2$	$\overline{10}^2$	$\overline{11}^2$	$\overline{100}^2$								

b. Expliquer les valeurs obtenues pour les puissances de 2.

c. Vérifier par le calcul que $\overline{1011}^2 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 = 11$. Expliquer ce calcul.

d. Déterminer la valeur de $\overline{10010111}^2$.

2 **En base 3**

a. Compléter un tableau de correspondance comme dans la question **1** **a.**

b. Déterminer la valeur de $\overline{2101}^3$.

c. Donner la valeur (en base 10) du plus grand nombre que l'on peut écrire avec trois chiffres en base 3 ?

3 **En base 12**

Pour écrire les nombres en base 12, il faut 12 chiffres. On les notera 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, α, β où α vaut 10 et β vaut 11.

Déterminer la valeur de $\overline{\beta 5 \alpha 1}^{12}$.

4 **En base *a***

On note $\overline{x_n\, x_{n-1}\, x_{n-2} \ldots x_1\, x_0}^{a}$ un nombre écrit en base a.

a. Quelle condition doivent vérifier les x_i, pour $0 \leqslant i \leqslant n$, afin que cette écriture soit valide ?

b. Donner une formule permettant de convertir ce nombre en base 10.

Partie 2. Convertir l'écriture d'un nombre de base 10 en base *a*.

On admettra que l'écriture $\overline{x_n\, x_{n-1}\, x_{n-2} \ldots x_1\, x_0}^{a}$ d'un nombre en base a avec $a \geqslant 2$ et avec $0 \leqslant x_i < a$ pour $0 \leqslant i \leqslant n$ signifie que :

$$\overline{x_n\, x_{n-1}\, x_{n-2} \ldots x_1\, x_0}^{a} = x_n \times a^n + x_{n-1} \times a^{n-1} + \ldots + x_1 \times a^1 + x_0 \times a^0.$$

1 **Un exemple en base 8**

On veut écrire en base 8 le nombre 371. On effectue la division euclidienne de 371 par 8, soit $371 = 8 \times 46 + 3$.

a. En réitérant le procédé avec 46, montrer que $371 = 5 \times 8^2 + 6 \times 8 + 3$.

b. En déduire l'écriture en base 8 du nombre 371.

2 Par le même procédé, écrire le nombre 191 en base 5, puis en base 12.

3 **Généralisation de l'algorithme**

Pour déterminer l'écriture en base a du nombre n, on effectue la division euclidienne de n par a, soit $n = a \times q_1 + r_1$, puis on réitère le procédé avec q_1. On fabrique ainsi deux suites (q_n) et (r_n).

a. Montrer que la suite (q_n) est strictement décroissante.

b. On stoppe l'algorithme dès que le quotient est nul. Montrer que l'algorithme s'arrête nécessairement après un nombre n_0 d'étapes.

c. Donner alors l'écriture du nombre n en base a.

d. En déduire l'unicité de l'écriture en base a.

Partie 3. Conversion de base *a* en base *b*

Pour convertir l'écriture d'un nombre d'une base a vers une base b, on la convertit d'abord de la base a vers la base 10, puis de la base 10 vers la base b.

Pour effectuer une conversion directement, il faudrait savoir effectuer des divisions euclidiennes dans d'autres bases que la base 10.

Dans la fenêtre ci-dessous, le nombre $\overline{1423}^{5}$ a été converti en base 12.

	A	B	C	D	E	F	G	H	I	J
1	base a	5								
2	base b	12								
3										
4	nombre en base a		**0**	**0**	**0**	**0**	**1**	**4**	**2**	**3**
5			78125	15625	3125	625	125	25	5	1
6	nombre en base 10		**238**							
7										
8			0	0	0	0	0	1	19	238
9	nombre en base b		**0**	**0**	**0**	**0**	**0**	**1**	**7**	**10**

1 Déterminer l'écriture en base 10, puis en base 12 du nombre $\overline{1423}^{5}$ et vérifier l'affichage proposé.

2 Réaliser la feuille de calcul ci-dessus, les cellules grisées étant des variables de saisie.

3 À l'aide de la feuille de calcul, convertir $\overline{325}^{6}$, puis $\overline{100}^{20}$ en base 2.

Ces réponses sont-elles correctes ? Expliquer.

Partie 4. Calcul en binaire : la base de l'informatique

Un ordinateur ne peut transmettre que deux types d'information : le courant passe ou le courant ne passe pas. Les informations sont donc codées en binaire, suivant les deux états : 1 si le courant passe, 0 sinon.

En regroupant ces signaux électriques (des bits) par paquets de 8, on forme un octet auquel on peut associer, par exemple, le nombre $\overline{10010011}^2$. Les octets décrivent 256 nombres (2^8) de 0 à 255.

Cette unité et ses multiples apparaissent souvent en informatique pour les stockages de données, codage des caractères, des couleurs, …

Par exemple, un processeur 64 bits peut lire simultanément 8 octets, de même trois octets consécutifs peuvent décrire $2^{24} = 16\,777\,216$ de nombres différents, à chacun desquels on peut associer, par exemple, chaque couleur d'un écran dit «16 millions de couleurs».

1 Calculer en binaire

On donne deux nombres écrits en binaire sur un octet :

$$a = \overline{11010011}^2 \text{ et } b = \overline{00011010}^2.$$

retenue
1
1 1 0 1 0 0 1 1
+ 0 0 0 1 1 0 1 0
= 0 1

a. En posant l'addition commencée ci-contre en binaire, calculer $a + b$ (lorsque l'on a $1 + 1 = 10$, on pose 0 et l'on retient 1).

b. De même poser la multiplication de a par b.

c. En convertissant en écriture décimale les nombres a et b et ceux obtenus aux questions **a.** et **b.**, vérifier les résultats précédents.

2 Écriture binaire et hexadécimale

L'écriture hexadécimale (base 16) s'est substituée dans de nombreux programmes à l'écriture binaire. Cette écriture est avantageuse car un seul caractère code des nombres de 0 à 15, et surtout, la conversion en binaire de ce caractère nécessite peu de calcul.

En hexadécimal, on notera les 16 chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

a. Donner l'écriture du nombre $a = \overline{11010011}^2$ en hexadécimale.

b. On découpe l'octet a en deux quartets $x = \overline{1101}^2$ et $y = \overline{0011}^2$. Donner l'écriture de x et y en hexadécimale. Comparer ce résultat à ceux de la question **a.**.

c. Montrer qu'en base 2, multiplier par 16 revient à ajouter quatre 0 à droite dans l'écriture d'un nombre en base 2. En déduire les raisons du phénomène observé aux questions précédentes.

De la théorie à la pratique

Comment un circuit électrique peut-il effectuer la multiplication de deux bits? Rien de plus simple ! Il suffit de mettre en série deux interrupteurs, chaque interrupteur étant commandé par un bit. Si le bit vaut 1, il ferme l'interrupteur, sinon celui-ci reste ouvert.

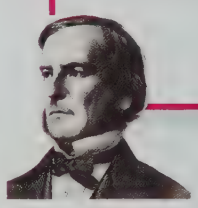
À la sortie du circuit, on obtient le produit : 1 si le courant passe, 0 sinon.

En effet, pour multiplier deux bits, on a quatre possibilités comme le montre le tableau ci-contre. Le courant ne passe que si les deux interrupteurs sont fermés, ce qui ne correspond qu'au dernier des produits (1×1).

$0 \times 0 = 0$
$1 \times 0 = 0$
$0 \times 1 = 0$
$1 \times 1 = 1$

Pour l'addition, l'affaire est plus délicate. En effet, la somme $1 + 1$ s'écrit avec deux bits ; l'additionneur est donc plus complexe car il doit prévoir une unité et une retenue.

Cet additionneur fut pourtant inventé par **Georges Boole** (1815-1864) bien avant l'avènement de la maîtrise de l'électricité et permettait d'automatiser un raisonnement logique. L'algèbre de Boole et sa théorie des connecteurs logiques resta donc théorique et ne fut mis en œuvre pour l'informatique que près d'un siècle plus tard.



OBJECTIF BAC

Sujets type BAC

Exercice résolu

Exercice 59

On souhaite déterminer le chiffre des unités de $2^n + 3^n$ selon les valeurs de n.

1. On choisit $n = 2012$.

a. Déterminer le chiffre des unités de 3^{2012}.

b. Déterminer le reste de 2^{2012} dans la division par 5.

En déduire le chiffre des unités de 2^{2012}.

c. Quel est alors le chiffre des unités de $2^{2012} + 3^{2012}$?

2. On étudie désormais le cas d'un entier n quelconque.

a. Compléter le tableau suivant :

n	0	1	2	3	4	5	6	7
Reste de 2^n modulo5								
Reste de 3^n modulo 5								
Reste de $2^n + 3^n$ modulo 5								

b. Conjecturer les valeurs des restes de $2^n + 3^n$ en fonction des valeurs de n.

c. Pour tout k et n entiers naturels, montrer que $2^n + 3^n$ et $2^{n+4k} + 3^{n+4k}$ ont même reste dans la division par 5.

d. En déduire l'ensemble des restes possibles de $2^n + 3^n$ en fonction de n.

e. En étudiant la parité de $2^n + 3^n$, donner son chiffre des unités en fonction de n.

3. En déduire le chiffre des unités de $2^{888} + 3^{888}$.

Voir résolution page suivante.

Exercice 60

D'après un sujet de Bac, Centres étrangers, juin 2005.

Partie A

Soit N un entier naturel impair.

On suppose que $N = a^2 - b^2$ où a et b sont deux entiers naturels.

a. Montrer que a et b n'ont pas la même parité.

b. Montrer que N peut s'écrire comme produit de deux entiers naturels p et q.

c. Quelle est la parité de p et celle de q ?

Partie B

On se propose de chercher les couples d'entiers naturels $(a\,;\,b)$ vérifiant la relation :

$$(E)\ a^2 - 250\,507 = b^2.$$

1. Soit X un entier naturel.

a. Donner dans un tableau les restes possibles de X modulo 9, puis ceux de X^2 modulo 9.

b. Sachant que $a^2 - 250\,507 = b^2$, déterminer les restes possibles modulo 9 de $a^2 - 250\,507$; en déduire les restes possibles de a^2 modulo 9.

c. Montrer que les restes possibles modulo 9 de a sont 1 et 8.

2. a. Justifier que si le couple $(a\,;\,b)$ vérifie la relation (E), alors $a \geqslant 501$.

b. Déterminer le plus petit entier $a \geqslant 501$ vérifiant $a \equiv 1\ [9]$.

c. Écrire un algorithme donnant la plus petite solution vérifiant $a \equiv 1\ [9]$.

d. Déterminer cette solution à l'aide de la calculatrice.

e. En déduire une factorisation de 250 507.

Exercice 61

D'après un sujet de Bac, National, juin 2009.

1. Soit n un nombre entier naturel.

a. Démontrer que pour tout nombre entier naturel k on a $2^{3k} \equiv 1\ [7]$.

b. Quel est le reste dans la division euclidienne de 2^{2009} par 7 ?

2. Soit a et b deux nombres entiers naturels inférieurs ou égaux à 9 avec $a \neq 0$.

On considère le nombre $N = a \times 10^3 + b$.

On rappelle qu'en base 10 ce nombre s'écrit sous la forme $N = \overline{a00b}^{10}$.

On se propose de déterminer parmi ces nombres entiers naturels N ceux qui sont divisibles par 7.

a. Vérifier que $10^3 \equiv -1\ [7]$.

b. En déduire tous les nombres entiers N cherchés.

Résolution

1. a. Le chiffre des unités est le reste dans la division euclidienne par 10.
$3^{2012} = (3^2)^{1006}$, on en déduit que :

$$\begin{aligned} 3^{2012} &\equiv 9^{1006} \ [10] \\ &\equiv (-1)^{1006} \ [10] \\ &\equiv 1 \ [10] \end{aligned}$$

Utiliser la congruence de 9 modulo 10 simplifie beaucoup les calculs.

Le chiffre des unités de 3^{2012} est donc 1.

b. $2^{2012} = 4^{1006}$, on en déduit que :

$$\begin{aligned} 2^{2012} &\equiv 4^{1006} \ [5] \\ &\equiv (-1)^{1006} \ [5] \\ &\equiv 1 \ [5] \end{aligned}$$

Les nombres congrus à 1 modulo 5 se terminent par 1 ou 6.
Or 2^{2012} est un nombre pair, il se termine donc par 6.

c. On en déduit que $2^{2012} + 3^{2012} \equiv 1 + 6 \equiv 7 \ [10]$. Le chiffre des unités de $2^{2012} + 3^{2012}$ est donc 7.

2. a.

n	0	1	2	3	4	5	6	7
Congruence de 2^n modulo5	1	2	4	3	1	2	4	3
Congruence de 3^n modulo 5	1	3	4	2	1	3	4	2
Congruence de $2^n + 3^n$ modulo 5	2	0	3	0	2	0	3	0

b. Il semble que lorsque n est impair, le reste soit nul ; lorsque n est un multiple de 4, le reste soit 2 ; et sinon le reste soit 3.

c. $2^{n+4k} + 3^{n+4k} = 2^n \times 2^{4k} + 3^n \times 3^{4k} = 2^n \times (16)^k + 3^n \times (81)^k$
d'où $2^{n+4k} + 3^{n+4k} \equiv 2^n \times 16^k + 3^n \times 81^k \ [5]$

$$\begin{aligned} &\equiv 2^n \times 1^k + 3^n \times 1^k \ [5] \\ &\equiv 2^n \times 1 + 3^n \times 1 \ [5] \\ &\equiv 2^n + 3^n \ [5] \text{ quel que soit l'entier naturel } n. \end{aligned}$$

La méthode consiste à utiliser les propriétés algébriques pour faire apparaître le terme $2n + 3n$.

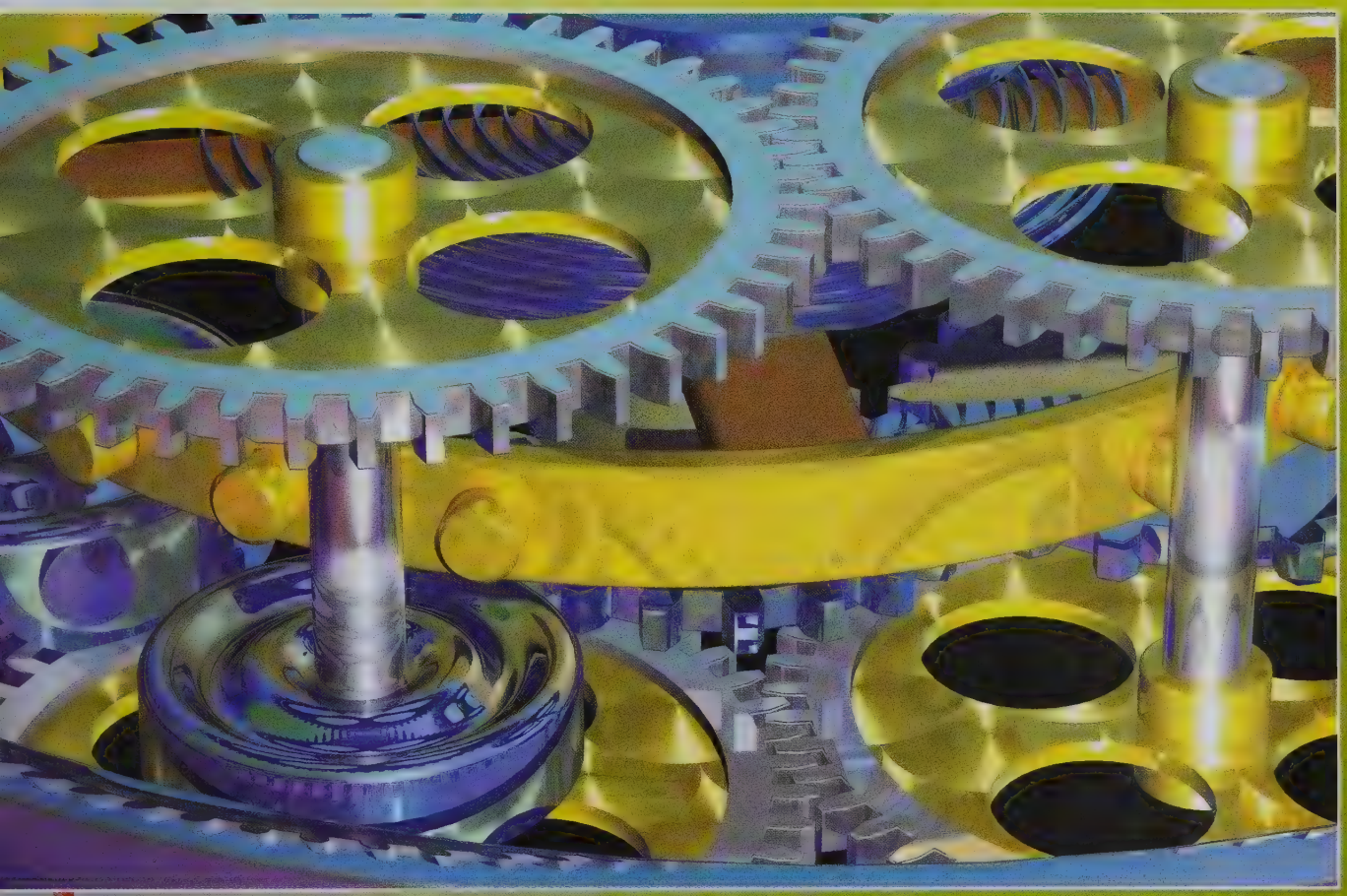
d. Tout entier n s'écrit de la forme $r + 4k$, où r est le reste de n dans la division euclidienne par 4 et k est un entier. La propriété montrée à la question **2c.** implique que $2^n + 3^n$ et $2^r + 3^r$ ont même reste dans la division par 5. Le reste r ne peut prendre que quatre valeurs : 0, 1, 2 ou 3. Les restes sont donnés dans le tableau de la question **2a** :
si $n \equiv 0 \ [4]$ alors $2^n + 3^n \equiv 2 \ [5]$
si $n \equiv 1 \ [4]$ alors $2^n + 3^n \equiv 0 \ [5]$
si $n \equiv 2 \ [4]$ alors $2^n + 3^n \equiv 3 \ [5]$
si $n \equiv 3 \ [4]$ alors $2^n + 3^n \equiv 0 \ [5]$

e. Le nombre $2^n + 3^n$ est impair pour tout n car 2^n est pair et 3^n est impair.
Avec les restes dans la division par 5 obtenus à la question **2d.**, on peut conclure :
si $n \equiv 0 \ [4]$ alors $2^n + 3^n \equiv 2 \ [5]$, donc le chiffre des unités est 7,
si $n \equiv 1 \ [4]$ alors $2^n + 3^n \equiv 0 \ [5]$, donc le chiffre des unités est 5,
si $n \equiv 2 \ [4]$ alors $2^n + 3^n \equiv 3 \ [5]$, donc le chiffre des unités est 3,
si $n \equiv 3 \ [4]$ alors $2^n + 3^n \equiv 0 \ [5]$, donc le chiffre des unités est 5.

3. $888 \equiv 0 \ [4]$, donc le chiffre des unités de $2^{888} + 3^{888}$ est 7.

Applications du PGCD

2



Si une roue à engrenage comportant 56 dents accroche une autre roue à engrenage de 78 dents, combien de tours complets doit effectuer la première roue pour que la seconde réalise aussi un nombre de tours complets ?

Le chapitre en bref

Réinvestir

- La notion de PGCD
- Les propriétés de divisibilité

Explorer

- Les propriétés du PGCD
- L'algorithme d'Euclide
- Le théorème de Bézout
- Le théorème de Gauss

Activités de recherche, p. 46

Activités d'exploration

1 Jeu concours

Réinvestir : La notion de PGCD.

Une enseigne veut offrir à un concours des lots identiques comprenant des DVD et des CD. Elle souhaite y consacrer au total 105 DVD et 180 CD.

a. Afin d'utiliser tous les DVD et CD disponibles, combien l'enseigne peut-elle proposer de lots ?

b. Quel est le plus grand nombre de lots qu'elle peut proposer ? Préciser alors le contenu d'un lot.

COUP DE POUCE

Le nombre de lot est un diviseur du nombre de DVD disponibles et du nombre de CD disponibles. On peut établir la liste des diviseurs communs de 105 et 180.

La notion rencontrée dans l'activité

a et b étant deux entiers naturels non simultanément nuls, on appelle **PGCD(a ; b)** le plus grand diviseur commun à a et b.

2 Propriétés des ensembles de diviseurs

Explorer : Les propriétés du PGCD.

On donne a et b deux entiers naturels non nuls. On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a\,;b)$ l'ensemble des diviseurs positifs communs à a et b.

Partie A. Sur un exemple

1. Déterminer $\mathcal{D}(42)$ et $\mathcal{D}(54)$.
2. En déduire $\mathcal{D}(42\,;54)$ puis PGCD(42 ; 54).

Partie B. Existence du PGCD

Désormais, a est un entier naturel quelconque.

1. Déterminer deux éléments de $\mathcal{D}(a)$.
2. Majorer le nombre d'éléments de $\mathcal{D}(a)$.
3. En déduire que $\mathcal{D}(a\,;b)$ est un ensemble non vide possédant un plus grand élément.

Partie C. Des cas particuliers

1. Montrer que si b divise a, $\mathcal{D}(a\,;b) = \mathcal{D}(b)$. En déduire le PGCD($a$; b).
2. Établir la liste des diviseurs de 0. En déduire PGCD(a ; 0).
3. Justifier la non existence de PGCD(0 ; 0).

Les propriétés rencontrées dans l'activité

Soit a et b deux entiers naturels non simultanément nuls.
On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a\,;\,b)$ l'ensemble des diviseurs positifs communs à a et b.

- $\mathcal{D}(a\,;\,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$ est un ensemble fini et non vide. Il possède toujours un plus grand élément, c'est le PGCD des entiers a et b.
- $\mathcal{D}(a\,;\,b) = \mathcal{D}(b\,;\,a)$ et $\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,a)$.
- $\mathcal{D}(a\,;\,0) = \mathcal{D}(a)$ et $\text{PGCD}(a\,;\,0) = a$.
- Si b divise a, $\mathcal{D}(b) \subset \mathcal{D}(a)$ et $\text{PGCD}(a\,;\,b) = b$.

VERS LE COURS
Démonstrations proposées, p. 37.

3 Recherche du PGCD

Explorer : L'algorithme d'Euclide.
Réinvestir : Les propriétés de divisibilité.

1 On veut déterminer le nombre $g = \text{PGCD}(4\,437\,;\,1\,914)$.

a. Effectuer la division euclidienne de 4 437 par 1 914 et vérifier que le reste vaut 609.

b. Montrer que g divise nécessairement 609. En déduire que g est un diviseur commun à 1 914 et 609.

c. Effectuer la division euclidienne de 1 914 par 609 et montrer que g divise le reste r de cette division.

d. Vérifier que ce reste r divise 609 puis, sans calculs, qu'il divise 1 914 et 4 437.

e. Montrer que $g = r$.

COUP DE POUCE

À la question **e.**, pour montrer que $g = r$, on peut vérifier que g $\quad r$ et r $\quad g$ à l'aide des questions **c.** et **d.**.

2 **Diviseurs du PGCD**

a. Déterminer les diviseurs de g.

b. Vérifier que chacun d'eux est un diviseur commun à 4 437 et 1 914.

c. Démontrer dans le cas général qu'un diviseur de $\text{PGCD}(a\,;\,b)$ divise a et b.

d. Soit d un diviseur commun à 4 437 et 1 914.
À l'aide des divisions successives, montrer que d divise nécessairement g.

e. En déduire la liste des diviseurs communs à 4 437 et 1 914.

L'algorithme rencontré dans l'activité, dit d'Euclide

Soit a et b deux entiers naturels non nuls.

L'algorithme d'Euclide consiste à effectuer la division euclidienne de a par b, puis les divisions euclidiennes successives du diviseur par le reste de chacune des divisions précédentes, jusqu'à ce que le reste soit nul.

Ce processus se termine toujours et le $\text{PGCD}(a\,;\,b)$ est alors le dernier reste non nul r_n.

$$a = b \times q_0 + r_0$$
$$b = r_0 \times q_1 + r_1$$
$$r_0 = r_1 \times q_2 + r_2$$
$$\cdots\cdots$$
$$r_{n-2} = r_{n-1} \times q_n + r_n$$
$$r_{n-1} = r_n \times q_{n+1} + 0$$

VERS LE COURS
Démonstration proposée, p. 38.

La propriété rencontrée dans l'activité

Soit a et b des entiers naturels non nul.
Les diviseurs communs à a et b sont les diviseurs de leur PGCD.

VERS LE COURS
Démonstration proposée, p. 38.

4 Du PGCD aux équations à deux inconnues

Explorer : Les équations diophantiennes.
Réinvestir : Les propriétés de divisibilité.

1 Une équation sans solution

a. Déterminer le nombre $g = \text{PGCD}(16 ; 36)$.

b. Montrer que l'équation $16u + 36v = 6$, où u et v sont des entiers relatifs, n'a pas de solution.

c. Donner une condition nécessaire pour que l'équation $16u + 36v = k$, où k un entier relatif quelconque, ait une solution.

COUP DE POUCE

1.b. Si g divise deux nombres, il divise toute combinaison linéaire de ces deux nombres.

2 Une équation avec une infinité de solution

a. Donner une solution de l'équation $(\mathscr{E}_1)$ $5u + 3v = 1$.

b. Montrer que si $(u_0 ; v_0)$ est une solution de $(\mathscr{E}_1)$, $(u_0 + 3 ; v_0 - 5)$ est aussi solution de $(\mathscr{E}_1)$.

c. En déduire une infinité de solutions de $(\mathscr{E}_1)$.

3 Montrer de même que l'équation $(\mathscr{E}_k)$ $5u + 3v = k$ où k est un entier relatif quelconque, admet une infinité de solution.

Les notions rencontrées dans l'activité

- On dit que deux entiers naturels non nuls a et b sont premiers entre eux (ou étrangers) si leur PGCD est égal à 1.
- **Identité de Bézout**

Soit a et b deux entiers naturels non nuls et g leur PGCD.
Il existe deux entiers relatifs u et v tels que $au + bv = g$.

- **Théorème de Bézout**

Soit a et b deux entiers naturels non nuls.
a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

VERS LE COURS
• Démonstrations proposées, pp. 39 et 40.

5 Diviser pour mieux régner

Explorer : Le théorème de Gauss.
Réinvestir : Les propriétés du PGCD.

1 Vrai/Faux

a. 3 divise 15 et 18 donc 3 divise 15×18.

b. 3 divise 150 donc 3 divise 15 et 10.

c. 3 et 10 divisent 7 110 donc 30 divise 7 110.

d. 6 et 9 divisent 666 donc $6 \times 9 = 54$ divise 666.

2 On donne $a = 8$ et $b = 14$.

a. Déterminer un entier naturel c tel que a divise bc mais a ne divise pas c.

b. Déterminer $g = \text{PGCD}(a ; b)$. Montrer alors que $\frac{a}{g}$ divise c.

3 On choisit désormais $a = 8$ et $b = 15$.
Existe-t-il un entier naturel c tel que a divise bc mais a ne divise pas c ? Expliquer.

Les notions rencontrées dans l'activité

- **Théorème de Gauss :** Soit a, b et c trois entiers naturels non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.
- Soit a, b et c trois entiers naturels non nuls.
Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

VERS LE COURS
Démonstrations proposées, p. 40.

Cours

La notion de plus grand diviseur commun peut être traitée dans $\mathbb{Z}$, mais sa recherche en est facilitée dans $\mathbb{N}$. Dans ce chapitre, nous nous placerons donc dans $\mathbb{N}$, mais l'ensemble des notions peuvent en général être étendues à $\mathbb{Z}$.

A. PGCD de deux entiers naturels

DÉFINITION

Soit a et b deux entiers naturels non simultanément nuls.
On appelle **PGCD(a ; b)** le plus grand diviseur commun à a et b.

EXEMPLE

Les diviseurs de 36 et 63 décrivent les ensembles :

$$\mathcal{D}(36) = \{1 ; 2 ; 3 ; 4 ; 6 ; 9 ; 12 ; 18 ; 36\} \quad \text{et} \quad \mathcal{D}(63) = \{1 ; 3 ; 7 ; 9 ; 21 ; 63\}.$$

Leurs diviseurs communs décrivent alors l'ensemble $\mathcal{D}(36 ; 63) = \{1 ; 3 ; 9\}$.
Le PGCD de 36 et 63 est donc PGCD(36 ; 63) = 9.

PROPRIÉTÉS

Soit a et b deux entiers naturels non simultanément nuls. On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a ; b)$ l'ensemble des diviseurs positifs communs à a et b.

- $\mathcal{D}(a ; b) = \mathcal{D}(a) \cap \mathcal{D}(b)$ est un ensemble fini et non vide. Il possède toujours un plus grand élément, le PGCD(a ; b).
- $\mathcal{D}(a ; b) = \mathcal{D}(b ; a)$ et PGCD(a ; b) = PGCD(b ; a).
- $\mathcal{D}(a ; 0) = \mathcal{D}(a)$ et PGCD(a ; 0) = a.
- Si b divise a, $\mathcal{D}(b) \subset \mathcal{D}(a)$ et PGCD(a ; b) = b.

DÉMONSTRATIONS

- Le nombre de diviseurs positifs de a est inférieur à a (il est compris entre 1 et a), donc $\mathcal{D}(a ; b)$ est un ensemble fini. De plus, 1 appartient à $\mathcal{D}(a ; b)$ qui n'est donc pas vide ; il possède ainsi un plus grand élément.
- L'ensemble des diviseurs de 0 est $\mathcal{D}(0) = \mathbb{N}^*$, donc $\mathcal{D}(a ; 0) = \mathcal{D}(a) \cap \mathcal{D}(0) = \mathcal{D}(a)$. Le plus grand diviseur de a étant lui-même, PGCD(a ; 0) = a.
- Si b divise a, tout diviseur de b est un diviseur de a, d'où $\mathcal{D}(b) \subset \mathcal{D}(a)$. On en déduit que : $\mathcal{D}(a ; b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b)$, et par suite que PGCD($a$; b) = b.

PROPRIÉTÉ

Soit a et b des entiers naturels non nul. En notant r le reste de la division euclidienne de a par b, on a alors $\mathcal{D}(a ; b) = \mathcal{D}(b ; r)$ et PGCD(a ; b) = PGCD(b ; r).

DÉMONSTRATION

En notant q le quotient de la division euclidienne de a par b, on a $a = bq + r$.
Soit d un élément de $\mathcal{D}(b ; r)$. Comme d divise b et r, alors d divise $a = bq + r$ d'où $d \in \mathcal{D}(a ; b)$.
On en déduit que $\mathcal{D}(b ; r) \subset \mathcal{D}(a ; b)$.
Soit d un élément de $\mathcal{D}(a ; b)$. Comme d divise a et b, alors d divise $r = a - bq$ d'où $d \in \mathcal{D}(b ; r)$.
On en déduit que $\mathcal{D}(a ; b) \subset \mathcal{D}(b, r)$.
En conclusion, $\mathcal{D}(b ; r) \subset \mathcal{D}(a ; b)$ et $\mathcal{D}(a ; b) \subset \mathcal{D}(b, r)$ donc $\mathcal{D}(a ; b) = \mathcal{D}(b ; r)$. Il en découle directement que PGCD(a ; b) = PGCD(b ; r).

EXEMPLE

En divisant 474 par 118, on obtient $474 = 118 \times 4 + 2$.
Il en découle que $\mathcal{D}(474 ; 118) = \mathcal{D}(118 ; 2)$ et PGCD(474 ; 118) = PGCD(118 ; 2).
Comme PGCD(118 ; 2) = 2, on peut en déduire immédiatement que PGCD(474 ; 118) = 2.

PROPRIÉTÉ (ALGORITHME D'EUCLIDE)

Soit a et b des entiers naturels non nuls.

L'algorithme d'Euclide consiste à effectuer la division euclidienne de a par b, puis les divisions euclidiennes successives du diviseur par le reste de chacune des divisions précédentes, jusqu'à ce que le reste soit nul.

Ce processus se termine toujours et le PGCD(a ; b) est alors le dernier reste non nul r_n.

$$a = b \times q_0 + r_0$$
$$b = r_0 \times q_1 + r_1$$
$$r_0 = r_1 \times q_2 + r_2$$
$$\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} \times q_n + r_n$$
$$r_{n-1} = r_n \times q_{n+1} + 0$$

DÉMONSTRATION

La suite (r_k) des restes est strictement décroissante car r_{k+1} est le reste dans la division euclidienne par r_k, donc $0 \quad r_{k+1} \quad r_k$.
D'après le principe de descente infinie, il existe donc un entier n tel que $r_{n+1} = 0$.
La propriété précédente justifie que :

$$\mathcal{D}(a ; b) = \mathcal{D}(b ; r_0) = \mathcal{D}(r_0 ; r_1) = \ldots = \mathcal{D}(r_{n-1} ; r_n) = \mathcal{D}(r_n ; 0) = \mathcal{D}(r_n).$$

On en déduit que le plus grand diviseur commun à a et b est r_n.

EXEMPLE

On applique l'algorithme pour calculer le PGCD(364 ; 247).
$364 = 247 \times 1 + 117$
$247 = 117 \times 2 + 13$
$117 = 13 \times 9 + 0$
On en déduit PGCD(364 ; 247) = 13.

PROPRIÉTÉ

Soit a et b deux entiers naturels non nuls.
Les diviseurs communs de a et b sont les diviseurs de leur PGCD.

DÉMONSTRATION

La démonstration est immédiate car la démonstration de la propriété précédente s'appuie sur le fait que $\mathcal{D}(a ; b) = \mathcal{D}(r_n) = \mathcal{D}(\text{PGCD}(a ; b))$.

EXEMPLE

Dans le premier exemple p. 37, les diviseurs communs de 36 et 63 décrivent l'ensemble $\mathcal{D}(36 ; 63) = \{1 ; 3 ; 9\}$ et PGCD(36 ; 63) = 9.

CONSÉQUENCE

Pour tous entiers naturels a, b et k : PGCD(ka ; kb) = $k \times$ PGCD(a ; b).

▶ Savoir-faire 1
Rechercher un PGCD à l'aide de l'algorithme d'Euclide, p. 41

EXEMPLE

On peut ainsi simplifier un calcul de PGCD lorsqu'un facteur commun évident apparaît.
PGCD(170 ; 210) = 10 × PGCD(17 ; 21)
= 10 × 1 = 10.

B. Théorème de Bézout

DÉFINITION

On dit que deux entiers naturels non nuls a et b sont premiers entre eux (ou étrangers) si leur PGCD est égal à 1.

EXEMPLES

- 12 et 35 sont premiers entre eux.
- Si $g = \text{PGCD}(a\,;\,b)$ alors $\frac{a}{g}$ et $\frac{b}{g}$ sont premiers entre eux. En effet, il existe a' et b' entiers naturels tels que $a = ga'$ et $b = gb'$, on a $g = \text{PGCD}(a\,;\,b) = \text{PGCD}(a'g\,;\,b'g) = g \times \text{PGCD}(a'\,;\,b')$, puis en simplifiant par g, on obtient bien $\text{PGCD}(a'\,;\,b') = 1$.

PROPRIÉTÉ (IDENTITÉ DE BÉZOUT)

Soit a et b deux entiers naturels non nuls et g leur PGCD.
Il existe deux entiers relatifs u et v tels que $\boldsymbol{au + bv = g}$.

DÉMONSTRATION

On considère l'ensemble E des combinaisons linéaires positives de a et b :

$$E = \{am + bn \in \mathbb{N}^*, \text{ avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{Z}\}.$$

E est non vide car il contient a et b, donc E admet un plus petit élément noté d (axiome du plus petit élément, p. 6). Il existe donc deux entiers relatifs u et v tels que $au + bv = d$.

- Montrons que $\boldsymbol{d = \text{PGCD}(a\,;\,b)}$.

Pour cela, on va montrer que $\text{PGCD}(a\,;\,b) \quad d$ et que $d \quad \text{PGCD}(a\,;\,b)$.
Comme le PGCD de a et b divise a et b, il divise toute combinaison linéaire de ces entiers.
En particulier, il divise d. On en déduit que $\text{PGCD}(a\,;\,b) \quad d$.

- Montrons que $\boldsymbol{d}$ **divise** $\boldsymbol{a}$ **et** $\boldsymbol{b}$.

On effectue la division euclidienne de a par d : il existe des entiers q et r tels que :

$$a = dq + r \quad \text{avec} \quad 0 \quad r \quad d.$$

Or $r = a - dq = a - (au + bv)q = a - auq - bvq = a(1 - uq) - bvq$ est une combinaison linéaire de a et b, positive ou nulle.
Si r n'était pas nul, on aurait construit un élément de E strictement inférieur à d, ce qui est absurde.
On en déduit que r est nul et par suite que d divise a.
On montre de même que d divise b.
d est donc un diviseur commun à a et b, et par définition du PGCD, $d \quad \text{PGCD}(a\,;\,b)$.
En conclusion, $d = \text{PGCD}(a\,;\,b)$ et il existe donc une combinaison linéaire de a et b telle que $au + bv = \text{PGCD}(a\,;\,b)$.

EXEMPLE

$\text{PGCD}(18\,;\,30) = 6$. On peut trouver un couple u et v tels que $18u + 30v = 6$, par exemple le couple $(2\,;\,-1)$ car $18 \times 2 + 30 \times (-1) = 36 - 30 = 6$.

REMARQUES

1. On établira un procédé algorithmique permettant de trouver un couple solution p. 49.
2. Il n'y a pas d'unicité du couple $(u\,;\,v)$ trouvé. Dans l'exemple précédent, le couple $(-3\,;\,2)$ convient aussi.
On déterminera l'ensemble de ces couples en résolvant les *équations diophantiennes*, p. 44.
3. Ce théorème n'admet pas de réciproque ; en effet si $d = au + bv$, d n'est pas nécessairement le PGCD des entiers a et b.
Contre-exemple : $2 = 1 + 1$ et pourtant 2 n'est pas le PGCD du couple $(1\,;\,1)$.

THÉORÈME (DE BÉZOUT)

Soit a et b deux entiers naturels non nuls.
Les entiers a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

DÉMONSTRATION

L'identité de Bézout justifie le sens direct du théorème.
Si PGCD(a ; b) = 1 alors il existe deux entiers relatifs u et v tels que $au + bv = 1$.
On suppose désormais qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.
Le PGCD des entiers a et b divise a et b, il divise donc $au + bv = 1$. Le seul diviseur positif de 1 étant lui-même, PGCD(a ; b) = 1.

▶ Savoir-faire 2
Déterminer un PGCD à l'aide d'une égalité de Bézout, p. 41

EXEMPLE

On peut appliquer le théorème pour démontrer que $2n + 1$ et $9n + 4$ sont premiers entre eux pour tout $n \in \mathbb{N}$ car $(2n + 1) \times 9 - (9n + 1) \times 2 = 1$.

C. Théorème de Gauss

THÉORÈME (DIT DE GAUSS)

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

DÉMONSTRATION

a divise bc, donc il existe un entier k tel que $bc = ka$.
a et b sont premiers entre eux. D'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = 1$.
En multipliant cette égalité par c, on obtient $auc + bvc = c$ et par suite, comme $bc = ka$, l'égalité devient $auc + kav = c$, soit en factorisant $a(uc + kv) = c$.
Ceci montre que a divise c.

EXEMPLE

Si 4 divise $3^{10} \times n$, comme 4 et 3^{10} sont premiers entre eux, on sait alors que 4 divise n.

PROPRIÉTÉ

Soit a, b et c trois entiers naturels non nuls.
Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

NOTE

Cette propriété est un corollaire du théorème de Gauss.

DÉMONSTRATION

Si a et b divisent c, il existe deux entiers k et k' tels que $c = ka = k'b$. On en déduit que a divise $k'b$; or a et b sont premiers entre eux donc, d'après le théorème de Gauss, a divise k'. Il existe donc un entier k'' tel que $k' = k''a$.
On obtient $c = k'b = k''ab$, d'où ab divise c.

▶ Savoir-faire 3
Résoudre des équations à l'aide du théorème de Gauss, p. 42

▶ Savoir-faire 4
Déterminer un diviseur composé, p. 42

EXEMPLE

Comme 4 et 7 divisent 700 et 4 et 7 sont premiers entre eux alors que $4 \times 7 = 28$ divise 700.

REMARQUE

La condition « a et b premiers entre eux » est essentielle dans le théorème et la propriété qui en découle. On peut proposer deux contre-exemples :

- 6 divise $8 \times 9 = 72$ mais 6 ne divise ni 8 ni 9.
- 4 et 6 divisent 12 mais 4×6 ne divise pas 12.

Savoir-faire

Savoir-faire 1 — Rechercher un PGCD à l'aide de l'algorithme d'Euclide

ÉNONCÉ **1.** Déterminer le PGCD(252 ; 364).

2. En déduire l'ensemble des diviseurs communs de 252 et 364.

SOLUTION

1. On exécute l'algorithme d'Euclide.

$364 = 252 \times 1 + 112$

$252 = 112 \times 2 + 28$

$112 = 28 \times 4 + 0$

Le PGCD(252 ; 364) est le dernier reste non nul, c'est-à-dire 28.

2. Les diviseurs communs de 252 et 364 sont les diviseurs de 28, c'est-à-dire 1, 2, 4, 7 et 28.

Exercices 4 et 6 p. 43

MÉTHODE

En exécutant l'algorithme, la première division aurait du être celle de 252 par 364.
Mais celle-ci donne $252 = 364 \times 0 + 252$ et nous mène donc à effectuer ensuite celle de 252 par 364.
On peut ainsi toujours commencer par diviser le plus grand des deux nombres par le plus petit.
Ceci sera toujours valable puisque :

$$\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,a).$$

Savoir-faire 2 — Déterminer un PGCD à l'aide de l'identité de Bézout

ÉNONCÉ **1.** Montrer que, pour tout entier naturel n, $2n + 5$ et $3n + 7$ sont premiers entre eux.

2. Déterminer le PGCD$(2n + 1\,;\,2n + 3)$ pour tout entier naturel n.

SOLUTION

1. On choisit les coefficients de Bézout : $u = 3$ et $v = -2$.

$3(2n + 5) - 2(3n + 7) = 6n + 15 - 6n - 14 = 1$.

D'après le théorème de Bézout, on en déduit que $2n + 5$ et $3n + 7$ sont premiers entre eux.

2. On peut trouver une combinaison linéaire de $2n + 1$ et $2n + 3$ indépendante de n :

$$-(2n + 1) + (2n + 3) = 2.$$

Le PGCD$(2n + 1\,;\,2n + 3)$ divise toute combinaison linéaire de $2n + 1$ et $2n + 3$, il divise donc 2.

On en déduit que PGCD$(2n + 1\,;\,2n + 3)$ vaut 1 ou 2, or $2n + 1$ et $2n + 3$ sont des nombres impairs quelque soit l'entier naturel n, donc 2 ne les divisent pas ; d'où PGCD$(2n + 1\,;\,2n + 3) = 1$.

Exercices 14 à 20 pp. 43 et 44

MÉTHODE

1. On cherche une égalité de Bézout valable pour tout entier n.
Le meilleur moyen consiste à choisir des coefficients de Bézout permettant d'éliminer n dans la combinaison linéaire $au + bv$.

2. Une égalité de Bézout (combinaison linéaire $au + bv = c$) n'est pas nécessairement une identité de Bézout ($au + bv = \text{PGCD}(a\,;\,b)$) mais elle permet de limiter la recherche du PGCD$(a\,;\,b)$ aux seuls diviseurs de c.

Savoir-faire 3 — Résoudre des équations à l'aide du théorème de Gauss

ÉNONCÉ **1.** Résoudre dans $\mathbb{Z}$ l'équation $3x = 5y$.
2. Résoudre dans $\mathbb{Z}$ l'équation $273x = 637y$.

SOLUTION

1. Puisque $3x = 5y$, 3 divise $5y$. Or 3 et 5 sont premiers entre eux donc d'après le théorème de Gauss, 3 divise y.
Il existe donc un entier relatif k tel que $y = 3k$.
On en déduit que $3x = 5 \times 3k$ puis que $x = 5k$.
Les solutions sont de la forme $(5k ; 3k)$ avec k un entier relatif ; or ceci est vrai quel que soit k car :
$3 \times (5k) = 5 \times (3k)$ pour tout k.
En conclusion, les solutions sont les couples $(5k ; 3k)$ avec k décrivant $\mathbb{Z}$.
2. On cherche d'abord le PGCD(273 ; 637).
$637 = 273 \times 2 + 91$
$273 = 91 \times 3 + 0$.
PGCD(273 ; 637) = 91. On peut donc simplifier l'équation par 91, on obtient $3x = 7y$.
Comme 3 et 7 sont premiers entre eux, on peut appliquer la méthode de la question **1.**
Les solutions sont les couples $(7k ; 3k)$ avec k décrivant $\mathbb{Z}$.

Exercices 25 à 26 p. 44

MÉTHODE

1. La démonstration se déroule en deux temps.
On montre tout d'abord que les solutions sont de la forme $(5k ; 3k)$ mais on ne sait pas pour quelles valeurs de k ceci est valable, on sait juste « qu'il existe k » donnant des solutions.
Ensuite, on montre que quel que soit l'entier relatif k, ces couples sont solutions de l'équation.

2. En simplifiant par le PGCD des deux nombres, on est assuré que les coefficients restants sont premiers entre eux.

Savoir-faire 4 — Déterminer un diviseur composé

ÉNONCÉ **1.** Montrer que le produit de trois entiers naturels consécutifs est divisible par 6.
2. Montrer que le produit de quatre entiers naturels consécutifs est divisible par 24.

SOLUTION

1. Trois entiers consécutifs comprennent nécessairement un nombre pair et un nombre divisible par 3.
Leur produit est donc divisible par 2 et par 3 ; or 2 et 3 sont premiers entre eux donc ce produit est divisible par $2 \times 3 = 6$.
2. Quatre entiers consécutifs comprennent nécessairement un nombre divisible par 3 et deux nombres pairs : un nombre divisible par 4 et un nombre divisible par 2 sans être divisible par 4. Le produit de ces deux nombres est donc divisible par $4 \times 2 = 8$.
Le produit de quatre entiers consécutifs est donc divisible par 8 et 3 qui sont premiers entre eux. Ce produit est donc divisible par $8 \times 3 = 24$.

Exercice 29 p. 44

MÉTHODE

La phrase « Trois entiers consécutifs comprennent nécessairement un nombre pair et un nombre divisible par 3 » ne signifie pas que ces nombres sont distincts.
Par exemple, le produit $5 \times 6 \times 7$ contient un seul nombre divisible par 2 et par 3.

Exercices d'application

PGCD de deux entiers naturels

1 **a.** Déterminer l'ensemble des diviseurs positifs communs de 52 et 78.
b. En déduire leur PGCD.

2 Peut-on trouver deux entiers naturels a et b tels que :
$\text{PGCD}(a\,;b) = 11$ et $a + b = 111$?

3 n est un entier naturel non nul.
a. Déterminer $\text{PGCD}(n\,;5n)$.
b. Déterminer $\text{PGCD}(n\,;n^2)$.

4 Calculer, à l'aide de l'algorithme d'Euclide, le PGCD des nombres suivants :
a. 47 et 1 182
b. 755 et 142
c. 2 125 et 2 482

Savoir-faire 1, p. 41

5 **a.** Montrer que la fraction $\frac{119}{247}$ est irréductible.
b. Simplifier la fraction $\frac{1\,846}{2\,418}$ pour la rendre irréductible.

6 **a.** Déterminer $\text{PGCD}(408\,;984)$.
b. En déduire le plus petit multiple commun de 408 et 984.
c. Réduire le nombre $a = \frac{1}{408} - \frac{1}{984}$.
d. En déduire que $\frac{1}{a}$ est un entier.

7 n est un entier naturel supérieur à 2.
Déterminer à l'aide de l'algorithme d'Euclide les PGCD des nombres suivants :
a. $n+1$ et n **b.** $2n+1$ et n **c.** $2n+1$ et $2n+3$

8 a et b sont deux entiers naturels tels que $\text{PGCD}(a\,;b) = 1$. L'algorithme d'Euclide a donné comme quotients successifs 2, 3, 4 et 5 (la dernière ligne est donc : $5 = 1 \times 5 + 0$). Déterminer a et b.

9 Déterminer sans calculs $\text{PGCD}(10\,000\,;11\,000)$.

10 **a.** Déterminer $\text{PGCD}(564\,;612)$.
b. En déduire la liste des diviseurs communs de 564 et 612.

11 Une grande entreprise offre pour Noël à ses meilleurs salariés des lots identiques comprenant des places de cinéma et des séances de balnéothérapie.
Elle dispose de 240 places de cinéma et 150 séances de balnéothérapie.
Déterminer tous les nombres possibles de salariés qui peuvent bénéficier de ces cadeaux.

12 Trouver les entiers naturels a 270 tels que $\text{PGCD}(a\,;270) = 15$.

13 Déterminer les couples $(a\,;b)$ d'entiers naturels tels que :
a. $a + b = 296$ et $\text{PGCD}(a\,;b) = 37$.
b. $ab = 3\,549$ et $\text{PGCD}(a\,;b) = 13$.

Théorème de Bézout

14 À l'aide du théorème de Bézout, montrer que les nombres suivants sont premiers entre eux :
a. 1510 et 503
b. 51 et 76
c. 1111 et 5000

15 À l'aide du théorème de Bézout, montrer que deux entiers naturels non nuls consécutifs sont premiers entre eux.

16 À l'aide du théorème de Bézout, montrer que pour tout entier naturel n, les entiers $3n + 7$ et $4n + 9$ sont premiers entre eux.

Savoir-faire 2, p. 41

17 Montrer que la fraction $\frac{n}{n^2+1}$ est irréductible pour tout entier naturel n.

18 À l'aide d'une combinaison linéaire, montrer que le PGCD de 5 004 et 2 002 est 2.

19 À l'aide d'une combinaison linéaire, déterminer le PGCD des nombres suivants :
a. 51 et 150
b. 61 et 150

20 À l'aide d'une combinaison linéaire, montrer que deux entiers naturels impairs consécutifs sont premiers entre eux.

21 **a.** Écrire l'algorithme d'Euclide pour déterminer $g = \text{PGCD}(78 ; 102)$.

b. En déduire deux entiers relatifs u et v tels que :

$$78u + 102v = g$$

COUP DE POUCE

Voir la méthode dans la résolution de problème, p. 49.

22 n est un entier naturel.

On donne : $a = 2n + 3$ et $b = 3n + 2$.

a. Montrer que $\text{PGCD}(a ; b)$ est divisible par 5.

b. Montrer que $\text{PGCD}(a ; b)$ divise $b - a$.

c. En déduire que $\text{PGCD}(a ; b) = 5$ si, et seulement si, $n - 1$ est divisible par 5.

23 On souhaite trouver les valeurs de n 5 telle que la fraction $\frac{n+11}{n-4}$ soit entière.

a. Montrer qu'alors $\text{PGCD}(n - 4 ; n + 11) = n - 4$.

b. À l'aide d'une combinaison linéaire indépendante de n, préciser les valeurs possibles de :

$$\text{PGCD}(n - 4 ; n + 11).$$

c. Conclure.

Théorème de Gauss

24 Déterminer les entiers relatifs x et y tels que :

a. $2x = 5y$

b. $12x = 20y$

c. $3(x + 3) = 2(y - 1)$

Savoir-faire 3, p. 42

25 On cherche les solutions entières de l'équation :

$$(E)\ 7x + 13y = 1$$

a. Déterminer une solution $(x_0 ; y_0)$ de (E).

b. Montrer qu'une solution $(x ; y)$ de (E) vérifie l'équation $7(x - x_0) = 13(y_0 - y)$.

c. Résoudre cette équation.

26 On cherche les solutions entières de l'équation :

$$(E)\ 12x + 18y = 30$$

a. Déterminer une solution $(x_0 ; y_0)$ de (E).

b. Montrer qu'une solution $(x ; y)$ de (E) vérifie l'équation $2(x - x_0) = 3(y_0 - y)$.

c. Résoudre cette équation.

27 n est un entier naturel non nul tel que n divise :

$$P(n) = n^2 + 3n + 2$$

a. Factoriser $P(n)$.

b. Montrer que n divise $n + 2$.

c. En déduire les valeurs possibles de n.

28 n est un entier naturel non nul tel que n divise :

$$P(n) = 2n^2 + 5n + 3$$

a. Factoriser $P(n)$.

b. Montrer que n divise $2n + 3$.

c. En déduire les valeurs possibles de n.

29 Montrer que, pour tout entier naturel n :

a. $n(n + 1)(n + 2)$ est divisible par 6.

b. $n(n + 1)(n + 2)(n + 3)$ est divisible par 24.

c. $n(n + 1)(n + 2)(n + 3)(n + 4)$ est divisible par 120.

Savoir-faire 4, p. 42

30 a et b sont deux entiers de parité différente premiers entre eux.

On cherche g le PGCD de $a + b$ et $a - b$.

a. Montrer que g divise $2a$ et $2b$.

b. Montrer que g est premier avec 2.

En déduire que g divise a et b.

c. Conclure.

31 On souhaite trouver les valeurs de l'entier naturel n telles que la fraction $\frac{n(2n+1)}{n+1}$ soit irréductible.

a. Montrer que si $n + 1$ divise $n(2n + 1)$, alors $n + 1$ divise $2n + 1$.

b. Montrer que $n + 1$ et $2n + 1$ sont premiers entre eux.

c. Conclure.

32 L'objectif est trouver l'ensemble des multiples de 17 dont le chiffre des unités est 3.

Le problème revient à résoudre l'équation :

$$(E)\ 17x \equiv 3\ [10]$$

a. Montrer que l'équation (E) équivaut à :

$$17(x - 9) \equiv 0\ [10].$$

b. À l'aide du théorème de Gauss, déterminer les valeurs possibles de x.

c. En déduire le premier de ces nombres supérieur à 1 000.

33 On souhaite déterminer l'ensemble E des entiers naturels n tels que le reste dans la division euclidienne de n par 7 est 3 et le reste dans la division euclidienne de n par 5 est 1.

a. Montrer que $n + 4$ est divisible par 5 et par 7.

b. En déduire que $n + 4$ est divisible par 35, puis donner la liste des valeurs possibles de n.

c. Déterminer la plus petite valeur de E supérieure à 2 000.

34 Dimitri sait qu'il a entre 60 et 100 paires de chaussettes. Dimitri est maniaque et aime bien qu'il y ait autant de paire de chaussettes dans chaque tiroir.

Qu'il ait 3 ou 5 tiroirs, il peut ranger autant de paire de chaussettes dans chaque tiroir, mais s'il a 4 tiroirs, alors il lui reste 3 paires non rangées.
Dimitri se demande combien il a de paires de chaussettes.

a. Montrer que le nombre de paires de chaussettes est un multiple de 15.

b. Justifier que le nombre de paires de chaussettes est impair.

c. Conclure.

Exercices d'entraînement

35 **PGCD de trois nombres**

Le PGCD de trois entiers naturels a, b et c est le plus grand multiple commun à ces trois nombres.
On le note PGCD(a ; b ; c).

a. Déterminer PGCD(56 ; 84 ; 105)

b. Montrer que PGCD(a ; b ; c) = PGCD(PGCD(a ; b) ; c).

c. En déduire PGCD(798 ; 966 ; 1 239).

d. Déterminer trois nombres a, b et c tels que PGCD(a ; b ; c) = 1 et tels qu'aucun des couples (a ; b), (a ; c) et (b ; c) ne soient des couples nombres premiers entre eux.

36 **Algorithme des différences**

Au collège, Mélanie a appris une autre méthode que l'algorithme d'Euclide pour rechercher le PGCD de deux nombres. Elle donne en exemple ci-contre le début de l'algorithme pour $a = 697$ et $b = 323$.

697 – 323 = 374
374 – 323 = 51
323 – 51 = 272
272 – 51 = 221
.....
.....

Elle remplace successivement le plus petit des deux nombres par la différence du plus grand par le plus petit des nombres. L'algorithme s'arrête lorsque la différence vaut 0 et le dernier nombre obtenu non nul est le PGCD.

Partie 1. Fonctionnement de l'algorithme

1. Terminer l'exemple de Mélanie.

2. Montrer que, pour tout entiers a et b :
PGCD(a ; b) = PGCD(a ; $b - a$)

3. En déduire que l'algorithme précédent mène bien toujours au PGCD(a ; b).

Partie 2. Comparaison avec l'algorithme d'Euclide

1. Effectuer l'algorithme d'Euclide.

2. Justifier que le nombre d'égalités nécessaire pour l'algorithme des différences est supérieur ou égal à celui de l'algorithme d'Euclide.

Partie 3. Un cas particulier

1. Comparer ces deux méthodes pour calculer le PGCD de 89 et 55.

2. La suite de Fibonacci est définie ainsi :
$u_0 = 1$, $u_1 = 1$ et, pour tout n 2, on a $u_{n+2} = u_{n+1} + u_n$

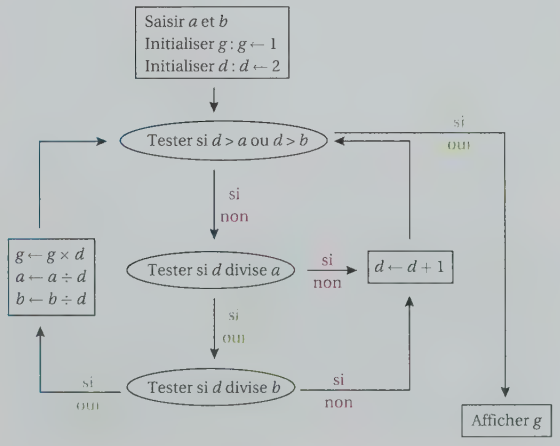
a. Montrer que la suite (u_n) est strictement croissante pour n 2.
En déduire pour n 0 le PGCD(u_{n+1} ; u_n) par l'algorithme des différences.

b. Montrer que, pour tout n 2, le reste de u_{n+2} dans la division euclidienne par u_{n+1} est u_n.
En déduire une comparaison entre le nombre d'égalités nécessaires de l'algorithme d'Euclide et de l'algorithme des différences.

c. Vérifier que 89 et 55 sont bien des nombres consécutifs de la suite de Fibonacci.

37 **L'algorithme de Marc**

Marc, qui n'aime pas Euclide, montre à Yanis son dernier algorithme pour calculer le PGCD de a et b.



a. Écrire pas à pas la suite des étapes que réalise l'algorithme si $a = 6$ et $b = 9$.

b. Écrire pas à pas la suite des étapes que réalise l'algorithme si $a = 3$ et $b = 4$.

c. Expliquer « simplement » son principe.

d. Yanis prétend que cet algorithme n'est pas capable de calculer PGCD(0 ; 5). A-t-il raison ? Expliquer.

e. Proposer une modification pour palier cette erreur.

38 Irrationnelle racine

On souhaite étudier l'irrationalité de $\sqrt{n}$ pour tout entier naturel n.

1. Montrer que si a est premier avec b, alors a est premier avec b^2, puis a^2 est premier avec b^2.

2. On suppose que $\sqrt{n} = \frac{a}{b}$ avec $\frac{a}{b}$ une fraction irréductible (a et b sont donc premiers entre eux).

a. Montrer que n divise a^2.

b. Montrer que a^2 divise n.

c. Conclure.

39 PPCM

On appelle PPCM de deux nombres, le plus petit multiple commun à ces deux nombres.

1. Exemples

a. Déterminer l'ensemble des 15 premiers multiples strictement positifs respectivement de 12 et de 20.

b. En déduire le PPCM(12 ; 20).

c. Conjecturer un résultat sur l'ensemble des multiples communs de 12 et 20.

2. PPCM et PGCD

a et b sont deux entiers naturels. On notera g le PGCD(a ; b) et E l'ensemble des multiples communs strictement positifs de a et b.

a. Montrer que E n'est pas vide.

b. En déduire qu'il possède un plus petit élément noté PPCM(a ; b).

c. Montrer que $\frac{ab}{g}$ est un multiple commun à a et à b.

d. Soit M un multiple commun à a et b.

À l'aide du théorème de Gauss, montrer que M est un multiple de $\frac{ab}{g}$.

e. Des questions **c.** et **d.** déduire le PPCM(a ; b).

3. Applications

a. Déterminer le PGCD, puis le PPCM de 3 285 et 3 577.

b. Réduire au même dénominateur $\frac{1}{3285} - \frac{1}{3577}$ et rendre la fraction obtenue irréductible.

40 Suites de nombres premiers entre eux

1. On étudie les nombres M_n tels que $M_n = 2^n - 1$ pour tout entier naturel non nul n.

a. Calculer les six premiers termes de la suite (M_n) et vérifier que deux termes consécutifs sont premiers entre eux.

b. Montrer que M_n et M_{n+1} sont premiers entre eux quel que soit n.

2. On étudie les nombres F_n tels que $F_n = 2^{2^n} + 1$ pour tout entier naturel n.

a. Calculer les quatre premiers termes de la suite (F_n) et vérifier que deux termes consécutifs sont premiers entre eux.

b. Calculer $F_{n+1} - (F_n - 2) \times F_n$.

c. En déduire que F_n et F_{n+1} sont premiers entre eux quel que soit n.

NOTE

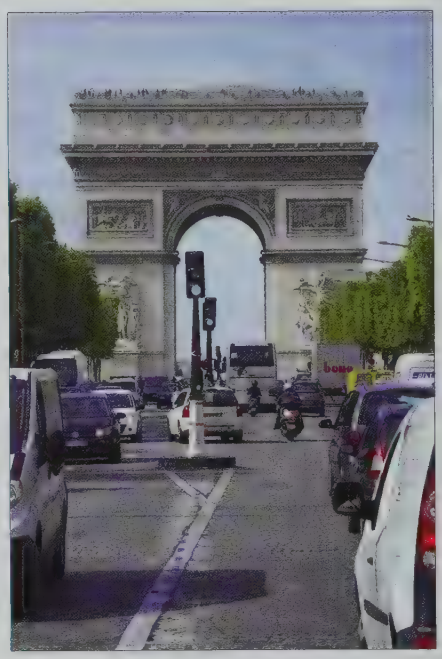
Ces suites génèrent des nombres célèbres : les nombres de Mersenne et de Fermat. Ces nombres aux propriétés nombreuses seront étudiés dans le chapitre 3, p. 74.

41 Feux non synchronisés

Sur un boulevard, deux feux tricolores se succèdent. Le premier passe au vert toutes les 1 minute 10 secondes et le second toutes les 1 minute 31 secondes.

Lorsque le premier feu passe au vert, un automobiliste met 14 secondes pour atteindre le second feu.

À midi pile, les deux feux passent au vert simultanément.



Le but de l'exercice est de trouver à quelle heure après 13 h un automobiliste devrait se présenter devant le premier feu afin que les deux feux passent au vert lorsqu'il sera à leur hauteur.

a. En notant x et y le nombre de fois que le premier et le second feu passe au vert à partir de midi, montrer que les solutions du problème doivent vérifier l'équation :

$$(E)\ 10x - 13y = -2.$$

b. Déterminer une solution particulière de (E).

c. Résoudre l'équation (E).

d. Déterminer la solution du problème.

42 Record

Stefan joue avec Élisa sur une console au *Bric-à-brac*. Le jeu consiste à fabriquer une maison avec des briques de deux formes différentes, à imbriquer entre elles sans laisser de trous. Une brique rouge rapporte 6 points et une brique bleue 15 points.

1. Élisa prétend avoir battu le record avec 10 600 points mais a oublié de l'enregistrer. Stefan prétend qu'elle ment. Peut-on arbitrer ce con it?

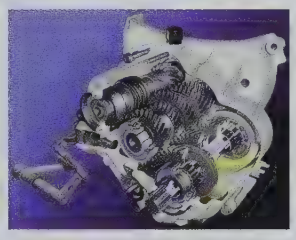
2. Stefan a lui enregistré son record, 6 810 points.
On appelle x le nombre de briques rouges et y le nombre de briques bleues.

a. Montrer que le couple $(x\,;y)$ ayant réalisé le record de Stefan vérifie l'équation $3x + 5y = 2\,270$.

b. Déterminer les solutions entières de cette équation.

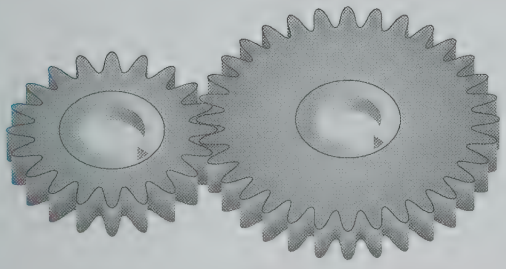
c. Stefan affirme qu'il a placé sur sa maison exactement 826 briques. Est-ce possible ? Si *non* expliquer, si *oui* donner le nombre de briques de chaque couleurs.

43



La transmission d'une boîte de vitesses d'une automobile comporte des roues crantées (pignons) ayant un nombre de dents différentes, permettant de différencier la vitesse de rotation de l'arbre primaire (vitesse fournie par le moteur) et la vitesse de rotation de l'arbre secondaire (vitesse de sortie permettant la traction du véhicule).

1. On suppose que l'arbre primaire comporte 20 dents et l'arbre secondaire 32. Soit le schéma ci-dessous pour simplifier.



a. Montrer qu'une dent de l'arbre secondaire ne rencontre pas tous les creux de l'arbre primaire, et préciser le nombre de creux qu'il rencontre.

b. Ce phénomène entraîne une usure moins régulière des pignons.
Quel nombre de dents aurait-il fallu proposer dans l'arbre secondaire pour l'éviter ?

2. Ces couples de pignons d'une Peugeot 207 1.4 VTI sont donnés ci-dessous en fonction des vitesses :

vitesse	1re	2e	3e	4e	5e
couple	12/41	21/38	32/41	40/39	43/33

Le couple 12/41 signifie 12 dents sur l'arbre primaire, 41 sur le secondaire.
Le choix de ces couples permet-il une usure la plus régulière possible des pignons ?

44 Chinoiseries

On souhaite résoudre le problème suivant :
Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

L'ARMÉE CHINOISE AUX FRONTIÈRES DE MANDCHOURIE
Le maréchal Ma et ses troupes

1. En notant n le nombre de soldats de l'armée de Han Xing, traduire l'énoncé à l'aide de congruences.

2. **a.** Justifier que 5×7 et 3 sont premiers entre eux.

b. Déterminer un multiple m_1 de 35, tel que $m_1 \equiv 1$ [3].

c. Déterminer de manière analogue m_2 et m_3 multiples respectifs de 3×7 et 3×5 tels que :

$$m_2 \equiv 1 \text{ [5] et } m_3 \equiv 1 \text{ [7]}$$

3. Montrer que $n_0 = 2m_1 + 3m_2 + 2m_3$ est solution du problème.

4. Soit k une autre solution du problème.

a. Montrer que $n_0 - k$ est divisible par 105.

b. En déduire l'ensemble des solutions du problème.

c. Déterminer n en supposant que l'armée de Han Xing comptait entre 7 000 et 7 100 soldats.

5. Résoudre de manière analogue le problème suivant.
Qu'il distribue les cartes par 2, par 3 ou par 5, il lui manque toujours une carte pour finir.
Combien a-t-il de cartes sachant que ce nombre est compris entre 60 et 100 ?

NOTES

Ce petit problème fut retrouvé dans le livre d'un mathématicien chinois, Sun Zi au IIIe siècle.
Les propriétés utilisées dans ce problème seront généralisées au XIIIe siècle par un de ses compatriotes, elles sont connues aujourd'hui sous le nom de « Théorème des Chinois ».

Activités de recherche et résolution de problèmes

45 L'algorithme d'Euclide

Algorithmique

On rappelle le principe général de l'algorithme d'Euclide présenté ci-contre :
On divise à chaque étape le diviseur par le reste de la division précédente.
Le PGCD est le dernier reste non nul.

$a = b \times q_0 + r_0$

$b = r_0 \times q_1 + r_1$

$r_0 = r_1 \times q_2 + r_2$

.....

$r_{n-2} = r_{n-1} \times q_n + r_n$

$r_{n-1} = r_n \times q_{n+1} + 0$

1 Réaliser l'algorithme d'Euclide pour déterminer le PGCD de 156 et 132.

2 On note A, B, Q et R les variables utilisées pour chaque boucle.
Une boucle comprend le calcul de Q et R puis la réaffectation des variables A et B pour la boucle suivante.

Compléter le tableau suivant des valeurs successives des variables :

Variables	Q	R	A	B
Entrée			156	132
1re boucle				
2e boucle				
3e boucle				

3 Quelle est parmi les propositions suivantes, la commande utilisée dans la boucle :

- Tant que $R = 0$
- Tant que $R \neq 0$
- Pour R allant de 1 à n
- Si $R = 0$

4 Lally programme son algorithme. Malheureusement celui-ci ne fonctionne pas. Le professeur lui indique qu'il contient trois erreurs.

a. Montrer que le programme de Lally n'exécute jamais la boucle « While » et proposer une modification permettant d'éviter ce problème.

b. Montrer qu'à la fin d'une boucle de ce programme, $A = B$, et proposer une modification afin que pour l'étape suivante A contienne le dividende et B le diviseur.

c. Expliquer pourquoi l'exécution du programme retourne toujours 0.

```
PROGRAM:EUCLIDE
:Prompt A,B
:While R≠0
:PartEnt(A/B)→Q
:A-B*Q→R
:R→B,B→A
:End
:Disp R
```

5 Programmer l'algorithme d'Euclide.

46 Recherche de coefficients de Bézout

Algorithmique

Le but de l'activité est de déterminer de manière algorithmique deux entiers relatifs u et v tels que $au + bv = \text{PGCD}(a\,;b)$ quels que soient les entiers naturels a et b.

Partie 1. Étude d'un exemple

Division 1 : $99 = 37 \times 2 + 25$
Division 2 : $37 = 25 \times 1 + 12$
Division 3 : $25 = 12 \times 2 + 1$
Division 4 : $12 = 1 \times 12 + 0$

1. Exécuter l'algorithme d'Euclide pour $a = 99$ et $b = 37$ et en déduire le PGCD(99 ; 37).
2. À l'aide de la première division de l'algorithme, déterminer deux entiers relatifs u_2 et v_2 tels que $99u_2 + 37v_2 = 25$.
3. À l'aide de la seconde division de l'algorithme, montrer que $12 = 99 \times (-u_2) + 37 \times (1 - v_2)$ et en déduire deux entiers relatifs u_3 et v_3 tels que $99u_3 + 37v_3 = 12$.
4. De même, à l'aide de la troisième division de l'algorithme, déterminer deux entiers relatifs u_4 et v_4 tels que $99u_4 + 37v_4 = 1$.

Partie 2. Cas général

On note (r_n) la suite des restes des divisions euclidiennes successives de l'algorithme d'Euclide et on souhaite construire deux suites d'entiers relatifs (u_n) et (v_n) telles que pour tout entier n on ait $r_n = au_n + bv_n$.

1. En choisissant :
$r_0 = a$ et $r_1 = b$, $u_0 = 1$ et $u_1 = 0$, $v_0 = 0$ et $v_1 = 1$,
vérifier que $r_0 = au_0 + bv_0$ et $r_1 = au_1 + bv_1$.
2. On suppose qu'à l'étape n, on connaît les nombres u_n, u_{n+1}, v_n et v_{n+1} tels que :
$r_n = au_n + bv_n$ et $r_{n+1} = au_{n+1} + bv_{n+1}$.
La division euclidienne de l'algorithme d'Euclide à l'étape $n + 1$ s'écrit :
$r_n = r_{n+1} \times q_{n+1} + r_{n+2}$ (voir l'encadré ci-contre).
Montrer que l'on peut écrire :
$r_{n+2} = au_{n+2} + bv_{n+2}$ avec $\begin{cases} u_{n+2} = u_n - u_{n+1} \times q_{n+1} \\ v_{n+2} = v_n - v_{n+1} \times q_{n+1} \end{cases}$
3. En supposant que le rang du premier reste nul soit $N + 2$, quels sont les termes des suites (u_n) et (v_n) réalisant $au_n + bv_n = \text{PGCD}(a\,;b)$.

L'algorithme d'Euclide avec $r_0 = a$ et $r_1 = b$:
Division 1 : $r_0 = r_1 \times q_1 + r_2$.
Division 2 : $r_1 = r_2 \times q_2 + r_3$.
...
Division $n + 1$:
$r_n = r_{n+1} \times q_{n+1} + r_{n+2}$.
...
Division $N + 1$:
$r_N = r_{N+1} \times q_{N+1} + r_{N+2}$ avec $r_{N+2} = 0$.

Partie 3. Mise en œuvre sur tableur

On souhaite réaliser la feuille de calcul ci-contre, les cellules en bleu étant les variables de saisies.

1. Compléter les colonnes B et C réalisant l'algorithme d'Euclide à l'aide de la fonction ENT.
2. Compléter les colonnes E et F à l'aide des relations de récurrences établies dans la **partie 2.**
3. À l'aide de la feuille de calcul, déterminer les entiers relatifs u et v tels que $354u + 273v = \text{PGCD}(354\,;273)$.

	A	B	C	D	E	F
1	Rang	rn	qn		Un	Vn
2	0	99			1	0
3	1	37	2		0	1
4	2	25	1		1	-2
5	3	12	2		-1	3
6	4	1	12		3	-8
7	5	0	######		-37	99
8	6	######	######		######	######

47 Utiliser une égalité de Bézout

Partie 1.

Étude du PGCD de $a = 3n + 1$ et $b = 5n + 3$ pour tout entier naturel non nul n.

1. À l'aide de la calculatrice.
   - **a.** Construire une table de valeur de a et b pour $n \geqslant 1$.
   - **b.** Ajouter une colonne contenant leur PGCD (utiliser la fonction PGCD de la calculatrice).
   - **c.** Conjecturer pour quelles valeurs de n les nombres a et b semblent premiers entre eux.
   - **d.** Conjecturer pour quelles valeurs de n, on a PGCD$(a\,;\,b) = 4$.
2. À l'aide d'une combinaison linéaire de a et b indépendante de n, démontrer que PGCD$(a\,;\,b)$ est un diviseur de 4.
3. Montrer que si n est pair, a et b sont impairs. En déduire leur PGCD.
4. Montrer que si $n \equiv 1$ [4], a et b sont divisibles par 4. En déduire leur PGCD.
5. Déterminer de même PGCD$(a\,;\,b)$ lorsque $n \equiv 3$ [4].
6. Déterminer sans calcul PGCD(3 001 ; 5 003).

Partie 2.

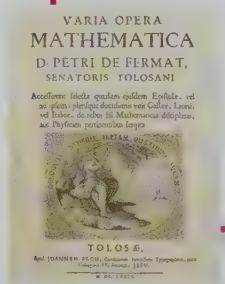
On étudie le PGCD de $a = 2n + 1$ et $b = n(n + 3)$ pour tout entier naturel n.

1. Avec la calculatrice, construire une table de valeur de a, b et PGCD$(a\,;\,b)$ pour $n \geqslant 0$ et conjecturer les valeurs de PGCD$(a\,;\,b)$ en fonction de n.
2. On note g le PGCD de a et $n + 3$.
   - **a.** Montrer que g est un diviseur de 5.
   - **b.** Montrer que $n + 3$ est divisible par 5 si et seulement si $n \equiv 2$ [5].
   - **c.** Montrer que a est divisible par 5 si et seulement si $n \equiv 2$ [5].
   - **d.** En déduire les valeurs de g en fonction des valeurs de n.
3. Montrer que a et n sont premiers entre eux.
4. En déduire que PGCD$(a\,;\,b) = g$.
5. Déterminer sans calcul le PGCD de $2 \times 10^n + 1$ et $10^{n-1}(10^{n-1} + 3)$ pour tout entier $n \geqslant 1$.

48 Les équations diophantiennes

Diophante d'Alexandrie vécut au III^e siècle ; c'est un des plus remarquables mathématiciens grecs de l'Antiquité.

Il s'intéressa aux nombres entiers et fractionnaires et étudia la résolution de nombreuses équations. Celles que l'on traite ici sont les équations linéaires à deux inconnues, mais ces résultats peuvent se généraliser à n inconnues.


VARIA OPERA
MATHEMATICA
D. PETRI DE FERMAT,
SENATORIS TOLOSANI
TOLOSÆ.

Une note de Fermat

Dans le tome 6 de son ouvrage *Arithmetica*, **Diophante** étudie le partage d'un carré en deux carrés ($x^2 + y^2 = z^2$).

C'est dans la marge de ce problème que **Pierre de Fermat** (1601-1665) inscrit sur son exemplaire du manuscrit en latin une note, précisant qu'il est impossible de décomposer une puissance quelconque, sauf le carré, en deux puissances de même exposant ($x^n + y^n = z^n$ pour $n \geqslant 3$), mais il faudra attendre 1994 pour avoir une démonstration de ce résultat par **Andrew Wiles**.

a et b étant deux entiers naturels non nuls et c un entier relatif, on veut résoudre l'équation $ax + by = c$.

Partie 1. Résolution de l'équation $au + bv = \text{PGCD}(a ; b)$

On note g le PGCD de a et b.

1. Justifier qu'il existe un couple $(u_0 ; v_0)$ solution de cette équation.
2. On suppose qu'il existe une autre solution $(u ; v)$ et on pose $a' = \frac{a}{g}$ et $b' = \frac{b}{g}$.
   a. Montrer que $au + bv = au_0 + bv_0$, puis que $a'(u - u_0) + b'(v - v_0) = 0$.
   b. En déduire que a' divise $b'(v_0 - v)$, puis à l'aide du théorème de Gauss que a' divise $v_0 - v$.
   c. Justifier qu'il existe un entier relatif k tel que $v = v_0 - ka'$. Montrer alors que $u = u_0 + kb'$.
   d. Réciproquement, montrer que, quel que soit l'entier relatif k, les couples $(u_0 + kb' ; v_0 - ka')$ sont solution de l'équation $au + bv = g$.
3. PGCD(15 ; 9) = 3. Déterminer l'ensemble des solutions entières de l'équation $15x + 9y = 3$.
4. Interprétation graphique
   a. Donner l'équation réduite de la droite correspondante à l'équation $15x + 9y = 3$.
   b. Construire cette droite pour $-10 \quad x \quad 10$ et marquer les couples solutions trouvés à la question 3.
   c. Interpréter cette construction et notamment le coefficient directeur de cette droite.

Partie 2. Résolution de l'équation $ax + by = c$

1. Montrer que si c n'est pas un multiple de g, le PGCD de a et b, alors l'équation (E_1) $ax + by = c$ n'a pas de solution.
2. On suppose désormais que c est un multiple de g et que $c = c'g$ avec c' un entier relatif. Montrer que l'équation (E_1) équivaut à l'équation (E_2) $a'x + b'y = c'$.
3. À l'aide d'une identité de Bézout, montrer qu'il existe un couple $(x_0 ; y_0)$ solution de (E_2).
4. Résoudre par la méthode de la **partie 1** l'équation (E_2).
5. Résoudre l'équation $15x + 9y = 21$.

Partie 3. Application

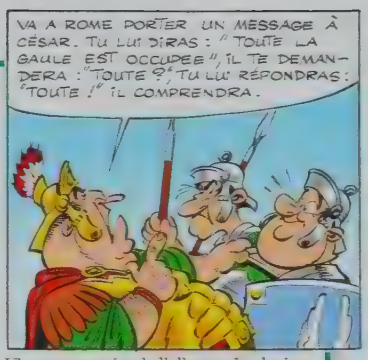
Léo prend le métro pour aller au travail. À la station *Bézout*, il doit changer de rame, la correspondance est sur le même quai. Il sait que son premier métro (ligne A – durée du trajet : 8 minutes) passe toutes les 7 minutes et le second (ligne B) toutes les 11 minutes. Ce matin, il a pris son premier métro à 6 h 52, il est arrivé à 7 h à la station *Bézout* et il a du attendre 6 minutes la rame de la ligne B.
Léo voudrait savoir à quelle heure partir entre 6 h et 9 h pour ne pas attendre la rame de la ligne B à la station *Bézout*.
On note x le nombre de rames de la ligne A et y le nombre de rames de la ligne B passées à la station *Bézout* **après** 7 h.

1. Montrer que, pour que l'attente soit nulle à la station *Bézout*, x et y doivent vérifier l'équation (E_1) $7x - 11y = -5$.
2. Déterminer une solution particulière de l'équation (E_1).
3. En appliquant la méthode utilisée dans la **partie 2**, déterminer l'ensemble des solutions entières de (E_1).
4. Déterminer à quelles heures entre 6 h et 9 h, Léo peut prendre son premier métro pour ne pas attendre à la station *Bézout*.

49 Chiffrements

Les plus anciennes techniques de chiffrement remontent au V^e siècle av. J.-C. avec les Hébreux qui intervertissaient des lettres (le A par le Z, le B par le Y...). Mais c'est à l'époque romaine, sous Jules César, que se développa le chiffrement par décalage. Le principe, assez simple, consistant à décaler toutes les lettres du même nombre de pas (si A devient E, B devient F, etc). Cette méthode simple et facile à décrypter perdura longtemps, notamment de part la faible alphabétisation des populations. Elle fut encore utilisée lors de la guerre de Sécession par les sudistes et aussi par les Russes pendant la Première guerre mondiale.

Des méthodes plus résistantes au déchiffrement apparurent pourtant depuis l'Antiquité, comme le chiffrement affine permettant un plus grand nombre de substitution de lettres et, plus proche de nous, le chiffrement poly-alphabétique, permettant dans un même texte à une lettre de ne pas toujours être codée par la même lettre.



Vignette extraite de l'album « Le devin ».

Quel que soit le mode de chiffrement, la première étape consiste à associer un nombre à chaque lettre, après avoir supprimé les accents et les espaces entre les mots. On utilisera ici la table suivante :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Partie 1. Chiffrement par décalage

Le principe de ce codage consiste à ajouter au nombre n de chaque lettre un entier naturel a appelé « clé de chiffrement » et garder son reste modulo 26.
Le nombre m ainsi obtenu est tel que $m \equiv n + a$ [26] et $0 \leqslant m \leqslant 25$.
Il suffit alors de coder le nombre m par la lettre correspondante.
Exemple : Si la clé est 15 :
- la lettre E chiffrée 4 est associée à la lettre T chiffrée 4 + 15 = 19.
- la lettre S chiffrée 18 est associée à la lettre H chiffrée 7 car 18 + 15 = 33 ≡ 7 [26].

1 Montrer que déchiffrer revient à chiffrer avec une clé à préciser.

2 « *Les sanglots longs des violons de l'automne blessent mon cœur d'une langueur monotone.* »
Ce vers de Paul Verlaine (1844-1896) servit de message secret pendant la Seconde guerre mondiale.
Si, à l'instar de Jules César, les alliés avaient décidé de chiffrer le vrai message par décalage, ils auraient, par exemple, proposé le mot GHEDUTXHPHQW.
La fréquence d'apparition des lettres dans langue française est très irrégulière. La lettre E apparaît en général au moins deux fois plus que les autres lettres fréquemment utilisées.
a. En supposant que cette propriété soit respectée, déterminer la clé de chiffrement.
b. En déduire le déchiffrement du message.

3 Plus récemment, un chiffrement par décalage a été utilisé sur des forums sur internet pour rendre un texte non immédiatement lisible (comme la réponse d'une charade).
La clé a été choisie de telle sorte que chiffrer une seconde fois le texte permet de déchiffrer le message. Quelle a été la clé choisie ?

Partie 2. Chiffrement affine

Le chiffrement affine nécessite une clé de chiffrement constituée de deux entiers a et b, avec $0 < a < 25$ et $0 < b < 25$.

Le principe consiste à associer au nombre n le nombre m tel que :

$$m \equiv an + b \ [26] \quad \text{et} \quad 0 \leqslant m \leqslant 25.$$

1 Si la clé est le couple (3 ; 11), déterminer le cryptage de la lettre T.

2 On peut s'appuyer sur un tableur pour créer une table de cryptage.

	A	B	C	D	E	F	G	H	I
1				S	E	C	R	E	T
2				18	4	2	17	4	19
3	a	3		13	23	17	10	23	16
4	b	11		N	X	R	K	X	Q

En informatique, chaque lettre est chiffrée par un nombre unique (code ASCII). En majuscule, le A est chiffré par le nombre 65, le B par le nombre 66, etc. La fonction CODE associe un nombre à une lettre et la fonction CAR associe une lettre à un nombre (par exemple, CODE(A) = 65 et CAR(65) = A).

a. Réaliser sur l'ordinateur une feuille de calcul semblable à celle ci-dessus.

b. Crypter le mot SOLUTION avec la clé (15 ; 16).

3 On considère qu'un cryptage est exploitable (et donc décryptable) si deux lettres distinctes sont cryptées par deux lettres distinctes.

a. On suppose dans cette question que $a = 15$.

Montrer que deux lettres distinctes sont cryptées par deux lettres distinctes (c'est-à-dire que si $n \neq n'$, alors $m \neq m'$).

b. Montrer que si a est premier avec 26, deux lettres distinctes sont toujours cryptées par deux lettres distinctes.

c. On suppose dans cette question que $a = 2$ et $b = 7$.

Donner un exemple de deux lettres cryptées par la même lettre (on pourra s'appuyer sur la feuille de calcul de la question **2 a.**).

d. On suppose désormais que a n'est pas premier avec 26 et on note g le PGCD de a et de 26.

Montrer que les lettres chiffrées par n et $n + \dfrac{26}{g}$ [26] sont cryptées par la même lettre. Conclure.

e. En déduire le nombre de couples $(a ; b)$ permettant un cryptage exploitable.

4 Pour tout cryptage affine de clé $(a ; b)$, on se propose de trouver une clé $(a' ; b')$ permettant de décrypter par le même procédé.

a. Montrer que si $aa' \equiv 1$ [26] et $a'b + b' \equiv 0$ [26], le couple $(a' ; b')$ convient.

b. Montrer qu'il existe deux entiers relatifs u et v tels que $au + 26v = 1$.

c. En déduire l'existence d'un nombre a' vérifiant l'égalité $aa' \equiv 1$ [26].

d. On suppose dans cette question que $a = 5$ et $b = 17$.

Déterminer un couple $(u ; v)$ tels que $5u + 26v = 1$.

En déduire une valeur de a', puis de b'.

Décrypter à l'aide du tableur le mot SFBIJFYL.

5 Stanislas intercepte le message crypté suivant : TU SATUMT NHMTTU.

Il n'a pas la clé mais pense la retrouver à l'aide du premier mot car il espère que celui-ci est LE.

a. Montrer que la clé $(a ; b)$ vérifierait alors le système $\begin{cases} 11a + b \equiv 19 \ [26] \\ 4a + b \equiv 20 \ [26] \end{cases}$.

b. En déduire que $7a \equiv -1$ [26].

c. Déterminer un couple $(u ; v)$ tels que $7u + 26v = 1$ et en déduire une valeur de a qui convient.

d. Déterminer b et décrypter le message à l'aide de la feuille de calcul.

Partie 3. Chiffrement de Vigenère

Un nouveau cap est franchi avec le chiffrement de **Vigenère**, dont la particularité est qu'une lettre n'est pas toujours codée par la même lettre dans un message, ce qui rend l'analyse des fréquences d'apparition des lettres (comme dans la **partie 1**) inutilisable.
Le principe est le suivant : on choisit une clé qui déterminera le décalage pour chaque lettre du message.
Cette clé sera reproduite autant de fois que nécessite la longueur du message.
Par exemple, le cryptage de « BONJOUR MON AMI » avec la clé CESAR se déroule ainsi :

En clair	B	O	N	J	O	U	R	M	O	N	A	M	I
Clé	C	E	S	A	R	C	E	S	A	R	C	E	S
Décalage	2	4	18	0	17	2	4	18	0	17	2	4	18
En codé	D	S	F	J	F	W	V	E	O	E	C	Q	A

Pour décrypter, il suffit de soustraire la clé au texte chiffré.

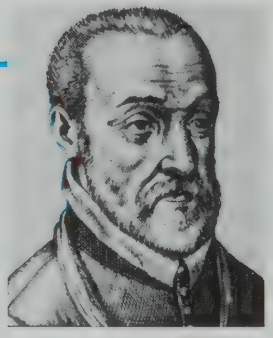
1. Crypter le mot SPECIALITE avec la clé BAC.

2. On suppose que la longueur de la clé est de 3 lettres.
On donne un texte crypté avec cette clé dont le début est donné ci-dessous.
Les lettres ont été regroupées par paquets de 3.
NEK UVG DST CIC VWW SYP BVD SIR FVE I IV FRC JXG OWQ OFG DYP GVQ NEI F…
En étudiant les fréquences d'apparition des lettres sur l'ensemble du texte, on a les résultats suivants :
- la première lettre de chaque mot la plus fréquente est le F ;
- la lettre centrale de chaque mot la plus fréquente est le I ;
- la dernière lettre de chaque mot la plus fréquente est le G.

a. En admettant que la lettre la plus fréquente d'un groupe de lettre assez grand soit un E, déterminer la clé de ce chiffrement.
b. Décrypter le début du texte proposé.

Déjouer les analyses fréquentistes

Blaise de **Vigenère** (1523–1596) était un diplomate français en poste en Italie, ce qui le motiva dans ces premiers travaux de cryptographie. Mais ce n'est que dix ans plus tard qu'il mettra en œuvre ce mode de chiffrement portant aujourd'hui son nom.
Cette méthode, bien plus sûre que le chiffrement par permutation de lettre (comme le chiffrement affine), n'est pas pour autant inviolable.
Comme nous l'avons vu, une analyse fréquentiste peut être réalisée dès lors que l'on connaît la longueur de la clé.
Des méthodes ont été mises en place, notamment par le Prussien Friedrich Wilhelm **Kasiski** (1805-1881) qui étudia les répétitions de séquences identiques de trois lettres dans le texte chiffré. En supposant que ces séquences proviennent d'un même groupe de lettre en clair, leur distance serait un multiple de la longueur de la clé. En étudiant l'ensemble de ces groupes, il découvrait le plus souvent la longueur de la clé.



Blaise de Vigenère (1523-1596)

OBJECTIF BAC

Sujets type BAC

Exercice résolu

Exercice 50 *D'après un sujet de Bac, Pondichéry 2010*

On se propose d'étudier des couples $(a\ ;\ b)$ d'entiers strictement positifs, tels que : $a^2 = b^3$.

Soit $(a\ ;\ b)$ un tel couple et $d = \text{PGCD}(a\ ;\ b)$. On note u et v les entiers tels que $a = du$ et $b = dv$.

1. Montrer que $u^2 = dv^3$.

2. En déduire que v divise u, puis que $v = 1$.

3. Soit $(a\ ;\ b)$ un couple d'entiers strictement positifs. Démontrer que l'on a $a^2 = b^3$ si et seulement si a et b sont respectivement le cube et le carré d'un même entier.

4. En déduire un algorithme permettant de déterminer tous les couples $(a\ ;\ b)$ possibles avec a et b des entiers inférieurs à 500.

5. Montrer que si n est le carré d'un nombre entier naturel et le cube d'un autre entier, alors :

$$n \equiv 0 \ [7] \text{ ou } n \equiv 1 \ [7].$$

Voir résolution page suivante.

Exercice 51

Soit $a = n^2 + 1$ et $b = n(n^2 - 1)$ pour n 1.

Soit $c = \text{PGCD}(a\ ;\ b)$.

a. Montrer que a et n sont premiers entre eux.

En déduire que $c = \text{PGCD}(a\ ;\ n^2 - 1)$.

b. Donner une combinaison linéaire de a et $n^2 - 1$, indépendante de n. En déduire les valeurs possibles de c.

c. Établir le lien entre la parité de n et celle de n^2.

d. En déduire la parité de a et $n^2 - 1$ en fonction de la parité de n.

e. Déterminer c selon la parité de n.

Exercice 52

a et b sont des entiers naturels :

a. Montrer que $\text{PGCD}(a\ ;\ 19) = 1$ ou 19.

b. Montrer que $ab \equiv 0 \ [19]$ équivaut à $a \equiv 0 \ [19]$ ou $b \equiv 0 \ [19]$.

c. En déduire que $a^2 \equiv 4 \ [19]$ équivaut à $a \equiv 2 \ [19]$ ou $a \equiv -2 \ [19]$.

d. Donner l'ensemble E des entiers naturels a inférieurs à 100 vérifiant $a^2 \equiv 4 \ [19]$.

e. Montrer que tous les éléments de E sont premiers avec 19.

Exercice 53 *D'après un sujet de Bac, National 2009*

a. Déterminer l'ensemble des couples $(x\ ;\ y)$ de nombres entiers relatifs, solution de l'équation $(E) : 8x \quad 5y = 3$.

b. Soit m un nombre entier relatif tel qu'il existe un couple $(p\ ;\ q)$ de nombres entiers vérifiant :

$$m = 8p + 1 \text{ et } m = 5q + 4.$$

Montrer que le couple $(p\ ;\ q)$ est solution de l'équation (E) et en déduire que $m \equiv 9 \ [40]$.

c. Déterminer le plus petit de ces nombres entiers m supérieurs à 2 000.

Exercice 54 *D'après un sujet de Bac, National 2011*

Zoé sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9. Si elle fait des tas de 5 jetons, il lui en reste 3.

Combien a-t-elle de jetons ?

1. Écrire un algorithme permettant de déterminer tous les nombres de jetons possibles que possède Zoé, en précisant le nombre total de divisions euclidiennes effectuées.

2. Montrer que trouver le nombre de jetons de Zoé revient à déterminer les éléments de l'ensemble S compris entre 300 et 400, S étant l'ensemble des entiers relatifs n vérifiant le système $\begin{cases} n \equiv 9 \ [17] \\ n \equiv 3 \ [5] \end{cases}$.

3. Recherche d'éléments de S

On désigne par $(u\ ;\ v)$ un couple d'entiers relatifs tels que $17u + 5v = 1$.

a. Justifier l'existence d'un tel couple.

b. On pose $n_0 = 3 \times 17u + 9 \times 5v$.

Démontrer que n_0 appartient à S.

c. Donner un exemple d'entier n_0 appartenant à S.

4. Caractérisation des éléments de S

a. Soit n un entier relatif appartenant à S.

Démontrer que $n - n_0 \equiv 0 \ [85]$.

b. En déduire qu'un entier relatif n appartient à S si et seulement si n peut s'écrire sous la forme :

$$n = 43 + 85k \text{ où } k \text{ est un entier relatif.}$$

5. Déterminer le nombre de jetons de Zoé.

Résolution

1. Comme $a^2 = b^3$, on a $(du)^2 = (dv)^3$.
On en déduit que $d^2u^2 = d^3v^3$ et, par simplification par d^2, que $u^2 = dv^3$.

2. $d = \text{PGCD}(a\,;\,b) = \text{PGCD}(du\,;\,dv) = d \times \text{PGCD}(u\,;\,v)$;
on en déduit que $\text{PGCD}(u\,;\,v) = 1$, c'est-à-dire que les nombres u et v sont premiers entre eux.

Comme $u^2 = dv^3$, on sait que v divise u^2, c'est-à-dire $u \times u$.
Or u et v étant premiers entre eux, en appliquant le théorème de Gauss, on obtient que v divise u.
Par suite, si v divise u, le nombre v est le $\text{PGCD}(u\,;\,v)$, donc $v = 1$.

3. On suppose que $a^2 = b^3$.
Comme $v = 1$ et $u^2 = dv^3$, on déduit que $d = u^2$ et par suite que :

$$a = du = u^3 \quad \text{et} \quad b = dv = d = u^2$$

D'où a et b sont respectivement le cube et le carré d'un même entier u.

Ne pas oublier d'établir l'implication réciproque.

Réciproquement, on suppose qu'il existe un entier u tel que $a = u^3$ et $b = u^2$.
On peut vérifier que $a^2 = b^3 = u^6$.

4. Si a et b sont respectivement le cube et le carré d'un entier strictement positif, on peut remarquer que a est nécessairement supérieur à b. Il suffit donc de construire la liste des cubes et carrés des entiers u décrivant $\mathbb{N}$ tant que a est inférieur à 100.
L'algorithme et son exécution ont été exécutés avec Algobox dans les fenêtres ci-dessous.

Code de l'algorithme

```
VARIABLES
    a EST_DU_TYPE NOMBRE
    b EST_DU_TYPE NOMBRE
    u EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
    a PREND_LA_VALEUR 1
    b PREND_LA_VALEUR 1
    u PREND_LA_VALEUR 1
    TANT_QUE (a<=500) FAIRE
        DEBUT_TANT_QUE
        AFFICHER "("
        AFFICHER a
        AFFICHER ";"
        AFFICHER b
        AFFICHER ")"
        u PREND_LA_VALEUR u+1
        a PREND_LA_VALEUR u*u*u
        b PREND_LA_VALEUR u*u
        FIN_TANT_QUE
FIN_ALGORITHME
```

Résultats

```
*** Algorithme lancé ***
(1;1)
(8;4)
(27;9)
(64;16)
(125;25)
(216;36)
(343;49)

*** Algorithme terminé ***
```

5. On étudie les restes du carré et du cube d'un entier naturel quelconque dans la division euclidienne par 7.

Reste de k	0	1	2	3	4	5	6
Reste de k^2	0	1	4	2	2	4	1
Reste de k^3	0	1	1	6	1	6	6

Les seuls restes communs entre k^2 et k^3 sont 0 et 1, donc si n est le carré d'un entier et le cube d'un autre entier alors $n \equiv 0\ [7]$ ou $n \equiv 1\ [7]$.

Nombres premiers

3

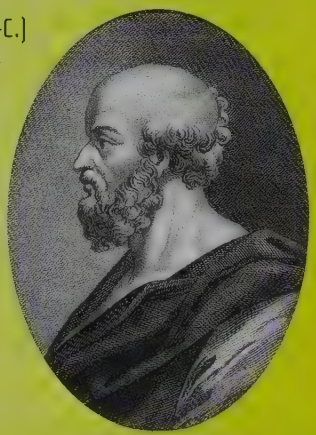
	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

Crible d'Érathostène

Ératosthène (276-194 av. J.-C.)

Ce mathématicien grec établit une méthode permettant d'identifier les nombres premiers inférieurs à un nombre donné, en les « passant au crible » des diviseurs premiers déjà rencontrés. Dès qu'un nombre premier est identifié, on élimine tous ses multiples.

Ératosthène était aussi astronome et il fut le premier à donner une méthode reconnue permettant de mesurer la circonférence de la Terre. La légende veut qu'il se soit laissé mourir de faim car, devenu aveugle, il ne pouvait plus admirer les étoiles.



Le chapitre en bref

Réinvestir

- Les diviseurs d'un entier
- La division euclidienne

Explorer

- Les nombres premiers et leurs propriétés

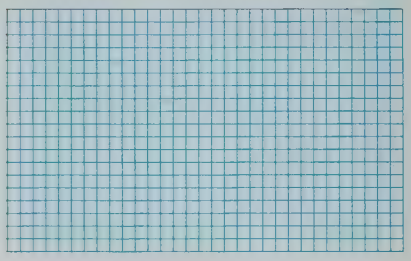
Activités de recherche p. 62

Activités d'exploration

1 Des carrés pour un rectangle

Explorer : Les nombres premiers.

On veut construire un rectangle avec des petits carrés identiques. On ne s'intéresse pas au rectangle constitué d'une seule ligne de petits carrés.



1. Peut-on construire un tel rectangle avec 91 carrés identiques ? Avec 97 carrés identiques ?
2. Quels sont les nombres de petits carrés compris entre 60 et 100 ne permettant pas de réaliser un tel rectangle ?

COUP DE POUCE

1. Faire un dessin et trouver le lien entre la longueur et la largeur du rectangle.
2. On peut éliminer les nombres qui possèdent un diviseur positif autre que 1 ou lui-même.

La notion rencontrée dans l'activité

On dit qu'un entier naturel p est **premier** s'il possède exactement deux diviseurs positifs, 1 et lui-même.

2 Tester la primalité d'un entier

Explorer : Tester la primalité d'un entier.
Réinvestir : Les critères de divisibilité.

Le but du problème est de minimiser le nombre de divisions à effectuer pour déterminer si un entier naturel est premier.

1. À l'aide de critères de divisibilité, montrer que 197 n'est pas divisible par 2, 3 ou 5.
2. Soit n, k, p et q des entiers naturels, p est un nombre premier.
   a. Montrer que si n n'est pas divisible par p, alors n n'est pas divisible par kp (on raisonnera par contraposée).
   b. En déduire sans calcul que par exemple 197 n'est pas divisible par 28.
   c. Montrer qu'il suffit alors de tester des diviseurs premiers pour évaluer la primalité de 197.
3. On supppose de plus dans cette question que $n = pq$ avec $p < q$.
   a. Montrer alors que $p^2 < n$ puis que $p < \sqrt{n}$.
   b. En déduire que si 197 n'est pas premier, il possède alors un diviseur inférieur à $\sqrt{197}$.
4. Montrer que pour justifier la primalité de 197, il suffit d'effectuer trois divisions.
5. Par le même principe, déterminer si 323 et 717 sont premiers, en effectuant un minimum de calculs.

VERS LE COURS
Démonstration proposée, p. 60.

La propriété rencontrée dans l'activité

Tout entier naturel non premier $n > 1$ admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

3 Déterminer les diviseurs d'un entier

Explorer : Décomposition d'un entier en produit de facteurs premiers.

1 Déterminer la liste des diviseurs positifs de 72, puis de 75.

2 On cherche désormais la liste des diviseurs positifs de 1 029.

a. Montrer qu'il suffit de tester les diviseurs inférieurs à $\sqrt{1029}$ pour déterminer la liste de tous les diviseurs positifs de 1 029. Combien de valeurs resterait-il à tester ?

b. Donner la décomposition en produit de facteurs premiers de 1 029.

COUP DE POUCE

Si 72 n'est pas divisible par un entier k, il ne sera divisible par aucun multiple de k.
Si k est un diviseur de 72, alors $\frac{72}{k}$ est aussi un diviseur de 72.

La propriété rencontrée dans l'activité

Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers. Cette décomposition est unique à l'ordre près des facteurs. On note alors :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$$

où $p_1, p_2, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont des entiers naturels non nuls.

VERS LE COURS
Démonstration proposée, p. 61.

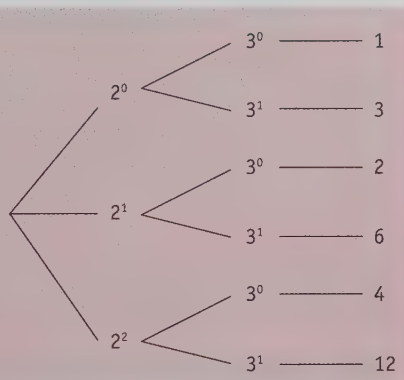
c. À l'aide d'un arbre, représenter l'ensemble des décompositions en produit de facteurs premiers des diviseurs positifs de 1 029.

d. En déduire le nombre puis la liste de ses diviseurs positifs.

COUP DE POUCE

Un arbre des diviseurs permet de faire la liste des diviseurs d'un entier naturel à partir de sa décomposition en produit de facteurs premiers.

Par exemple, l'arbre des diviseurs de 12, ci-contre, comporte six branches finales permettant de lister les diviseurs de 12.



3 On souhaite déterminer le nombre de diviseurs positifs de 3 024.

a. Donner la décomposition en produit de facteurs premiers de 3 024.

b. En déduire le nombre de diviseurs positifs de 3 024.

La propriété rencontrée dans l'activité

En notant $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ la décomposition d'un entier naturel n en produit de facteurs premiers, tout diviseur de n admet une décomposition en produit de facteurs premiers de la forme :

$$p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$$

où $\beta_1, \beta_2, \ldots, \beta_r$ sont des entiers naturels tels que pour tout $1 \leqslant i \leqslant r$, on a $0 \leqslant \beta_i \leqslant \alpha_i$.

VERS LE COURS
Démonstration proposée, p. 61.

A. Nombres premiers

DÉFINITION

On dit qu'un entier naturel p est **premier** s'il possède deux diviseurs distincts positifs, 1 et lui-même.

EXEMPLES

- 1 n'est pas premier .
- 17 est un nombre premier.
- 27 n'est pas un nombre premier car 27 est divisible par 3.

REMARQUE

La liste des nombres premiers inférieurs à 5 000 est donnée sur la page de garde I.

PROPRIÉTÉ

Tout entier naturel **non premier** $n > 1$ admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

DÉMONSTRATION

Puisque n n'est pas premier, il admet des diviseurs autres que 1 et lui-même.

Soit E l'ensemble des diviseurs de n privé de 1 et de lui-même. E n'est pas vide car n n'est pas premier.
D'après l'axiome du plus petit élément, il existe un plus petit élément de E noté p.
Si p n'était pas premier, p possèderait un diviseur p' distinct de 1 et lui-même.
En conséquence $p' < p$ et p' divise n (car il divise p) ; d'où $p' \in E$.
Ceci contredit le fait que p est le plus petit élément de E, donc p est premier.

On suppose que $n = pq$ avec $p < q$ car p est le plus petit diviseur premier de n.
Comme $p < q$, on a $p \times p < p \times q$. On en déduit $p^2 < n$, puis $p < \sqrt{n}$. ■

▶ Savoir-faire 1
Déterminer si un nombre est premier, p. 62

B. Décomposition d'un entier en produit de facteurs premiers

PROPRIÉTÉ

Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers.
Cette **décomposition est unique** à l'ordre près des facteurs.
On note alors $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ où $p_1, p_2, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont des entiers naturels non nuls.

EXEMPLE

On peut décomposer 300 par étapes de plusieurs manières :

$$300 = 2 \times 150 = 2 \times 15 \times 10 = 2 \times 3 \times 5 \times 2 \times 5$$

ou encore $300 = 3 \times 100 = 3 \times 10 \times 10 = 3 \times 2 \times 5 \times 2 \times 5$.

Dans tous les cas, la décomposition sera $300 = 2^2 \times 3 \times 5^2$.

DÉMONSTRATION

Existence

Si n est premier, la propriété est établie.

Sinon, le plus petit diviseur de $n > 1$ est premier (voir la démonstration de la première propriété, p. 60) ; on le note p_1.

On peut donc définir $n_1 = \dfrac{n}{p_1}$ avec $n_1 < n$.

- Si n_1 est premier, la propriété est établie,
- sinon, on réitère le processus : il existe p_2 premier et l'on peut donc définir $n_2 = \dfrac{n_1}{p_2}$ avec $n_2 < n_1$.

On peut créer ainsi une suite (n_k) d'entiers naturels, strictement décroissante. Cette suite est nécessairement finie (principe de descente infinie) et son dernier terme est premier.

En regroupant les facteurs premiers identiques, on obtient $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$.

Unicité

On démontre l'unicité par récurrence à l'aide du théorème de Gauss.

L'unicité de la décomposition est claire pour $n = 2$.

On suppose que la décomposition est unique pour tout entier inférieur strictement à un n donné et on montre que la décomposition de n en produit de facteurs premiers est unique.

On suppose que n admette deux décompositions distinctes en produit de facteurs premiers :

$$n = p_1 \times p_2 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_s$$

Si p_1 était premier avec q_i pour tout $1 \leqslant i \leqslant s$, alors d'après un corollaire du théorème de Gauss, p_1 serait premier avec $q_1 \times q_2 \times \ldots \times q_s$; or p_1 divise $q_1 \times q_2 \times \ldots \times q_s$ d'où une contradiction.

Donc il existe i tel que p_1 et q_i ne sont pas premiers entre eux. Comme ce sont des nombres premiers, on a nécessairement $p_1 = q_i$.

Le nombre $n_1 = \dfrac{n}{p_1}$ admettrait donc deux décompositions distinctes :

$$n_1 = p_2 \times p_3 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_{i-1} \times q_{i+1} \times \ldots \times q_s$$

ce qui contredit l'hypothèse de récurrence car $n_1 < n$ (car $p_2 \geqslant 2$). On en déduit que n admet une décomposition unique.

On a ainsi démontré par récurrence l'unicité de la décomposition pour tout $n \geqslant 2$.

PROPRIÉTÉ

En notant $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ la décomposition d'un entier naturel n en produit de facteurs premiers, tout diviseur de n admet une décomposition en produit de facteurs premiers de la forme :

$$p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$$

où $\beta_1, \beta_2, \ldots, \beta_r$ sont des entiers naturels tels que, pour tout $1 \leqslant i \leqslant r$, on a $0 \leqslant \beta_i \leqslant \alpha_i$.

▶ Savoir-faire 2 Déterminer la décomposition d'un entier en produit de facteurs premiers, p. 62

▶ Savoir-faire 4 Déterminer l'ensemble des diviseurs d'un entier, p. 63

▶ Savoir-faire 5 Dénombrer les diviseurs d'un entier, p. 63

EXEMPLE

Comme $300 = 2^2 \times 3 \times 5^2$, alors le nombre $2^1 \times 3^0 \times 5^2 = 2 \times 5^2 = 50$ est un diviseur de 300.

DÉMONSTRATION

Les nombres de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$ où $\beta_1, \beta_2, \ldots, \beta_r$ sont des entiers naturels tels que, pour tout $1 \leqslant i \leqslant r$, $0 \leqslant \beta_i \leqslant \alpha_i$ sont clairement des diviseurs de $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$.

Réciproquement, en notant d un diviseur de $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$, tout facteur premier de d divise n, donc appartient à la liste $p_1, p_2, \ldots, p_n$. On en déduit que la décomposition en produit de facteurs premiers de d peut s'écrire par extension $p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$, le cas où $\beta_i = 0$ correspondant à l'absence du facteur p_i.

Savoir-faire

Savoir-faire 1 Déterminer si un nombre est premier

ÉNONCÉ Déterminer si 481 et 487 sont des nombres premiers.

SOLUTION

$481 = 13 \times 37$. Il n'est donc pas premier.

487 n'est divisible par aucun nombre premier inférieur à $\sqrt{487} \approx 22{,}1$.

En effet 487 n'est pas divisible par 2, 3, 5, 7, 11, 13, 17 et 19.

Il est donc premier.

Exercices 1 à 9 p. 64

MÉTHODE

- Si un nombre n'est pas premier, il suffit de proposer une décomposition pour le justifier.
- Si un nombre est premier, il faut alors justifier qu'il n'existe pas de diviseur premier inférieur à sa racine carrée et ainsi utiliser la contraposée de la propriété :

« Tout entier naturel non premier $n > 1$ admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$ »

Savoir-faire 2 Déterminer la décomposition d'un entier en produit de facteurs premiers

ÉNONCÉ Déterminer la décomposition de 1 716 en produit de facteurs premiers.

SOLUTION

$$\begin{aligned} 1\,716 &= 2 \times 858 \\ &= 2 \times 2 \times 429 \\ &= 2 \times 2 \times 3 \times 143 \\ &= 2 \times 2 \times 3 \times 11 \times 13 \end{aligned}$$

La décomposition de 1 716 est :

$1\,716 = 2^2 \times 3 \times 11 \times 13$

Exercices 14 à 21 p. 64

MÉTHODE

On cherche un diviseur premier de $n = 1\,716$.

On teste les nombres premiers dans l'ordre croissant jusqu'à trouver un diviseur p ou atteindre $\sqrt{n}$ (ce qui signifierait que n est premier).

On réitère le procédé avec le quotient $\frac{n}{p}$, jusqu'à obtenir un quotient premier.

On réordonne les facteurs premiers et l'on regroupe les facteurs identiques.

Savoir-faire 3 Calcul du PGCD et du PPCM

Ce calcul est réalisé à l'aide de la décomposition en produit de facteurs premiers.

ÉNONCÉ Déterminer le PGCD et le PPCM des entiers 13 734 et 91 260.

SOLUTION

On décompose les deux entiers en produit de facteurs premiers :

$13\,734 = 2 \times 3^2 \times 7 \times 109$ et $91\,260 = 2^2 \times 3^3 \times 5 \times 13^2$

Les diviseurs communs aux deux entiers sont de la forme $2^a \times 3^b$ où $0 \leqslant a \leqslant 1$ et $0 \leqslant b \leqslant 2$, le plus grand d'entre eux est alors $2 \times 3^2 = 18$.

Les multiples communs aux deux entiers sont de la forme $K \times 2^2 \times 3^3 \times 5 \times 7 \times 13^2 \times 109$, où K est un entier.

Le plus petit d'entre eux est obtenu pour $K = 1$:

$2^2 \times 3^3 \times 5 \times 7 \times 13^2 \times 109 = 69\,631\,380$.

Exercices 21 et 23 p. 65

MÉTHODE

Le PGCD de deux entiers est égal au produit de leurs diviseurs premiers communs, chacun d'eux étant élevé de son plus petit exposant.

Le PPCM de deux entiers est égal au produit de tous leurs diviseurs premiers des deux décompositions élevés de son plus grand exposant.

Savoir-faire 4 Déterminer l'ensemble des diviseurs d'un entier

ÉNONCÉ Déterminer la liste des diviseurs de 315.

SOLUTION

On détermine la décomposition de 315 en produit de facteurs premiers.

$315 = 3 \times 105$
$= 3 \times 3 \times 35$
$= 3 \times 3 \times 5 \times 7$

D'où $315 = 3^2 \times 5 \times 7$.

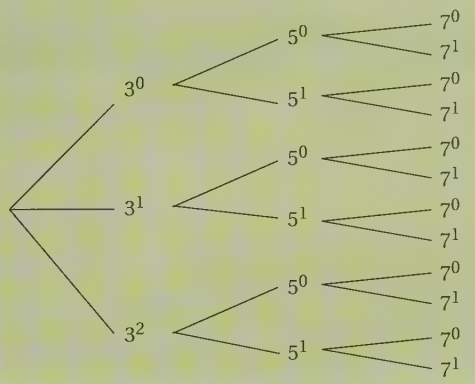
On en déduit la liste des diviseurs de 315 :

$\{1 ; 3 ; 5 ; 7 ; 9 ; 15 ; 21 ; 35 ; 45 ; 63 ; 105 ; 315\}$.

Exercices 24 et 25 p. 65

MÉTHODE

L'arbre permet de ne pas oublier de diviseur.



Savoir-faire 5 Dénombrer les diviseurs d'un entier

ÉNONCÉ Déterminer le nombre de diviseurs de 13 000.

SOLUTION

On détermine la décomposition de 13 000 en produit de facteurs premiers :

$13\,000 = 2^3 \times 5^3 \times 13$

Un diviseur de 13 000 est de la forme $2^{\alpha 1} \times 5^{\alpha 2} \times 13^{\alpha 3}$ avec $0 \leqslant \alpha_1 \leqslant 3$, $0 \leqslant \alpha_2 \leqslant 3$ et $0 \leqslant \alpha_3 \leqslant 1$.

Il y a donc quatre valeurs possibles pour α_1 et α_2, et deux valeurs possibles pour α_3, soit :

$4 \times 4 \times 2 = 32$ combinaisons possibles.

13 000 possède donc 32 diviseurs.

Exercices 26 et 27 p. 65

MÉTHODE

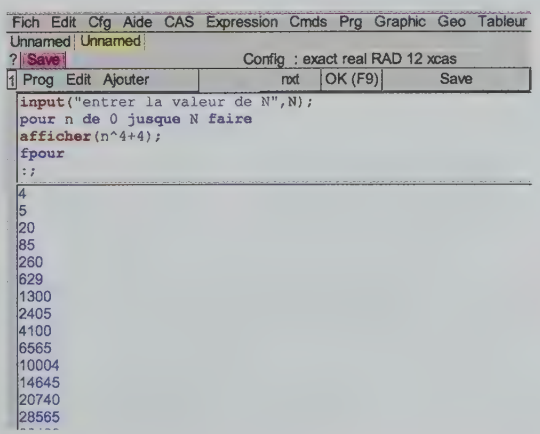
Le produit s'appuie sur la représentation des diviseurs à l'aide d'un arbre.
Même sans le dessiner, on peut dénombrer les branches de l'arbre en multipliant les choix possibles pour chaque facteur premier.
Il y a donc 4 branches pour le facteur 2,
puis 4 branches pour le facteur 5,
suivi de 2 branches pour le facteur 13.

Savoir-faire 6 Utiliser un algorithme pour émettre une conjecture

ÉNONCÉ Soit n un entier naturel. L'entier $N = n^4 + 4$ est-il premier ?

SOLUTION

La boucle ci-contre, écrite à l'aide de Xcas, calcule les termes consécutifs de la suite des entiers de la forme $n^4 + 4$.
On peut constater que 5, obtenu pour $n = 1$, est le seul entier premier.
On démontre cette conjecture en essayant de trouver une factorisation de $n^4 + 4$.
$N = n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 - 2n)(n^2 + 2 + 2n)$.
Or l'entier $n^2 + 2 + 2n$ est supérieur ou égal à 2 ; pour que N soit premier il est donc nécessaire que $n^2 + 2 - 2n$ soit égal à 1, ce qui n'est vrai que pour $n = 1$.



Exercice 35 p. 66

Exercices d'application

Nombres premiers

1 Montrer que les nombres suivants ne sont pas premiers.
a. 2013 **b.** 2015 **c.** 2021

Savoir-faire 1, p. 62

2 Déterminer si les nombres suivants sont premiers.
a. 307 **b.** 407 **c.** 507 **d.** 607

3 Déterminer si les nombres suivants sont premiers.
a. 2011 **b.** 2017 **c.** 2019 **d.** 2021

4 Si un nombre inférieur à 250 n'est divisible par aucun nombre premier inférieur ou égal à 13, est-il premier ?

5 On peut décomposer 107 de cette façon :

$$107 = 2 \times 3 \times 5 + 7 \times 11.$$

En déduire, sans effectuer de division, que 107 est premier.

6 On étudie la primalité de la suite de nombres :

$$u_n = p_1 \times p_2 \times \ldots \times p_n + 1,$$

où les nombres p_1, p_2, ..., p_n décrivent les nombres premiers 2, 3, 5 ... dans l'ordre croissant. Par exemple, $u_1 = 2 + 1$, $u_2 = 2 \times 3 + 1 = 7$ et $u_3 = 2 \times 3 \times 5 + 1 = 31$.

1. Étudier la primalité de u_4 et u_5.

2. Montrer que u_6 admet un diviseur premier compris entre 50 et 60.

7 On étudie la suite (u_n) de nombres définis pour tout $n > 1$ comme la somme des $2n$ premiers nombres premiers.
a. Montrer que u_1, u_2 et u_3 sont premiers.
b. Étudier la primalité de u_n pour tout $n \leqslant 8$.

8 On étudie la suite (u_n) de nombres définis pour tout entier n par $u_n = 3^n + 2$.
a. Vérifier la primalité de u_n pour $n \leqslant 4$.
b. Montrer que pour tout entier n, u_n n'est divisible ni par 2 ni par 3.
c. Étudier la primalité de u_5 et de u_6.

9 **a.** Montrer que pour tout nombre inférieur à 1 000, il suffit de tester au maximum 11 diviseurs pour déterminer sa primalité.
b. Quel est le seul nombre non premier inférieur à 1 000 nécessitant de tester les 11 diviseurs.

10 On dit que deux nombres impairs consécutifs sont **jumeaux** s'ils sont premiers (comme 17 et 19 par exemple). On définit de même des **triplés**, trois nombres impairs consécutifs premiers.
a. Y-a-t-il des triplés inférieurs à 100 ?
b. Montrer que parmi trois nombres impairs consécutifs, l'un d'eux est divisible par 3.
c. Conclure quant à l'existence des triplés.

11 Soit p un nombre premier.
a. Existe-t-il un entier n tel que n et $n + p$ soit simultanément des carrés d'entiers.
b. Exprimer, lorsqu'il existe, n en fonction de p.
c. Déterminer n pour $p = 17$.

12 **a.** Justifier que tout nombre premier supérieur à 10 a pour chiffre des unités 1, 3, 7 ou 9.
b. En déduire que le nombre $(2012 \times 2013)^{2014} - 1$ n'est pas premier.

13 **1.** Vérifier qu'aucun des nombres $n^3 + 1$ n'est premier pour $1 \leqslant n \leqslant 10$.
2. Montrer que $n + 1$ divise $n^3 + 1$ pour tout $n \in \mathbb{N}$.
3. En déduire que $n^3 + 1$ ne peut être premier quel que soit l'entier $n \geqslant 1$.

Décomposition d'un entier en produit de facteurs premiers

14 Décomposer en produit de facteurs premiers les nombres suivants :
a. 286 **b.** 36 **c.** 700 **d.** 89

Savoir-faire 2, p. 62

15 Décomposer en produit de facteurs premiers les nombres suivants :
a. 256 **b.** 405 **c.** 361 **d.** 2310

16 **a.** Décomposer en produit de facteurs premiers les nombres 450 et 630.
b. En déduire la décomposition de 450×630.
c. En déduire la décomposition de $450 + 630$.

17 **a.** Décomposer 126 en produit de facteurs premiers.
b. En déduire la plus petite valeur a telle $126 \times a$ soit un carré d'entier.
c. En déduire la plus petite valeur b telle $126 \times b$ soit un cube d'entier.

18 **a.** Décomposer 6615 en produit de facteurs premiers.
b. En déduire la plus petite valeur a telle que $6615 \times a$ soit un carré d'entier.
c. En déduire la plus petite valeur b telle que $6615 \times b$ soit un cube d'entier.

19 **a.** Décomposer en produit de facteurs premiers les nombres 1176 et 504 .
b. En déduire un moyen rapide de réduire $\frac{1176}{504}$ en une fraction irréductible.

20 **a.** Décomposer en produit de facteurs premiers les nombres 819 et 195.
b. En déduire un moyen rapide de réduire la somme $\frac{1}{819}+\frac{1}{195}$ en une fraction irréductible.

21 Montrer qu'un entier est un carré si et seulement si les facteurs premiers de sa décomposition ont des exposants pairs.

22 Décomposer en produit de facteurs premiers 260 et 364. En déduire le PGCD et le PPCM de 260 et 364.

Savoir-faire 3, p. 62

23 **a.** Décomposer en produit de facteurs premiers 21 et 3234.
b. En déduire tous les couples $(x\,;y)$ d'entiers naturels tels que PGCD $(x\,;y) = 21$ et PPCM $(x\,;y) = 3234$.

24 Donner la liste des diviseurs des nombres suivants :
a. 45 **b.** 57 **c.** 80

Savoir-faire 4, p. 63

25 Donner la liste des diviseurs des nombres suivants :
a. 36 **b.** 100 **c.** 81

26 Déterminer le nombre de diviseurs des nombres :
a. 174 **b.** 96 **c.** 2000

Savoir-faire 5, p. 63

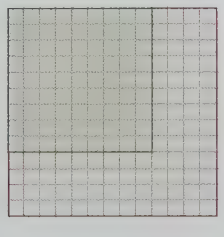
27 **a.** Décomposer 1694 en produit de facteurs premiers.
b. Déterminer le nombre des diviseurs de 1694.
c. Déterminer le nombre des diviseurs de 1694^2 et de 1694^3.

28 Des nombres sont dits **amiables** si chacun d'eux est la somme des diviseurs stricts de l'autre.
1. Vérifier que 220 et 284 sont amiables.
2. Montrer que 1184 possède un ami.
3. Montrer que deux nombres amiables ont même somme de leurs diviseurs.

Les « amis »
Nombres connus dès l'Antiquité par Pythagore qui aurait dit : « Un ami est celui qui est l'autre moi-même comme sont 220 et 284 », il aura fallu attendre 1867 et un jeune italien de 16 ans pour dénicher le second couple amiable de l'exercice.
Aujourd'hui, seuls 7500 ont été trouvés et on ne sait toujours pas si cette liste peut être infinie…

29 **1.** Peut-on construire un pavé droit avec 539 cubes identiques ?
2. Combien de pavés droits de formes différentes peut-on construire avec 84 cubes identiques ?

30 Un carré est pavé de n petits carrés identiques.
a. Peut-on lui ôter 28 petits carrés et former à nouveau un carré ?
b. Quelles peuvent être alors les dimensions de ces carrés ?



31 Montrer qu'un nombre est un carré d'entier si et seulement si il possède un nombre impair de diviseurs.

Exercices d'approfondissement

32 **Premier au milieu**
On souhaite montrer que si deux nombres premiers supérieurs à 3 sont distants de 8, leur moyenne n'est pas un nombre premier.
a. Donner les quatre premiers couples de nombres premiers distants de 8.
b. Déterminer un diviseur commun des moyennes de ces couples.
c. En notant p un nombre premier supérieur à 3, préciser les restes possibles de p dans la division euclidienne par 3.
d. Démontrer la conjoncture de la question **b.** dans le cas général.

33 **Premier dans le désordre**
On dit qu'un nombre premier est permutable si tout nombre obtenu en permutant ses chiffres est aussi premier.
a. 113 est-il permutable ?
b. Montrer que, hormis ceux inférieurs à 10, les nombres permutables ne peuvent être constitués que

des chiffres 1, 3, 7 ou 9.

c. Déterminer tous les nombres à deux chiffres permutables.

34 On dit qu'un nombre p premier est un **nombre de Sophie Germain** si $2p + 1$ est aussi un nombre premier.

a. Déterminer les six plus petits nombres de Sophie Germain.

b. On appelle chaîne de Cunningham de première espèce, une suite de nombres premiers vérifiant la relation $p_{i+1} = 2 \times p_i + 1$.

À l'aide de la question **a.**, déterminer une chaîne de Cunningham de première espèce.

Marie-Sophie Germain (1776-1831) fut une des premières mathématiciennes françaises reconnues. Cette autodidacte fut reconnue pour ses travaux sur le dernier théorème de Fermat que vérifient les nombres qui portent désormais son nom.

35 **La formule d'Euler**

On étudie la fonction f définie sur $\mathbb{N}$ par :

$$f(n) = n^2 + n + C \text{ où } C \text{ est un entier.}$$

On note $\pi(C)$ le nombre de premiers consécutifs obtenus à partir de $n = 0$.

1. Construire à l'aide de la calculatrice une table de valeurs de f pour $C = 5$.

2. Déterminer $\pi(5)$.

3. Montrer que $\pi(C) = 0$ si C n'est pas premier.

4. Montrer que $\pi(C) \leqslant C$.

5. En s'appuyant sur la liste des nombres premiers, déterminer la valeur de $C < 20$ telle que $\pi(C)$ soit maximal.

6. La constante $C \leqslant 1000$, donnant le maximum de nombres premiers consécutifs, fut proposée par Leonhard Euler, il s'agit de $C = 41$. Déterminer $\pi(41)$.

7. Démontrer qu'une fonction polynôme à coefficients entiers ne pourra jamais produire uniquement des nombres premiers.

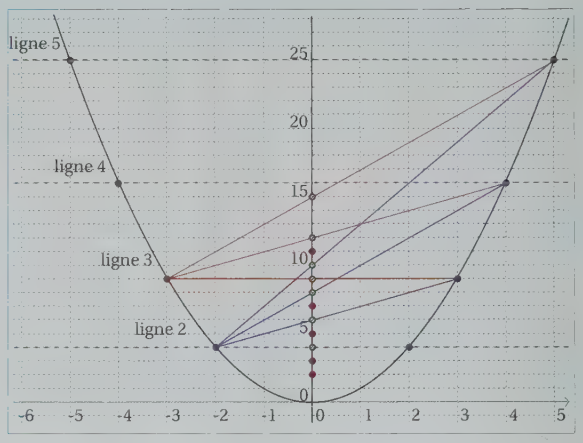
▸ Savoir-faire 6, p. 63

36 **Crible géométrique**

On a représenté ci-après la parabole d'équation $y = x^2$.

Chaque ligne pointillée coupe la courbe en deux points. Son numéro correspond à l'abscisse du point de la courbe. Sur chaque ligne, on relie le point d'intersection avec la courbe, d'abscisse négative, avec tous ceux d'abscisses positives des autres lignes dont le numéro lui est supérieur ou égal.

Les points d'intersection avec les segments dessinés sont marqués en noir, les points restants (sauf celui d'ordonnée 1) sont en rose.



1. Construire et compléter la parabole jusqu'à la ligne 7.

2. Que peut-on penser des ordonnées des points coloriés en rose d'ordonnée inférieure à 20 ?

3. a et b sont deux entiers naturels.

a. Déterminer l'équation de la droite reliant les points $A(-a\,;\,f(-a))$ et $B(b\,;\,f(b))$.

b. Vérifier que la droite (AB) coupe l'axe des abscisses au point de coordonnées $(0\,;\,ab)$.

4. Justifier que les ordonnées de tous les points coloriés en rose sont des nombres premiers.

5. Expliquer pourquoi 22 n'a pas été marqué par le crible.

37 **Irrationalité de $\sqrt{n}$**

Soit n un entier naturel non nul. On suppose qu'il existe deux entiers naturels a et b tels que $\sqrt{n} = \dfrac{a}{b}$.

a. Montrer que b^2 divise a^2.

b. À l'aide de leur décomposition en produit de facteurs premiers, montrer que $\dfrac{a^2}{b^2}$ est un carré d'entier.

c. En déduire une condition nécessaire pour que $\sqrt{n}$ soit rationnel.

d. Par un procédé analogue, énoncer un résultat sur l'irrationalité de $\sqrt[k]{n}$ où k est un entier naturel supérieur à 2.

38 **Formule magique**

Soit n un entier naturel non nul.

On note N le nombre de diviseurs de n, et P le produit des diviseurs de n.

On veut démontrer que $P = \sqrt{n^N}$.

1. Vérifier cette propriété pour $n = 45$ et pour $n = 36$.

2. Soit m un entier naturel non nul. On suppose que $N = 2m$ est pair.

En associant les diviseurs 2 par 2, montrer que $P = n^m$.

En déduire la propriété voulue.

3. On suppose désormais que $N = 2m + 1$ est impair.

a. Montrer n est un carré d'entier.

b. En associant les diviseurs 2 par 2, montrer que $P = n^m \times \sqrt{n}$.

En déduire la propriété voulue.

Activités de recherche et résolution de problèmes

Travaux pratiques avec l'outil informatique

Problèmes de recherche

39 Tester la primalité d'un entier avec un tableur

Algorithmique

Le tableur possède une fonction MOD, donnant le reste dans une division euclidienne. Dans la fenêtre ci-contre, le nombre 759 est testé et il est divisible au moins par 3, 11 et 23.

	A	B	C
1			
2		Nombre testé	759
3	Recherche de diviseur inférieur à		27
4			
5	diviseur	reste	
6	2	1	
7	3	0	diviseur
8	5	4	
9	7	3	
10	9	3	
11	11	0	diviseur
12	13	5	
13	15	9	
14	17	11	
15	19	18	
16	21	3	
17	23	0	diviseur
18	25	9	
19	27	3	
20	29	5	fin du test
21	31	15	fin du test

1. Sur quelle propriété peut-on s'appuyer pour limiter la recherche de diviseurs à la valeur calculée en C3.

2. Dans la colonne A, pour ne pas tester tous les entiers, on saisit les valeurs 2 et 3, puis on construit la liste des nombres impairs. Justifier ce choix et préciser comment construire cette colonne.

3. La colonne C est complétée à l'aide de fonctions SI imbriquées.
   a. Quelle est la condition permettant d'afficher « fin du test » ?
   b. Quelle est la condition permettant d'afficher « diviseur » ?
   c. Écrire en langage naturel l'instruction permettant de compléter la colonne C.

4. Réaliser cette feuille de calcul.

5. Les nombres de Fermat sont les entiers de la forme $F_n = 2^{2^n} + 1$, où n est un entier naturel.
   a. Avec le tableur, tester la primalité de F_0, F_1, F_2, F_3 et F_4.
   b. Une feuille de calcul de tableur possède en général 65 535 lignes. Peut-on tester la primalité de F_5 ? Expliquer.
   c. Vérifier que F_5 possède un diviseur premier inférieur à 1 000. Trouver un diviseur premier de F_5.

Le mathématicien **Pierre de Fermat** conjectura au XVII^e siècle que ces nombres étaient tous premiers (faute d'un tableur !). En réalité, on sait désormais qu'aucun d'eux ne l'est pour n allant de 5 à 32.
Mais l'incertitude reste pour $n > 32$.

40 Programmer un test de primalité

Algorithmique

```
PROGRAM:PREMIER
:Prompt N
:2→D
:While D<N
:If partDéc(N/D)
=0
:Then
:Disp "N EST DIV
ISIBLE PAR",D
:Stop
:Else
:D+1→D
:End
:End
:Disp "N EST PRE
MIER"
```

1. Mathis a programmé sur sa calculatrice l'algorithme ci-contre.
   a. Expliquer son fonctionnement.
   b. Pour le nombre premier 257, déterminer le nombre de divisions effectuées par cet algorithme.

2. Pour diminuer le nombre de calculs, Émile lui propose de limiter la recherche aux diviseurs inférieurs à $\sqrt{N}$, en remplaçant le test de boucle par « While D < $\sqrt{N}$ ».

a. Pour $N = 49$, l'algorithme retourne que N est premier. Expliquer et corriger cette erreur.
b. Pour le nombre premier 257, déterminer le nombre de divisions effectuées par cet algorithme.

3. On souhaite améliorer l'algorithme en testant d'abord si le nombre N est divisible par 2, puis en ne testant que les nombres impairs.
a. Programmer l'algorithme en réalisant ces modifications.
b. Pour le nombre premier 257, déterminer le nombre de divisions effectuées par cet algorithme.

41 Décomposition d'un entier en produit de facteurs premiers

Algorithmique

1. Exécuter pas à pas le programme ci-contre pour $N = 18$.

2. **a.** Expliquer son fonctionnement.
b. Les facteurs obtenus sont-ils nécessairement premiers ? Justifier.
c. Que retourne l'algorithme si N est premier ?

3. On souhaite diminuer le nombre de calculs effectués.
a. Modifier l'algorithme afin d'identifier les facteurs 2 dans une première boucle, avant de tester les diviseurs impairs à partir de 3 dans une seconde boucle.
b. Quel gain réalise-t-on pour $N = 18$? pour $N = 59$?
c. Proposer une modification permettant de limiter les diviseurs à tester par la valeur de $\sqrt{N}$.

```
PROGRAM:DECOMPO
:Prompt N
:While N>1
:2→D
:While partDéc(N
/D)≠0
:D+1→D
:End
:Disp D
:N/D→N
:End
```

42 Nombres premiers jumeaux

On appelle **nombres premiers jumeaux**, deux nombres premiers distants de 2 (comme 3 et 5 par exemple).

1. Montrer que tous les couples de nombres premiers jumeaux autres que (3 ; 5) peuvent s'écrire de la forme $(6k - 1 ; 6k + 1)$, avec k un entier naturel non nul.

2. La réciproque est-elle vraie ?

3. Construire la feuille de calcul ci-contre pour k allant de 1 à 50.

4. Les cellules coloriées correspondent aux couples dont l'un des termes est divisible par 5 (et non premier).
a. Conjecturer une périodicité suivant les valeurs de k pour ces couples.
b. À l'aide de congruences, démontrer ce résultat.

5. Démontrer un résultat analogue en étudiant les congruences de ces nombres modulo 7. Colorier alors les couples dont l'un des termes est divisible par 7.

6. Montrer que parmi les nombres restant non coloriés :
• les nombres inférieurs à 120 sont nécessairement premiers ;
• les nombres composés supérieurs à 120 sont divisibles par 11 ou 13.
En déduire les couples qui doivent être encore éliminés.

7. Déterminer la liste des 19 couples de jumeaux inférieurs à 300.

	A	B	C
1	k	6k-1	6k+1
2	1	5	7
3	2	11	13
4	3	17	19
5	4	23	25
6	5	29	31
7	6	35	37
8	7	41	43
9	8	47	49
10	9	53	55
11	10	59	61
12	11	65	67
13	12	71	73
14	13	77	79
15	14	83	85
16	15	89	91
17	16	95	97
18	17	101	103
19	18	107	109
20	19	113	115
21	20	119	121
22	21	125	127
23	22	131	133

De nombreuses interrogations subsistent quant à l'infinitude et la répartition des nombres jumeaux. Le problème **43** donne quelques éléments de réponse.

43 Lister les nombres premiers ▸ Algorithmique

Partie 1. Interprétation

On souhaite faire la liste des nombres premiers inférieurs à un entier naturel N donné.
On sait qu'un entier naturel d est premier s'il n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{d}$.
Dans un programme permettant de tester la primalité d'un entier, on teste usuellement tous les nombres impairs. Mais dès lors que l'on connait la liste des nombres premiers inférieurs à d, il suffit de tester les diviseurs premiers qui sont inférieurs à $\sqrt{d}$.
Le programme réalisé ci-dessous en Python a été exécuté pour $N = 20$ (première fenêtre).

```
>>> liste_premiers(20)
2
3
5
7
11
13
17
19
il y a 8 nombres premiers inferieurs a 20
```

File Edit Format Run Options Windows Help

```
def liste_premiers(N):
    premiers = [2,3]
    d=3
    rang=1
    while d<(N-1):
        d=d+2
        i=1
        while (d%premiers[i]!=0 and (premiers[i]*premiers[i]<=d)):
            i=i+1
        if d%premiers[i]!=0:
            rang=rang+1
            premiers +=[d]
    for i in range(rang+1):
        print(premiers[i])
    print 'il y a',rang+1, 'nombres premiers inferieurs a',N
```

1. La variable **premiers** est une liste de nombres. Le terme de rang i de cette liste est **premiers[i]**, son premier terme est **premiers[0]** qui vaut 2. La variable **rang** contient le rang du dernier terme de la liste.
Expliquer l'action des trois dernières lignes du programme en justifiant le rôle de **rang + 1**.
2. Expliquer le rôle des variables N, d et i.
3. Justifier la condition d < (N – 1) sur la première boucle **while**.
4. la commande % donne le reste de la division euclidienne. L'instruction != signifie ≠.
Expliquer les conditions de la seconde boucle **while**.
5. Quel rôle peut avoir alors l'instruction **premiers += [d]** ?
6. Réaliser cet algorithme et afficher les nombres premiers inférieurs à 100 000, puis déterminer leur proportion exacte parmi les entiers inférieurs à 100 000.

Partie 2. Conception

On souhaite désormais afficher et dénombrer la liste des couples de nombres premiers jumeaux inférieurs à un entier naturel N donné, comme dans la fenêtre ci-contre.
Pour cela, une fois la liste des nombres premiers inférieurs à N établie, on effectue un test conditionnel entre un nombre de la liste et son suivant, et on n'affiche ces nombres que s'ils sont jumeaux.

```
>>> liste_premiers_jumeaux(20)
3 et 5 jumeaux
5 et 7 jumeaux
11 et 13 jumeaux
17 et 19 jumeaux
il y a 4 paires de nombres premiers
jumeaux inferieurs a 20
```

1. Réaliser ce programme à partir de celui réalisé dans la **partie 1.**
2. Déterminer le plus grand couple de nombres premiers jumeaux inférieurs à 10 000.

3. Déterminer la proportion de couples de nombres jumeaux inférieurs à 1 000, puis inférieurs à 10 000, puis à 100 000.

4. Que peut-on en conclure sur ces proportions ?

Partie 3. Encore plus fort

On cherche désormais, dans la liste des entiers inférieurs à N donné, à déterminer l'intervalle le plus long ne contenant aucun nombre premier.

1. Réaliser ce programme dont une fenêtre exécutée est proposée ci-contre.

```
>>> trou_liste_premiers(100)
il y a  7 nombres entiers consecutifs non
premiers entre 89 et 97
```

2. Déterminer le « trou » le plus grand inférieur à 1 000 puis inférieur à 10 000.

44 La répartition des nombres premiers

Euclide démontra dès le IIIe siècle avant J.-C., qu'il existe une infinité de nombres premiers. Pourtant sa répartition reste bien étrange : la liste des entiers peut contenir des «déserts» de nombres premiers, suivi par exemple de deux nombres premiers jumeaux (nombres impairs consécutifs et premiers).
La densité et la répartition des nombres premiers intriguent encore.

Mythe ou réalité ?

Euclide (env. 325-265 av. J.-C.) est un mathématicien grec à qui l'o doit entre autres cette démonstration de l'infinitude de l'ensembl des nombres premiers.
Il regroupe les connaissances mathématiques de son époque dan une encyclopédie en treize volumes : *Les éléments*. Il pose notam ment les bases de l'arithmétique dans les livres VII à IX, où il défini entre autres, la division « euclidienne ».
Son œuvre est si complète que certains doutent encore qu'il n'a jamais vécu et prônent la thèse d'un travail collectif. Aucune versio originelle des *Éléments* ne datant de son époque, nous ne conna trons sans doute jamais la vérité à son sujet.

Partie 1. Infinitude

2, 3, 5, 7, 11, 13, 17, 19, 23, 29... Plus on s'avance dans la liste des nombres premiers, plus ils se raréfient. Il y a, par exemple, 25 % des nombres inférieurs à 100 qui sont premiers, 16,8 % des nombres inférieurs à 1 000 et 9,6 % des nombres inférieurs à 100 000.
Alors pourquoi n'y aurait-il pas à terme épuisement du stock ?

Pour répondre à cette question, on raisonne par l'absurde. On suppose qu'il existe un nombre fini de nombres premiers et l'on construit un nombre premier supplémentaire.
Si l'ensemble des nombres premiers est fini, notons $p_1, p_2, \ldots, p_n$ ses éléments.
On définit le nombre $N = p_1 \times p_2 \times \ldots \times p_n + 1$.

1. Montrer que N ne fait pas partie de la liste $p_1, p_2, \ldots, p_n$.

2. Montrer par l'absurde que N n'est divisible par aucun nombre premier de la liste $p_1, p_2, \ldots, p_n$.

3. En déduire que N est premier et conclure.

Partie 2. Proportion de nombres premiers parmi les entiers

On note $\pi(n)$ la quantité de nombres premiers inférieurs à un entier n donné.

1. À l'aide de la liste des nombres premiers, déterminer $\pi(20)$, $\pi(100)$ et $\pi(200)$.

2. On donne, dans le tableau ci-contre, certaines valeurs de $\pi(n)$, que l'on reproduira en ajoutant trois colonnes à compléter au fur et à mesure.
   a. Compléter la troisième colonne du tableau avec la proportion de nombres premiers inférieurs à n notée en pourcentage.
   b. Peut-on conjecturer les variations et la limite de cette proportion lorsque n tend vers l'infini ?

n	$\pi(n)$
1 000	168
10 000	1 229
100 000	9 592
1 000 000	78 498
10 000 000	664 579
100 000 000	5 761 455

3 On admet que $\pi(n)$ peut être approché par $\pi(n) \approx \frac{n}{\ln(n)-1}$.

a. Compléter une autre colonne avec les valeurs obtenues par cette approximation.

b. Compléter une dernière colonne donnant l'erreur commise par cette approximation exprimée en pourcentage.

c. Calculer $\lim \frac{\pi(n)}{n}$ et interpréter ce résultat.

Partie 3. Des trous dans la liste des nombres premiers

Bien que les nombres premiers se raréfient, il en existe une infinité. Peut-on alors trouver dans $\mathbb{N}$ des listes de longueur quelconque d'entiers consécutifs ne contenant aucun nombre premier ?

Soit n un entier naturel.
On construit le nombre N, produit de tous les nombres premiers inférieurs ou égaux à n.

1 Montrer que pour tout entier k avec $2 \leqslant k \leqslant n$, il existe un nombre premier inférieur à n qui divise k.

2 En déduire qu'aucun nombre de la liste $N+2$, $N+3$, $N+4$, …, $N+n$ n'est premier.

3 Combien de nombres contient cette liste ?

4 En déduire une méthode pour trouver 6 entiers consécutifs non premiers.

5 Donner un ordre de grandeur de N permettant de lister 50 entiers consécutifs non premiers (on pourra utiliser la liste des nombres premiers).

Partie 4. Les nombres de la forme $4k + 3$

Les nombres premiers impairs peuvent se diviser en deux familles : ceux dont le reste dans la division euclidienne par 4 est 3 et ceux dont le reste est 1.
Dans le tableau ci-contre, on a coloré en vert les nombres premiers dans la liste des nombres impairs de la forme $4k + 1$ et $4k + 3$ pour $k \leqslant 16$.
On a vu qu'il existe une infinité de nombres premiers, mais leur répartition suivant ces deux catégories reste à établir.
On suppose qu'il n'existe qu'un nombre fini de nombres premiers de la forme $4k + 3$, que l'on note $p_1, p_2, \ldots, p_n$.
On construit alors le nombre $N = 4p_1 \times p_2 \times \ldots \times p_n - 1$.

k	$4k+1$	$4k+3$
0	1	3
1	5	7
2	9	11
3	13	15
4	17	19
5	21	23
6	25	27
7	29	31
8	33	35
9	37	39
10	41	43
11	45	47
12	49	51
13	53	55
14	57	59
15	61	63
16	65	67

1 Montrer que N est un entier impair supérieur à 2.

2 Montrer par l'absurde que N n'est divisible par aucun nombre premier de la liste $p_1, p_2, \ldots, p_n$.

3 En déduire que tous les diviseurs premiers de N sont de la forme $4k + 1$.

4 En utilisant la décomposition en produit de facteurs premiers de N, déduire de la question 3 que N est de la forme $4k + 1$.

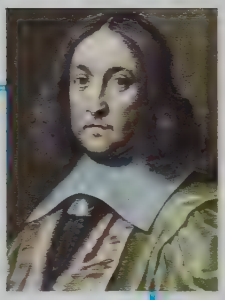
5 Montrer à l'aide de sa définition que N est de la forme $4k + 3$.

6 En déduire une contradiction et conclure.

Forme des nombres premiers

On ne peut démontrer par un raisonnement analogue qu'il existe une infinité de nombres premiers de la forme $4k + 1$ car le produit de deux nombres de la forme $4k + 3$ est de la forme $4k+1$, donc on ne peut connaitre la forme de N à partir de ses diviseurs premiers.
Pourtant il y a bien aussi une infinité de nombres de la forme $4k + 1$. La densité d'apparition de ces deux formes est assez proche bien que les nombres de la forme $4k + 3$ soient légèrement plus nombreux.
Pour les nombres inférieurs à 10^9, les nombres premiers de la forme $4k + 1$ représentent 2,542 349 1 % et ceux de la forme $4k + 3$ représentent 2,542 404 2 % des nombres premiers, soit 551 nombres de plus pour la seconde catégorie. Cet écart tend encore à diminuer pour les nombres plus grands.
Pour plus d'informations :
http://math.univ-lyon1.fr/~deleglis/Calculs/pik.html

45 Petit théorème de Fermat



Pierre de Fermat : ses démonstrations

Mathématicien français (env. 1605-1665) dont les travaux en arithmétique furent riches et controversés. Peu enclin à démontrer ses résultats, il déclenchait souvent les foudres de ses pairs.
Il écrivit un jour à Mersenne (voir p. 75) :
« *J'ai si peu de commodité d'écrire mes démonstrations, que je me contente d'avoir découvert la vérité et de savoir le moyen de la prouver, lorsque j'aurai le loisir de le faire.* »
Ce qui explique que certaines conjectures de Fermat se sont avérées fausses.

De conjectures...

Son théorème le plus célèbre, appelé depuis « **grand théorème** de Fermat », ne fut démontré qu'en 1994 par l'Anglais Andrew Wiles. Il resta donc plus de 300 ans à l'état de conjecture. Fermat avait à ce sujet seulement annoté la marge d'un livre des mots suivants : « *J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir.* ». La démonstration d'Andrew Wiles occupe plusieurs centaines de pages.

...en théorème

Il démontra un autre théorème très important pour l'arithmétique, qui porte depuis, assez injustement peut-être, le nom de « **petit théorème** de Fermat », en comparaison du grand théorème cité. Cette propriété fournit de très nombreux résultats sur la recherche des diviseurs de très grands nombres. Ses applications modernes mènent, par exemple, au cryptage RSA qui sera traité dans le problème 47.

Partie 1. Une approche numérique du théorème

On étudie les nombre de la forme $a^n - a$, a et n étant des entiers naturels non nuls.

1 Quelques conjectures

a. À l'aide de la calculatrice, construire une table de ces nombres pour a variant de 1 à 10 et $n = 3$, puis vérifier que tous ces nombres sont divisibles par 3 (on pourra modifier la table pour faire apparaître cette divisibilité).

b. En reprenant la question **a.** pour n variant de 2 à 10, conjecturer pour quelles valeurs de n les nombres $a^n - a$ sont divisibles par n.

2 On suppose désormais que $a^n - a$ est divisible par n pour tout entier a.

a. Montrer que si a et n sont premiers entre eux alors $a^{n-1} - 1$ est divisible par n.

b. En déduire que si n est un nombre premier, alors $a^{n-1} - 1$ est divisible par n si a n'est pas un multiple de n.

c. Réciproquement, montrer que si a est un multiple de n, alors $a^{n-1} - 1$ n'est pas divisible par n.

d. Donner un exemple numérique illustrant les trois questions précédentes.

Partie 2. Le petit théorème de Fermat

THÉORÈME

Si p est un entier naturel premier et a est un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p.

COROLLAIRE

Si p est un entier naturel premier et a est un entier naturel quelconque, alors $a^p - a$ est divisible par p.

L'objectif de cette partie est de démontrer le théorème et son corollaire.
On note A l'ensemble des $(p-1)$ premiers multiples positifs de a non nuls :

$$A = \{a, 2a, 3a, \ldots, (p-1) \times a\} = \{k \times a, \text{ pour } 1 \leqslant k \leqslant p-1\}$$

1 À l'aide du théorème de Gauss, montrer que p ne divise aucun élément de A.

2 On s'intéresse aux restes des éléments de A dans la division euclidienne par p.

a. Montrer que ces restes sont tous non nuls.

b. Montrer que si deux éléments de A ont le même reste, alors ces éléments sont égaux.

c. En déduire que la liste non ordonnée de ces restes décrit l'ensemble $\{1, 2, 3, \ldots, p-1\}$.

3 On note P le produit de tous les éléments de A : $P = a \times 2a \times 3a \times \ldots \times (p-1)a$.

a. Montrer que $P \equiv 1 \times 2 \times 3 \times \ldots \times (p-1)$ $[p]$ à l'ordre près des facteurs.

b. Montrer que $P = 1 \times 2 \times 3 \times \ldots \times (p-1) \times a^{p-1}$.

c. En déduire que $[1 \times 2 \times 3 \times \ldots \times (p-1)] \times (a^{p-1} - 1) \equiv 0$ $[p]$.

d. À l'aide du théorème de Gauss, montrer que p divise $a^{p-1} - 1$.

4 À partir du **petit théorème** de Fermat, démontrer le corollaire.

Partie 3. Quelques applications numériques

1 Déterminer un diviseur premier des nombres suivants :

a. $2^{10} - 1$ **b.** $4^{16} - 4$ **c.** $4^{14} - 4$

2 Déterminer un diviseur premier de $6^6 - 1$. En déduire que $6^6 + 6$ est divisible par 42.

3 En écrivant 999 999 sous la forme $10^n - 1$, déterminer un diviseur premier de 999 999 autre que 3.

4 Pour tout entier n, on considère le nombre $a = n^5 - n$.

a. À l'aide des congruences, montrer que a est divisible par 2 et par 3.

b. Montrer que a est divisible par 5.

c. En déduire que a est divisible par 30.

5 Pour tout entier n, on considère le nombre $a = n^{13} - n$.

a. À l'aide des congruences, montrer que a est divisible par 2 et par 3.

b. À l'aide d'une factorisation, montrer que a est divisible par 13 et 7.

c. En déduire que a est divisible par 546.

6 On cherche les nombres premiers p qui divisent $2^p + 5$.

a. Justifier que p divise $2^p - 2$.

b. En déduire les valeurs de p qui divisent $2^p + 5$.

7 p est un nombre premier, a et b sont deux entiers relatifs.

a. À l'aide du corollaire du petit théorème de Fermat, montrer que si p divise $a + b$, alors p divise $a^p + b^p$.

b. En déduire un diviseur de $5^{11} + 6^{11}$ et vérifier ce résultat.

c. Déduire de la question **a.** une valeur de p telle que $5^p + 7^p$ soit divisible par p.

d. Déterminer, par une démarche analogue, une valeur de p telle que $11^p - 4^p$ soit divisible par p.

Partie 4. Les menteurs de Fermat

Un **nombre de Carmichaël** est un nombre n non premier tel que $a^n - a$ soit divisible par n pour tout entier naturel a.

1 Ces nombres sont aussi appelés «les menteurs de Fermat» en référence au petit théorème de Fermat. Expliquer cette appellation.

Pour la suite de cette partie, on suppose que n est un nombre de Carmichaël et p est un entier premier qui divise n.

Alwin Korselt (1864-1947)

Mathématicien allemand, il s'intéressa à ces nombres sans en avoir jamais trouvés. En 1899, il démontre le théorème cité page 74, mais l'Américain Robert Carmichaël trouva le plus petit d'entre eux (561) en 1910.

Ces nombres rares sont pourtant plus de 100 000 entre 1 et 10^{15}, et il en existe une infinité. Ils font partie de la famille des nombres pseudo-premiers, dont les exploitations sont aujourd'hui très importantes en cryptographie.

2 On suppose que p^2 divise n.

a. Montrer que p^n est divisible par p^2.

b. Montrer que $p^n - p$ est divisible par p^2.

c. En déduire une contradiction et conclure.

3 On admet le théorème suivant dû à Korselt :

« Tout entier naturel n est un nombre de Carmichaël si et seulement si aucun carré de nombre premier ne divise n et, pour chaque diviseur premier p de n, le nombre $p - 1$ divise $n - 1$. »

a. Montrer qu'un nombre de Carmichaël est impair.

b. Montrer que si p est un diviseur de n, alors $p \equiv n\ [p-1]$.

c. En déduire que si n est le produit de deux nombres premiers p et q distincts, alors $q - 1$ est divisible par $p - 1$.

d. Montrer de même que $p - 1$ est divisible par $q - 1$.

e. Conclure en montrant qu'un nombre de Carmichaël est produit d'au-moins trois nombres premiers impairs différents.

f. Vérifier que 561 et 1105 sont des nombres de Carmichaël.

46 Quête des nombres premiers

De tout temps...

Depuis l'Antiquité, avec Euclide ou Ératosthène, la quête des nombres premiers n'a jamais cessé. De nombreux mathématiciens ont essayé de trouver des formules générant des nombres premiers.

Le XVII^e siècle fut le théâtre d'une grande effervescence sur ce sujet. Une riche correspondance en témoigne entre Pierre de Fermat (1605-1665), Marin Mersenne (1588-1648), Blaise Pascal (1623-1662) ou encore René Descartes (1596-1650).

Aujourd'hui encore, cette quête n'a pas abouti.

Pourtant les nombres premiers sont au cœur des techniques de chiffrement actuelles comme le cryptage RSA (voir Activité de recherche 47, p. 77). La recherche d'un nombre premier non encore connu est une clé essentielle à la sécurité de ces cryptages.

Partie 1. Les nombres de Fermat

Les nombres de Fermat sont de la forme $F_n = 2^{2^n} + 1$ pour n un entier naturel.

Le mathématicien Pierre de Fermat conjectura au XVII^e siècle que ces nombres étaient tous premiers.

1 **Secrets d'une conjecture**

La liste ci-dessous est celle des nombres de la forme $2^m + 1$ avec m un entier non nul.

m	1	2	3	4	5	6	7	8	9	10
$2^m + 1$	3	5	9	17	33	65	129	257	513	1025

a. Parmi les nombres $2^m + 1$, pour $m \leqslant 10$, lesquels sont premiers ?

b. Expliquer la conjecture de Fermat.

2 **Une implication**

m est un entier strictement supérieur à 1.

a. Exprimer en fonction de x et m la somme $1 - x + x^2 - x^3 + \ldots + (-x)^{m-1}$.

b. Montrer que s'il existe un entier n tel que $m = 2n + 1$, alors $x^m + 1$ est divisible par $x + 1$.

c. En déduire que si m n'est pas une puissance de 2, alors $2^m + 1$ n'est pas premier (m peut s'écrire sous la forme $2^k \times q$ avec q un nombre impair strictement supérieur à 1).

d. Application : Déduire de la question **2 c.** un diviseur de $2^{20} + 1$.

3 **Une réciproque ?**

a. Énoncer la contraposée de la propriété démontrée à la question **2** **c.**.

b. Énoncer la réciproque de la propriété énoncée à la question **3** **a.**.

c. Vérifier que F_5 est divisible par 641.

d. Que peut-on penser de la propriété énoncée à la question **3** **b.** ?

Évidemment la propriété espérée par Pierre de Fermat est celle énoncée à la question **3** **b.**
« Si m est une puissance de 2, alors $2^m + 1$ est premier ». Cette propriété permettrait de générer une infinité de nombres premiers à l'aide de cette formule.
Malheureusement, il ne put démontrer cette propriété ; en effet, F_5 est un contre-exemple qui lui aurait évité bien des recherches.
En 1640, Pierre de Fermat reconnaît ses difficultés dans une lettre adressée à Bernard Frénicle de Bessy : « *je n'ai pu encore démontrer nécessairement la vérité de cette proposition* ».
Toutefois, la propriété « Si m n'est pas une puissance de 2, alors $2^m + 1$ n'est pas premier » lui a permis d'imaginer ces nombres de la forme $2^{2^n} + 1$, ce qui n'est déjà pas si mal…
Les quatre siècles de recherche qui ont suivi, ont révélé qu'aucun d'eux ne l'est pour n allant de 5 à 32. Mais l'incertitude reste pour n supérieur à 32…

Partie 2. Les nombres de Mersenne

Les nombres de Mersenne sont de la forme $M_p = 2^p - 1$, avec p un nombre premier.
Ces nombres étudiés dès l'Antiquité, ont pris le nom de Mersenne quand ce dernier fournit une liste de ceux d'entre eux qui sont premiers jusqu'à $p = 257$. Bien que cette liste fût fausse, Mersenne savait que tous les nombres M_p n'étaient pas premiers.

Marin Mersenne (1588-1648)

Religieux français, il est aussi mathématicien et philosophe ; il correspondait avec Fermat et Descartes ou encore Blaise Pascal.
Son apport aux sciences physiques fut également important, notamment par son travail sur les ondes et la propagation du son.
Par ailleurs, il dessina le premier les plans d'un sous-marin (prénom prédestiné ?).

A. Une condition nécessaire

1 Vérifier que M_2, M_3, M_5 et M_7 sont premiers.

2 On étudie les nombres $M_n = 2^n - 1$, avec n un entier naturel non premier.

a. On suppose que d est un diviseur de n supérieur à 1.
Soit x un entier supérieur à 1.

b. Exprimer en fonction de x et de n la somme $1 + x + x^2 + x^3 + \ldots + x^{n-1}$.

c. En déduire que $x^n - 1$ est divisible par $x - 1$.

d. Montrer que M_n est divisible par $2^d - 1$.

3 En déduire une condition nécessaire pour que M_n soit premier.

4 Cette condition est-elle suffisante ? (On pourra étudier le cas de M_{11}.)

B. Un théorème de Fermat pour limiter les calculs

Pour trouver les nombres premiers de Mersenne, on démontre le théorème suivant.

Théorème (petit théorème de Fermat)

Un diviseur premier positif d'un nombre de Mersenne (avec p premier supérieur à 2) est toujours de la forme $2\alpha p + 1$ avec α un entier naturel.

1 Montrer que p est impair.

2 Soit q un nombre premier impair. On étudie l'ensemble E des entiers naturels non nuls k vérifiant $2^k \equiv 1 \ [q]$.

a. À l'aide du petit théorème de Fermat (voir Activité de recherche 45, p. 72) montrer que E n'est pas vide.

b. En déduire que E possède un plus petit élément noté m.

c. Soit n un entier naturel. En effectuant la division euclidienne de n par m, montrer que si $2^n \equiv 1 \ [q]$ alors m divise n.

3 On suppose que q est un diviseur premier de $M_p = 2^p - 1$, avec p un nombre premier impair.

a. Montrer que q est impair.

b. Montrer que $2^p \equiv 1 \ [q]$.

c. À l'aide de la question **2 c.**, montrer que m divise p. En déduire que $m = p$.

4 Montrer que p divise $q - 1$. En déduire que $2p$ divise $q - 1$.

5 Démontrer le théorème.

C. Applications aux nombres de Mersenne premiers

1 Montrer que pour étudier la primalité de M_{13}, à l'aide entre autre du théorème précédent, il suffit de tester si ce nombre est divisible par 53 et 79.
Conclure quant à la primalité de M_{13}.

2 Étudier de même la primalité de M_{11}.

GIMPS : vous pouvez y participer !

Fondé en 1996 par l'Américain George Woltman, le *Great Internet Mersenne Prime Search* (GIMPS) est un projet de calcul partagé où les volontaires installent sur leur propre ordinateur un logiciel client pour traiter une partie des calculs permettant de chercher les nombres premiers de Mersenne.
Le Norvégien Odd Magnar Strindmo a ainsi mis à disposition, pendant 29 jours, son processeur Intel Core2.
C'est ainsi que le 46e nombre premier de Mersenne a été trouvé en avril 2009. Il s'agit de $2^{42\,643\,801} - 1$, le deuxième plus grand nombre premier connu.
En effet, le 47e nombre premier de Mersenne a été identifié un an plus tôt : $2^{43\,112\,609} - 1$. Ceci est la preuve que certains nombres de Mersenne ont peut-être été oubliés et que ce classement peut encore bouger.
Le GIMPS a trouvé 13 nombres premiers de Mersenne en 13 ans. Pour connaître l'état actuel des travaux, on peut se rendre sur le site officiel http://www.mersenne.org/ et pourquoi pas, participer !

Partie 3. Les nombres parfaits

Un nombre entier est dit **parfait** s'il est la somme de ses diviseurs stricts (sauf lui-même). Ces nombres ont intrigué dès l'Antiquité et Euclide montra 300 av. J.-C. que chacun des nombres de Mersenne premiers donnait naissance à un nombre parfait.

1 **Quelques nombres parfaits**

a. Déterminer les nombres parfaits inférieurs à 10.

b. Montrer que 28 est un nombre parfait.

c. Donner sa décomposition de 496 en produit de facteurs premiers.

d. En déduire que 496 est parfait.

2 **Un théorème d'Euclide**

On suppose que $M_n = 2^n - 1$ est un nombre premier. On étudie les nombres $P_n = 2^{n-1}(2^n - 1)$.

a. À l'aide de sa décomposition en produit de facteurs premiers, établir la liste des diviseurs de P_n et montrer que P_n est parfait.

b. Donner alors les quatre premiers nombres parfaits que l'on peut générer ainsi.

3 **Une étonnante propriété**

a. On rappelle que $M_3 = 2^3 - 1 = 7$. Vérifier que la somme des entiers de 1 à 7 vaut P_3.

b. Vérifier de même que la somme des entiers de 1 à M_5 vaut P_5.

c. À l'aide des suites arithmétiques, montrer que, pour tout entier n, la somme des entiers de 1 à M_n vaut P_n.

Les nombres parfaits sont-ils tous pairs ?

Euclide montra la propriété de la question **2**, mais au XVIII^e siècle Leonhard Euler prouva que tous les nombres parfaits pairs étaient ceux proposés par Euclide.

La recherche inachevée des nombres premiers de Mersenne conditionne donc la découverte de nouveaux nombres parfaits pairs.

Quant aux nombres parfaits impairs, les recherches actuelles incitent à croire qu'il n'en existe pas.

Si un tel nombre existait, il comporterait au moins 75 facteurs premiers dont 9 facteurs distincts, il serait supérieur à 10^{300}. Mais qui sait…

47 Cryptographie RSA

RSA : Rivest Shamir Adleman

Du nom des trois chercheurs qui ont imaginé en 1977 cet algorithme de cryptage. Ils reçurent en 2002 le *ACM Turing Award*, l'équivalent du prix Nobel en informatique pour cette invention.

En pratique

Le système RSA est très coûteux en calcul mais il garantit une grande sécurité car la clé privée ne voyage pas, et ainsi elle court moins le risque d'être divulguée.

Dans la pratique, pour traiter des données confidentielles comme du texte envoyé *via* internet, le coût de calcul est trop important. On utilise alors un encodage moins coûteux fonctionnant aussi avec une clé. Pour transmettre cette clé, on la crypte avec le système RSA, garantie qu'elle ne sera pas interceptée.

La solidité du cryptage RSA vient de la construction d'un couple de clés : une clé pour celui qui crypte et l'autre clé pour celui qui décrypte.

Ces clés sont construites à partir d'un entier n , produit de deux nombres premiers p et q.

Mais pour « casser » le cryptage, il faut connaître p et q.

Tout le secret repose donc dans l'utilisation de très grands nombres premiers p et q permettant de construire $n = p \times q$, tels que le temps de calcul nécessaire pour les identifier demanderait de nombreuses années aux plus gros calculateurs informatiques actuels.

Ce nombre n doit donc augmenter au fur et mesure des progrès des calculateurs pour garder une avance confortable.

Pour se donner une idée des calculs, les clés actuellement utilisées sont supérieures à 10^{300}.

Partie 1. Les propriétés nécessaires

On s'appuiera dans cette partie entre autre sur le petit théorème de Fermat, démontré dans l'**Activité de recherche 45**, p. 72.

On définit $n = p \times q$, produit de deux entiers distincts.

On pose $m = (p-1)(q-1)$ et on choisit un nombre entier a premier avec m.

1 Montrer qu'il existe deux entiers b et c tels que $ab - mc = 1$ et justifier que l'on peut choisir b positif.

2 On note x un entier naturel quelconque.

a. À l'aide du petit théorème de Fermat, montrer que si x est non divisible par p, on a $x^{p-1} \equiv 1 \ [p]$.

En déduire que $x^{mc} \equiv 1 \ [p]$, puis que $x^{ab} \equiv x \ [p]$.

b. Montrer que si x est divisible par p, on a $x^{ab} \equiv x \ [p]$. En déduire le résultat quel que soit l'entier x.

3 Pour tout entier x, démontrer de même que $x^{ab} \equiv x \ [q]$.

4 En déduire que pour tout entier x, on a $x^{ab} \equiv x \ [n]$.

Partie 2. Le principe de fonctionnement

Soit n un entier naturel produit de deux nombres premiers p et q.
Sa connaissance permet de trouver les entiers m, a et b de la **Partie 1.**.
Les messages à crypter sont des entiers x compris entre 0 et $n-1$.

Cryptage

x est crypté par $C(x) \equiv x^a \ [n]$.
Les données n et a sont nécessaires pour crypter et le couple $(n\ ;\ a)$ est la **clé publique**, connue de tous.

Décryptage

y est décrypté par $D(y) \equiv y^b \ [n]$.
Les données n et b sont nécessaires pour décrypter et b est la **clé privée**, connue seulement de la personne qui reçoit le message.

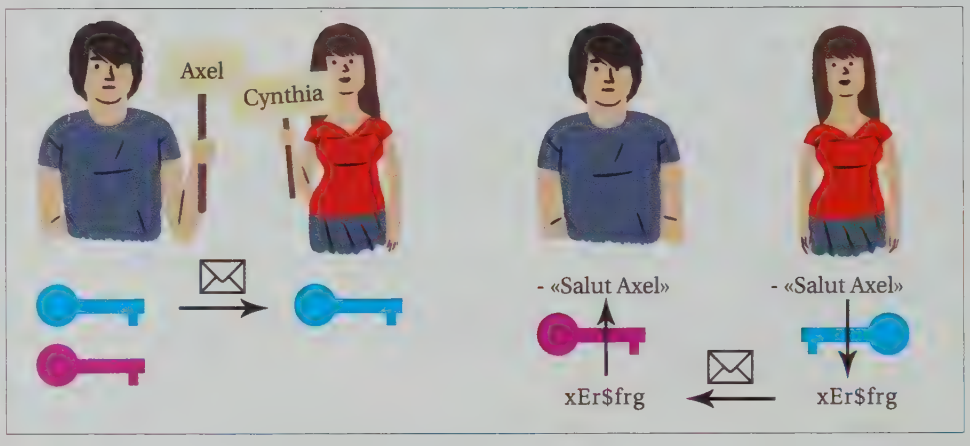
On peut vérifier que $D(C(x)) \equiv (x^a)^b \equiv x^{ab} \equiv x \ [n]$; on retrouve donc la valeur x après cryptage, puis décryptage.
Dans la pratique, c'est celui qui doit déchiffrer qui fabrique le couple de clés (**publique** et **privée**), il envoie alors la **clé publique** à tous ceux qui souhaitent crypter un message, il reçoit les messages et peut les décrypter. Ainsi la **clé privée** ne voyage pas, cela garantit sa non divulgation.

Étape 1

Axel crée ses clés et envoie la **clé publique** à Cynthia

Étape 2

Cynthia crypte et envoie son message qu'Axel décrypte avec sa **clé privée**



1 Axel souhaite recevoir en message crypté l'âge de Cynthia.
Il choisit $p = 3$ et $q = 11$.

a. Calculer n et m, puis déterminer le plus petit entier qu'il peut choisir pour a.

b. Déterminer alors le plus petit entier qu'il peut choisir pour b.

c. Axel envoie sa clé publique (33 ; 3) à Cynthia. Cette dernière crypte son âge et lui envoie le nombre 29. Retrouver l'âge de Cynthia.

2 En retour, Cynthia souhaite qu'Axel lui envoie en message crypté son numéro de téléphone. Les numéros sont cryptés deux par deux.

a. Justifier que n doit être supérieur ou égal à 100.

b. Montrer que la clé publique la plus petite possible que Cynthia peut envoyer est alors (106 ; 3).

c. Crypter alors avec cette clé le numéro de téléphone d'Axel : 06 13 87 11 45.

OBJECTIF BAC

Sujets type BAC

Exercice résolu

Exercice 48

On note $p\ \ p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, la décomposition en facteurs premiers de l'entier naturel n.

1. Exprimer en fonction des entiers α_i pour $1 \leqslant i \leqslant r$, le nombre de diviseurs de n.

2. À l'aide de la question **1.**, déterminer le plus petit entier ayant exactement 6 diviseurs positifs.

3. Déterminer de même le plus petit entier ayant exactement 12 diviseurs positifs.

4. Soit N un nombre ayant un nombre premier de diviseurs positifs.

a. Montrer que N admet un unique diviseur premier.

b. En déduire le plus petit entier ayant exactement 17 diviseurs positifs.

Voir résolution page suivante.

Exercice 49

ROC : *Restitution Organisée de Connaissances*

Soit p un nombre premier.

Montrer que si p divise ab alors p divise a ou b.

Exercice 50

1. Donner la décomposition en produit facteurs premiers de 2012.

2. Combien 2012 a-t-il de diviseurs positifs ?

3. Combien 2012^{2012} a-t-il de diviseurs positifs ?

4. Déterminer les diviseurs positifs de 2012^{2012} compris entre 500 et 1000 ?

Exercice 51

Les **repunits** sont des nombres de la forme $u_n = \dfrac{10^n - 1}{9}$ définis pour $n > 0$.

1. Justifier que u_n est un entier pour tout $n > 0$.

2. Calculer les quatre premiers termes de (u_n) et préciser le nombre de chiffres de u_n ?

3. Montrer que u_3 et u_4 ne sont pas premiers.

4. Montrer que si n est pair, u_n est divisible par 11.

5. Montrer que si n est divisible par 3, u_n est un divisible par 111. En déduire leur plus petit diviseur premier.

Pour les exercices **52** à **54**, on s'appuiera sur le petit théorème de Fermat, démontré dans le problème **45**, p. 72, dont l'énoncé est le suivant :
Si p est un entier naturel premier et a est un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p.

Exercice 52

1. k est un entier naturel et x est un entier supérieur à 1.

a. Exprimer en fonction de x et k la somme :

$$1 + x + x^2 + x^3 + \ldots + x^{k-1}.$$

b. En déduire que $x^k - 1$ est divisible par $x - 1$.

2. Soit n un entier naturel non nul.

On suppose que d est un diviseur de n supérieur à 1.

a. Montrer que pour tout entier a , $a^n - 1$ est divisible par $a^d - 1$.

b. En déduire quatre diviseurs de $3^{2016} - 1$ inférieurs à 3000.

c. À l'aide du petit théorème de Fermat, donner un autre diviseur de $3^{2016} - 1$.

Exercice 53 *D'après Bac Amérique du nord, 2011*

On considère la suite (u_n) définie, pour tout entier naturel n non nul, par $u_n = 2^n + 3^n + 6^n - 1$.

1. Calculer les six premiers termes de la suite.

2. Montrer que, pour tout entier naturel n non nul, u_n est pair.

3. Montrer que, pour tout entier naturel n pair non nul, u_n est divisible par 4.

On note (E) l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).

4. Les entiers 2, 3, 4, 5 et 7 appartiennent-ils à l'ensemble (E) ?

5. Soit p un nombre premier strictement supérieur à 3.

a. Montrer à l'aide du petit théorème de Fermat que :

$$6 \times 2^{p-2} \equiv 3 \ [p] \quad \text{et} \quad 6 \times 3^{p-2} \equiv 2 \ [p].$$

b. En déduire que $6 \times u_{p-2} \equiv 0 \ [p]$.

c. Le nombre p appartient-il à l'ensemble (E) ?

Résolution

1. L'exposant de chaque facteur premier p_i de n est un entier β_i avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour $1 \leqslant i \leqslant r$.
Il y a donc $\alpha_i + 1$ valeurs possibles pour β_i, d'où le nombre N de diviseurs de n est :

$$N = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1).$$

2. Si $N = 6$, on peut le décomposer de deux façons : $N = 2 \times 3$ ou $N = 6$.
On identifie alors les facteurs $(\alpha_i + 1)$ sachant que le cas $\alpha_i + 1 = 1$ ne fournit pas de facteur premier (car $\alpha_i = 0$).

- Pour $N = 6 = \alpha_1 + 1$, $\alpha_1 = 5$, d'où, en choisissant le plus petit facteur premier 2, $n = 2^5 = 32$.
- Pour $N = 2 \times 3 = (\alpha_1 + 1)(\alpha_2 + 1)$, $\alpha_1 = 1$ et $\alpha_2 = 2$.

Une fois les exposants α_i identifiés, le plus petit entier n s'obtient en associant le plus grand exposant au plus petit facteur premier, c'est-à-dire ici $n = 2^2 \times 3^1 = 12$.
En conclusion, le plus petit entier ayant exactement 6 diviseurs positifs est 12.

3. Par la même démarche, on a quatre cas envisageables.

- Pour $N = 12 = \alpha_1 + 1$ et $\alpha_1 = 11$, d'où $n = 2^{11} = 2048$.
- Pour $N = 3 \times 4 = (\alpha_1 + 1)(\alpha_2 + 1)$ et $\alpha_1 = 2$ et $\alpha_2 = 3$, d'où $n = 2^3 \times 3^2 = 8 \times 9 = 72$.
- Pour $N = 2 \times 6 = (\alpha_1 + 1)(\alpha_2 + 1)$ et $\alpha_1 = 1$ et $\alpha_2 = 5$, d'où $n = 2^5 \times 3^1 = 32 \times 3 = 96$.
- Pour $N = 2 \times 2 \times 3 = (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1)$ et $\alpha_1 = 1$, $\alpha_2 = 1$ et $\alpha_3 = 2$, d'où $n = 2^2 \times 3^1 \times 5^1 = 4 \times 3 \times 5 = 60$.

En conclusion, le plus petit entier ayant exactement 12 diviseurs positifs est 60.

4. a. N est premier, il n'admet donc pas de décomposition en produit de plusieurs facteurs premiers d'où $N = \alpha_1 + 1$ et n possède un unique facteur premier d'exposant $N - 1$.
b. Pour $N = 17$, on obtient $n = 2^{16}$.

Exercice 54 ▸ Algorithmique *D'après Bac Amérique du sud novembre 2010*

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

L'objet de l'exercice est l'étude des diviseurs de $A(n)$.

1. Les premiers termes

a. Écrire en langage naturel un algorithme permettant de calculer tous les termes $A(n)$ inférieurs à 5 000.

b. Exécuter cet algorithme et étudier la primalité des termes obtenus.

2. Quelques résultats

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

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

c. Montrer que tout entier d diviseur de $A(n)$ est premier avec n.

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

3. Recherche de critères

Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que $n^k \equiv 1\ [d]$.

a. Soit k un tel entier.
En utilisant la division euclidienne de k par s, montrer que s divise k.

b. En déduire que s est un diviseur de 8.

c. Montrer que si de plus d est premier, alors s est un diviseur de $p - 1$.
On pourra utiliser le petit théorème de Fermat.

4. Recherche des diviseurs premiers de $A(n)$ dans le cas où n est un entier pair.
Soit p un diviseur premier de $A(n)$.

a. Montrer que p est impair.

b. En examinant successivement les valeurs possibles pour s, montrer que $s = 8$.

c. En déduire que $p \equiv 1\ [8]$.

5. Application

a. Déterminer les nombres premiers inférieurs à 144 et congrus à 1 modulo 8.

b. Appliquer ce qui précède à la recherche de diviseur premiers de $A(12)$.

BILAN QCM

Se tester sur... L'arithmétique

CORRIGÉS P. 159

Pour chaque question, il y a une ou plusieurs bonnes réponses.

1 Le nombre 64 possède :
A 1 diviseur entier naturel
B 6 diviseurs entiers naturels
C 7 diviseurs entiers naturels
D 14 diviseurs entiers naturels

2 $3^{100} + 6$ est divisible par :
A 3 B 6 C 9 D 100

3 a est un entier vérifiant $a \equiv 2$ [7]
a. $a^3 - 1$ est :
A divisible par 7 B non divisible par 7
C impair D divisible par 3
b. $a^{1\,000} - 1$ est :
A divisible par 7 B non divisible par 7
C congru à 1 modulo 7 D divisible par 1 000

4 Si n est un entier, les reste possibles de n^2 dans la division par 4 sont :
A 1, 2, 3 ou 4 B 0, 1, 2 ou 3
C 0, 1, 4 ou 9 D 0 ou 1

5 Il n'existe pas d'entier n tel que :
A $n^2 \equiv 2$ [3] B $n^2 \equiv 2$ [4]
C $n^2 \equiv 2$ [5] D $n^2 \equiv 2$ [7]

6 L'algorithme d'Euclide donne le PGCD de 92 et 78 en :
A 1 division euclidienne B 2 divisions euclidiennes
C 4 divisions euclidiennes D 5 divisions euclidiennes

7 n est un entier. On donne les nombres $a = 2n + 7$ et $b = 3n + 1$
a. On peut trouver une combinaison linéaire de a et b égale à :
A 1 B 6 C 19 D 38
b. Le PGCD de a et b :
A vaut 1 B vaut 19
C divise 19 D est un multiple de 19

8 Si x et y sont deux entiers tels que $9x = 6y$. On peut affirmer que :
A x divise $6y$ B x divise y
C 9 divise y D 3 divise y

9 Le couple $(-2 ; 1)$ est solution de l'équation $3x + 7y = 1$.
L'ensemble des solutions est constitué des couples de la forme :
A $(-2 + 7k ; 1 + 3k)$ pour tout $k \in \mathbb{Z}$.
B $(-2 + 7k ; 1 - 3k)$ pour tout $k \in \mathbb{Z}$.
C $(-2 - 7k ; 1 + 3k)$ pour tout $k \in \mathbb{Z}$.
D $(-2 + 3k ; 1 - 7k)$ pour tout $k \in \mathbb{Z}$.

10 n est un entier tel que $3n \equiv 3$ [5], alors :
A $n \equiv 1$ [5]
B $n \equiv 0$ [5]
C On ne peut pas connaître le reste n dans la division euclidienne par 5.
D Cette égalité est impossible car 5 n'est pas divisible par 3.

11 Pour déterminer si 131 est un nombre premier :
A Il faut tester les diviseurs premiers inférieurs ou égaux à 65.
B Il faut tester les diviseurs premiers inférieurs ou égaux à 11.
C Il suffit de tester les diviseurs premiers inférieurs ou égaux à 11.
D Il suffit de tester les diviseurs impairs inférieurs ou égaux à 131.

12 Les nombres suivants sont premiers :
A 51 B 71 C 91 D 107

13 Le nombre 1 444 admet exactement :
A 1 diviseur premier
B 2 diviseurs premiers
C 9 diviseurs premiers
D aucun diviseur premier

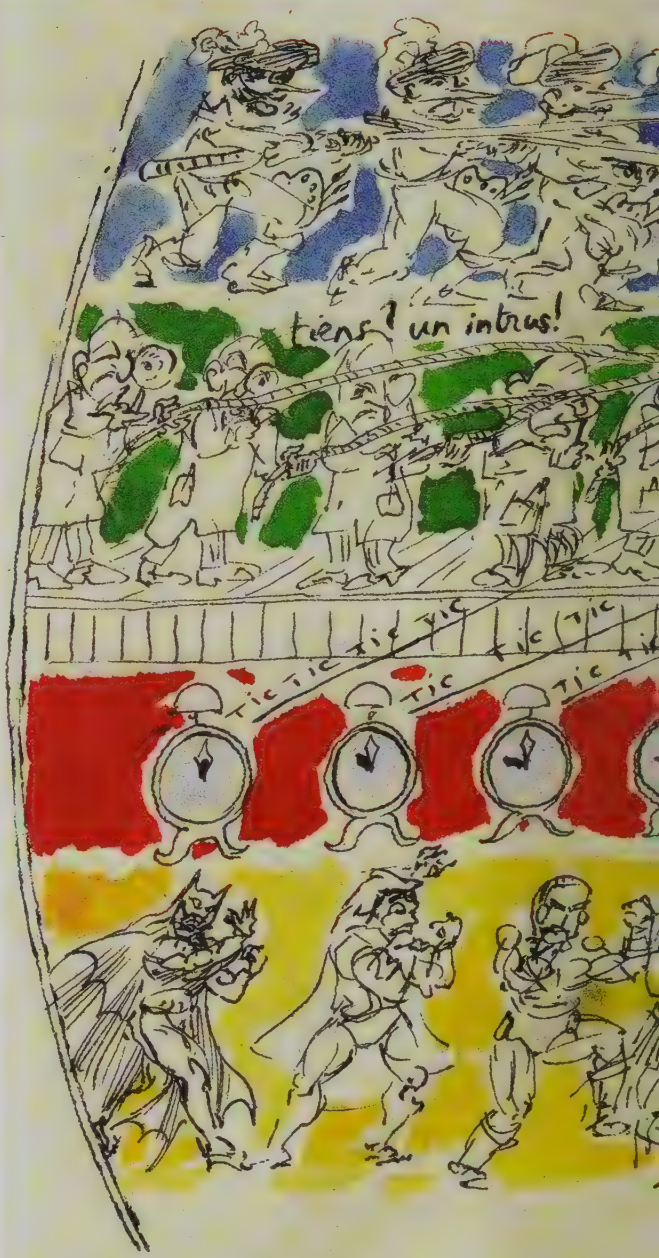
14 Le nombre 360 admet exactement :
A 2 diviseurs
B 3 diviseurs
C 6 diviseurs
D 24 diviseurs

15 p est q sont deux nombres premiers distincts, alors :
A p et q sont premiers entre eux.
B $pq + 1$ est un nombre premier.
C $p + q$ est un nombre pair.
D p^q est un nombre premier.

16 Le nombre $2^{96} - 1$ est :
A divisible par 2
B divisible par 96
C divisible par 97
D un nombre premier

17 Un nombre premier $n > 2$ vérifie nécessairement :
A $n \equiv 1$ [2] B $n \equiv 1$ ou -1 [3]
C $n \equiv 1$ ou -1 [5] D $n \equiv 1$ ou -1 [6]

PARTIE B



$$AX = Y$$

$$\forall i,\ y_i = \sum_{j=1}^{p} a_{ij} x_j$$

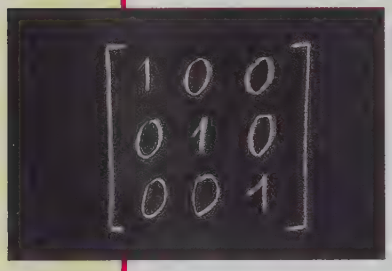
Multiplication d'une matrice par un vecteur, Paul Kichilov.

INTRODUCTION

Liu-Hui, mathématicien chinois

La première notion de matrice

On distingue les prémisses de la notion de matrice dans le plus célèbre des traités mathématiques de la Chine ancienne le *Chiu-chang Suan-shu* ou *l'Art mathématique en neuf sections*, (date incertaine : environ I^er^ siècle après J.-C.) qu'étudia et commenta Liu-Hui au III^e^ siècle.
Cette œuvre a eu une très grande influence sur les mathématiques en Extrême-Orient. Elle fut imprimée pour la première fois au cours du X^e^ siècle. On y trouve un algorithme de résolution des systèmes d'équations, l'algorithme de fang-cheng qui porte le nom d'algorithme de Gauss en Occident.



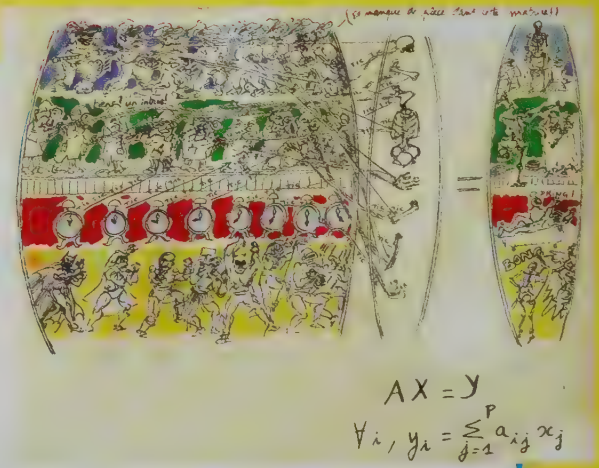
Vers l'algèbre linéaire

Objet utilisé sous diverses formes à travers les siècles, il faut cependant attendre Sir Arthur Cayley (mathématicien britannique ; 1821-1895) pour voir définitivement formalisée la notion de matrice. Cayley est considéré comme l'inventeur des matrices : il définit les opérations sur ces tableaux et pose les premiers pas de l'algèbre linéaire.

Arthur Cayley (1821-1895), mathématicien britannique

Matrices et arts plastiques

« Les peintres prennent un os chacun (premier peintre-1^er^ os, 2^e^ peintre-2^e^ os, ...) pour reconstituer le squelette et organiser une séance de " modèle vivant ".
Les savants font de même mais commettent une erreur en plaçant le crâne et ne savent plus où placer le fémur.
Les aiguilles du réveil tournent en sens inverse : tictac, tictac, tictac... lorsque " dring ! " le réveil sonne, le squelette a eu le temps de se recouvrir de chair et l'homme se réveille, " ressuscite ".
Enfin, les instincts belliqueux des héros des comics américains les ont conduits à provoquer un adversaire terriblement invincible : le squelette reconstitué doué de la force (supposée) des morts. Un seul coup de poing les étend pour le compte. »



PAUL KICHILOV (1966-), *Multiplication d'une matrice par un vecteur*, Tangente HS n° 23 Maths et arts plastiques

Matrices carrées. Évolution de processus

4

Une modélisation par un processus de marche aléatoire des photons du Soleil.

Le chapitre en bref

Réinvestir

- Les probabilités conditionnelles
- Les suites

Explorer

- La notion de matrice
- L'étude de processus d'évolution grâce à l'emploi d'opérations sur des matrices carrées et colonnes

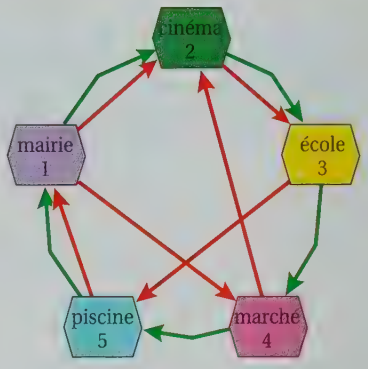
Activités de recherche, p. 101

Activités d'exploration

1 Tous les trajets

Explorer : La description d'une situation par une matrice et l'addition de matrices.

Sur le schéma ci-contre (encore appelé « **graphe** »), on a représenté cinq lieux importants d'une grande ville numérotés de 1 à 5.
On a fléché en rouge les trajets possibles en bus d'un lieu à un autre et en vert les trajets possibles en tram d'un lieu à un autre. (Attention ! les flèches simplement orientées signifient que le trajet n'est possible que dans le sens indiqué.)



1 **a.** On souhaite représenter les possibilités de trajets en bus directs entre deux lieux, dans le tableau B ci-dessous, appelé **matrice**, où chaque colonne correspond à un même lieu de départ et chaque ligne à un même lieu d'arrivée.

$$B = \begin{pmatrix} \dots & 0 & \dots & \dots & \dots \\ 1 & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Le coefficient de la **ligne 2/colonne 1** vaut 1 car il existe un bus qui va du lieu 1 au lieu 2.

Le coefficient de la **ligne 1/colonne 2** vaut 0 car aucun bus ne va directement du lieu 2 au lieu 1.

Compléter cette matrice B des transports en bus.

b. Créer de même la matrice T des transports directs entre deux lieux en tram.

2 Créer la matrice M de tous les transports directs entre deux lieux. Que peut-on dire des trois matrices ?

Notions rencontrées dans l'activité

On appelle **matrice carrée** de taille n, tout tableau de nombres réels à n lignes et n colonnes. Soit A et B deux matrices carrées **de même taille**.
La matrice notée $A + B$ est la matrice dont les coefficients sont obtenus en additionnant deux à deux les coefficients qui ont la même position dans A et B.

2 Sauts aléatoires

Réinvestir : L'outil matrice pour décrire l'évolution d'un processus.
Explorer :
- La multiplication d'une matrice carrée par une matrice colonne.
- La notion de marche aléatoire.

Deux familles de puces sautent simultanément sur deux marches consécutives d'un escalier.
À chaque saut, $1/5^{e}$ des puces situées sur la marche 1 réussit à monter sur la marche 2. En revanche, à chaque saut, $3/10^{e}$ des puces de la marche 2 redescendent sur la marche 1.

1 Écrire la matrice M de transition pour un saut qui donne les fréquences de passage d'une marche à l'autre.(Chaque colonne correspond à une même marche de départ et chaque ligne à une même marche d'arrivée.)

2 On sait qu'au départ il y a seulement 40 puces sur la marche 1 et 1000 sur la marche 2. On note P_0 la matrice constituée d'une colonne et donnant cette répartition par marche :

$P_0 = \begin{pmatrix} 40 \\ 1000 \end{pmatrix}$

a. Calculer le nombre de puces sur chaque marche après 1 saut ; écrire le résultat sous la forme d'une matrice colonne P_1.

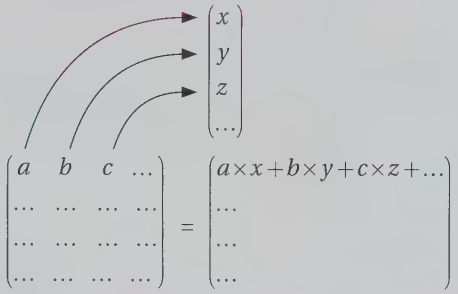
b. Décrire les opérations permettant d'obtenir les coefficients de P_1 à partir de ceux des matrices M et P_0.

c. Déterminer la répartition du nombre de puces après 2 sauts et 3 sauts.

3 Que se passe-t-il si au départ il y a 600 puces sur la marche 1 et 400 sur la marche 2 ?

Notion rencontrée dans l'activité

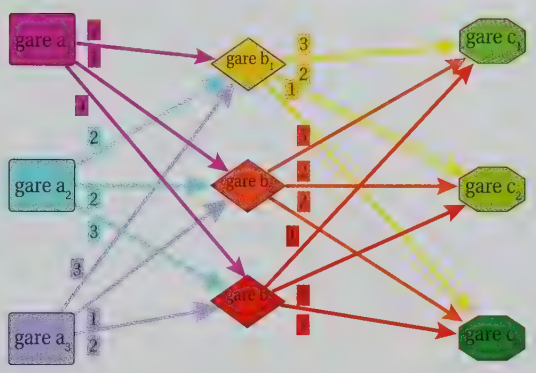
Soit A une matrice carrée de taille n et B une matrice colonne à n lignes. La matrice notée $A \times B$ est la matrice colonne dont les coefficients de chaque ligne sont obtenus comme l'indique le schéma ci-contre pour la première ligne.



3 Correspondances

Réinvestir : L'outil matrice pour décrire des relations.
Explorer : La multiplication de matrices carrées.

Le schéma indique les connexions entres les gares de trois villes A, B et C. Les entiers au-dessus des liens indiquent le nombre de liaisons en train d'une gare de la ville A vers une gare de la ville B ou d'une gare de la ville B vers une gare de la ville C.



NOTE
On aurait aussi pu choisir d'écrire la matrice des liaisons de la ville A (gares en colonnes) vers la ville B (gares en lignes) et de même pour les liaisons de B vers C. Cet autre choix aurait fait apparaître de façon moins naturelle les opérations à faire sur ces matrices.

1 Représenter ces informations sous forme matricielle en utilisant une matrice M pour les liaisons de la ville A (gares en lignes) vers la ville B (gares en colonnes) et une matrice N pour les liaisons de la ville B (gares en lignes) vers la ville C (gares en colonnes).

2 Pour aller de la gare a_1 de la ville A à la gare c_1 de la ville C, on peut passer par les gares b_1, b_2 ou b_3. Combien de liaisons différentes sont-elles possibles ? Faire le lien entre ce calcul et des opérations faites sur les coefficients des matrices M et N précédentes.

3 Établir la matrice des liaisons de la ville A (gares en lignes) vers la ville C (gares en colonnes).

Notion rencontrée dans l'activité

Soit A et B deux **matrices carrées de même taille.** Le produit de la matrice A par la matrice B est la matrice de même taille, notée $A \times B$, dont les colonnes correspondent au produit de la matrice A par chaque colonne de la matrice B.

A. Matrices carrées et matrices colonnes

DÉFINITION

Soit n un entier naturel non nul.

On appelle **matrice carrée de taille** (ou d'ordre) n, tout tableau de nombres réels à n **lignes** et n **colonnes**.

Ces nombres réels sont numérotés a_{ij} avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$ où i correspond au numéro de la ligne et j correspond au numéro de la colonne du réel a_{ij}.

Une telle matrice A s'écrit donc de la manière suivante :

$$A = \overbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & & & & \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}}^{n \text{ colonnes}} \Big\} n \text{ lignes}$$

REMARQUES

- Pour p et q entiers strictement positifs, on définit de même des matrices à p lignes et q colonnes (si $p = q$ ce ne sont donc pas des matrices carrées).
- Les nombres réels du tableau sont appelés coefficients de la matrice.
- De par la définition, deux matrices A et B sont égales si et seulement si elles contiennent les mêmes coefficients situés aux mêmes positions.

EXEMPLE

$M = \begin{pmatrix} 1,2 & 1 & 4 \\ -7 & 0 & 9 \\ 0,5 & 5 & 12 \end{pmatrix}$ est une matrice carrée de taille 3.

Le coefficient m_{23} est le coefficient situé à l'intersection de la 2e ligne et de la 3e colonne : $m_{23} = 9$.

DÉFINITION

Soit n un entier naturel non nul.

On appelle **matrice colonne** ou vecteur colonne, tout tableau de nombres réels à n lignes et 1 colonne.

Une telle matrice A s'écrit : $A = \overbrace{\begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}}^{1 \text{ colonne}} \Big\} n \text{ lignes}$

REMARQUE

Les coordonnées des vecteurs sont représentées sous forme de matrice colonne à deux lignes, pour les vecteurs du plan, et à trois lignes pour les vecteurs de l'espace.

B. Opérations sur les matrices

Somme de deux matrices carrées

Soit A et B deux matrices carrées **de même taille** ou soit A et B deux matrices colonnes.
La **somme** de A et B est la matrice notée $\boldsymbol{A + B}$ dont les coefficients sont obtenus en **additionnant deux à deux** les coefficients qui ont la même position dans A et B.

EXEMPLE

Soit $A = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix}$ et $B = \begin{pmatrix} 5 & 1 \\ 2 & 0,1 \end{pmatrix}$. Alors $A + B = \begin{pmatrix} 0,2+5 & 1+1 \\ 3+2 & 0,7+0,1 \end{pmatrix} = \begin{pmatrix} 5,2 & 2 \\ 5 & 0,8 \end{pmatrix}$.

Produit d'une matrice par un réel

Soit A une matrice et k un nombre réel.
Le **produit** de la matrice $\boldsymbol{A}$ par le **nombre réel** $\boldsymbol{k}$ est la matrice notée $\boldsymbol{kA}$ dont les coefficients sont obtenus **en multipliant tous les coefficients de la matrice A par le nombre k.**

▶ Savoir-faire 1
Utiliser sa calculatrice pour le calcul matriciel, p. 93

EXEMPLE

Soit $A = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix}$ et $k = 1,5$. Alors $1,5A = \begin{pmatrix} 1,5\times0,2 & 1,5\times0,2 \\ 1,5\times3 & 1,5\times0,7 \end{pmatrix} = \begin{pmatrix} 0,3 & 1,5 \\ 4,5 & 1,15 \end{pmatrix}$.

Produit d'une matrice carrée par une matrice colonne

Soit A une matrice **carrée de taille n** et B une matrice **colonne à n lignes.**

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots\ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots\ldots & a_{2n} \\ \ldots\ldots & & & & \\ \ldots\ldots & & & & \\ a_{n1} & a_{n2} & a_{n3} & \ldots\ldots & a_{nn} \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{pmatrix}$$

Le produit de la matrice A par la matrice colonne B est la **matrice colonne à n lignes,** notée $\boldsymbol{A \times B}$, dont le coefficient de la ligne i est le nombre $a_{i1} \times b_1 + a_{i2} \times b_2 + a_{i3} \times b_3 + \ldots + a_{in} \times b_n$.

EXEMPLE

Soit les matrices $A = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix}$ et $B = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$.

$A \times B = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix} \times \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 0,2\times5+1\times2 \\ 3\times5+0,7\times2 \end{pmatrix}$, soit $A \times B = \begin{pmatrix} 3 \\ 16,4 \end{pmatrix}$.

Multiplication de deux matrices carrées

Soit A et B **deux matrices carrées de même taille.**
Le **produit** de la matrice A par la matrice B est la matrice de même taille, notée $A \times B$, dont les colonnes correspondent **au produit de la matrice A par chaque colonne de la matrice B.**

EXEMPLES

Soit les matrices $A = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix}$ et $B = \begin{pmatrix} 5 & 1 \\ 2 & 0,1 \end{pmatrix}$.

$A \times B = \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix} \times \begin{pmatrix} 5 & 1 \\ 2 & 0,1 \end{pmatrix} = \begin{pmatrix} 0,2\times5+1\times2 & 0,2\times1+1\times0,1 \\ 3\times5+0,7\times2 & 3\times1+0,7\times0,1 \end{pmatrix}$, soit $A \times B = \begin{pmatrix} 3 & 0,3 \\ 16,4 & 3,07 \end{pmatrix}$.

$B \times A = \begin{pmatrix} 5 & 1 \\ 2 & 0,1 \end{pmatrix} \times \begin{pmatrix} 0,2 & 1 \\ 3 & 0,7 \end{pmatrix} = \begin{pmatrix} 5\times0,2+1\times3 & 5\times1+1\times0,7 \\ 2\times0,2+0,1\times3 & 2\times1+0,1\times0,7 \end{pmatrix}$, soit $B \times A = \begin{pmatrix} 4 & 5,7 \\ 0,7 & 2,07 \end{pmatrix}$.

REMARQUE IMPORTANTE

La multiplication des matrices **n'est pas commutative** ; en général, $A \times B \neq B \times A$.

C. Calcul matriciel

Propriétés

Soit A , B et C des matrices carrées.

Addition des matrices carrées A et B

- Propriété de commutativité : $A + B = B + A$.
- Propriété d'associativité : $(A + B) + C = A + (B + C) = A + B + C$.

Multiplication d'une matrice carrée A par un nombre réel k

Pour tous réels k et k' et toutes matrices A et B :

- $(k + k')A = kA + k'A$
- $k(A + B) = kA + kB$
- $(kk')A = k(k'A)$
- $(kA)B = A(kB) = k(A \times B)$

Multiplication de matrices

- Propriété d'associativité : $(A \times B) \times C = A \times (B \times C) = A \times B \times C$.
- Propriété de distributivité : $A \times (B + C) = A \times B + A \times C$ et $(A + B) \times C = A \times C + B \times C$.
- La multiplication de matrices n'est pas commutative.

DÉMONSTRATION

Ces propriétés découlent des propriétés analogues connues pour les nombres réels et des définitions des opérations sur les matrices. ■

Définition

Soit A une matrice carrée. On note A^2 la matrice $A \times A$; A^3 la matrice $A \times A \times A$ et plus généralement pour un entier naturel n non nul :

A^n la matrice égale au **produit de n facteurs égaux** à la matrice A.

D. Application à l'évolution de processus

1 Généralités

Lorsqu'on s'intéresse à l'évolution conjointe de plusieurs données reliées entre elles par des relations linéaires, on peut déterminer le passage d'un état des données à un autre en utilisant le produit matriciel.

Si les états possibles à un instant sont numérotés de 1 à n, on peut les représenter par une matrice colonne à n lignes.

Définition

On appelle **matrice de transition** des états la matrice carrée A de taille n dont le coefficient de la ligne i et de la colonne j donne à chaque instant le nombre, ou la proportion, ou la probabilité, des transitions possibles de l'état numéroté j à l'état numéroté i.

NOTE

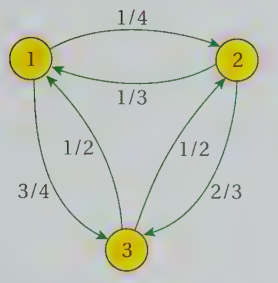
Raisonnement repris dans le cas particulier des marches aléatoires.

Par définition du produit matriciel, à chaque instant les données observées passent des états représentés par la matrice colonne X aux états représentés par la matrice colonne X' de telle sorte que $X' = A \times X$.

2 Marches aléatoires

EXEMPLE

Soit le graphe suivant constitué de 3 sommets. On se déplace d'un sommet à un autre sur ce graphe en suivant les arêtes orientées.
À chaque déplacement (ou pas) sur une arête, les probabilités de se trouver sur le sommet extrémité sachant que l'on est parti du sommet origine sont indiquées sur la figure.



Dans le cadre de marches aléatoires

On suppose que ces probabilités sont identiques quel que soit le parcours déjà effectué sur le graphe, donc « arriver au sommet j à partir du sommet i » est un événement indépendant de tous les événements qui ont précédé et sa probabilité est donc toujours la même. On parle de **probabilité de transition** d'un sommet vers un autre.

DÉFINITION

La **matrice de transition** d'une marche aléatoire est la matrice carrée dont le coefficient situé à l'intersection de la ligne i et de la colonne j est la probabilité de transition du sommet j vers le sommet i, soit encore **la probabilité d'arriver en i sachant qu'on est parti de j.**

REMARQUES

- Les probabilités de transition **du premier sommet** vers chacun des sommets du graphe constituent la **1re colonne** de la matrice, les probabilités de transition **du 2e sommet** vers chacun des sommets du graphe constituent la **2e colonne** de la matrice et ainsi de suite…
- **Important :** en lien avec le choix fait, la somme des coefficients d'une même colonne est donc toujours égale à 1.

Dans l'exemple précédent, la matrice de transition est : $A = \begin{pmatrix} 0 & 1/3 & 1/2 \\ 1/4 & 0 & 1/2 \\ 3/4 & 2/3 & 0 \end{pmatrix}$.

DÉFINITION

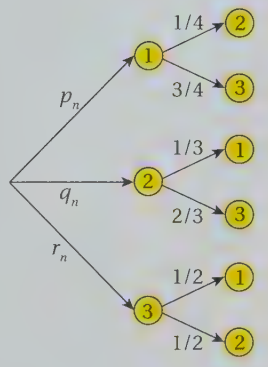
La matrice colonne **état de la marche aléatoire après n pas** est la matrice colonne donnant les probabilités d'arrivée en chaque sommet après n pas.

REMARQUE

Dans le cadre de marches aléatoires, on travaille aussi souvent avec des matrices de transition dont le coefficient situé à l'intersection de la ligne i et de la colonne j est la probabilité de transition du sommet i vers le sommet j ; les matrices des états sont alors écrites sous la forme de matrices formées d'une ligne.

EXEMPLE (SUITE)

Soit $X_n = \begin{pmatrix} p_n \\ q_n \\ r_n \end{pmatrix}$ la matrice colonne des états de l'exemple précédent.



L'arbre de probabilité ci-contre permet d'établir les relations entre les probabilités d'arrivées en chaque sommet après n pas et les probabilités d'arrivée en chaque sommet après $n + 1$ pas.
À l'aide du théorème de probabilités, connu sous le nom de **formule des probabilités totales**, on déduit de cet arbre les relations suivantes :

$$p_{n+1} = \frac{1}{3}q_n + \frac{1}{2}r_n \qquad q_{n+1} = \frac{1}{4}p_n + \frac{1}{2}r_n \qquad r_{n+1} = \frac{3}{4}p_n + \frac{2}{3}q_n$$

Par définition du produit matriciel, les relations de l'exemple sont équivalentes à l'égalité : $X_{n+1} = A \times X_n$.

Propriété

Pour une marche aléatoire associée à un déplacement sur un graphe dont la matrice de transition est notée A et la matrice colonne de l'état après n pas (n entier positif), est notée X_n.
On note alors, pour tout $n \geqslant 0$, $X_{n+1} = A \times X_n$ et, pour tout $n \geqslant 0$, $X_n = A^n \times X_0$.

Démonstration

La première relation se démontre par la formule des probabilités totales de façon analogue à la preuve donnée dans l'exemple.
On en déduit par une démonstration par récurrence très immédiate la seconde relation. ■

Exemple (suite)

On suppose que la marche aléatoire a pour départ le sommet n° 1 du graphe. Après 3 pas, l'état de la marche aléatoire est $X_3 = A^3 \times X_0$.

Comme $X_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, on obtient à l'aide de la calculatrice, $X_3 = \begin{pmatrix} 11/24 \\ 3/8 \\ 1/6 \end{pmatrix}$.

Ce qui implique par exemple que la probabilité d'être arrivé au sommet n° 2 après 3 pas est $\frac{3}{8}$.

▶ Savoir-faire 2
Utiliser le calcul matriciel pour déterminer l'évolution d'un processus, p. 94

Autre exemple

On considère à présent un mobile effectuant une marche aléatoire sur le graphe précédent de telle sorte que, à chaque pas :

- avec une probabilité de $\frac{1}{2}$, le mobile choisit comme dans l'exemple précédent de suivre une des arêtes issues du sommet sur lequel il est (avec la répartition probabiliste précédente pour le choix de l'arête).
- sinon : le mobile se place directement et de façon équirépartie sur n'importe quel sommet du graphe, y compris celui sur lequel il est.

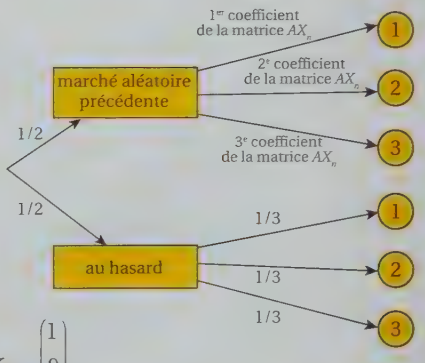
Notons : $X_n = \begin{pmatrix} p_n \\ q_n \\ r_n \end{pmatrix}$ la matrice colonne des états après n pas du mobile et $A = \begin{pmatrix} 0 & \frac{1}{3} & \frac{1}{2} \\ \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{4} & \frac{2}{3} & 0 \end{pmatrix}$ la matrice de transition associée à la marche aléatoire précédente.

L'arbre de probabilités ci-contre décrit l'évolution des probabilités de passage d'un sommet à un autre.

Par le théorème des probabilités totales, on déduit de cet arbre la relation suivante :

$$X_{n+1} = \begin{pmatrix} p_{n+1} \\ q_{n+1} \\ r_{n+1} \end{pmatrix} = \frac{1}{2} AX_n + \frac{1}{2} \begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix} = \frac{1}{2} AX_n + \frac{1}{2} B$$

si on note B la matrice colonne $\begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix}$.



Si le départ de la marche aléatoire est le sommet 1, $X_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Pour déterminer par exemple la probabilité que le mobile soit arrivé au sommet 3 après 2 pas, on calcule $X_1 = \frac{1}{2} A \times X_0 + \frac{1}{2} B$, puis $X_2 = \frac{1}{2} A \times X_1 + \frac{1}{2} B$.

On trouve grâce à la calculatrice : $X_2 = \begin{pmatrix} 101/288 \\ 31/96 \\ 47/144 \end{pmatrix}$.

Donc la probabilité d'être arrivé au sommet 3 après 2 pas est $\frac{47}{144}$.

Savoir-faire 1 — *Utiliser sa calculatrice pour le calcul matriciel*

ÉNONCÉ On donne les matrices carrées de taille 3 suivantes :

$$A = \begin{pmatrix} 1 & -3 & 2 \\ 4 & 7{,}5 & 0 \\ 6 & 5 & -1 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} \frac{1}{3} & \frac{2}{7} & \frac{1}{4} \\ 4 & \frac{10}{11} & 0 \\ 6 & 5 & -\frac{1}{2} \end{pmatrix}$$

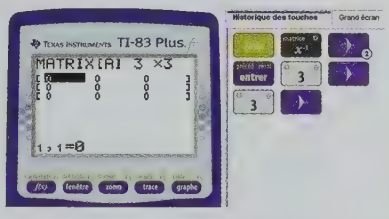
À l'aide de la calculatrice, déterminer la matrice $A + \frac{2}{3}B$.

SOLUTION

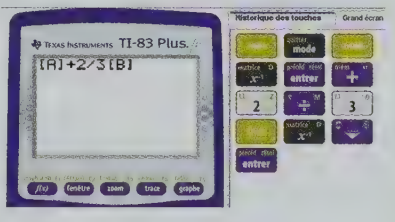
• Pour un modèle de la marque TI

Sélectionner la touche du clavier pour entrer dans le mode « matrice » ; choisir le mode EDIT (tout à droite), puis indiquer le nombre de lignes et de colonnes.

On entre ensuite les coefficients de la matrice.



On quitte le mode d'édition des matrices. On utilise alors les matrices précédemment éditées pour le calcul demandé en sélectionnant leur nom dans le mode « matrice » aux différentes étapes du calcul.

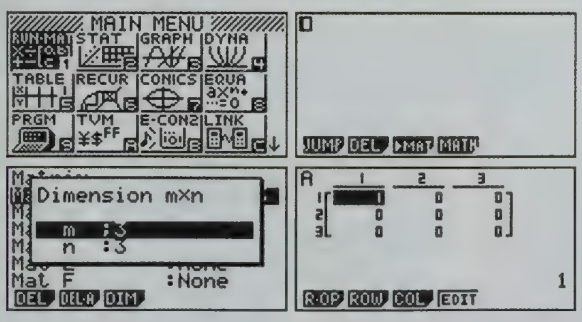


Pour des coefficients sous forme fractionnaire, on utilise la touche MATH, puis le mode FRAC.

• Pour un modèle de la marque CASIO

L'écran du mode RUNMAT permet d'entrer dans le mode matrice (touche F3 ▶ MAT) ; indiquer le nombre de lignes et de colonnes.

On entre ensuite les coefficients de la matrice.



On quitte le mode d'édition des matrices.

MÉTHODE

Pour les deux modèles de calculatrice :

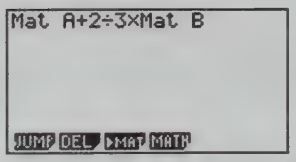
- on crée d'abord les matrices en entrant leurs coefficients,
- puis on effectue les calculs en rappelant les matrices par leur nom.

La calculatrice peut être employée pour la plupart des calculs matriciels vus en Terminale.

Comme pour tout calcul avec des nombres réels, dans un certain nombre de cas, le résultat donné par la calculatrice est approché, ce dont on peut se contenter selon les indications des énoncés.

Les flèches du clavier permettent la visualisation de tous les coefficients de la matrice affichée lorsque certains sont dissimulés en raison de la taille de l'écran.

On utilise alors les matrices précédemment éditées pour le calcul demandé en les faisant précéder de l'indication MAT que l'on sélectionne sur le clavier.



Pour des coefficients sous forme fractionnaire, on utilise la touche F↔D

Solution affichée par la calculatrice : $A + \frac{2}{3}B = \begin{pmatrix} \frac{11}{9} & -\frac{59}{21} & \frac{13}{6} \\ \frac{20}{3} & \frac{535}{66} & 0 \\ 10 & \frac{25}{3} & -\frac{4}{3} \end{pmatrix}$.

Exercices 8 et 9 p. 95

Savoir-faire 2 — *Utiliser le calcul matriciel pour déterminer l'évolution d'un processus*

ÉNONCÉ Les deux occupations de Patapon le chat, sur une journée, sont : « *dormir* » et « *manger* ».
On remarque que le matin à 7 h, il dort toujours.
S'il dort à une heure donnée, la probabilité qu'il dorme (à nouveau ou encore) une heure après est 3/4.
En revanche, s'il mange à une heure donnée, la probabilité qu'il mange à nouveau une heure après est 1/5.

Quelle est la probabilité pour que Patapon soit en train de manger à midi ?

SOLUTION

On note X_n la matrice colonne donnant les probabilités que Patapon dorme ou mange n heures après 7 h :

$$X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Pour tout n entier positif, $X_{n+1} = A \times X_n$ où A est la matrice de transition :

$$A = \begin{pmatrix} \frac{3}{4} & \frac{4}{5} \\ \frac{1}{4} & \frac{1}{5} \end{pmatrix}.$$

On détermine grâce à la calculatrice :

$$X_5 = A^5 \times X_0 \approx \begin{pmatrix} 0{,}76 \\ 0{,}24 \end{pmatrix}.$$

La probabilité cherchée est environ 0,24.

MÉTHODE

Le problème s'apparente à une marche aléatoire dont la matrice des états à chaque heure est une matrice colonne donnant la probabilité que Patapon dorme (état 1) et la probabilité qu'il mange (état 2). La matrice de transition est donc la matrice donnant dans la 1re colonne les probabilités que Patapon dorme ou mange 1 heure après avoir dormi et dans la 2de colonne les probabilités qu'il dorme ou mange 1 heure après avoir mangé.
On cherche la matrice colonne des états 5 heures après 7 h et on observe le 2e coefficient de cette matrice qui correspond à la probabilité que Patapon mange.

Exercices 38 et 39 p. 98

Exercices d'application

Définition des matrices et premières opérations

1 Des élèves ont habituellement cours dans trois salles de classes S1, S2 et S3.
Un jour donné, on leur propose trois informations sur l'orientation, une dans chaque salle ; ils peuvent choisir une des trois salles en fonction de leur intérêt pour l'information qui y est dispensée. La matrice suivante donne les pourcentages de transition d'une salle à une autre lors de cet événement :

$$M = \begin{pmatrix} 25\,\% & 35\,\% & 20\,\% \\ 40\,\% & 10\,\% & 20\,\% \\ 35\,\% & 55\,\% & 60\,\% \end{pmatrix}$$

Représenter cette situation par un graphe dont les sommets sont les salles reliés par des arêtes orientées indiquant les flux de population d'élèves ce jour-là.

2 La matrice suivante donne le nombre d'itinéraires possibles entre 4 points de contrôle d'une course d'orientation.

$$M = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 3 & 1 \\ 2 & 3 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}$$

Représenter la situation par un graphe.
Quelle propriété possède cette matrice ?

3 Compléter la matrice grâce aux informations données.

$$A = \begin{pmatrix} 2 & \ldots & 3 \\ \ldots & 0 & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix} \text{ et } \begin{array}{l} a_{23} = 7\,;\, a_{33} = -3\,;\, a_{32} = 8\,; \\ a_{12} = 5\,;\, a_{21} = 0{,}5\,;\, a_{31} = 2{,}4. \end{array}$$

4 Écrire la matrice carrée B de taille 4 dont les coefficients vérifient pour $1 \leqslant i \leqslant 4$ et pour $1 \leqslant j \leqslant 4$:

$$b_{ij} = i^2 + 2j.$$

5 Écrire la matrice carrée C de taille 5 dont les coefficients vérifient pour $1 \leqslant i \leqslant 5$ et pour $1 \leqslant j \leqslant 5$:

$$c_{ij} = |i - j| \text{ si } i \neq j \text{ et } c_{ij} = 1 \text{ sinon.}$$

6 Soit $A = \begin{pmatrix} 1 & -3 \\ 1{,}5 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -12 \\ 1{,}6 & 8 \end{pmatrix}$.

Calculer $A + B$.

7 Soit $A = \begin{pmatrix} 1 & 0 & 4 \\ 2 & 3 & 8 \\ 5 & 6 & 11 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & x & y \\ 6 & z & t \\ u & v & w \end{pmatrix}$.

Déterminer B et k tels que $A = kB$.

8 Soit $A = \begin{pmatrix} 5 & -2 \\ 3 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 7 \\ 11 & 0{,}5 \end{pmatrix}$.

a. Calculer $A + 2B$ et de $3B - 5A$.
b. Vérifier le résultat à l'aide d'une calculatrice.

9 Soit $A = \begin{pmatrix} 12 & 2 \\ 7 & -4 \end{pmatrix}$, $B = \begin{pmatrix} -2 & 9 \\ -7 & 20{,}5 \end{pmatrix}$ et $C = \begin{pmatrix} 1 & 5 \\ 8 & -1 \end{pmatrix}$

a. Calculer $2A + 4B - 3C$.
b. Vérifier le résultat à l'aide d'une calculatrice.

▸ Savoir-faire 1, p. 93

10 Soit A la matrice des prix TTC de 3 types de tablettes de chocolat différents dans 3 supermarchés d'une ville en 2010 (prix d'une tablette en colonne, supermarchés en ligne) :

$$A = \begin{pmatrix} 2{,}50 & 1{,}80 & 2{,}20 \\ 2{,}45 & 1{,}70 & 2{,}25 \\ 2{,}40 & 1{,}70 & 2{,}15 \end{pmatrix}.$$

Soit B la matrice des prix des mêmes produits dans les mêmes supermarchés en 2011 :

$$B = \begin{pmatrix} 2{,}60 & 1{,}85 & 2{,}35 \\ 2{,}45 & 1{,}80 & 2{,}35 \\ 2{,}50 & 1{,}75 & 2{,}20 \end{pmatrix}.$$

Quel calcul matriciel donne les augmentations des prix Hors Taxes de ces tablettes de chocolat entre 2010 et 2011 ? (La TVA pour le chocolat est 19,6 %.)
Donner le résultat de ce calcul matriciel.

11 Soit la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Compléter :

$$A = \ldots\ldots \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \ldots\ldots \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \ldots\ldots \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \ldots\ldots \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

12 Déterminer les réels x, y et z tels que :

$$\begin{pmatrix} x^2 & -2 \\ 3 & y+1 \end{pmatrix} = 2\begin{pmatrix} x & z \\ 1{,}5 & x+y \end{pmatrix}$$

Matrices produits et puissances de matrices

13 On nomme N la matrice carrée des notes en maths, physique et SVT d'un élève de Terminale aux trois trimestres d'une année scolaire (matières en colonne et trimestres en ligne).
On souhaite calculer une moyenne scientifique en affectant aux maths le coefficient 7, et à la physique et aux SVT le coefficient 6.

On nomme C la matrice colonne formée par ces trois coefficients.
Quelle matrice donne les moyennes scientifiques trimestrielles de l'élève ?

14 Pour les matrices suivantes, calculer le produit $A \times B$:

a. $A = \begin{pmatrix} 5 & -2 \\ 3 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 \\ 11 \end{pmatrix}$

b. $A = \begin{pmatrix} 1 & -3 & 2 \\ 4 & 7{,}5 & 0 \\ 6 & 5 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 3 \\ -2 \\ 5 \end{pmatrix}$

15 **1.** On considère une suite géométrique (u_n) de raison q définie pour $n \geqslant 0$. Soit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ 1 \end{pmatrix}$.

Montrer que, pour tout $n \geqslant 0$:
$X_{n+1} = M \times X_n$ où M est la matrice diagonale $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$.

2. On considère une suite arithmétique (u_n) de raison r définie pour $n \geqslant 0$ et, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ 1 \end{pmatrix}$.

Déterminer une matrice carrée M de taille 2 telle que :
pour tout $n \geqslant 0$, $X_{n+1} = M \times X_n$

16 Pour les matrices suivantes, calculer les produits $A \times B$ et $B \times A$:

a. $A = \begin{pmatrix} 5 & -2 \\ 3 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 7 \\ 11 & 0{,}5 \end{pmatrix}$

b. $A = \begin{pmatrix} 1 & -2 \\ 4 & 7{,}5 \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{2} & -\frac{1}{3} \\ 2 & \frac{1}{4} \end{pmatrix}$

c. $A = \begin{pmatrix} \sqrt{2} & 1 \\ 1 & \sqrt{2} \end{pmatrix}$ et $B = \begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & -1 \end{pmatrix}$

17 **1.** Soit les matrices $A = \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Calculer les produits $A \times B$ et $B \times A$; on appelle B la matrice nulle.

2. Soit les matrices $A = \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$ et $C = \begin{pmatrix} 2 & -2 \\ -1 & 1 \end{pmatrix}$.

Calculer les produits $A \times C$ et $C \times A$.

3. Tirer une conclusion des calculs précédents.

18 Pour les matrices suivantes, compléter à la main le produit $A \times B$:

$A = \begin{pmatrix} 5 & -2 & 1 \\ 3 & -4 & 2 \\ 8 & 7 & 20 \end{pmatrix}$ $B = \begin{pmatrix} 2 & 6{,}5 & -1 \\ 11 & 0{,}5 & 8 \\ -3 & 4 & 1 \end{pmatrix}$

et $A \times B = \begin{pmatrix} -15 & \ldots & -20 \\ -44 & 25{,}5 & \ldots \\ 33 & 135{,}5 & \ldots \end{pmatrix}$

19 Pour les matrices suivantes, compléter à la main le produit $A \times B$:

$A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & -2 & 1 \\ 3 & 5 & 1 \end{pmatrix}$ $B = \begin{pmatrix} -2 & 2 & 2 \\ -1 & -1 & 1 \\ 4 & 3 & 0 \end{pmatrix}$

et $A \times B = \begin{pmatrix} \ldots & 9 & 4 \\ 8 & 3 & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix}$

20 Pour les matrices suivantes, compléter à la main le produit $A \times B$:

$A = \begin{pmatrix} \frac{1}{4} & 1 & 0 & 1 \\ 2 & -3 & 4 & 8 \\ 0 & -1 & 2 & 1 \\ 3 & 5 & -\frac{1}{3} & 0 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 2 & 3 & 2 \\ 4 & 1 & 2 & 1 \\ 3 & 1 & 4 & 1 \\ 2 & 3 & 4 & 4 \end{pmatrix}$

et $A \times B = \begin{pmatrix} \ldots & \frac{9}{2} & \frac{27}{4} & \frac{11}{2} \\ 18 & 29 & 48 & 37 \\ 4 & \ldots & 10 & 5 \\ 22 & \frac{32}{3} & \ldots & \frac{32}{3} \end{pmatrix}$

21 On considère une matrice A quelconque de taille 4. Que donne le produit $A \times B$ lorsque :

a. $B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$? **b.** $B = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$?

22 **Algorithmique** Un programmateur de logiciel souhaite intégrer le produit matriciel de deux matrices carrées aux fonctions qu'il crée. Il peut entrer les matrices sous la forme de tableau et rappeler la valeur d'un coefficient par la syntaxe $A[i, j]$, compléter son algorithme de calcul du produit de deux matrices carrées de taille n.

```
Afficher « entrer la taille des 2 matrices carrées »
Lire n
Afficher « entrer les coefficients de la matrice A »
Pour i de 1 à n
        Pour j de 1 à n
                Lire A[i, j]
Afficher « entrer les coefficients de la matrice B »
Pour i de 1 à n
        Pour j de 1 à n
                Lire B[i, j]
Pour i de 1 à n
        Pour j de 1 à n
..... à compléter .....
Afficher « La matrice produit a pour coefficients : »
Pour i de 1 à n
        Pour j de 1 à n
                Afficher P[i, j]
                Aller à la ligne
```

23 Soit la matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

1. Calculer A^2 et A^3.

2. Que peut-on conjecturer pour A^n pour tout entier n strictement positif ?

3. Démontrer la conjecture à l'aide d'un raisonnement par récurrence.

24 Soit la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

1. Que peut-on conjecturer pour A^n pour tout entier n strictement positif ?

2. Démontrer la conjecture à l'aide d'un raisonnement par récurrence.

25 Soit la matrice $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix}$.

Cette **matrice** est appelée **diagonale**.

1. Calculer A^2 et A^3.

2. Que peut-on conjecturer pour A^n pour tout entier n strictement positif ?

3. Démontrer la conjecture.

26 On donne les matrices $A = \begin{pmatrix} 5 & -2 \\ 3 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 7 \\ 3 & -1 \end{pmatrix}$.

1. Calculer A^2 et B^2, puis $A^2 - B^2$.

2. Calculer $(A + B)(A - B)$.

3. Comparer les deux réponses et justifier.

27 Soit les matrices :

$M = \begin{pmatrix} 0 & 2 & 0 \\ 0 & -3 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $A = \begin{pmatrix} 2 & 1 & -7 \\ 4 & 3 & 1 \\ 8 & -5 & 0 \end{pmatrix}$

et $B = \begin{pmatrix} 7 & 8 & 2 \\ 4 & 3 & 1 \\ -3 & 0 & 5 \end{pmatrix}$.

1. Calculer $M \times A$ et $M \times B$.

2. Expliquer le résultat obtenu.

28 Soit la matrice A :

$A = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$ où a, b et c sont trois nombres réels.

1. Calculer A^2 et A^3.

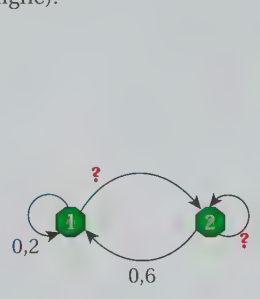
2. Que vaut A^n pour tout entier n strictement supérieur à 3 ? Le justifier.

Matrices et évolution de processus, marches aléatoires

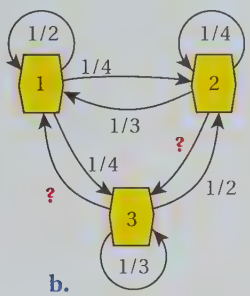
29 On considère une marche aléatoire entre les sommets d'un graphe.

Pour chacun des graphes suivants :

- compléter les probabilités manquantes ;
- écrire la matrice de transition pour la marche aléatoire (sommet de départ en colonne, sommet d'arrivée en ligne).



a.

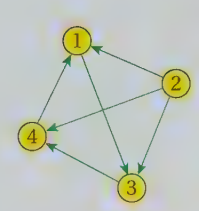


b.

30 On considère une marche aléatoire sur le graphe ci-contre.

À chaque pas, on passe d'un sommet à un autre par une arête issue de ce sommet choisie de façon équiprobable.

Donner la matrice de transition de cette marche aléatoire.



31 On donne les matrices de transition d'une marche aléatoire entre les sommets d'un graphe (sommet de départ en colonne, sommet d'arrivée en ligne).

Représenter pour chacune d'entre elles un graphe illustrant la marche aléatoire.

a. $\begin{pmatrix} 0 & \frac{1}{4} & 0 & \frac{1}{2} \\ 1 & 0 & \frac{2}{5} & \frac{1}{2} \\ 0 & 0 & \frac{1}{5} & 0 \\ 0 & \frac{3}{4} & \frac{2}{5} & 0 \end{pmatrix}$ **b.** $\begin{pmatrix} 0 & 0,6 & 0,5 \\ 0,7 & 0 & 0,5 \\ 0,3 & 0,4 & 0 \end{pmatrix}$

c. Une matrice carrée de taille 7 dont les coefficients vérifient, pour $1 \leqslant i \leqslant 7$ et pour $1 \leqslant j \leqslant 7$:

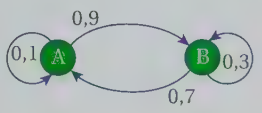
$c_{ij} = 1$ si $j = i + 1$ et $c_{ij} = 0$ sinon.

32 On considère un mobile se déplaçant sur le graphe probabiliste ci-dessous et partant du sommet A.

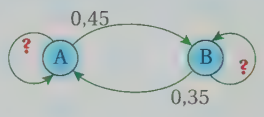
Donner la probabilité pour que :

a. le mobile soit en A après 5 pas ;

b. le mobile soit en B après 7 pas.



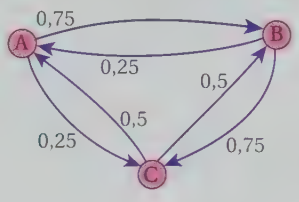
33 Même exercice pour le graphe ci-dessous et pour un mobile partant de B.



34 On considère un mobile se déplaçant sur le graphe probabiliste ci-dessous. Le mobile part du sommet A. Donner la probabilité pour que :

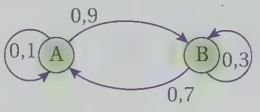
a. le mobile soit en B après 3 pas ;

b. le mobile soit en C après 4 pas.



35 On considère un mobile qui à chaque instant :

- suit les arêtes du graphe probabiliste ci-dessous avec la probabilité 0,7 ;
- ou choisit au hasard de façon équiprobable un des sommets du graphe (y compris celui sur lequel il est) avec la probabilité 0,3.



On note $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ la matrice colonne donnant la probabilité que le mobile occupe le sommet A ou B, n instants après son départ.

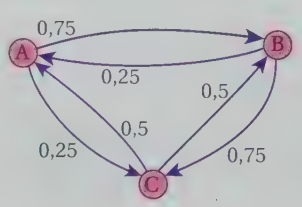
1. Déterminer une relation entre X_{n+1} et X_n. (On utilisera des matrices carrée et colonne que l'on explicitera.)

2. S'il part de A, donner la probabilité que le mobile soit en B après 4 pas.

3. S'il part de B, donner la probabilité que le mobile soit à nouveau en B après 5 pas.

36 On considère un mobile qui à chaque instant :

- suit les arêtes du graphe probabiliste ci-dessous avec la probabilité 0,8 ;
- ou choisit au hasard de façon équiprobable un des sommets du graphe (y compris celui sur lequel il est) avec la probabilité 0,2.



On note $X_n = \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$, la matrice colonne donnant la probabilité que le mobile occupe le sommet A, B ou C, n instants après son départ.

1. Déterminer une relation entre X_{n+1} et X_n. (On fera intervenir des matrices carrée et colonne que l'on explicitera.)

2. S'il part de A, donner la probabilité que le mobile soit en C après 4 pas.

3. S'il part de B, donner la probabilité que le mobile soit à nouveau en B après 5 pas.

37 Reprendre l'exercice précédent en considérant que la probabilité de suivre les indications du graphe probabiliste est de 0,6 et que sinon le mobile choisit exclusivement le sommet C avec la probabilité 0,4.

38 Pour les lycées Pascal et Montaigne d'une même ville, on a observé, en raison de l'offre d'options proposées, que d'une année à la suivante :

- 15 % des lycéens quittent le lycée Pascal pour le lycée Montaigne et 10 % des lycéens quittent le lycée Montaigne pour le lycée Pascal.
- De plus, dans chaque lycée, l'arrivée d'élèves venant du collège compense chaque année le départ des élèves vers les études supérieures ou les abandons.

1. Écrire la matrice de transition entre les états annuels des effectifs des élèves par lycée.

2. Si on suppose que les effectifs en 2009 des deux lycées sont identiques, donner le rapport des effectifs en 2013.

3. Le recteur décidera de modifier l'offre des options dans les lycées lorsque le lycée Montaigne aura 1/4 d'élèves en plus que le lycée Pascal. Cette modification aura-t-elle lieu ?

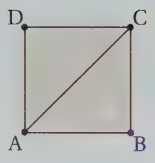
▸ Savoir-faire 2, p. 94

39 Un homme politique voit sa cote de popularité évoluer de la façon suivante :

- chaque mois, 3 % des personnes qui lui étaient favorables ne le sont plus,
- mais 3,5 % des personnes qui ne lui étaient pas favorables le deviennent.

Sa cote de popularité est actuellement de 41 %.
Peut-il espérer gagner l'élection présidentielle qui a lieu dans 1 an ?

40 On considère une marche aléatoire sur la figure ci-contre. À chaque sommet, chacune des arêtes issues de ce sommet a la même probabilité d'être choisie (y compris celle qui vient d'être éventuellement empruntée).



1. Dresser la matrice de transition d'un sommet à un autre.

2. Si on part du sommet C, quelle est la probabilité d'arriver au sommet D en 4 étapes ?

3. Si on part du sommet A, quelle est la probabilité d'arriver au sommet B en 5 étapes ?

41 Un œuvre d'art constituée de 5 ampoules alignées présente les caractéristiques d'allumage aléatoire suivantes :

- si une ampoule est allumée, la suivante est allumée avec une probabilité de 0,35 ;
- et si une ampoule est éteinte, la suivante est éteinte avec une probabilité de 0,65.

1. Établir la matrice de transition entre l'état d'une ampoule (en colonne) et l'état de l'ampoule suivante.

2. La première ampoule est allumée, quelle est la probabilité que la dernière le soit aussi ?
Même question si la première ampoule est éteinte.

Exercices d'approfondissement

42 Un produit pas si difficile

n désigne un entier naturel pair non-nul ($n = 2k$ pour k entier supérieur ou égal à 1).
On considère la matrice carrée A de taille n telle que pour $1 \leqslant i \leqslant n$ et pour $1 \leqslant j \leqslant n$:

$$a_{ij} = i + j.$$

Et la matrice colonne B telle que, pour $1 \leqslant j \leqslant n$:

$$b_j = (-1)^j.$$

Déterminer la matrice colonne $A \times B$.

43 Une formule pour des puissances

On donne la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

1. Calculer les matrices A^n pour $n = 2, 3, 4$ et 5.

2. Conjecturer le résultat de A^n en fonction de n pour tout entier naturel n.

3. Démontrer la conjecture.

44 Prévisions météorologiques

Un météorologue amateur a fait les constatations suivantes pour le mois de juin :

- s'il pleut un jour donné, alors le jour suivant : il pleut 1 fois sur 3, le ciel est couvert sans pluie 1 fois sur 3, sinon il fait beau ;
- si le ciel est couvert sans pluie un jour donné, alors le jour suivant : il pleut 1 fois sur 4, le ciel reste couvert sans pluie 1 fois sur 3, sinon il fait beau ;
- s'il fait beau un jour donné alors le jour suivant : il pleut 1 fois sur 4, le ciel est couvert sans pluie 1 fois sur 4, sinon il fait beau.

1. Un lundi du mois de juin, il fait beau.
a. Donner la probabilité pour que le mercredi soit pluvieux.
b. Donner la probabilité pour que le dimanche soit pluvieux.

2. Un lundi du mois de juin est couvert sans pluie, donner la probabilité qu'il pleuve le mercredi et le jeudi. (On pourra utiliser la formule des probabilités conditionnelles.)

45 Une matrice de Leslie

Pour observer le vieillissement de la population féminine jeune d'un pays, on divise la population des femmes de moins de 45 ans en 3 classes :
les femmes de moins de 15 ans, les femmes d'âge entre 15 à 30 ans et les femmes de 30 à 45 ans .
On note tous les 15 ans dans un vecteur colonne la répartition de ces femmes dans les 3 catégories.
On suppose que la matrice de passage d'une répartition à une autre tous les 15 ans est donnée par :

$$A = \begin{pmatrix} 0 & 1{,}5 & 1 \\ 0{,}99 & 0 & 0 \\ 0 & 0{,}9 & 0 \end{pmatrix}.$$

1. Expliquer à quoi correspondent les 4 coefficients non-nuls de cette matrice.

2. On suppose à présent qu'à un moment donné, la répartition est de 1 million de femmes par catégorie.
a. Donner la répartition dans les 3 catégories de la population féminine dans 60 ans.
b. Comparer cette répartition avec celle d'une population où le 2e et le 3e coefficient de la ligne 1 seraient échangés.

Ce type de modèle d'étude de la dynamique d'une population structurée en âge est dû à P.H. Leslie (1945) ; il est l'un des plus utilisés en dynamique des populations et en démographie.

46 **Une autre matrice de Leslie**

On considère la matrice colonne donnant la répartition d'une population d'insectes suivant des critères d'âge. Sur une période de temps déterminée, on constate que :

- la plus jeune partie de la population ne peut pas se reproduire et la moitié de ses individus atteint le 2^e stade de développement ;
- la partie de la population qui a atteint ce 2^e stade de développement ne peut pas se reproduire non plus et seul 1/3 de ses éléments atteint le 3^e stade de développement ;
- en moyenne, chaque individu qui atteint le 3^e stade de développement donne naissance à 6 petits, puis meurt.

1. Pour une répartition initiale de la population qu'on choisira, observer l'évolution de la matrice colonne donnant la répartition sur au-moins 3 périodes de temps.
Que constate-t-on ? Que peut-on dire de la suite des matrices colonnes donnant la répartition ?

2. Démontrer que ce phénomène se produit quelle que soit la répartition initiale de la population.

47 **Un problème d'endémie** (*d'après un document* DGESCO)

Un individu vit dans un lieu où il est susceptible d'attraper une maladie par piqûre d'insecte. Il peut être dans l'un des trois états suivants : immunisé (I), malade (M), non malade et non immunisé (S). D'un mois à l'autre, son état peut changer suivant les règles suivantes :

- étant immunisé, il peut le rester avec une probabilité 0,9 ou passer à l'état S avec une probabilité 0,1 ;
- étant dans l'état S, il peut le rester avec une probabilité 0,5 ou passer à l'état M avec une probabilité 0,5 ;
- étant malade, il peut le rester avec une probabilité 0,2 ou passer à l'état I avec une probabilité 0,8.

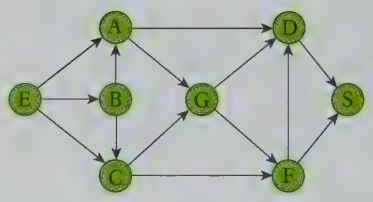
Montrer que cette situation s'apparente à une marche aléatoire dont on donnera la matrice de transition.
À l'aide d'une calculatrice ou d'un ordinateur, calculer la probabilité qu'un individu soit malade ou immunisé au bout de trois mois, de six mois, d'un an, de deux ans, pour chacune des situations suivantes :

- au départ, il est immunisé ;
- au départ, il est non malade et non immunisé ;
- au départ, il est malade.

Pouvez-vous donner des éléments sur la proportion d'individus malades dans la population étudiée ?

48 **Circuits touristiques** (*d'après un document* DGESCO, TES)

Pour traverser une chaîne de montagnes, il faut passer par plusieurs sommets, reliés entre eux par des voies ne pouvant être franchies que dans un seul sens.
On donne ci-dessous le graphe associé à cette situation (E est le point d'entrée et S est le point de sortie).



1. Écrire la matrice M de transition d'un sommet à un autre en une étape (une étape est le passage d'un sommet à un autre par une des voies directes du graphe). Les sommets sont classés dans l'ordre E, A, B, C, G, D, F, S.

2. Sans utiliser de calculatrice, justifier que la première colonne de la matrice M^2 est $\begin{pmatrix}0\\1\\0\\1\\2\\1\\1\\0\end{pmatrix}$.

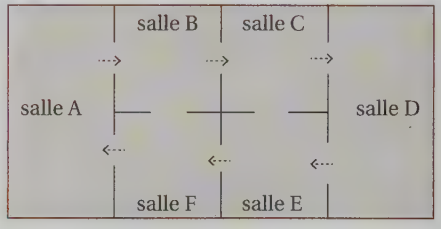
Que représentent les coefficients de cette colonne ?

3. Déterminer à l'aide d'une calculatrice la première colonne de la matrice M^3 ; que représente le dernier coefficient de cette colonne ? Justifier.

4. Combien de parcours comportent 6 étapes ? Décrire les sommets successifs de ces randonnées.

5. Justifier sans calcul que pour tout $n \geqslant 7$, M^n est la matrice dont tous les coefficients sont nuls.

49 Lors d'une exposition consacrée à la peinture impressionniste, les services d'organisation ont divisé un hall rectangulaire en 6 pièces pour 6 thèmes différents. On peut suivre un parcours thématique fléché comme ci-dessous.



Les organisateurs ont constaté que 75 % des visiteurs suivent le fléchage suggéré, tandis que les autres empruntent dans chaque salle de façon équirépartie une des portes de la salle (y compris celle par laquelle ils sont entrés).

1. Si tous les visiteurs partent de la salle A à l'ouverture du musée et changent de salle toutes les 10 minutes, quelle est la répartition des visiteurs dans les salles une heure après l'ouverture ?

2. Quelle est la probabilité qu'un visiteur parti de la salle A ait visité la salle D au cours des 40 premières minutes ?

Activités de recherche et résolution de problèmes

Travaux pratiques utilisant l'outil informatique

Problèmes de recherche

50 Un jeu de l'oie

Le jeu de l'oie simplifié suivant est constitué de 8 cases.

On joue à ce jeu avec un dé tétraédrique qui comporte 4 faces numérotées de 1 à 4.

Pour jouer un coup, on lance le dé et on avance d'autant de cases que ce qu'indique le dé.

Mais si on arrive sur la case 3, l'échelle permet un passage direct sur la case 6. En revanche, si on arrive sur la case 7, le puits nous fait retomber sur la case 2.

On gagne lorsque le lancer du dé permet d'arriver exactement sur la case 8, sinon on repart en reculant.

8 Arrivée	7	6	5
1 Départ	2	3	4

À l'aide d'un tableur, on souhaite calculer les probabilités d'arrivée sur la case 8 en différents nombres de coups.

1 Sur une feuille de calcul, compléter la matrice de transition d'une case à l'autre pour ce jeu de l'oie. (Les probabilités de transition des cases 1, 3, 5 et 8 vers les autres cases sont déjà complétées.)

	A	B	C	D	E	F	G	H	I
1	matrice de transition à chaque coup	0		0		0			0
2		0,25		0		0,5			0
3		0		0		0			0
4		0,25		0		0			0
5		0,25		0		0			0
6		0,25		0		0,25			0
7		0		0		0			0
8		0		0		0,25			1

2 Pour déterminer les probabilités d'arrivées sur chaque case après 1 coup, il faut effectuer le produit de la matrice carrée de transition par la matrice colonne des états au départ.

a. Compléter la feuille de calcul précédente comme indiqué ci-après pour y faire apparaître les matrices colonnes des états. On obtient alors la feuille de calcul ci-dessous.

Tableur et matrices

La commande = PRODUITMAT() permet de multiplier des matrices avec un tableur ; les formules de calcul habituelles sur les cellules permettent de créer facilement des sommes de matrices ou un produit de matrice par un réel.

ECARTYPEP =PRODUITMAT(

	A	PRODUITMAT(**matrice1**; matrice2)			E	F	G	H	I	J	K	L	M
1	matrice de transition à chaque coup	0		0		0			0				
2		0,25		0		0,5			0				
3		0		0		0			0				
4		0,25		0		0			0				
5		0,25		0		0			0				
6		0,25		0		0,25			0				
7		0		0		0			0				
8		0		0		0,25			1				
9													
10													
11	nombre de coups joués	0	1	2	3	4	5	6	7	8	9	10	11
12													
13	probabilité d'être sur la case 1	1	MAT(										
14	probabilité d'être sur la case 2	0											
15	probabilité d'être sur la case 3	0											
16	probabilité d'être sur la case 4	0											
17	probabilité d'être sur la case 5	0											
18	probabilité d'être sur la case 6	0											
19	probabilité d'être sur la case 7	0											
20	probabilité d'être sur la case 8	0											

b. Pour faire afficher dans les cellules C13 à C20 le produit attendu :

- sélectionner cette plage de cellules ;
- entrer dans la ligne de saisie la formule : =PRODUITMAT(... ;...) en complétant cette formule par la plage de cellules correspondant à la matrice de transition et la plage de cellules correspondant à la matrice colonne de départ ;
- valider la formule par les touches CTRL + MAJ + ENTREE (**attention** : la touche entrée seule produit un message d'erreur).

3 Pour obtenir les états après différents nombres de coups :

- s'assurer que la formule précédente donne bien par recopie vers la droite, les matrices colonnes attendues, sinon modifier cette formule en conséquence.
- recopier alors la formule vers la droite.

a. Quelle est la probabilité d'arriver dans la case 8 en 2 coups ?

b. Quel est le nombre minimal de coups à jouer pour avoir une probabilité supérieure à 1/2 d'avoir terminé la partie ?

c. Même question pour une probabilité supérieure à 0,99.

d. Quelle est la probabilité d'être arrivé dans la case 8 après exactement 10 coups ?

51 Une décomposition en une somme bien pratique

1 **Un exemple pour démarrer.** Soit la matrice $M = \begin{pmatrix} 0{,}44 & 0{,}24 \\ 0{,}56 & 0{,}76 \end{pmatrix}$.

a. À l'aide d'une calculatrice ou d'un autre outil, calculer M^n pour $n = 2, 3, 4$ et 5.
Quelle conjecture peut-on émettre ?

b. Vérifier que $M = A + 0{,}2B$ avec $A = \begin{pmatrix} 0{,}3 & 0{,}3 \\ 0{,}7 & 0{,}7 \end{pmatrix}$ et $B = \begin{pmatrix} 0{,}7 & -0{,}3 \\ -0{,}7 & 0{,}3 \end{pmatrix}$.

c. Calculer $A \times B$ et $B \times A$.

d. Montrer que, pour tout $n \geqslant 1$, $A^n = A$ et $B^n = B$.

e. À l'aide des résultats précédents et d'un raisonnement par récurrence, démontrer que :

pour tout $n \geqslant 1$, $M^n = A + 0{,}2^n B$.

f. En déduire la démonstration de la conjecture émise à la question **a.**

2 **Généralisation à un certain type de matrices**

a. Soit x et y deux nombres réels tels que $x + y = 1$, et soit les matrices $A = \begin{pmatrix} x & x \\ y & y \end{pmatrix}$ et $B = \begin{pmatrix} y & -x \\ -y & x \end{pmatrix}$.

Calculer $A \times B$ et $B \times A$.

b. Montrer que, pour tout $n \geqslant 1$, $A^n = A$ et $B^n = B$.

c. Soit la matrice carrée $M = \begin{pmatrix} p & q \\ 1-p & 1-q \end{pmatrix}$

où p et q désignent des nombres réels tels que $p - q \neq 1$.

Montrer que $M = A + (p - q)\,B$ où A et B sont des matrices :

$$A = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \text{ et } B = \begin{pmatrix} y & -x \\ -y & x \end{pmatrix} \text{ avec } x = \frac{q}{1-p+q} \text{ et } y = \frac{1-p}{1-p+q}$$

d. À l'aide d'un raisonnement par récurrence, démontrer que :

pour tout $n \geqslant 1$, $M^n = A + (p - q)^n B$.

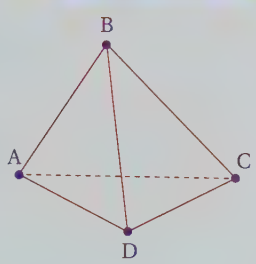
e. Dans le cas où $|p - q| < 1$, que peut-on dire des coefficients de la matrice M^n lorsque n tend vers $+\infty$?

Note
Cette décomposition particulière est pratique pour l'étude de la convergence des suites formées par les coefficients des matrices M^n. (Voir chapitre 6.)

52 Marche aléatoire sur un tétraèdre et algorithmes

Algorithmique

On considère un mobile effectuant une marche aléatoire sur un tétraèdre ABCD.



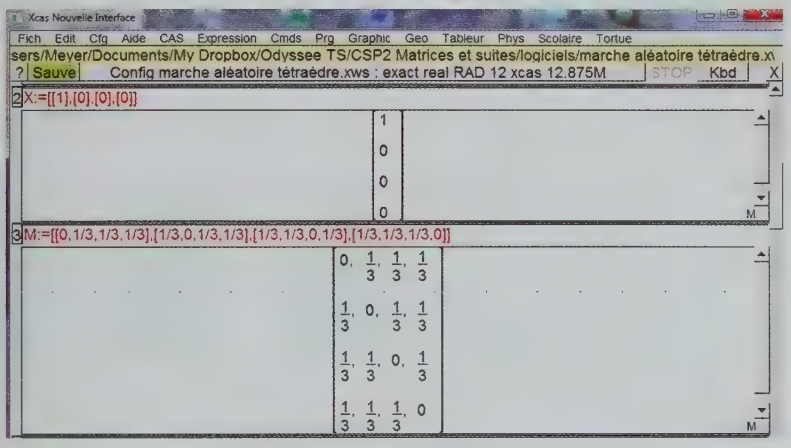
1 Première situation

À chaque pas, le mobile passe d'un sommet à un autre par une arête issue de ce sommet choisie de façon équiprobable.

a. Donner la matrice M de transition entre les états de cette marche aléatoire.

La calculatrice ou un tableur peuvent fournir des valeurs approchées des différents états de la marche aléatoire après un certain nombre de pas.

Le logiciel de calcul formel **Xcas** permet d'en déterminer les valeurs exactes :



La syntaxe sur Xcas :

Pour entrer les matrices, on entre les coefficients par ligne entre crochets du type [ ], les coefficients et les lignes sont séparés par des virgules, comme ci-dessus.

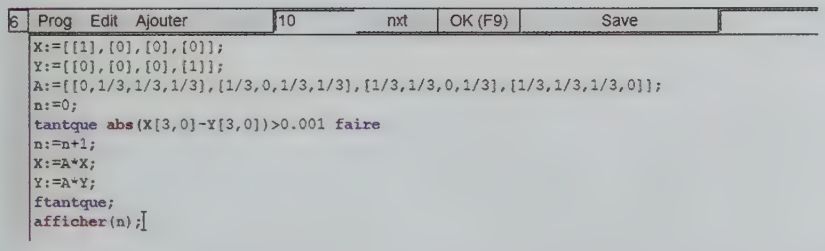
Les opérations sur les matrices sont notées +,* comme pour les nombres réels.

Attention : sous **Xcas**, la numérotation des lignes et des colonnes commence par 0 donc le coefficient A [0, 3] est le coefficient de la 1re ligne, 4e colonne.

b. Si on part du sommet A, quelle est la probabilité d'arriver au sommet D après 4 pas ?

c. La probabilité d'arriver en D après 4 pas est-elle indépendante du sommet de départ ? Justifier.

d. On donne le programme suivant rédigé sous **Xcas** :



Exécuter et interpréter la réponse de ce programme en lien avec la marche aléatoire.

2 Seconde situation

On suppose à présent que pour chaque pas de la marche aléatoire :

- avec une probabilité de 0,8 : le mobile choisit de suivre de façon équirépartie une des arêtes issues du sommet sur lequel il est ;
- avec une probabilité de 0,2 : le mobile choisit de sauter directement et aléatoirement sur n'importe quel sommet du tétraèdre, y compris celui sur lequel il est.

a. Montrer que si on note X_n (pour n entier positif) la matrice colonne des états de la marche aléatoire après n pas, alors pour tout $n \geqslant 0$:

$$X_{n+1} = 0{,}8 \times A \times X_n + 0{,}2 \times B \text{ où } B \text{ est la matrice colonne } B = \begin{pmatrix} 0{,}25 \\ 0{,}25 \\ 0{,}25 \\ 0{,}25 \end{pmatrix}.$$

b. Si on part du sommet A, quelle est la probabilité d'arriver au sommet D après 4 pas ?

c. Si on part du sommet D, quelle est la probabilité d'arriver au sommet D après 4 pas ?

d. Écrire un algorithme pour déterminer le plus petit nombre de pas pour lequel la probabilité d'être arrivé en A en partant de A est 1/4 à 10^{-6} près.

53 La collection de figurines

L'entreprise d'œufs surprises en chocolat CHILDREN propose pour les mois à venir une collection de 3 types de figurines réparties en proportions égales à l'intérieur des œufs.
(On suppose le nombre d'œufs suffisamment important pour qu'après chaque achat la répartition des figurines suive toujours une loi équirépartie.)

Partie 1. Un argument de vente

La firme annonce qu'un client ayant effectué 6 achats a au moins 3 chances sur 4 d'avoir la collection complète formée des trois types de figurines.
Pour un client donné, pour tout entier $n \geqslant 1$, on représente l'état de la collection après n achats par la matrice colonne $X_n = \begin{pmatrix} p_n \\ q_n \\ r_n \end{pmatrix}$ où p_n désigne la probabilité que le client ait un type de figurine de la collection, q_n désigne la probabilité qu'il ait deux types de figurines et où r_n désigne la probabilité qu'il ait les trois types de figurines.

1. Donner la matrice colonne X_1 correspondant à la situation après le 1er achat du client.

2. Justifier que, pour tout $n \geqslant 1$, $X_{n+1} = MX_n$ où M désigne la matrice $M = \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ \frac{2}{3} & \frac{2}{3} & 0 \\ 0 & \frac{1}{3} & 1 \end{pmatrix}$.

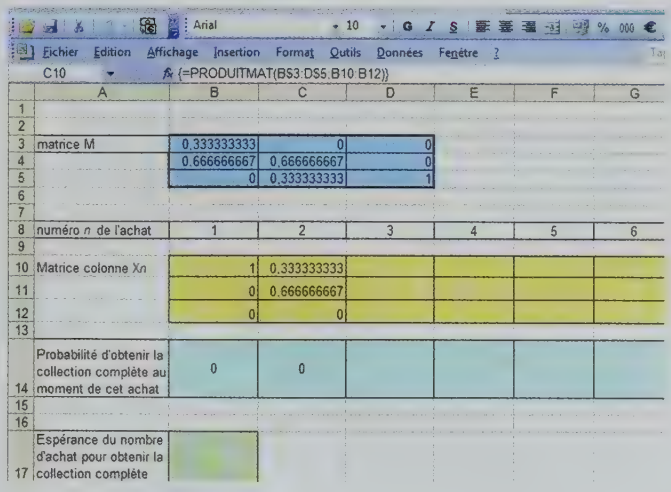
3. Utiliser la calculatrice ou un tableur pour déterminer si l'affirmation de la firme CHILDREN sur la probabilité d'obtenir la collection complète après 6 achats est exacte.

Partie 2. Nombre moyen d'achats pour avoir la collection complète

On suppose que le client effectuera au maximum 25 achats de ce type de produit pour obtenir la collection complète.
On souhaite déterminer dans ces conditions le nombre d'achats moyen qui permet d'avoir les 3 types de figurines.

1. À l'aide d'un tableur, créer une feuille de calcul qui calcule et affiche les matrices colonnes des états de la collection entre 1 et 25 achats.

2 Compléter cette feuille de calcul par une ligne qui donne pour chaque nombre d'achats la probabilité qu'il s'agisse du moment où le client obtient la collection complète.
Justifier le calcul avec rigueur.



3 On définit la variable aléatoire X égale au nombre d'achats permettant d'obtenir la collection complète ou qui prend la valeur 0 si ce nombre d'achats est supérieur à 25.
Quel est le nombre moyen d'achats (espérance) qui permet d'obtenir la collection complète ?

Partie 3. Nombre moyen d'achats pour avoir la collection complète (suite)

À présent, on note m le nombre maximal d'achats qu'un acheteur envisage de faire (m désigne un entier supérieur ou égal à 1).
Pour déterminer la valeur exacte de l'espérance du nombre d'achats nécessaires à l'obtention de la collection complète, on introduit les variables aléatoires suivantes :

- Y_1 : le nombre d'œufs à acheter pour obtenir un 1er type de figurine ;
- Y_2 : le nombre d'œufs à acheter pour avoir un 2e type de figurine (lorsqu'on en a déjà 1) ;
- Y_3 : le nombre d'œufs à acheter pour avoir un 3e type de figurine (lorsqu'on en a déjà 2).

Par convention, Y_2 et Y_3 prennent la valeur 0 quand les m achats ne suffisent pas pour obtenir un 2e type de figurine ou un 3e type de figurine.

1 Déterminer la loi de probabilité de la variable aléatoire Y_1.

2 Montrer que la loi de la variable aléatoire Y_2 est une loi géométrique tronquée de paramètres m et $\frac{2}{3}$, loi rappelée dans le tableau suivant :

Valeurs de Y_2	0	1	2	3	4	…	m
Probabilités	$\left(\frac{1}{3}\right)^m$	$\frac{2}{3}$	$\frac{1}{3}\times\frac{2}{3}$	$\left(\frac{1}{3}\right)^2\times\frac{2}{3}$	$\left(\frac{1}{3}\right)^3\times\frac{2}{3}$		$\left(\frac{1}{3}\right)^{m-1}\times\frac{2}{3}$

3 Montrer que la loi de la variable aléatoire Y_3 est une loi géométrique tronquée de paramètres m et $\frac{1}{3}$.

4 Espérances des lois géométriques tronquées

a. Justifier que pour tout x réel différent de 1 : $1 + x + x^2 + x^3 + \ldots\ldots + x^m = \frac{1-x^{m+1}}{1-x}$.

b. En utilisant un calcul de dérivées, en déduire le calcul, pour tout $x \neq 1$ de la somme :
$$1 + 2x + 3x^2 + 4x^3 + \ldots\ldots + mx^{m-1}$$

5 **a.** Calculer $E(Y_2)$, $E(Y_3)$.

b. Déduire de ce qui précède que les espérances des variables aléatoires Y_2 et Y_3 tendent respectivement vers 3 et vers $\frac{3}{2}$ lorsque m tend vers $+\infty$.

c. Justifier que, sans limiter le nombre d'achats, le nombre moyen d'œufs CHILDREN à acheter pour espérer avoir la collection complète est 5,5.

54 Un algorithme pour déterminer des valeurs approchées de racines carrées *(D'après TJ Fletcher : L'Algèbre linéaire par ses applications)*

On doit à Théon de Smyrne une méthode de calcul de valeurs approchées de $\sqrt{2}$ par un algorithme énoncé à peu près ainsi :

« En partant de (1 ; 1) :

- on calcule les valeurs successives de $(x\,;y)$ en remplaçant à chaque étape $(x\,;y)$ par $(x+2y\,;x+y)$;
- $\frac{x}{y}$ donne une approximation de $\sqrt{2}$. »

Théon de Smyrne

Mathématicien grec du IIe siècle après J.-C. Dans son ouvrage, *Exposition des connaissances mathématiques utiles à la lecture de Platon,* on trouve une approche des irrationnels par une double suite de côtés et de diagonales de carrés.

Partie 1. Approximation de racine de 2

Soit la matrice carrée $A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. On définit pour $n \geqslant 0$, la suite de matrices colonnes (R_n) telle que $R_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $R_{n+1} = A \times R_n$ pour tout $n \geqslant 0$.

1. Pour tout $n \geqslant 0$, on définit par x_n et y_n les nombres obtenus par itérations successives de l'algorithme de Théon de Smyrne. Montrer que, pour tout $n \geqslant 0$, R_n est la matrice $\begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

2. Calculer alors R_{10} à l'aide d'une calculatrice, puis comparer $\frac{x_{10}}{y_{10}}$ avec $\sqrt{2}$.

Partie 2. Démonstration de la convergence

1. **a.** Justifier que les deux suites (x_n) et (y_n) sont à termes strictement positifs.

   b. Démontrer que, pour tout $n \geqslant 0$, $\frac{x_n}{y_n} \geqslant 1$.

   c. Démontrer que, pour tout $n \geqslant 0$, $\frac{x_{n+1}}{y_{n+1}} - \sqrt{2} = \frac{\sqrt{2}-1}{\frac{x_n}{y_n}+1}\left(\sqrt{2} - \frac{x_n}{y_n}\right)$.

   d. En déduire que, pour tout $n \geqslant 0$, $\left|\frac{x_{n+1}}{y_{n+1}} - \sqrt{2}\right| \leqslant \frac{1}{2}\left|\sqrt{2} - \frac{x_n}{y_n}\right|$.

   e. Prouver alors par récurrence que, pour tout $n \geqslant 0$, $\left|\frac{x_n}{y_n} - \sqrt{2}\right| \leqslant \left(\frac{1}{2}\right)^n (\sqrt{2}-1)$. Conclure sur la convergence de la suite $\left(\frac{x_n}{y_n}\right)$.

2. **a.** Déterminer un entier n pour lequel $\frac{x_n}{y_n}$ donne une valeur approchée à 10^{-8} près de $\sqrt{2}$.

   b. À l'aide d'un calcul matriciel, calculer le quotient $\frac{x_n}{y_n}$ pour cette valeur de n.

Partie 3. Extension de la méthode

1. Remplacer le coefficient a_{12} de la matrice A par un entier naturel différent de 2.
   Calculer la matrice colonne R_n correspondante pour quelques valeurs de n et faire une conjecture sur la convergence de la suite des quotients $\left(\frac{x_n}{y_n}\right)$ si R_n est la matrice $\begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

2. Énoncer une généralisation de la méthode de Théon de Smyrne pour le calcul d'une racine carrée.

3. Démontrer ce résultat généralisé.

OBJECTIF BAC

Sujets type BAC

Exercice résolu

Exercice 55 *D'après Bac ES, France métropolitaine, juin 2008*

Deux fabricants de parfums lancent simultanément leur nouveau produit qu'ils nomment respectivement Aurore et Boréale.

Afin de promouvoir celui-ci, chacun organise une campagne de publicité. L'un d'eux contrôle l'efficacité de sa campagne par des sondages hebdomadaires. Chaque semaine, il interroge les mêmes personnes qui toutes se prononcent en faveur de l'un de ces deux produits.

Au début de la campagne, 20 % des personnes interrogées préfèrent Aurore et les autres préfèrent Boréale.

Les arguments publicitaires font évoluer cette répartition : 10 % des personnes interrogées préférant Aurore et 15 % des personnes interrogées préférant Boréale changent d'avis d'une semaine sur l'autre.

La semaine du début de la campagne est notée semaine 0.

Pour tout entier naturel n, on désigne par la matrice colonne $P_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ l'état probabiliste la semaine n après le début de la campagne où a_n désigne la probabilité qu'une personne interrogée au hasard préfère Aurore la semaine n et b_n désigne la probabilité qu'une personne choisie au hasard préfère Boréale la semaine n.

1. a. Donner la matrice P_0.

b. Cette situation peut-être assimilée à une marche aléatoire sur un graphe à deux sommets.

Écrire la matrice de transition M entre les états P_n de cette marche aléatoire.

2. a. Calculer P_1 à la main.

b. Exprimer, pour tout n, P_n en fonction de P_0 et n.

c. En déduire P_4 à l'aide de la calculatrice (on donnera des valeurs approchées au centième) et interpréter ce résultat.

3. Écrire en langage naturel un algorithme permettant de déterminer si le parfum Aurore sera préféré au parfum Boréale durant une des 10 premières semaines suivant le début de cette campagne.

4. Le fabricant de parfum qui a lancé la campagne estime qu'en fait chaque semaine seuls 80 % des consommateurs voient leur comportement influencé comme décrit ci-dessus par la publicité. Les 20 % restant choisissent de façon équiprobable un des deux parfums.

On désigne à nouveau par la matrice colonne P_n l'état probabiliste la *n-ième* semaine après le début de la campagne.

a. Établir, pour tout $n \geqslant 0$, une relation entre P_{n+1} et P_n faisant intervenir la matrice M et la matrice colonne $N = \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix}$.

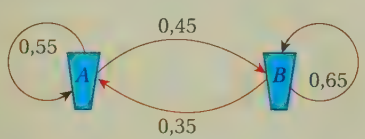
b. Si les conditions initiales sont celles du début de l'énoncé, déterminer, à l'aide de la calculatrice, l'état probabiliste des choix de parfums après 4 semaines de publicité (arrondir les résultats au centième).

Voir résolution page suivante.

Exercice 56 Algorithmique

On considère un ensemble de particules pouvant être dans l'état A, l'état B ou l'état C à chaque unité de temps.

On remarque que 80 % des particules A ou B changent d'état en une unité de temps en suivant les probabilités indiquées par le graphe ci-dessous :



Les 20 % de particules restantes passent à l'état C stable à chaque unité de temps.

On note $X_n = \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$, la matrice colonne donnant la proportion de particules dans chaque état n unités de temps après le début de l'observation.

1. Montrer que, pour tout $n \geqslant 0$, $X_{n+1} = 0{,}8\,M X_n + 0{,}2\,N X_n$ où M et N sont des matrices que l'on explicitera.

2. Si on suppose que les particules sont toutes dans l'état A au départ, déterminer les probabilités de chaque état des particules après 10 unités de temps.

3. Écrire un algorithme permettant de déterminer l'instant à partir duquel 50 % des particules aura atteint l'état stable C.

Résolution

1. a. On détermine la matrice colonne $P_0 = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$ où a_0 désigne la probabilité qu'une personne préfère le parfum Aurore au début de la campagne. Ainsi $a_0 = 20\ \% = 0{,}2$ et b_0 désigne la probabilité qu'une personne préfère le parfum Boréale au début de la campagne, donc $b_0 = 80\ \% = 0{,}8$.

Ainsi $P_0 = \begin{pmatrix} 0{,}2 \\ 0{,}8 \end{pmatrix}$.

b. D'après l'énoncé, les probabilités de transition entre les états de cette marche aléatoire sont données par la matrice carrée : $M = \begin{pmatrix} 0{,}9 & 0{,}15 \\ 0{,}1 & 0{,}85 \end{pmatrix}$.

2. a. Par propriété de la matrice de transition entre les états de cette marche aléatoire :

$$P_1 = M \times P_0 = \begin{pmatrix} 0{,}9 \times 0{,}2 + 0{,}15 \times 0{,}8 \\ 0{,}1 \times 0{,}2 + 0{,}85 \times 0{,}8 \end{pmatrix} = \begin{pmatrix} 0{,}3 \\ 0{,}7 \end{pmatrix}$$

b. Par propriété de la matrice de transition entre les états de cette marche aléatoire :

$$P_n = M^n \times P_0 = \begin{pmatrix} 0{,}9 & 0{,}15 \\ 0{,}1 & 0{,}85 \end{pmatrix}^n \times P_0$$

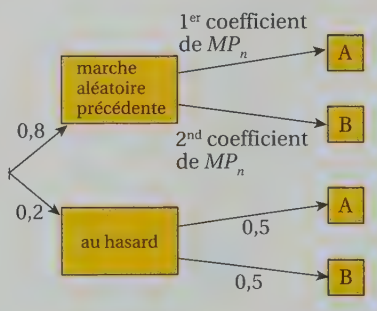
c. À l'aide de la calculatrice, on trouve $P_4 = M^4 \times P_0 = \begin{pmatrix} 0{,}9 & 0{,}15 \\ 0{,}1 & 0{,}85 \end{pmatrix}^4 \times \begin{pmatrix} 0{,}2 \\ 0{,}8 \end{pmatrix} \approx \begin{pmatrix} 0{,}47 \\ 0{,}52 \end{pmatrix}$.

Ainsi, après 4 semaines de campagne publicitaire, on peut dire que la probabilité qu'une personne interrogée préfère le parfum Aurore est d'environ 0,47 et la probabilité qu'elle préfère Boréale est d'environ 0,52.

3.

```
La matrice colonne P prend la valeur (0,2 / 0,8)
La matrice carrée M prend la valeur (0,9  0,15 / 0,1  0,85)
Le nombre entier Semaine prend la valeur 0
Tant que p1 < p2 et Semaine ≤ 10 faire
    | P prend la valeur M × P
    | Semaine prend la valeur Semaine + 1
Fin Tant que
Si Semaine < 10
    | afficher : « le parfum Aurore sera préféré au parfum Boréale
    | après un nombre de semaines de campagne égal à : »
    | afficher Semaine
Sinon afficher : « durant les 10 premières semaines suivant le début de
la campagne, le parfum Aurore ne sera pas préféré au parfum Boréale ».
Fin si
```

4. a. Dans le nouveau cas envisagé, l'arbre de probabilités ci-contre décrit l'évolution des probabilités de choix de parfums des personnes interrogées la $(n + 1)$-ième semaine suivant le début de la campagne.



On en déduit que $P_{n+1} = 0{,}8 \times M \times P_n + 0{,}2 \times N$.

b. Il s'agit de calculer P_4 ; on le détermine de proche en proche en utilisant $P_0 = \begin{pmatrix} 0{,}2 \\ 0{,}8 \end{pmatrix}$ et la relation :

$P_{n+1} = 0{,}8 \times M \times P_n + 0{,}2 \times N$ (on peut utiliser la touche « REP » ou « ANS » de la calculatrice).

On trouve $P_4 \approx \begin{pmatrix} 0{,}50 \\ 0{,}50 \end{pmatrix}$.

Matrices carrées inversibles et applications

5

Une mesure de moutarde, plus une de genièvre et une de paprika font 13 euros ; cinq mesures de moutarde, plus une de genièvre et une de paprika font 16 euros ; trois mesures de moutarde, plus deux de genièvre et deux de paprika font 25 euros. Quel est le prix du genièvre ?

Le chapitre en bref

Réinvestir

- Les matrices
- Les opérations sur ces matrices

Explorer

- Les matrices inversibles et leurs applications : l'évolution d'un processus

Activités de recherche p. 124

Activités d'exploration

1 Un tour de passe-passe ▸ Algorithmique

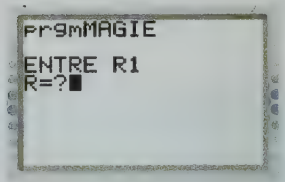
Explorer : Les notions de matrice unité et de matrice inverse.

Roxane propose à Lise : « Choisis deux nombres ; d'une part, au double du premier tu ajoutes cinq fois le second et, d'autre part, au premier tu ajoutes le triple du second.
Entre les deux résultats dans le programme que j'ai créé sur ma calculatrice et elle te redonnera tes nombres de départ. »
Lise répond : « Oui, ça marche ! Laisse-moi voir ton programme. »
Voici la description de l'algorithme écrit par Roxane :

```
Variables : x1, x2, r1, r2
Entrées : lire r1, r2
Traitement :   Affecter la valeur 3r1−5r2 à x1

               Affecter la valeur −r1+2r2 à x2

Sortie : Afficher x1 et x2.
```



1. Comme Lise, choisir deux nombres, faire les opérations demandées puis tester l'algorithme pour les nombres obtenus.

2. Soit les matrices colonnes $X = \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$ et $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.
   - **a.** Déterminer la matrice carrée A telle que $AX = R$.
   - **b.** Déterminer la matrice carrée B qui selon l'algorithme est telle que $BR = X$.
   - **c.** Calculer les produits matriciels $A \times B$ et $B \times A$.

3. Par quelles matrices multiplie-t-on successivement la matrice colonne X dans le déroulement de ce jeu. Quel est alors le résultat de ce produit ? L'algorithme proposé par Roxane est-il efficace ?

La notion rencontrée dans l'activité

On dit que A est une **matrice inversible** de taille n s'il existe une matrice B telle que :

$$A \times B = B \times A = \begin{pmatrix} 1 & 0 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 0 & 1 \end{pmatrix} = I_n,$$ où I_n est la matrice identité de taille n.

2 Un problème de dimensions ▸ Algorithmique

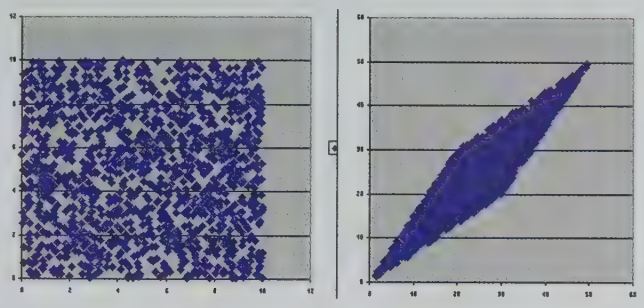
Réinvestir : La notion de matrice inverse.
Explorer : L'écriture matricielle d'un système linéaire.

Le plan est muni d'un repère orthonormé $(O ; \vec{i}, \vec{j})$.

Partie A. On considère une application qui à tout point M du plan de coordonnées $(x ; y)$ associe le point N de coordonnées $(3x + 2y ; 2x + 3y)$.

1 Choisir un point M du plan et chercher le point image N par cette application.

2 Par cette application, on souhaite observer l'image d'un carré.
À l'aide d'un logiciel de programmation ou d'un tableur, écrire un algorithme qui choisit un millier de fois un point au hasard dans un carré de côté 10 unités et affiche son point image par cette application.
Que constate-t-on ? Peut-on obtenir n'importe quel point du plan par cette application ?



3 **a.** Montrer qu'il existe un unique point M dont l'image par cette application est $N(4 ; 5)$. Donner ses coordonnées.
b. Pour un point quelconque $N(x' ; y')$ du plan, montrer qu'il existe un unique point M dont l'image par cette application est N. Donner ses coordonnées en fonction de x' et de y'.

4 **a.** Déterminer la matrice A telle que le système d'équations $\begin{cases} 3x+2y=x' \\ 2x+3y=y' \end{cases}$ soit équivalent à l'égalité $A\times\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} x' \\ y' \end{pmatrix}$.

b. Écrire le système linéaire donnant les coordonnées du point antécédent $M(x ; y)$ en fonction des coordonnées $(x' ; y')$ d'un point N.
Écrire la matrice B telle que ce système soit équivalent à l'égalité $\begin{pmatrix} x \\ y \end{pmatrix}=B\times\begin{pmatrix} x' \\ y' \end{pmatrix}$.

c. Que peut-on dire des matrices A et B ? Justifier le résultat.

Partie B. On considère maintenant une application qui à tout point M du plan de coordonnées $(x ; y)$ associe le point N de coordonnées $(3x + 2y ; 6x + 4y)$.

1 À l'aide d'un logiciel de programmation ou d'un tableur, écrire un algorithme qui choisit un millier de fois un point au hasard dans un carré de côté 10 unités et affiche son point image par cette application. Que constate-t-on ?
Peut-on obtenir n'importe quel point du plan par cette application ?

2 **a.** Montrer qu'il n'existe pas de point M dont l'image par cette application est $N(4 ; 5)$.

b. Déterminer la matrice A telle que le système d'équations $\begin{cases} 3x+2y=x' \\ 6x+4y=y' \end{cases}$ soit équivalent à l'égalité $A\times\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} x' \\ y' \end{pmatrix}$.

c. Montrer qu'il n'existe pas de matrice B telle que $B \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

La propriété rencontrée dans l'activité

Soit $AU = V$ l'écriture matricielle d'un système linéaire où A est une matrice carrée, U et V deux matrices colonnes.

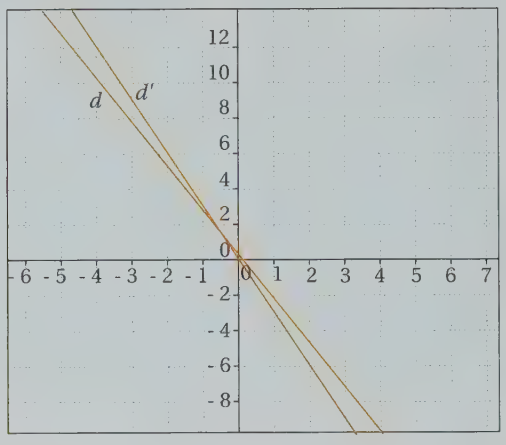
Si la matrice carrée A est inversible, alors le **système linéaire a une unique solution**. Cette solution est constituée des coefficients de l'unique matrice colonne égale au produit $A^{-1}V$.

3 Des droites sécantes et des matrices de taille 2 inversibles

Réinvestir : La notion de matrice inverse.
Explorer : Une condition nécessaire et suffisante pour qu'une matrice de taille 2 soit inversible.

1 Soit la matrice $A = \begin{pmatrix} 10 & 4 \\ 6 & 2 \end{pmatrix}$.

On cherche s'il existe une matrice $B = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$ telle que $A \times B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.



a. Montrer que le couple $(x ; y)$ correspond aux coordonnées d'un point situé sur deux droites du plan dont on donnera les équations cartésiennes.
b. Conclure sur l'existence et l'unicité de ce couple.
c. Reprendre le raisonnement pour le couple $(x' ; y')$.
d. Déterminer les valeurs de x, y, x' et y' en résolvant les systèmes d'équations préalablement obtenus.
e. Vérifier que $B \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2 Généralisation.
Soit la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

a. À l'aide de la question **1**, conjecturer une condition suffisante sur les coefficients a, b, c et d pour que la matrice A soit inversible.

b. Montrer que, si cette condition est vérifiée, la matrice $B = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est la matrice inverse de A.

c. Montrer dans le cas où cette condition n'est pas vérifiée qu'il est impossible de trouver une matrice inverse pour A.
Conclure.

La propriété rencontrée dans l'activité

Une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de taille 2 est inversible, si et seulement si :

$$ad - bc \neq 0.$$

Cours

A. Matrice inverse d'une matrice carrée

1 Matrice unité et matrice inverse

DÉFINITION

Soit n un entier naturel non-nul. On appelle **matrice unité de taille** (ou d'ordre) n, la matrice carrée de taille n dont les coefficients sont :

pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$: $a_{ij} = 0$ si $i \neq j$ et $a_{ij} = 1$ si $i = j$.

Ce que l'on peut traduire ainsi : tous les coefficients sont nuls exceptés ceux de la diagonale issue du coin en haut à gauche qui valent tous 1.

On note en général cette matrice $I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & \ddots & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$

PROPRIÉTÉ

Pour toute matrice carrée A de taille n, on a $A \times I_n = I_n \times A = A$.

DÉMONSTRATION

On note B la matrice unité I_n.

Pour tout entier i tel que $1 \leqslant i \leqslant n$ et tout entier j tel que $1 \leqslant j \leqslant n$, le coefficient situé à l'intersection de la ligne i et de la colonne j du produit $A \times I_n = A \times B$ est égal à :

$$a_{i1} \times b_{1j} + a_{i2} \times b_{2j} + a_{i3} \times b_{3j} + \dots + a_{in} \times b_{nj}$$

Or $b_{ij} = 0$ si $i \neq j$; donc cette somme ne contient que des termes nuls sauf le terme $a_{ij} \times b_{jj} = a_{ij} \times 1 = a_{ij}$. On a donc $A \times I_n = A$.

On procède de même pour démontrer que $I_n \times A = A$. ■

REMARQUE

Pour la multiplication de matrices, la matrice unité joue donc le même rôle que le nombre 1 pour la multiplication de nombres réels.

Par convention, pour toute matrice carrée A de taille n, on a $A^0 = I_n$.

DÉFINITION

Soit A une matrice carrée de taille n.

A est une **matrice inversible** s'il existe une matrice B telle que $A \times B = B \times A = I_n$.

Dans ce cas, on dit que la matrice B est l'**inverse** de la matrice A et on note $B = A^{-1}$.

PROPRIÉTÉ (ADMISE)

Pour montrer que la matrice A est inversible de matrice inverse B, il suffit de montrer que $A \times B = I_n$ ou de montrer que $B \times A = I_n$.

EXEMPLE

Soit les matrices $A = \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0{,}5 \\ 4{,}5 & 2{,}5 \end{pmatrix}$.

$$A \times B = \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 0{,}5 \\ 4{,}5 & 2{,}5 \end{pmatrix} = \begin{pmatrix} 10\times1-2\times4{,}5 & 10\times0{,}5-2\times2{,}5 \\ -18\times1+4\times4{,}5 & -18\times0{,}5+4\times2{,}5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Soit $A \times B = I_2$, donc B est la matrice inverse de A et $B = A^{-1}$.

PROPRIÉTÉ

Soit A une matrice inversible de taille n.
Pour toutes matrices M et N carrées ou colonnes de taille n, on a :

$$\boldsymbol{A \times M = N \Leftrightarrow M = A^{-1} \times N}$$

DÉMONSTRATION

Soit deux matrices M et N carrées ou colonnes de taille n.
Si $AM = N$ alors en multipliant les deux membres de chaque égalité à gauche par A^{-1}, on en déduit que $A^{-1}(AM) = A^{-1}N$.
À l'aide des propriétés du calcul matriciel, on obtient :
$(A^{-1}A)M = A^{-1}N$, donc $I_n M = M = A^{-1}N$.
Réciproquement, si $M = A^{-1}N$, en multipliant chaque membre de l'égalité à gauche par A et en appliquant les mêmes propriétés, on obtient $AM = N$. ■

PROPRIÉTÉ

Soit A une matrice inversible.
Pour tout réel $k \neq 0$, la matrice kA est inversible et sa matrice inverse est $\frac{1}{k}A^{-1}$.

DÉMONSTRATION

D'après une des propriétés précédentes, pour la matrice carrée inversible A de taille n, il suffit de vérifier que le produit $kA \times \frac{1}{k}A^{-1}$ est égal à I_n.

Or, à l'aide des propriétés du calcul matriciel, on obtient :

$$kA \times \frac{1}{k}A^{-1} = (k \times \frac{1}{k})\, A \times A^{-1} = 1I_n = I_n.$$ ■

▶ Savoir-faire 1
Résoudre une équation matricielle à l'aide de l'inverse d'une matrice, p. 116

2 Existence de l'inverse d'une matrice de taille 2

PROPRIÉTÉ

Soit M une matrice carrée de taille 2, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

M est **inversible** si, et seulement si, $\boldsymbol{ad - bc \neq 0}$.

DÉMONSTRATION

Cette condition est une conséquence du théorème vu en classe de 1re sur la colinéarité de deux vecteurs et de l'interprétation géométrique des solutions d'un système de 2 équations à 2 inconnues.
Les étapes de la démonstration sont proposées dans **l'activité d'exploration 3.** ■

▶ Savoir-faire 2
Calcul de l'inverse d'une matrice carrée de taille 2, p. 116

B. Application aux systèmes linéaires

EXEMPLE

Soit le système linéaire d'inconnues x et y : (S) $\begin{cases} 10x+4y=3 \\ 6x+2y=-5 \end{cases}$.

On pose $A=\begin{pmatrix} 10 & 4 \\ 6 & 2 \end{pmatrix}$, $U=\begin{pmatrix} x \\ y \end{pmatrix}$ et $V=\begin{pmatrix} 3 \\ -5 \end{pmatrix}$.

Par définition de la multiplication matricielle, la matrice AU est égale à la matrice colonne $\begin{pmatrix} 10x+4y \\ 6x+2y \end{pmatrix}$.

Le système (S) peut s'écrire sous la forme $AU = V$ par égalité des matrices colonnes.

REMARQUE

On montre de manière analogue que tout système linéaire de n équations à n inconnues peut s'écrire sous la forme matricielle : $\boldsymbol{AU = V}$ où A est la matrice carrée de taille n des coefficients du système, U est la matrice colonne des inconnues et V est la matrice colonne formée par les seconds membres des équations.

THÉORÈME

Soit $AU = V$ l'écriture matricielle d'un système linéaire.

Si la matrice carrée A est inversible, alors **le système a une unique solution** égale à la **matrice colonne solution** $A^{-1}V$.

DÉMONSTRATION

À l'aide de la propriété démontrée au paragraphe **A.** 1, dans le cas où A est inversible :

$$AU = V \Leftrightarrow U = A^{-1}V.$$

REMARQUE

Ce théorème est complété par la propriété suivante qui, dans le cas des systèmes linéaires de deux équations à deux inconnues, est une conséquence de l'interprétation graphique des solutions (voir **activité d'exploration 3**).

PROPRIÉTÉ (ADMISE)

Soit $AU = V$ l'écriture matricielle d'un système linéaire.

Si la matrice carrée $\boldsymbol{A}$ **n'est pas inversible**, alors :

- soit le système a une infinité de solutions,
- soit le système n'a pas de solution.

NOTE

Dans le cas des systèmes linéaires de trois équations à trois inconnues, voir aussi le problème 49.

EXEMPLE (SUITE)

Soit le même système linéaire d'inconnues x et y : (S) $\begin{cases} 10x+4y=3 \\ 6x+2y=-5 \end{cases}$.

Son écriture matricielle est $AU = V$ avec $A=\begin{pmatrix} 10 & 4 \\ 6 & 2 \end{pmatrix}$, $U=\begin{pmatrix} x \\ y \end{pmatrix}$ et $V=\begin{pmatrix} 3 \\ -5 \end{pmatrix}$.

A est inversible et $A^{-1}=\begin{pmatrix} -0{,}5 & 1 \\ 1{,}5 & -2{,}5 \end{pmatrix}$, donc $U=A^{-1}V=\begin{pmatrix} -6{,}5 \\ 17 \end{pmatrix}$.

Le système a donc pour unique couple solution $(x\,;y) = (0{,}5\,;1)$.

▶ Savoir-faire 3
À l'aide du calcul matriciel, résoudre un système linéaire, p. 117

Savoir-faire

Savoir-faire 1 — Résoudre une équation matricielle à l'aide de l'inverse d'une matrice

ÉNONCÉ

a. Soit $A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ et $B = \begin{pmatrix} -2{,}5 & 1{,}5 \\ 2 & -1 \end{pmatrix}$. Montrer que B est la matrice inverse de la matrice A.

b. Soit $M = \begin{pmatrix} 3 & 3 \\ 4 & 6 \end{pmatrix}$ et $N = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Déterminer la matrice colonne X vérifiant $MX = X + N$.

SOLUTION

a. $A \times B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ ou $B \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$;

donc B est la matrice inverse de A : $B = A^{-1}$.

b. À l'aide des propriétés du calcul matriciel :

$MX = X + N \Leftrightarrow MX - X = N$

$\Leftrightarrow (M - I_2)X = N$

$\Leftrightarrow AX = N$ puisque $M - I_2 = A$.

Or A est inversible d'inverse la matrice B, donc $AX = N \Leftrightarrow X = BN$.

Après le calcul de BN, on obtient la solution $X = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

Exercices 1 et 2 p. 119 et 17 et 18 p. 120

MÉTHODE

a. Une des égalités $A \times B = I_2$ ou $B \times A = I_2$ suffit pour prouver que B est l'inverse de A.

L'autre égalité est alors vraie aussi.

b. On résout l'équation en utilisant les règles de calcul matriciel, un peu comme une équation dans les nombres réels, mais en prenant garde à l'ordre des facteurs pour la multiplication des matrices.

Savoir-faire 2 — Calcul de l'inverse d'une matrice carrée de taille 2

ÉNONCÉ

Soit la matrice carrée $A = \begin{pmatrix} 5 & 1 \\ 3 & 4 \end{pmatrix}$.

a. Montrer que A est une matrice inversible.

b. Déterminer la matrice inverse de A à la main.

c. Déterminer la matrice inverse de A à l'aide de la calculatrice.

SOLUTION

a. $5 \times 4 - 1 \times 3 \neq 0$, les coefficients des deux lignes de cette matrice ne sont pas proportionnels, la matrice est donc inversible.

b. Soit $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice inverse de la matrice A.

Les coefficients a et c sont solutions du système : $\begin{cases} 5a + c = 1 \\ 3a + 4c = 0 \end{cases}$.

Par élimination : si on soustrait 3 fois la première ligne du système à 5 fois la seconde, on obtient $c = -\dfrac{3}{17}$, puis grâce à la seconde ligne du système : $a = -\dfrac{4}{3}c$, donc $a = \dfrac{4}{17}$.

MÉTHODE

a. On utilise la propriété :

M est inversible si, et seulement si, $ad - bc \neq 0$.

b. Les deux systèmes sont obtenus grâce aux quatre égalités conséquences du produit $A \times B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(On peut aussi utiliser les quatre égalités liées au produit $B \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ qui donnent deux autres systèmes.)

c. Pour déterminer l'inverse d'une matrice A à l'aide de la calculatrice :

- on entre la matrice A (voir Savoir-Faire **2** du chapitre 4) et on quitte le mode matrice ;
- on sélectionne le nom de la matrice A, puis on utilise la touche x^{-1} de la calculatrice pour obtenir l'inverse ;
- on met éventuellement le résultat sous forme fractionnaire.

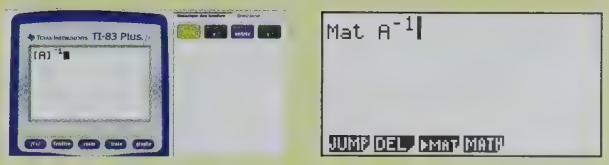
De même, b et d étant solutions du système $\begin{cases} 5b+d=0 \\ 3b+4d=1 \end{cases}$ on trouve $b=-\frac{1}{17}$ et $d=\frac{5}{17}$.

c. On trouve bien comme matrice inverse :

$$B=\begin{pmatrix} \frac{4}{17} & -\frac{1}{17} \\ -\frac{3}{17} & \frac{5}{17} \end{pmatrix}.$$

Exercices 10 à 12 p. 119

T.I **CASIO**



REMARQUE Dans le cas où la matrice n'est pas inversible, la calculatrice affiche un message d'erreur le signalant :
- sur TI : ERR : SINGULAR MAT
- sur Casio : Ma ERROR

Savoir-faire 3 — Résoudre un système linéaire à l'aide du calcul matriciel

ÉNONCÉ L'espace est rapporté à un repère. Les points A, B et C ont pour coordonnées :

A(1 ; −2 ; 4), B(−2 ; −6 ; 5) et C(−4 ; 0 ; −3).

a. Montrer que ces trois points définissent un plan.

b. On suppose que ce plan ne contient pas l'origine du repère, déterminer une équation cartésienne de ce plan.

SOLUTION

a. Les vecteurs $\overrightarrow{AB}$ (−3 ; −4 ; 1) et $\overrightarrow{BC}$ (−2 ; 6 ; −8) ne sont pas colinéaires puisque leurs coordonnées ne sont pas proportionnelles ; ainsi les points A, B et C ne sont pas alignés et définissent donc un plan.

b. Une équation cartésienne du plan (ABC) est de la forme $ax + by + cz + 1 = 0$ où a, b et c sont solutions du système $\begin{cases} a-2b+4c+1=0 \\ -2a-6b+5c+1=0 \\ -4a-3c+1=0 \end{cases}$.

L'écriture matricielle de ce système est $AX = B$ où $A=\begin{pmatrix} 1 & -2 & 4 \\ -2 & -6 & 5 \\ -4 & 0 & -3 \end{pmatrix}$, $X=\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ et $B=\begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$.

À l'aide de la calculatrice (ou d'un autre outil), on trouve que A est une matrice inversible d'inverse :

$$A^{-1}=\begin{pmatrix} -\frac{9}{13} & \frac{3}{13} & -\frac{7}{13} \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ \frac{12}{13} & -\frac{4}{13} & \frac{5}{13} \end{pmatrix}.$$

On en déduit que $X=A^{-1}\times B=\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$.

Une équation cartésienne du plan (ABC) est donc $x-y-z+1=0$.

Exercices 26 à 28 p. 121

MÉTHODE

Un point appartient au plan si et seulement si ses coordonnées vérifient l'équation du plan.

Le coefficient constant de l'équation cartésienne du plan est non nul puisque l'origine O n'appartient pas au plan donc, quitte à diviser les 2 membres de l'équation par ce coefficient non nul, on peut se ramener à une équation cartésienne de la forme $ax + by + cz + 1 = 0$.

On écrit le système en utilisant le fait que A, B et C sont trois points du plan.

L'écriture matricielle du système nécessite de transformer les équations en soustrayant à chaque membre le coefficient constant.

Comme la solution du système est donnée par le produit $A^{-1} \times B$, on peut directement demander ce produit à la calculatrice.

REMARQUE : La calculatrice fournit une matrice inverse pour A. On utilise ce résultat pour en déduire que A est inversible et que le système a un unique triplet solution.

(Des arguments pour justifier que la matrice est inversible avant de chercher à déterminer son inverse sont abordés après la classe de terminale.)

Savoir-faire 4 — *Utiliser une décomposition particulière pour le calcul de puissances d'une matrice*

ÉNONCÉ Soit la matrice $A = \begin{pmatrix} 6{,}25 & -9 \\ 4{,}5 & -6{,}5 \end{pmatrix}$.

a. À l'aide d'une calculatrice, vérifier que la matrice A est égale au produit des matrices $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 0{,}25 & 0 \\ 0 & -0{,}5 \end{pmatrix}$ et où P désigne la matrice inversible $P = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$.

b. En déduire les coefficients de la matrice A^n pour tout $n \geqslant 0$.

SOLUTION

a. À l'aide de la calculatrice, on obtient $P^{-1} = \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix}$, et on vérifie également que $P \times D \times P^{-1}$ donne la matrice $A = \begin{pmatrix} 6{,}25 & -9 \\ 4{,}5 & -6{,}5 \end{pmatrix}$.

b. On démontre la propriété « $A^n = P \times \begin{pmatrix} 0{,}25^n & 0 \\ 0 & (-0{,}5)^n \end{pmatrix} \times P^{-1}$ » par récurrence sur $n \geqslant 0$:

$P \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times P^{-1} = I_2 = A^0$, donc la propriété est vraie au rang $n = 0$.

On suppose la propriété vraie au rang k, c'est-à-dire « $A^k = P \times \begin{pmatrix} 0{,}25^k & 0 \\ 0 & (-0{,}5)^k \end{pmatrix} \times P^{-1}$ », alors au rang $k+1$:

$$A^{k+1} = A \times A^k = P \times D \times P^{-1} \times P \times \begin{pmatrix} 0{,}25^k & 0 \\ 0 & (-0{,}5)^k \end{pmatrix} \times P^{-1}$$

$$= P \times D \times I_2 \times \begin{pmatrix} 0{,}25^k & 0 \\ 0 & (-0{,}5)^k \end{pmatrix} \times P^{-1}$$

$$= P \times \begin{pmatrix} 0{,}25 & 0 \\ 0 & -0{,}5 \end{pmatrix} \times \begin{pmatrix} 0{,}25^k & 0 \\ 0 & (-0{,}5)^k \end{pmatrix} \times P^{-1}$$

$= P \times \begin{pmatrix} 0{,}25^{k+1} & 0 \\ 0 & (-0{,}5)^{k+1} \end{pmatrix} \times P^{-1}$. La propriété est encore vraie au rang $k+1$.

On peut affirmer que la propriété « $A^n = P \times \begin{pmatrix} 0{,}25^n & 0 \\ 0 & (-0{,}5)^n \end{pmatrix} \times P^{-1}$ » est vraie pour tout $n \geqslant 0$.

On en déduit les coefficients de la matrice A^n pour tout $n \geqslant 0$:

$$A^n = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 0{,}25^n & 0 \\ 0 & (-0{,}5)^n \end{pmatrix} \times \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix} ; \text{ donc } A^n = \begin{pmatrix} 9\times 0{,}25^n - 8\times(-0{,}5)^n & -12\times 0{,}25^n + 12\times(-0{,}5)^n \\ 6\times 0{,}25^n - 6\times(-0{,}5)^n & -8\times 0{,}25^n + 9\times(-0{,}5)^n \end{pmatrix}.$$

MÉTHODE

On vérifie grâce à la calculatrice que le produit $P \times D \times P^{-1}$ est bien égal à la matrice A.

Cette décomposition présente un avantage certain pour le calcul de A^n comme on le voit dans la démonstration par récurrence : les produits $P^{-1} \times P$ donnent la matrice unité et les produits de la matrice diagonale D par elle-même s'effectuent très simplement.

Une matrice que l'on peut décomposer en un tel produit est dite **diagonalisable**.

Exercices 22 à 24 p. 120

Exercices d'application

Matrices inverses

Pour les exercices 1 à 4

Montrer que la matrice B est l'inverse de la matrice A.

1 **a.** $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$ et $B = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$.

b. $A = \begin{pmatrix} -\frac{1}{2} & \frac{1}{4} \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}$.

Savoir-faire 1, p. 115

2 **a.** $A = \begin{pmatrix} 5 & -6 \\ 3 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -3 \\ 1{,}5 & -2{,}5 \end{pmatrix}$

b. $A = \begin{pmatrix} -1 & 1 \\ \frac{4}{3} & -\frac{1}{3} \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{3} & 1 \\ \frac{4}{3} & 1 \end{pmatrix}$.

3 $A = \begin{pmatrix} -\frac{2}{3} & \frac{1}{3} & 0 \\ -\frac{2}{3} & \frac{4}{3} & -3 \\ 1 & -1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 4 & 6 \\ 2 & 1 & 2 \end{pmatrix}$.

4 $A = \begin{pmatrix} 2 & 4 & 5 \\ -1 & 2 & 3 \\ 2 & -4 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{4} & -\frac{2}{5} & \frac{1}{20} \\ \frac{1}{8} & -\frac{3}{10} & -\frac{11}{40} \\ 0 & \frac{2}{5} & \frac{1}{5} \end{pmatrix}$.

5 Montrer que les matrices A et B sont inverses l'une de l'autre :

$A = \begin{pmatrix} a & a+1 \\ a-1 & a \end{pmatrix}$ et $B = \begin{pmatrix} a & -1-a \\ 1-a & a \end{pmatrix}$.

6 **a.** Vérifier que la matrice $\begin{pmatrix} 2 & -0{,}5 \\ 4 & 3 \end{pmatrix}$ admet pour inverse la matrice $\begin{pmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{2} & \frac{1}{4} \end{pmatrix}$.

b. Déterminer sans calculs supplémentaires la matrice inverse de la matrice $\begin{pmatrix} 4 & -1 \\ 8 & 6 \end{pmatrix}$.

7 **1.** Vérifier que la matrice $\begin{pmatrix} 4 & 6 & 2 \\ 0 & 10 & 4 \\ 2 & 0 & 0 \end{pmatrix}$ admet pour inverse la matrice $\begin{pmatrix} 0 & 0 & 0{,}5 \\ 1 & -0{,}5 & -2 \\ -2{,}5 & 1{,}5 & 5 \end{pmatrix}$.

2. Déterminer sans calcul la matrice inverse de chaque matrice.

a. $\begin{pmatrix} 2 & 3 & 1 \\ 0 & 5 & 2 \\ 1 & 0 & 0 \end{pmatrix}$ **b.** $\begin{pmatrix} 0 & 0 & 2 \\ 4 & -2 & -8 \\ -10 & 6 & 20 \end{pmatrix}$ **c.** $\begin{pmatrix} 2 & 3 & 1 \\ 0 & 2{,}5 & 1 \\ 4 & 0 & 0 \end{pmatrix}$.

8 Si A et B sont deux matrices inverses l'une de l'autre, A^2 est-elle la matrice inverse de B^2 ?

9 Si A et B sont deux matrices carrées de même taille inversibles, d'inverses respectives A^{-1} et B^{-1}, déterminer :

a. la matrice inverse de la matrice $A \times B$.

b. la matrice inverse de la matrice $B \times A$.

Pour les exercices 10 à 12

Pour chacune des questions :

a. Déterminer si la matrice A est inversible.

b. Si elle est inversible, déterminer son inverse sans utiliser la calculatrice.

c. Vérifier le résultat à l'aide de la calculatrice.

10 **a.** $A = \begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix}$ **b.** $A = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$

Savoir-faire 2, p. 116

11 **a.** $A = \begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}$ **b.** $A = \begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}$

12 **a.** $A = \begin{pmatrix} 2 & -3 \\ -0{,}5 & 0{,}75 \end{pmatrix}$ **b.** $A = \begin{pmatrix} 7 & 4 \\ 1{,}5 & 1 \end{pmatrix}$

13 Déterminer à la main la matrice inverse de la matrice $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, puis vérifier à l'aide d'une calculatrice.

14 Déterminer à la main la matrice inverse de la matrice $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ puis vérifier à l'aide d'une calculatrice.

15 Démontrer que la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 3 & 5 \end{pmatrix}$ n'est pas inversible.

16 Démontrer que la matrice $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 1 \\ 2 & 4 & 5 \end{pmatrix}$ n'est pas inversible.

Calcul matriciel à l'aide des matrices inverses

POUR LES EXERCICES 17 À 19

Dans chaque cas, déterminer la matrice colonne X vérifiant l'équation matricielle proposée. (On justifiera l'existence et l'unicité de la solution.)

17 **a.** $AX = B$ où $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$.

b. $AX = B$ où $A = \begin{pmatrix} -1 & 5 \\ 6 & 8 \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{3} \end{pmatrix}$.

▸ Savoir-faire 1, p. 116

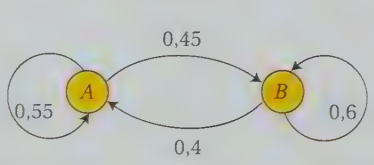
18 **a.** $AX = X + B$ où $A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 0,5 \\ -1 \end{pmatrix}$.

b. $X = AX + B$ où $A = \begin{pmatrix} 3 & 7 \\ -1 & -3 \end{pmatrix}$ et $B = \begin{pmatrix} 11 \\ 8 \end{pmatrix}$.

19 **a.** $A^2 \times X = B$ où $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 3,5 \\ -12 \end{pmatrix}$.

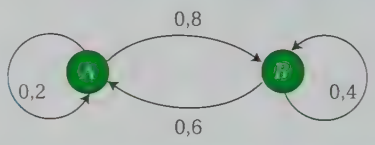
b. $A^2 \times X = X + 2B$ où $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{3} \end{pmatrix}$.

20 On considère une marche aléatoire sur le graphe ci-dessous :



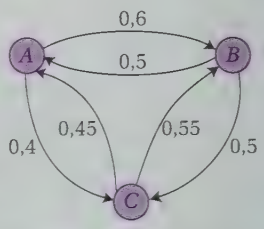
a. Écrire la matrice de transition d'un état au suivant.
b. Donner la matrice colonne de l'état initial pour lequel les probabilités d'être situé sur chaque sommet après 1 pas sont équiréparties.
c. Existe-t-il un état initial pour lequel les probabilités d'être situé sur chaque sommet après 2 pas sont équiréparties ? Justifier.

21 On considère une marche aléatoire sur le graphe ci-dessous :



Donner la matrice colonne de l'état initial pour lequel les probabilités d'être situé sur chaque sommet après 2 pas sont $\begin{pmatrix} \frac{2}{5} \\ \frac{3}{5} \end{pmatrix}$.

22 On considère une marche aléatoire sur le graphe ci-contre. .



Donner :
a. La matrice de transition d'un état au suivant.
b. La matrice colonne de l'état initial pour lequel les probabilités d'être situé sur chaque sommet après 2 pas sont : $\begin{pmatrix} 0,325 \\ 0,31125 \\ 0,36375 \end{pmatrix}$.
c. La matrice colonne de l'état initial pour lequel les probabilités d'être situé sur chaque sommet après 4 pas sont équiréparties. Justifier.

23 Soit la matrice $A = \begin{pmatrix} 7 & -4 \\ 8 & -5 \end{pmatrix}$.

a. À l'aide d'une calculatrice, vérifier que la matrice A est égale au produit des matrices : $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}$ et où P désigne la matrice inversible $P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.
b. En déduire les coefficients de A^n pour tout $n \geqslant 0$.

▸ Savoir-faire 4, p. 118

24 Soit la matrice $A = \begin{pmatrix} 3 & -6 & 4 \\ 2 & -7 & 5 \\ 4 & -18 & 12 \end{pmatrix}$.

a. À l'aide d'une calculatrice, vérifier que la matrice A est égale au produit des matrices : $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ et où P désigne la matrice inversible $P = \begin{pmatrix} -1 & 2 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix}$.
b. En déduire les coefficients de A^n pour tout $n \geqslant 0$.

25 Soit une matrice A égale au produit des matrices : $P \times D \times P^{-1}$ où D désigne la matrice diagonale : $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ et où P désigne une matrice inversible.

a. Montrer que si $\lambda \neq 0$ et $\mu \neq 0$, la matrice est inversible.

b. Montrer que si $\lambda = 0$ ou $\mu = 0$, la matrice A n'est pas inversible.

Applications aux systèmes

Pour les exercices 26 à 28

a. Donner l'écriture matricielle $AU = V$ du système.
b. Déterminer l'inverse de A à l'aide de la calculatrice.
c. En déduire la solution du système.

26 **a.** $\begin{cases} 2x + 4y = 5 \\ \frac{1}{2}x + 3y = -8 \end{cases}$ **b.** $\begin{cases} -2x - y = 4 \\ 2y + 5x = -3 \end{cases}$

Savoir-faire 3, p. 117

27 **a.** $\begin{cases} 3x + 5y + 3z = 7 \\ 2x + 5y + 8z = -1 \\ x + 8y + 5z = 4 \end{cases}$ **b.** $\begin{cases} 14 - y + x = 0 \\ 12y = 7x + 3z \\ 11x - 19y = 8 - 5z \end{cases}$

28 $\begin{cases} 2a + 3b + 5c - 4d = 1 \\ a + 2b + 2c + d = 2 \\ -6a + b + 5c + 2d + 3 = 0 \\ a + 3b + 4c + 2d = 0{,}5 \end{cases}$

Pour les exercices 29 à 31

Résoudre le système à la main, puis à l'aide d'un calcul matriciel à la calculatrice.

29 $\begin{cases} 5x = 7 + y \\ 2{,}5x - y = 2 \end{cases}$

30 $\begin{cases} x + y + z = 6 \\ x = 1 - y \\ 5x + 2y - 3 = 0 \end{cases}$

31 $\begin{cases} x + y = 3 \\ y + 2z = 5 \\ x - t = 6 \\ z + t = 2 \end{cases}$

32 Louna veut calculer sa moyenne à l'aide des trois notes qu'elle a obtenues aux trois devoirs du trimestre. Elle remarque que :

- Si le professeur affecte le coefficient 1 à tous les devoirs, sa moyenne sera de 11.
- Mais si le professeur décide d'affecter un coefficient 2 au premier devoir sa moyenne sera de 11,25.
- En revanche, s'il décide d'affecter un coefficient 2 plutôt au deuxième devoir, sa moyenne devient 10,5.

Quelles sont les notes de Louna ce trimestre ?

33 **Le problème de Chiu-chang Suan-shu**

« Trois gerbes d'une bonne récolte, deux gerbes d'une récolte médiocre, et une gerbe d'une mauvaise récolte sont vendues pour 39 Dou.
Deux gerbes d'une bonne, trois d'une médiocre et une d'une mauvaise sont vendues pour 34 Dou.
Enfin une bonne gerbe, deux médiocres, et trois mauvaises sont vendues pour 26 Dou.

Quel est le prix reçu pour chaque gerbe de bonne récolte, chaque gerbe de récolte médiocre, et chaque gerbe d'une mauvaise récolte ? »

Ce problème et sa résolution, présentés dans un ouvrage chinois du 1er siècle avant J.-C., constituent d'une certaine façon la première apparition de l'écriture d'un système sous forme matricielle.

34 Dans un repère de l'espace, montrer que les points A(1 ; −2 ; 4), B(−2 ; −6 ; 5) et C(−4 ; 0 ; −3) définissent un plan.
Déterminer une équation cartésienne de ce plan de la forme $1x + by + cz + d = 0$.

35 On donne la matrice $A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}$.

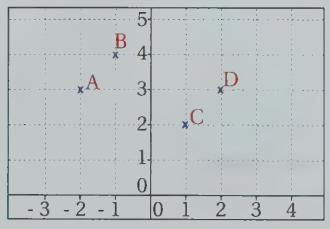
1. À l'aide de la calculatrice, donner la matrice inverse de A en écrivant les coefficients sous forme fractionnaire.

2. Dans un repère de l'espace, on donne trois plans $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ d'équations respectives :

$$\mathcal{P} : x + 2y + z - 4 = 0,$$
$$\mathcal{Q} : 2x + 3y + 4z - 2 = 0$$
$$\text{et } \mathcal{R} : 3x + 4y + z + 8 = 0.$$

Quelle est l'intersection de ces trois plans ?

36 Existe-t-il une fonction polynôme de degré 3 dont la courbe représentative passe par les points A, B, C et D du repère ci-dessous ?



37 Déterminer une fonction polynôme de degré 3 qui admet un maximum local égal à 15 en $x = -1$ et un minimum local égal à −12 en $x = 2$.

Exercices d'approfondissement

38 Une matrice triangulaire supérieure

1. Soit la matrice $A = \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix}$ où a désigne un nombre réel.

a. Montrer que $A = I - aN$, où I désigne la matrice unité de taille 3 et N, est une matrice carrée de taille 3 telle que N^3 a tous ses coefficients nuls (on peut noter $N^3 = 0$).

b. Montrer que la matrice A est inversible d'inverse $I + aN + a^2 N^2$.

2. Soit la matrice $B = \begin{pmatrix} 1 & b & 0 & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix}$ où b désigne un nombre réel.

Montrer que B est inversible et déterminer sa matrice inverse.

39 À la recherche d'une matrice inverse

D'après un sujet de BTS

On considère la matrice $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. La matrice I désigne la matrice unité de taille 3 et la matrice O désigne la matrice carrée de taille 3 dont tous les coefficients sont nuls.

1. Calculer A^2 et A^3. En déduire A^n pour tout entier $n > 3$.

2. À tout nombre réel x, on associe la matrice notée $M(x)$ où $M(x) = I + xA + \frac{x^2}{2} A^2$

a. Déterminer $M(0)$ et $B = M(4)$.

b. Pour tous nombres réels x et y, montrer que $M(x + y) = M(x) \times M(y)$.

3. Écrire les coefficients de la matrice $M(x)$ en fonction de x.

4. a. Déterminer le nombre réel x' tel que $M(x) \times M(x') = I$.

b. Montrer que la matrice B est inversible et donner sa matrice inverse.

40 Le bon itinéraire

Pour aller travailler le matin, Nino prend l'itinéraire A ou l'itinéraire B.

S'il rencontre des bouchons sur l'itinéraire choisi, il change d'itinéraire le lendemain.

Les statistiques de Bison futé font apparaître que l'itinéraire A est encombré avec la probabilité 1/3 et l'itinéraire B avec la probabilité 1/4.

a. Si Nino prend l'itinéraire A le lundi, avec quelle probabilité prend-il ce même itinéraire le vendredi qui suit ?

b. S'il y a équiprobabilité dans le choix de l'itinéraire pour Nino le mercredi, quelle est la probabilité qu'il ait choisi l'itinéraire B le lundi qui précédait ?

41 Un modèle de production agricole

Trois exploitations agricoles, notées R, S et T, produisent respectivement des radis, des salades et des tomates.

Une partie de chaque production est consommée dans les trois exploitations, le reste est disponible pour la vente dans une coopérative locale. Plus précisément :

- 10 % de la production de radis est consommée par l'exploitation R, 10 % de cette même production est consommée par l'exploitation S et également 10 % est consommée par l'exploitation T.
- 5 % de la production de salades est consommée par l'exploitation R, 10 % de cette même production est consommée par l'exploitation S et 5 % est consommée par l'exploitation T.
- Enfin, 5 % de la production de tomates est consommée par l'exploitation R, 10 % de cette même production est consommée par l'exploitation S et 5 % est consommée par l'exploitation T.

On note $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ la matrice colonne des productions, exprimées en kg par semaine, des trois légumes.

1. Montrer que la matrice colonne donnant les consommations pour chacun des trois légumes dans les exploitations est égale à AX, où A est une matrice carrée l'on précisera.

2. Si la production des trois légumes est $X = \begin{pmatrix} 150 \\ 190 \\ 150 \end{pmatrix}$, calculer la matrice colonne Y des quantités de chaque légume disponibles pour la vente à la coopérative.

3. Si les quantités de légumes disponibles pour la vente à la coopérative doivent être $\begin{pmatrix} 93 \\ 98 \\ 133 \end{pmatrix}$, calculer la production nécessaire des trois légumes X.

42 Les dimensions d'une boîte

Les diagonales des trois faces rectangulaires d'une boîte parallélépipédique mesurent 16 cm ; 33 cm et 35 cm.

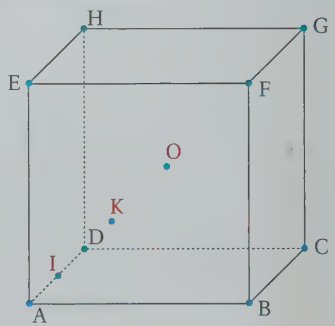
Retrouver les dimensions exactes de la boîte.

43 Points coplanaires

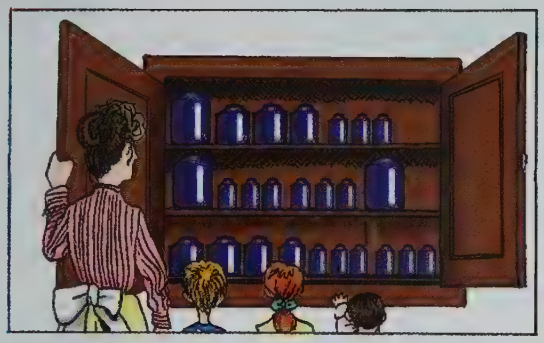
ABCDEFGH est un cube de centre O.

On note I le milieu de [AD] et K le milieu de [OI].

Montrer que K est un point du plan (BDE).



44 Un casse-tête mathématique de Sam Loyd



Mrs. Hubbard has invented a clever system for keeping tabs on her blackberry jam. She filled twenty-five jars and arranged the three sizes so as to have twenty quarts on each shelf.
Can you guess her secret so as to tell how much one of the big jars contains?
D'après Samuel Loyd (1841-1911), *compositeur américain de casse-têtes numériques et logiques.*

REMARQUE
Un quart US pour la mesure des liquides est un quart de gallon (unité pour les liquides), soit 0,946 352 946 ℓ.

45 Puissances et inverse. *D'après un sujet de BTS*

Soit la matrice $M = \begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}$.

1. Calculer M^2 à la main.

2. Déterminer les réels a et b tels que $M^2 = aM + bI$ où I désigne la matrice unité de taille 3.

3. Exprimer alors M^3 en fonction de M et I et en déduire les coefficients de la matrice M^3.

4. Déduire l'égalité $I = \frac{1}{2}M \times (3I - M)$ de ce qui précède. Montrer alors que M est inversible et déterminer sa matrice inverse.

46 Évolution des proportions

Dans une réaction chimique impliquant deux composés A et B, on sait qu'à chaque minute, 60 % du composé A ne réagit pas, le reste se transformant en B, tandis que seul 30 % du composé B se transforme en A. Aucun autre composé n'est produit lors de la réaction.
On considère deux suites de nombres réels (u_n) et (v_n) donnant les proportions des composés n minutes après le début de la réaction (n entier positif).
On note P_n la matrice colonne égale à $\begin{pmatrix} u_n \\ v_n \end{pmatrix}$.

1. Montrer que $P_{n+1} = MP_n$ où M est une matrice carré d'ordre 2 que l'on explicitera. En déduire que $P_n = M^n P_0$.

2. a. Montrer que la matrice M est inversible, donner son inverse M^{-1}.

b. Après 3 minutes d'expérience, un dosage fait apparaître que la proportion de composé A est 42 %.
Retrouver les proportions initiales de chaque composé en début de réaction.

3. a. Vérifier que $M^2 - M = 0{,}3(M - I)$ où I désigne la matrice unité de taille 2. En déduire que, pour tout $n \geqslant 0$:
$$M^{n+1} - M^n = 0{,}3^n(M - I).$$
(On pourra utiliser un raisonnement par récurrence.)
b. Calculer M^n en fonction de n et en déduire le terme général des suites (u_n) et (v_n) en fonction de n, u_0 et v_0.

47 Équation de plan

L'espace est rapporté à un repère.
Soit les points A(1 ; −2 ; 4), B(−2 ; −6 ; 5) et C(−4 ; 0 ; −3).

1. Montrer que les trois points définissent un plan.

2. Démontrer alors que les points O, A, B et C ne sont pas coplanaires.

3. En déduire qu'une équation cartésienne du plan (ABC) est de la forme $ax + by + cz + 1 = 0$ où a, b et c sont trois nombres réels. Déterminer cette équation.

48 Vrai ou Faux ?

On considère les populations, exprimées en milliers d'habitants, de trois villes A, B et C d'un pays. On suppose que chaque année, un habitant de ces trois villes reste dans sa ville ou déménage dans une des deux autres.
La matrice $M = \begin{pmatrix} 0{,}9 & 0{,}1 & 0{,}05 \\ 0{,}05 & 0{,}8 & 0{,}1 \\ 0{,}05 & 0{,}1 & 0{,}85 \end{pmatrix}$ donne les probabilités de transition des populations d'une ville à l'autre chaque année.
Répondre par *Vrai* ou *Faux* aux affirmations. Justifier.

1. D'une année à l'autre, 10 % de la population de la ville A déménage dans la ville B.

2. Si en 2000 la matrice colonne de répartition des populations était $\begin{pmatrix} 50 \\ 50 \\ 50 \end{pmatrix}$, en 2005 il y aura environ 58 000 habitants dans la ville C.

3. Si en 2004, la population est équirépartie entre les 3 villes, alors en 2000 la population de la ville B était moins du double de la population de la ville C.

4. On suppose qu'à ces mouvements de populations se rajoutent chaque année des nouveaux arrivants représentés, en milliers, par la matrice colonne $\begin{pmatrix} 5{,}3 \\ 2{,}2 \\ 1 \end{pmatrix}$. Si la matrice colonne de la population en 2002 est $\begin{pmatrix} 50 \\ 50 \\ 50 \end{pmatrix}$, c'est que la population de la ville A en 2000 était d'environ 31 000 habitants.

Activités de recherche et résolution de problèmes

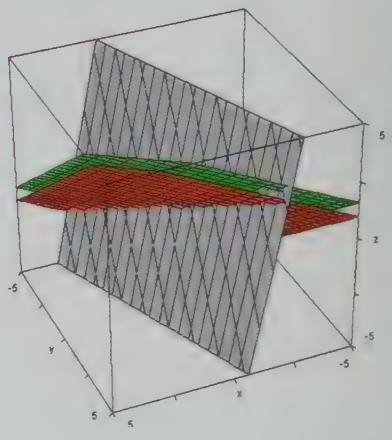
Travaux pratiques utilisant l'outil informatique

Problèmes de recherche

49 Interprétation géométrique d'un système de 3 équations à 3 inconnues

1 Soit (S) le système linéaire d'inconnues x, y et z :

$$(S)\begin{cases}2x+3y-4z=1\\4x+6y-8z=-3\\5x+2y+z=2\end{cases}.$$



a. Montrer, en utilisant les deux premières lignes de (S) et un raisonnement par l'absurde que ce système n'a pas de solution.

b. Donner l'écriture matricielle $AU = V$ de ce système.

c. On se place dans un repère orthonormé de l'espace. À quel type d'objets correspondent chaque équation du système ?
Pour ces objets, à quoi correspondent les coefficients de chaque ligne de la matrice A ?

d. La représentation ci-contre des objets est obtenue à l'aide d'un logiciel. Associer chaque objet à sa représentation.

e. Par un argument géométrique, justifier que le système n'a pas de solution.

2 Soit $(S)\begin{cases}2x+4y+5z=-2\\-x+2y+3z=10\\2x-4y-z=15\end{cases}$ le système linéaire d'inconnues x, y et z.

a. À l'aide d'un logiciel de géométrie dans l'espace, représenter dans un repère orthonormé les objets associés à ces trois équations et conjecturer le nombre de solutions du système.
Que peut-on alors dire de la matrice associée aux coefficients de ce système ?

b. Par un raisonnement géométrique, démontrer le résultat conjecturé.

c. À l'aide d'une calculatrice ou d'un logiciel de calcul formel, résoudre le système en utilisant le calcul matriciel et interpréter la solution.

3 Soit $(S')\begin{cases}2x+3y-4z=1\\5x+2y+z=8\\x-4y+9z=6\end{cases}$ le système linéaire d'inconnues x, y et z.

a. Montrer que les triplets (1 ; 1 ; 1) et (0 ; 3 ; 2) sont deux solutions du système (S').

b. Dans un repère orthonormé de l'espace, représenter les objets associés à ces trois équations et conjecturer le nombre de solutions du système.

c. Par un raisonnement géométrique, démontrer le résultat conjecturé.

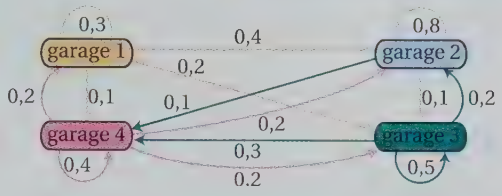
d. Interpréter géométriquement les solutions de ce système, puis les donner toutes.

50 Retour à la case départ

Algorithmique

Une municipalité a mis en place un système de location de vélos baptisé VEL'HOPLA.
Les vélos peuvent être empruntés et rendus à quatre endroits différents de la ville. Les garages à vélo sont numérotés de 1 à 4.

Les statistiques portant sur les premiers mois d'utilisation de VEL'HOPLA font apparaître que, chaque jour, 70 % des vélos se répartissent suivant le graphe ci-contre :



Au-dessus de chaque arête orientée entre deux garages à vélo est indiquée la probabilité qu'un vélo emprunté chaque jour dans le garage de l'origine de l'arête soit rendu au garage de l'extrémité de l'arête.
On considère que les 30 % des vélos restants sont répartis chaque jour de façon équiprobable entre les quatre garages.
On souhaite observer l'évolution de la répartition des vélos entre les différents garages sur une semaine.

1 Écrire la matrice A de transition entre les garages correspondant au graphe du comportement quotidien de 70 % des utilisateurs.

2 Pour le n-ième jour de l'étude menée ($n \geqslant 1$), on note X_n la matrice colonne donnant les fréquences de répartition des vélos entre les 4 garages. Montrer que, pour tout $n \geqslant 1$:

$$X_{n+1} = 0{,}7 \times A \times X_n + 0{,}3 \times B, \text{ où } B \text{ est la matrice colonne } B = \begin{pmatrix} 0{,}25 \\ 0{,}25 \\ 0{,}25 \\ 0{,}25 \end{pmatrix}.$$

3 On suppose que les vélos sont équitablement répartis entre les 4 garages au début de l'étude.

a. Donner la matrice colonne X_1.

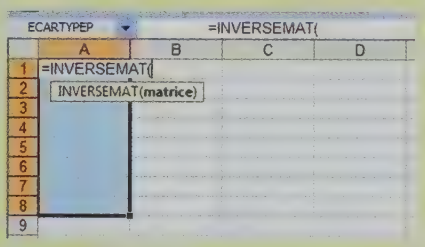
b. Calculer les matrices colonnes X_2 à X_7 correspondant à l'étude de la répartition des vélos sur une semaine.
(On pourra utiliser la calculatrice ou un tableur ou un logiciel de calcul formel.)

4 On donne à présent une répartition des vélos dans les quatre garages un mercredi : $\begin{pmatrix} 0{,}14241 \\ 0{,}37068 \\ 0{,}25441 \\ 0{,}2325 \end{pmatrix}$

a. Déterminer la répartition des vélos le lundi précédent.

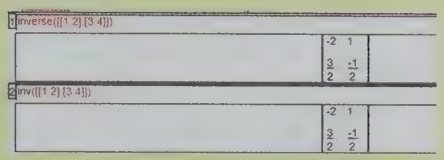
b. Écrire un algorithme qui permettrait de retrouver la répartition des vélos le mercredi précédent.
À l'aide d'un tableur ou d'une calculatrice ou d'un logiciel de programmation, déterminer alors cette répartition.
Que se passe-t-il ? Que peut-on en déduire ?

- **Syntaxe du tableur pour l'inverse :**
« =INVERSEMAT(…) »



Valider la formule par CTRL + SHIFT + ENTREE

- **Syntaxe du logiciel Xcas pour l'inverse :**
« Inverse(…) ou inv(…) »



5 Pour éviter de devoir transporter dans des camions, des vélos d'un garage à un autre pour compenser les déséquilibres, la municipalité cherche une répartition optimale des vélos entre les quatre garages.

a. Justifier qu'une répartition optimale correspond à une matrice colonne X solution de l'équation matricielle : $X = 0{,}7 \times A \times X + 0{,}3 \times B$.

b. À l'aide d'un outil (calculatrice ou logiciel), vérifier que la matrice $I_4 - 0{,}7 \times A$ est inversible et donner son inverse.

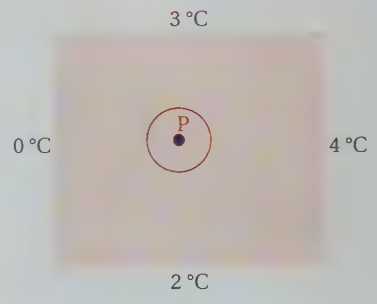
c. Déterminer alors une répartition optimale des 7 000 vélos de la commune entre les quatre garages.

51 Distribution de la température dans une plaque

Algorithmique

On considère une plaque polygonale pour laquelle la température des côtés n'est pas homogène (côtés en contact avec des sources de chaleur, par exemple).

On cherche à déterminer la température en un point intérieur à la plaque.



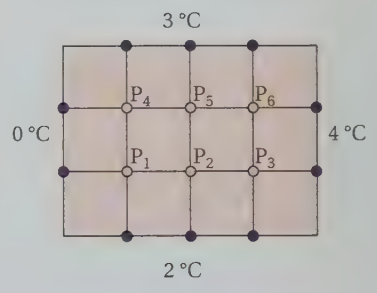
On admettra que :

« Si P est un point du bord de la plaque, sa température est celle du bord.

Si P est un point intérieur à la plaque, pour tout cercle de centre P entièrement contenu dans la plaque la température en P est la moyenne des températures sur le cercle. »

Partie 1. Une première distribution

Soit six points, intérieurs à la plaque, déterminés grâce au quadrillage figurant sur la figure ci-contre.



On note t_i la température au point P_i (pour $i = 1, 2, ..., 6$).

En première approximation du principe de physique énoncé plus haut, on suppose que la température en un point est la moyenne des températures aux 4 points reliés à ce point par un segment du quadrillage.

Ainsi, par exemple, la température t_1 en P_1 vérifie $t_1 = \frac{1}{4}(0 + 2 + t_2 + t_4)$.

1 Écrire le système vérifié par les six températures des points intérieurs à la plaque.

2 Montrer que l'on peut traduire ce système sous la forme matricielle : $T = MT + \frac{1}{4}B$ où T désigne la matrice colonne formée des six températures intérieures, B la matrice colonne $\begin{pmatrix} 2 \\ 2 \\ 6 \\ 3 \\ 3 \\ 7 \end{pmatrix}$ et M est une matrice carrée que l'on explicitera.

3 On admet que la matrice $I_6 - M$ est inversible.

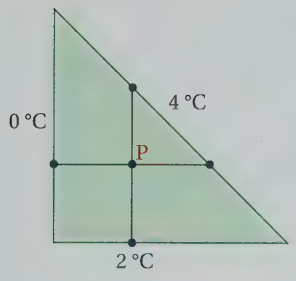
Résoudre le système à l'aide d'un calcul matriciel (utiliser la calculatrice ou un autre outil).

Donner des valeurs approchées des six températures aux points intérieurs.

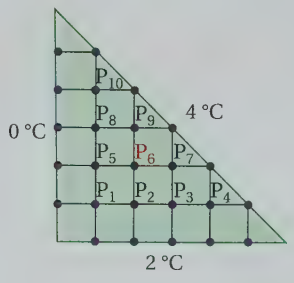
Partie 2. Précision du découpage

On considère à présent une plaque triangulaire .

1. Estimer la température au point P à l'aide du premier découpage proposé ci-contre.



2. On remplace ce découpage peu précis par le quadrillage ci-contre.



À l'aide d'un calcul matriciel, déterminer la matrice colonne T des 10 températures intérieures à la plaque triangulaire.
En déduire une estimation plus précise de la température en P_6.

3. Rédiger en langue naturelle le principe d'un algorithme qui permettrait le calcul des températures intérieures à la plaque pour un autre type de découpage à choisir.

52 Chiffrement de Hill

Algorithmique

En 1929, Lester Hill propose un nouvel algorithme de chiffrement.
Son idée est de procéder à des substitutions de lettres mais par un procédé impliquant des polygrammes, c'est-à-dire des paquets de plusieurs lettres.

Lester S. Hill (1891-1961)
Mathématicien et professeur américain, spécialiste des applications des mathématiques à la communication.

Partie 1. Un exemple de codage avec des bigrammes

Algorithme du chiffrement

On découpe le message en blocs de 2 lettres (en supprimant espace et ponctuation) ; on associe à chaque lettre un nombre selon le tableau suivant :

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 obtient ainsi pour chaque bloc de deux lettres un bloc de deux entiers N_1N_2 compris entre 0 et 25.
On convertit alors chaque bloc N_1N_2 en un autre bloc P_1P_2 de nombres entiers compris entre 0 et 25 par le procédé suivant : $\begin{cases} P_1 \equiv 7N_1 + 3N_2 \,[26] \\ P_2 \equiv 5N_1 + 8N_2 \,[26] \end{cases}$.
En utilisant le tableau précédent, on associe à chaque bloc P_1P_2 un bloc de deux lettres pour constituer le message codé.

1. Par cette méthode, coder les deux premières lettres du message « JE SUIS TRES JOYEUX ».

2. En utilisant un tableur, écrire un algorithme permettant le codage rapide de tout le message et donner alors ce message codé.

REMARQUES SUR UN TABLEUR

- L'instruction = **CODE**(lettre en majuscule) **– 65** permet d'obtenir la correspondance entre lettre et nombre du tableau donné p. 127.
- L'instruction = **MOD**(n ; 26) donne le reste de la division euclidienne de n par 26.
- L'instruction = **CAR**(nombre + 65) permet d'obtenir la correspondance entre nombre et lettre du tableau donné p. 127.

Partie 2. Déchiffrement du message ; matrice inverse

On souhaite mettre en place un algorithme de déchiffrement de l'algorithme de Hill précédent.

1. Soit la matrice carrée $A = \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix}$.

Montrer que la matrice A est inversible et déterminer sa matrice inverse à coefficients réels.
On écrira cette matrice inverse sous la forme $\frac{1}{41}B$ où B est une matrice à coefficients entiers (41 est le nombre obtenu en calculant : $7 \times 8 - 3 \times 5$).

2. Montrer qu'il existe un unique entier m compris entre 0 et 25 tel que $41m \equiv 1$ [26].
Déterminer cet entier m.

3. Montrer que la matrice carrée mB est une matrice telle que $mB \times \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} N_1 \\ N_2 \end{pmatrix}$ [26].

(Cette congruence sur les matrices colonnes signifie la congruence des coefficients de chaque ligne.)
Déterminer alors quatre entiers a, b, c et d compris entre 0 et 25 tels que :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} N_1 \\ N_2 \end{pmatrix} [26].$$

(On admet que les entiers a, b, c et d sont uniques.)

4. En déduire un algorithme de décodage de ce chiffrement de Hill et déchiffrer le message :

« XZEQGCXWCODTHVNQFGDRCKB XWRKSHQNRHVHVVVGN ».

Partie 3. Une condition suffisante pour pouvoir coder

1. Dans le déchiffrement précédent, quelle condition particulière sur 41 et 26 permet de répondre à la **question 2** de la **partie 2** ?

2. On souhaite adopter le chiffrement de Hill donné par le procédé : $\begin{cases} P_1 \equiv 6N_1 + 2N_2 \ [26] \\ P_2 \equiv 7N_1 + 3N_2 \ [26] \end{cases}$.

Montrer que le nombre $6 \times 3 - 2 \times 7$ n'est pas premier avec 26. Donner le PGCD de ces deux nombres.

3. Comparer les produits $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} N_1 - 13 \\ N_2 + 13 \end{pmatrix}$ et $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} N_1 \\ N_2 \end{pmatrix}$. Le procédé de codage est-il satisfaisant ? Justifier.

4. Pour un procédé de chiffrement du type $\begin{cases} P_1 \equiv aN_1 - bN_2 \ [26] \\ P_2 \equiv cN_1 - dN_2 \ [26] \end{cases}$, l'unicité de la correspondance dans le codage est une conséquence de l'inversibilité de la matrice modulo 26.
Montrer que cette condition est vérifiée lorsque $ad - bc$ et 26 sont premiers entre eux.

Sujets type BAC

Exercice résolu

Exercice 53 **Un codage par trigrammes** (méthode de Hill)

Nicolas a codé un message par la méthode suivante.

Il a choisi A une matrice carrée de taille 3 : $A = \begin{pmatrix} x & y & z \\ 0 & 5 & 2 \\ 1 & 0 & 0 \end{pmatrix}$

et il a codé son texte grâce à un tableur en trois étapes, suivant les indications ci-dessous :

Étape 1 : à chaque lettre du texte, il associe un nombre entre 0 et 25 selon sa place dans l'alphabet (de 0 pour A à 25 pour Z) ; par exemple O devient 14.

Étape 2 : il considère les nombres obtenus précédemment par triplets et écrit les nombres résultant du produit de la matrice A par chaque triplet ; par exemple, $0 \times 1 + 5 \times 14 + 2 \times 13 = 96$.

Étape 3 : il cherche les congruents modulos 26 des nombres obtenus à l'étape **2**, puis il associe à chacun de ces congruents une lettre de l'alphabet par le procédé réciproque de l'étape **1**. Par exemple, $96 = 3 \times 26 + 18$, donc $96 \equiv 18$ [26] et enfin 18 correspond à la lettre S.

Mais Nicolas a oublié les coefficients de la première ligne de la matrice A et il a en partie perdu des données de son tableau de codage.

Texte	étape 1	étape 2	étape 3	Texte codé
B	1	57	5	F
O	14	96	18	S
N	13	1	1	B
J	9	80	2	C
O	14	?	?	?
U	20	?	?	?
R	17	53	1	B
A	0	38	12	M
?	?	?	17	R
?	?	?	2	C
?	?	?	6	G
?	?	?	14	O

1. Retrouver les données manquantes des cases bleues du tableau.

2. Déterminer l'entier k du tableau en utilisant les deux lignes qui précèdent.

3. Retrouver la 1re ligne de la matrice A.

4. Retrouver les données manquantes des cases roses du tableau en justifiant la méthode utilisée.
En déduire la fin du message de départ.

Voir résolution page suivante.

Exercice 54 *D'après un sujet de BTS*

Une agence de voyages propose un circuit pour visiter trois villes A, B et C.
Le client peut choisir la durée de séjour dans chacune des villes. L'agence propose des tarifs qui diffèrent selon la période touristique (haute, moyenne et basse saisons). Les prix journaliers, en centaines d'euros par personne, sont donnés dans le tableau suivant :

	Ville A	Ville B	Ville C
Haute saison	2,5	3,5	1,5
Moyenne saison	2	2	1,5
Basse saison	1	1	1

Soit P la matrice $\begin{pmatrix} 2{,}5 & 3{,}5 & 1{,}5 \\ 2 & 2 & 1{,}5 \\ 1 & 1 & 1 \end{pmatrix}$ qui représente les prix journaliers par ville et par période.

1. a. Monsieur Meyer choisit un circuit de 14 jours qui comprend 6 jours dans la ville A, 5 jours dans la ville B et 3 jours dans la ville C. On associe à ce choix la matrice colonne $M = \begin{pmatrix} 6 \\ 5 \\ 3 \end{pmatrix}$.
Que représentent les coefficients de la matrice $P \times M$?
b. Monsieur Meyer dispose d'un budget de 2 600 euros, à quelle période pourra-t-il faire son voyage ?

2. Soit la matrice $Q = \begin{pmatrix} -1 & 4 & -4{,}5 \\ 1 & -2 & 1{,}5 \\ 0 & -2 & 4 \end{pmatrix}$.

a. Calculer le produit matriciel $P \times Q$.
b. Dans une publicité, l'agence de voyage affirme qu'un circuit complet de 14 jours est possible au prix de 2 600 euros en haute saison, 2 250 euros en moyenne saison et 1 400 euros en basse saison.
Comment se compose ce voyage ?

Résolution

1. Le codage s'effectue en multipliant à l'**étape 2** la matrice A par les triplets successifs d'éléments de la colonne B ; pour déterminer les données manquantes des cases bleues du tableau, on effectue donc d'abord le produit matriciel suivant :

$$A \times \begin{pmatrix} 9 \\ 14 \\ 20 \end{pmatrix} = \begin{pmatrix} x & y & z \\ 0 & 5 & 2 \\ 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 9 \\ 14 \\ 20 \end{pmatrix} = \begin{pmatrix} 9x+14y+20z \\ 110 \\ 9 \end{pmatrix}$$

Les cellules bleues C7 et C8 de l'**étape 2** contiennent donc respectivement les nombres 110 et 9. On réduit ces nombres modulo 26 à l'**étape 3**, donc les cellules D7 et D8 contiennent respectivement les nombres 6 ($110 = 4 \times 26 + 6$) et 9. La cellule E7 contient donc la lettre G et la cellule E8 la lettre J.

2. Le produit de la matrice A par le triplet suivant de la colonne B donne :

$$\begin{pmatrix} x & y & z \\ 0 & 5 & 2 \\ 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 17 \\ 0 \\ k \end{pmatrix} = \begin{pmatrix} 17x+kz \\ 2k \\ 17 \end{pmatrix}.$$

De l'égalité $2k = 38$, on tire $k = 19$.

3. Pour déterminer les coefficients de la première ligne de la matrice A, on utilise les produits de la matrice A par les trois premiers triplets de nombres de la colonne B et, plus précisément, on s'intéresse au premier coefficient de chaque vecteur colonne ainsi obtenu ce qui nous donne le système ci-contre :

$$\begin{cases} x+14y+13z=57 \\ 9x+14y+20z=80 \\ 17x+0y+19z=53 \end{cases}$$

La traduction matricielle de ce système est $B \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 57 \\ 80 \\ 53 \end{pmatrix}$ avec $B = \begin{pmatrix} 1 & 14 & 13 \\ 9 & 14 & 20 \\ 17 & 0 & 19 \end{pmatrix}$.

Grâce à la calculatrice, on trouve que la matrice B est inversible et on en déduit :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = B^{-1} \times \begin{pmatrix} 57 \\ 80 \\ 53 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$$

4. Le nombre situé dans la cellule B11 est $k = 19$ qui correspond à la lettre initiale T.

La question précédente a permis de déterminer la matrice $A = \begin{pmatrix} 2 & 3 & 1 \\ 0 & 5 & 2 \\ 1 & 0 & 0 \end{pmatrix}$.

Grâce à la calculatrice, on vérifie que cette matrice est inversible d'inverse A^{-1} :

$$A^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 2 & -1 & -4 \\ -5 & 3 & 10 \end{pmatrix}.$$

On note respectivement a, b et c les nombres contenus dans les cellules B11, B12 et B13, les coefficients du vecteur colonne $A \times \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ sont congrus à ceux du vecteur colonne $\begin{pmatrix} 2 \\ 6 \\ 14 \end{pmatrix}$ modulo 26.

À l'aide des propriétés des congruences par rapport aux opérations dans $\mathbb{Z}$, les coefficients du vecteur colonne $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ sont donc aussi congrus à ceux du vecteur colonne $A^{-1} \times \begin{pmatrix} 2 \\ 6 \\ 14 \end{pmatrix}$ modulo 26.

Or $A^{-1} \times \begin{pmatrix} 2 \\ 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 14 \\ -58 \\ 148 \end{pmatrix}$; d'où $a \equiv 14$ [26], $b \equiv -58 \equiv 20$ [26] et $c \equiv 148 \equiv 18$ [26].

Donc les lettres de la fin du message sont O, U et S. Le message complet est : « BONJOUR A TOUS ».

Matrices et études asymptotiques de processus discrets

6

La photo ci-dessus est celle de Larry Page et Sergey Brin, créateurs de l'algorithme **PageRank**. Cet algorithme repose sur des éléments de la théorie des graphes, du calcul matriciel et utilise des théorèmes de convergence de marche aléatoire.

Le chapitre en bref

Réinvestir

- Le calcul matriciel et ses applications aux processus d'évolution

Explorer

- Le comportement asymptotique de certains processus d'évolution

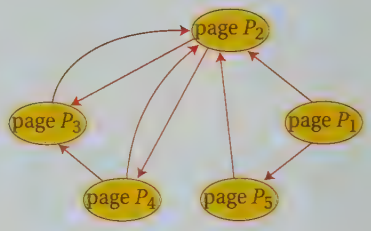
Activités de recherche, p. 144

Activités d'exploration

1 Comment un moteur de recherche classe les pages Web

Réinvestir : Une matrice pour décrire l'évolution d'un processus et les opérations sur les matrices.
Explorer : La convergence d'un processus vers un état stable.

On a représenté ci-contre cinq pages Internet comprenant des articles sur le sujet « les élèves de Terminale S font-ils des études scientifiques ? ».
Sur certaines des pages, un lien pointe vers une autre des pages ; ce lien est matérialisé par la flèche orientée.



1 Laquelle de ces pages semble être *a priori* la plus pertinente pour le sujet traité ?

2 On suppose qu'un utilisateur qui arrive sur l'une des ces pages suivra de façon équiprobable un des liens de cette page vers les autres pages. Établir la matrice A donnant les probabilités de passage d'une page à une autre par un utilisateur.

3 On suppose qu'un utilisateur est situé au départ sur la page P_1.

a. À l'aide de la calculatrice ou d'un logiciel de calcul formel, compléter le tableau qui donne les probabilités d'arrivées successives sur chaque page après 1 clic, 2 clics, 5 clics et 10 clics.

Pages	Après 0 clic	Après 1 clic	Après 2 clics	Après 5 clics	Après 10 clics
P_1	1				
P_2	0				
P_3	0				
P_4	0				
P_5	0				

b. Quelle est la page qui a la plus grande probabilité d'être fréquentée après 10 clics ? Comparer avec la réponse donnée à la question **1**.

c. Observer l'évolution de ces probabilités lorsque le nombre n de clics devient de plus en plus grand. Vers quelles probabilités limites de fréquentation de chaque page semble tendre la répartition ?

4 Pour un utilisateur situé au départ sur une autre page que la page 1, observer l'évolution des mêmes probabilités. Que constate-t-on ?

5 On note X la matrice colonne formée des probabilités limites de fréquentation conjecturées à la question **3** **c**. Montrer que si la répartition des utilisateurs au départ se fait suivant ces probabilités, alors la répartition reste stable à chaque clic.
Cette matrice colonne est appelée **état stable du système**.
Écrire l'égalité matricielle vérifiée par X.

6 On définit la pertinence de la page P_i par sa probabilité p_i dans la matrice colonne stable $X = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \end{pmatrix}$.

a. Quel classement, selon la pertinence, de ces 5 pages peut-on proposer pour le sujet traité ?

b. Déduire de l'égalité matricielle vérifiée par X que $p_2 = \frac{1}{2}p_1 + p_3 + \frac{1}{2}p_4 + p_5$.

c. Quelle relation vérifie la pertinence d'une page ?

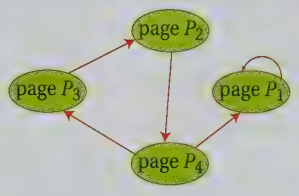
d. De cette manière, retrouver les relations entre les pertinences de chacune des pages pour le sujet traité à partir des données du graphe.

2 Amélioration du procédé de classement du moteur de recherche

Réinvestir : Une matrice pour décrire l'évolution d'un processus et les opérations sur les matrices.
Explorer : Une condition particulière pour la convergence.

NOTE
Cette situation arrive très fréquemment en réalité puisque sur les milliards de pages Web existantes, les liens pointant d'une page vers une autre sont relativement peu fréquents.

Ce graphe donne les relations entre quatre pages Web.



1 Pour un utilisateur situé au départ page 1, que se passe-t-il ?

2 L'algorithme suivant pallie le problème en modélisant la situation de la façon suivante :
« Pour un utilisateur qui sur un thème donné arrive sur une page Web :

- dans 15 % des cas, il choisit au hasard de façon équirépartie une page quelconque y compris la page en cours ;
- dans 85 % des cas, il suit de façon équirépartie un des liens proposés par la page en cours vers une autre page. »

Pour n entier positif, on note X_n la matrice colonne donnant la répartition des probabilités de fréquentation des quatre pages après n clics.
On note A le matrice de transition donnant les probabilités de passage d'une page à une autre par les liens représentés sur le graphe ci-dessus et C la matrice colonne égale à $\begin{pmatrix} 0{,}25 \\ 0{,}25 \\ 0{,}25 \\ 0{,}25 \end{pmatrix}$.

NOTE
L'algorithme proposé ici est adapté de l'algorithme **PageRank** (PR), inventé en 1998 par Larry Page, cofondateur de Google. Cet algorithme sert de système de classement à ce célèbre moteur de recherche.

Justifier que la suite de matrices colonnes (X_n) vérifie la relation : $X_{n+1} = 0{,}85AX_n + 0{,}15C$.

Un phénomène d'évolution

Dans cette activité, ce **phénomène d'évolution** se modélise par une relation de la forme $\boldsymbol{X_{n+1} = AX_n + B}$ où A est une matrice carrée de taille p, B une matrice colonne de dimension p et (X_n) une suite de vecteurs colonnes de dimension p.

3 On considère toujours un utilisateur situé au départ sur la page 1. À l'aide de la calculatrice ou d'un logiciel de calcul formel, compléter le tableau ci-dessous qui donne les probabilités d'arrivées successives sur chaque page après 1 clic, 2 clics, 5 clics ou10 clics.

Pages	Après 0 clic	Après 1 clic	Après 2 clics	Après 5 clics	Après 10 clics
P_1	1				
P_2	0				
P_3	0				
P_4	0				

4 On suppose que, quelle que soit la page de départ, la suite des matrices colonnes (X_n) converge vers une matrice colonne X (état stable du système) vérifiant $X = 0{,}85AX + 0{,}15C$.

a. Montrer que X vérifie l'égalité matricielle : $(I_4 - 0{,}85A)\,X = 0{,}15C$.

b. À quelle condition peut-on alors déterminer X de façon unique ?

c. Trouver X à l'aide de la calculatrice, puis comparer avec les résultats du tableau.

L'état stable X associé à l'algorithme définit la pertinence des pages associées à une information comme dans l'**activité 1**, il s'ensuit un classement des pages. En pratique, la recherche de l'état stable ne se fait pas par la résolution de l'équation matricielle (les dimensions trop importantes rendent les calculs très longs). On approche l'état stable très rapidement par une suite de matrices colonnes construites à partir de l'algorithme comme dans cette activité.

A. Suites récurrentes et matrices

1 Écriture matricielle de relations de définition de suites récurrentes

Différents types de suites définies par des relations de récurrence se ramènent à l'étude d'une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = AX_n + B$ où A est une matrice carrée et B une matrice colonne.

EXEMPLE SUITE COUPLÉES

Soit deux suites de nombres réels (u_n) et (v_n) définies par :

$u_0 = 5$ et $v_0 = -2$ et, pour tout $n \geqslant 0$: $u_{n+1} = 1{,}7u_n + 0{,}6v_n + 3$ et $v_{n+1} = -5u_n + 0{,}1v_n - 1$.

Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$, alors les relations de récurrence ci-dessus s'écrivent aussi pour tout $n \geqslant 0$:

$X_{n+1} = AX_n + B$, où A est la matrice carrée $A = \begin{pmatrix} 1{,}7 & 0{,}6 \\ -5 & 0{,}1 \end{pmatrix}$ et B la matrice colonne $B = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$.

Justification de la relation : le produit matriciel AX_n est égal à la matrice colonne $\begin{pmatrix} 1{,}7u_n + 0{,}6v_n \\ -5u_n - 0{,}1v_n \end{pmatrix}$; on a donc bien l'équivalence de cette relation avec les relations de définition des deux suites.

EXEMPLE SUITE DÉFINIE PAR UNE RELATION DE RÉCURRENCE D'ORDRE 2

Soit la suite (u_n) définie par $u_0 = 11$; $u_1 = -2$ et $u_{n+2} = 3u_{n+1} - 0{,}5u_n$ pour tout $n \geqslant 0$.

Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}$ alors la relation de récurrence ci-dessus s'écrit aussi, pour tout $n \geqslant 0$:

$X_{n+1} = AX_n$ où A est la matrice carrée $A = \begin{pmatrix} 0 & 1 \\ -0{,}5 & 3 \end{pmatrix}$.

Justification de la relation : pour tout $n \geqslant 0$, la matrice colonne X_{n+1} est égale à $X_{n+1} = \begin{pmatrix} u_{n+1} \\ u_{n-2} \end{pmatrix}$ et le produit matriciel AX_n est égal à la matrice colonne $\begin{pmatrix} u_{n-1} \\ -0{,}5u_n + 3u_{n-1} \end{pmatrix}$.

L'égalité matricielle $X_{n+1} = AX_n$ est donc équivalente au système d'égalités, formé d'une égalité triviale et de la relation de récurrence définissant la suite : $\begin{cases} u_{n-1} = u_{n-1} \\ u_{n-2} = 3u_{n-1} - 0{,}5u_n \end{cases}$.

REMARQUE

La matrice colonne X_0 est la matrice $\begin{pmatrix} u_0 \\ v_0 \end{pmatrix}$ dans le premier exemple et la matrice $\begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$ dans le second exemple.

2 Calcul de termes à l'aide de l'écriture matricielle des relations de définition de suites récurrentes

Les écritures précédentes permettent, en utilisant le calcul matriciel, de calculer des termes de la suite et de disposer aussi, dans le cas suivant, d'une écriture pour le terme général.

PROPRIÉTÉ

Soit une suite de matrices colonnes (X_n) telle que pour tout $n \geqslant 0$, $X_{n+1} = AX_n$. Alors :

$X_n = A^n X_0$ pour tout $n \geqslant 0$.

DÉMONSTRATION

▶ Savoir-faire 1
Calculer des termes d'une suite en utilisant l'écriture matricielle de la relation de récurrence, p. 138

On démontre la propriété «Pour tout entier naturel n, $X_n = A^n X_0$» par récurrence sur n.
$A^0 X_0 = X_0$ donc la propriété est vraie au rang $n = 0$.
On suppose la propriété vraie au rang k, c'est-à-dire $X_k = A^k X_0$, alors au rang $k + 1$, on a :

$$X_{k+1} = A X_k = A \times (A^k X_0) = (A \times A^k) X_0 = A^{k+1} X_0$$

La propriété est encore vraie au rang $k + 1$.
Conclusion : la propriété $\boldsymbol{X_n = A^n X_0}$ est vraie pour tout $n \geqslant 0$.

B. Convergence et état stable

Soit une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = AX_n + B$.

1 Propriété de la limite dans le cas de la convergence

DÉFINITION

On dit que la **suite de matrices colonnes** (X_n) de taille p est **convergente** si les p suites formées par les termes correspondant à la même ligne sont convergentes.
La limite de cette suite est alors la matrice colonne formée des p limites obtenues.

Dans tous les autres cas, on dit que **la suite** est **divergente**.

THÉORÈME

Si une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = A X_n + B$ est convergente, alors sa limite X est une matrice colonne vérifiant l'égalité $X = AX + B$.

DÉMONSTRATION

Dans l'égalité $X_{n+1} = AX_n + B$, le membre de droite converge vers X. De plus, comme conséquence des théorèmes concernant les limites de sommes et de produit par un nombre réel des suites convergentes, le membre de gauche converge vers $AX + B$. D'où, par unicité de la limite : $X = AX + B$.

▶ Savoir-faire 2
Déterminer une suite de matrices colonnes constante vérifiant une relation de récurrence, p. 138

REMARQUE

Le théorème précédent permet donc de dire que, dans le cas de la convergence, la limite de la suite de matrices colonnes est à rechercher parmi les suites constantes vérifiant la relation de récurrence.

2 Recherche d'une suite constante ou d'un état stable

La recherche d'une matrice colonne X vérifiant une relation du type $X = AX + B$ fait intervenir les résultats vus dans le chapitre 5 sur le calcul matriciel et la résolution de systèmes.

PROPRIÉTÉ

Soit I la matrice identité de même taille qu'une matrice A.
Si la matrice $I - A$ est inversible, pour toute matrice colonne B de même taille que A, il existe une et une seule matrice colonne X vérifiant $X = AX + B$.

DÉMONSTRATION

Par les propriétés du calcul matriciel, $X = AX + B \Leftrightarrow (I - A)X = B \Leftrightarrow X = (I - A)^{-1} \times B$ en multipliant à gauche les deux membres de dernière égalité par l'inverse de $I - A$.
Il y a donc une et une seule matrice colonne X solution de $X = AX + B$.

REMARQUE

Puisqu'il n'y a qu'une seule matrice colonne limite solution, **pour toute matrice colonne X_0 pour laquelle la suite (X_n) est convergente**, la limite X est indépendante des valeurs de X_0.

PROPRIÉTÉ (ADMISE)

Dans le cas où la matrice $I - A$ n'est pas inversible :

- soit il n'existe **aucune** matrice colonne vérifiant $X = AX + B$ (dans le cadre de la recherche d'une limite, cela signifie qu'il ne peut y avoir convergence) ;
- soit il existe **une infinité** de matrices colonnes X solution de $X = AX + B$ dont l'une est éventuellement la limite recherchée dans le cas de la convergence.

NOTE

Le paragraphe C suivant donne un exemple fréquent de ce type de situation.

REMARQUE

Dans ce cas, on recherche donc les éventuelles solutions en résolvant le système dont l'écriture matricielle est $X = AX + B$ ou $(I - A)X = B$.

D'autres conditions liées à la limite peuvent se rajouter à celles données par le système et permettre de déterminer parmi les solutions celle correspondant à la limite dans le cas de la convergence.

C. Application aux marches aléatoires

1 Comportement asymptotique d'une marche aléatoire

DÉFINITIONS

- On dit qu'une **marche aléatoire** est **convergente** si la suite des matrices colonnes (X_n) des états de la marche aléatoire converge.
- Dans le cas de l'étude d'une marche aléatoire telle que la suite des états de la marche aléatoire vérifie une relation du type $X_{n+1} = AX_n + B$, une suite constante vérifiant $X = AX + B$ est aussi appelée **état stable** de la marche aléatoire.

REMARQUE

Une marche aléatoire peut être convergente ou divergente selon l'état initial X_0. S'il y a convergence, d'après le théorème du paragraphe précédent, ce ne peut être que vers un état stable.

EXEMPLE

Soit la marche aléatoire pour laquelle on passe à chaque pas du sommet A au sommet B avec une probabilité de 1 et du sommet B au sommet A avec une probabilité de 1.

La matrice de transition de cette marche aléatoire est $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Si on note $X_0 = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$ l'état initial de la marche aléatoire alors, pour tout $n \geqslant 0$:

$$X_n = M^n X_0 \text{ avec } M^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ si } n \text{ est pair et } M^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ si } n \text{ est impair.}$$

Ainsi $X_n = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$ lorsque n est pair et $X_n = \begin{pmatrix} b_0 \\ a_0 \end{pmatrix}$ lorsque n est impair.

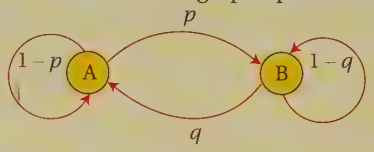
On en déduit que la suite des états (X_n) diverge pour toutes les valeurs de X_0 sauf dans le cas $a_0 = b_0 = \dfrac{1}{2}$ où la suite est alors constante de terme égal à X_0.

▶ Savoir-faire 3
Étudier le comportement asymptotique d'une marche aléatoire, p. 139

2 Cas des marches aléatoires sur un graphe probabiliste à deux sommets

PROPRIÉTÉ

Soit une marche aléatoire sur un graphe probabiliste à deux sommets du type :



avec $0 < p < 1$ et $0 < q < 1$.

La matrice de transition est $M = \begin{pmatrix} 1-p & q \\ p & 1-q \end{pmatrix}$.

Quel que soit l'état initial X_0 de cette marche aléatoire, elle converge vers un état stable unique $X = \begin{pmatrix} a \\ b \end{pmatrix}$ tel que $X = MX$ et $a + b = 1$.

DÉMONSTRATION

Pour tout $n \geqslant 0$, si on note $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ l'état probabiliste après n pas, alors $a_n + b_n = 1$.

À l'aide de la relation $X_{n+1} = M \times X_n$ où M est la matrice de transition, on en déduit que, pour tout entier $n \geqslant 0$:

$$a_{n+1} = (1-p)a_n + qb_n = (1-p)a_n + q(1-a_n) = (1-p-q)\,a_n + q.$$

Soit la suite (u_n) définie, pour tout entier naturel n, par $u_n = a_n - \dfrac{q}{p+q}$. Pour tout entier $n \geqslant 0$:

$$u_{n+1} = a_{n+1} - \frac{q}{p+q} = (1-p-q)\,a_n + q - \frac{q}{p+q} = (1-p-q)\,a_n - \frac{q(1-p-q)}{p+q}$$

$$= (1-p-q)\left(a_n - \frac{q}{p+q}\right) = (1-p-q)\,u_n.$$

La suite (u_n) est donc une suite géométrique de raison $1 - p - q$. Comme $|1-p-q| < 1$ (car $0 < p + q < 2$), cette suite **converge** vers 0.

On en déduit que la suite (a_n) converge vers $\dfrac{q}{p+q}$ puisque, pour tout $n \geqslant 0$, $a_n = u_n + \dfrac{q}{p+q}$.

Enfin, la suite (b_n) converge vers $\dfrac{p}{p+q}$ puisque, pour tout $n \geqslant 0$, $b_n = 1 - a_n$.

Ces limites sont bien indépendantes de l'état initial X_0.

Par le théorème de convergence vu au paragraphe **B**, la limite est un état stable $\begin{pmatrix} a \\ b \end{pmatrix}$. ■

REMARQUES

a. Pour la convergence, on peut aussi utiliser la décomposition proposée p. 102 qui donne M^n convergente car $|(1-p)-q| < 1$, donc $X_n = M^n X_0$ converge quel que soit X_0.

b. Ici, la matrice $I_2 - M$ n'est pas inversible car $I_2 - M = \begin{pmatrix} p & -q \\ p & -q \end{pmatrix}$; on peut rechercher l'état limite en utilisant les deux conditions qui suffisent à le déterminer : $\begin{pmatrix} a \\ b \end{pmatrix}$ est stable et $a + b = 1$.

En effet, $\begin{pmatrix} a \\ b \end{pmatrix}$ stable implique $\begin{cases} (1-p)a + qb = a \\ pa + (1-q)b = b \end{cases} \Leftrightarrow b = \dfrac{p}{q}a$.

De plus, cet état stable vérifie $a + b = 1$ puisque la somme de la probabilité d'être en A et de la probabilité d'être en B fait 1 : donc a est solution de $a + \dfrac{p}{q}a = 1 \Leftrightarrow \dfrac{q+p}{q}a = 1 \Leftrightarrow a = \dfrac{q}{p+q}$.

Une seule valeur convient pour a et on en déduit $b = \dfrac{p}{p+q}$ grâce à la relation précédente.

Il n'y a donc qu'un seul état stable $\begin{pmatrix} a \\ b \end{pmatrix}$ vérifiant $a + b = 1$. C'est l'état limite indépendant de l'état initial X_0.

▶ Savoir-faire 4
Déterminer l'état stable limite pour une marche aléatoire sur un graphe probabiliste d'ordre 2, p. 140

Savoir-faire

Savoir-faire 1 — Calculer des termes d'une suite en utilisant l'écriture matricielle de la relation de récurrence

ÉNONCÉ

a. Soit deux suites couplées de nombres réels (u_n) et (v_n) définies par :

$u_0 = -1$ et $v_0 = -2$ et, pour tout $n \geqslant 0$, $u_{n+1} = 3u_n - 2v_n$ et $v_{n+1} = 5u_{n+1} + v_n$.

Déterminer les termes u_5 et v_5 à l'aide du calcul matriciel.

b. Soit (u_n) une suite vérifiant $u_{n+2} = 1{,}5u_{n+1} + 2u_n$ pour tout $n \geqslant 0$.

Déterminer les termes u_0 et u_1 sachant que $u_4 = 30{,}5$ et $u_5 = 59{,}75$.

SOLUTION

a. Pour tout $n \geqslant 0$:

$u_{n+1} = 3u_n - 2v_n$ et

$v_{n+1} = 5u_{n+1} + v_n = 5(3u_n - 2v_n) + v_n = 15u_n - 9v_n$.

Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$ alors les relations de récurrence ci-dessus s'écrivent aussi, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$ où A est la matrice carrée $A = \begin{pmatrix} 3 & -2 \\ 15 & -9 \end{pmatrix}$ et avec $X_0 = \begin{pmatrix} -1 \\ -2 \end{pmatrix}$.

On calcule alors $X_5 = A^5 \times X_0 = \begin{pmatrix} 441 \\ 1863 \end{pmatrix}$, donc $u_5 = 441$ et $v_5 = 1863$.

b. Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$, alors la relation de récurrence $u_{n+2} = 1{,}5u_{n+1} + 2u_n$ s'écrit aussi, pour tout $n \geqslant 0$: $X_{n+1} = AX_n$ où A est la matrice carrée $A = \begin{pmatrix} 0 & 1 \\ 2 & 1{,}5 \end{pmatrix}$.

On connaît $X_4 = \begin{pmatrix} 30{,}5 \\ 59{,}75 \end{pmatrix}$, et comme $X_4 = A^4 \times X_0$, on en déduit que $X_0 = (A^{-1})^4 \times X_4 = \begin{pmatrix} 8 \\ -4 \end{pmatrix}$, donc $u_0 = 8$ et $u_1 = -4$.

Exercices 8 et 9 p. 141

MÉTHODE

a. Pour traduire l'écriture des relations de récurrence par une égalité matricielle du type $X_{n+1} = AX_n$, il est nécessaire d'expliciter u_{n+1} et v_{n+1} en fonction de u_n et v_n.

Par propriété du cours : « pour tout entier naturel n : $X_n = A^n \times X_0$ », on en déduit le calcul des termes souhaités à l'aide d'une calculatrice, par exemple.

b. La relation de récurrence faisant intervenir deux termes consécutifs, on introduit une matrice colonne correspondant à deux termes consécutifs de la suite.

Ici, on demande de retrouver les premiers termes de la suite ; on utilise alors la même propriété du cours mais on a ensuite recours à la matrice inverse de A pour résoudre l'équation matricielle ainsi obtenue.

On fait les calculs (en vérifiant que la matrice A est inversible) à l'aide d'une calculatrice, par exemple.

Savoir-faire 2 — Déterminer une suite de matrices colonnes constante vérifiant une relation de récurrence

ÉNONCÉ

a. Soit une suite de matrices colonnes (X_n) telle que, pour tout $n \geqslant 0$:

$$X_{n+1} = AX_n + C \text{ où } A = \begin{pmatrix} 5 & -3 \\ 2 & -4 \end{pmatrix} \text{ et } C = \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

Déterminer s'il existe une telle suite (X_n) qui soit constante. Si oui, donner les toutes.

b. Même exercice avec $A = \begin{pmatrix} 2 & -2 \\ -3 & 7 \end{pmatrix}$ et $C = \begin{pmatrix} -1 \\ 3 \end{pmatrix}$.

SOLUTION

a. Il s'agit de résoudre l'équation matricielle : $X = AX + C$ qui équivaut à $(I - A)X = C$. Or la matrice $(I - A)$ est inversible donc cette équation a une unique solution : $X = (I-A)^{-1}C = \begin{pmatrix} \frac{9}{14} \\ \frac{6}{7} \end{pmatrix}$.

La suite constante est donc définie par $X_n = \begin{pmatrix} \frac{9}{14} \\ \frac{6}{7} \end{pmatrix}$ pour tout $n \geqslant 0$.

b. Il s'agit de résoudre l'équation matricielle : $X = AX + C$ qui équivaut à $(I - A)X = C$.
Or la matrice $(I - A)$ n'est pas inversible ; on détermine donc les solutions $X = \begin{pmatrix} a \\ b \end{pmatrix}$ de l'équation matricielle en résolvant le système $\begin{cases} a - 2b = -1 \\ -3a + 6b = 3 \end{cases}$; ce système équivaut à $a = 2b - 1$; il a donc une infinité de solutions.
Les suites de matrices colonnes constantes du type $\begin{pmatrix} 2b-1 \\ b \end{pmatrix}$ pour $b \in \mathbb{R}$ vérifient la relation de récurrence.

Exercices 23 à 27 p. 143

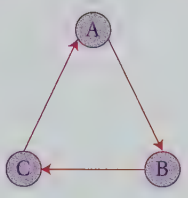
MÉTHODE

On cherche une matrice colonne constante solution de l'équation matricielle $X = AX + C$, cette équation équivaut à $(I - A)X = C$.
D'après le cours sur les matrices inversibles et les systèmes, il y a une unique solution dans le cas où la matrice $(I - A)$ est inversible. C'est le cas de la question **a.**
Sinon, on détermine les éventuelles solutions par la résolution du système correspondant à l'égalité matricielle $(I - A)X = C$. Ce système a soit une infinité de solutions que l'on détermine en fonction d'un paramètre (cas de la **question b.**), soit aucune solution.

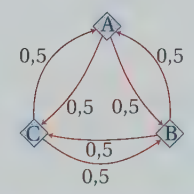
Savoir-faire 3 — Étudier le comportement asymptotique d'une marche aléatoire

ÉNONCÉ

1. On considère une marche aléatoire sur le graphe ci-contre où l'on part du sommet A.
Montrer que la marche aléatoire n'est pas convergente.



2. On considère une marche aléatoire sur le graphe ci-contre où l'on part du sommet A.
Montrer que la marche aléatoire est convergente.



SOLUTION

Soit, pour $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$ donnant les probabilités d'être situé en chacun des sommets, n instants après le départ.

1. Pour tout $n \geqslant 0$, $X_{n+1} = A \times X_n$ où A est la matrice carrée $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.
Comme $A^3 = I_3$, on peut en déduire, par exemple, que :
pour tout $n \geqslant 0$: $X_{3n} = X_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et $X_{3n+1} = X_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.
Donc la suite (X_n) n'est pas convergente.

2. Pour tout $n \geqslant 0$:
$X_{n+1} = A \times X_n$ où A est la matrice carrée $A = \begin{pmatrix} 0 & 0{,}5 & 0{,}5 \\ 0{,}5 & 0 & 0{,}5 \\ 0{,}5 & 0{,}5 & 0 \end{pmatrix}$.

MÉTHODE

1. La marche aléatoire apparaît clairement comme périodique ; le calcul de A^3 le prouve.

La suite (u_n), définie pour tout $n \geqslant 0$ par $u_n = a_n - \frac{1}{3}$, est géométrique de raison $-0{,}5$ car, pour tout $n \geqslant 0$:

$$a_{n+1} - \frac{1}{3} = 0{,}5b_n + 0{,}5c_n - \frac{1}{3} = 0{,}5(1 - a_n) - \frac{1}{3}$$
$$= -0{,}5a_n + \frac{1}{6} = -0{,}5\left(a_n - \frac{1}{3}\right).$$

La suite (u_n) converge alors vers 0 donc la suite (a_n) converge vers $\frac{1}{3}$.

Le même type de raisonnement permet de montrer que les suites (b_n) et (c_n) convergent vers $\frac{1}{3}$, donc la suite (X_n) converge vers $\begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix}$.

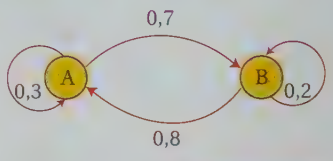
Exercices 16 à 17 p. 142

MÉTHODE

2. Le calcul des premiers termes permet de conjecturer la convergence vers 1/3 de la suite des probabilités pour chaque sommet.
La suite auxiliaire (u_n) introduite est géométrique de raison q avec $-1 < q < 1$, donc elle converge vers 0.
Cela permet d'en déduire la convergence de la suite (a_n) puisque, pour tout $n \geqslant 0$, $a_n = u_n + \frac{1}{3}$.

Savoir-faire 4 — Déterminer l'état stable limite d'une marche aléatoire sur un graphe probabiliste d'ordre 2

ÉNONCÉ On considère une marche aléatoire sur le graphe à 2 sommets :
À chaque pas, la probabilité de passer de A à B est 0,7 et la probabilité de passer de B à A est 0,8.
Étudier la convergence de cette marche aléatoire.



SOLUTION

Comme $0 < 0{,}8 < 1$ et que $0 < 0{,}7 < 1$, la marche aléatoire converge quel que soit l'état initial vers un état stable pour le graphe.

- **Recherche des états stables**

L'état $X = \begin{pmatrix} a \\ b \end{pmatrix}$ est stable pour cette marche aléatoire pour X solution de : $X = MX \Leftrightarrow (I_2 - M)X = 0$ avec $I_2 - M$ non inversible car $M = \begin{pmatrix} 0{,}3 & 0{,}8 \\ 0{,}7 & 0{,}2 \end{pmatrix}$ donc $I_2 - M = \begin{pmatrix} 0{,}7 & -0{,}8 \\ -0{,}7 & 0{,}8 \end{pmatrix}$.

On recherche donc les solutions du système :

$$\begin{cases} 0{,}7a - 0{,}8b = 0 \\ -0{,}7a + 0{,}8b = 0 \end{cases} \Leftrightarrow \begin{cases} b = \frac{7}{8}a \\ b = \frac{7}{8}a \end{cases} \Leftrightarrow b = \frac{7}{8}a.$$

Les solutions sont les couples $\begin{pmatrix} a \\ \frac{7}{8}a \end{pmatrix}$ pour tout a réel.

MÉTHODE

D'après la propriété du cours, p. 137, sur les graphes probabilistes d'ordre 2, la suite des matrices colonnes (X_n) *état de la marche aléatoire,* donnant les probabilités d'arrivée en chaque sommet après n pas, est une suite convergente quel que soit l'état initial X_0 et la limite est un état stable pour le graphe probabiliste.
La matrice $I_2 - M$ n'est pas inversible. On recherche donc l'état stable limite en utilisant les deux conditions qui suffisent à déterminer un état stable limite unique :
$\begin{pmatrix} a \\ b \end{pmatrix}$ est stable (système à écrire) et $a + b = 1$.

- **Une autre condition pour l'état limite**

Les coefficients de l'état stable $\begin{pmatrix} a \\ b \end{pmatrix}$ recherché vérifient de plus $a + b = 1$, puisque la somme de la probabilité d'être en A et de la probabilité d'être en B est égale à 1 à chaque pas.

On résout donc l'équation $a + \frac{7}{8}a = 1 \Leftrightarrow a = \frac{8}{15}$

L'état stable de ce graphe probabiliste est donc $\begin{pmatrix} \frac{8}{15} \\ \frac{7}{15} \end{pmatrix}$, ce qui signifie ici que **quel que soit l'état initial de la marche aléatoire**, les probabilités d'être en A et en B tendent respectivement vers 8/15 et 7/15.

Exercices 28 à 30 p. 143

Exercices d'application

Suites et matrices

Pour les exercices 1 à 4

Pour les suites définies, traduire la relation de récurrence par une égalité matricielle du type $X_{n+1} = AX_n$ en explicitant X_n et A. Donner la matrice colonne correspondant aux premiers termes :

1 (u_n) et (v_n) définies par : $u_0 = 7$ et $v_0 = -2$ et, pour tout $n \geqslant 0$:

$$u_{n+1} = 15u_n + 3v_n \text{ et } v_{n+1} = 1{,}2\,u_n + 8v_n.$$

2 (u_n) et (v_n) définies par : $u_0 = 3$ et $v_0 = 25$ et, pour tout $n \geqslant 0$:

$$v_{n+1} = 2\,u_n + 5v_n \text{ et } u_{n+1} = 0{,}5u_n - 3v_{n+1}.$$

3 (u_n) définie par $u_0 = 13$, $u_1 = -1$ et, pour tout $n \geqslant 0$:

$$u_{n+2} = -1{,}5u_{n+1} + 4u_n.$$

4 (u_n) définie par $u_0 = 0{,}5$; $u_1 = 1$, $u_2 = -7$ et, pour tout $n \geqslant 1$, $u_{n+2} = 1{,}5u_{n+1} + 2u_n - 3u_{n-1}$.

Pour les exercices 5 et 6

Pour les suites définies, traduire la relation de récurrence par une égalité matricielle du type $X_{n+1} = AX_n + B$ en explicitant X_n, A et B.

5 (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$$u_{n+1} - 0{,}25 = 0{,}5u_n - 0{,}8v_n$$
$$\text{et } v_{n+1} = 0{,}7u_n + 0{,}4v_n + 0{,}3.$$

6 (u_n) vérifiant, pour tout $n \geqslant 0$, $u_{n+2} = 2u_n + 8u_{n+1} - 1$.

7 Dans une zone de marais, on s'intéresse à la population de libellules. On note p_0 la population initiale et p_n la population au bout de n années.
Des chercheurs utilisent la relation suivante pour déterminer la population de libellules :
pour tout $n \geqslant 0$, $P_{n+1} = AP_n$ où P_n désigne la matrice colonne $P_n = \begin{pmatrix} p_n \\ p_{n+1} \end{pmatrix}$ et $A = \begin{pmatrix} 0 & 1 \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$.
Montrer que ce modèle de calcul correspond à un accroissement annuel géométrique de la population de libellules.

8 Soit des suites de nombres réels (u_n) et (v_n) vérifiant pour tout $n \geqslant 0$:

$$u_{n+1} = 5u_n + 3v_n \text{ et } v_{n+1} = -2u_n + 6v_n.$$

a. On donne $u_0 = 1$ et $v_0 = 1$. Déterminer les termes u_6 et v_8 grâce au calcul matriciel.
b. On donne $u_6 = 1\,476\,330$ et $v_6 = -333\,492$.
Déterminer les termes u_0 et v_0 grâce au calcul matriciel.

Savoir-faire 1, p. 138

9 On considère une suite de nombres réels (u_n), vérifiant pour tout $n \geqslant 1$, $u_{n+1} = 0{,}2u_n - 0{,}6u_{n-1}$.
a. On donne $u_0 = 20$ et $u_1 = 10$.
Déterminer u_7 grâce au calcul matriciel.
b. On donne $u_5 = 9{,}68$ et $u_6 = -3{,}704$.
Déterminer u_0 grâce au calcul matriciel.

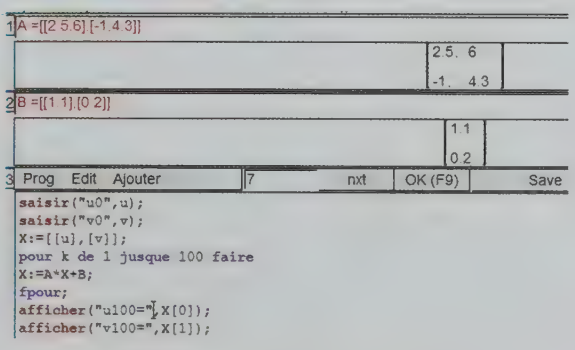
10 **Algorithmique** On considère des suites de nombres réels (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$$u_{n+1} = \frac{1}{4}u_n + 2v_n + 5 \text{ et } v_{n+1} = -5\,u_n + \frac{7}{3}v_n - 1.$$

Compléter l'algorithme suivant pour qu'il calcule et affiche u_{20} et v_{20}, pour u_0 et v_0 entrés par l'utilisateur.

```
Entrées :
u : nombre réel
v : nombre réel
Sorties :
.....
début
    pour i de 1 à 20 faire
        w prend la valeur u
        u prend la valeur .....
        v prend la valeur .....
    fin pour
    Afficher : « les valeurs de u20 et v20 sont »
    Afficher .....
    Afficher .....
fin
```

11 **Algorithmique** Déterminer ce que fait l'algorithme suivant formulé avec le logiciel **Xcas** :



12 On considère des suites de nombres réels (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$$u_{n+1} = 0{,}5u_n - 3v_n + 7 \text{ et } v_{n+1} = u_n - 2v_n - 5.$$

On donne $u_5 = -14{,}5$ et $v_5 = -52$.

Déterminer les termes u_0 et v_0.

13 On considère des suites de nombres réels (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$$u_{n+1} = u_n + 2v_n \text{ et } v_{n+1} = 2u_n + v_n.$$

a. Montrer que la suite (w_n) définie par $w_n = u_n + v_n$ est géométrique. Exprimer w_n en fonction de u_0, v_0 et n.

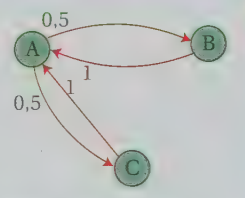
b. Montrer que la suite (t_n) définie par $t_n = u_n - v_n$ est géométrique. Exprimer t_n en fonction de u_0, v_0 et n.

c. En déduire l'expression du terme général de chacune des suites (u_n) et (v_n) en fonction de u_0, v_0 et n.

d. Soit la matrice carrée $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Déterminer les coefficients de la matrice A^n en fonction de n.

Comportement asymptotique

14 Un mobile se déplace sur le graphe probabiliste ci-contre:



a. Donner la matrice carrée M de transition associée à cette marche aléatoire.

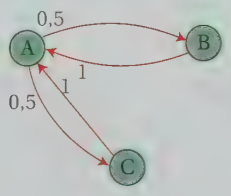
b. Montrer que si le mobile part de A, la marche aléatoire n'est pas convergente.

c. Que peut-on dire du comportement de cette marche aléatoire si le mobile part de B ou de C ?

Savoir-faire 3, p. 11

15 Un mobile se déplace sur le graphe ci-dessous de la façon suivante à chaque instant :

- avec une probabilité de 0,4, le mobile suit une des arêtes du graphe probabiliste issues du sommet où il est situé;
- Sinon, le mobile saute aléatoirement de façon équirépartie sur un des 3 sommets.



On considère, pour $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$ donnant les probabilités que le mobile soit situé en chacun des sommets, n instants après le départ.

On suppose que le mobile est initialement au sommet A.

1. Déterminer une matrice carrée M et une matrice colonne N telles que l'on puisse écrire, pour tout $n \geqslant 0$:

$$X_{n+1} = M \times X_n + N.$$

2. Déterminer X_1, X_2 et X_3.

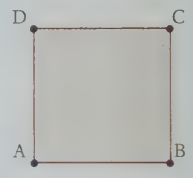
3. a. Démontrer que, pour tout $n \geqslant 0$, $b_n = c_n$.

b. En déduire que, pour tout $n \geqslant 0$, $b_n = \dfrac{1 - a_n}{2}$.

4. Montrer que la suite (u_n) définie, pour tout $n \geqslant 0$, par $u_n = a_n - \dfrac{3}{7}$ est géométrique de raison $(-0{,}4)$.

5. En utilisant les résultats précédents, démontrer que la marche aléatoire converge et déterminer son état limite.

16 Soit un carré ABCD et la marche aléatoire suivante :



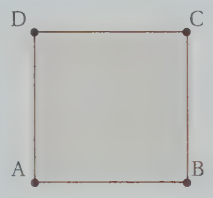
à partir de chaque sommet du carré, on peut emprunter une des arêtes vers un autre sommet de manière équiprobable.

Étudier le comportement asymptotique de cette marche aléatoire.

17 Un mobile se déplace sur les sommets du carré ABCD ci-dessous de la façon suivante :

À chaque instant :

- 4 fois sur 5, le mobile suit de façon équirépartie une des arêtes issues du sommet où il est situé ;
- le reste du temps le mobile saute aléatoirement de façon équirépartie sur un des 4 sommets du carré.



On considère, pour $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} a_n \\ b_n \\ c_n \\ d_n \end{pmatrix}$ donnant les probabilités que le mobile soit situé en chacun des sommets, n instants après le départ.

On suppose que le mobile est initialement au sommet A.

a. Déterminer une matrice carrée M et une matrice colonne N telles que l'on puisse écrire, pour tout $n \geqslant 0$:

$$X_{n+1} = M \times X_n + N.$$

b. Déterminer X_1, X_2 et X_3.

c. Démontrer que, tout $n \geqslant 1$, $a_n = c_n$ et $b_n = d_n$.

d. Justifier que, pour tout $n \geqslant 1$, $a_n + b_n = 0{,}5$.

e. Montrer que la suite (u_n) définie, pour tout $n \geqslant 0$, par $u_n = a_n - b_n$ est géométrique de raison $(-0{,}8)$.

Exprimer u_n en fonction n.

f. En utilisant les résultats précédents, démontrer que la marche aléatoire converge et déterminer son état limite.

18 On considère des suites de nombres réels (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$u_0 = 1$ et $v_0 = 1$

$u_{n+1} = 14u_n - 18v_n$ et $v_{n+1} = 9u_n - 11{,}5v_n$.

1. Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$ alors déterminer la matrice carrée A telle que les relations de récurrence ci-dessus s'écrivent, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.

2. a. Vérifier que la matrice A est égale au produit des matrices $P \times D \times P^{-1}$, où $D = \begin{pmatrix} 2 & 0 \\ 0 & 0{,}5 \end{pmatrix}$ est une matrice diagonale et $P = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$ est une matrice inversible .

b. En déduire que, pour tout $n \geqslant 0$:

$$X_n = (P \times D^n \times P^{-1})X_0.$$

3. a. Déduire de ce qui précède le terme général des suites (u_n) et (v_n).

b. Déterminer les limites des deux suites.

19 On considère des suites de nombres réels (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$u_0 = 5$ et $v_0 = 6$

$u_{n+1} = -0{,}1u_n + 0{,}8v_n$ et $v_{n+1} = -0{,}4u_n + 1{,}1v_n$.

1. Si on définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$ alors déterminer la matrice carrée A telle que les relations de récurrence ci-dessus s'écrivent, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.

2. a. Vérifier que la matrice A est égale au produit des matrices $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 0{,}3 & 0 \\ 0 & 0{,}7 \end{pmatrix}$ et où P désigne la matrice inversible $P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

b. En déduire que, pour tout $n \geqslant 0$: $X_n = (P \times D^n \times P^{-1})X_0$.

3. Déduire de ce qui précède les limites des suites (u_n) et (v_n).

Convergence et état stable

Pour les exercices 20 et 21

Pour chacune des matrices M :

- déterminer si l'équation $MX = X$ a une unique matrice colonne solution ;
- déterminer la (ou les) matrice(s) colonne(s) solutions.

20 **a.** $M = \begin{pmatrix} 5 & 2{,}5 \\ 0{,}4 & 1 \end{pmatrix}$ **b.** $M = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$

21 **a.** $M = \begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix}$ **b.** $M = \begin{pmatrix} 0{,}3 & 0{,}85 \\ 0{,}7 & 0{,}15 \end{pmatrix}$

22 Pour chacune des matrices M :

- écrire la matrice $I_3 - M$ et déterminer si elle est inversible (on peut utiliser une calculatrice) ;
- en déduire le nombre de matrices colonnes solutions de l'équation $MX = X$;
- déterminer la (ou les) matrices colonnes solutions.

a. $M = \begin{pmatrix} 5 & 6 & 2 \\ 0 & 11 & 4 \\ 2 & 0 & 1 \end{pmatrix}$ **b.** $M = \begin{pmatrix} 5 & 4 & 4 \\ 1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$

23 Soit une suite de matrices colonnes (X_n) telle que, pour tout $n \geqslant 0$:

$$X_{n+1} = AX_n + C \text{ où } A = \begin{pmatrix} 6 & -2 \\ 3 & -3 \end{pmatrix} \text{ et } C = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$$

Déterminer s'il existe une telle suite (X_n) qui soit constante. Si oui, donner les toutes.

▸ Savoir-faire 2, p. 138

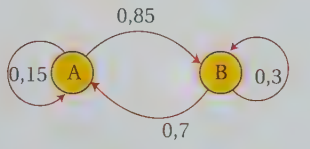
24 Même exercice avec $A = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$ et $C = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$

25 Même exercice avec $A = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$ et $C = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

26 Même exercice avec $A = \begin{pmatrix} 2 & 2 & 3 \\ 5 & 5 & 6 \\ 2 & 1 & 3 \end{pmatrix}$ et $C = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$

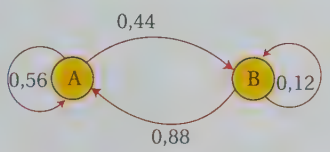
27 Même exercice avec $A = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & 4 & 6 \end{pmatrix}$ et $C = \begin{pmatrix} 1 \\ 1 \\ 5 \end{pmatrix}$

28 On considère une marche aléatoire sur le graphe probabiliste suivant.

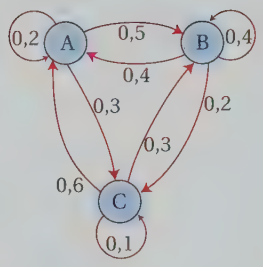


Déterminer l'état stable $X = \begin{pmatrix} a \\ b \end{pmatrix}$ de cette marche aléatoire.

29 Même exercice pour le graphe probabiliste :



30 Même exercice pour le graphe probabiliste ci-contre :



31 *D'après Bac ES*

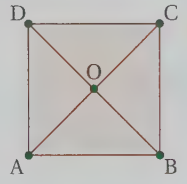
La population d'une ville se répartit entre locataires et propriétaires. La population globale ne varie pas mais, chaque année, pour raisons familiales ou professionnelles, 10 % des propriétaires deviennent locataires tandis que 20 % des locataires deviennent propriétaires.

L'évolution des populations de propriétaires et de locataires s'apparente à une marche aléatoire sur un graphe probabiliste à deux sommets.

1. Représenter ce graphe et écrire la matrice de transition M de cette marche aléatoire.

2. Déterminer l'état stable de la marche aléatoire. Interpréter le résultat.

32 **Algorithmique** Soit une marche aléatoire sur la figure ci-dessous.



À partir de chaque sommet, on peut emprunter une des arêtes vers un autre sommet de manière équiprobable.

1. On s'intéresse aux passages en O lors d'une marche aléatoire sur ce graphe.

a. Si, à l'étape i de la marche aléatoire, on est sur un des sommets du carré, quelle est la probabilité de se trouver en O à l'étape suivante ?

Que se passe-t-il si on est en O à l'étape i ?

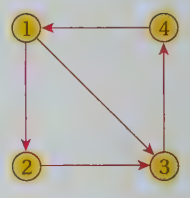
b. Compléter l'algorithme de simulation suivant où la variable « *compteur* » détermine le nombre de passages en O pour une marche de 5 000 pas démarrant en A.

```
Début
  être_en_O prend la valeur 0
  compteur prend la valeur 0
  Pour i de 1 à 5000 faire
      Si être_en_O = 0
          alors choisir un nombre au hasard p dans
          {0 ;1 ;2}
              Si p = 0
                  alors compteur prend la valeur
                        compteur + 1
                        être_en_O prend la valeur .....
                  sinon être_en_O prend la valeur .....
              Fin si
          sinon être_en_O prend la valeur .....
      Fin si
  Fin pour
  afficher compteur
Fin
```

c. Programmer cet algorithme et l'exécuter plusieurs fois.

2. On suppose que la marche aléatoire converge quel que soit son sommet de départ. Déterminer les probabilités d'arrivée en chaque sommet.

33 On considère une marche aléatoire sur le graphe ci-contre.



À chaque sommet, on emprunte une arête orientée vers un autre sommet, de façon équirépartie s'il y en a plusieurs.

On admet que cette marche aléatoire converge quel que soit le sommet de départ.

Que peut-on dire des probabilités d'arrivée sur chaque sommet ?

Exercices d'approfondissement

34 **Flux entre deux aquariums**

Deux aquariums A et B d'un magasin d'aquariophilie sont communicants.

On a constaté que chaque jour 80 % des poissons de l'aquarium A passent dans l'aquarium B et que 45 % des poissons de l'aquarium B passent dans l'aquarium A.

On définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$

où a_n désigne la population de poissons de l'aquarium A et b_n désigne la population de poissons de l'aquarium B, n jours après le premier jour d'observation.

On suppose que le premier jour d'observation les populations de poissons sont équiréparties entre les deux aquariums.

1. Déterminer la matrice carrée M telle que, pour tout $n \geqslant 0$, $X_{n+1} = MX_n$.

2. Déterminer un état X stable pour les flux de circulation des poissons entre les deux aquariums.

3. a. Vérifier que $M = P - 0{,}25Q$ où P et Q sont les matrices suivantes :

$$P = \begin{pmatrix} 0{,}36 & 0{,}36 \\ 0{,}64 & 0{,}64 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 0{,}64 & -0{,}36 \\ -0{,}64 & 0{,}36 \end{pmatrix}$$

b. Calculer $P \times Q$ et $Q \times P$.

c. Justifier que, pour tout $n \geqslant 1$, $P^n = P$ et $Q^n = Q$.

d. Démontrer que, pour tout $n \geqslant 1$, $M^n = P + (-0{,}25)^n Q$.

4. Montrer que $a_n > 0{,}35$ pour tout $n \geqslant 2$.

Interpréter ce résultat.

35 **Perturbation d'un équilibre** (*D'après F. Liret, Maths en pratique*)

Dans des conditions stables, deux espèces A et B de bactéries vivent en symbiose à des concentrations moyennes a et b.

On déplace l'équilibre en augmentant la concentration de A et celle de B, puis on mesure chaque jour l'écart en pourcentage par rapport à l'équilibre des concentrations de chaque espèce. Au bout de n jours cet écart est noté u_n pour la bactérie A et v_n pour la bactérie B. Une modélisation a conduit à la loi d'évolution suivante :

$$\begin{cases} u_{n+1} = \dfrac{3u_n - 6v_n}{5} \\ v_{n+1} = \dfrac{2u_n + 3v_n}{5} \end{cases} \text{ pour tout } n \geqslant 0$$

1. Si on note $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$, déterminer la matrice carrée telle que, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.

2. La matrice A est-elle inversible ? Montrer que si les concentrations de A et de B retrouvent un équilibre, ce ne peut être que pour les valeurs initiales a et b.

3. On déplace l'équilibre en augmentant de 18 % la concentration de A et de 12 % celle de B, donc les conditions initiales sont $\begin{cases} u_0 = 0{,}18 \\ v_0 = 0{,}12 \end{cases}$.

Calculer les premiers termes des suites (u_n) et (v_n).

Que peut-on dire des variations des écarts en concentration par rapport aux concentrations à l'équilibre ?

Les suites (u_n) et (v_n) semblent-elles convergentes ?

4. On définit, pour tout $n \geqslant 0$, la suite (d_n) par :

$$d_n = {u_n}^2 + 3{v_n}^2.$$

a. Montrer que (d_n) est une suite géométrique de raison 0,84.

b. En déduire que les suites (u_n) et (v_n) convergent vers 0. Conclure sur la perturbation de l'équilibre.

36 **Des proies et des prédateurs.**

Dans les montagnes du Devoluy, les rapaces mangent les souris.

On recense chaque année ces populations.

Si on désigne par (u_n) et (v_n) les deux suites de populations de prédateurs et de proies n années après le premier recensement, on a pu établir que, pour tout $n \geqslant 0$,

$$u_{n+1} = 0{,}4u_n + 0{,}3v_n \text{ et } v_{n+1} = -pu_n + 1{,}2v_n$$

où p est un paramètre appelé paramètre de prédation.

À l'aide d'un tableur, on a observé l'évolution des populations de rapaces et de souris sur une longue durée et ceci pour trois valeurs différentes du paramètre de prédation (voir écran ci-dessous). Les populations initiales sont $u_0 = 100$ et $v_0 = 100$.

1. Retrouver les trois valeurs différentes p_1, p_2 et p_3 du paramètre de prédation.

2. Pour chaque valeur du paramètre de prédation, émettre une conjecture sur le comportement à long terme des suites de prédateurs et de proies.

3. Pour la valeur p_3 du paramètre de prédation, on admet que les deux suites convergent.

Montrer qu'il faut alors s'attendre à l'extinction des deux espèces et ceci quelles que soient les populations initiales.

4. Pour la valeur p_2 du paramètre de prédation, on admet que les deux suites convergent.

Montrer qu'à long terme, les populations de prédateurs et de proies se stabilisent de telle sorte que les proies sont toujours deux fois plus nombreuses que les prédateurs et ceci quelles que soient les populations initiales.

	A	B	C	D	E	F	G	H	I	J
1			paramètre de prédation:			paramètre de prédation:			paramètre de prédation:	
2			$p1$ = ?			$p2$ = ?			$p3$ = ?	
3	n		Un (prédateurs)	Vn (proies)		Un (prédateurs)	Vn (proies)		Un (prédateurs)	Vn (proies)
4	0		100	100		100	100		100	100
5	1		70	90		70	80		70	70
6	2		55	87		52	68		49	49
7	3		48,1	87,9		41,2	60,8		34,3	34,3
8	4		45,61	91,05		34,72	56,48		24,01	24,01
9	5		45,559	95,577		30,832	53,888		16,807	16,807
10	6		46,8967	101,0247		28,4992	52,3328		11,7649	11,7649
11	7		49,06609	107,16063		27,09952	51,39968		8,23543	8,23543
12	8		51,774625	113,872929		26,259712	50,839808		5,764801	5,764801
13	9		54,8717287	121,115127		25,7558272	50,5038848		4,0353607	4,0353607
14	10		58,28322967	128,876634		25,45349632	50,30233088		2,82475249	2,82475249
15	11		61,97628211	137,166992		25,27209779	50,18139853		1,977326743	1,977326743
16	12		65,94061047	146,007506		25,16325868	50,10883912		1,38412872	1,38412872
17	13		70,17849595	155,426824		25,09795521	50,06530347		0,968890104	0,968890104
18	14		74,69944555	165,45864		25,05877312	50,03918208		0,678223073	0,678223073
19	15		79,51737018	176,140534		25,03526387	50,02350925		0,474756151	0,474756151
20	16		84,64910833	187,51343		25,02115832	50,01410555		0,332329306	0,332329306
21	17		90,11367233	199,621383		25,01269499	50,00846333		0,232630514	0,232630514
22	18		95,93188398	212,511558		25,007617	50,005078		0,16284136	0,16284136
23	19		102,1262211	226,234305		25,0045702	50,0030468		0,113988952	0,113988952
24	20		108,7207799	240,8433		25,00274212	50,00182808		0,079792266	0,079792266
25	21		115,7413019	256,395726		25,00164527	50,00109685		0,055854586	0,055854586
26	22		123,2152384	272,95248		25,00098716	50,00065811		0,03909821	0,03909821
27	23		131,1718394	290,578405		25,0005923	50,00039487		0,027368747	0,027368747
28	24		139,6422572	309,342534		25,00035538	50,00023692		0,019158123	0,019158123
29	25		148,659663	329,318363		25,00021323	50,00014215		0,013410686	0,013410686

exercice 36

37 Fumeurs/Non-fumeurs (*D'après bac ES*)

On a divisé une population en deux catégories : « fumeurs » et « non-fumeurs ». Une étude statistique a permis de constater que, d'une génération à l'autre :

- 60 % des descendants de fumeurs sont des fumeurs,
- 10 % des descendants de non-fumeurs sont des fumeurs.

On suppose que le taux de fécondité des fumeurs est le même que celui des non-fumeurs. On désigne par :

- f_n le pourcentage de fumeurs à la génération de rang n,
- $g_n = 1 - f_n$ le pourcentage de non-fumeurs à la génération de rang n, où n est un entier naturel.

On considère qu'à la génération 0, il y a autant de fumeurs que de non-fumeurs. On a donc $f_0 = g_0 = 0{,}5$.

1. La situation s'apparente à une marche aléatoire sur un graphe probabiliste à deux sommets. Représenter ce graphe et écrire la matrice de transition M.

2. Déterminer le pourcentage de fumeurs à la génération de rang 2.

3. Déterminer l'état probabiliste stable et l'interpréter.

4. Montrer que, pour tout entier naturel n :

$$f_{n+1} = 0{,}5f_n + 0{,}1.$$

5. On pose, pour tout entier naturel n, $u_n = f_n - 0{,}2$.

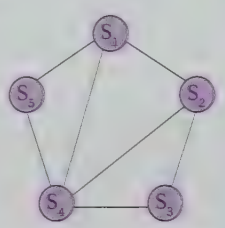
a. Montrer que la suite (u_n) est une suite géométrique dont on précisera le premier terme et la raison.

b. Donner l'expression de u_n puis de f_n en fonction de n.

c. Déterminer la limite de la suite (f_n) lorsque n tend vers $+\infty$ et l'interpréter.

38 Degrés des sommets d'un graphe

Le graphe ci-contre est formé de 5 sommets. On considère la marche aléatoire suivante : à partir d'un sommet, on emprunte de manière équiprobable une des arêtes le reliant à un autre sommet.



1. Écrire la matrice de transition M d'un état à un autre pour cette marche aléatoire.

2. À l'aide d'une calculatrice, observer les premiers termes de la suite des matrices colonnes états de la marche aléatoire lorsque l'on part du sommet S_1.
Cette suite semble-t-elle converger ? Conjecturer un état limite pour cette suite.

3. On note A le nombre d'arêtes de ce graphe et, pour chaque sommet S_i de ce graphe, on appelle degré de S_i et on note $\deg(S_i)$ le nombre d'arêtes issues de ce sommet.

a. Montrer qu'un état stable de cette marche aléatoire est la matrice colonne X dont le coefficient de la ligne i est $\dfrac{\deg(S_i)}{2A}$.

b. Comparer ce résultat avec la conjecture émise à la question **2**.

39 Algorithmique Limite d'une suite

On considère une suite de nombres réels (u_n) définie par :

$u_0 = a$ et $u_1 = a$ pour a nombre réel fixé

$u_{n+2} = 5u_{n+1} - 6u_n$ pour tout $n \geqslant 0$.

On définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}$.

1. Écrire un algorithme qui, pour une valeur de a entrée par l'utilisateur, calcule les premiers termes de la suite (u_n) et faire une conjecture sur la limite de cette suite selon les valeurs de a.

2. Écrire le vecteur X_0 en fonction de a.
Montrer que, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$ où A désigne la matrice carrée : $\begin{pmatrix} 0 & 1 \\ -6 & 5 \end{pmatrix}$.

3. a. Vérifier que les matrices carrées $P = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ et $Q = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$ sont inverses l'une de l'autre.

b. Montrer que la matrice A est égale au produit des matrice $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ et où $P^{-1} = Q$ d'après la question précédente.

4. a. À l'aide d'un raisonnement par récurrence, démontrer que, pour tout $n \geqslant 0$, $X_n = (P \times D^n \times P^{-1})X_0$.

b. Pour $n \geqslant 0$, exprimer en fonction de n la matrice D^n.

5. En déduire que, pour tout $n \geqslant 0$, $u_n = a \times (2 \times 2^n - 3^n)$.

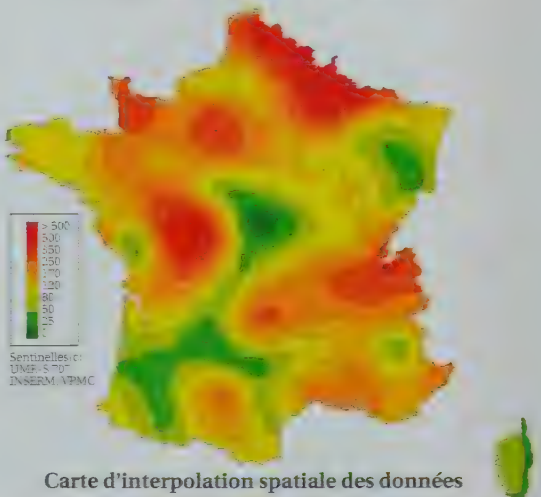
6. Montrer la conjecture établie pour la limite à la question **1**.

40 Une épidémie

Lors d'une épidémie de grippe A en France, les autorités sanitaires ont pu constater qu'un individu peut être :

- soit malade,
- soit immunisé car ayant déjà contracté une forme assez proche du virus,
- soit ni malade ni immunisé.

Grippe Semaine 200940
en nombre de cas pour 100 000 habitants



Carte d'interpolation spatiale des données
basée sur les incidences départementales

De plus d'une semaine à l'autre :

- une personne malade le sera encore avec une probabilité de 0,4 sinon elle est guérie et immunisée ;
- une personne immunisée a une probabilité de 0,1 de perdre cette immunisation donc de passer à l'état ni malade ni immunisé car le virus se transforme légèrement ;
- une personne ni malade ni immunisée tombe malade avec une probabilité de 0,3.

La première semaine du mois de septembre 2009, le centre de veille sanitaire estime que 1 % de la population est malade et 10 % de la population est immunisée.

On considère, pour $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} m_n \\ i_n \\ r_n \end{pmatrix}$ donnant, n semaines après la première observation, les proportions d'individus malades, immunisés ou ni l'un ni l'autre.

1. Donner le vecteur X_0. Déterminer la matrice carrée A telle que, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.

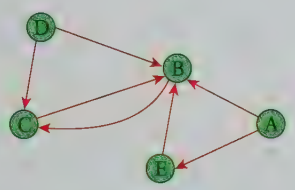
2. a. À l'aide d'une calculatrice, faire un bilan sur la population les six premières semaines après la première observation.

b. Le ministère décide de lancer une grande campagne de vaccination si les prévisions conduisent à une probabilité supérieure à 10 % pour qu'un individu soit malade. D'après les premières observations, la campagne de vaccination sera-t-elle lancée ?

3. On admet que la suite de matrices colonnes (X_n) converge vers une matrice colonne constante.
Quelle relation doit vérifier cette matrice colonne ?
Déterminer cette matrice colonne.
Dans les conditions de cette modélisation, la campagne de vaccination est-elle maintenue ?

41 Une marche aléatoire

On considère une marche aléatoire sur le graphe suivant : à chaque sommet, on emprunte une arête orientée vers un autre sommet, de façon équirépartie s'il y en a plusieurs.



Étudier le comportement asymptotique de cette marche aléatoire.
(Distinguer les cas selon le sommet de départ – on pourra commencer par observer les premiers pas au tableur.)

42 Partie de fléchettes *(D'après bac ES)*

Lors d'une partie de fléchettes, un joueur envoie une à une des fléchettes vers une cible.

La tentative est réussie quand la fléchette atteint la cible, elle échoue dans le cas contraire.
Pour la 1re fléchette, les chances de réussite ou d'échec sont égales.
Pour chaque lancer suivant, la probabilité qu'il réussisse dépend uniquement du résultat du lancer précédent :

- elle est de 0,7 quand le lancer précédent atteint la cible ;
- elle est de 0,4 quand il a échoué.

On note :

- C_n l'événement « la n-ième fléchette atteint la cible »,
- E_n l'événement « le n-ième lancer a échoué ».

1. La partie ne comporte que deux fléchettes.
Traduire la situation à l'aide d'un arbre pondéré.
En déduire la probabilité pour que la 2de fléchette atteigne la cible.

Dans toute la suite de l'exercice, n désigne un entier supérieur ou égal à 1 et on considère que le jeu se déroule avec n fléchettes.
On désigne par c_n la probabilité d'atteindre la cible lors du n-ième lancer et par e_n la probabilité que ce lancer échoue.

On note $P_n = \begin{pmatrix} c_n \\ e_n \end{pmatrix}$ la matrice colonne qui traduit l'état probabiliste lors du n-ième lancer.

La matrice $P_1 = \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix}$ traduit donc l'état probabiliste initial lors du 1er lancer.

2. a. Cette situation s'apparente à une marche aléatoire sur un graphe probabiliste à 2 sommets.
Dessiner ce graphe et donner la matrice de transition, notée A, associée à cette marche aléatoire.

b. Donner l'état P_2.

3. a. À l'aide de la relation $P_{n+1} = A \times P_n$ où A est la matrice de transition, exprimer la probabilité c_{n+1} d'atteindre la cible lors du $(n+1)$-ième lancer en fonction des probabilités c_n et e_n.

b. Montrer que, pour tout entier $n \geqslant 1$, on a :

$$c_{n+1} = 0{,}3c_n + 0{,}4.$$

4. Soit la suite (u_n) définie, pour tout entier naturel $n \geqslant 1$, par $u_n = c_n - \frac{4}{7}$.

a. Montrer que la suite (u_n) est une suite géométrique de raison 0,3.

b. En déduire u_n, puis c_n en fonction de n.

c. Calculer la limite de c_n quand n tend vers l'infini. Interpréter cette limite.

Activités de recherche et résolution de problèmes

Travaux pratiques avec l'outil informatique

Thèmes d'étude du chapitre

43 Un effet papillon

Soit deux suites (u_n) et (v_n) vérifiant, pour tout $n \geqslant 0$:

$$u_{n+1} = 0{,}8u_n + 3 \text{ et } v_{n+1} = -0{,}6\,u_n + 1{,}25v_n + 4.$$

1. Dans chaque cas, calculer les 100 premiers termes de chaque suite pour les valeurs initiales données et émettre une conjecture sur la convergence de chaque suite.
   a. $u_0 = 2$ et $v_0 = 5$ **b.** $u_0 = 5$ et $v_0 = 2$ **c.** $u_0 = 3$ et $v_0 = 4$ **d.** $u_0 = 6$ et $v_0 = 8$
2. Si on pose $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$, déterminer la matrice carrée A et le vecteur colonne B tels que pour tout $n \geqslant 0$, $X_{n+1} = AX_n + B$.
3. Dans le cas où les deux suites sont convergentes, montrer que les limites sont indépendantes des valeurs de u_0 et de v_0 , puis déterminer ces limites.
4. **a.** Montrer que la suite (w_n) définie, pour tout $n \geqslant 0$, par $w_n = u_n - 15$ est géométrique de raison 0,8.
   b. Exprimer alors le terme général u_n en fonction de n et de u_0.
   c. En déduire que, quelle que soit la valeur de u_0, la suite (u_n) converge et donner sa limite.
5. **a.** Montrer que, pour tout $n \geqslant 0$:
   $(3v_{n+1} - 4u_{n+1})w_{n+1} = (3v_n - 4u_n)w_n$.
   b. En déduire que, pour tout $n \geqslant 0$:
   $(3v_n - 4u_n)w_n = (3v_0 - 4u_0)w_0$.
   c. Montrer que la suite (v_n) est convergente si et seulement si $3v_0 - 4u_0 = 0$.

L'effet papillon

En 1972, le météorologue américain Edward Lorenz fait une conférence intitulée : *« Prédictibilité : le battement d'ailes d'un papillon au Brésil peut-il provoquer une tornade au Texas ? »*. Cette conférence met en évidence la faillibilité des prévisions météorologiques sensibles à des variations infimes des conditions initiales. Dans une toute autre mesure, ce problème montre qu'en modifiant par exemple de 0,001 une des valeurs initiales, on peut passer d'une suite convergente à une suite divergente.

44 Un système proie-prédateur : points d'équilibre et stabilité

Dans un milieu où interagissent deux populations, on définit la suite de nombres réels (u_n) comme le nombre de proies et la suite (v_n) comme le nombre de prédateurs du milieu en fonction du nombre de jours n écoulés depuis le début de l'étude.

Le mathématicien italien Volterra (1860-1940) propose un des premiers modèles d'études de la dynamique de deux populations *proie-prédateur* pour expliquer le phénomène suivant. Lors de la Première guerre mondiale, l'interruption de la pêche de poissons pour commercialisation, dont les requins et sardines, a eu pour effet de modifier l'équilibre entre ces deux espèces dans la mer Adriatique. Suite à l'arrêt de la pêche commerciale, la population de requins (prédateurs) a augmenté alors que la population de sardines (proies) a diminué.

On suppose que, pour tout $n \geqslant 0$:

$$u_{n+1} - u_n = u_n(0{,}045 - 0{,}001v_n) \text{ et } v_{n+1} - v_n = v_n(-0{,}025 + 0{,}0002u_n)$$

Partie 1. Variations des nombres de proies et prédateurs

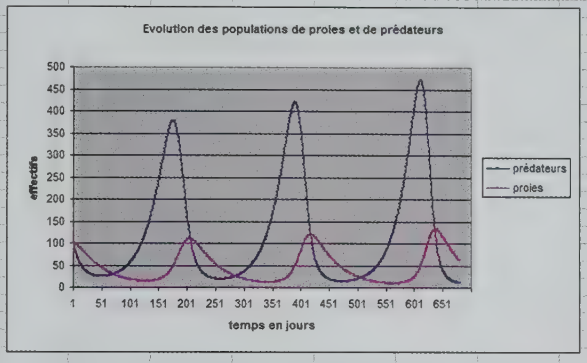
1 **a.** Montrer que ces relations impliquent qu'en l'absence de prédateurs, les proies augmentent et que cette augmentation est proportionnelle au nombre de proies.

b. Commenter de même la variation du nombre de prédateurs en l'absence de proies.

2 À l'aide d'un tableur, on a représenté les variations du nombre de proies et du nombre de prédateurs au cours du temps pour des populations initiales de 100 individus.

a. Quelles sont les formules entrées en B3 et C3 ?

	A	B	C
1	*n*	proies (Un)	prédateurs (Vn)
2	0	100	100
3	1	94,5	99,5
4	2	89,34975	98,89305
5	3	84,53441946	98,18793761
6	4	80,03820803	97,39329123
7	5	75,84474289	96,51749585
8	6	71,93741166	95,56862738
9	7	68,29963549	94,55440364
10	8	64,91508779	93,48214981
11	9	61,76786478	92,35877645
12	10	58,84261428	91,19076793
13	11	56,12462874	89,98417936
14	12	53,59990837	88,74464061
15	13	51,25519964	87,47736552
16	14	49,07801379	86,18716535
17	15	47,05662952	84,87846519
18	16	45,18008336	83,55532246
19	17	43,43815068	82,22144668
20	18	41,82131987	80,88022004
21	19	40,32076171	79,53471805
22	20	38,92829557	78,18773018
23	21	37,6363538	76,84177994
24	22	36,43794531	75,49914432
25	23	35,32661915	74,16187245



b. Commenter les représentations proposées en recopiant et en complétant la phrase : « Une hausse du nombre de proies est suivie dans le temps d'une ..... du nombre de prédateurs, qui entraîne conjointement une ..... du nombre de proies qui est suivie dans le temps d'une ..... du nombre de prédateurs et ce phénomène se répète de façon cyclique. »
Justifier d'un point de vue biologique ces constatations.

Partie 2. États d'équilibre ; déplacement de l'équilibre

1 On suppose à présent qu'on a atteint un équilibre et que les nombres de proies et de prédateurs sont constants au cours du temps.

a. Montrer qu'il existe uniquement deux couples $\begin{pmatrix} u \\ v \end{pmatrix}$ de suites constantes vérifiant le système proposé : le couple $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et un couple $\begin{pmatrix} a \\ b \end{pmatrix}$ que l'on explicitera.

b. On suppose que les deux suites de populations convergent. Que peut-on dire des limites de ces deux suites ? Justifier.

2 **Retour au problème historique**
On peut modéliser l'effet de la pêche commerciale par la modification des paramètres liés à la mortalité des espèces dans le système initial.
On suppose qu'avec l'effet de la pêche sur chaque espèce, les populations de proies et de prédateurs vérifient les relations modifiées :

$$u_{n+1} - u_n = u_n((0{,}045 - k) - 0{,}001v_n) \text{ et } v_{n+1} - v_n = v_n(-(0{,}025 + \ell) + 0{,}0002u_n)$$

où k et ℓ désignent des nombres réels strictement positifs.

a. On reprend les mêmes conditions initiales ($u_0 = v_0 = 100$).
Pour $k = \ell = 0{,}01$, représenter à l'aide d'un tableur sur un même graphique les nuages de points représentant les évolutions des populations de proies sans pêche commerciale et avec pêche commerciale. Faire de même pour les prédateurs.
Comparer ces observations avec le problème initial.
b. On suppose que les deux suites de populations, vérifiant le système modifié, convergent vers un état d'équilibre qui ne correspond pas à l'extinction des deux espèces. Déterminer cet état d'équilibre en fonction de k et ℓ.
c. Comparer ce nouvel état avec celui de la **question 1** et conclure par rapport au problème initialement posé.

Partie 3. Stabilité des états d'équilibre : linéarisation du problème

1 Un procédé appelé « linéarisation au voisinage du point d'équilibre » permet d'écrire que pour des populations initiales $\begin{pmatrix} u_0 \\ v_0 \end{pmatrix}$ proches de $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, on peut estimer que la matrice colonne $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$ des populations de proies et prédateurs vérifie pour tout $n \geqslant 0$:

$$X_{n+1} - X_n = AX_n \text{ où } A \text{ désigne la matrice carrée : } \begin{pmatrix} 0{,}045 & 0 \\ 0 & -0{,}025 \end{pmatrix}$$

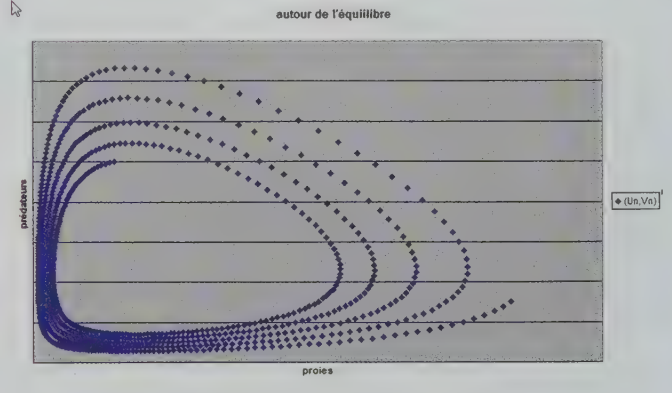
a. Exprimer $(I + \mathrm{A})^n$ en fonction de n.
b. En déduire u_n et v_n en fonction de u_0, v_0 et n.
c. Que peut-on dire du comportement des suites (u_n) et (v_n) lorsque n tend vers $+\infty$?
Interpréter le résultat en termes de proies et de prédateurs. (*Remarque* : on dit que le point d'équilibre $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ est instable.)

2 On suppose que le même procédé de « linéarisation au voisinage du point d'équilibre » permette d'écrire que, pour des populations initiales $\begin{pmatrix} u_0 \\ v_0 \end{pmatrix}$ proches de $\begin{pmatrix} a \\ b \end{pmatrix}$, on peut estimer cette fois que la matrice colonne $Y_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix} - \begin{pmatrix} a \\ b \end{pmatrix}$ vérifie $Y_{n+1} - Y_n = BY_n$ où B désigne la matrice carrée $\begin{pmatrix} -1 & -0{,}125 \\ 0{,}009 & -1 \end{pmatrix}$.

a. Calculer la matrice $(I + B)^2$.
b. En déduire que, pour tout $n \geqslant 0$:

$$u_{n+2} - a = -0{,}001\,125(u_n - a) \text{ et } v_{n+2} - b = -0{,}001\,125(v_n - b).$$

c. Commenter cette affirmation : « au voisinage du point d'équilibre $\begin{pmatrix} a \\ b \end{pmatrix}$, les populations de proies et prédateurs oscillent autour du point d'équilibre »



Note
La matrice B proposée dans ce problème ne correspond pas à la linéarisation réelle du système au voisinage de ce point d'équilibre. Avec des calculs plus complexes, la linéarisation réelle permet de conclure que les populations de proies et de prédateurs oscillent autour du point d'équilibre mais sans s'écarter ni retourner vers l'équilibre.

45 Évolution d'un caractère génétique, la diversité biologique en question

On s'intéresse à un caractère génétique du muflier (fleur plus communément appelée gueule de loup).
La couleur du muflier est déterminée par l'assemblage au moment de la fécondation de deux gènes hérités de deux « plantes parents » et qui peuvent être de type a et A.
Chaque « plante parent » cède à une « plante fille » un de ses deux gènes de façon équiprobable.

Un muflier ayant le génotype AA produit des fleurs rouges ; un muflier ayant le génotype Aa produit des fleurs mauves et un muflier ayant le génotype aa produit des fleurs blanches.

Une jardinerie possède de façon équirépartie les trois sortes de couleurs de mufliers.

Elle décide de cloisonner ses serres de façon à ce qu'une plante soit toujours fertilisée par une plante du même génotype qu'elle.

1 Montrer que deux « plantes-mères » ayant le génotype Aa peuvent donner une « plante fille » avec le génotype AA ou aa, avec une probabilité de 0,25 et « une plante fille » de génotype Aa avec une probabilité de 0,5.

2 Pour tout $n \geqslant 0$, on désigne par $X_n = \begin{pmatrix} r_n \\ m_n \\ b_n \end{pmatrix}$ la matrice colonne donnant les probabilités de répartition des fleurs par couleur après la n-ième fertilisation.

a. Donner la matrice colonne X_0.

b. Montrer que, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$ où A désigne la matrice carrée : $\begin{pmatrix} 1 & 0{,}25 & 0 \\ 0 & 0{,}5 & 0 \\ 0 & 0{,}25 & 1 \end{pmatrix}$.

c. Donner les probabilités de répartition des fleurs par couleur à la 4e génération.

3 **a.** Vérifier que les matrices carrées suivantes sont inverses l'une de l'autre :

$P = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & 1 & 1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 0{,}5 & 0 \\ 0 & 0{,}5 & 1 \\ 0 & -0{,}5 & 0 \end{pmatrix}$.

b. Montrer que la matrice A est égale au produit des matrices $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0{,}5 \end{pmatrix}$ et où $P^{-1} = Q$ d'après la question précédente.

c. Démontrer à l'aide d'un raisonnement par récurrence que, pour tout $n \geqslant 0$: $X_n = (P \times D^n \times P^{-1})X_0$.

d. Pour $n \geqslant 0$, exprimer en fonction de n la matrice D^n.

e. En déduire que les probabilités r_n, m_n et b_n de répartition des couleurs à la n-ième génération sont données en fonction de n par :

$$r_n = \frac{1}{3} + (0{,}5 - 0{,}5^{n+1}) \times \frac{1}{3},\ m_n = 0{,}5^n \times \frac{1}{3} \text{ et } b_n = (0{,}5 - 0{,}5^{n+1}) \times \frac{1}{3} + \frac{1}{3}$$

4 Quelles sont les limites de ces probabilités lorsque n tend vers $+\infty$?
Que peut-on en conclure ?
Justifier que ce cloisonnement des cultures ne favorise pas la diversité biologique.

46 Le problème des urnes d'Ehrenfest

Un paradoxe

L'expérience des urnes d'Ehrenfest est une expérience qui tend à lever un paradoxe de la thermodynamique.

- À l'échelle macroscopique un système évolue sans retour en arrière (réversibilité) possible. Par exemple, la chaleur se transmet du corps le plus chaud vers le corps le plus froid pour tendre vers un équilibre et l'inverse n'est pas possible.
- À l'échelle microscopique, selon les lois de la dynamique des particules, chaque particule a un comportement totalement réversible.

Cette expérience montre que la superposition des comportements de particules aux évolutions réversibles peut créer une situation macroscopique pour laquelle la réversibilité est impossible ou plutôt improbable (au moins dans notre échelle de temps).

Le couple de physiciens Paul et Tatiana Ehrenfest propose ce modèle en 1907 pour justifier certains des « paradoxes » apparus entre la théorie de la mécanique statistique naissante et la thermodynamique.

Partie 1. L'expérience simulée avec 100 boules

Soit deux urnes A et B et 100 boules réparties entre ces deux urnes (on ne fixe pas pour l'instant la répartition initiale).

À chaque instant, on prélève au hasard une des 100 boules et on la change d'urne. On observe alors l'évolution de la répartition des boules entre les deux urnes en fonction du temps.

Simulation de l'expérience à l'aide d'un tableur

Pour simuler le choix d'une boule parmi les 100 réparties dans les deux urnes suivant les conditions de cette expérience, on adopte le principe suivant :

À chaque instant, on choisit au hasard un nombre entre 1 et 100 ; si ce nombre est inférieur ou égal au nombre de boules dans A, on convient que c'est une boule de A et on la bascule dans B, sinon on convient que c'est une boule de l'urne B et on la bascule dans A.

On choisit au départ de mettre 50 boules dans l'urne A, et on observe le nombre de boules dans cette urne à chaque instant.

1. Créer les colonnes A, B et C d'une feuille de calcul comme ci-contre pour 200 tirages successifs et faire afficher la représentation de l'évolution du nombre de boules dans l'urne A. (On pourra aussi faire afficher le nombre de boules dans l'urne B.)

	A	B	C
1	instant	choix d'une boule	nombre de boules dans A
2	0		50
3	1	37	49
4	2	2	48
5	3	43	47
6	4	60	48
7	5	93	49
8	6	20	48
9	7	52	49

2. Faire afficher dans la colonne D de cette feuille de calcul les instants éventuels de réversibilité du système, c'est-à-dire les instants où on retrouve la répartition initiale. Puis faire afficher le temps de réversibilité de l'expérience, c'est-à-dire le premier instant pour lequel on retrouve la répartition initiale.

	A	B	C	D	E	F	G
1	instant	choix d'une boule	nombre de boules dans A	instants de réversibilité			
2	0		50				
3	1	37	49			temps de réversibilité	4
4	2	16	48				
5	3	56	49				
6	4	92	50	4			
7	5	62	51				
8	6	35	50	6			
9	7	21	49				

3. Modifier à plusieurs reprises le nombre initial de boules dans l'urne A (en prenant des valeurs plus ou moins éloignées de 50) et observer l'évolution du nombre de boules dans A en fonction du temps ? Que peut-on conjecturer ?

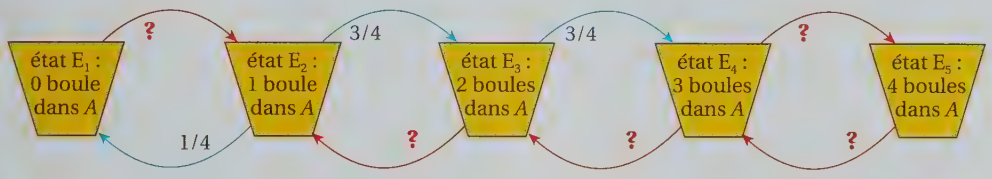
4. Observer également le temps de réversibilité pour différentes valeurs du nombre initial de boules dans l'urne A. Formuler une conclusion pour cette expérience par rapport au paradoxe qu'elle souhaitait expliquer.

Partie 2. L'expérience avec 4 boules

À présent, on considère l'expérience avec un total de quatre boules réparties entre les urnes A et B.
L'urne A peut ainsi contenir 0 boule (état 1), 1 boule (état 2), 2 boules (état 3), 3 boules (état 4) ou 4 boules (état 5).
Pour tout $n \geqslant 0$, on note X_n la matrice colonne donnant la probabilité de ces états à l'instant n. Par exemple :

si l'urne A contient trois boules au départ : $X_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ et l'égalité $X_2 = \begin{pmatrix} 0{,}5 \\ 0 \\ 0{,}5 \\ 0 \\ 0 \end{pmatrix}$ signifie qu'à

l'instant 2, l'urne A a la probabilité 0,5 de ne contenir aucune boule et la probabilité 0,5 de contenir 2 boules.
L'expérience des urnes d'Ehrenfest s'apparente à une marche aléatoire sur le graphe ci-dessous : les sommets de ce graphe représentent les états possibles de l'urne A et, sur les arêtes reliant ces sommets, les probabilités de transition entre ces états sont indiquées.



1 **a.** Justifier les valeurs des probabilités données sur ce graphe.

b. Compléter ce graphe par les probabilités manquantes.

c. Donner la matrice de transition associée à cette marche aléatoire, c'est-à-dire la matrice A telle que pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.

2 **a.** Lorsque les 4 boules sont situées au départ dans l'urne A, quelle est la probabilité d'être revenu à cet état initial après 1 tirage ? après 2 tirages ? après 3 tirages ? après 4 tirages ?

b. Même question pour une répartition initiale avec 2 boules dans chaque urne.
Comparer ces résultats.

3 **a.** Déterminer un état probabiliste X stable pour cette marche aléatoire.

b. Montrer que cette matrice colonne stable correspond à un état de répartition des boules suivant la loi binomiale de paramètres (4 ; 0,5).

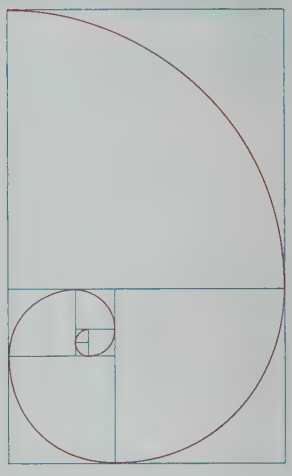
4 De façon générale, un théorème dit que la loi binomiale de paramètres (n ; 0,5) fournit un état stable X pour la marche aléatoire correspondant à l'expérience des urnes avec un total de n boules, état stable vers lequel celle-ci converge.
Ce théorème dit de plus que la durée moyenne de retour de l'état E_i à l'état E_i est l'inverse du coefficient i de cette matrice colonne « stable ».

a. Comparer dans le cas de 4 boules : la durée moyenne de retour à l'état initial dans le cas où les 4 boules sont dans A avec la durée moyenne de retour à l'état initial dans le cas où la répartition est de 2 boules dans A et 2 boules dans B.

b. On revient vers un problème de physique. On suppose que les instants sont comptabilisés en unité de temps égale à 10^{-6} seconde, que l'expérience concerne 100 particules, toutes situées au départ dans l'urne A.
Montrer que le temps moyen de retour à l'état initial est supérieur à 1 million de fois l'âge de l'univers (l'âge de l'univers est estimé à 15 milliards d'années).

47 Suite de Fibonacci et nombre d'or

Le mathématicien italien **Fibonacci** (environ 1175-1250) introduit un type de suites de nombres vérifiant une relation de récurrence élémentaire : un terme de la suite est la somme des deux termes qui le précèdent.
Une telle suite est appelée **suite de Fibonacci** et ses termes sont entièrement déterminés dès lors que l'on a défini les deux premiers termes de la suite.
La plus célèbre des suites de Fibonacci est celle dont les deux premiers termes valent 1 que l'on peut illustrer par les longueurs successives des rectangles de la construction ci-dessous.
Cette suite de nombres entiers est d'autant plus intéressante que son étude se trouve reliée à un nombre connu depuis l'Antiquité pour son utilisation dans le domaine artistique : le nombre d'or de valeur $\frac{1+\sqrt{5}}{2}$.



Partie 1. Les premiers termes

On considère la suite de nombres réels (u_n) définie par :

$$u_0 = 1 \; ; \; u_1 = 1 \; ; \; u_{n+2} = u_{n+1} + u_n \text{ pour tout } n \geqslant 0.$$

1. Calculer ses premiers termes et comparer avec les longueurs de la figure formée des rectangles emboîtés ci-contre.
2. À l'aide d'un tableur, créer une feuille de calcul qui affiche les 101 premiers termes de cette suite ainsi que les 100 premiers quotients $\frac{u_{n+1}}{u_n}$. Faire une conjecture.
3. On définit, pour tout $n \geqslant 0$, la matrice colonne $X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$.
   a. Déterminer une matrice carrée A telle que, pour tout $n \geqslant 0$, $X_{n+1} = AX_n$.
   b. En déduire un procédé de calcul direct de u_{20} à l'aide de la calculatrice. Retrouver u_{20}.

Partie 2. Le terme général

1. Vérifier que les matrices carrées $P = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}$ et $Q = \begin{pmatrix} \frac{-(\sqrt{5}-5)}{10} & \frac{\sqrt{5}}{5} \\ \frac{\sqrt{5}+5}{10} & -\frac{\sqrt{5}}{5} \end{pmatrix}$ sont inverses l'une de l'autre.
2. Montrer que la matrice A est égale au produit des matrices : $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{pmatrix}$ et où $P^{-1} = Q$ d'après la question précédente.
3. Démontrer que, pour tout $n \geqslant 0$, $X_n = (P \times D^n \times P^{-1})X_0$.
4. En déduire que, pour tout $n \geqslant 0$, $u_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n$.

Partie 3. Comportement asymptotique

1. Calculer la limite de la suite u_n.
2. **a.** À l'aide des notations : $q_1 = \frac{1+\sqrt{5}}{2}$, $q_2 = \frac{1-\sqrt{5}}{2}$, $a = \frac{5+\sqrt{5}}{10}$ et $b = \frac{5-\sqrt{5}}{10}$, montrer que :

$$\text{pour tout } n \geqslant 0, \; \frac{u_{n+1}}{u_n} = q_1 \frac{a + b\left(\frac{q_2}{q_1}\right)^{n+1}}{a + b\left(\frac{q_2}{q_1}\right)^{n}}.$$

   b. En déduire la limite du quotient de 2 termes consécutifs de la suite de Fibonacci.

OBJECTIF BAC

Sujets type BAC

Exercice résolu

Exercice 48 **Concurrence** *(D'après un sujet du concours PLP)*

Trois marques ***X***, ***Y*** et ***Z*** d'un dentifrice occupent un secteur de consommation.

Chaque mois, les consommateurs de la population étudiée utilisent une et une seule de ces marques.

Soit n un entier naturel. Pour un consommateur pris au hasard, on désigne par X_n (respectivement Y_n ou Z_n) l'évènement : « La marque X (respectivement Y ou Z) est utilisée au cours du n-ième mois ».

Les probabilités des événements X_n, Y_n et Z_n sont respectivement notées x_n, y_n et z_n.

Au cours du mois d'essai ($n = 0$), on a observé les valeurs initiales : $x_0 = 0{,}1$, $y_0 = 0{,}2$ et $z_0 = 0{,}7$.

D'autre part, par sondage, on a pu déterminer les intentions des consommateurs que l'on supposera constantes.

La probabilité, pour un consommateur ayant utilisé la marque X au cours du mois n, d'adopter la marque X (respectivement Y ou Z) au cours du mois suivant est 0,4 (respectivement 0,3 et 0,3).

La probabilité, pour un consommateur ayant utilisé la marque Y au cours du mois n, d'adopter la marque X (respectivement Y ou Z) au cours du mois suivant est 0,3 (respectivement 0,4 et 0,3).

La probabilité, pour un consommateur ayant utilisé la marque Z au cours du mois n, d'adopter la marque X (respectivement Y ou Z) au cours du mois suivant est 0,2 (respectivement 0,1 et 0,7).

1. Pour tout entier naturel n, exprimer x_{n+1}, y_{n+1} et z_{n+1}, en fonction de x_n, y_n et z_n.

2. On considère les matrices :

$$A = \begin{pmatrix} 0{,}2 & 0{,}1 \\ 0{,}2 & 0{,}3 \end{pmatrix},\ U_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix} \text{ et } B = \begin{pmatrix} 0{,}2 \\ 0{,}1 \end{pmatrix}.$$

Montrer que, pour tout entier naturel n, on a : $U_{n+1} = AU_n + B$.

3. On désigne par I la matrice unité de taille 2.

a. Montrer que la matrice $I - A$ est inversible.

b. Déterminer une matrice C telle que $C = AC + B$.

4. Pour tout entier naturel n, on pose $V_n = U_n - C$.

Pour tout entier naturel n, démontrer que, $V_n = A^n V_0$.

5. **a.** Vérifier à l'aide d'une calculatrice que :

$$A = P\begin{pmatrix} 0{,}4 & 0 \\ 0 & 0{,}1 \end{pmatrix}P^{-1} \text{ où } P = \begin{pmatrix} 1/3 & -1/3 \\ 2/3 & 1/3 \end{pmatrix}.$$

En déduire que, pour tout entier naturel n :

$$A^n = P\begin{pmatrix} 0{,}4^n & 0 \\ 0 & 0{,}1^n \end{pmatrix}P^{-1}.$$

b. Que peut-on dire des coefficients de la matrice A^n lorsque n tend vers $+\infty$?

c. Que conclure de l'utilisation, à long terme, des marques X, Y et Z ?

Voir résolution page suivante.

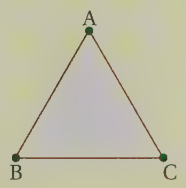
Exercice 49 ***Marche aléatoire sur un triangle***

On considère une marche aléatoire sur le triangle ABC ci-contre.

On suppose qu'à chaque pas :

la probabilité de rester au sommet occupé est 0,5,

la probabilité de quitter ce sommet pour un des deux autres est à chaque fois de 0,25.



1. Donner la matrice M de transition de cette marche.

2. On suppose que cette marche aléatoire converge quelle que soit la position initiale.

L'état limite X de la marche aléatoire dépend-il de la position initiale ? Déterminer cet état limite X.

3. On va montrer à présent que la marche aléatoire converge quelle que soit la position initiale.

On considère la matrice $B = 4M - 2I$ où I désigne la matrice unité de taille 3.

a. Prouver que $B^2 = 2I + B$.

b. Démontrer l'existence de deux suites de nombres réels (u_n) et (v_n) telles que, pour tout $n \geqslant 0$:

$M^n = u_n I + v_n B$;

$u_{n+1} = 0{,}5u_n + 0{,}5v_n$ et $v_{n+1} = 0{,}25u_n + 0{,}75v_n$.

c. Pour tout entier naturel n, on pose $w_n = u_n + 2v_n$.

Montrer que la suite (w_n) est constante.

d. Pour tout entier naturel n, on pose $t_n = u_n - v_n$.

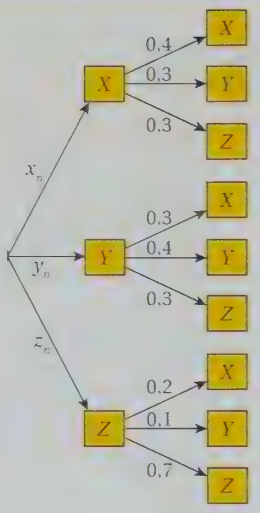
Montrer que la suite (t_n) est géométrique.

e. En déduire l'expression du terme général de chacune des suites (t_n), (u_n) et (v_n) en fonction de n.

f. Que peut-on dire des coefficients de M^n quand n tend vers $+\infty$? Conclure.

Résolution

1. Pour tout entier naturel n, l'arbre de probabilités suivant donne l'évolution du choix des consommateurs entre les mois n et $n+1$.



Le théorème des probabilités totales permet d'écrire :

$x_{n+1} = 0{,}4x_n + 0{,}3y_n + 0{,}2z_n$

$y_{n+1} = 0{,}3x_n + 0{,}4y_n + 0{,}1\,z_n$

$z_{n+1} = 0{,}3x_n + 0{,}3y_n + 0{,}7z_n$

2. Comme, pour tout entier naturel n, $x_n + y_n + z_n = 1$, on déduit des relations précédentes que :

$x_{n+1} = 0{,}4x_n + 0{,}3y_n + 0{,}2\,(1 - x_n - y_n) = 0{,}2x_n + 0{,}1y_n + 0{,}2$

et $y_{n+1} = 0{,}3x_n + 0{,}4y_n + 0{,}1\,(1 - x_n - y_n) = 0{,}2x_n + 0{,}3y_n + 0{,}1$.

Ces deux égalités sont équivalentes à l'égalité matricielle $U_{n+1} = AU_n + B$ pour les matrices U_n, A et B définies comme dans l'énoncé.

3. a. La matrice $I - A$ a pour coefficients : $\begin{pmatrix} 0{,}8 & -0{,}1 \\ -0{,}2 & 0{,}7 \end{pmatrix}$.

Les lignes de cette matrice ne sont pas proportionnelles donc cette matrice est inversible.

b. L'équation matricielle $C = AC + B$ est équivalente à l'équation $(I - A)C = B$. Et comme $(I - A)$ est inversible, cette équation a pour unique solution la matrice colonne $C = (I - A)^{-1}B$.

À l'aide de la calculatrice, on obtient $C = \begin{pmatrix} \frac{5}{18} \\ \frac{2}{9} \end{pmatrix}$.

4. On pose $V_n = U_n - C$. On montre la propriété $V_n = A^n V_0$ par récurrence sur $n \geqslant 0$.

$A^0 V_0 = I_2 V_0 = V_0$, donc la propriété est vraie au rang $n = 0$.

On suppose la propriété vraie au rang k, alors :

$V_{k+1} = U_{k+1} - C = AU_k + B - C$, or $C = AC + B$, donc $V_{k+1} = AU_k + B - AC - B = A(U_k - C) = AV_k$.

En utilisant l'hypothèse de récurrence, on obtient $V_{k+1} = A\,A^k\,V_0 = A^{k+1}\,V_0$. La propriété est encore vraie au rang $k+1$.

La propriété $V_n = A^n V_0$ est donc bien vraie pour tout entier naturel n.

5. a. La calculatrice donne bien $P\begin{pmatrix} 0{,}4 & 0 \\ 0 & 0{,}1 \end{pmatrix} P^{-1} = A$.

On démontre alors la relation $A^n = P \times \begin{pmatrix} 0{,}4^n & 0 \\ 0 & 0{,}1^n \end{pmatrix} \times P^{-1}$ par récurrence sur $n \geqslant 0$:

$P \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times P^{-1} = I_2 = A^0$, donc la propriété est vraie au rang $n = 0$.

On suppose la propriété vraie au rang k, alors au rang $k+1$:

$$A^{k+1} = A \times A^k = P \times \begin{pmatrix} 0{,}4 & 0 \\ 0 & 0{,}1 \end{pmatrix} \times P^{-1} \times P \times \begin{pmatrix} 0{,}4^k & 0 \\ 0 & 0{,}1^k \end{pmatrix} \times P^{-1} = P \times \begin{pmatrix} 0{,}4 & 0 \\ 0 & 0{,}1 \end{pmatrix} \times \begin{pmatrix} 0{,}4^k & 0 \\ 0 & 0{,}1^k \end{pmatrix} \times P^{-1}$$

$$= P \times \begin{pmatrix} 0{,}4^{k-1} & 0 \\ 0 & 0{,}1^{k-1} \end{pmatrix} \times P^{-1}.$$ La propriété est encore vraie au rang $k+1$.

La propriété $A^n = P \times \begin{pmatrix} 0{,}4^n & 0 \\ 0 & 0{,}1^n \end{pmatrix} \times P^{-1}$ est donc vraie pour tout $n \geqslant 0$.

b. Comme les suites de terme général $0{,}4^n$ et $0{,}1^n$ ont pour limite 0 lorsque n tend vers $+\infty$, les coefficients de la matrices A^n convergent vers 0.

c. On en déduit que les coefficients de la matrice V_n convergent vers 0, ce qui implique que (U_n) converge vers C.

Les suites de probabilités (x_n), (y_n) et (z_n) convergent respectivement vers $\frac{5}{18}$, $\frac{2}{9}$ et $1 - \frac{5}{18} - \frac{2}{9} = \frac{1}{2}$.

On peut donc dire qu'à long terme, la moitié des consommateurs utiliseront la marque Z.

BILAN QCM

Se tester sur... Matrices et suites

CORRIGÉS P. 160

Pour chaque question, il y a une ou plusieurs bonnes réponses.

1 On donne les matrices M et N :

$M = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 4 \\ 3 & 0 & -1 \end{pmatrix}$ et $N = \begin{pmatrix} 2 & -1 & 0 \\ 3 & -3 & 1 \\ 1 & 0 & 2 \end{pmatrix}$

alors $M + N$ est égale à :

A $\begin{pmatrix} 3 \\ 6 \\ 5 \end{pmatrix}$ B $\begin{pmatrix} 3 & 1 & -1 \\ 3 & -2 & 5 \\ 4 & 0 & 1 \end{pmatrix}$ C $\begin{pmatrix} 2 & -2 & 1 \\ 0 & -3 & 4 \\ 3 & 0 & -2 \end{pmatrix}$

2 Avec les même données qu'au **1.**, le produit $M \times N$ est égal à :

A $\begin{pmatrix} 7 & -7 & 0 \\ 7 & -3 & 9 \\ 5 & -3 & -2 \end{pmatrix}$ B $\begin{pmatrix} 7 & 7 & 0 \\ 7 & -3 & 9 \\ 5 & -3 & -2 \end{pmatrix}$ C $\begin{pmatrix} 7 & -7 & 0 \\ 7 & -3 & 9 \\ 5 & -6 & -2 \end{pmatrix}$

3 Pour a un nombre réel, le produit de la matrice carrée $A = \begin{pmatrix} 1 & a & a \\ a & a & 1 \\ a & 1 & a \end{pmatrix}$ par la matrice colonne $B = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$:

A est un multiple de B

B n'est jamais égale à la matrice colonne nulle

C est égale à A

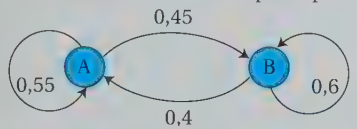
4 Si A et B sont deux matrices carrées telles que $A \times B = 0$ alors :

A A ou B est une matrice nulle

B A et B sont des matrices nulles

C on ne peut pas savoir

5 Une marche aléatoire partant de B sur le graphe suivant a pour probabilité d'arriver au sommet A après 3 pas



A $\frac{3779}{8000}$ B $\frac{4221}{8000}$ C $\frac{469}{1000}$ D $\frac{531}{1000}$

6 Si M désigne la matrice de transition d'un sommet à un autre pour une marche aléatoire sur un graphe probabiliste à 3 sommets, alors la probabilité d'être situé sur le 2nd sommet après 3 pas en étant parti du 1er sommet est :

A le 2e terme de $M^3 \times \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ B le 1er terme de $M^3 \times \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$

C le 3e terme de $M^2 \times \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ D le 1er terme de $M^2 \times \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

7 On donne la matrice $M = \begin{pmatrix} 4 & -6 \\ 1 & -1 \end{pmatrix}$, alors :

A la matrice A est inversible

B la matrice $I - A$ est inversible

C la matrice $A - I$ n'est pas inversible.

8 Le système d'équations : $\begin{cases} x + y = 3 \\ 4x - 2y + z = 0 \\ 5x - y - z = 3 \end{cases}$

A a pour unique solution $\begin{cases} x = 1 \\ y = 2 \\ z = 0 \end{cases}$

B a parmi ses solutions $\begin{cases} x = 1 \\ y = 2 \\ z = 0 \end{cases}$

C a une infinité de solutions.

9 Une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = AX_n + B$ est :

A toujours convergente

B peut converger ou diverger

C converge si il existe une matrice colonne constante X vérifiant $X = AX + B$

10 Si la suite de matrices colonnes (X_n) vérifiant la relation de récurrence $X_{n+1} = AX_n + B$, avec

$A = \begin{pmatrix} 0{,}2 & 0{,}7 \\ -0{,}1 & -0{,}5 \end{pmatrix}$ et $B = \begin{pmatrix} 0{,}2 \\ -0{,}2 \end{pmatrix}$

est convergente alors sa limite est :

A $\begin{pmatrix} -\frac{16}{127} \\ \frac{18}{127} \end{pmatrix}$ B $\begin{pmatrix} \frac{4}{3} \\ -\frac{2}{3} \end{pmatrix}$ C $\begin{pmatrix} -\frac{4}{3} \\ \frac{2}{3} \end{pmatrix}$ D $\begin{pmatrix} \frac{16}{127} \\ -\frac{18}{127} \end{pmatrix}$

11 Si une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = AX_n + B$ converge, c'est :

A vers une matrice colonne constante X vérifiant $X = AX$

B vers une matrice colonne constante X vérifiant $X - B = AX$

C vers une matrice colonne constante égale à X_0

12 Une marche aléatoire sur un graphe probabiliste d'ordre 2 converge :

A dans tous les cas

B cela dépend des valeurs des probabilités de transition.

C cela dépend des valeurs des probabilités de la répartition initiale.

Corrigés des exercices

Arithmétique

Chapitre 1

1 **a.** 1, 2, 3, 6, 9, 18, 27, 54.
b. 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 36, 48, 72, 144.
c. 1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200.

2 **a.** 1, 2, 4, 5, 10, 20, 25, 50, 100.
b. 1, 2, 4, 5, 10, 20, 25, 50, 100
et 7, 14, 28, 35, 70, 140, 175, 350, 700.

5 $b = ka$ et $c = k'a$,
donc $bc = ka \times k'a = kk' \times a^2$.

6 **1.** $n = 2k$, alors $n^2 = 4k^2$ est pair.
2. $n = 2k + 1$, alors $n^2 = 4k^2 + 4k + 1$ est impair.
3. Si $n = 2k$, alors $n^2 - n = 4k^2 - 2k$ est pair.
Si $n = 2k + 1$, alors $n^2 - n = 4k^2 + 2k$ est pair.

8 **1.** Comme $51 = 17 \times 3$, si $51n + 4$ était divisible par 17 alors 4 serait divisible par 17.
2. 3013.

9 **1.** n semble de la forme $19k - 1$ ou $19k + 1$.
2. et **3.** $n^2 + 18 = (n - 1)(n + 1) + 19$, d'où $n^2 + 18$ est divisible par 19 si $n - 1$ ou $n + 1$ est divisible par 19.
4. $n - 1 = 19k$ équivaut à $n = 19k + 1$, et $n + 1 = 19k$ équivaut à $n = 19k - 1$.

13 Dividende 434, diviseur 23, quotient 18 et reste 20.

14 **a.** $500 = 17 \times 39 + 7$.
b. $-500 = 17 \times (-30) + 10$.

16 $23 \times 2 + 1 = 47$ multiples de 13.

17 $250 = bq + 3$
d'où $-250 = -bq - 3 = b \times (1 - q) + b - 3$.
$b - 3 = 10$ d'où $b = 13$.

19 **a.** $n = 5q + q = 6q$. Ce sont les multiples de 6.
b. $n = 5q + n$, donc $q = 0$, ce qui signifie que $n < 5$.

25 **a.** Reste 3 si $n > 3$, reste 0 si $n = 1$ ou 3, reste 1 si $n = 2$.
b. Reste 4 si $n > 4$, reste 0 si $n = 1$ ou 2 ou 4, reste 1 si $n = 3$.

28 **1.** $7322 - 7305 = 17$ donc ils ont même reste dans la division par 17.
2. $7305 \equiv 7322$ [17] donc $7305^3 \equiv 7322^3$ [17].

29 **1.** **a.** $2a + 3b \equiv 5$ [11].
b. $a^2 + b^2 \equiv 6$ [11]. **c.** $ab \equiv 8$ [11].
2. $a^2 - b^2 \equiv 0$ [11].

31 **a.** $2014^{2014} \equiv 1^{2014} \equiv 1$ [11].
b. $2012^{2012} \equiv (-1)^{2012} \equiv 1$ [11].

33 **a.** $2^{11} + 1 \equiv (2^2)^5 \times 2 + 1$
$\equiv 1^5 \times 2 + 1 \equiv 0$ [3].
b. $5^{10} + 1 \equiv (5^2)^5 + 1 \equiv (-1)^5 + 1 \equiv 0$ [13].

37 **a.** $x \equiv 5$ [7]. **b.** $x \equiv 3$ [7].

44 **a.** 4 ou 8. **b.** 4 ou 8. **c.** 3, 4 ou 6.

45 Impossible car $221 = 13 \times 17$. Les 19 bonbons restant pourraient être en partie distribués.

46 $n = 4k + 5$ or $39 = 4 \times 9 + 3$ donc il manque $2 + 4k$ élèves. Le professeur a (toujours !) raison.

47 **a.** 7$, qui n'auraient pu être partagés au cent près.
b. Il aurait fallu 5 braqueurs supplémentaires pour être 16.

48 **1.** $414 - 11 = 403 = 13 \times 31$.
Pour qu'il y ait un reste, il ne peut avoir une seule classe. On exclut aussi le cas de 403 classes avec un élève par classe.
Il y a donc 13 ou 31 classes.
2. S'il y a 12 classes, il restera 6 élèves non affectés.
S'il y a 30 classes, il restera 24 élèves non affectés.

49 **a.**

Valeurs de n	0	1	2	3	4	5	6	7
Congruence de 4^n mod 11	1	4	5	9	3	1	4	5
Congruence de 3^n mod 11	1	3	9	5	4	1	3	9

b. $4^{n+k} - 3^{n+k} \equiv 4^n \times 4^k - 3^n \times 3^k$ [11], vrai si $k = 5$.
c. $n \equiv 0$ [5].
d. $2015 \equiv 0$ [5]
donc $4^{2015} - 3^{2015} \equiv 4^0 - 3^0 \equiv 0$ [11].

50 **1.** $13^{13} \equiv 3^{13} \equiv 9^6 \times 3 \equiv 3$ [10]. Le chiffre des unités est 3.
$2023^{2023} \equiv 3^{2023} \equiv 9^{1011} \times 3 \equiv -3$ [10]. Le chiffre des unités est 7.
2. $n^n \equiv 3^n$. Si $n \equiv 0$, 1, 2 ou 3 [4], alors le chiffre des unités est dans l'ordre 1, 3, 9 ou 7.

52
2. **a.** $\sum a_n \times 10^n \equiv \sum a_n \times 1^n \equiv \sum a_n$ [9].
et $\sum a_n \times 10^n \equiv \sum a_n \times 1^n \equiv \sum a_n$ [3].
b. Un nombre est divisible par 3 (resp. 9) si la somme des chiffes qui le compose est divisible par 3 (resp. 9).
c. 127392 est divisible par 3 mais pas par 9.
3. **a.** Seuls 47586 et 124153 sont divisibles par 3.
b. $\sum a_n \times 10^n \equiv \sum a_n \times (-1)^n$ [11].

53 **1.** $a + b \equiv r + r'$ [9] avec r et r' la somme des chiffres de a et b dans la division par 9.
2. $a + b + 9$ au lieu de $a + b$ est une réponse fausse mais la preuve serait juste.
3. $a \times b \equiv r \times r'$ [9].
4. Si la preuve est juste, Léa ne peut affirmer que le calcul est juste ou faux. Si la preuve est fausse, le calcul est faux. La preuve est fausse pour le **c.** qui est donc faux. La preuve est juste au **b.** bien que le calcul soit faux.

Chapitre 2

1 **a.** {1 ; 2 ; 13 ; 26}.
b. PGCD(52 ; 78) = 26.

3 **a.** PGCD(n ; $5n$) = n.
b. PGCD(n ; n^2) = n.

5 **a.** PGCD(119 ; 247) = 1.
b. $\frac{1846}{2418} = \frac{71}{93}$.

7 **a.** 1 **b.** 1 **c.** 1.

10 **a.** PGCD(564 ; 612) = 12.
b. 1 ; 2 ; 3 ; 4 ; 6 ; 12.

14 **a.** $1510 - 3 \times 503 = 1$.
b. $3 \times 51 - 2 \times 76 = 1$.
c. $(-9) \times 1111 + 2 \times 5000 = 1$.

15 $(n + 1) - n = 1$.

16 $4 \times (3n + 7) - 3 \times (4n + 9) = 1$.

17 $n \times (-n) + n^2 + 1 = 1$ donc n et $n^2 + 1$ sont premiers entre eux.

18 $(-2) \times 5004 + 5 \times 2002 = 2$, donc le PGCD divise 2, or 2 est un diviseur du PGCD donc PGCD(5004 ; 2002) = 2.

21 **a.** $102 = 78 + 24$
$78 = 24 \times 3 + 6$
$24 = 6 \times 4 + 0$
PGCD(102 ; 78) = 6.
b. $6 = 78 - (102 - 78) \times 3 = 4 \times 78 - 3 \times 102$.

25 **a.** $(2 ; -1)$.
b. Par soustraction membre à membre.
c. $(2 + 13k ; -1 + 7k)$ pour k entier relatif.

27 **a.** $P(n) = (n + 1)(n + 2)$.
b. n est premier avec $n + 1$, donc n divise $n + 2$.
c. n divise 2, donc $n = 1$ ou 2.

30 **a.** g divise $2a$ et $2b$ car ce sont des combinaisons linéaires de $a + b$ et $a - b$.
b. g est premier avec 2 car a et b sont de parités différentes.
c. En appliquant le Théorème de Gauss, g divise a et b et donc leur PGCD.
Réciproquement, PGCD(a ; b) divise g, donc g = PGCD(a ; b).

Chapitre 3

1 **a.** $2013 = 3 \times 671$.
b. $2015 = 5 \times 403$.
c. $2021 = 43 \times 47$.

4 Oui car $\sqrt{250} \approx 15{,}8$.

8 **a.** $u_0 = 3$, $u_1 = 5$, $u_2 = 11$ et $u_3 = 29$ sont premiers.
b. Se montre par contraposée.
c. $u_5 = 245$ et $u_6 = 731$ ne sont pas premiers.

9 **1.** $\sqrt{1\,000} \approx 31{,}6$. Les 11 diviseurs premiers inférieurs ou égaux à 31 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.
2. $31^2 = 961$.

14 **a.** $286 = 2 \times 11 \times 13$.
b. $36 = 2^2 \times 3^2$.
c. $700 = 2^2 \times 5^2 \times 7$.
d. $89 = 89$.

16 **a.** $450 = 2 \times 3^2 \times 5^2$ et $630 = 2 \times 3^2 \times 5 \times 7$.
b. $450 \times 630 = 2^2 \times 3^4 \times 5^3 \times 7$.
c. $450 + 630 = 2 \times 3^2 \times 5 \times (5 + 7)$
$= 2 \times 3^2 \times 5 \times 12 = 2^3 \times 3^3 \times 5$.

24 **a.** {1 ; 3 ; 5 ; 9 ; 15 ; 45}.
b. {1 ; 3 ; 19 ; 57}.
c. {1 ; 2 ; 4 ; 5 ; 8 ; 10 ; 16 ; 20 ; 40 ; 80}.

27 **a.** $1\,694 = 2 \times 7 \times 11^2$.
b. 12 diviseurs.
c. 45 diviseurs. 112 diviseurs.

Se tester sur l'arithmétique

QCM

1 C	**2** A	**3** **a.** A **b.** B, C
4 D	**5** A, B, C	**6** D
7 **a.** C, D **b.** C		**8** A, D
9 B, C	**10** A	**11** C
12 B, D	**13** B	**14** D
15 A	**16** C	**17** A, C, D

Matrices

Chapitre 4

4 Par exemple pour $i = 2$ et $j = 3$: $b_{23} = 2^2 + 2 \times 3 = 10$.

$$B = \begin{pmatrix} 3 & 5 & 7 & 9 \\ 6 & 8 & 10 & 12 \\ 11 & 13 & 15 & 19 \\ 18 & 20 & 22 & 24 \end{pmatrix}.$$

9 $2A + 4B - 3C = \begin{pmatrix} 13 & 25 \\ -38 & 77 \end{pmatrix}$.

12 $-2 = 2z$ donc $z = -1$; $x^2 = 2x$ donc $x = 0$ ou $x = 2$ et $y = 1 - 2x$.

14 **a.** $A \times B = \begin{pmatrix} -12 \\ -38 \end{pmatrix}$. **b.** $A \times B = \begin{pmatrix} 19 \\ -3 \\ 3 \end{pmatrix}$.

18 Les coefficients manquants sont : 35,5 ; −33 et 68.

23 Pour tout $n \geqslant 1$: $A^n = 2^{n-1}A$.

26 $A^2 - B^2 = \begin{pmatrix} -6 & -9 \\ 0 & -12 \end{pmatrix}$

et $(A + B)(A - B) = \begin{pmatrix} 21 & -78 \\ 18 & -39 \end{pmatrix}$.

Les deux réponses sont différentes car $A \times B \neq B \times A$.

32 **a.** 0,39376 . **b.** $\approx 0{,}5782464$.

35 **1.** Si $A = \begin{pmatrix} 0{,}1 & 0{,}7 \\ 0{,}9 & 0{,}3 \end{pmatrix}$ et $B = \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix}$ alors, pour tout $n \geqslant 0$: $X_{n+1} = 0{,}7AX_n + 0{,}3B$.
2. La probabilité d'être en B est environ 0,532.
3. La probabilité d'être à nouveau en B est environ 0,543.

37 **1.** Si $A = \begin{pmatrix} 0 & 0{,}25 & 0{,}5 \\ 0{,}75 & 0 & 0{,}5 \\ 0{,}25 & 0{,}75 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ alors pour tout $n \geqslant 0$: $X_{n+1} = 0{,}6AX_n + 0{,}4B$.
2. La probabilité d'être en C est environ 0,56.
3. La probabilité d'être à nouveau en B est environ 0,255.

38 **1.** $A = \begin{pmatrix} 0{,}85 & 0{,}1 \\ 0{,}15 & 0{,}9 \end{pmatrix}$.

2. et **3.** L'effectif du lycée Montaigne en 2013 sera $291/221^e$ de l'effectif du lycée Pascal et $291/221 > 1{,}25$.

42 Pour $n = 2k$ avec k entier supérieur ou égal à 1 :
$A \times B$ est la matrice colonne C telle que pour $1 \leqslant j \leqslant n$: $c_j = k$.

44 **1.** **a.** 13/48. **b.** environ 0,273.
2. $\frac{13}{48} \times \frac{1}{3} = \frac{13}{144}$.

49 **1.** Si A désigne la matrice de transition d'une salle à l'autre en suivant le fléchage et si B désigne la matrice de transition entre les salles par chaque porte de façon équirépartie, les états probabilistes pour les visiteurs dans chaque salle vérifient alors, pour tout $n \geqslant 0$: $X_{n+1} = 0{,}75AX_n + 0{,}25BX_n$.
Calculer alors X_6.
2. L'événement « avoir visité la salle D au bout de 40 minutes » est l'événement « être dans la salle D après 3 changements de salle » puisqu'y arriver plus rapidement est impossible. Sa probabilité est le quatrième coefficient de X_3, soit environ 0,61.

Chapitre 5

6 **1.** On vérifie que le produit des 2 matrices A et B donne I_2.
2. La matrice est $2A$, son inverse est $0{,}5B$.

8 Vrai, car
$A^2 \times B^2 = (A \times A) \times (B \times B) = A \times (A \times B) \times B$
$= A \times I \times B = A \times B = I$.

11 **1.** $3 \times 4 - 6 \times 2 = 0$, donc la matrice A n'est pas inversible.
2. $2 \times 4 - 2 \times 0 \neq 0$ donc la matrice A est inversible d'inverse :

$$A^{-1} = \begin{pmatrix} 0{,}5 & -0{,}25 \\ 0 & 0{,}25 \end{pmatrix}.$$

15 Par l'absurde, si A est inversible d'inverse B alors les coefficients de la ligne 1 colonne 1 et de la ligne 2 colonne 1 du produit $A \times B = I_3$ donnent :
$b_{11} + b_{21} + b_{31} = 1$ et $b_{11} + b_{21} + b_{31} = 0$.
Impossible, donc A n'est pas inversible.

20 **a.** $M = \begin{pmatrix} 0{,}55 & 0{,}4 \\ 0{,}45 & 0{,}6 \end{pmatrix}$.

b. $M^{-1} \times \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix} = \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}$.

c. $\left(M^{-1}\right)^2 \times \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix} = \begin{pmatrix} 16/9 \\ -7/9 \end{pmatrix}$, ce vecteur colonne ne constitue pas un état probabiliste.

31 $z = 2 - t$; $x = 6 + t$; $y = 5 - 2z = 1 + 2t$;
d'où $x + y = 3$ équivaut à $7 + 3t = 3$,
donc $t = -4/3$; $x = 14/3$; $y = -5/3$ et $z = 10/3$.

37 Si $f(x) = ax^3 + bx^2 + cx + d$ alors a, b, c et d sont solutions du système :

$$\begin{cases} -a + b - c + d = 15 \\ 3a - 2b + c = 0 \\ 8a + 4b + 2c + d = -12 \\ 12a + 4b + c = 0 \end{cases}.$$

On trouve $f(x) = 2x^3 - 3x^2 - 12x + 8$.

40 **a.** La probabilité est $2\,311/5\,184 \approx 0{,}446$.
b. La probabilité est 0,16.

44 Si x, y et z désignent respectivement les tailles des grands, moyens et petits pots ; le nombre de pots sur chaque étagère permet d'écrire : $\begin{cases} x + 3y + 3z = 20 \\ 2x + 6z = 20 \\ 4y + 6z = 20 \end{cases}$.
On trouve $x = 20/3$; $y = 10/3$ et $z = 10/9$.

45 **1.** $M^2 = \begin{pmatrix} -2 & 3 & -3 \\ -9 & 10 & -9 \\ -3 & 3 & -2 \end{pmatrix}$.

2. $M^2 = 3M - 2I$. **3.** $M^3 = 7M - 6I$.

4. $\frac{1}{2}M \times (3I - M) = \frac{3}{2}M - \frac{1}{2}M^2 = I$ en utilisant la question **2** ; M a pour inverse la matrice égale à $\frac{1}{2}(3I - M)$.

Chapitre 6

2 Si pour tout $n \geqslant 0$, on note $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$
alors $A = \begin{pmatrix} -5{,}5 & -15 \\ 2 & 5 \end{pmatrix}$ et $X_0 = \begin{pmatrix} 3 \\ 25 \end{pmatrix}$.

7 Pour tout $n \geqslant 0$, l'accroissement annuel est $p_{n+1} - p_n$;
or $p_{n+2} - p_{n+1} = -\frac{1}{2}p_n + \frac{3}{2}p_{n+1} - p_n$
$= \frac{3}{2}(p_{n+1} - p_n)$.

12 Si pour tout $n \geqslant 0$ on note $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$,
alors $X_{n+1} = AX_n + B$ avec $A = \begin{pmatrix} 0{,}5 & -3 \\ 1 & -2 \end{pmatrix}$ et $B = \begin{pmatrix} 7 \\ -5 \end{pmatrix}$.
A est inversible donc $X_n = A^{-1}(X_{n+1} - B)$.
À partir de X_5, on calcule les termes de proche en proche (ou on programme ce calcul).
On trouve : $u_0 = 27{,}5$ et $v_0 = 10{,}25$.

14 **1.** $M = \begin{pmatrix} 0 & 1 & 1 \\ 0{,}5 & 0 & 0 \\ 0{,}5 & 0 & 0 \end{pmatrix}$.

2. Si on part de A, pour tout $n \geqslant 0$, la probabilité a_n d'être en A vaut 1 si n pair et 0 si n impair ; la marche aléatoire n'est donc pas convergente.

3. Si on part de B ou C, pour tout $n \geqslant 0$, la probabilité a_n d'être en A vaut 1 si n impair et 0 si n pair ; la marche aléatoire n'est donc pas convergente.

17 **1.** $M = \begin{pmatrix} 0 & 0,4 & 0 & 0,4 \\ 0,4 & 0 & 0,4 & 0 \\ 0 & 0,4 & 0 & 0,4 \\ 0,4 & 0 & 0,4 & 0 \end{pmatrix}$ et $N = \begin{pmatrix} 0,05 \\ 0,05 \\ 0,05 \\ 0,05 \end{pmatrix}$.

2. $X_1 = \begin{pmatrix} 0,05 \\ 0,45 \\ 0,05 \\ 0,45 \end{pmatrix}$ et $X_3 = \begin{pmatrix} 0,122 \\ 0,378 \\ 0,122 \\ 0,378 \end{pmatrix}$.

3. Démonstration par récurrence en utilisant que, pour tout $n \geqslant 1$:
$a_{n+1} = c_{n+1} = 0,4b_n + 0,4d_n + 0,05$
et $b_{n+1} = d_{n+1} = 0,4a_n + 0,4c_n + 0,05$.
4. Pour tout $n \geqslant 1$:
$a_n = c_n$; $b_n = d_n$ et $a_n + b_n + c_n + d_n = 1$.
5. Pour tout $n \geqslant 0$:
$a_{n+1} - b_{n+1} = 0,4b_n + 0,4d_n + 0,05 - (0,4a_n + 0,4c_n + 0,05)$
$= (-0,8)(a_n - b_n)$
d'où $u_n = (-0,8)^n$.
6. En utilisant les deux questions précédentes, pour tout $n \geqslant 1$, $a_n = \frac{1}{2} \times (0,5 + u_n)$.
La suite (a_n) converge alors vers 0,25. On en déduit la même limite pour les trois autres suites.

21 **a.** $M - I_2$ est une matrice inversible ; l'unique solution est la matrice colonne $X = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

b. $M - I_2$ n'est pas inversible ; les solutions sont les matrices colonnes $X = \begin{pmatrix} a \\ \frac{14}{17}a \end{pmatrix}$ pour $a \in \mathbb{R}$.

27 $I_3 - A$ n'est pas inversible. On cherche alors des solutions au système :
$\begin{cases} -a - 2b - c = 1 \\ -c = 1 \\ -2a - 4b - 5c = 5 \end{cases} \Leftrightarrow \begin{cases} a = -2b \\ c = -1 \end{cases}$.
Ce sont les suites de terme constant du type : $\begin{pmatrix} -2b \\ b \\ -1 \end{pmatrix}$ pour b.

33 La marche aléatoire converge vers un état stable du système qui est :
$X = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ où a, b, c et d sont solution du système : $\begin{cases} d = a \\ 0,5a = b \\ 05a + b = c \\ c = d \end{cases}$
et vérifient $a + b + c + d = 1$; donc $X = \begin{pmatrix} 2/7 \\ 1/7 \\ 2/7 \\ 2/7 \end{pmatrix}$.

34 **1.** $M = \begin{pmatrix} 0,2 & 0,45 \\ 0,8 & 0,55 \end{pmatrix}$. **2.** $X = \begin{pmatrix} 0,36 \\ 0,64 \end{pmatrix}$.
3. b. Ces deux produits donnent la matrice nulle de taille 2.
c. Montrer que $P^2 = P$ et $Q^2 = Q$, puis utiliser une démonstration par récurrence.
d. Utiliser les deux questions précédentes.
4. On trouve, pour tout $n \geqslant 0$:
$a_n = 0,36 + (-0,25)^n \times (a_0 - 0,36)$
donc : $a_n > 0,35$ pour tout $n \geqslant 2$.

37 **1.** Matrice de transition $M = \begin{pmatrix} 0,6 & 0,1 \\ 0,4 & 0,9 \end{pmatrix}$.
2. $f_2 = 27,5$ %.
3. L'état stable est $X = \begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix}$, une telle répartition de fumeurs/non fumeurs dans la population est stable d'une génération à la suivante.
4. Pour tout $n \geqslant 0$,
$f_{n+1} = 0,6f_n + 0,1g_n = 0,6f_n + 0,1(1 - f_n)$
$= 0,5f_n + 0,1$.
5. a. Pour tout $n \geqslant 0$,
$u_{n+1} = 0,5f_n + 0,1 - 0,2 = 0,5(f_n - 0,2) = 0,5u_n$.
La suite (u_n) est géométrique de raison 0,5 et de premier terme 0,5 – 0,2 = 0,3.
b. et **c.** Pour tout $n \geqslant 0$, $u_n = 0,3 \times 0,5^n$ et $f_n = 0,3 \times 0,5^n + 0,2$. La suite (f_n) converge vers 0,2. La proportion de fumeurs à long terme se rapproche de 20 %.

Se tester sur les matrices

QCM

1 B	**2** A	**3** A	**4** C
5 C	**6** A	**7** C	**8** B, C
9 B	**10** d	**11** B	**12** B, C

Édition : Christiane Lalubie
Maquette : Nicolas Balbo - Laurent Romano – Lauriane Tiberghein - Graphismes
Mise en page et schémas : DESK (53940 Saint-Berthevin)
Illustrations : Laurent Bourlaud
Iconographie : Nelly Gras (Hatier Illustration)

Achevé d'imprimer en Italie par L.E.G.O. S.p.A. - Lavis (TN)
Dépôt légal: 95405-4/02 - Novembre 2014

INDEX

TABLE DES ILLUSTRATIONS

4	-5	ph ©	J.-G. Berizzi/RMN
6	-hd	ph ©	Thierry Hubin/Museum des Sciences naturelles, Bruxelles
6	-mg	ph ©	Mike Kiev/fotolia.com
7		ph ©	Riou/Photocuisine
9		ph ©	A. Scorza/Afp
10		ph ©	Shutterstock
11		ph ©	L. Cerino/Rea
18		ph ©	D. van Ravenswaay/SPL/Cosmos
20		ph ©	F. Hanoteau
22	-bg	©	CG92/Arch. dép. Hauts-de-Seine/ Bibliothèque André-Desguine/G. Vannet
22	-d	ph ©	Costa/Leemage
26		ph ©	F. Durand/Sipa Press
28		ph ©	F. Raux/RMN (Musée du Louvre)
30		ph ©	MP/Leemage
33		ph ©	Pasieka/SPL/Cosmos
34		ph ©	F. Hanoteau
45		ph ©	Masterfile
46		ph ©	Iconotec/Photononstop
47	-d	ph ©	Kharbine-Tapabor
47	-g	ph ©	zelione/fotolia.com
50		ph ©	Kharbine-Tapabor
51		ph ©	E. Notarianni/CIT'images
52		©	2012 Les Editions Albert René / Goscinny-Uderzo - (vignette extraite de l'album « Le Devin »)
54		ph ©	Akg-Images
57		ph ©	Interfoto/La Collection
66		ph ©	The Granger Collection NYC/Rue des Archives
70		ph ©	Roger-Viollet
72	-hd	ph ©	Leemage
72	-hg	ph ©	Collection privée, Migny/ Kharbine-Tapabor
75		ph ©	J. Vigne/Kharbine-Tapabor
77		ph ©	jim/fotolia.com
82	-83	©	Paul Kichilov
84	-b	©	Paul Kichilov
84	-h	ph ©	Archives Hatier
84	-md	ph ©	Royal Astronomical Society/SPL/Biosphoto
84	-mg	ph ©	Marek/fotolia.com
85		ph ©	J.-F. Colonna/CNRS
98		ph ©	Gunnar/Age Fotostock
104		ph ©	Gyro Photographyaman/Age Fotostock
109		ph ©	Bruno Morandi/hemis.fr
125		ph ©	iNNOCENt/fotolia.com
131	-b	ph ©	John MacDougall/Afp
131	-hd	ph ©	Mifune/fotolia.com
131	-hg	ph ©	thingamajiggs/fotolia.com
151		ph ©	nextrecord/fotolia.com
152	-d	Coll.	Smithsonian Institution, Washington
152	-g	ph ©	Smithsonian Institution, Washington

Malgré nos efforts, il nous a été impossible de joindre certains photographes ou leurs ayants-droit, ainsi que des éditeurs ou leurs ayants-droit de certains documents, pour solliciter l'autorisation de reproduction, mais nous avons naturellement réservé en notre comptabilité des droits usuels.

UTILISER SA CALCULATRICE

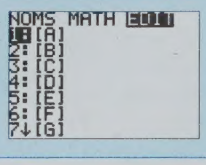
Matrices

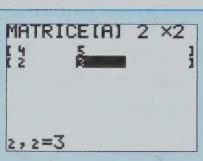
TI-83 Plus.fr

Soit les matrices $A = \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 4 \\ 4{,}5 & 6 \end{pmatrix}$

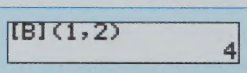
Créer une matrice : indiquer sa dimension et entrer ses termes

2nde x^{-1}





Afficher un terme donné d'une matrice

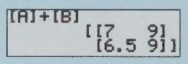


Séquence de touches : 2nde x^{-1} 2 (1 , 2)

Faire les opérations sur les matrices

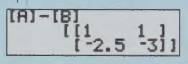
On entre les matrices A et B dans la calculatrice et on réalise les opérations suivantes.

- **addition**



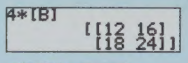
Séquence de touches : 2nde x^{-1} 1 + 2nde x^{-1} 2

- **soustraction**



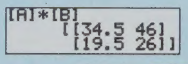
Séquence de touches : 2nde x^{-1} 1 − 2nde x^{-1} 2

- **multiplication par un réel**



Séquence de touches : 4 × 2nde x^{-1} 2

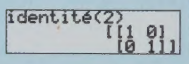
- **produit**

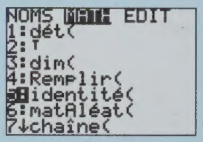


Séquence de touches : 2nde x^{-1} 1 × 2nde x^{-1} 2

Matrice particulière

- **matrice identité**

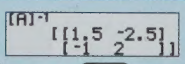




Séquence de touches : 2nde x^{-1} (2)

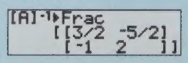
Inverse d'une matrice (si elle existe)

- **matrice inversible**



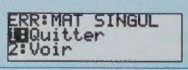
Séquence de touches : 2nde x^{-1} 1 x^{-1}

Pour des coefficients sous forme fractionnaire :



- **matrice non inversible (singulière)**

Si la matrice choisie n'est pas inversible (matrice B par exemple), voilà le message affiché :

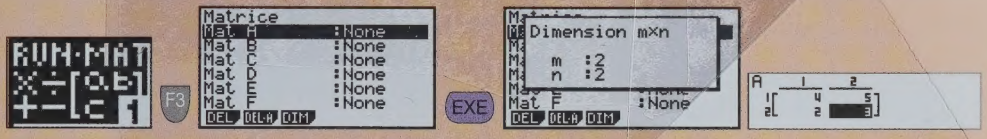


UTILISER SA CALCULATRICE

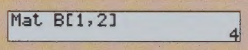
Casio graph 75

Soit les matrices $A = \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 4 \\ 4{,}5 & 6 \end{pmatrix}$

Créer une matrice : indiquer sa dimension et entrer ses termes



Afficher un terme donné d'une matrice

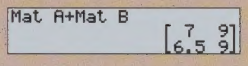


Séquence de touches : OPTN F2 F1 ALPHA log SHIFT + 1 , 2 SHIFT −

Faire les opérations sur les matrices

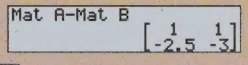
On entre les matrices A et B dans la calculatrice et on réalise les opérations suivantes.

- **addition**



Séquence de touches : OPTN F2 F1 ALPHA X,θ,T + OPTN F2 F1 ALPHA log

- **soustraction**

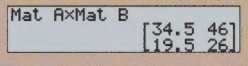


Séquence de touches : OPTN F2 F1 ALPHA X,θ,T − OPTN F2 F1 ALPHA log

- **multiplication par un réel**

Séquence de touches : 4 × OPTN F2 F1 ALPHA log

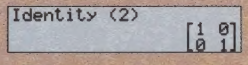
- **produit**



Séquence de touches : OPTN F2 F1 ALPHA X,θ,T × OPTN F2 F1 ALPHA log

Matrice particulière

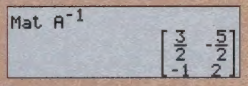
- **matrice identité**



Séquence de touches : OPTN F2 F6 F1 (2)

Inverse d'une matrice (si elle existe)

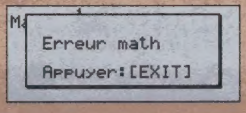
- **matrice inversible**



Séquence de touches : OPTN F2 F1 ALPHA X,θ,T SHIFT)

- **matrice non inversible (singulière)**

Si la matrice choisie n'est pas inversible (matrice B par exemple), voilà le message affiché :



Avec ODYSSÉE Tle S

Pour vous aider à réussir vous trouverez sur le site www.odyssee-hatier.com :

Des QCM interactifs :

- Pour faire le point sur vos connaissances
- Pour réviser avant un contrôle

Des fichiers logiciels :

- Pour vous aider à programmer votre calculatrice (TI ou Casio)
- Pour commencer les TP sur logiciels (géométrie, algorithmique, tableurs...)

+ Une boîte à outils :

- Des adresses pour télécharger des logiciels de mathématiques
- Des liens vers des sites de démonstrations

44 4503 7
ISBN 978-2-218-95405-4
9 782218 954054

Couverture : Olivier Damiens
Photos : Fusée Ariane V – (2005)
© ESA/CNES/CSG/NOVAPIX
Euclide, fresque de Raphaël, (1509-1510), Rome, Vatican, chambre de la Signature.
Ph © E. Lessing/AKG-Images