Term S

ENSEIGNEMENT DE SPÉCIALITÉ

Nouvelle Collection Indice

Maths

PROGRAMME 2012

Sous la direction de :

Michel PONCY

Jean-Louis BONNAFET

Marie-Christine RUSSIER

Sébastien CANTE

Martine FEID

Yves GUICHARD

Catherine LEBERT

Pierre-Marie LONGIN

Yvette MASSIERA

Jean-Manuel MENY

Frédérique MOUNIER

Denis VIEUDRIN

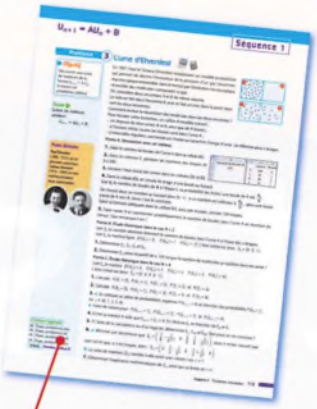
Fabienne VINCEROT

éco responsable

Bordas

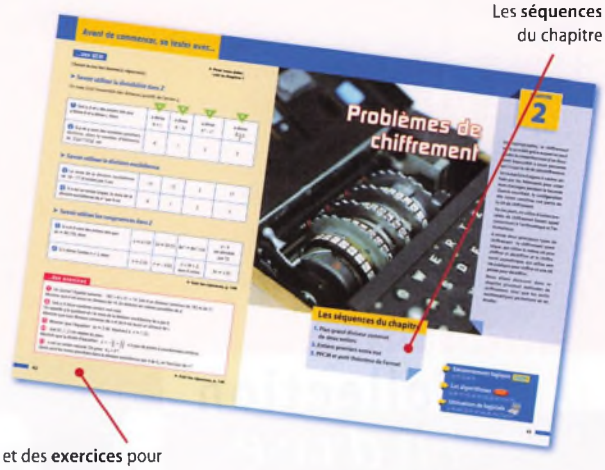
Pour découvrir votre manuel

Un découpage par séquences qui prend appui sur la résolution de problèmes



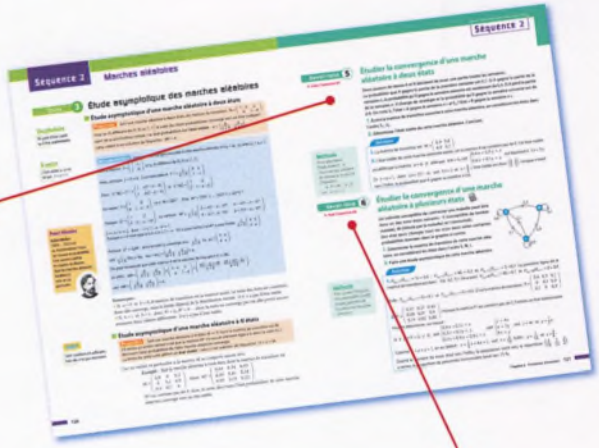
Des **fichiers à télécharger** sur
www. **bordas-indice.fr**
pour réaliser certains problèmes

Les **séquences** du chapitre



Un **QCM** et des **exercices** pour se tester avant de commencer le chapitre, retrouvez les corrections détaillées sur
www. **bordas-indice.fr**

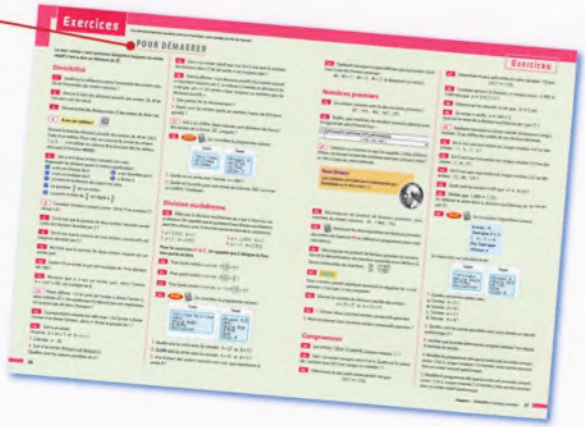
Un cours simple et complet



Les **savoir-faire** indispensables pour assimiler les notions du cours

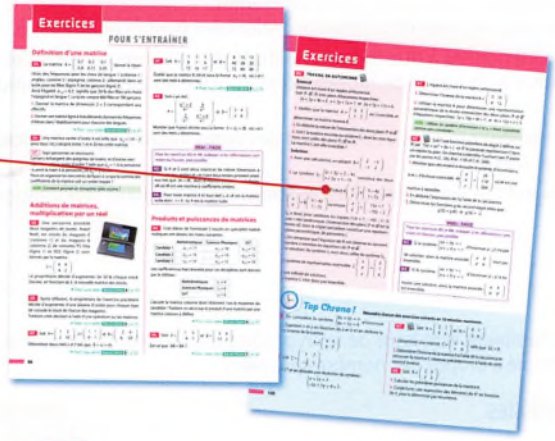
Les exercices

POUR DÉMARRER
Un grand choix d'exercices très simples pour démarrer le chapitre

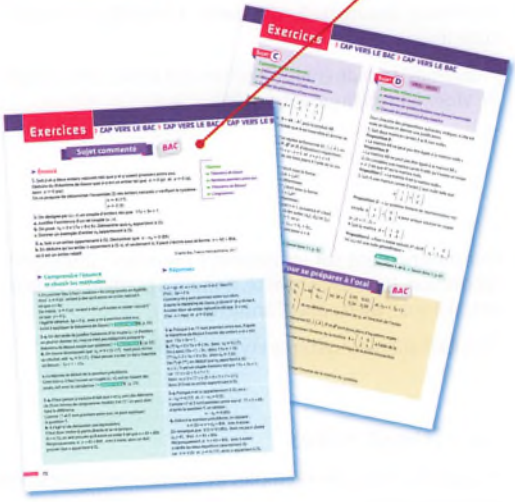


Des renvois à des exercices reprenant ces savoir-faire

POUR S'ENTRAÎNER
De nombreux exercices, regroupés par **objectifs** et de **difficultés graduées**, comprenant notamment des exercices corrigés pour vous aider à **réviser**



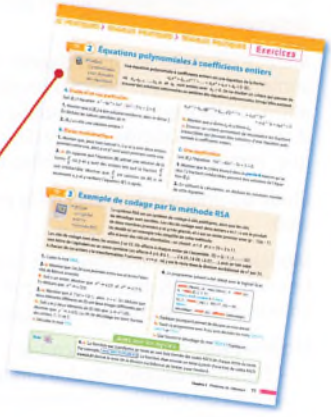
CAP VERS LE BAC
Un sujet commenté et des sujets d'écrit et d'oral pour se préparer au Baccalauréat



POUR FAIRE LE POINT
Un QCM corrigé sur les notions essentielles du chapitre.
Retrouvez les corrections détaillées sur
www. **bordas-indice.fr**

POUR ALLER PLUS LOIN
Des exercices d'**approfondissement** pour aller plus loin

TRAVAUX PRATIQUES
Des TP qui combinent l'expérimentation avec des logiciels et la résolution théorique



L'enseignement de spécialité prend appui sur la résolution de problèmes.
Cette approche permet une introduction motivée des notions mentionnées dans le programme.

Plusieurs exemples de problèmes sont donnés à titre indicatif. L'étude des situations envisagées dans le cadre de cet enseignement conduit à un travail de modélisation et place les élèves en position de recherche.

Les thèmes abordés sont particulièrement propices à l'utilisation des outils informatiques (logiciels de calcul, tableur) et à la mise en œuvre d'algorithmes.

Le niveau d'approfondissement des notions est guidé par les besoins rencontrés dans la résolution des problèmes traités.

Arithmétique

Les problèmes étudiés peuvent notamment être issus de la cryptographie ou relever directement de questions mathématiques, par exemple à propos des nombres premiers.

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

Il s'agit d'étudier des exemples de processus discrets, déterministes ou stochastiques, à l'aide de suites ou de matrices.
On introduit le calcul matriciel sur des matrices d'ordre 2. Les calculs sur des matrices d'ordre 3 ou plus sont essentiellement effectués à l'aide d'une calculatrice ou d'un logiciel.

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.

Sommaire

Les pictos du manuel

- Utilisation de la calculatrice
- Utilisation de logiciels
- Mise en œuvre d'algorithmes
- Raisonnement logique

Avant de commencer, se tester avec...

...des QCM

Choisir la (ou les) bonne(s) réponse(s).

➤ Savoir manipuler les entiers

	A	B	C	D
1 k désignant un entier relatif, un entier qui précède un multiple de 7 est de la forme	$7k+6$	$7(k-1)$	$7k-1$	$7k+8$
2 Indiquer quels ensembles ne contiennent que des entiers.	$\mathbb{N}$	$\mathbb{R}$	$\mathbb{Z}$	$\mathbb{Q}$
3 n désignant un entier relatif, l'entier $9n+6$ est toujours un multiple de	6	3	9	2
4 n étant un entier naturel, quel nombre est un entier ?	$\cos(2\pi n)$	$\sqrt{2}$	$\frac{n(n+1)}{2}$	$\frac{n}{3}$

➤ Savoir utiliser la divisibilité des entiers

5 Le reste de la division euclidienne de 24 par 5 est	5	4	-1	0,8
6 Le reste d'une division euclidienne par 7 ne peut pas prendre la valeur	0	7	3,5	6
7 Parmi ces nombres, quels sont ceux qui n'ont que deux diviseurs entiers naturels ?	1	0	2	10
8 Si un entier non nul n est divisible par 9, alors	$\frac{9}{n}$ est un entier	il est divisible par 3	le reste de la division de n par 3 est 0	$\frac{n}{9}$ est un entier
9 L'entier $17^3 - 7^3$ est multiple de	17	7	10	5

➤ Voir les réponses, p. 140

...des exercices

10 Poser, à la main, la division euclidienne de 737 par 7.

11 Rappeler comment distinguer un entier pair d'un entier impair à l'aide d'une division euclidienne.

12 Quels sont les entiers n s'écrivant sous la forme $3k$ avec $k \in \mathbb{Z}$?

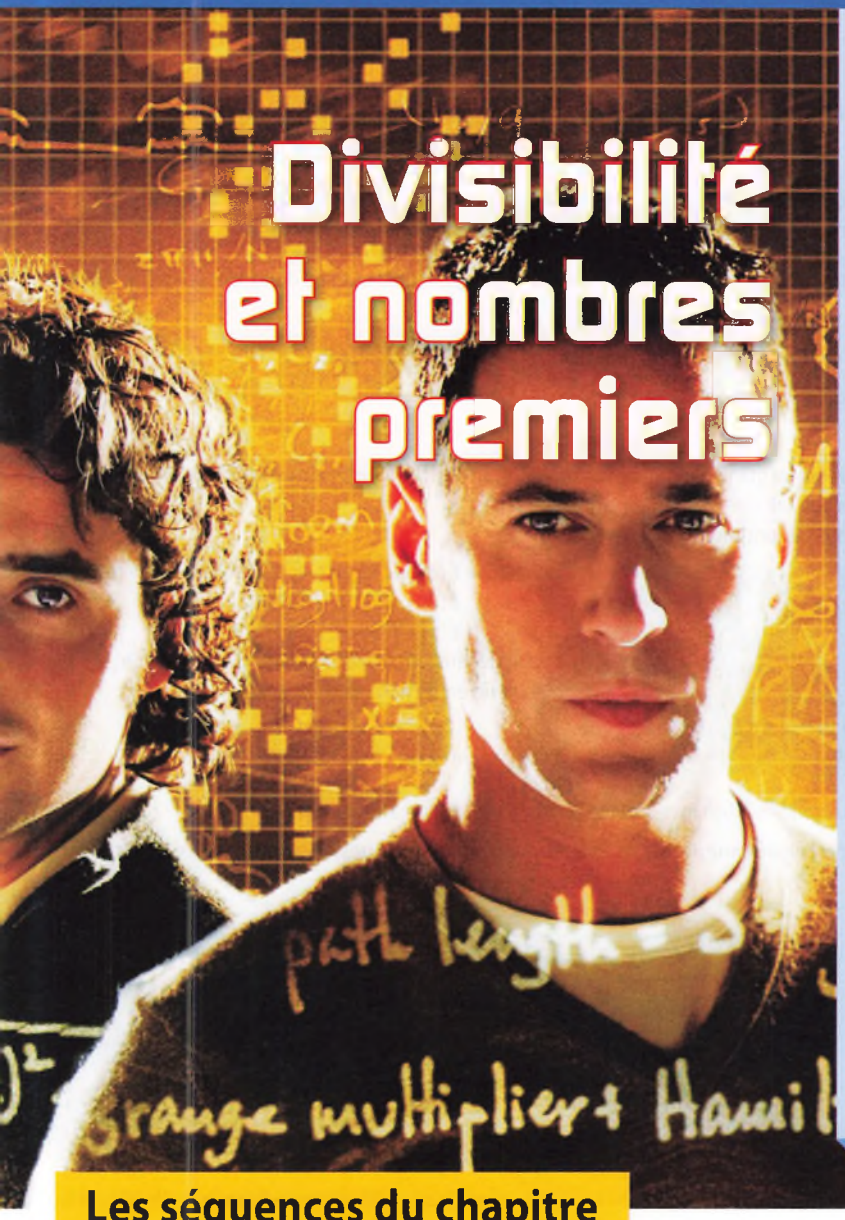
13 Donner la liste des entiers naturels diviseurs de 30.

14 Trouver dix solutions de l'équation $2x + y = 1$, où x et y sont des entiers relatifs.

➤ Voir les réponses, p. 140

CHAPITRE 1

Divisibilité et nombres premiers



Longtemps, l'arithmétique, c'est-à-dire l'étude des entiers, n'a passionné que les amoureux des mathématiques.

Depuis quelques dizaines d'années, les découvertes dans ce domaine ont été rendues plus visibles et économiquement cruciales par le rôle essentiel des propriétés des entiers dans les applications informatiques, au point que certains projets ont pu être classés top secret.

Il n'est donc pas étonnant de les trouver en bonne place dans des séries comme *Numb3rs*, même si son utilisation au quotidien, comme la détection d'erreurs dans un code-barres, peut sembler moins romanesque.

ISBN 1-4157-4240-5
0 97361 37744 5

Les séquences du chapitre

Le raisonnement logique Ilogique
Voir p. 11, 12, 16, 27, 28, 30, 31 et 39

Les algorithmes ALGO
Voir p. 8, 14, 17, 18, 19, 20, 26, 27, 28, 29, 31, 32, 34, 40 et 41

Utilisation de logiciels TICE
Voir p. 12, 15, 20, 26, 28, 34 et 35

Séquence 1 — Divisibilité et division euclidienne

Problème 1 — Diviseurs d'un entier ALGO

Objectif
Revoir la notion de diviseur d'un entier.

Cours 1
Divisibilité dans $\mathbb{Z}$

Partie A

Un triangle rectangle a des côtés de longueurs entières. L'un des côtés de l'angle droit a pour longueur 6. On aimerait déterminer les longueurs des deux autres côtés.

1. En notant x et y les longueurs cherchées (avec $x > y$), vérifier que l'on doit avoir $(x-y)(x+y) = 36$.

2. Quels sont les diviseurs positifs de 36 ?

3. Quels sont les couples d'entiers naturels $(a\,;b)$ vérifiant $ab = 36$?

4. En déduire les longueurs cherchées.

Partie B

Ayant à traiter un grand nombre de tels triangles, on cherche à systématiser la recherche des couples $(a\,;b)$ tels que $ab = n$ où n est un entier naturel.
On propose l'algorithme suivant :

```
Entrée : n entier, n > 2
Traitement :
Pour j de 1 à E(√n)
    Si j est un diviseur de n alors
        afficher j et n/j
    Fin Si
Fin Pour
```

La fonction E utilisée ici est la fonction partie entière :
$E(2{,}1) = E(2{,}9) = E(2) = 2$
$E(\pi) = E(3) = E(3{,}201) = 3$
Et plus généralement, $E(x) = n$ pour tout réel $x \in [n\,;n+1[$, n étant un entier naturel.

1. Quels seront les affichages obtenus lorsqu'on entre $n = 36$? $n = 38$?

2. Tester cet algorithme avec la calculatrice. Le programme correspondant est donné ci-dessous :

Casio

```
======DIVISEUR======
"N"?→N
For 1→J To Int (√N)
If N÷J=Int (N÷J)
Then J
N÷J
IfEnd
Next
"FIN"
```

Texas

```
PROGRAM:DIVISEUR
:Prompt N
:For(J,1,partEnt
(√(N))
:If N/J=partEnt(
N/J)
:Then
:Disp J
:Pause N/J
:End
:End
```

3. Expliquer pourquoi l'instruction $\frac{N}{j} = E\left(\frac{N}{j}\right)$ traduit la condition « j est un diviseur de N ».

4. Soit a et b deux entiers naturels tels que $ab = n$ avec $a \leqslant b$. Montrer que l'on a $a \leqslant \sqrt{n} \leqslant b$ et en déduire que le programme proposé affiche bien tous les couples d'entiers naturels $(a\,;b)$ tels que $ab = n$.

5. Justifier, avec ce qui précède, qu'un entier n a un nombre fini de diviseurs entiers naturels.

Problème 2 — Le code-barres

Objectif
Travailler la notion de diviseur et la notion de reste d'une division euclidienne.

Le code-barres de nombreux produits est constitué de treize chiffres. Les douze premiers chiffres permettent d'identifier le produit. Le treizième chiffre est une clé de contrôle qui permet de détecter une éventuelle erreur dans les 12 chiffres d'identification.
Si l'on note $a_1, a_2, \ldots, a_{13}$ les 13 chiffres d'un code-barres, la clé a_{13} est déterminée de façon à ce que l'entier $S = 3 \times (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) + a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}$ soit un multiple de 10.

Cours 1 et 2
Divisibilité dans $\mathbb{Z}$
Division euclidienne

1. Vérifier que le code 4971850187820 satisfait la contrainte définissant un code-barres valide.

2. Déterminer la clé de contrôle du code d'identification suivant :
978204732850.

3. Dans la suite, on notera r le reste de la division de $S - c$ par 10 où c est la clé. Vérifier que $c = 10 - r$ dans le cas de la question **2**.

4. a. Quelles sont les valeurs possibles d'un reste dans une division euclidienne par 10 ?
b. Pour l'une de ces valeurs, la clé ne peut pas être égale à $10 - r$. Laquelle ?
Quelle est la clé dans ce cas ?
c. Démontrer que lorsque le reste r est non nul, l'entier $10 - r$ est une clé qui convient.

5. Démontrer que la clé correspondant à une séquence $a_1, a_2, \ldots, a_{12}$ est unique, ce qui signifie que l'on a l'implication suivante : « Si c et c' sont deux entiers satisfaisant la définition de la clé pour la séquence d'identification $a_1, a_2, \ldots, a_{12}$ alors $c = c'$ ».

6. Peut-il correspondre plusieurs séquences $a_1, a_2, \ldots, a_{12}$ d'identification à une clé c donnée ?

7. On suppose qu'on a fait une erreur sur le chiffre a_2 en entrant un code-barres dans une base de données (et aucune autre erreur). Notons b_2 le chiffre qui s'est substitué à a_2 et :

$$S' = 3 \times (b_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) + a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}.$$

a. Donner un encadrement de la différence $a_2 - b_2$.
b. Calculer et encadrer la différence $S - S'$ et montrer que cette différence ne peut pas être un multiple de 10.
c. En déduire que le code obtenu ne satisfait pas les contraintes définissant un code-barres.

8. Le raisonnement précédent montre que la présence d'une erreur unique, sur un chiffre de rang pair, peut être détectée. Montrer de même que la présence d'une erreur unique, faite sur un chiffre de rang impair, peut être détectée.

9. Donner un exemple montrant que lorsque deux erreurs sont commises, elles ne seront pas nécessairement détectées.

Problème 3 Le calendrier

Objectif
Redécouvrir la signification du quotient et du reste dans une division euclidienne.

Cours 2
Division euclidienne

On sait que le 1er janvier 2013 est un mardi. À partir de ce renseignement, on aimerait pouvoir déterminer le jour de la semaine de n'importe quelle date de l'année 2013, puis de l'année 2014.


Calendrier Aztèque

1. On se propose de chercher quel jour de la semaine tombe le 1er mai et si l'on aura un jour de congé de plus ou non en 2013.
a. Combien de jours n s'écoulent entre ces deux dates ?
(Ne compter qu'une seule des deux dates extrêmes.)
b. En divisant le nombre précédent par 7, en déduire le nombre q de semaines complètes qui se sont écoulées entre ces deux dates.
c. Calculer alors le nombre r de jours restant après ces q semaines pour atteindre la date du 1er mai. Écrire n en fonction de 7, q et r.
d. En déduire quel jour de la semaine est le 1er mai 2013.

2. Déterminer de la même façon quel est le jour de la semaine du 11 novembre 2013. On écrira comme en **1. c.** l'égalité reliant le nombre n' de jours écoulés du 1er janvier au 11 novembre, 7 et les entiers q' et r' définis comme à la question **1**.

3. Quel est le jour de la semaine du 11 novembre 2014 ?

Cours 1

Divisibilité dans $\mathbb{Z}$

Notation

b divise a se note $b|a$.

Définition Soit a et b deux entiers.
On dit que **b divise a** (ou que b est un **diviseur** de a) lorsqu'il existe un entier k tel que $a = kb$.
On dit aussi, dans ce cas, que a est **multiple** de b.

Exemple : 3 divise 12 puisque $12 = 3k$ où k est l'entier 4. 3 est donc un diviseur de 12 et 12 un multiple de 3. On peut écrire $3|12$.

À noter

Le mot « entier » sans précision désignera toujours un entier relatif (c'est-à-dire un élément de $\mathbb{Z}$).

Propriété Soit a et b deux entiers. On a les équivalences suivantes :
$$b|a \Leftrightarrow (-b)|a \Leftrightarrow b|(-a) \Leftrightarrow (-b)|(-a).$$

Démonstration Si b divise a, il existe un entier q tel que $bq = a$.
On a alors $(-b)(-q) = a$, $b(-q) = -a$ et $(-b)q = -a$.
Comme q et $-q$ sont des entiers, cela établit la propriété.

a et $-a$ ont donc les mêmes diviseurs dans $\mathbb{Z}$ et les diviseurs négatifs de a sont les opposés des diviseurs positifs de a. En conséquence, on se restreindra souvent par la suite à l'étude de la divisibilité dans $\mathbb{N}$.

Propriété Soit n un entier naturel non nul.
Tout diviseur positif d de n est compris entre 1 et n.
Tout entier naturel non nul a donc un nombre fini de diviseurs.

Notation

On notera $D(n)$ l'ensemble des diviseurs dans $\mathbb{N}$ de l'entier naturel n.

Démonstration Soit $n \in \mathbb{N} - \{0\}$ et soit d un entier naturel divisant n. Il existe un entier naturel k tel que $n = kd$. Comme $n > 0$ et $d > 0$, on a $k > 0$, soit $k \geqslant 1$ puisque k est entier.
D'où $kd \geqslant d$, c'est-à-dire $n \geqslant d$.
Ainsi n a au plus n diviseurs dans $\mathbb{N}$ et au plus $2n$ diviseurs dans $\mathbb{Z}$.

Exemple : L'ensemble des diviseurs de 6 dans $\mathbb{N}$ est $D(6) = \{1 ; 2 ; 3 ; 6\}$ et les diviseurs de 6 dans $\mathbb{Z}$ sont $1 ; 2 ; 3 ; 6$ et leurs opposés $-1 ; -2 ; -3 ; -6$.

Remarques :

- Pour tout entier a : $1 \times a = a$ donc 1 divise a et a divise a. Tout entier a admet donc au moins un diviseur dans $\mathbb{N}$ et tout entier a distinct de 1 admet au moins deux diviseurs dans $\mathbb{N}$.
- Pour tout entier a, on a $a \times 0 = 0$: tout entier divise 0 et $D(0) = \mathbb{N}$.

À noter

Un multiple d'un multiple de a est un multiple de a.

Propriétés

(1) Pour tous entiers a, b, c, si a divise b et b divise c, alors a divise c.

(2) Pour tous entiers a, b, c, si a divise b et divise c, alors a divise les entiers $mb + nc$ (où m et n sont entiers). En particulier, a divise les entiers $b + c$ et $b - c$.

Vocabulaire

$mb + nc$ (où m et n sont entiers) est appelée une **combinaison linéaire à coefficients entiers** de b et c.

Démonstrations

(1) Si a divise b et b divise c, il existe des entiers k et k' tels que $ka = b$ et $k'b = c$. D'où $(k'k)a = c$.
Comme kk' est un entier (car c'est un produit d'entiers), on en déduit que a divise c.

(2) Si a divise b et divise c, il existe des entiers k et k' tels que $ka = b$ et $k'a = c$.
Dans ce cas, pour tous entiers m et n, on a $(km + k'n)a = mb + nc$.
On en déduit que a divise toute combinaison linéaire de b et c.

Exemples :

- Si un entier n divise 16, alors, d'après la propriété (1), n divise également 2×16, 3×16, 4×16, …, $16k$ où k est entier.
- Si un entier a divise 5 et 3, alors, d'après la propriété (2), a divise l'entier $5 - 3 = 2$. Cette propriété (2) permet aussi d'écrire que a divise l'entier $1 \times 5 - 2 \times 3 = -1$ (a est donc égal à 1 ou à -1).

Savoir-faire 1

➤ Voir les exercices 48 à 51

Utiliser une relation de divisibilité

1. Déterminer les entiers puis les entiers naturels n tels que 6 divise $n+17$.

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

3. Déterminer les entiers n tels que $2n+3$ divise $n-2$.

Méthode

1. Pour déterminer les entiers n tels qu'un entier A divise une expression $f(n)$, on applique la définition de la divisibilité.

2. Pour déterminer les entiers n tels que $f(n)$ divise A, on résout les équations $f(n)=d$ pour tout diviseur d de A.

3. Pour résoudre un problème du type $h(n) \mid g(n)$, on se ramène à un problème de la forme précédente : $f(n) \mid A$ par des combinaisons judicieusement choisies.

Solution

1. 6 divise $n+17$ si, et seulement si, il existe un entier k tel que $n+17=6k$, ce qui équivaut à $n=6k-17$. Les entiers solutions sont donc les entiers de la forme $6k-17$, avec k entier.
Les entiers naturels solutions sont donc les entiers de la forme $6k-17$, avec k entier au moins égal à 3 (en effet $6k-17 \geqslant 0$ équivaut à $k \geqslant \frac{17}{6}$, c'est-à-dire à $k \geqslant 3$ puisque k est entier).

2. Les diviseurs de 6 sont : -6 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 6.
Ainsi $2n-5 \mid 6$ équivaut à $2n-5=-6$ ou $2n-5=-3$ ou $2n-5=-2$ ou $2n-5=-1$ ou $2n-5=1$ ou $2n-5=2$ ou $2n-5=3$ ou $2n-5=6$.
D'où $2n-5 \mid 6 \Leftrightarrow 2n=-1$ ou $n=1$ ou $2n=3$ ou $n=2$ ou $n=3$ ou $2n=7$ ou $n=4$ ou $2n=11$.
Les équations $2n=-1$, $2n=3$, $2n=7$ et $2n=11$ n'ont pas de solution dans $\mathbb{Z}$, donc les entiers cherchés sont : 1 ; 2 ; 3 ; 4.

3. Soit n un entier tel que $2n+3$ divise $n-2$. Pour un tel entier n, $2n+3$ divise $2n+3$ et divise $n-2$, donc $2n+3$ divise la combinaison $(2n+3)-2(n-2)$, c'est-à-dire 7. (On choisit les coefficients de la combinaison $(2n+3)-2(n-2)$ de façon à obtenir une expression ne dépendant plus de n.)
Les diviseurs de 7 étant -7, -1, 1 et 7, on en déduit que :

$$2n+3=-7 \text{ ou } 2n+3=-1 \text{ ou } 2n+3=1 \text{ ou } 2n+3=7$$

soit : $n=-5$ ou $n=-2$ ou $n=-1$ ou $n=2$.
On vérifie alors explicitement par des calculs que ces quatre entiers sont bien solutions.
On conclut ensuite les entiers solutions sont : -5 ; -2 ; -1 ; 2.

Logique Il ne faut pas oublier ici la réciproque car on a raisonné à l'aide d'implications.

Savoir-faire 2

➤ Voir l'exercice 5

Résoudre des équations diophantiennes

1. Déterminer les entiers naturels x et y tels que $x^2-y^2=25$.

2. Déterminer les entiers x et y tels que $x^2-y^2=25$.

Méthode

Pour résoudre une équation diophantienne, on peut essayer de se ramener par factorisation à une équation du type $A \times B = C$, où on connaît les diviseurs de C.

Solution

1. L'égalité $x^2-y^2=25$ s'écrit aussi $(x-y)(x+y)=25$.
En particulier, si x et y sont des entiers solutions, $x-y$ et $x+y$ sont des diviseurs de 25.
Pour un couple $(x\,;y)$ solution, comme x et y sont positifs, $x+y$ est positif et $x+y>x-y$.
Le produit $(x-y)(x+y)$ étant positif, on en déduit que $x-y$ est également positif et donc $x>y$.
Les décompositions de 25 en produit de deux entiers naturels sont : $25=1\times25$ et $25=5\times5$.
Si $x-y=1$, alors $x+y=25$ et, par addition, $2x=26$, soit $x=13$ et $y=12$.
Si $x-y=5$, alors $x+y=5$ et $2x=10$, soit $x=5$ et $y=0$.
On a donc $(x\,;y)=(13\,;12)$ ou $(x\,;y)=(5\,;0)$.
On vérifie alors que ces deux couples sont effectivement solutions (on n'a pas raisonné par équivalences).
Conclusion : les couples d'entiers naturels solutions sont les couples (13 ; 12) et (5 ; 0).

2. Pour résoudre dans $\mathbb{Z}\times\mathbb{Z}$ cette équation, on remarque que l'on a l'équivalence suivante :

$$(x\,;y) \text{ solution} \Leftrightarrow (-x\,;y) \text{ solution} \Leftrightarrow (x\,;-y) \text{ solution} \Leftrightarrow (-x\,;-y) \text{ solution.}$$

Les couples d'entiers solutions sont donc les couples :

$$(-13\,;12)\,;\ (13\,;-12)\,;\ (13\,;12)\,;\ (-13\,;-12)\,;\ (5\,;0)\,;\ (-5\,;0).$$

Cours 2

Division euclidienne

Théorème Soit a et b deux entiers naturels, b étant distinct de zéro.
Il existe un unique couple d'entiers $(q\,;r)$ satisfaisant les deux conditions :
$$a = bq + r \text{ et } 0 \leqslant r < b.$$
L'entier q est égal à la partie entière de $\frac{a}{b}$, c'est-à-dire à l'unique entier n tel que $n \leqslant \frac{a}{b} < n+1$.

Démonstration Si un couple $(q\,;r)$ satisfait les deux conditions, on a nécessairement :
$$qb \leqslant a < (q+1)b.$$
Cet entier q doit donc vérifier $q \leqslant \frac{a}{b} < q+1$, on a donc nécessairement $q = E\left(\frac{a}{b}\right)$
(où E désigne la fonction partie entière).
On a alors nécessairement $r = a - qb$ pour satisfaire l'égalité $a = bq + r$ et on a bien, avec cet entier, l'encadrement $0 \leqslant r < b$ et l'égalité $a = bq + r$.

Définition L'entier q est appelé **quotient** de la division euclidienne de a par b, l'entier r est appelé **reste** de la division.

Effectuer la division euclidienne de a par b, c'est déterminer le couple $(q\,;r)$.

Exemple : $19 = 5 \times 3 + 4$. Le quotient de la division euclidienne de 19 par 5 est 3.
Mais le quotient de la division euclidienne de 19 par 3 n'est pas 5, car $4 > 3$.

Calcul pratique d'une division euclidienne

	Tableur	Casio	Texas
quotient Q de la division euclidienne de A par B	ENT(A/B)	Intg($A \div B$) (touche OPTN menu *NUM*)	partEnt(A/B) (touche math menu *NUM*)
reste R	MOD(A;B)	$A-B\times Q$	$A-B^{*}Q$

Propriété On peut étendre le résultat : pour a et b entiers, $b \neq 0$, il existe un unique couple $(q\,;r)$ d'entiers tel que $a = bq + r$ et $0 \leqslant r < |b|$.

Exemple : $-19 = (-5) \times 4 + 1$.
Comme $0 \leqslant 1 < |-5|$, le couple (quotient ; reste) de la division de -19 par -5 est $(4\,;1)$.

Propriété Soit a et b deux entiers, $b \neq 0$.
b divise a si, et seulement si, le reste de la division euclidienne de a par b est nul.

Propriété b désignant un entier naturel, $b \geqslant 2$, tout entier s'écrit sous une, et une seule, des formes bq, $bq+1$, $bq+2$, …, $bq+(b-1)$ (où q est entier).

Logique
Cette propriété peut être utilisée pour raisonner par « disjonction des cas » (voir Savoir-faire 4).

Cet énoncé n'est qu'une réécriture du principe de division euclidienne exposé ci-dessus.

Exemples :
- Tout entier s'écrit sous l'une des formes $2q$, $2q+1$.
- Tout entier s'écrit sous l'une des formes $3q$, $3q+1$, $3q+2$.

Propriété Soit b un entier supérieur ou égal à 2.
Parmi b entiers consécutifs, l'un est multiple de b.

Démonstration Notons N le plus grand de ces entiers consécutifs.
L'entier N s'écrit sous la forme $N = bq + r$ avec q, r entiers et $0 \leqslant r \leqslant b-1$.
L'entier $N - r$ (qui est l'un des b entiers consécutifs N, $N-1$, $N-2$, …, $N-(b-1)$ considérés) s'écrit donc sous la forme $N - r = bq$: c'est un multiple de b.

Exemples :
- Soit n un entier, alors n ou $n+1$ est pair.
- Soit n un entier, alors l'un des entiers n, $n+1$, $n-1$ est multiple de 3.

Savoir-faire 3

➤ Voir les exercices 69 et 70

Utiliser la définition de la division euclidienne

Énoncé 1 Le reste de la division euclidienne de 2 015 par l'entier naturel b est 500. Quelles sont les valeurs possibles de b ?

Conseil
Dans l'écriture d'une division euclidienne, penser à la condition sur le reste, elle est indispensable.

Solution

Notons q le quotient de cette division. On recherche un entier naturel b tel que $2\,015 = bq + 500$, donc tel que $bq = 1\,515$. b est donc un diviseur de 1 515.
Les diviseurs positifs de 1 515 sont les entiers : 1 ; 3 ; 5 ; 15 ; 101 ; 303 ; 505 ; 1 515.
Comme le reste dans la division par b est égal à 500, on a $b > 500$. b ne peut donc prendre que les valeurs 505 et 1 515. Ces deux valeurs correspondent aux deux divisions :

$$2\,015 = 505 \times 3 + 500 \quad \text{et} \quad 2\,015 = 1\,515 \times 1 + 500.$$

Énoncé 2 Un entier a s'écrit sous la forme $a = 8k + 6$ où k est un entier.
Déterminer le quotient et le reste de la division euclidienne de a par 4.

Solution

On a $a = 4 \times 2k + (4 + 2)$, soit $a = 4 \times (2k + 1) + 2$.
$2k + 1$ est un entier puisque k est entier et l'entier 2 vérifie $0 \leqslant 2 < 4$.
Le quotient de la division de a par 4 est donc $2k + 1$ et le reste est 2.

Savoir-faire 4

➤ Voir les exercices 72 et 73

Utiliser les restes de la division euclidienne

Énoncé 1 Soit n un entier non multiple de 5.
Démontrer que n^2 s'écrit sous l'une des formes $5k + 1$, $5k - 1$ où k est un entier.

Méthode
Dans le cas d'une divisibilité par 5, on peut écrire tout entier sous l'une des formes $5k$, $5k + 1$, $5k + 2$, $5k + 3$, $5k + 4$ et raisonner par disjonction des cas.

Solution

N'étant pas multiple de 5, n s'écrit sous la forme $5q + r$ avec $1 \leqslant r \leqslant 4$.
On a donc : $n^2 = (5q + r)^2$, soit $n^2 = 25q^2 + 10q + r^2 = 5(5q^2 + 2q) + r^2$.
Ce qui s'écrit encore : $n^2 = 5 \times t + r^2$ où $t = 5q^2 + 2q$ est entier (comme somme de produits d'entiers).
- Si $r = 1$, n^2 est de la forme $5k + 1$ avec $k = t$.
- Si $r = 2$, $n^2 = 5 \times t + 4$ s'écrit $n^2 = 5t + 5 - 1$, soit $n^2 = 5k - 1$ où $k = t + 1$ est entier.
- Si $r = 3$, $n^2 = 5 \times t + 9$ s'écrit $n^2 = 5t + 2 \times 5 - 1$, soit $n^2 = 5k - 1$ où $k = t + 2$ est entier.
- Si $r = 4$, $n^2 = 5 \times t + 16$ s'écrit $n^2 = 5t + 3 \times 5 + 1$, soit $n^2 = 5k + 1$ où $k = t + 3$ est entier.

Pour tout entier n, son carré n^2 s'écrit donc soit sous la forme $5k + 1$, soit sous la forme $5k - 1$ (avec k entier).

Énoncé 2 Soit $a = n(n + 4)(n - 4)$ où n est un entier.
Établir que a est multiple de 3 quelle que soit la valeur de n.

Solution

L'entier n s'écrit sous l'une des formes $3q$, $3q + 1$, $3q + 2$, avec q entier.
- Si $n = 3q$, alors $a = 3 \times q(n + 4)(n - 4)$.

a s'écrit donc sous la forme $a = 3b$ où $b = q(n + 4)(n - 4)$ est un entier.
- Si $n = 3q + 1$, alors $a = n(n + 4)(3q - 3)$, soit $a = 3 \times n(n + 4)(q - 1)$.

a s'écrit donc sous la forme $a = 3b$ où $b = n(n + 4)(q - 1)$ est un entier.
- Si $n = 3q + 2$, alors $a = n(3q + 6)(n - 4)$, soit $a = 3 \times n(q + 2)(n - 4)$.

a s'écrit donc sous la forme $a = 3b$ où $b = n(q + 2)(n - 4)$ est entier.
Pour toute valeur de l'entier n, a s'écrit sous la forme $3b$, avec b entier.
a est donc un multiple de 3.

Problème 4 Le crible de Matiassevitch

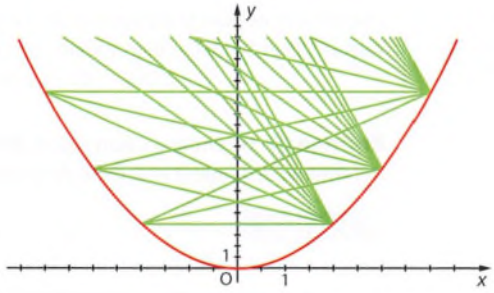
Objectif
Découvrir les notions de nombre premier et nombre composé.

Cours 3
Les nombres premiers

Point Histoire
Youri Matiassevitch (né en 1947) est un mathématicien russe. Il a notamment apporté une réponse au « dixième problème de Hilbert ».

Un nombre premier est un entier p supérieur ou égal à 2 qui n'admet pas d'autre diviseur que 1 et p.
Soit $\mathcal{P}$ la parabole d'équation $y = x^2$ dans le plan muni d'un repère $(O ; \vec{u}, \vec{v})$.
Soit i et j deux entiers naturels, $P_i(i ; i^2)$ le point d'abscisse i de la parabole $\mathcal{P}$ et $N_j(-j ; j^2)$ le point d'abscisse $-j$ de cette parabole.

1. Dans cette question, $n = 20$.
On a tracé sur la figure ci-dessous les segments $[P_i N_j]$ pour $2 \leqslant i \leqslant E(\sqrt{n})$ et $2 \leqslant j \leqslant E\left(\frac{n}{2}\right)$.



a. Que peut-on penser des ordonnées des points de l'axe $(O ; \vec{v})$ qui appartiennent à l'un des segments verts ? qui n'appartiennent à aucun des segments verts ?
b. Démontrer que le coefficient directeur de la droite $(P_i N_j)$ est $i - j$.
c. Démontrer que l'ordonnée à l'origine de la droite $(P_i N_j)$ est $i \times j$.

2. Dans un dictionnaire, on trouve la définition suivante pour le mot *cribler* : « passer au crible : tamiser, trier, calibrer ». Expliquer pourquoi on parle de crible des nombres premiers pour la figure obtenue lorsqu'on trace tous les segments $[P_i N_j]$ pour i et j supérieurs ou égaux à 2.

3. Dans la construction qui suit, on choisit $n = 100$.
On trace la parabole d'équation $y = x^2$.
On construit les segments $[P_i N_j]$ pour $2 \leqslant i \leqslant E(\sqrt{n})$ et $2 \leqslant j \leqslant E\left(\frac{n}{2}\right)$
Expliquer pourquoi la figure constitue un crible des nombres premiers inférieurs ou égaux à n.

Problème 5 Test de primalité et infinité des nombres premiers ALGO

Objectif
Découvrir un test de primalité et l'infinité des nombres premiers.

Cours 3
Les nombres premiers

Entrer les programmes suivants dans la calculatrice :

Algorithme	Casio	Texas

Entrée : N entier naturel
Traitement :
Pour J de 2 à $E(\sqrt{N})$
  Si J divise N
  alors afficher J
  et stopper
  le programme
  Fin Si
Fin Pour
Sortie : Afficher N
	======PPD ======
	"N":?→N
	For 2→J To Int√(N)
	N÷J→Q
	If Q=Int(Q)
	Then J
	Stop
	IfEnd
	Next
	N
		PROGRAM:PPD
		:Prompt N
		:For(J,2,partEnt(√(N)))
		:N/J→Q
		:If Q=partEnt(Q)
		:Then
		:Disp J
		:Stop
		:End
		:End
		:Disp N

1. a. Quelle est la sortie lorsqu'on entre $N = 11$?
b. Quelle est la sortie lorsqu'on entre $N = 12$?

2. a. Justifier qu'un entier sera toujours affiché quelle que soit l'entrée N.
b. Établir que l'entier affiché par le programme est toujours un nombre premier, diviseur de N.
c. En déduire que tout entier N non premier admet au moins un diviseur premier au plus égal à sa racine carrée.

3. Expliquer comment se servir de ce programme comme test de primalité (c'est-à-dire comme test permettant de reconnaître si un nombre est premier ou non).

4. On se demande s'il est possible qu'un tel algorithme n'affiche en sortie qu'un nombre fini de valeurs différentes. Pour cela, on note $p_1, p_2, \ldots, p_k$ les entiers que l'on a déjà obtenus à l'affichage après un certain nombre d'essais et on cherche à établir que l'on peut obtenir d'autres entiers à l'affichage.
On exécute l'algorithme avec l'entrée $N = p_1 p_2 \ldots p_k + 1$.
a. Quel est le reste de la division euclidienne de N par p_1 ?
b. Établir que l'algorithme affichera une valeur non encore obtenue avec cette entrée N.
c. Expliquer pourquoi on a ainsi établi qu'il existe une infinité de nombres premiers.

Problème 6

Les nombres de Fermat

Objectif
Découvrir des nombres historiques.

Cours 4
Décomposition en facteurs premiers

En 1640, le mathématicien Pierre de Fermat pensait que les nombres $F_n = 2^{(2^n)} + 1$ (que l'on appelle aujourd'hui les nombres de Fermat) sont tous premiers.

1. Vérifier avec une calculatrice (en utilisant par exemple le programme du problème précédent) que les entiers F_j sont premiers pour $0 \leqslant j \leqslant 4$.

2. Il faut attendre 1732 pour avoir une preuve (apportée par le mathématicien Leonhard Euler) du caractère non premier de F_5.
Aujourd'hui, l'instruction du logiciel Xcas `factoriser_entier(2^(2^5)+1)` ou l'instruction `factor(2^(2^5)+1)` avec le logiciel Derive retourne de façon quasi instantanée la factorisation 641×6700417.
Il faut attendre 1880 pour que le français F. Landry obtienne la factorisation de F_6.
On peut vérifier qu'un logiciel de calcul formel, avec un ordinateur actuel, retourne de façon quasi instantanée la factorisation de F_6.

```
factoriser_entier(2^(2^6)+1)
                    274177.67280421310721
```

Aujourd'hui encore, on ne sait factoriser que peu de nombres de Fermat. Pour comprendre cela, on peut commencer par se donner une idée de la taille de ces nombres. En supposant que l'on écrive 5 chiffres par seconde, et sachant que F_{30} a plus de 10^8 chiffres, combien de temps faudra-t-il pour écrire un tel entier ?

3. Vérifier que tous les nombres de Fermat sont impairs.

4. Démontrer, par récurrence, que pour tout entier $n \geqslant 1$, on a :
$$F_0 F_1 \ldots F_{n-1} = F_n - 2.$$

5. Déduire des deux questions précédentes que si d est un diviseur commun à deux nombres de Fermat, alors $d = 1$.

6. Sachant que tout entier admet au moins un facteur premier, déduire de ce qui précède une démonstration de l'infinité des nombres premiers.

Cours 3

Les nombres premiers

Définitions

- Un entier naturel n distinct de 1 est dit **premier** lorsqu'il admet pour seuls diviseurs dans $\mathbb{N}$ les entiers 1 et n.
- Un entier distinct de 1 non premier est dit **composé**.

1 n'est ni premier, ni composé.

Les nombres premiers inférieurs à 20 sont 2, 3, 5, 7, 11, 13, 17 et 19.

À noter

Tout entier naturel $n \geqslant 2$ admet donc au moins un diviseur premier.

Propriété

Soit $n \geqslant 2$ un entier naturel.

Le plus petit diviseur de n compris entre 2 et n est premier.

Démonstration

Soit n un entier strictement supérieur à 1.

Soit p le plus petit des diviseurs de n compris entre 2 et n.

Raisonnons par l'absurde pour établir que p est premier : s'il ne l'était pas, il serait composé et il admettrait un diviseur d tel que $1 < d < p$; mais d serait alors un diviseur de n plus petit que p, ce qui contredit la définition de p.

Propriété

Tout entier naturel composé n admet un diviseur premier au plus égal à $\sqrt{n}$.

Démonstration

Soit n un entier naturel composé.

D'après la propriété précédente, le plus petit diviseur de n compris entre 2 et n est premier.

Notons-le d. d est distinct de n puisque n est composé.

On peut donc écrire $n = d \times d'$, avec $2 \leqslant d \leqslant d' \leqslant n$ ($d' \neq 1$ sinon on aurait $n = d$).

On en déduit $dd \leqslant dd'$, soit $d^2 \leqslant n$ ou encore $d \leqslant \sqrt{n}$.

Point Histoire

Cette démonstration a plus de 2 000 ans, elle a été réalisée par **Euclide** au III^e^ siècle avant J.-C.

Propriété

Il existe une infinité de nombres premiers.

Démonstration

Raisonnons par l'absurde en supposant qu'il existe un nombre fini d'entiers premiers.

Soit p le plus grand d'entre eux et soit N le produit de tous ces nombres premiers : $2 \times 3 \times 5 \times 7 \times \ldots \times p$.

Soit à présent l'entier $N' = N + 1$: le reste de la division euclidienne de N' par 2, 3, 5, … ou p est 1, donc N' n'est divisible par aucun des entiers 2, 3, 5, …, p.

Or, d'après la deuxième propriété de cette page, l'un au moins des entiers premiers divise N'.

On a ainsi abouti à une contradiction.

Propriété **Test de primalité**

Soit $n \geqslant 2$ un entier naturel.

Si aucun des entiers compris entre 2 et $\sqrt{n}$ ne divise n, alors n est premier.

Logique

La contraposée de l'implication « si p alors q » est l'implication « si non q alors non p ».

Démonstration

On a vu ci-dessus que si l'entier $n \geqslant 2$ est composé, alors il admet un diviseur inférieur ou égal à $\sqrt{n}$.

La contraposée de cette implication est la propriété énoncée.

Exemple : Soit $n = 149$. Alors, $\sqrt{n} \approx 12{,}2$.

On divise successivement n par 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 et 12 pour savoir s'il est premier.

On peut aller plus vite en divisant uniquement n par les nombres premiers inférieurs à $\sqrt{n}$, soit 2, 3, 5, 7 et 11 : n n'est divisible par aucun de ces nombres, donc il est premier.

Savoir-faire 5

➤ Voir l'exercice 81

Reconnaître si un entier est premier ALGO

1. Le nombre $n = 2\,017$ est-il premier ?

2. On cherche à automatiser la réponse à ce type de question. Pour cela, écrire un algorithme, à traduire ensuite sur calculatrice, testant si un entier naturel n donné en entrée est premier.

Méthode
Pour savoir si un entier naturel n est premier, on le divise successivement par 2, 3, 5, 7, ... jusqu'à $\sqrt{n}$.

Solution

1. $E\left(\sqrt{2017}\right) = 44$, on teste donc chacun des entiers 2, 3, 4, ..., 44.
Comme aucun de ces entiers n'est un diviseur de 2 017, on peut en conclure que 2 017 est premier.

Remarque : Lorsqu'on déroule cet algorithme à la main, on peut éviter certaines divisions. Si l'on a constaté que 2 ne divise pas n alors il est inutile de tester les multiples de 2 (4,6,8, ...) : ils ne diviseront pas non plus n. On peut faire le même raisonnement avec chacun des entiers qui suivent. Ce raisonnement montre qu'il nous suffit de tester les entiers **premiers** compris entre 2 et $\sqrt{n}$ (c'est également ce qu'affirme la deuxième propriété de la page de cours ci-contre). Cela n'apporte bien sûr une amélioration à l'algorithme utilisé que si l'on dispose déjà d'une liste des nombres premiers inférieurs à $\sqrt{n}$ ou si l'on peut rapidement éliminer les multiples d'entiers déjà testés.

2.

Algorithme

Entrée : N entier naturel
Traitement :
Pour J de 2 à $E\left(\sqrt{N}\right)$
  Si J divise N
    alors afficher
    « NON PREMIER »
    stopper le programme
  Fin Si
Fin Pour
Sortie : Afficher « PREMIER »

Casio

```
======PRIMALIT======
"N":?→N
For 2→J To Intg (√N)
If N÷J=Intg (N÷J)
Then "NON PREMIER"
Stop
IfEnd
Next
"PREMIER"
```

Texas

```
PROGRAM:PRIMALIT
:Prompt N
:For(J,2,partEnt
(√(N)))
:If N/J=partEnt(
N/J)
:Then
:Disp "NON PREMI
ER"
:Stop
:End
:End
:Disp "PREMIER"
```

Point Histoire
Avant les outils de calculs modernes, on dressait et utilisait des tables de nombres premiers.

Savoir-faire 6

➤ Voir l'exercice 82

Démontrer qu'un nombre n'est pas premier

1. Pour $n \in \mathbb{N}$, on pose $f(n) = n^2 + 5n + 6$. Établir que $f(n)$ est composé pour tout entier n.

2. Pour $n \in \mathbb{N}$, on pose $g(n) = n^2 + 3n - 10$. Établir que $g(n)$ est composé pour tout entier $n \geqslant 3$.

Méthode
Pour montrer qu'un nombre n'est pas premier, on l'écrit sous la forme $m \times n$, avec m et n strictement supérieurs à 1.

Solution

1. On obtient les racines de f à l'aide du discriminant : -2 et -3.
On en déduit la factorisation : $f(n) = (n + 2)(n + 3)$.
Comme n est un entier naturel, $n + 2$ et $n + 3$ sont des entiers au moins égaux à 2 et l'entier $f(n)$ est donc un nombre composé.

2. On calcule les racines de g à l'aide du discriminant : 2 et -5.
Pour tout entier naturel n, on a donc $g(n) = (n - 2)(n + 5)$.
Pour $n \geqslant 4$, on a $n - 2 \geqslant 2$ et $n + 5 \geqslant 9$, donc $g(n)$ est le produit de deux entiers strictement supérieurs à 1 et est donc composé.
Pour $n = 3$, le facteur $n - 2$ est égal à 1 et l'argument précédent n'est plus valable mais $g(3) = 8$ et 8 est composé.

Cours 4

Décomposition en facteurs premiers

Point Histoire

Ce théorème, qui est un théorème central de l'arithmétique, est explicité pour la première fois par **Gauss**, mathématicien allemand, en 1801, mais il semble acquis depuis des travaux d'Euclide dans l'Antiquité bien qu'ils n'aient pas été publiés dans les *Éléments*.

Théorème de décomposition en facteurs premiers

Tout entier naturel au moins égal à 2 est premier ou produit de nombres premiers.

Démonstration On raisonne par l'absurde.

La propriété est vraie pour les premiers entiers : 2 ; 3 ; $4 = 2^2$; 5 ; $6 = 2 \times 3$... Supposons qu'elle ne soit pas vraie pour tous les entiers et notons n le premier entier ni premier, ni produit de nombres premiers.

n admet un diviseur premier p et on peut donc écrire $n = pd$ où $1 < d < n$.

Comme n est le premier entier ne satisfaisant pas la propriété, d la satisfait : mais l'écriture $n = pd$ mène alors à une contradiction.

Théorème d'unicité de la décomposition (admis)

La décomposition d'un entier naturel n en produit de nombres premiers est unique.

Ce résultat pourra être démontré avec des résultats du chapitre 2 (théorème de Gauss).

Exemple : Soit n un entier égal au carré d'un entier m dont la décomposition en facteurs premiers est $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Comme on a $m^2 = p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$, on peut affirmer que la décomposition de n est $p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$.

On peut de ce fait facilement caractériser les carrés parfaits par leur décomposition en facteurs premiers.

Algorithme de décomposition en facteurs premiers ALGO

À noter

On peut dérouler l'algorithme à la main si l'entier à décomposer n'est pas trop grand :

N	D
924	2
462	2
231	3
77	7
11	11
1	

$924 = 2^2 \times 3 \times 7 \times 11$

Algorithme

Entrée : N entier naturel, $N \geqslant 2$
Traitement :
D prend la valeur 2
Tant Que $N \neq 1$
  Tant Que D divise N
    Afficher D
    D prend la valeur N/D
  Fin Tant Que
  D prend la valeur $D + 1$
Fin Tant Que

Casio

```
======DECOMP  ======
"N":?→N
2→D
While N≠1
While Ints (N÷D)=N÷D
D
N÷D→N
WhileEnd
D+1→D
WhileEnd
"FIN"
```

Texas

```
PROGRAM:DECOMP
:Prompt N
:2→D
:While N≠1
:While partEnt(N
/D)=N/D
:Pause D
:N/D→N
:End
:D+1→D
:End
```

Propriété **Une caractérisation des diviseurs d'un entier**

Un entier naturel d divise un entier naturel n si, et seulement si, les exposants des facteurs premiers de la décomposition de d sont au plus égaux à ceux de la décomposition de n.

Démonstration

(1) Supposons que l'entier d divise n. Soit p un facteur premier de d apparaissant avec l'exposant α. p^α divise d, donc divise n. Donc p apparaît au moins avec l'exposant α dans la décomposition de n.

(2) Réciproquement, soit $n = p_1^a p_2^b \dots p_r^\ell$, et $d = p_1^{a'} p_2^{b'} \dots p_r^{\ell'}$, avec :

$$0 \leqslant a' \leqslant a,\ 0 \leqslant b' \leqslant b, \dots,\ 0 \leqslant \ell' \leqslant \ell.$$

Dans ce cas d divise n : $n = p_1^{a-a'} p_2^{b-b'} \dots p_r^{\ell-\ell'} \times d$

où $p_1^{a-a'} p_2^{b-b'} \dots p_r^{\ell-\ell'}$ est entier puisque $a - a', b - b', \dots, \ell - \ell'$ sont positifs.

Exemple : $12 = 2^2 \times 3$. Les diviseurs positifs de 12 sont donc les entiers s'écrivant sous la forme $2^\beta \times 3^\delta$ avec $0 \leqslant \beta \leqslant 2$ et $0 \leqslant \delta \leqslant 1$, c'est-à-dire les entiers :

$$2^0 \times 3^0 = 1\ ;\ 2^0 \times 3^1 = 3\ ;\ 2^1 \times 3^0 = 2\ ;\ 2^1 \times 3^1 = 6\ ;\ 2^2 \times 3^0 = 4\ ;\ 2^2 \times 3^1 = 12.$$

Savoir-faire 7

➤ Voir les exercices 97 et 98

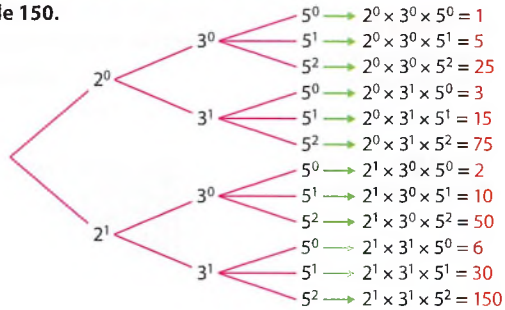
Déterminer les diviseurs d'un entier

Déterminer l'ensemble des diviseurs de 150.

Méthode
Pour déterminer tous les diviseurs d'un entier, on le décompose en facteurs premiers, puis on se sert d'un arbre donnant tous les cas possibles.

Solution

$150 = 2 \times 3 \times 5^2$.
Ses diviseurs sont de la forme $2^p \times 3^q \times 5^r$, avec $p \in \{0 ; 1\}$, $q \in \{0 ; 1\}$ et $r \in \{0 ; 1 ; 2\}$.
Il y en a donc $2 \times 2 \times 3 = 12$.
On peut obtenir tous ses diviseurs à l'aide d'un arbre comme celui ci-contre.



Savoir-faire 8

➤ Voir l'exercice 99

Déterminer le nombre de diviseurs d'un entier ALGO

1. Peut-on trouver un entier naturel b tel que le nombre de diviseurs dans $\mathbb{N}$ de l'entier $A = 50 \times 2^b$ soit égal à 14 ?

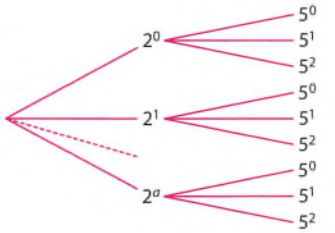
2. Un entier n a pour décomposition en facteurs premiers : $n = p^a q^b r^c$ (où p, q, r sont des nombres premiers). Quel est le nombre de diviseurs positifs de n ?

3. En s'aidant de l'algorithme et du programme de décomposition en facteurs premiers proposé dans le cours ci-contre, écrire un programme pour la calculatrice retournant le nombre de diviseurs de l'entier naturel non nul N donné en entrée.

Méthode
Pour déterminer le nombre de diviseurs d'un entier, on peut s'aider de l'arbre construit sur ses facteurs premiers.

Solution

1. On décompose A en facteurs premiers :
$A = 2^a \times 5^2$, où $a = b + 1$ est un entier naturel non nul.
On construit un arbre (ou plutôt un schéma de l'arbre : on ne connaît pas la valeur de a).
On construit $a + 1$ branches au départ, car un facteur 2^p, avec $0 \leqslant p \leqslant a$, apparaît dans la décomposition des diviseurs de A.
On trace ensuite 3 branches car les diviseurs de A ont dans leur décomposition l'un des facteurs 5^0, 5^1, 5^2.



On en déduit le nombre de diviseurs de A : $3(a + 1)$. Comme 14 n'est pas divisible par 3, on ne peut pas donner à b de valeur satisfaisant la condition imposée.

2. En appliquant le principe multiplicatif (principe de l'arbre) : le nombre de diviseurs de n est égal à $(1 + a)(1 + b)(1 + c)$.

3. Un entier N ayant pour décomposition en facteurs premiers $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ possède $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$ diviseurs positifs.
Dans le programme de décomposition donné dans le cours ci-contre, on introduit une variable S qui prendra successivement les valeurs $\alpha_1 + 1$, $\alpha_2 + 1$, …, $\alpha_k + 1$ et une variable P qui prendra successivement les valeurs : 1, $\alpha_1 + 1$, $(\alpha_1 + 1) \times (\alpha_2 + 1)$, $(\alpha_1 + 1) \times (\alpha_2 + 1) \times (\alpha_3 + 1)$, … , $(\alpha_1 + 1) \times (\alpha_2 + 1) \times (\alpha_3 + 1) \times \ldots \times (\alpha_k + 1)$.

Casio

```
======NBDIV  ======
"N":?→N
1→P
2→D
While N≠1
1→S
While Ints (N÷D)=N÷D
S+1→S
N÷D→N
WhileEnd
P×S→P
D+1→D
WhileEnd
P
```

Texas

```
PROGRAM:NBDIV
:Prompt N
:1→P
:2→D
:While N≠1
:1→S
:While partEnt(N
/D)=N/D
:S+1→S
:N/D→N
:End
:P*S→P
:D+1→D
:End
:Disp P
```

Problème 7 Deux traitements pour une même sortie ALGO

Objectif
Introduire la notion de congruence.

Cours 5
Congruences dans $\mathbb{Z}$

Entrer les deux programmes ci-dessous dans la calculatrice (A et B sont des entiers naturels, M est un entier au moins égal à 2).

PROGRAMME 1

Casio

```
"A":?→A:"B":?→B
"M":?→M
(A−B)÷M→K
If Int≥ (K)=K
Then "OUI"
Else "NON"
IfEnd
```

Texas

```
:Prompt A,B
:Prompt M
:(A−B)/M→K
:If K=partEnt(K)

:Then
:Disp "OUI"
:Else
:Disp "NON"
:End
```

PROGRAMME 2

Casio

```
"A":?→A:"B":?→B
"M":?→M
Int≥ (A÷M)→Q
A−Q×M→R
(B−R)÷M→J
If Int≥ (J)=J
Then "OUI"
Else "NON"
IfEnd
```

Texas

```
:Prompt A,B
:Prompt M
:partEnt(A/M)→Q
:A−Q*M→R
:(B−R)/M→J
:If J=partEnt(J)
:Then
:Disp "OUI"
:Else
:Disp "NON"
:End
```

1. Tester ces deux programmes pour quelques triplets d'entiers ($M \geqslant 2$).
Les sorties semblent-elles différer ?

2. Lorsque la sortie est « OUI » pour le programme 1, les entiers A et B sont dits *congrus modulo M*, ce que l'on note $A \equiv B\ (M)$.
Lorsque la sortie est « NON », les entiers A et B ne sont pas congrus modulo M : $A \not\equiv B\ (M)$.
a. Donner un triplet (A, B, M) tels que $A \equiv B\ (M)$, puis un triplet (A, B, M) tels que $A \not\equiv B\ (M)$.
b. En interprétant le programme 1, donner la définition de l'expression « A et B sont congrus modulo M » en utilisant l'expression « est divisible par ».

3. Il semble que des entrées identiques dans les programmes 1 et 2 donnent des sorties identiques. L'objectif de cette question est de vérifier si cette propriété est bien générale.
a. Que contient la mémoire R après la ligne $A - Q * M \rightarrow R$ du programme 2 ?
b. Vérifier que le test conditionnel du programme 2 renvoie « OUI » lorsque $(B - R)$ est multiple de M.
c. En déduire que le programme 2 affiche « OUI » si, et seulement si, les entiers A et B ont le même reste dans la division euclidienne par M.
d. Montrer l'identité des sorties (pour des entrées identiques) des deux programmes, c'est-à-dire l'équivalence suivante : « $A - B$ est multiple de M si, et seulement si, A et B ont le même reste dans la division euclidienne par M ».

Problème 8 Puissances d'un entier modulo *m* TICE

Objectif
Découvrir les propriétés des congruences à l'aide d'un logiciel de calcul formel.

Cours 5
Congruences

Dans cette activité, on suppose connue la notion de congruence modulo m.
L'objectif est de découvrir des propriétés de calculs des congruences.

1. Ouvrir une feuille tableur dans le logiciel Xcas.
Entrer ensuite dans la cellule **A0** : `m:=11` et dans la cellule **A1** : `p:=7`.
Dans les cellules de la colonne **B**, entrer les entiers : 1 ; 2 ; 3 ; …

2. `irem(a,b)` retourne le reste de la division euclidienne de a par b.
Inscrire la formule `=irem((B0)^p,m)` dans la cellule **C0** et recopier cette formule vers le bas.
L'instruction `hasard` de Xcas tire un entier naturel au hasard (entre 0 et 2^{32}).
Entrer dans la cellule **E0** la formule `=B0+m*hasard`. Recopier ensuite cette formule vers le bas.
Justifier que les entiers obtenus en colonne **E** sont congrus modulo m aux entiers de la même ligne de la colonne **B**.

3. Afficher dans la cellule **D0** le reste du nombre de la cellule **E0** à la puissance p, modulo m.
Recopier la formule utilisée vers le bas.
Comparer les contenus des colonnes **C** et **D**.
Quelle propriété pourrait-on conjecturer à partir de cette observation ?

	A	B	C	D	E
0	11	1	1	1	3920694889
1	7	2	7	7	10396290038
2	0	3	9	9	20789418961
3	0	4	5	5	19587653672
4	0	5	3	3	7803329429
5	0	6	8	8	5408759439

Modifier les valeurs de m et p dans les cellules **A0** et **A1** (en entrant par exemple `m:=17`, `p:=13`).
La propriété semble-t-elle encore satisfaite ?

4. Entrer, dans une ligne de commande de Xcas, les instructions `factoriser(a^2-b^2)`, `factoriser(a^3-b^3)`, `factoriser(a^4-b^4)`, `factoriser(a^5-b^5)`…
Que peut-on conjecturer ? En observant les factorisations obtenues ci-dessous, conjecturer une formule de factorisation de $a^n - b^n$ précise puis démontrer cette formule.

2	**factoriser(a^3-b^3)**
	$(a-b)\cdot(a^2+a\cdot b+b^2)$
3	**factoriser(a^5-b^5)**
	$(a-b)\cdot(a^4+a^3\cdot b+a^2\cdot b^2+a\cdot b^3+b^4)$
4	**factoriser(a^7-b^7)**
	$(a-b)\cdot(a^6+a^5\cdot b+a^4\cdot b^2+a^3\cdot b^3+a^2\cdot b^4+a\cdot b^5+b^6)$

5. Déduire de la conjecture prouvée à la question précédente une démonstration de la conjecture faite en question **3**.

Problème 9 La preuve par neuf

Objectif
Redécouvrir les critères de divisibilité usuels.

Cours 6
Critères de divisibilité

Dans cette activité, le cours sur les congruences est supposé avoir été travaillé.
On rappelle que tout entier naturel s'écrit sous la forme $n = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \ldots + 10^pa_p$ où $a_0, a_1, \ldots, a_p$ sont des entiers compris entre 0 et 9 (a_0 est le chiffre des unités, a_1 le chiffre des dizaines…).

1. Vérifier que 10 est congru à 1 modulo 3.

2. En déduire que $10^k \equiv 1\ (3)$ pour tout entier naturel k non nul.

3. En déduire qu'un entier naturel n est congru à la somme de ses chiffres modulo 3.

4. En déduire le critère de divisibilité par 3 usuel : « Un entier est divisible par 3 si, et seulement si, la somme de ses chiffres en écriture décimale est multiple de 3 ».

5. Établir de même qu'un entier est congru modulo 9 à la somme de ses chiffres et en déduire le critère de divisibilité par 9 usuel.

6. Soit A et B deux entiers et $P = AB$. On note a, b, p les restes respectifs des divisions de A, B, P par m où m est un entier au moins égal à 2. On note q le reste de la division de ab par m.
a. Montrer que $p = q$.
b. Max ne dispose pas de calculatrice et effectue le produit de $A = 2\,015$ par $B = 2\,018$. Il trouve $P = 4\,046\,170$. Déterminer a, b, p, q en choisissant $m = 9$ et en utilisant les résultats de la question **5**. Qu'en déduit-on pour le calcul de Max ?
c. Si Max avait choisi $m = 3$, déterminer a, b, p, q lui aurait-il permis de détecter son erreur ?
d. Le procédé utilisé à la question **b.** est appelé « preuve par 9 ».
Ce procédé permet-il de détecter toutes les erreurs lors d'une multiplication de deux entiers ?

Cours 5

Congruences dans $\mathbb{Z}$

Notation

On écrit
$a \equiv b\ (m)$
ou bien $a \equiv b\ (\text{mod } m)$
ou encore
$a \equiv b$ (modulo m).
On parle de relation
de congruence modulo m.

Définition Soit m un entier naturel.
Deux entiers a et b sont dits **congrus modulo m** lorsque $a - b$ est multiple de m.

Exemples : • $12 \equiv 2\ (5)$ car $12 - 2$ est multiple de 5.
• $4 \equiv -3\ (7)$ car $4 - (-3)$ est multiple de 7.

Théorème Soit m un entier naturel non nul.
Deux entiers a et b sont congrus modulo m si, et seulement si, la division euclidienne de a par m a le même reste que la division euclidienne de b par m.

Démonstration

(1) Supposons que a et b aient le même reste r dans la division euclidienne par m.
On a donc : $a = mq + r$ et $b = mq' + r$, avec q et q' entiers et $0 \leqslant r < m$.
D'où l'on déduit : $a - b = mq + r - mq' - r = m(q - q')$.
Comme $q - q'$ est un entier, $a - b$ est divisible par m.

(2) Réciproquement, supposons que $a - b$ soit divisible par m. Il existe k entier tel que :
$a - b = km$.
Soit r le reste de la division euclidienne de b par m, on a l'égalité : $b = mq + r$, avec q entier et $0 \leqslant r < m$.
On a donc $a = b + km = mq + r + km = (q + k)m + r$, avec $0 \leqslant r < m$.
Puisque $q + k$ est un entier, ceci prouve que la division euclidienne de a par m donne pour quotient $q + k$ et pour reste r : a et b ont bien même reste dans la division euclidienne par m.

À noter

Pour $m = 1$, $a \equiv b\ (m)$
est vrai pour tous entiers
a et b.
Pour $m = 0$, $a \equiv b\ (m)$
signifie $a = b$.
Les valeurs 0 et 1 pour
le nombre m seront
donc systématiquement
exclues par la suite.

Corollaire Soit m un entier naturel au moins égal à deux, et a un entier.
Il existe un unique entier $r \in [0\,;\, m - 1]$ tel que $r \equiv a(m)$, cet entier est le reste de la division euclidienne de a par m.

En particulier, deux entiers distincts compris entre 0 et $m - 1$ ne sont pas congrus modulo m.

Propriétés Soit m un entier, $m \geqslant 2$ et a, b, c des entiers.
(1) $a \equiv a\ (m)$.
(2) Si $a \equiv b\ (m)$ et $b \equiv c\ (m)$, alors $a \equiv c\ (m)$.

Ces propriétés sont évidentes avec la caractérisation de la congruence par les restes.

Propriétés **Compatibilité avec les opérations**
Soit m un entier, $m \geqslant 2$ et a, b, a', b' des entiers.
(1) Si $a \equiv b\ (m)$ et $a' \equiv b'\ (m)$, alors $a + a' \equiv b + b'\ (m)$.
(2) Si $a \equiv b\ (m)$ et $a' \equiv b'\ (m)$, alors $aa' \equiv bb'\ (m)$.
(3) Pour $n \in \mathbb{N}^*$, si $a \equiv b\ (m)$, alors $a^n \equiv b^n\ (m)$.

Vocabulaire

On dit que la congruence
modulo m est **compatible**
avec l'addition
(respectivement
la multiplication)
pour traduire la propriété (1)
(respectivement (2)).

Démonstrations

(1) Si $a \equiv b\ (m)$ et $a' \equiv b'\ (m)$, m divise $a - b$ et $a' - b'$.
m divise donc la combinaison linéaire $(a - b) + (a' - b') = (a + a') - (b + b')$ et on a donc :
$a + a' \equiv b + b'\ (m)$.

(2) De même, si $a \equiv b\ (m)$ et $a' \equiv b'\ (m)$, m divise $a - b$ et $a' - b'$ et m divise la combinaison $a'(a - b) + b(a' - b') = aa' - bb'$. D'où $aa' \equiv bb'\ (m)$.

(3) Raisonnons par récurrence. Si a et b sont des entiers tels que $a \equiv b\ (m)$ alors la relation $a^n \equiv b^n\ (m)$ est vraie pour $n = 1$. Soit $n \geqslant 1$ un entier pour lequel $a^n \equiv b^n\ (m)$. Alors, avec la propriété (2), on a : $a^n \times a \equiv b^n \times b\ (m)$, c'est-à-dire $a^{n+1} \equiv b^{n+1}\ (m)$. L'hérédité est ainsi établie.
On a donc $a^n \equiv b^n\ (m)$ pour tout entier naturel n.

Exemple : Si a et b sont deux entiers tels que $a \equiv b\ (7)$, comme $4 \equiv -3\ (7)$, on peut affirmer que $4a \equiv -3b\ (7)$. On notera la « non-compatibilité » avec la division ; on a par exemple $3 \times 4 \equiv 3 \times 6\ (6)$ mais 4 et 6 ne sont pas congrus modulo 6.

Savoir-faire 9

➤ Voir les exercices 106 et 107

Résoudre une congruence

1. Déterminer les entiers x tels que $2+x \equiv 4\ (6)$.

2. Déterminer les entiers x tels que $2\times x \equiv 4\ (6)$.

3. Déterminer les entiers x tels que $x^3 \equiv 4^3\ (7)$.

Méthode
Pour résoudre une équation formée d'une congruence, on applique les règles de calcul, ou on fait un tableau recensant tous les cas possibles pour la variable.

Solution

1. La compatibilité de la congruence avec l'addition permet d'écrire :

$$2+x \equiv 4\ (6) \Leftrightarrow 2+x+(-2) \equiv 4+(-2)\ (6)$$

soit : $2+x \equiv 4\ (6) \Leftrightarrow x \equiv 2\ (6)$.

Les entiers x solutions sont donc les entiers de la forme $2+6k$ avec $k \in \mathbb{Z}$.

2. On raisonne par disjonction des cas.

x est nécessairement congru à l'un des entiers 0, 1, 2, 3, 4, 5 modulo 6 :

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

On en déduit l'équivalence suivante : $2x \equiv 4\ (6) \Leftrightarrow x \equiv 2\ (6)$ ou $x \equiv 5\ (6)$.

L'ensemble des entiers x tels que $2x \equiv 4\ (6)$ est donc constitué des entiers de la forme $2+6k$ avec $k \in \mathbb{Z}$ et des entiers de la forme $5+6k$ avec $k \in \mathbb{Z}$.

Remarque : Il est important ici de remarquer qu'il n'est pas légitime de « simplifier » par 2 la congruence pour la résoudre. D'après ce qui précède, on constate que l'équation $2\times x \equiv 4\ (6)$ n'est pas équivalente à l'équation $x \equiv 2\ (6)$ qui serait obtenue en « simplifiant » par 2 (ni d'ailleurs à l'équation $x \equiv 2\ (3)$ dans laquelle on aurait également « simplifié » le module de la congruence).

3. On remarque que $4^3 \equiv 1\ (7)$. On raisonne par disjonction des cas.

Modulo 7, x est nécessairement congru à 0, 1, 2, 3, 4, 5 ou 6 :

x modulo 7	0	1	2	3	4	5	6
x^3 modulo 7	0	1	1	6	1	6	6

L'ensemble des entiers x tels que $x^3 \equiv 4^3\ (7)$, c'est-à-dire tels que $x^3 \equiv 1\ (7)$, est donc constitué des entiers de la forme $1+7k$ ou $2+7k$ ou $4+7k$ avec $k \in \mathbb{Z}$.

Savoir-faire 10

➤ Voir les exercices 108 et 109

Déterminer des restes à l'aide des congruences

1. Déterminer le reste de la division de 2^n par 3 en fonction de l'entier naturel n.

2. En déduire le reste de la division de $2^{2\,013}$ par 3.

3. Déterminer le reste de la division euclidienne de $2^{3n}-2^n$ par 3, n désignant un entier naturel.

Méthode
Pour s'engager dans la détermination du reste de la division par n des puissances successives d'un entier, chercher d'abord ces restes avec les exposants les plus petits.

Solution

1. On commence par calculer les restes pour les premières valeurs de l'entier n :

Valeurs de n	0	1	2	3	4	5	6	7	8	…
2^n modulo 3	1	2	1	2	1	2	1	2	1	…

Ces calculs semblent montrer qu'il y a deux cas selon la parité de n.

Si $n=2p$ avec $p \in \mathbb{N}$, alors $2^{2p}=4^p$. Or $4 \equiv 1\ (3)$, d'où $4^p \equiv 1^p\ (3)$ et $4^p \equiv 1\ (3)$.

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

Ainsi le reste de la division euclidienne de 2^n par 3 est 1 si n est pair, et 2 si n est impair.

2. 2 013 est impair, donc le reste de la division par 3 de 2^{2013} est 2.

3. Pour tout entier n : $2^{3n}-2^n=2^n\times(2^{2n}-1)$. Pour tout entier naturel n, $2n$ est pair et on a donc, d'après la question **1.** : $2^{2n} \equiv 1\ (3)$. D'où $2^n\times(2^{2n}-1) \equiv 0\ (3)$ pour tout entier naturel n.

Le reste de la division euclidienne de $2^{3n}-2^n$ par 3 est donc 0 pour tout entier naturel n.

Cours 6

Critères de divisibilité

Propriété Soit m un entier naturel tel que $m \geqslant 2$.
Pour tout entier a, on a l'équivalence suivante : a divisible par $m \Leftrightarrow a \equiv 0\ (m)$.

Cette propriété est une conséquence immédiate de la définition des congruences ou de la caractérisation par les restes puisque $a \equiv 0\ (m)$ signifie que le reste de la division euclidienne de a par m est 0.

Exemple : On a $7 \equiv -1\ (4)$ car $7 - (-1)$ est multiple de 4.
Pour tout entier naturel n, on a donc $7^{2n} \equiv (-1)^{2n}\ (4)$, soit $7^{2n} \equiv 1 (4)$.
On en déduit que, pour tout entier naturel n, l'entier $7^{2n} - 1$ est congru à 0 modulo 4, c'est-à-dire est divisible par 4.

Remarque : On peut également démontrer que $7^{2n} - 1$ est multiple de 4 pour tout entier naturel n par une démonstration par récurrence.

Définition Écriture décimale d'un entier
Soit d un entier naturel. Notons $a_0, a_1, \ldots, a_n$ les chiffres de son écriture décimale (entiers entre 0 et 9).
On a $d = a_0 + 10 \times a_1 + 10^2 \times a_2 + \ldots + 10^n \times a_n$.
Cette somme $\sum_{j=0}^{n} 10^j a_j$ sera parfois notée sous la forme $\overline{a_n a_{n-1} \ldots a_1 a_0}$.

Exemple : $2\,013 = 3 + 1 \times 10 + 0 \times 10^2 + 2 \times 10^3$.

Les propriétés des congruences permettent d'établir efficacement de nombreux « critères de divisibilité ».

Propriété Critères de divisibilité usuels

(1) Un entier est **pair** (c'est-à-dire divisible par 2) si, et seulement si, son chiffre des unités est 0, 2, 4, 6 ou 8.

(2) Un entier est **divisible par 5** si, et seulement si, son chiffre des unités est 0 ou 5.

(3) Un entier est **divisible par 3** si, et seulement si, la somme de ses chiffres est un multiple de 3.

(4) Un entier est **multiple de 9** si, et seulement si, la somme de ses chiffres est multiple de 9.

(5) Un entier $d = \overline{a_n a_{n-1} \ldots a_1 a_0}$ est **divisible par 4** si, et seulement si, l'entier $\overline{a_1 a_0}$ est divisible par 4.

À noter
On démontre ainsi des critères de divisibilité découverts et utilisés depuis la classe de Sixième.

Démonstrations Soit $d = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$ où $a_0, a_1, \ldots, a_n$ sont des entiers entre 0 et 9 (chiffres de l'écriture décimale de d).

(1) $10 \equiv 0\ (2)$, d'où $10^p \equiv 0\ (2)$ pour $p \geqslant 1$, donc $\sum_{j=0}^{n} 10^j a_j \equiv a_0\ (2)$.
On a ainsi établi que le reste de la division euclidienne de d par 2 est égal au reste de la division de a_0 par 2. En particulier, d est divisible par 2 si, et seulement si, a_0 est divisible par 2, c'est-à-dire pour a_0 égal à 0, 2, 4, 6 ou 8.

(2) $10 \equiv 0\ (5)$, d'où $10^p \equiv 0\ (5)$ pour $p \geqslant 1$, donc $d \equiv a_0\ (5)$.
On a ainsi établi que le reste de la division euclidienne de d par 5 est égal au reste de la division de a_0 par 5. En particulier, d est divisible par 5 si, et seulement si, a_0 est divisible par 5, c'est-à-dire pour a_0 égal à 0 ou 5.

(3) $10 \equiv 1\ (3)$, d'où $10^p \equiv 1\ (3)$, et $d \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0\ (3)$.
On a ainsi établi que le reste de la division euclidienne de d par 3 est égal au reste de la division euclidienne de la somme de ses chiffres par 3. En particulier, ces deux restes sont nuls en même temps, d'où le critère.

(4) Comme $10 \equiv 1\ (9)$, le raisonnement fait avec **(3)** précédemment conduit au critère de divisibilité par 9.

(5) Pour $p \geqslant 2$, on a $10^p \equiv 0\ (4)$. Ainsi, $d \equiv 10a_1 + a_0\ (4)$. Or, $10a_1 + a_0$ n'est autre que $\overline{a_1 a_0}$, donc d est divisible par 4 si, et seulement si, $\overline{a_1 a_0}$ est divisible par 4.

Exemple : a est un chiffre. Tout entier dont trois chiffres sont égaux à a et tous les autres chiffres égaux à 0 est multiple de 3. La somme des chiffres de cet entier est en effet $3a$, qui est un multiple de 3.

Savoir-faire 11

➤ Voir les exercices 120 et 121

Utiliser une congruence pour montrer une divisibilité

1. Pour $n \in \mathbb{Z}$, on pose $g(n) = n^2 - 3n + 6$. Pour quels entiers $g(n)$ est-il divisible par 5 ?

2. Montrer que, pour tout entier naturel n, le nombre $5^{2n} - 14^n$ est divisible par 11.

Méthode

Pour prouver qu'un entier N est divisible par m, on peut chercher à montrer que $N \equiv 0\ (m)$. On profite alors des propriétés des congruences pour mener un raisonnement efficace.

Solution

1. La question revient à résoudre l'équation $g(n) \equiv 0\ (5)$.

On opère par disjonction des cas : n est congru à 0, 1, 2, 3 ou 4 modulo 5.

Par exemple lorsque $n \equiv 3\ (5)$, on peut écrire, en utilisant les propriétés sur les congruences, que :

$$g(n) \equiv 3^2 - 3 \times 3 + 6\ (5).$$

D'où $g(n) \equiv 6\ (5)$ ou encore $g(n) \equiv 1(5)$.

En traitant les autres cas de façon analogue, on obtient le tableau ci-dessous :

n modulo 5	0	1	2	3	4
$g(n)$ modulo 5	1	4	4	1	0

Les entiers n tels que $g(n)$ est multiple de 5 sont les entiers $4 + 5k$, avec k entier.

2. $5^{2n} = (5^2)^n = 25^n$. Or $25 \equiv 3\ (11)$, d'où $5^{2n} \equiv 3^n\ (11)$.

Comme $14 \equiv 3\ (11)$, on a : $14^n \equiv 3^n\ (11)$. D'où $5^{2n} - 14^n \equiv 0\ (11)$.

Ceci montre que, quel que soit l'entier naturel n, le nombre $5^{2n} - 14^n$ est divisible par 11.

Savoir-faire 12

➤ Voir les exercices 127 et 128

Établir un critère de divisibilité

1. En utilisant la congruence $10 \equiv -1\ (11)$, déterminer un critère de divisibilité par 11.

2. L'appliquer aux nombres 201 520 142 013 et 201 420 132 012.

3. Établir que l'entier $A = 201\,520\,142\,013^{2016} - 2\,018^{672}$ est divisible par 11.

Méthode

Pour déterminer un critère de divisibilité par m, on écrit le nombre donné sous la forme $10^n a_n + \ldots + 10a_1 + a_0$ et on utilise des congruences modulo m.

Solution

1. Soit $N = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$: $N = 10^n a_n + \ldots + 10^2 a_2 + 10\,a_1 + a_0$.

Comme $10 \equiv -1\ (11)$, on en déduit que $N \equiv \sum_{j=0}^{n} (-1)^j \times a_j\ (11)$.

On en déduit un critère de divisibilité par 11 : N est divisible par 11 si, et seulement si, la somme alternée $a_0 - a_1 + a_2 - a_3 + \ldots$ est divisible par 11.

On remarquera que ce qui précède établit en fait que N et la somme alternée de ses chiffres ont toujours le même reste dans la division euclidienne par 11.

2. Pour 201 520 142 013 : $3 - 1 + 0 - 2 + 4 - 1 + 0 - 2 + 5 - 1 + 0 - 2 = 3$,

qui n'est pas divisible par 11, donc 201 520 142 013 n'est pas divisible par 11.

Pour le nombre 201 420 132 012 : $2 - 1 + 0 - 2 + 3 - 1 + 0 - 2 + 4 - 1 + 0 - 2 = 0$,

et ainsi 201 420 132 012 est divisible par 11.

3. D'après la question précédente, on a $201\,520\,142\,013 \equiv 3\ (11)$.

On en déduit que $201\,520\,142\,013^3 \equiv 3^3\ (11)$.

Comme $3^3 \equiv 5\ (11)$, on a obtenu $201\,520\,142\,013^{3\times 672} \equiv 5^{672}\ (11)$.

Par ailleurs $8 - 1 + 0 - 2 = 5$, donc $2\,018 \equiv 5\ (11)$.

Finalement l'entier A est congru, modulo 11, à $5^{672} - 5^{672} = 0$ et A est bien multiple de 11.

Remarque : Le nombre A n'est pas accessible à la plupart des calculatrices (dépassement de capacité), ce qui amène à conduire un raisonnement tel que celui qui précède.

Exercices

Les exercices dont les numéros sont sur fond blanc sont corrigés à la fin du manuel.

POUR DÉMARRER

Le mot « entier » sans précision désignera toujours un entier relatif (c'est-à-dire un élément de $\mathbb{Z}$).

Divisibilité

1 Quelle est la différence entre l'ensemble des entiers relatifs et l'ensemble des entiers naturels ?

2 Dresser la liste des diviseurs positifs des entiers 36, 49 et 126 sans outil de calcul.

3 Dresser la liste des diviseurs dans $\mathbb{Z}$ des entiers 36, 49 et 126.

4 **Avec un tableur** TICE

Dresser la liste des diviseurs positifs des entiers 36, 49 et 126 à l'aide d'un tableur. Pour cela, en colonne **A**, entrer les entiers 1, 2, 3, …, n et utiliser en colonne **B** la fonction **SI()** du tableur ainsi que la fonction **MOD()**.

5 Soit a et b deux entiers naturels non nuls.
Regrouper les phrases ayant la même signification :

A a est un diviseur de b.
B a est divisible par b.
C a est un multiple de b.
D a divise b.
E Le reste de la division de a par b est zéro.
F Le quotient $\frac{a}{b}$ est un entier.
G La partie entière de $\frac{a}{b}$ est égale à $\frac{a}{b}$.

6 Combien d'entiers compris entre −50 et 75 le nombre 17 divise-t-il ?

7 Est-il vrai que le produit de deux entiers naturels consécutifs est toujours divisible par 2 ?

8 Est-il vrai que la somme de trois entiers consécutifs est toujours divisible par 3 ?

9 Montrer que la somme de deux entiers impairs est un entier pair.

10 Existe-t-il un entier m qui soit multiple de 14 et diviseur de 100 ?

11 Montrer que si n est un entier pair, alors l'entier $A = n(n^2 + 20)$ est multiple de 8.

12 Pierre affirme : « Si le carré de l'entier a divise l'entier n, alors a divise $\sqrt{n}$ ». Son professeur lui répond que son implication n'a a priori pas de sens. Pourquoi ?

13 La proposition suivante est-elle vraie : « Si l'entier a divise l'entier b et divise l'entier c, alors a^2 divise le produit bc » ?

14 Soit n un entier.
On pose $a = 2n + 7$ et $b = n + 1$.
1. Calculer $a - 2b$.
2. Soit d un entier divisant a et divisant b.
Quelles sont les valeurs possibles de d ?

15 Soit n un entier relatif non nul. Est-il vrai que le nombre de diviseurs dans $\mathbb{Z}$ de cet entier n est toujours pair ?

16 Fatima affirme : « Les diviseurs positifs d'un entier naturel n marchent toujours par 2 : si a divise n, il existe un diviseur b de n tel que $ab = n$. Un entier a donc toujours un nombre pair de diviseurs positifs. »
1. Que penser de ce raisonnement ?
2. Quels sont les entiers ayant un nombre impair de diviseurs positifs ?

17 Soit a un chiffre. Deux naturels sont diviseurs de chacun des entiers de la forme $\overline{aa}$. Lesquels ?

18 ALGO On considère le programme suivant :

Casio	Texas
"N":?→N N÷37→N N÷3→N	:Prompt N :N/37→N :N/3→N :Disp N

1. Quelle est la sortie avec l'entrée $n = 666$?
2. Quelle est la sortie pour une entrée de la forme $\overline{aaa}$ (où a est un chiffre) ? Expliquer.

Division euclidienne

19 Effectuer la division euclidienne de a par b dans les cas ci-dessous. On rappelle que le quotient d'une division euclidienne peut être obtenu avec la fonction partie entière de la calculatrice.

1. $a = 2\,013$; $b = 7$.
2. $a = -2\,013$; $b = 7$.
3. $a = 7$; $b = 2\,013$.
4. $a = -7$; $b = 2\,013$.

Pour les exercices 20 à 22, on rappelle que E désigne la fonction partie entière.

20 Pour quels entiers n a-t-on $E\left(\frac{n}{7}\right) = 0$?

21 Pour quels entiers n a-t-on $E\left(\frac{n}{7}\right) = \frac{n}{7}$?

22 Pour quels entiers n a-t-on $n - 7 \times E\left(\frac{n}{7}\right) = 0$?

23 ALGO On considère le programme suivant :

Casio	Texas
"A":?→A:"B":?→B A→R While R≥B R−B→R WhileEnd	:Prompt A,B :A→R :While R≥B :R−B→R :End :Disp R

1. Quelle sera la sortie avec les entrées $A = 27$ et $B = 5$?
2. Quelle sera la sortie avec les entrées $A = 31$ et $B = 7$?
3. A et B étant des entiers naturels non nuls, que représente la sortie R ?

24 Expliquer pourquoi on peut affirmer que tout entier s'écrit sous l'une des formes suivantes :
$4k$; $4k+1$; $4k+2$; $4k+3$ (k désignant un entier).

Nombres premiers

25 Les entiers suivants sont-ils des nombres premiers ?
87 ; 113 ; 143 ; 187 ; 277.

26 Établir, sans machine, les résultats suivants obtenus avec le logiciel de calcul formel Xcas :

```
1 isPrime(47);isPrime(127);isPrime(223)
        ( vrai, vrai, vrai )                    M
```

27 Chercher sur Internet ce que l'on appelle « crible d'Ératosthène » et dresser la liste des nombres premiers compris entre 1 et 100 à l'aide de cette méthode.

Point Histoire

Cette méthode a été établie par le mathématicien grec **Ératosthène** au III^e^ siècle avant J.-C.

28 Décomposer en produit de facteurs premiers, sans machine, les entiers suivants : 45 ; 1 400 ; 735.

29 Retrouver les décompositions en facteurs premiers des entiers de l'exercice 28 en utilisant un programme pour votre calculatrice.

30 Décomposer en produit de facteurs premiers le numérateur et le dénominateur des fractions suivantes et en déduire la forme irréductible des fractions : $\frac{76}{24}$; $\frac{13\,650}{1\,785}$.

31 *Logique*

Pour n entier naturel, expliquer pourquoi la négation de « n est premier » n'est pas « n est composé ».

32 Donner le nombre de diviseurs positifs des entiers :
$a = 3^2 \times 5^7$ et $b = 2 \times 11^3$.

33 1. Donner deux nombres entiers consécutifs premiers.
2. Peut-on donner trois nombres entiers consécutifs premiers ?

Congruences

34 Les entiers 128 et 15 sont-ils congrus modulo 11 ?

35 Soit r un entier compris entre 0 et 6. Quelle est la valeur de r sachant que 2013 est congru à r modulo 7 ?

36 Déterminer le plus petit entier positif r tel que :
$2017 \equiv r\ (10)$.

37 Déterminer le plus petit entier en valeur absolue r tel que :
$2017 \equiv r\ (10)$.

38 Combien existe-t-il d'entiers p compris entre −2 000 et 2 000 tels que $p \equiv 2012\ (11)$?

39 Déterminer les naturels m tels que $27 \equiv 5\ (m)$.

40 Un entier n vérifie $n \equiv 100\ (11)$.
Quel est le reste de la division euclidienne de n par 11 ?

41 Expliquer pourquoi un entier naturel est toujours congru modulo 10 au chiffre des unités de son écriture décimale.

42 Est-il vrai que tout entier est congru modulo 4 à l'un des entiers −1 ; 0 ; 1 ; 2 ?

43 Est-il vrai que tout entier est congru modulo 3 à l'un des entiers 7 ; 8 ; 9 ?

44 Est-il vrai que tout entier est congru modulo 3 à l'un des entiers −3 ; 28 ; 137 ?

45 Quels sont les entiers n tels que $n^2 \equiv 3n\ (n)$?

46 Vérifier que $1\,000 \equiv 1\ (37)$.
En déduire le reste dans la division euclidienne de $10^{3\,000\,000}$ par 37.

47 *ALGO* On considère l'algorithme suivant :

```
Entrée : A
Tant que A ⩾ 3
|  A − 7 → A
Fin Tant que
Afficher A
```

Sa traduction sur calculatrice est :

Casio	Texas
"A":?→A While A≥3 A-7→A WhileEnd	:Prompt A :While A≥3 :A-7→A :End :Disp A

1. Quelles seront les sorties avec :
a. l'entrée $A = 3$?
b. l'entrée $A = 4$?
c. l'entrée $A = 7$?
d. l'entrée $A = 8$?

2. Quelles sont les sorties possibles avec pour entrée un naturel quelconque A ?

3. Justifier que la sortie obtenue est congrue modulo 7 au naturel A donnée en entrée.

4. Modifier le programme afin que la sortie soit un entier compris entre −3 et 3, congru modulo 7 à l'entrée, cette entrée pouvant être un entier naturel quelconque.

5. Modifier le programme afin que la sortie soit un entier compris entre −3 et 3, congru modulo 7 à l'entrée, cette entrée pouvant être un entier relatif quelconque.

Exercices

POUR S'ENTRAÎNER

Le mot « entier » sans précision désignera toujours un entier relatif (c'est-à-dire un élément de $\mathbb{Z}$).

Divisibilité

48 Déterminer les entiers puis les entiers naturels n tels que 7 divise $n + 54$.

→ Pour vous aider Savoir-faire 1, p. 11

49 Déterminer les entiers n tels que n divise $n + 12$.

→ Pour vous aider Savoir-faire 1, p. 11

50 Déterminer les entiers n tels que $3n + 7$ divise 6.

→ Pour vous aider Savoir-faire 1, p. 11

51 Déterminer tous les entiers n tels que $3n + 4$ divise $n + 7$.

→ Pour vous aider Savoir-faire 1, p. 11

52 Déterminer l'ensemble des entiers naturels n tels que $2n + 9$ divise $n + 11$.

53 Soit n un entier et a un entier divisant $n - 1$ et $n^2 + n + 3$. Établir que a est un diviseur de 5.

54 **TRAVAIL EN AUTONOMIE**

Énoncé

Déterminer les entiers n tels que $n + 2$ divise $n^3 - 2$.

Solution

Soit n un entier solution : $n + 2$ divise $n^3 - 2$.

Comme $n + 2$ divise $n + 2$, on en déduit que $n + 2$ divise la combinaison :

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

$n + 2$ divise donc la combinaison :

$$(-2 - 2n^2) + 2n(n + 2) = -2 + 4n.$$

Et $n + 2$ divise la combinaison :

$$4(n + 2) - (-2 + 4n) = 10.$$

$n + 2$ est donc nécessairement l'une des valeurs :

$$-10\ ;\ -5\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 5\ ;\ 10$$

et n l'une des valeurs :

$$-12\ ;\ -7\ ;\ -4\ ;\ -3\ ;\ -1\ ;\ 0\ ;\ 3\ ;\ 8.$$

Réciproquement, on vérifie que chacune de ces valeurs de n est effectivement solution (par exemple : $8^3 - 2 = 510$, $8 + 2 = 10$ et 10 divise 510 donc 8 est solution).

55 Déterminer les entiers n tels que $n + 2$ divise $n^2 + 2$.

56 Soit a et b deux entiers.

1. Montrer que si 2 divise $a^2 + b^2$, alors 2 divise $(a + b)^2$.
2. Montrer que si 3 divise $a^3 + b^3$, alors 3 divise $(a + b)^3$.

57 Logique

1. Pour n entier, réduire $2(3n + 7) - 6(n + 1)$.
2. Démontrer l'implication suivante : « Pour tout entier n, si $n + 1$ divise $3n + 7$, alors $n + 1$ divise 8. »
3. La réciproque de l'implication précédente est-elle vraie ?

58 Déterminer tous les couples $(x\ ;\ y)$ d'entiers tels que :

$$x^2 = y^2 + 17.$$

→ Pour vous aider Savoir-faire 2, p. 11

59 Résoudre l'équation $x^2 = 9y^2 + 7$, avec x et y entiers.

→ Pour vous aider Savoir-faire 2, p. 11

60 1. Développer $(x - 5)(y - 3)$.

2. Déterminer les couples d'entiers $(x\ ;\ y)$ solutions de l'équation :

$$xy = 3x + 5y.$$

61 Logique

Soit a, b, m, n, d des entiers. On rappelle que si d divise a et b, alors d divise $am + bn$.

L'implication suivante est-elle vraie : « Soit a et b des entiers. S'il existe des entiers m et n tels que d divise $am + bn$, alors d divise a ou divise b. » ?

62 ALGO

On définit la suite (u_n) pour tout entier naturel n par :

$$u_n = 2^{3n} - 1.$$

1. On considère le programme suivant :

Casio	Texas
"N":?→N 0→U For 1→J To N 8×U+7→U Next	:Prompt N :0→U :For(J,1,N) :8*U+7→U :End :Disp U

Vérifier pour quelques valeurs de l'entrée N que la sortie de l'algorithme est égale au terme u_N. Puis expliquer pourquoi.

2. Démontrer, par récurrence, que u_n est multiple 7 pour tout entier naturel n.

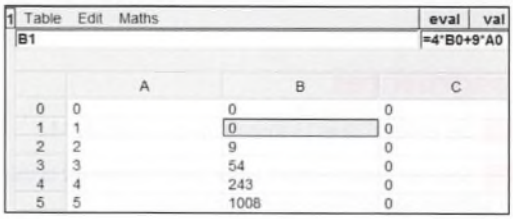
63 Montrer par récurrence que, pour tout entier naturel n, $4^{2n} - 2^n$ est divisible par 7.

64 Avec un tableur TICE

On définit une suite (u_n) pour tout entier naturel n par :

$$u_n = 2^{2n} - 3n - 1.$$

1. En colonne A d'un tableur, on a entré les entiers 0, 1, 2, 3… En cellule B0, on a entré 0 et en cellule B1 la formule `=4*B0+9*A0`, formule qui a été ensuite recopiée vers le bas.



Vérifier que l'on calcule bien ainsi les termes de la suite (u_n).

2. Démontrer que u_n est un multiple de 9 pour tout entier naturel n.

VRAI – FAUX

Pour les exercices **65** à **68**, indiquer si les affirmations sont vraies ou fausses, puis justifier. a, b, c et d sont des entiers.

65 Si a divise b et c divise d, alors $a + c$ divise $b + d$.

66 Si a divise b, alors a divise b^2.

67 La somme de deux entiers impairs consécutifs est divisible par 4.

68 Si 3 divise le produit ab, avec a et b entiers, alors 3 divise a et 3 divise b.

Division euclidienne

69 Le reste de la division euclidienne de 1 789 par l'entier naturel b est 497.
Déterminer les valeurs possibles de b et du quotient.

→ Pour vous aider Savoir-faire 3, p. 13

70 Le reste de la division euclidienne de 225 par un entier naturel b est 4. Déterminer les valeurs possibles de b.

→ Pour vous aider Savoir-faire 3, p. 13

71 Par quels entiers naturels faut-il diviser 12 pour que le quotient de la division euclidienne soit égal au reste ?

72 Soit n un entier.
Établir que n^2 s'écrit sous la forme $4k$ ou sous la forme $4k + 1$.

→ Pour vous aider Savoir-faire 4, p. 13

73 Soit n un entier, on pose :

$$f(n) = (n - 11)(n - 22)(n - 33)(n - 44)(n - 55).$$

Établir que $f(n)$ est multiple de 5 pour tout entier n.

→ Pour vous aider Savoir-faire 4, p. 13

74 Soit n un entier naturel tel que $n \geqslant 3$.
Montrer que $3n + 1 = 2(n + 2) + n - 3$.
En déduire le reste de la division euclidienne de $3n + 1$ par $n + 2$.

75 Déterminer, selon les valeurs de l'entier naturel n, le reste de la division euclidienne de $7n + 3$ par $2n - 1$.

76 ALGO

On considère l'algorithme ci-contre :

1. Quelle est la sortie de l'algorithme avec $a = 24$? $a = 25$?

2. Quelles entrées donneront la sortie OUI et quelles entrées donneront la sortie NON ?

3. Traduire le programme sur calculatrice et contrôler les réponses faites précédemment.

```
Entrée : a entier naturel
Traitement :
q prend la valeur 0
m prend la valeur 7
Tant que m ⩽ a
    q prend la valeur q + 1
    m prend la valeur m + 7
Fin Tant que
Sortie :
Si a – 7q = q alors afficher OUI
sinon afficher NON
```

VRAI – FAUX

Pour les exercices **77** à **80**, indiquer si les affirmations sont vraies ou fausses, puis justifier.
a, a', b désignent des entiers naturels (b non nul).

77 Si dans la division euclidienne de a par b le quotient est q, alors dans la division euclidienne de a par q, le quotient est b.

78 Le quotient de la division euclidienne de a par b peut être égal à b.

79 Si dans la division euclidienne de a par b le quotient est q et dans la division de a' par b le quotient est q', alors dans la division de $a + a'$ par b le quotient est $q + q'$.

80 Si dans la division de a par b le reste est r et dans la division de a' par b le reste est r', alors le reste de la division de aa' par b est égal au reste de la division de rr' par b.

Nombres premiers

81 Les nombres premiers inférieurs à 42 sont :
2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41.
Expliquer pourquoi le nombre 1 789 est premier.
On justifiera le raisonnement fait.

→ Pour vous aider Savoir-faire 5, p. 17

82 1. Montrer que le nombre $f(n) = n^2 + 18n + 77$ n'est premier pour aucune valeur de l'entier naturel n.

2. Peut-on trouver un entier n tel que $f(n)$ soit premier ?

→ Pour vous aider Savoir-faire 6, p. 17

83 Soit n un entier naturel.
1. Développer $(n^2 + 8)^2$ et en déduire une factorisation de :

$$g(n) = n^4 + 64.$$

2. Établir que, pour tout entier naturel n, l'entier $g(n)$ n'est pas premier.

84 **TRAVAIL EN AUTONOMIE**

Énoncé
Soit p et q deux nombres premiers consécutifs au moins égaux à 3.
Établir que la somme $p + q$ est le produit d'au moins trois nombres premiers (éventuellement non distincts).

Solution
Comme p et q sont distincts de 2 et premiers, ils sont impairs et $p + q$ est pair.
On a donc $p + q = 2A$ où $A = \frac{p+q}{2}$ est entier.
Comme A, moyenne de p et q, est strictement compris entre p et q, qui sont des nombres premiers consécutifs, A n'est pas premier et s'écrit donc comme un produit d'au moins deux nombres premiers.
$p + q$ s'écrit donc comme un produit d'au moins trois nombres premiers.

Exercices

85 p et q sont deux nombres premiers tels que l'équation $x^2 - px + q = 0$ a deux solutions dans $\mathbb{N}$. Identifier p et q.

86 Logique

1. Montrer que si l'entier n est premier, alors $n + 7$ n'est pas premier.

2. La réciproque de l'implication précédente est-elle vraie ?

3. L'implication « Si n est premier, alors $n + 11$ est composé » est-elle vraie ?

87 1. Dresser un tableau de 6 colonnes et 15 lignes. Inscrire les entiers 6, 7, 8, 9, 10, 11 en ligne 1 et poursuivre ainsi le remplissage ligne par ligne des entiers jusqu'à l'entier 95. Entourer les nombres premiers dans le tableau obtenu.

2. Que remarque-t-on sur la répartition des nombres premiers dans cette grille ? En déduire une conjecture sur les nombres premiers puis la démontrer.

3. En raisonnant par disjonction des cas, déduire de la conjecture faite à la question 2, que si p est premier et au moins égal à 5, alors $p^2 - 1$ est divisible par 24.

88 Logique

1. Montrer l'implication suivante : « Pour tout entier $p > 3$, si p est premier, alors $8p^2 + 1$ est composé ».

2. La réciproque de l'implication précédente est-elle vraie ?

AIDE : On pourra raisonner par disjonction des cas sur les valeurs possibles des restes de la division de p par 3.

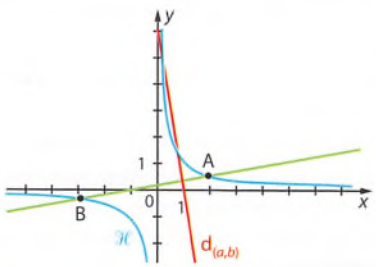
89 Montrer que la somme de deux entiers naturels impairs consécutifs n'est pas un nombre premier.

90 **Des diviseurs premiers** ROC

1. Rappeler la démonstration du résultat suivant : « Soit n un entier au moins égal à 2. Le plus petit diviseur de n compris entre 2 et n est premier. »

2. Quels sont les entiers n tels que le plus grand diviseur de n compris entre 2 et $n - 1$ est premier ?

91 Dans le plan muni d'un repère orthonormé, on note $\mathcal{H}$ l'hyperbole d'équation $y = \frac{1}{x}$. Soit a et b deux entiers naturels non nuls et A et B deux points de $\mathcal{H}$ d'abscisses respectives a et $-b$. $d_{(a,b)}$ est la perpendiculaire à la droite (AB) passant par le point I(1 ; 0) et $f(a ; b)$ l'ordonnée à l'origine de la droite $d_{(a,b)}$.



Démontrer que $f(a ; b)$ décrit l'ensemble des entiers naturels composés lorsque a et b décrivent l'ensemble des entiers naturels au moins égaux à 2.

92 Pour un couple $(a ; b)$ d'entiers naturels, on définit la fonction f par $f(x) = ax + b$. On cherche à savoir s'il est possible de donner à a et b des valeurs telles que $f(n)$ soit un nombre premier quel que soit l'entier naturel n.

1. Établir que, dans ce cas, b doit être premier.

2. En utilisant l'image de b par f, conclure.

VRAI – FAUX

Pour les exercices **93** à **96**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

93 Tous les nombres premiers sont impairs.

94 La réciproque de l'implication précédente est vraie.

95 Soit P le trinôme défini par :

$$P(n) = n^2 + n + 41.$$

Le discriminant de P est strictement négatif, donc P n'est pas factorisable, donc l'entier $P(n)$ est premier.

96 Soit p un nombre premier et f la fonction définie par :

$$f(n) = n^2 + n + p.$$

Alors le nombre $f(p - 1)$ n'est jamais premier.

Décomposition en facteurs premiers

97 Décomposer 231 en facteurs premiers et, à l'aide d'un arbre, donner tous ses diviseurs positifs.

→ Pour vous aider Savoir-faire 7, p. 19

98 1. Soit p un nombre premier. Quels sont les diviseurs positifs de p^2 ?

2. Quels sont les entiers qui admettent exactement 3 diviseurs positifs ?

→ Pour vous aider Savoir-faire 7, p. 19

99 Quel est le nombre de diviseurs positifs de l'entier :

$$n = 2^3 \times 5^6 \times 11 \times 17^{10} \times 21^5 ?$$

→ Pour vous aider Savoir-faire 8, p. 19

100 **TRAVAIL EN AUTONOMIE** Logique

Énoncé

1. Établir l'implication suivante : « Si un entier naturel n s'écrit sous la forme p^2q^3 où p et q sont des nombres premiers, alors n admet exactement 12 diviseurs positifs ».

2. Énoncer la réciproque de l'implication précédente et donner sa valeur de vérité.

Solution

1. En utilisant le principe de l'arbre du savoir-faire 8, le nombre de diviseurs positifs de p^2q^3 est $3 \times 4 = 12$.

2. La réciproque s'énonce ainsi : « Si un entier naturel n admet 12 diviseurs positifs, alors n est de la forme p^2q^3 avec p et q premiers ». Cette réciproque est fausse : 2^{11} admet 12 diviseurs $1, 2, 2^2, \ldots, 2^{11}$ et n'est pas de la forme p^2q^3.

101 Donner la forme de la décomposition en facteurs premiers des entiers naturels ayant exactement 15 diviseurs positifs.

102 Soit p un nombre premier.
Déterminer les entiers naturels x et y tels que $x^2 - y^2 = p$.

VRAI – FAUX

Pour les exercices **103** à **105**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

103 Soit a, b, c, d des entiers distincts. Si $ab = cd$, alors l'un au moins des quatre entiers n'est pas premier.

104 Si le nombre des diviseurs positifs d'un entier n est un nombre premier, alors n est une puissance d'un nombre premier.

105 La réciproque de l'implication précédente est vraie.

Congruences

106 **1.** Déterminer les entiers n tels que $n + 3 \equiv 2\ (5)$.

2. Quel est le plus petit entier supérieur à 100 vérifiant la condition ci-dessus ?

→ Pour vous aider Savoir-faire 9, p. 23

107 **1.** Déterminer les entiers x tels que $3x \equiv 2\ (5)$.

2. Déterminer les entiers x tels que $2x \equiv 3\ (5)$

→ Pour vous aider Savoir-faire 9, p. 23

108 Logique

1. Établir l'implication suivante : « Pour tout entier naturel n, si n est divisible par 6 alors $7^n \equiv 1\ (9)$ ».

2. Énoncer la réciproque de l'implication précédente et donner sa valeur de vérité.

→ Pour vous aider Savoir-faire 10, p. 23

109 Déterminer le reste de la division euclidienne par 7 des nombres suivants : 57^{2018} ; 83^{2019} ; 2018^{2018}.

→ Pour vous aider Savoir-faire 10, p. 23

110 Logique ROC

1. Démontrer l'implication suivante : « Pour tous entiers a, b, c et tout entier naturel $m \geqslant 2$, si $a \equiv b\ (m)$ alors $ac \equiv bc\ (m)$ ».

2. Énoncer la réciproque de l'implication précédente et préciser si cette réciproque est vraie ou fausse.

111 Est-il vrai que $3^{2n} \equiv 2^n\ (7)$ pour tout entier naturel n ?

112 Pour tout entier naturel n, on pose $a^n = 1^n + 2^n + 3^n + 4^n$.
Établir que a^n n'est jamais multiple de 10^3.

AIDE : On pourra réduire a^n modulo 8 pour $n \geqslant 3$.

113 Trouver le reste de la division par 5 du nombre $2\,018^{2\,018}$.

114 Quel est le reste de la division euclidienne par 8 du nombre 3^n, où n est un entier naturel ?

115 ALGO

On considère l'algorithme ci-contre :

```
Entrée : N entier naturel
Traitement :
N → S
Tant que S > 4
    S prend la valeur S – 8
Fin Tant que
Sortie : S
```

1. Donner les sorties de l'algorithme pour les entrées $N = 0$, $N = 1$, $N = 2, \ldots$, $N = 16$.

2. Expliquer pourquoi on aura $N \equiv S\ (8)$ pour une entrée quelconque N et la sortie S correspondante.

3. En utilisant le représentant de 7 modulo 8 donné par l'algorithme, donner le reste de la division euclidienne de $7^k + 1$ par 8 suivant les valeurs de l'entier k.

116 Des caméléons vivent dans un parc zoologique. Quand j'y suis passé, il y en avait 13 verts, 15 bruns et 17 orange. Quand deux caméléons de couleurs distinctes se croisent, ils prennent la troisième couleur. Quand deux caméléons de même couleur se croisent, ils gardent bien sûr leur couleur. Comment organiser les rencontres pour obtenir un parc unicolore ?

AIDE : On cherchera à établir que la différence entre deux populations est invariante modulo 3.

VRAI – FAUX

Pour les exercices **117** à **119**, indiquer si les affirmations sont vraies ou fausses, puis justifier.
m désigne un entier au moins égal à 2.

117 Si a est un entier tel que $2a \equiv 6\ (m)$, alors $a \equiv 3\ (m)$.

118 Le nombre 19^{52} est congru à 1 modulo 8.

119 Si deux entiers naturels a et b sont tels que $a^2 \equiv b^2\ (m)$, alors $a \equiv b\ (m)$.

Congruences et divisibilité

120 Démontrer que, quel que soit l'entier naturel n, le nombre $N = n(8n + 1)(13n + 1)$ est divisible par 6.

→ Pour vous aider Savoir-faire 11, p. 25

121 Montrer que, pour tout entier naturel n, $7^{2n} - 23^n$ est divisible par 13.

→ Pour vous aider Savoir-faire 11, p. 25

122 Logique

Pour tout entier naturel n, on pose $f(n) = n^3 + n - 2$.

1. Établir l'implication suivante : « Pour tout entier naturel n, si la division de n par 7 a pour reste 1, alors $f(n)$ est divisible par 7 ».

2. Énoncer la réciproque de l'implication précédente.
Est-elle vraie ?

Exercices

123 Est-il vrai que pour tout entier naturel n, $7^{2n}+3$ est divisible par 4 ?

124 **TRAVAIL EN AUTONOMIE** ALGO

Énoncé

1. On considère l'algorithme suivant :

Entrée : Un entier naturel N
Traitement :
Tant que $N > 5$
| N prend la valeur $N - 11$
Fin Tant que
Sortie : Afficher N

Donner les sorties de l'algorithme pour :
$N=1$, $N=2$, $N=3$, ..., $N=11$.

2. Établir que pour tout entier n impair, l'entier :
$A = 108^n + 98^n + 88^n + 78^n + 68^n + 58^n + 48^n + 38^n + 28^n + 18^n + 8^n$
est multiple de 11.

Solution

1. Les sorties obtenues sont :
0 ; 1 ; 2 ; 3 ; 4 ; 5 ; −5 ; −4 ; −3 ; −2 ; −1.

2. On détermine le représentant modulo 11 fourni par l'algorithme pour chacun des entiers 8, 18, 28, ..., 108.
Ce sont les entiers $-3, -4, -5, 5, 4, 3, 2, 1, 0, -1, -2$.
On a donc $A \equiv (-5)^n + (-4)^n + \ldots + 5^n$ (11). Comme n est impair, on a ainsi $A \equiv 0$ (11). A est donc divisible par 11.

125 Déterminer les valeurs possibles du chiffre x tel que l'entier $\overline{71x4}$ soit divisible par 3.

126 Déterminer les chiffres x et y tels que l'entier $\overline{9x2y}$ soit divisible par 4 et par 3.

127 On note respectivement u et d le chiffre des unités et celui des dizaines d'un entier naturel N.

1. Montrer que $N \equiv 2d + u$ (4).

2. En déduire un critère de divisibilité par 4.

→ Pour vous aider Savoir-faire 12, p. 25

128 1. Démontrer que, pour tout entier n supérieur ou égal à 1, $10^n \equiv 10$ (45).

2. En déduire un critère de divisibilité par 45.

3. Appliquer ce critère aux entiers :
$a = 20\,152\,016$ et $b = 20\,152\,035$.

→ Pour vous aider Savoir-faire 12, p. 25

129 Démontrer que deux entiers qui s'écrivent avec les mêmes chiffres (mais pas nécessairement dans le même ordre !) ont pour différence un multiple de 9.

VRAI – FAUX

Pour les exercices **130** à **133**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

130 Si un entier a est congru modulo m à un entier b non nul, alors a n'est pas multiple de m.

131 Un entier supérieur à 10 est divisible par 25 si, et seulement si, le nombre formé par les deux derniers chiffres de son écriture décimale est divisible par 25.

132 Un entier est divisible par 9 si la somme des chiffres de la somme des chiffres de la somme de ses chiffres est égale à 9.

133 La réciproque de l'implication précédente est vraie.

Top Chrono !

Résoudre chacun des exercices suivants en 10 minutes maximum.

134 Établir que si un entier n est tel que $n+3$ divise n^2+1 alors $n+3$ divise 10. En déduire l'ensemble des entiers n tels que $n+3$ divise n^2+1.

135 Déterminer les entiers naturels n tels que les six entiers $n+1$, $n+3$, $n+7$, $n+9$, $n+13$, $n+15$, soient premiers.

AIDE : Raisonner avec n modulo 5.

136 Établir que, pour tout entier naturel n, l'entier $7^{2n} - 335^n$ est divisible par 13.

137 Déterminer les entiers n tels que $g(n) = 2n^3 + n^2 + 2$ soit multiple de 5.

138 ALGO

Écrire un algorithme prenant en entrée un entier naturel N et un nombre premier p et fournissant en sortie l'exposant de p dans la décomposition de N en facteurs premiers.

139 ALGO

Écrire un algorithme prenant en entrée un entier naturel N et fournissant en sortie un entier R compris entre −10 et 10 congru à N modulo 21.

140 Déterminer les restes de la division euclidienne de 7^n par 9 suivant les valeurs de n et en déduire le reste de la division euclidienne de $2\,014^{2\,012}$ par 7.

Choisir la (ou les) bonne(s) réponse(s).

Utiliser la divisibilité dans $\mathbb{Z}$

→ Pour vous aider Savoir-faire 1 et 2, p. 11

	A	B	C	D
141 Pour $n \in \mathbb{Z}$, si $n-3$ divise $5n+2$ alors	$n-3$ divise 13	$n-3$ divise 17	n divise 20	17 divise $n-3$
142 Pour x et y entiers naturels, l'équation $x^2 - 25y^2 = 101$ admet	pour unique solution, le couple (51 ; 10)	aucune solution	deux solutions	une infinité de solutions

Utiliser la division euclidienne

→ Pour vous aider Savoir-faire 3 et 4, p. 13

143 Le reste entier de la division euclidienne de 2 012 par un naturel b est 666. Les valeurs possibles de b sont au nombre de	4	0	2	1
144 n est le plus petit entier positif ayant pour reste 1 dans la division par 4 et dans la division par 5. n est égal à	6	5	21	1
145 n est un entier naturel. n^2 peut être de la forme (k désignant un entier)	$4k$	$4k+1$	$4k+2$	$4k+3$

Raisonner avec des nombres premiers

→ Pour vous aider Savoir-faire 5, 6 et 8, p. 17 et 19

146 Si p est premier, alors	$p+1$ est composé	p^3 a 8 diviseurs dans $\mathbb{Z}$	p n'admet aucun diviseur entre 2 et $\sqrt{p}$	on ne peut pas écrire p sous la forme d'un produit de deux entiers
147 L'entier $n = 2^3 \times 199^2$ possède	12 diviseurs positifs	36 diviseurs positifs	6 diviseurs positifs	5 diviseurs positifs
148 Pour $n \in \mathbb{Z}$, on pose : $A(n) = n^4 + 10n^2 + 21$. Le nombre de valeurs de n pour lesquelles $A(n)$ est premier est	0	1	2	une infinité

Savoir utiliser les congruences

→ Pour vous aider Savoir-faire 9, 11 et 12, p. 23 et 25

149 Les solutions dans $\mathbb{Z}$ de l'équation $2x \equiv 7\ (3)$ sont	$x = 2$	les nombres $2+3k,\ k \in \mathbb{Z}$	les nombres $2+7k,\ k \in \mathbb{Z}$	l'équation n'a pas de solution
150 Lorsque n varie dans $\mathbb{N}$, le chiffre des unités de 13^n peut prendre	une seule valeur	3 valeurs distinctes	4 valeurs distinctes	une infinité de valeurs
151 $8^n - 6^n$ est multiple de 7 pour	les entiers naturels n pairs	les entiers naturels n impairs	tous les entiers naturels n	aucun entier naturel n
152 Si l'entier n s'écrit 22…22 avec k chiffres 2, alors n est multiple de 3 pour	aucune valeur de k	$k = 3$	$k \equiv 0\ (3)$	k multiple de 9

➤ Voir les réponses, p. 140

TP 1 Le nombre de zéros de *n*!

TICE ALGO → Utiliser un logiciel de calcul formel pour le calcul sur de grands entiers.

Fichier logiciel 01_TSspe_TP1.xws

www. bordas-indice.fr

La suite des factorielles des entiers naturels est une suite à croissance très rapide. On va s'intéresser ici aux puissances de 10 divisant les termes de cette suite.

A. Découvrir la notation factorielle

n désignant un entier naturel non nul, on définit *n*! (lire « factorielle *n* ») par $n! = 1 \times 2 \times 3 \times \ldots \times n$.

1. Calculer 2!, 3!, 4! et 10!

2. Avec le logiciel Xcas, calculer quelques factorielles (en entrant par exemple 21!, 52! ou 103!).

B. Le nombre de zéros de *n*!

1. On a programmé avec le logiciel Xcas une fonction déterminant le nombre de zéros terminant (à droite) l'écriture décimale de l'entier *n*. Une ligne a été effacée. Quelle peut être cette ligne ?
Tester le bon fonctionnement du programme en entrant par exemple nbZero(5300) dans une ligne de commandes.

```
Prog  Edit  Ajouter
nbZero(n):={
local compteur,q;
compteur:=0;
q:=n/10;
tantque q==floor(q) faire
.....................;
q:=q/10;
ftantque;
retourne compteur;
}:;
```

2. On propose ci-contre un autre algorithme ayant le même rôle. Compléter la dernière ligne.
Tester le bon fonctionnement de cette nouvelle version.

```
Prog  Edit  Ajouter
nbZ(n):={
local c,p;
c:=1;
p:=10^c;
tantque irem(n,p)==0 faire
c:=c+1;
p:=10^c;
ftantque;
retourne ..... ;}:;
```

3. La fonction **factoriser_entier**() du logiciel Xcas retourne la factorisation en nombres premiers de l'entier donné en argument.
À l'aide de cette instruction et de l'un des programmes des questions précédentes, faire une conjecture sur le nombre de zéros terminant l'écriture décimale de *n*!.

C. Vers une étude théorique

1. Programmer une fonction nbCinq(m) dont l'entrée *m* est un entier naturel et dont la sortie est l'exposant de 5 dans la décomposition de *m* en facteurs premiers.

2. On définit la séquence suivante :

seq(nbCinq(n!)-nbZero(n!),n,1,100).

Quel affichage s'attend-on à obtenir ? Vérifier.

3. Justifier que l'exposant de 5 dans la décomposition en facteurs premiers de *n*! est toujours inférieur à l'exposant de 2 dans cette décomposition.

4. Démontrer la conjecture faite à la question **3.** de la **partie A**.

D. Un autre algorithme

On définit avec Xcas la fonction ci-dessous, dans laquelle l'entrée *n* est un naturel non nul.

```
Prog  Edit  Ajouter                                    8
nbZeroFactoriel(n):={
local j,S,quotient;
j:=1;S:=0;
quotient:=floor(n/5^j);
tantque quotient!=0 faire // tantque q différent de 0
S:=S+quotient;j:=j+1;quotient:=floor(n/5^j);
ftantque;
retourne S;}:;
```

1. Vérifier pour quelques valeurs de *n* que nbZeroFactoriel(n) retourne le nombre de zéros terminant *n*!.

2. Pour deux naturels non nuls *m* et *a*, quel lien existe-t-il entre le nombre de multiples non nuls de *m* inférieurs à *a* et la partie entière de $\frac{a}{m}$?

3. Expliquer le principe de fonctionnement de l'algorithme précédent.

4. Soit (u_n) la suite telle que, pour *n* entier naturel, u_n est égal au nombre de zéros terminant *n*!.

a. Justifier que la suite (u_n) est croissante.

b. Écrire un programme permettant de déterminer les entiers *n* tels que $u_n = 1\,000$.

Aides pour les logiciels

Xcas

B. Ne pas oublier les ; pour terminer chaque instruction. L'instruction local sert à déclarer des variables qui ne sont utiles qu'à l'intérieur de la fonction programmée. Ce qui suit l'instruction retourne peut être considéré comme l'image de *n* par la fonction : le paramètre *n* est l'entrée, ce qui suit l'instruction retourne est la sortie du programme.
B. 1. La fonction **floor** est la fonction partie entière.
C. 2. Pour comprendre le rôle et la syntaxe d'une instruction comme **seq**(), consulter le menu aide/index et entrer le mot seq.

TP 2 Table de multiplication modulo 7

TICE → Utiliser un tableur pour résoudre des équations avec congruences.

Pour résoudre une équation du type $2x = 5$, on s'appuie sur notre connaissance des tables usuelles.
Mais pour une équation avec congruence ?

A. Construction et utilisation d'une table

On veut construire, sur tableur, une table donnant les restes des divisions euclidiennes des produits ab par 7, a et b décrivant l'ensemble $E = \{0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6\}$.

1. Entrer les valeurs prises par a en colonne A de la cellule A2 à la cellule A8 puis les valeurs prises par b en ligne 1, de la cellule B1 à la cellule H1.

2. Laquelle des formules suivantes doit-on entrer en B2 pour dresser ensuite la table ci-contre complète par recopie automatique ?

a. `=MOD(A2*B1;7)`
b. `=MOD(A$2*B$1;7)`
c. `=MOD($A2*B$1;7)`
d. `=MOD($A$2*$B$1;7)`

	A	B	C	D	E	F	G	H
1		0	1	2	3	4	5	6
2	0	0	0	0	0	0	0	0
3	1	0	1	2	3	4	5	6
4	2	0	2	4	6	1	3	5
5	3	0	3	6	2	5	1	4
6	4	0	4	1	5	2	6	3
7	5	0	5	3	1	6	4	2
8	6	0	6	5	4	3	2	1

3. Construire la table.

4. À l'aide de la table obtenue, déterminer les entiers x tels que $2x \equiv 5\ (7)$.

5. Déterminer les entiers x tels que $3x \equiv x\ (7)$.

6. Déterminer les entiers x tels que $x^2 \equiv 1\ (7)$.

7. Déterminer les entiers n tels que $5n + 3$ soit multiple de 7.

B. Une autre table

En utilisant le principe précédent, résoudre dans $\mathbb{Z}$ l'équation $3x \equiv 1\ (26)$ puis l'équation $x^2 \equiv 5\ (26)$.

Aides pour les logiciels

Excel ou **Open Office**

A. 1. MOD(*A*;*B*) renvoie le reste de la division euclidienne de *A* par *B*.
A. 2. Revoir si nécessaire le rôle du symbole $.

TP 3 Alignement de restes

TICE → Utiliser un tableur pour déterminer des quotients et des restes.

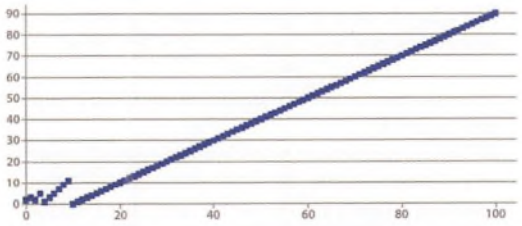
Lorsque dividende et diviseur dépendent d'une variable, le reste en dépend *a priori* aussi. Des conjectures graphiques vont nous permettre ici de préciser cette dépendance.

A. Un premier cas

Pour tout naturel n, on pose $A(n) = n^2 + 5n - 7$ et $B(n) = n + 3$. On cherche à connaître le quotient $q(n)$ et le reste $r(n)$ de la division euclidienne de $A(n)$ par $B(n)$.

1. En colonne A, entrer les entiers n de 0 à 100, en colonne B les entiers $A(n)$, en colonne C les entiers $B(n)$, en colonne D les entiers $q(n)$ et les entiers $r(n)$ en colonne E.

2. On a représenté ci-dessous la suite des restes.



Obtenir cette représentation ainsi que celle de la suite $(q(n))$.

3. À partir des graphiques, émettre une conjecture pour les expressions de $q(n)$ et $r(n)$ en fonction de n pour $n \geqslant 10$.

4. Démontrer les conjectures précédentes et donner les couples $(q(n) ; r(n))$ pour tout entier naturel n.

B. Un second cas

Pour tout entier naturel n, on pose :

$$u(n) = 2n^3 + 11n^2 + 18n + 8 \text{ et } v(n) = 2n + 5.$$

Exprimer le quotient $q(n)$ et le reste $r(n)$ de la division euclidienne de $u(n)$ par $v(n)$ pour tout naturel n.

Aides pour les logiciels

Excel ou **Open Office**

A. 1. MOD(*A*;*B*) renvoie le reste de la division euclidienne de *A* par *B*.

Xcas

B. `f(x):=a*x^2+b*x+c` puis `solve([f(1)=1,f(2)=7,f(3)=11],[a,b,c])` permet de déterminer la fonction f dont les images de 1, 2, 3 sont respectivement 1, 7, 11.

Sujet commenté BAC

➤ Énoncé

Thèmes
- Congruences
- Raisonnement par disjonction des cas
- Divisibilité

1. Établir que l'équation (F) : $14x^2 + 7y^2 = 10^{2n}$ (où x et y sont des entiers relatifs) n'a pas de solution.

2. On considère l'équation (G) : $3x^2 + 7y^2 = 10^{2n}$ où x et y sont des entiers relatifs.
a. Démontrer que si $(x ; y)$ est solution de (G), alors $3x^2 \equiv 2^n\ (7)$.
b. Quels sont les restes possibles dans la division euclidienne de $3x^2$ par 7 ?
c. Quels sont les restes possibles dans la division euclidienne de 2^n par 7.
d. Quel est l'ensemble des solutions de l'équation (G) ?

D'après Bac, Nouvelle-Calédonie, 2009.

➤ Comprendre l'énoncé et choisir les méthodes

1. Deux nombres égaux ont les mêmes diviseurs, et en particulier les mêmes facteurs premiers.
On factorise les deux membres de façon à faire apparaître une incompatibilité entre les facteurs des deux membres.

2. a. On cherche à réduire modulo 7 chacun des membres de l'équation de départ. On utilise pour cela les propriétés des congruences, notamment la compatibilité avec l'addition et la multiplication. Il faut penser à l'égalité $10^{2n} = 100^n$ et réduire 100 modulo 7. On établit ici une implication qui n'est pas une équivalence, c'est souvent le cas lorsque l'on doit résoudre une équation diophantienne.
b. Pour déterminer les restes possibles d'une expression dans une division par un nombre m (constant), on raisonne en général par disjonction des cas.

→ Savoir-faire 4 et 10, p. 13 et 23

Les congruences sont un outil efficace pour traiter ce genre de questions et permettent de conclure à l'aide de la propriété suivante : « Pour tout entier $m \geqslant 2$ et tout entier a, il existe un unique entier r tel que $0 \leqslant r \leqslant m-1$ et $a \equiv r\ (m)$: le reste de la division euclidienne de a par m ».
c. On peut se souvenir que les restes des puissances a^n d'un entier naturel dans la division par un entier m sont périodiques.
Pour déterminer la période, on réduit, modulo 7, les premières puissances $2^1, 2^2, 2^3, 2^4 \ldots$ On constate que cette période est ici égale à 3. On raisonne ensuite modulo 3 sur l'entier n par disjonction des cas.

→ Savoir-faire 10, p. 23

d. Deux nombres égaux sont nécessairement congrus modulo 7. Comme les deux membres de l'équation ont été étudiés modulo 7, on essaie de savoir dans quels cas ils sont égaux modulo 7.

➤ Réponses

1. Si le couple $(x ; y)$ est une solution, on a :
$$7(2x^2 + y^2) = 2^{2n} \times 5^{2n}.$$
Le nombre du membre de gauche admet 7 comme facteur premier, ce qui n'est pas le cas du membre de droite. L'équation n'a pas de solution.

2. a. $7y^2 \equiv 0\ (7)$ donc, pour tout couple d'entiers $(x ; y)$ on a : $3x^2 + 7y^2 \equiv 3x^2\ (7)$.
Par ailleurs $10^2 - 2 = 14 \times 7$, donc $10^2 \equiv 2\ (7)$ et $(10^2)^n \equiv 2^n\ (7)$. Si le couple $(x ; y)$ est solution de (G), on a donc $3x^2 \equiv 2^n\ (7)$.

b. On complète le tableau suivant :

$x \equiv \ldots\ (7)$	0	1	2	3	4	5	6
$3x^2 \equiv \ldots\ (7)$	0	3	5	6	6	5	3

Les restes possibles dans la division de $3x^2$ par 7 sont donc 0, 3, 5 et 6.

c. Tout entier naturel n s'écrit sous l'une des formes $3q$, $3q+1$, $3q+2$ (où q est un entier naturel).
Si $n = 3q$, on a $2^n = 2^{3q} = (2^3)^q$.
Comme $2^3 \equiv 1\ (7)$, on a :
$$(2^3)^q \equiv 1^q\ (7), \text{ soit } 2^n \equiv 1\ (7).$$
Si $n = 3q+1$, on a $2^n = 2 \times 2^{3q}$, d'où $2^n \equiv 2\ (7)$.
De même, si $n = 3q+2$, on a $2^n = 2^2 \times 2^{3q}$, donc :
$$2^n \equiv 4\ (7).$$
Les restes dans la division euclidienne de 2^n par 7 sont donc 1, 2 ou 4.
d. D'après les questions précédentes, pour tout couple $(x ; y)$ d'entiers, l'entier $3x^2 + 7y^2$ est congru à 0, 3, 5 ou 6 modulo 7. Tandis que l'entier 10^{2n} est congru, modulo 7, à 1, 2 ou 4. Ces deux entiers ne sont donc jamais congrus modulo 7 et *a fortiori* jamais égaux.
L'équation (G) n'a donc aucune solution.

Pour se préparer à l'écrit BAC

Sujet A

Capacités mises en œuvre

- *Raisonner par disjonction des cas avec les restes d'une division euclidienne*
- *Calculer avec des congruences*

On se propose de déterminer les couples $(n\,;\,m)$ d'entiers naturels non nuls vérifiant la relation :

$$(F) : 7^n - 3 \times 2^m = 1.$$

1. Montrer qu'il y a exactement deux couples solutions pour $m \leqslant 4$.

2. On suppose $m \geqslant 5$.

a. Montrer que si le couple $(n\,;\,m)$ vérifie **(F)**, alors :

$$7^n \equiv 1\ (32).$$

b. En étudiant les restes de la division par 32 des puissances de 7, montrer que si le couple $(n\,;\,m)$ vérifie **(F)**, alors n est divisible par 4.

c. En déduire que si le couple $(n\,;\,m)$ vérifie **(F)**, alors :

$$7^n \equiv 1\ (5).$$

d. Pour $m \geqslant 5$, existe-t-il des couples $(n\,;\,m)$ vérifiant **(F)** ?

3. Déterminer l'ensemble des couples d'entiers naturels non nuls $(n\,;\,m)$ vérifiant **(F)**.

Savoir-faire

Question 2. c. → Savoir-faire 11, p. 25
Question 2. d. → Savoir-faire 7, p. 19

Sujet B VRAI – FAUX

Capacités mises en œuvre

- *Raisonner avec les congruences*
- *Reconnaître un nombre premier*

Pour chacune des propositions suivantes, indiquer si elle est vraie ou fausse et donner une justification.

1. On considère l'équation **(E)** :

$$x^2 + y^2 \equiv 0\ (3).$$

Proposition : « Il existe des couples $(x\,;y)$ d'entiers relatifs solutions de **(E)** qui ne sont pas des couples de multiples de 3 ».

2. Soit n un entier, $n \geqslant 3$.

Proposition : « Pour tout naturel k $(2 \leqslant k \leqslant n)$, le nombre $1 \times 2 \times 3 \times \ldots \times n + k$ n'est pas premier ».

3. Soit $N = 11^{2011}$.

Proposition : « L'entier n est congru à 4 modulo 7 ».

4. Soit n un entier tel que $n+3$ divise n^2+3.

Proposition : « Un tel entier n est tel que $n+3$ divise 6 ».

5. On considère l'équation :

$$81x^2 = y^2 + 17.$$

Proposition : « Il existe un unique couple $(x\,;\,y)$ d'entiers naturels solution de l'équation ».

Savoir-faire

Question 1. → Savoir-faire 4, p. 13
Savoir-faire 9, p. 23
Question 2. → Savoir-faire 6, p. 17
Question 3. → Savoir-faire 11, p. 25
Question 4. → Savoir-faire 1, p. 11
Question 5. → Savoir-faire 2, p. 11

Sujet C

Capacités mises en œuvre

- *Connaître les critères de divisibilité*
- *Reconnaître un nombre premier*
- *Calculer avec les congruences*

On considère la suite (u_n) d'entiers naturels définie par $u_0 = 1$ et pour tout entier naturel n :

$$u_{n+1} = 10 \times u_n + 21.$$

1. Calculer u_1, u_2 et u_3.

2. **a.** Démontrer par récurrence que pour tout entier n :

$$3u_n = 10^{n+1} - 7.$$

b. En déduire l'écriture décimale de u_n.

3. Montrer que u_2 est un nombre premier.

4. Démontrer que, pour tout entier naturel n, u_n n'est divisible ni par 2, ni par 3, ni par 5.

5. **a.** Démontrer que pour tout entier naturel n :

$$3u_n \equiv 4 - (-1)^n\ (11)$$

b. En déduire que, pour tout entier naturel n, u_n n'est pas divisible par 11.

6. **a.** Donner le reste de la division euclidienne de 10^4 par 17. En déduire que $10^{16} \equiv 1\ (17)$.

b. En déduire que, pour tout entier naturel k, u_{16k+8} est divisible par 17.

Savoir-faire

Question 3. → Savoir-faire 5, p. 17
Question 4. → Savoir-faire 12, p. 25
Question 5. b. → Savoir-faire 11, p. 25
Question 6. → Savoir-faire 10, p. 23

Sujet D ROC

Capacités mises en œuvre

- *Démontrer une propriété du cours*
- *Calculer avec des congruences*
- *Connaître la notion de reste dans une division euclidienne*

Partie A : Restitution organisée de connaissances

Prérequis : deux entiers a et b sont congrus modulo l'entier $m \geqslant 2$ si, et seulement si, ils ont même reste dans la division euclidienne par m.

Établir que, pour tous entiers a, b, a', b', si $a \equiv b\,(m)$ et $a' \equiv b'(m)$, alors $aa' \equiv bb'(m)$.

Partie B

On considère l'équation **(F)** : $11x^2 - 7y^2 = 5$ où x et y sont des entiers relatifs.

1. Démontrer que si le couple $(x\,;y)$ est solution de **(F)** alors :
$$x^2 \equiv 2y^2\,(5).$$

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

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

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

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

4. En déduire que si le couple $(x\,;y)$ est solution de **(F)**, alors x et y sont des multiples de 5.

5. Démontrer que si x et y sont des multiples de 5 alors le couple $(x\,;y)$ n'est pas solution de **(F)**.
Que peut-on en déduire pour l'équation **(F)** ?

Savoir-faire

Question B.3. → Savoir-faire 10, p. 23
Question B.4. → Savoir-faire 9, p. 23

Sujet E ROC

Capacités mises en œuvre

- *Connaître les propriétés de divisibilité dans $\mathbb{Z}$*
- *Démontrer une propriété du cours*
- *Connaître les propriétés des nombres premiers*

Partie A : Restitution organisée de connaissances

1. *Prérequis : Tout entier $n > 1$ admet au moins un diviseur premier.*

Démontrer que tout entier $n > 1$ est premier ou peut se décomposer en produit de facteurs premiers (on ne demande pas de démontrer l'unicité de cette décomposition).

2. Donner la décomposition en produit de facteurs premiers de 629.

Partie B

Pour tout entier naturel non nul n, on désigne par $\mathscr{P}_n$ le plan d'équation $z = n^4 + 4$.

1. Déterminer l'ensemble des points de $\mathscr{P}_1$ dont les coordonnées $(x\,;y\,;z)$ sont des entiers relatifs vérifiant $z = xy$.
Pour la suite de l'exercice, on suppose $n \geqslant 2$.

2. Développer $(n^2 - 2n + 2)(n^2 + 2n + 2)$.

3. Démontrer que, quel que soit l'entier naturel $n \geqslant 2$, l'entier $n^4 + 4$ n'est pas premier.

4. En déduire que le nombre de points du plan $\mathscr{P}_n$ dont les coordonnées $(x\,;y\,;z)$ sont des entiers relatifs vérifiant $z = xy$ est au moins égal à 8.

5. Déterminer les points de $\mathscr{P}_5$ dont les coordonnées $(x\,;y\,;z)$ sont des entiers relatifs vérifiant $z = xy$.

Savoir-faire

Question B.3. → Savoir-faire 6, p. 17
Question B.4. → Savoir-faire 8, p. 19
Questions A.2., B.1. et B.5. → Savoir-faire 7, p. 19

Pour se préparer à l'oral BAC

153 Déterminer les entiers n tels que $n + 4$ divise $6n + 7$.

154 Quel est le reste de la division euclidienne de $2\,016^{2\,017}$ par 11 ?

155 En utilisant des congruences, déterminer les entiers n tels que $n^2 + n + 2\,021$ soit divisible par 7.

156 Déterminer tous les entiers x et y tels que $25x^2 = y^2 + 2\,017$.

157 Montrer que, pour tout entier naturel n, le nombre $1\,789^{2n} - 2\,027^n$ est divisible par 13.

158 Déterminer les entiers x tels que $3x^2 \equiv 52\,(7)$.

POUR ALLER PLUS LOIN

Le mot « entier » sans précision désignera toujours un entier relatif (c'est-à-dire un élément de $\mathbb{Z}$).

159 Logique

Soit a et b deux entiers naturels non nuls. Soit p un nombre premier. On note α l'exposant de p dans la décomposition de a et β l'exposant de p dans la décomposition de b.

1. Établir que si $\alpha < \beta$ alors l'exposant de p dans la décomposition de $a+b$ est égal à α.

2. La réciproque de l'implication précédente est-elle vraie ?

160 Somme de trois carrés

1. Quels sont les restes possibles de la division euclidienne par 8 d'un carré d'entier ?

2. En déduire qu'un entier ayant pour reste 7 dans sa division par 8 ne peut pas s'écrire comme la somme de trois carrés d'entiers.

161 Les rep-units

Les rep-units sont les entiers $N_2 = 11$, $N_3 = 111\ldots$ et pour tout $k \geqslant 2$, N_k entier dont l'écriture décimale comporte k chiffres, tous égaux à 1.

1. Citer deux nombres premiers n'apparaissant jamais dans la décomposition en facteur premier d'un rep-unit.

2. Décomposer en facteurs premiers N_3, N_4 et N_5.

3. Dans cette question, on cherche à savoir si un rep-unit peut être le carré d'un entier.

a. Soit n un entier qui vérifierait n^2 est un rep-unit.
Établir que n est congru à 1 ou 9 modulo 10 (indication : raisonner modulo 10 par disjonction des cas).

b. En déduire que $n^2 \equiv 1\ (20)$.

c. En déduire une contradiction et conclure quant au problème posé.

162 Majoration du quantième premier ROC

1. Restitution organisée de connaissances
Rappeler la démonstration de l'infinité des nombres premiers donnée dans le cours.

2. On note (p_n) la suite des nombres premiers (pris dans l'ordre croissant) : $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7\ldots$
Soit n un entier naturel non nul.
En considérant le nombre $A = p_1 p_2 \ldots p_n - 1$ et un raisonnement similaire à celui qui a été utilisé dans le cours pour établir l'infinité des nombres premiers, établir l'inégalité :

$$p_{n+1} < p_1 p_2 \ldots p_n.$$

163 Un polynôme de nombres premiers

On définit la fonction g par $g(x) = ax^2 + bx + c$ où a, b et c sont des entiers naturels, a non nul.
On cherche si l'on peut donner à a, b et c des valeurs telles que $g(n)$ soit premier pour tout entier naturel n.

1. Établir que c doit être premier.

2. Conclure à l'aide de l'image de kc, où k est un entier.

164 Critère de divisibilité symétrique

Soit $n = \overline{a_k a_{k-1} \ldots a_1 a_0}$ un naturel. Le critère de divisibilité par 3 ou par 9 ne dépend pas de l'ordre des chiffres de l'entier considéré : tout entier obtenu en permutant les chiffres de n sera divisible par 9 (respectivement par 3) si, et seulement si, n l'est.
On aimerait prouver que seuls 9 et 3 possèdent cette propriété, plus précisément : « Si un naturel $d \geqslant 2$ vérifie que d divise n implique d divise tout entier m obtenu par une permutation quelconque des chiffres de n, alors $d = 3$ ou $d = 9$ ».
Soit d un entier, au moins égal à 2, vérifiant la propriété « si d divise n, alors d divise tout entier m s'écrivant avec les mêmes chiffres que n ».

1. Soit $A = 10^{r+2}$, $r+1$ étant le nombre de chiffres de l'écriture décimale de d. On note B le reste de la division de A par d. Montrer que $A + d - B$ s'écrit sous la forme $\overline{10a_r a_{r-1} \ldots a_0}$ et est multiple de d.

2. Conclure, en utilisant les entiers $\overline{a_r a_{r-1} \ldots a_0 10}$ et $\overline{a_r a_{r-1} \ldots a_0 01}$, que d est égal à 3 ou 9.

3. Existe-t-il un entier $d \geqslant 2$ vérifiant la propriété suivante : « Pour tout naturel n, d divise n si, et seulement si, d divise le produit des chiffres de n » ?

165 Les nombres de Fermat

On appelle nombres de Fermat les entiers $F_n = 2^{(2^n)} + 1$.

1. Établir que, pour tout entier naturel k, on a :

$$F_{n+k} - 1 = (F_n - 1)^{2^k}.$$

2. En déduire que $F_{n+k} \equiv 2\ (F_n)$.

3. En déduire que deux nombres de Fermat distincts n'ont pas de facteur premier commun.

4. Retrouver alors l'infinitude de l'ensemble des nombres premiers.

Point Histoire

En 1640, le mathématicien **Pierre de Fermat** pensait que les nombres $F_n = 2^{(2^n)} + 1$ (que l'on appelle aujourd'hui les nombres de Fermat) sont tous premiers.
Aujourd'hui, on ne sait ni si une infinité de nombres de Fermat sont premiers ni si une infinité de nombres de Fermat sont composés.

166 Les premiers de la forme $6n+1$ ou $6n-1$

On note (p_n) la suite des nombres premiers (pris dans l'ordre croissant) : $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7\ldots$

1. Quels sont les nombres premiers qui ne sont pas congrus à 1 ou à -1 modulo 6 ?

2. Soit f un entier naturel non nul et $A = p_1 p_2 \ldots p_f - 1$.

a. Justifier que les facteurs premiers de A sont des nombres premiers p_i avec $i > f$.

b. Justifier que $A \equiv -1\ (6)$ et en déduire que l'un au moins des facteurs premiers de A est congru à -1 modulo 6.

c. En déduire qu'il existe une infinité de nombres premiers de la forme $6n+5$ (on pourra raisonner par l'absurde).

167 Le code ISBN

Les livres publiés sont marqués d'un code ISBN (*international standard book number*). Ce code est constitué d'un identifiant de 9 chiffres, suivi d'une clef qui est un chiffre ou la lettre X (10 en numérotation romaine). On note $a_1a_2\dots a_9K$ un code ISBN. La clef K est calculée de façon à ce que la somme :

$$K+\sum_{j=2}^{10} j\times a_{11-j}\equiv 0\ (11).$$

1. Calculer la clef correspondant à l'identifiant 2–04–732853.
2. Déterminer une méthode de calcul de la clef K à l'aide de la division euclidienne de $\sum_{j=2}^{10} j\times a_{11-j}$ par 11.
3. Montrer qu'une erreur unique sur un chiffre lors de la frappe d'un code ISBN peut être détectée automatiquement.
4. Montrer que lorsque deux chiffres consécutifs distincts sont intervertis (erreur de frappe assez fréquente), le code obtenu ne peut être un code ISBN.

168 Le numéro INSEE

Le numéro INSEE d'un individu est constitué d'un identifiant de 13 chiffres suivi d'une clef K de deux chiffres.
On le retrouve sur les cartes vitales. L'identifiant comporte un certain nombre d'informations relatives à cet individu.

1. Le premier chiffre (à gauche) est, par exemple, 1 pour un homme, 2 pour une femme. La clef K est calculée de la façon suivante : soit r le reste de la division euclidienne de l'identifiant A (les 13 chiffres de gauche) par 97, on pose $K=97-r$.
Vérifier ceci sur le numéro INSEE d'une personne de votre famille ayant une carte vitale.
2. On écrit l'identifiant A sous la forme $A=H\times 10^6+L$ avec $0\leqslant L\leqslant 10^6$. Montrer que $K=97-s$ où s est le reste de la division de $27H+L$ par 97.
3. Déterminer les restes des entiers 10^n dans la division par 97 pour $1\leqslant n\leqslant 12$.
4. Montrer que si exactement un des 15 chiffres d'un numéro INSEE est erroné, alors le code n'est plus un code INSEE valide (on étudiera les cas où l'erreur est dans H, dans L, dans K).

169 Le code RIB

Un relevé d'identité bancaire (RIB) comporte un identifiant de 21 chiffres suivi d'une clef de 2 chiffres. Pour un identifiant A (les 21 chiffres de gauche), la clef K (les deux chiffres de droite) est égale à $K-r$ où r est le reste de la division de $100A$ par 97.

1. Calculer (en expliquant le calcul) la clef K pour l'identifiant :
16945004000458155381 1.
Comment mener ce calcul avec une calculatrice ?
(On pourra écrire $100A$ sous la forme $10^{12}a+10^6b+c$.)
2. Déterminer les restes des entiers 10^n dans la division par 97, pour $1\leqslant n\leqslant 20$.
3. Montrer que si l'on se trompe sur un seul chiffre en relevant un code RIB, alors le code obtenu n'est plus un code RIB valide.
4. Établir que si deux chiffres consécutifs distincts sont intervertis, alors le code n'est plus un code RIB valide.

170 Le nombre de diviseurs ALGO

Soit $n\geqslant 2$ un entier. Pour tout naturel k tel que $1\leqslant k\leqslant n$, on définit $g_n(k)$ par $g_n(k)=E\left(\frac{n}{k}\right)-E\left(\frac{n-1}{k}\right)$.

1. Écrire un programme pour votre calculatrice prenant en entrée un entier $n\geqslant 2$ et un entier $k\ (1\leqslant k\leqslant n)$ et fournissant en sortie l'entier $g_n(k)$.
Émettre une conjecture sur l'expression de $g_n(k)$ en fonction de n et k, puis démontrer cette conjecture.
2. Écrire un programme pour votre calculatrice prenant en entrée un entier $n\geqslant 2$ et fournissant en sortie la somme :

$$d_n=\sum_{k=1}^{n} g_n(k).$$

Que représente la sortie d_n pour l'entier n donné en entrée ?
3. On définit la suite (u_n) pour tout entier $n\geqslant 2$ par :

$$u_n=n\times E\left(\frac{1}{-1+d_n}\right).$$

a. Modifier le programme précédent pour qu'il affiche la valeur de u_n correspondant à l'entrée n.
b. Émettre, à l'aide du programme précédent, une conjecture sur l'expression de u_n en fonction de n.
Démontrer ensuite cette conjecture.
4. Modifier le programme pour qu'il affiche maintenant en sortie la somme :

$$S_n=\sum_{k=1}^{n}(k\times g_n(k)).$$

Que représente cette somme pour l'entier n donné en entrée ?

171 Factorielle 2013 ALGO

1. Écrire un programme pour votre calculatrice prenant en entrée un entier N et affichant en sortie l'exposant du facteur 23 dans la décomposition en facteurs premiers de N.
2. Modifier le programme afin qu'il affiche l'exposant de 23 dans la décomposition de 2 013! (où 2 013! désigne l'entier $2\times 3\times\dots\times 2\,013$).
3. Déterminer par un raisonnement l'exposant de 23 dans la décomposition en facteurs premiers de 2 013!.

172 Puissances modulaires ALGO

Écrire un programme pour votre calculatrice prenant en entrée un naturel A, un naturel $N\geqslant 1$ et un naturel $M\geqslant 2$ et fournissant en sortie le reste de la division de A^N par M.
On pourrait imaginer entrer simplement l'instruction :

$$A^N-M\times E\left(\frac{A^N}{M}\right),$$

mais il est demandé d'écrire un programme qui permette de dépasser la limite de capacité de calcul de cette instruction.

PISTE : Déterminer le reste de A^p à partir du reste de A^{p-1}.

173 Écriture en base *b* ALGO

On considère l'algorithme suivant :

Entrée : N, B deux entiers, $N \geqslant 1$, $B \geqslant 2$.
Traitement :
Tant que $N \neq 0$
  Q prend la valeur $E\left(\frac{N}{B}\right)$
  R prend la valeur $N - B \times Q$
  Afficher R
  N prend la valeur Q
Fin Tant que

1. Traduire l'algorithme pour votre calculatrice.

2. Avec $B = 10$, quel lien existe-t-il entre l'entrée N et les affichages ? Expliquer.

3. Justifier que le programme se terminera pour toute entrée $(N ; B)$.

4. On suppose que $B = 2$ et $N < 10^3$.
a. Justifier que $N \leqslant 2^{10}$.
b. Justifier que les affichages obtenus permettent d'écrire N sous la forme d'une somme de puissances de 2.
Donner une telle écriture pour les entiers 12 et 901.

174 Divisibilité par 6 ALGO

1. Traduire pour votre calculatrice l'algorithme suivant :

Entrée : un naturel N
Traitement :
Tant que $N \geqslant 10$:
  N s'écrivant $\overline{a_k\, a_{k-1} \ldots a_0}$, calculer
  $S = a_0 + 4 \times (a_1 + a_2 + \ldots + a_k)$.
  N prend la valeur S
Fin Tant que
Sortie : Afficher N

2. Justifier que l'algorithme se terminera quel que soit le naturel N donné en entrée.

3. Comment peut-on utiliser cet algorithme pour contrôler la divisibilité de l'entrée N par 6 ?

175 PROBLÈME DE SYNTHÈSE

Pour tout entier naturel non nul n, on pose $M_n = 2^n - 1$.
M_n est appelé nombre de Mersenne.

1. Calculer M_1, M_2, M_3 et M_4.

2. Pour a entier distinct de 1 et pour n entier naturel au moins égal à 2, montrer l'implication « si $a^n - 1$ est premier, alors $a = 2$ ». (On pourra utiliser la somme $1 + a + a^2 + \ldots + a^{n-1}$.)

3. Montrer l'implication suivante : « Pour tout entier naturel $n \geqslant 2$, si d divise n alors M_d divise M_n ».

4. Montrer l'implication suivante : « Pour tout entier naturel $n \geqslant 2$, si n est composé alors M_n est composé ».

5. Énoncer la contraposée de l'implication précédente.
Puis énoncer la réciproque de cette contraposée.
Cette réciproque est-elle vraie ?

6. Soit a et b deux naturels non nuls et r le reste de la division euclidienne de a par b. Montrer que le reste de la division euclidienne de M_a par M_b est M_r.

Point Histoire

Marin Mersenne (1588–1648) est un religieux français mathématicien et philosophe.

176 PROBLÈME DE SYNTHÈSE

1. Donner cinq nombres premiers de la forme $4n - 1$ et cinq nombres premiers de la forme $4n + 1$ (n entier).

2. Montrer qu'il existe une infinité de nombres premiers de la forme $4n - 1$ ou une infinité de premiers de la forme $4n + 1$.

3. On suppose qu'il n'existe qu'un nombre fini de nombres premiers $q_1, q_2, \ldots, q_f$ de la forme $4n - 1$.
On pose $A = 4q_1 q_2 \ldots q_f - 1$.
a. Établir que A est impair et que $A \geqslant 658\,811$.
b. Montrer qu'aucun des entiers q_i ne divise A.
En déduire que l'on doit avoir $A \equiv 1\ (4)$.
c. Conclure qu'il existe une infinité de nombres premiers de la forme $4n - 1$.

Prises d'initiatives

177 553 n'est pas premier mais en modifiant un chiffre (un seul), on peut obtenir un nombre premier : en modifiant le chiffre des dizaines en un 6, on obtient en effet 563 qui est premier. Cette propriété est-elle vérifiée pour tout entier naturel n ?

178 Quel est le chiffre des unités de l'entier $n^5 - n$ avec $n \in \mathbb{N}$?

179 Prendre cinq entiers au hasard. Vérifier que l'on peut en choisir trois dont la somme est multiple de 3. Démontrer que cela se réalisera quels que soient les cinq entiers choisis.

180 Déterminer les couples $(x ; y)$ d'entiers tels que :

$$x^2 - 7y^2 = 117.$$

181 Pour $n \in \mathbb{N}^*$, on définit $f(n) = 2\,014n + 2\,015$ et $r(n)$ comme étant le reste de la division de $f(n)$ par 8.
Exprimer $r(n)$ en fonction de n.

182 Soit n un entier.
Montrer que si $\sqrt{n}$ est un rationnel, alors $\sqrt{n}$ est un entier.

183 Démontrer que pour deux couples d'entiers $(a ; b)$ et $(c ; d)$ distincts, les nombres $a\sqrt{2} + b\sqrt{3}$ et $c\sqrt{2} + d\sqrt{3}$ sont distincts.

184 Est-il vrai que tout entier naturel non nul possède une infinité de multiples dont l'écriture décimale utilise au moins une fois chacun des 10 chiffres ?

Avant de commencer, se tester avec...

...des QCM

➤ Pour vous aider, voir le chapitre 1

Choisir la (ou les) bonne(s) réponse(s).

➤ Savoir utiliser la divisibilité dans $\mathbb{Z}$

On note $D(a)$ l'ensemble des diviseurs positifs de l'entier a.

	A	B	C	D
1 Soit a, b et c des entiers tels que a divise b et a divise c. Alors	a divise $b+c$	a divise $b-2c$	a divise b^2-c^2	a divise $\frac{b+c}{2}$
2 Si p et q sont des nombres premiers distincts, alors le nombre d'éléments de $D(p) \cap D(q)$ est	0	1	2	3

➤ Savoir utiliser la division euclidienne

3 Le reste de la division euclidienne de $5k-17$ (k entier) par 5 est	-17	-2	3	17
4 Si a est un entier impair, le reste de la division euclidienne de a^2 par 4 est	0	1	2	3

➤ Savoir utiliser les congruences dans $\mathbb{Z}$

5 Si a et b sont des entiers tels que $4a \equiv 4b$ (10), alors	$a \equiv b$ (10)	$2a \equiv 2b$ (5)	$8a^3 \equiv 8b^3$ (10)	$a-b$ est divisible par 10
6 Si 5 divise l'entier $n+3$, alors	$n \equiv 2$ (5)	$n \equiv -3$ (5)	$n = 5k+2$, avec k entier	$3n \equiv 1$ (5)

➤ Voir les réponses, p. 140

...des exercices

7 On donne l'égalité suivante : $182 = 8 \times 21 + 14$. Soit d un diviseur commun de 182 et de 21.
Montrer que d est aussi un diviseur de 14. En déduire les valeurs possibles de d.

8 Soit a, b deux nombres entiers non nuls.
On appelle q le quotient et r le reste de la division euclidienne de a par b.
Montrer que tout diviseur commun de a et de b est aussi un diviseur de r.

9 Montrer que l'équation $3x \equiv 3$ (6) équivaut à $x \equiv 1$ (2).

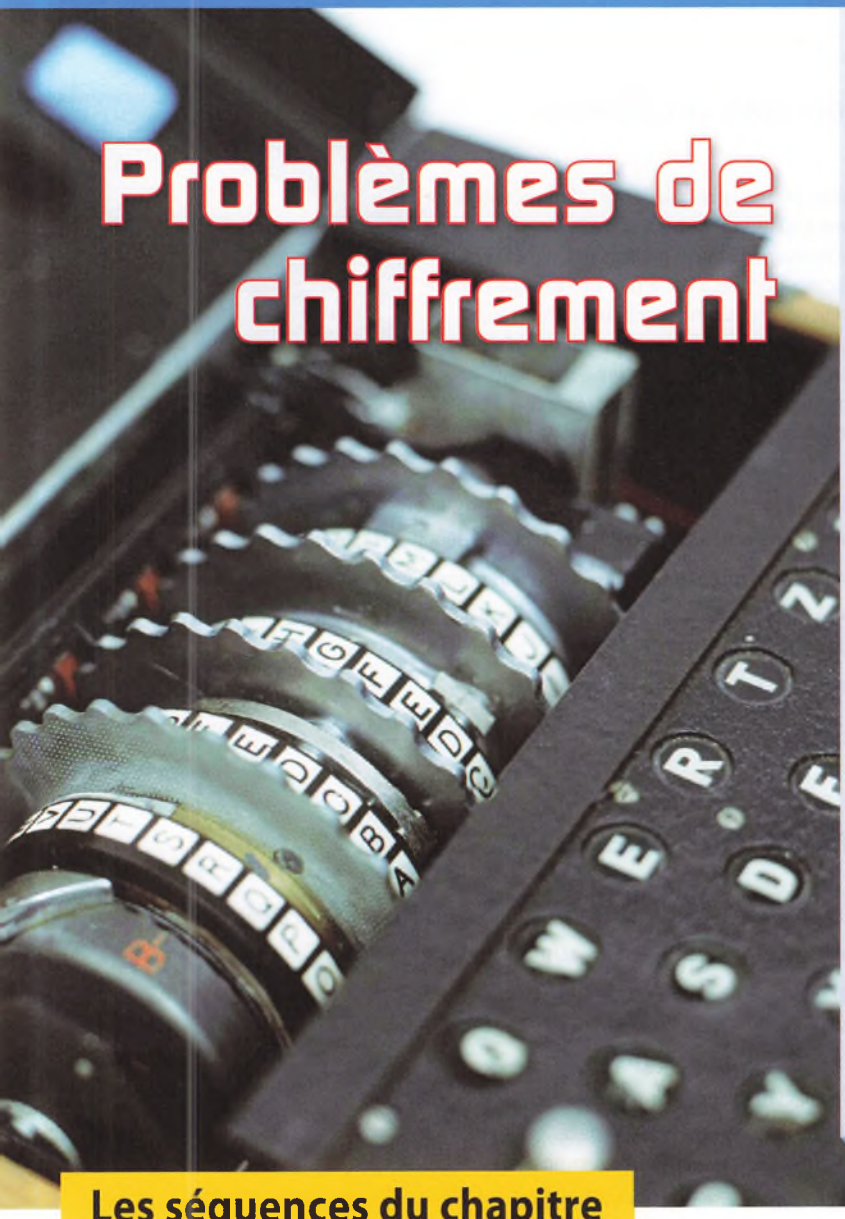
10 Soit $(O ; \vec{i}, \vec{j})$ un repère du plan.
Montrer que la droite d'équation $y = -\frac{x}{3} + \frac{11}{12}$ n'a pas de points à coordonnées entières.

11 n est un entier naturel. On pose $A_n = 3^n$.
Quels sont les restes possibles dans la division euclidienne par 4 de A_n en fonction de n ?

➤ Voir les réponses, p. 140

CHAPITRE 2

Problèmes de chiffrement



En cryptographie, le chiffrement est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Sur la machine Enigma ci-contre, utilisée par les Allemands pour coder leurs messages pendant la Seconde Guerre mondiale, la configuration des rotors constitue une partie de la clé de chiffrement.

De nos jours, on utilise d'autres procédés de chiffrement faisant appel notamment à l'arithmétique et l'informatique.

Il existe deux principaux types de chiffrement : le chiffrement symétrique, qui utilise la même clé pour chiffrer et déchiffrer et le chiffrement asymétrique, qui utilise une clé publique pour chiffrer et une clé privée pour déchiffrer.

Nous allons découvrir dans ce chapitre plusieurs méthodes de chiffrement, ainsi que les outils mathématiques permettant de les étudier.

Les séquences du chapitre

1. Plus grand diviseur commun de deux entiers
2. Entiers premiers entre eux
3. PPCM et petit théorème de Fermat

Raisonnement logique Logique
p. 63, 65 et 76

Les algorithmes ALGO
p. 44, 45, 48, 49, 53, 64, 66, 67, 70 et 76

Utilisation de logiciels TICE
p. 45, 49, 50, 51, 57, 64, 65, 70, 71 et 76

Problème 1 Un panneau publicitaire

Objectif
Redécouvrir la notion de PGCD de deux entiers naturels.

Cours 1
Généralités sur le PGCD

Partie A
Un panneau publicitaire a la forme d'un rectangle de dimensions 4,50 mètres et 1,80 mètre.
On veut le recouvrir d'encarts publicitaires carrés de même côté de façon optimale, c'est-à-dire que la régie publicitaire ne veut perdre aucun espace sur ce panneau.
On se propose de déterminer la taille maximale des encarts publicitaires que la régie peut vendre à ses clients.
Soit d la mesure en centimètres du côté de chaque carré.
Montrer que d divise 450 et 180.

Partie B
On note $D(a)$ l'ensemble des diviseurs positifs de l'entier a.

1. Décomposer 450 et 180 en facteurs premiers. En déduire $D(450)$ et $D(180)$.

2. Déterminer $D(450) \cap D(180)$. Quel est le plus grand diviseur commun de 450 et 180 ?

Le plus grand élément de $D(a) \cap D(b)$ *s'appelle le plus grand diviseur commun de a et de b, et on le note* PGCD $(a\,;b)$.

3. Résoudre alors le problème posé dans la **partie A**.

4. Retrouver le plus grand diviseur commun de 450 et de 180 en utilisant les décompositions de la question **1**.

Problème 2 Algorithme des différences ALGO

Objectif
Étendre la notion de PGCD à deux entiers relatifs et découvrir quelques propriétés du PGCD.

Cours 1
Généralités sur le PGCD

Partie A. PGCD de deux entiers relatifs
On appelle $D(a)$ l'ensemble des diviseurs (positifs et négatifs) de a, pour a entier non nul.

1. Soit $a = 110$ et $b = 66$. Déterminer $D(a)$ et $D(b)$.

2. Donner les valeurs des PGCD suivants :
a. PGCD (110 ; 66) **b.** PGCD (–110 ; 66) **c.** PGCD (– 66 ; 110) **d.** PGCD (–110 ; – 66)

Partie B. PGCD de la différence de deux entiers
Soit a et b deux entiers naturels non nuls.

1. Soit d un diviseur commun de a et de b.
Montrer que d est aussi un diviseur commun de $a - b$ et de b.

2. Soit d' un diviseur commun de $a - b$ et de b.
Montrer que d'est aussi un diviseur commun de a et de b.

3. En déduire que $D(a) \cap D(b) = D(a-b) \cap D(b)$ et que PGCD $(a\,;b)$ = PGCD $(a-b\,;b)$.

4. Soit $x = 4a + 3b$ et $y = 3a + 2b$.
Montrer que d est un diviseur commun de a et de b équivaut à dire que d est un diviseur commun de x et de y. En déduire que $D(a) \cap D(b) = D(x) \cap D(y)$
et que PGCD $(a\,;b)$ = PGCD $(x\,;y)$.

Partie C. Algorithme de calcul

1. Justifier que l'algorithme suivant détermine le PGCD de deux nombres entiers naturels. (*Max (a, b) renvoie le plus grand des deux nombres a et b ; de même Min (a, b) renvoie le plus petit des deux nombres a et b.*)

2. Programmer cet algorithme sur la calculatrice.

```
Saisir a, b
  Tant que a ≠ b
    c prend la valeur Max (a, b)
    b prend la valeur Min (a, b)
    a prend la valeur c – b
  Fin Tant que
Afficher a
```

Problème 3 Algorithme d'Euclide ALGO

Objectif
Découvrir un algorithme de calcul du PGCD de deux entiers naturels.

Cours 2
Détermination du PGCD par l'algorithme d'Euclide

Point Histoire
L'algorithme d'Euclide a été décrit par **Euclide** dans le livre VII des *Éléments* au IIIe siècle av. J.-C.

1. a et b sont deux entiers naturels non nuls tels que $a \geqslant b$. On appelle q le quotient et r le reste dans la division euclidienne de a par b. Soit d un diviseur commun de a et de b.
a. Montrer que d est aussi un diviseur commun de b et de r.
b. Montrer qu'un diviseur commun de b et r est aussi un diviseur commun de a et de b.
c. En déduire que PGCD $(a\,;b)$ = PGCD $(b\,;r)$.

2. On a effectué les divisions euclidiennes suivantes :
• $260 = 91 \times 2 + 78$ • $91 = 78 \times 1 + 13$ • $78 = 6 \times 13 + 0$
Compléter : PCGD (260 ; 91) = PGCD (91 ; …) = PCGD (… ; …) = PGCD (13 ; 0) = …

Remarque : Cette méthode de détermination du PGCD de deux nombres naturels non nuls s'appelle la « détermination du PGCD par l'algorithme d'Euclide ».

3. Déterminer le PGCD des nombres a et b suivants par l'algorithme d'Euclide.
a. $a = 123$ et $b = 95$.
b. $a = 715$ et $b = 55$.
c. $a = 616$ et $b = 52$.

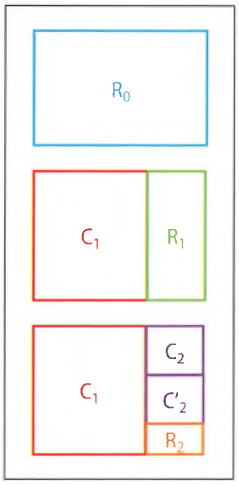
Problème 4 Pavage d'un rectangle TICE

Objectif
Visualiser géométriquement un algorithme.

Cours 2
Détermination du PGCD par l'algorithme d'Euclide

Point Histoire
Dans la tradition grecque, un couple d'entiers naturels étant considéré comme la longueur et la largeur d'un rectangle, leur PGCD était alors la mesure du côté du plus grand carré permettant de carreler entièrement ce rectangle.

1. Soit un rectangle R_0 de dimensions 21 et 15 centimètres. On se propose de paver ce rectangle par des carrés de même côté a, c'est-à-dire de recouvrir exactement ce rectangle par des carrés de côté a.
a. On construit un carré C_1 de côté 15 centimètres intérieur au rectangle R_0 comme sur le dessin ci-contre : ce rectangle R_0 est alors partagé en C_1 et en un nouveau rectangle R_1.
Montrer que si des carrés de côté a conviennent pour le pavage de R_0, ces carrés pavent C_1 et donc R_1.
b. On construit deux carrés identiques C_2 et C'_2 de côté le plus grand possible à l'intérieur du rectangle R_1 : R_1 est alors partagé en deux carrés et un nouveau rectangle R_2. Montrer que si des carrés de côté a conviennent pour le pavage de R_0, ces carrés pavent aussi C_2, C'_2 et donc R_2.
c. On constate alors que l'on peut paver le rectangle R_2 avec des carrés. Quelle est la taille maximale de ces carrés ? Ces carrés pavent-ils R_0 ?
d. La détermination de R_1 provient de l'égalité $21 = 15 \times 1 + 6$.
La détermination de R_2 provient de l'égalité $15 = 6 \times 2 + 3$.
Quelle est la dernière égalité utile dans cette démarche ?



2. Recommencer le pavage d'un rectangle de dimensions 21 et 10 centimètres.
Écrire les égalités numériques correspondant aux constructions géométriques effectuées.

3. On se propose de paver à présent un rectangle de dimensions 210 millimètres et 188 millimètres.
La construction géométrique paraissant difficile avec ces dimensions, on va opérer algébriquement.
a. Écrire les égalités numériques correspondant aux constructions à réaliser.
En déduire la taille maximale des carrés qui pavent ce rectangle.
b. Recommencer ces opérations à l'aide d'un tableur : on place dans les cellules **A2** et **B2** les dimensions du rectangle initial puis, dans les cellules suivantes des colonnes **A** et **B**, les dimensions du rectangle restant après chaque construction.

4. À l'aide d'un tableur, réaliser l'opération de pavage pour un rectangle de dimensions 452 et 620 mm, puis pour un rectangle de dimensions 216 et 960 mm.

Cours 1

Généralités sur le PGCD

Notation

Le plus grand commun diviseur de a et de b est noté **PGCD** $(a\,;b)$.

À noter

CASIO :
Sélectionner OPTN puis NUM puis *GCD*.
TEXAS :
Sélectionner math puis NUM puis *pgcd(* ou *gcd(*.

Définition Soit a et b des entiers naturels non nuls.
Le plus grand élément de $D(a) \cap D(b)$, ensemble des diviseurs positifs communs de a et de b, est **le plus grand commun diviseur** de a et b, ou encore **PGCD** de a et b.

Remarque : En particulier, le PGCD de a et a est a ; celui de 1 et a est 1.
De plus, le PGCD de a et 0 est a, car $D(0) = \mathbb{N}$.
Ainsi, le PGCD de deux entiers naturels est un entier au moins égal à 1.

Propriété Soit a et b des entiers naturels au moins égaux à 2.
Le plus grand diviseur commun de a et b est égal au produit des facteurs premiers communs de a et de b, avec pour chacun d'eux, l'exposant le plus petit de ceux qu'il a dans a et dans b.

Démonstration Soit d un diviseur commun de a et b, naturels au moins égaux à 2.
Comme d divise a, sa décomposition en facteurs premiers est formée de facteurs premiers de a avec un exposant au plus égal à celui qu'ils ont dans a.
De même, la décomposition en facteurs premiers de d est formée de facteurs premiers de b avec un exposant au plus égal à celui qu'ils ont dans b.
Ainsi, la décomposition de d comprend les facteurs premiers communs à a et à b, avec un exposant au plus égal au plus petit des exposants dans les décompositions de a et de b.
Pour que d soit le plus grand des diviseurs communs, ces exposants sont égaux au plus petit de ceux se trouvant dans les décompositions de a et de b.

Exemple : $700 = 2^2 \times 5^2 \times 7$ et $90 = 2 \times 3^2 \times 5$.
D'où $\text{PGCD}(700\,;90) = 2 \times 5 = 10$.

On peut généraliser la définition précédente à des entiers quelconques.
Soit a et b deux entiers non nuls simultanément.
Comme $D(-a) = D(a)$ et $D(-b) = D(b)$, alors $\text{PGCD}(a\,;b) = \text{PGCD}(|a|\,;|b|)$.
On pourra ainsi limiter l'étude du PGCD de deux entiers à celle du PGCD de deux naturels.
Par exemple $\text{PGCD}(255\,;-123) = \text{PGCD}(255\,;123) = \text{PGCD}(-255\,;-123) = 3$.

Propriétés
(1) a et b sont deux entiers naturels. Si a divise b, alors $\text{PGCD}(a\,;b) = a$.
(2) **Propriété fondamentale :** Soit a non nul tel que $a = bk + r$ où k est un entier.
Alors $D(a) \cap D(b) = D(b) \cap D(r)$ et $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a - bk)$.

Démonstrations
(1) En effet, si a divise b, tout diviseur de a est un diviseur de b, et ainsi $D(a) \cap D(b) = D(a)$, et le plus grand élément de $D(a)$ est a.
(2) Pour démontrer l'égalité des deux ensembles $E = D(a) \cap D(b)$ et $F = D(b) \cap D(r)$, on montre que E est inclus dans F, et que F est inclus dans E.
E est l'ensemble des diviseurs communs de a et de b et F est l'ensemble des diviseurs communs de b et de r.
Si d est un élément de E alors d divise b, donc d divise bk, et comme d divise a, il divise toutes les combinaisons linéaires de a et de b donc en particulier $a - bk = r$.
Puisque d divise b et r, il appartient bien à F.
Si d est un élément de F, alors d divise b, donc d divise bk et, comme d divise r, alors d divise $a = bk + r$.
Comme d divise a et b, d appartient à E.
Les ensembles E et F étant égaux, le plus grand élément de l'un est égal au plus grand élément de l'autre, d'où $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r) = \text{PGCD}(a\,;a - bk)$.

Exemple : $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a - b) = \text{PGCD}(b\,;a + b)$.

Cette propriété s'applique en particulier si k est le quotient et r le reste lors de la mise en œuvre de l'algorithme d'Euclide : si $a = bk + r$, alors $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$.

Savoir-faire 1

➤ Voir l'exercice 7

Déterminer le PGCD de deux entiers

Déterminer le PGCD de 330 et 252.

Méthode
Pour calculer le PGCD de deux entiers pas trop grands, on les décompose d'abord en facteurs premiers.

Solution

On décompose 330 et 252 en facteurs premiers.

330	2	252	2
165	5	126	2
33	11	63	3
3		21	3

Comme $330 = 2 \times 5 \times 11 \times 3$ et $252 = 2^2 \times 3^2 \times 7$, on en déduit :
PGCD (330 ; 252) = $2 \times 3 = 6$.

On peut aussi utiliser le programme donné dans le chapitre 1.

Savoir-faire 2

➤ Voir les exercices 52 et 53

Déterminer le PGCD de deux entiers dépendant d'un naturel *n*

Déterminer, selon les valeurs de l'entier *n*, le PGCD de $A = 3n + 1$ et de $B = n - 2$.

Méthode
Pour déterminer le PGCD de deux nombres dépendant d'un entier *n*, on peut utiliser la propriété fondamentale.

Solution

Pour éliminer *n*, on calcule $A - 3B$: $A - 3B = 3n + 1 - 3(n - 2) = 3n + 1 - 3n + 6 = 7$.
On peut donc écrire $A = 3B + 7$.
En utilisant la propriété fondamentale du cours, on a PGCD $(A ; B)$ = PGCD $(A ; 7)$.
Comme 7 est un nombre premier, il n'a que deux diviseurs : 1 et lui-même.
Alors PGCD $(A ; B) = 1$ ou PGCD $(A ; B) = 7$.
PGCD $(A ; B) = 7 \Leftrightarrow$ PGCD $(B ; 7) = 7 \Leftrightarrow 7$ divise $B \Leftrightarrow B \equiv 0\ (7)$
$\Leftrightarrow n - 2 \equiv 0\ (7) \Leftrightarrow n \equiv 2\ (7) \Leftrightarrow n = 2 + 7k$, avec $k \in \mathbb{Z}$.
Quand *n* est congru à 2 modulo 7, le PGCD de *A* et *B* est 7, sinon le PGCD de *A* et *B* est 1.

Savoir-faire 3

➤ Voir les exercices 54 et 55

Démontrer l'égalité de deux PGCD

Soit *a* et *b* deux entiers naturels non nuls.
Soit $x = 3a + 5b$ et $y = 2a + 3b$. Montrer que $(x ; y)$ et $(a ; b)$ ont le même PGCD.

Méthode
Pour démontrer l'égalité de deux PGCD *d* et *d'*, on peut :
- soit utiliser la propriété fondamentale ;
- soit montrer que $d \mid d'$ et que $d' \mid d$ et donc que $d = d'$.

Solution

- **Première méthode en utilisant la propriété fondamentale**

Égalités	Égalités de PGCD
$3a + 5b = (2a + 3b) + a + 2b$	PGCD $(x ; y)$ = PGCD $(3a + 5b ; 2a + 3b)$ = PGCD $(2a + 3b ; a + 2b)$
$2a + 3b = 2(a + 2b) - b$	PGCD $(2a + 3b ; a + 2b)$ = PGCD $(a + 2b ; -b)$ = PGCD $(a + 2b ; b)$
$a + 2b = 2b + a$	PGCD $(a + 2b ; b)$ = PGCD $(a ; b)$

On en déduit que PGCD $(x ; y)$ = PGCD $(a ; b)$.

- **Deuxième méthode**

Soit d = PGCD $(a ; b)$ et d' = PGCD $(x ; y)$.
Alors *d* divise *a* et *b*, et aussi $3a + 5b$ et $2a + 3b$. Donc *d* divise le PGCD de *x* et *y*. Ainsi *d* divise *d'*.
Comme *d'* divise *x* et *y*, *d'* divise toute combinaison linéaire de *x* et *y*, et il divise en particulier :
$2x + 3y = 2(3a + 5b) - 3(2a + 3b) = b$.
d' divise $-3x + 5y = -3(3a + 5b) + 5(2a + 3b) = a$. Ainsi *d'* divise *a* et *b*. Donc $d = d'$.

Cours 2

Détermination du PGCD par l'algorithme d'Euclide ALGO

Soit a et b deux entiers naturels non nuls tels que $a \geqslant b$.

Pour déterminer le plus grand commun diviseur de a et b, on suit le raisonnement ci-dessous.

On effectue la division euclidienne de a par b : $a = bq_1 + r_1$, avec $0 \leqslant r_1 < b$.

- Si $r_1 = 0$, alors PGCD $(a\,;b) = r$ (dans ce cas, b divise a).
- Si $r_1 \neq 0$, alors PGCD $(a\,;b)$ = PGCD $(b\,;r_1)$, et on effectue la division euclidienne de b par r_1.
  On a : $b = r_1q_2 + r_2$, avec $0 \leqslant r_2 < r_1$.
- Si $r_2 = 0$, alors PGCD $(a\,;b)$ = PGCD $(b\,;r_1) = r_1$.
- Si $r_2 \neq 0$, alors PGCD $(b\,;r_1)$ = PGCD $(r_1\,;r_2)$, et on effectue la division euclidienne de r_1 par r_2.
  On a : $r_1 = r_2a_3 + r_3$, avec $0 \leqslant r_3 < r_2$.

À noter
La suite des restes est strictement décroissante et à valeurs dans $\mathbb{N}$, ce qui justifie l'existence d'un reste nul.

Cette succession de divisions euclidiennes permet de déterminer des restes r_1, r_2, r_3, ... tels que $0 \leqslant \ldots < r_3 < r < r_1$. Puisque ces restes sont entiers, il existe un reste qui est nul.

Notons r_n le dernier reste non nul. On a alors :

$$\text{PGCD}\,(a\,;b) = \text{PGCD}\,(b\,;r_1) = \text{PGCD}\,(r_1\,;r_2) = \ldots = \text{PGCD}\,(r_n\,;0) = r_n.$$

Ces divisions successives peuvent être organisées dans le tableau suivant :

	Diviseur	Reste
a	b	r_1
b	r_1	r_2
r_1	r_2	r_3
...	...	...
r_{n-1}	r_n	0

Propriété Le PGCD de deux naturels non nuls a et b tels que b ne divise pas a est le dernier nombre de la colonne des diviseurs, c'est-à-dire le dernier reste non nul de la suite des divisions de l'algorithme d'Euclide.

Corollaires

(1) L'ensemble des diviseurs communs à deux entiers a et b est l'ensemble des diviseurs de leur PGCD : si d = PGCD $(a\,;b)$, alors $D(a) \cap D(b) = D(d)$.

(2) Soit a et b des entiers non nuls ; si k est un entier naturel non nul :

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

À noter
Si on multiplie deux entiers par un naturel non nul, leur PGCD est multiplié par cet entier naturel.

Démonstrations

(1) La propriété vue dans le paragraphe précédent permet d'écrire :
$D(a) \cap D(b) = D(b) \cap D(r_1) = D(r_1) \cap D(r_2) = \ldots = D(r_n) \cap D(0) = D(r_n) = D(d)$, puisque $r_n = d$.

(2) On note d le PGCD de a et b et d' celui de ka et kb.
Comme d divise a et b, alors kd divise ka et kb, d'où kd divise leur PGCD d'.
On peut ainsi écrire $d' = k'(kd)$, avec k' entier.
d' divise aussi ka et kb, d'où $k'kd$ divise ka et kb : on en déduit que $k'd$ divise a et b, donc $k'd$ divise leur PGCD d.
Ainsi, k' vaut 1, et on a bien l'égalité $d' = kd$.

Exemple : Pour déterminer les diviseurs communs de 345 et de 1 305, on détermine le PGCD de 345 et 1 305, par exemple à l'aide de la calculatrice.
Ici, PGCD (345 ; 1 305) = 15 et les diviseurs communs de 345 et de 1 305 sont les diviseurs de 15 soit {1 ; 3 ; 5 ; 15}.

Remarque : Dans l'algorithme d'Euclide associé aux entiers naturels a et b, si $a < b$, la première division permet d'inverser les rôles de a et b.
En effet, la première division fournit $a = 0 \times b + a$ et, de cette façon, a devient le premier reste de la suite des divisions, donc la seconde division est celle de b par a, avec $b > a$.

Savoir-faire 4

➤ Voir l'exercice 56

Déterminer le PGCD de deux entiers par l'algorithme d'Euclide

Déterminer le PGCD de 8 820 et 3 150.

Conseil
Compléter le tableau en utilisant le programme de la division euclidienne de votre calculatrice proposée au chapitre 1.

Solution

$8\,820 = 3\,150 \times 2 + 2\,520$; $3\,150 = 2\,520 \times 1 + 630$; $2\,520 = 630 \times 4$.
Le dernier reste non nul de la suite des divisions successives est 630, donc le PGCD de 8 820 et 3 150 est 630.

a	b	Restes
8 820	3 150	2 520
3 150	2 520	630
2 520	630	0

Savoir-faire 5

➤ Voir l'exercice 62

Programmer l'algorithme d'Euclide avec une calculatrice ALGO

Programmer l'algorithme d'Euclide à l'aide de la calculatrice.

Conseil
Le fait que a soit plus petit ou plus grand que b n'est pas à prendre en compte avec cet algorithme.

Solution

Saisir a, b
  Tant que $b \neq 0$ — *Début de la boucle*
    q prend la valeur Partie entière de $\left(\frac{a}{b}\right)$
    r prend la valeur $a - b \times q$
    a prend la valeur b — *Le nouveau dividende est b*
    b prend la valeur r — *Le nouveau diviseur est r*
  Fin Tant que
Afficher a — *C'est le dernier reste non nul*

```
?→A:?→B↵
While B≠0↵
Int (A÷B)→Q↵
A-B×Q→R:B→A:R→B↵
WhileEnd↵
A
```

Casio

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

Texas

Savoir-faire 6

Programmer l'algorithme d'Euclide avec un tableur ALGO TICE

1. **Utiliser un tableur pour déterminer le PGCD de deux naturels non nuls par l'algorithme d'Euclide.**

2. **Modifier la feuille de calcul afin que le tableur affiche des cellules vides après le dernier reste non nul.**

Conseil
Pour calculer le quotient de a par b, on utilise la fonction ENT du tableur.

Solution

1. On entre les deux naturels a et b dans les cellules **A1** et **B1**. On calcule en **C1** le quotient q de la division euclidienne de a par b, et en **D1** le reste r. On remplace a par b et b par r et on réitère la division.

	A	B	C	D
1	284	128	=ENT(A1/B1)	=A1-B1*C1
2	=B1	=D1	=ENT(A2/B2)	=A2-B2*C2
3	=B2	=D2	=ENT(A3/B3)	=A3-B3*C3
4	=B3	=D3	=ENT(A4/B4)	=A4-B4*C4
5	=B4	=D4	=ENT(A5/B5)	=A5-B5*C5

2. L'instruction `" "` affiche une cellule vide.
Il suffit alors de remplacer l'instruction entrée en **D1** par `=SI(A1-B1*C1=0;" ";A1-B1*C1)`, puis faire de même pour les instructions entrées en ligne 2.

	A	B	C	D
1	284	128	=ENT(A1/B1)	=SI(A1-B1*C1=0;"";A1-B1-C1)
2	=SI(OU(D1=0;D1="");"";B1)	=SI(OU(D1=0;D1="");"";D1)	=SI(OU(D1=0;D1="");"";ENT(A2/B2))	=SI(OU(D1=0;D1="");"";A2-B2*C2)

Fichiers logiciels
02_TSspe_SF6.xls
02_TSspe_SF6.xlsx
02_TSspe_SF6.ods
www. bordas-indice.fr

Problème 5

Chiffrement affine

TICE

Objectif
Découvrir la notion de nombres premiers entre eux.

Cours 3
Théorème de Bézout

Le chiffrement affine est une méthode de cryptographie basée sur un chiffrement par substitution. On choisit deux entiers naturels a et b comme clé. Chaque lettre du texte à chiffrer est remplacée par son équivalent numérique x. L'équivalent numérique de la lettre chiffrée est l'entier z compris entre 0 et 25 tel que :

$$z \equiv ax + b \ (26).$$

A	B	C	D	E	F	G
0	1	2	3	4	5	6

H	I	J	K	L	M	N
7	8	9	10	11	12	13

O	P	Q	R	S	T	U
14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

Partie A. Avec la calculatrice

Dans cette partie, on choisit $a = 15$ et $b = 8$.

1. Chiffrer le mot INDICE.

2. On veut déchiffrer le mot MKAIUQ (avec $a = 15$ et $b = 8$).

a. Montrer que déchiffrer la lettre M revient à trouver une solution de l'équation **(E)** : $15x - 26y = 4$, où x désigne le nombre entier compris entre 0 et 25 correspondant à la lettre déchiffrée et y un entier.

b. En remarquant que l'équation **(E)** peut s'écrire $y = \dfrac{15x - 4}{26}$, comment peut-on utiliser la table de valeurs de la calculatrice pour déchiffrer la lettre M ?

c. Déchiffrer alors le mot MKBIUQ.

Partie B. Avec un tableur

Dans cette partie, $a = 15$ et $b = 8$.

1. Écrire le message à coder sur la première ligne d'une feuille de calcul.

2. Transformer chaque lettre en un entier sur la deuxième ligne en utilisant la fonction **CODE**.

Remarque : la formule `=CODE(A1)` fournit le code ASCII de la lettre écrite en **A1**. Le code ASCII de A est 65, celui de B est 66, ..., celui de Z est 90.

A4 : =MOD(15*A3+8;26)

	A	B	C	D	E
1	M	A	T	H	S
2	77	65	84	72	83
3	12	0	19	7	18
4	6	8	7	9	18
5	G	I	H	J	S

3. En remarquant que l'équivalent numérique d'une lettre est égal à son code ASCII moins 65, calculer l'équivalent numérique de chaque lettre sur la troisième ligne.

4. En utilisant la fonction **MOD**, déterminer l'équivalent numérique de chaque lettre chiffrée sur la quatrième ligne.

5. Afficher le message chiffré sur la cinquième ligne à l'aide de la fonction **CAR** (celle-ci donne la lettre associée à un code ASCII, par exemple `CAR(90)=Z`).

6. Vérifier les résultats obtenus dans la question **1.** de la **partie A**.

Partie C. Messages indéchiffrables

1. Modifier les valeurs de a et b dans le tableur de la **partie B** en choisissant $a = 2$ et $b = 7$. Coder le mot MATHS. Que se passe-t-il ?

2. Montrer que résoudre l'équation $z \equiv 2x + 7 \ (26)$ revient à résoudre l'équation **(E')** : $2x - 26q = z - 7$ où q est un entier relatif.

3. Montrer que z est un entier impair.

4. Que se passe-t-il si on choisit $a = 2$ et $b = 8$? $a = 13$ et $b = 8$?
Quelle semble être la condition nécessaire sur a pour que l'on puisse déchiffrer les messages ?

Problème 6 Chiffrement à clé publique

Objectif
Travailler avec une relation de Bézout.

Cours 3
Théorème de Bézout

Point Histoire
Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par **Whitfield Diffie** et **Martin Hellman**.

Dans un chiffrement asymétrique (ou chiffrement à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) : une clé publique pour le chiffrement et une clé secrète pour le déchiffrement. La clé de chiffrement est accessible à tous, mais pas la clé de déchiffrement.

Exemple : Les lettres A, B, …, Z sont représentées par les nombres 0, 1, 2,…, 25.
On choisit quatre entiers naturels supérieurs ou égaux à 3 : a, b, c, d.
On calcule alors les nombres : $M = ab - 1$; $e = cM + a$; $f = dM + b$; $n = \dfrac{ef - 1}{M}$.

Le couple $(n\,;e)$ représente la clé publique et l'entier f représente la clé privée.

1. Montrer que $ef - 1$ est divisible par M. En déduire que n est un entier strictement supérieur à 25.

2. En écrivant $ef - Mn = 1$ et en utilisant la propriété fondamentale du PGCD (voir cours 1), montrer que le plus grand diviseur commun de e et de n est 1.

3. Benjamin désire envoyer un message à Adel. Il chiffre successivement les lettres de son message en associant à tout entier m compris entre 0 et 25 le reste p de la division euclidienne de $e \times m$ par n.
On choisit $a = 3$, $b = 4$, $c = 5$ et $d = 6$.

a. Déterminer la clé publique et la clé privée.

b. Montrer que $p \equiv 58m$ (369).

c. En utilisant l'égalité de la question **2.**, montrer que $m \equiv 70p$ (369).

d. Adel envoie à Benjamin le message suivant : CA VA. Chiffrer ce message.

e. Adel a reçu le message suivant de Benjamin : 74 – 211. Déchiffrer ce message.

Problème 7 Chiffrement de Vigenère TICE

Objectif
Découvrir le chiffrement de Vigenère.

Cours 3
Théorème de Bézout

Point Histoire
Blaise de Vigenère (1523–1596) est un diplomate et cryptographe français. Il a laissé son nom au chiffrement de Vigenère qui lui a été faussement attribué au XIX[e] siècle.

Ce chiffrement introduit le principe de clé. Une clé se présente généralement sous la forme d'un mot ou d'une phrase. On associe à chaque caractère une lettre de la clé pour effectuer la substitution. Plus la clé est longue et variée, mieux le texte sera chiffré. Chiffrons le mot MODULO avec la clé MATH.

On attribue à chaque lettre de l'alphabet un nombre entre 0 et 25, comme dans le tableau du problème 5.
Soit x le nombre correspondant à la lettre à chiffrer et y le nombre correspondant à la lettre de la clé.
La lettre chiffrée sera obtenue avec le nombre z, où z est le reste de $x + y$ dans la division euclidienne par 26.
Le mot MODULO devient YOWBXO.

	M	O	D	U	L	O
x	12	14	3	20	11	14
clé	M	A	T	H	M	A
y	12	0	19	7	12	0
z	24	14	22	1	23	14
	Y	O	W	B	X	O

1. On veut chiffrer le mot VIGENERE avec la clé MATH à l'aide d'un tableur. Pour cela, on utilise :
- la fonction **CODE**, qui associe à la lettre son code ASCII dans lequel A prend la valeur 65, B la valeur 66, …, Z la valeur 90 ;
- la fonction **MOD**(*N*;*M*), qui calcule le reste dans la division euclidienne de N par M ;
- la fonction **CAR**, qui retranscrit les nombres entiers compris entre 65 et 90 en lettres majuscules.

a. Saisir dans la zone de cellules **A1:H1** les lettres de ce mot, et dans la zone **B1:H1** la clé MATH en répétant les lettres.

b. Expliquer pourquoi l'instruction saisie en **A1:H1** `=CAR(MOD(CODE(A1)+CODE(A2)–2*65;26)+65))` permet de chiffrer la lettre V.

c. Chiffrer alors le mot VIGENERE.

2. On veut **déchiffrer** le mot EPXJUAEPFE, la clé étant toujours MATH.

a. Montrer que déchiffrer le premier E avec la lettre du mot clé M revient à résoudre l'équation **(1)** :
$x + 26q = -8$, où x est un entier compris entre 0 et 25, et q un entier relatif.

b. Montrer que l'équation **(1)** est équivalente à l'équation **(2)** : $x \equiv 18$ (26).

c. Que faut-il transformer dans la feuille de calcul de la question **1.** pour déchiffrer le mot EPXJUAEPFE ? Déchiffrer ce mot.

Cours 3

Théorème de Bézout

À noter

Deux nombres premiers sont premiers entre eux.
La réciproque est fausse.

Définition Deux entiers sont **premiers** entre eux lorsque leur PGCD est égal à 1.

Cela revient à dire que leurs seuls diviseurs communs sont –1 et 1.

Exemple : 25 et 14 sont premiers entre eux, car leur PGCD est 1.

Remarque : Il ne faut pas confondre nombres premiers et nombres premiers entre eux.
Par exemple, 7 est un nombre premier, mais 7 et 14 ne sont pas premiers entre eux.

Propriété Soit a et b deux entiers naturels non nuls et d le PGCD de a et b.
Alors il existe deux entiers naturels non nuls a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Démonstration Soit d = PGCD $(a ; b)$, alors a et b sont des multiples de d et il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$. De plus comme a et b sont deux entiers naturels non nuls, a' et b' sont aussi deux entiers naturels non nuls.
Donc PGCD $(a ; b)$ = PGCD $(da' ; db')$ = d' PGCD $(a' ; b')$.
D'où PGCD $(a' ; b') = 1$ et a' et b' sont bien premiers entre eux.

Point Histoire

Le théorème ci-contre a été attribué au mathématicien français **Étienne Bézout** (1730–1783) qui a généralisé un résultat établi par **Bachet de Méziriac** en 1621.

Théorème de Bézout Deux entiers a et b sont premiers entre eux si, et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.

Démonstration On suppose a et b premiers entre eux ; leur PGCD est 1.
Ainsi, l'un des deux au moins est non nul, par exemple a.
Soit l'ensemble E des entiers de la forme $au + bv$, avec u et v entiers.
Cet ensemble n'est pas vide, car il contient a (avec $u = 1$ et $v = 0$) et $-a$ (avec $u = -1$ et $v = 0$).
E contient a et $-a$, et l'un de ces deux entiers est strictement positif, donc E contient au moins un entier strictement positif.
Soit δ le plus petit d'entre eux : il existe ainsi u_0 et v_0 entiers tels que $\delta = au_0 + bv_0$.
La division euclidienne de a par δ s'écrit $a = \delta q + r$, avec $0 \leqslant r < \delta$.
D'où $r = a - \delta q = a - (au_0 + bv_0)q = a(1 - qu_0) + b(-v_0q)$.
Ainsi, r appartient à E car il est de la forme $au + bv$ avec u et v entiers ($u = 1 - q_0$ et $v = -v_0q$).
Comme δ est le plus petit élément strictement positif de E, l'inégalité $0 \leqslant r < \delta$ montre que r est nul, d'où $a = \delta q$ et δ divise a.
On montre de même que δ divise b, d'où $\delta = 1$ car a et b sont premiers entre eux : il existe bien deux entiers u_0 et v_0 tels que : $au_0 + bv_0 = 1$.
S'il existe des entiers u et v tels que $au + bv = 1$ alors, si d est le PGCD de a et b, il divise a et b, donc $au + bv$, c'est-à-dire 1. Ainsi, d vaut 1, et a et b sont premiers entre eux.

Vocabulaire

La relation $au + bv = 1$ est parfois appelée identité de Bézout relative aux entiers a et b.

Exemple : Comme 11 et 6 sont premiers entre eux, le théorème de Bézout assure l'existence de solutions entières pour l'équation $11x + 6y = 1$.

Corollaire Si d est le PGCD de deux entiers a et b, alors il existe des entiers u et v tels que :
$au + bv = d$.

Démonstration Soit a et b des entiers non nuls dont le PGCD est d.
Soit les entiers a' et b' tels que $a = da'$ et $b = db'$.
Comme a' et b' sont premiers entre eux, il existe des entiers u et v tels que
$ua' + vb' = 1$.
En multipliant les deux membres de cette égalité par d, on obtient : $ua'd + vb'd = d$, d'où :
$ua + vb = d$.
Si a ou b est nul, l'égalité est bien réalisée.

Exemple : PGCD $(15 ; 27) = 3$, donc on peut trouver deux entiers u et v tels que
$15u + 27v = 3$.
On peut choisir par exemple $u = 2$ et $v = -1$, ou encore $u = -7$ et $v = 4$.

Remarque : Un nombre premier est premier avec tous les entiers naturels non nuls strictement inférieurs à lui.

Savoir-faire 7

➤ Voir les exercices 69 et 70

Montrer que deux entiers sont premiers entre eux

Énoncé 1 Montrer que deux entiers consécutifs sont premiers entre eux.

Solution

Soit n et $n+1$ deux entiers consécutifs. On a l'égalité : $1 \times (n+1) + (-1) \times n = 1$.
Il existe un couple d'entiers $(1 ; -1)$ tel que $1 \times (n+1) + (-1) \times n = 1$.
Alors, d'après le théorème de Bézout, deux entiers consécutifs sont premiers entre eux.

Méthode
Pour démontrer que deux entiers sont premiers entre eux, on peut :
- soit utiliser le théorème de Bézout ;
- soit considérer le PGCD de ces deux nombres et montrer qu'il vaut 1.

Énoncé 2 Soit n un entier. Montrer que la fraction $F = \dfrac{2n+1}{2n+3}$ est irréductible.

Solution

F est irréductible si, et seulement si, $2n+1$ et $2n+3$ sont premiers entre eux.
Soit d un diviseur commun de $A = 2n+1$ et de $B = 2n+3$; d divise A et B donc divise toute combinaison linéaire de A et B et en particulier d divise $B - A = 2$.
d est alors un diviseur de 2, c'est-à-dire $d = 1$ ou $d = -1$, ou $d = 2$, ou $d = -2$.
Or A et B sont impairs, donc non divisibles par 2, ni par -2. Donc $d = 1$ ou $d = -1$.
Ainsi, PGCD $(A ; B) = 1$ et A et B sont premiers entre eux. F est bien irréductible pour tout entier n.

Savoir-faire 8

➤ Voir l'exercice 83

Déterminer des coefficients de l'identité de Bézout avec l'algorithme d'Euclide ALGO

Méthode
Pour déterminer des coefficients u et v de l'identité de Bézout, on écrit toutes les divisions de l'algorithme d'Euclide : on reporte alors chaque reste obtenu en partant de la fin.

Montrer que 99 et 56 sont premiers entre eux, puis déterminer des entiers u et v tels que : $99u + 56v = 1$.

Solution

On pose $a = 99$ et $b = 56$.
Le dernier reste non nul dans la suite des divisions euclidiennes est 1, donc 99 et 56 sont premiers entre eux. On a ainsi trouvé deux coefficients u et v : $u = -13$ et $v = 23$.

Division euclidienne	Reste	Égalité avec a et b
$99 = 56 \times 1 + 43$	$43 = 99 - 56$	$43 = a - b$
$56 = 43 \times 1 + 13$	$13 = 56 - 43$	$13 = b - (a - b) = 2b - a$
$43 = 13 \times 3 + 4$	$4 = 43 - 3 \times 13$	$4 = a - b - 3(2b - a) = 4a - 7b$
$13 = 4 \times 3 + 1$	$1 = 13 - 4 \times 3$	$1 = 2b - a - 3(4a - 7b) = -13a + 23b$

Savoir-faire 9

➤ Voir l'exercice 84

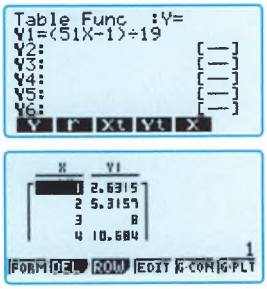
Déterminer des coefficients de l'identité de Bézout à l'aide de la calculatrice

Méthode
Pour déterminer des coefficients u et v de l'identité de Bézout $ux + vy = 1$ avec la calculatrice, on exprime y en fonction de x, puis on forme une table de valeurs en entrant en $Y1$ cette expression.

Déterminer un couple d'entiers $(x ; y)$ solution de l'équation (E) : $51x - 19y = 1$.

Solution

Comme 51 et 19 sont premiers entre eux, le théorème de Bézout assure l'existence d'un couple d'entiers $(x ; y)$ solution de (E).
L'équation (E) s'écrit aussi : $y = \dfrac{51x - 1}{19}$.
Dans la table de valeurs de la calculatrice, on saisit Y1=(51*X −1)/19, puis on construit un tableau de valeurs avec x variant à partir de 1 avec un pas de 1.
Le premier couple solution est obtenu quand $Y1$ est un entier : pour $X = 3$, on a $Y1 = 8$, donc un couple solution est $(3 ; 8)$.



Cours 4

Théorème de Gauss et applications

Théorème de Gauss Soit a, b, c des entiers.
Si a divise le produit bc et si a est premier avec b, alors a divise c.

Démonstration Si a est premier avec b, alors, d'après le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$.
En multipliant les deux membres de cette égalité par c, on obtient : $acu + bcv = c$.
Or, a divise acu et a divise bc par hypothèse, donc a divise bcv : on en déduit que a divise $acu + bcv$, c'est-à-dire c.

Exemple : Soit a et b deux entiers tels que $3a = 4b$.
Ici, 4 divise le produit $3a$ et les entiers 3 et 4 sont premiers entre eux, donc 4 divise a.

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

L'hypothèse « a et b premiers entre eux » est fondamentale.

Exemple : 36 est divisible par 4 et par 6, mais pas par leur produit 24.

Démonstration Comme n est divisible par a et b, il existe des entiers k et k' tels que : $n = ka = k'b$.
Cette égalité montre que a divise $k'b$.
Comme a et b sont premiers entre eux, le théorème de Gauss assure que a divise k', donc il existe un entier q tel que $k' = qa$.
On en déduit : $n = qab$, donc n est divisible par ab.

Point Histoire
Carl Friedrich Gauss (1777–1855) publia dès 1801 un important ouvrage de théorie des nombres : *Disquisitiones arithmeticae.*

À noter
Le corollaire 2 est très souvent utilisé pour prouver une divisibilité.

Corollaire 2
Si un entier premier divise un produit de facteurs ab, alors il divise au moins l'un des facteurs a ou b.

Démonstration Soit p un nombre premier divisant le produit ab.
Si p divise a, la conclusion est assurée.
Si p ne divise pas a, comme p est premier, alors a et p sont premiers entre eux ;
comme p divise ab, alors p divise b d'après le théorème de Gauss.

Corollaire 3
Si un entier p premier divise un produit de nombres premiers, alors p est égal à l'un deux.

Démonstration Soit p, a et b trois nombres premiers tels que p divise le produit ab.
Puisque a et p sont premiers, alors p est premier avec a ou $p = a$.
Si $p = a$, la conclusion est assurée.
Si $p \neq a$, alors d'après le théorème de Gauss, p divise b.
Comme p et b sont des nombres premiers alors $p = b$.

Corollaire 4
p est un entier premier avec les entiers a et b si, et seulement si, p est premier avec leur produit ab.

Démonstration Soit p un nombre premier avec a et b. Soit d un entier naturel non nul.
Si d divise p et ab, alors d divise pa et ab et d divise PGCD $(pa ; ab)$.
Or PGCD $(pa ; ab) = a \times$ PGCD $(p ; b) = a$ car PGCD $(p ; b) = 1$.
Donc d divise a. Comme d divise aussi p, d est un diviseur commun de p et a donc $d = 1$.
Ainsi, PGCD $(p ; ab) = 1$.
Réciproquement : soit p un nombre premier avec le produit ab, et d un entier naturel non nul.
Si d divise p et a alors d divise p et ab, donc d divise PGCD $(p ; ab) = 1$ donc $d = 1$ et PGCD $(p ; a) = 1$.
De même, on démontre que PGCD $(p ; b) = 1$ donc p est premier avec a et avec b.

Exemple : 22 est premier avec 57 et 35 donc 22 est premier avec 57×35, soit 995.

Savoir-faire 10 Résoudre une équation du type $ax + by = c$

➤ Voir l'exercice 85

Méthode
Pour résoudre une équation du type $ax = by$, avec a et b premiers entre eux et x et y entiers, on utilise le théorème de Gauss.

Énoncé 1 Déterminer les entiers x et y tels que $7x = 3y$.

Solution

7 divise $3y$ et les entiers 3 et 7 sont premiers entre eux. D'après le théorème de Gauss, 7 divise y.
Ainsi, $y = 7k$, avec k entier. En reportant dans l'équation : $7x = 3 \times 7k$, d'où $x = 3k$.
Les solutions sont les couples $(3k ; 7k)$, avec k entier quelconque.

➤ Voir l'exercice 86

Énoncé 2

1. Déterminer les entiers x et y tels que $6x + 11y = 1$.
2. Déterminer les entiers x et y tels que $6x + 11y = 7$.

Solution

1. Comme 6 et 11 sont premiers entre eux, le théorème de Bézout assure l'existence d'une solution. Pour déterminer une solution particulière de cette équation, on peut utiliser l'algorithme d'Euclide (savoir-faire 8) ou la calculatrice (savoir-faire 9).
Le couple $(2 ; -1)$ est une solution particulière de cette équation.
Ainsi : $6x + 11y = 6 \times 2 + 11 \times (-1)$.
En transformant cette équation, on obtient (E) : $6(x - 2) = 11(-1 - y)$.
On peut alors appliquer le théorème de Gauss : comme 6 et 11 sont premiers entre eux, alors 6 divise $(-1 - y)$ et 11 divise $(x - 2)$. Il existe un entier k tel que $x - 2 = 11k$, et un entier k' tel que $-1 - y = 6k'$.
Réciproquement, en reportant les valeurs de x et y dans l'équation (E), on trouve : $6 \times 11k = 11 \times 6k'$ et, par suite, $k = k'$.
Ainsi, les solutions sont les couples de la forme $(2 + 11k ; -1 - 6k)$, avec k entier quelconque.

2. Puisque $6 \times 2 + 11 \times (-1) = 1$, on a : $7 \times 6 \times 2 + 7 \times 11 \times (-1) = 7$. D'où $6 \times 14 + 11 \times (-7) = 7$.
Ainsi, $(14 ; -7)$ est une solution particulière de cette équation. On utilise alors la même méthode que ci-dessus : les couples solutions sont de la forme $(14 + 11k ; -7 - 6k)$, avec k entier quelconque.

Méthode
Pour résoudre une équation du type $ax + by = 1$, avec a et b premiers entre eux et x et y entiers, on cherche une solution particulière $(u ; v)$ de cette équation, puis on écrit :
$ax + by = au + bv$.

Savoir-faire 11 Utiliser le théorème de Gauss

➤ Voir l'exercice 87

Méthode
Pour montrer une divisibilité par $k = ab$, il suffit de montrer la divisibilité par a et par b, dès lors que a et b sont premiers entre eux.

Montrer que $A = n^3 - n$ est divisible par 6 pour tout entier n.

Solution

A peut s'écrire $A = n(n^2 - 1) = n(n + 1)(n - 1)$. Comme 2 et 3 sont premiers entre eux, pour montrer la divisibilité par $6 = 2 \times 3$, d'après le corollaire du théorème de Gauss, il suffit de montrer que A est divisible par 2 et par 3. On peut utiliser les congruences.

- *Divisibilité par 2* : on raisonne par disjonction des cas.

Si $n \equiv 0\ (2)$, alors $A \equiv 0 \times 3 \times (-1) \equiv 0\ (2)$.
Si $n \equiv 1\ (2)$, alors $A \equiv 1 \times 2 \times 0 \equiv 0\ (2)$.
Donc A est divisible par 2.

- *Divisibilité par 3* : on raisonne comme précédemment.

Si $n \equiv 0\ (3)$, alors $A \equiv 0\ (3)$.
Si $n \equiv 1\ (3)$, alors $A \equiv 1 \times 2 \times 0 \equiv 0\ (3)$.
Si $n \equiv 2\ (3)$, alors $A \equiv 2 \times 3 \times 1 \equiv 0\ (3)$.
Donc A est divisible par 3.
A est divisible par 2 et par 3, donc il est divisible par 6 pour tout entier n.

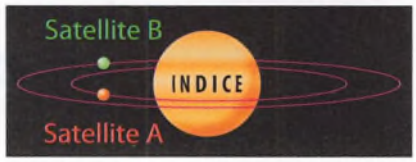
Séquence 3 — PPCM et petit théorème de Fermat

Problème 8 Satellites

Objectif
Découvrir le PPCM de deux entiers.

Cours 5
Plus petit commun multiple de deux entiers

La planète Indice a deux satellites.
Le satellite A effectue une révolution autour de la planète Indice en 68 heures. Le satellite B effectue la même révolution en 200 heures.
À 10 heures, le 1er janvier 2012, les deux satellites sont alignés.



1. Décomposer 68 et 200 en produit de nombres premiers.

2. À l'aide de ces décompositions, déterminer le plus petit multiple commun non nul de 68 et 200.

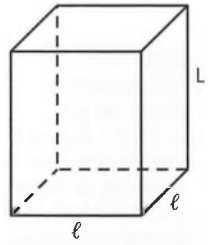
3. À quelles dates et heures retrouvera-t-on une configuration identique à celle du 1er janvier 2012 ? Combien chaque satellite aura-t-il alors effectué de révolutions ?

Problème 9 Remplissage d'une boîte

Objectif
Résoudre un problème faisant intervenir le PGCD et le PPCM de deux entiers.

Cours 5
Plus petit commun multiple de deux entiers

1. Soit B une boîte en forme de pavé droit de hauteur L, à base carrée de côté ℓ, où ℓ et L sont des entiers naturels non nuls tels que $\ell < L$.
On veut remplir la boîte B avec des cubes tous identiques dont l'arête a est un entier naturel non nul (les cubes devant remplir complètement la boîte B sans laisser d'espace vide).



a. Dans cette question, on pose $\ell = 882$ et $L = 945$.
Quelle est la plus grande valeur possible pour a ?
Quelles sont les valeurs possibles pour a ?
b. Dans cette question, le volume de la boîte B est $V = 77\,760$. On sait que, pour remplir la boîte B, la plus grande valeur possible de a est 12. Que représente 12 pour les nombres ℓ et L ?
Montrer qu'il y a exactement deux boîtes B possibles, dont on donnera les dimensions.

2. On veut remplir une caisse cubique C, dont l'arête c est un entier naturel non nul, avec des boîtes B toutes identiques telles que décrites dans la question **1.** (Les boîtes B, empilées verticalement et posées côte à côte horizontalement, doivent remplir complètement la caisse C sans laisser d'espace vide.)
Dans cette question, $\ell = 882$ et $L = 945$.
a. Justifier que c est un multiple commun de ℓ et L. Quelle est la plus petite arête c pour la caisse C ?
b. Quel est l'ensemble de toutes les valeurs possibles pour l'arête c ?

3. Dans cette question, le volume de la boîte B est 15 435. On sait que la plus petite arête possible pour la caisse C est 105. On cherche les dimensions ℓ et L de la boîte B.
a. Décomposer 15 435 et 105 en produit de nombres premiers.
b. En déduire les dimensions ℓ et L de la boîte B.

Problème 10 Nombres de Carmichaël

Objectif
Découvrir des nombres remarquables liés au petit théorème de Fermat.

Cours 6
Petit théorème de Fermat

1. Soit $P(a) = a^n - 1$, où a est un entier différent de 1, et n un entier supérieur ou égal à 1.
a. Calculer $1 + a + a^2 + \ldots + a^{n-1}$.
b. Montrer que $P(a)$ peut s'écrire sous la forme $k(a - 1)$, où k est un entier.

2. **a.** Montrer que $a^{2 \times 280} - 1 = k(a^2 - 1)$, avec k entier, puis que $a^{561} - a = k \times a(a^2 - 1)$.
b. En utilisant les congruences modulo 3, montrer que $a^{561} - a$ est divisible par 3.

3. **a.** Montrer que $a^{561} - a = k' \times a(a^{10} - 1)$ avec k' entier.
b. En utilisant les congruences modulo 11, montrer que $a^{561} - a$ est divisible par 11.

4. **a.** Montrer que $a^{561} - a = k'' \times a(a^{16} - 1)$ avec k'' entier.

b. En utilisant les congruences modulo 17, montrer que $a^{561} - a$ est divisible par 17.

5. En déduire que $a^{561} \equiv a$ modulo 561.

Un entier n non nul différent de 1 et qui n'est pas premier est appelé nombre de Carmichaël si, pour tout a entier, n divise $a^n - a$.

6. Pourquoi 561 est-il un nombre de Carmichaël ?

Point Histoire

Robert Daniel Carmichaël (1879–1967) est un mathématicien américain qui a étudié les propriétés de ces nombres, appelés aussi nombres absolument pseudo-premiers, dans le cadre de l'étude de la primalité d'un entier naturel.

Problème 11 Chiffrement par exponentiation

TICE

Objectif

Découvrir le petit théorème de Fermat et l'appliquer à un problème de chiffrement.

Cours 6
Petit théorème de Fermat

Vocabulaire

L'**exponentiation modulaire** est un type d'élévation à la puissance exécutée modulo un entier.
Elle est particulièrement utilisée en informatique, spécialement dans le domaine de la cryptographie.

Soit p un nombre premier et a un entier naturel non divisible par p. On appelle M(a) l'ensemble des $p-1$ premiers multiples strictement positifs de a, soit $M(a) = \{a ; 2a ; 3a ; \dots ; (p-1)a\}$.

Partie A. Une congruence remarquable

Dans cette partie, on prendra $p = 31$ et a un entier naturel non divisible par 31.

1. Justifier que 31 est premier avec tous les éléments de M (a).

2. On appelle r_k le reste de la division euclidienne de ka par 31, avec k entier naturel.
Donc $r_1, r_2, r_3, \dots, r_{30}$ sont les restes de la division euclidienne par 31 des éléments de M(a).
a. Montrer, en raisonnant par l'absurde, que, pour $k \neq k'$, avec k et k' éléments de l'ensemble $\{1 ; 2 ; \dots ; 29 ; 30\}$, on a $r_k \neq r_{k'}$.
b. En déduire que $r_1, r_2, r_3, \dots, r_{30}$ sont distincts deux à deux et appartiennent à l'ensemble :
$\{1 ; 2 ; 3 ; \dots ; 30\}$.

3. En déduire que $r_1 \times r_2 \times r_3 \times \dots \times r_{30} = 30 \times 29 \times \dots \times 2 \times 1$, puis que :
$30 \times 29 \times \dots \times 2 \times 1 \times a^{30} \equiv 30 \times 29 \times \dots \times 2 \times 1\ (31)$.

4. Montrer que $a^{30} \equiv 1\ (31)$.

Partie B. Chiffrement d'un message

Pour chiffrer un message, on traduit d'abord chaque lettre ou symbole en son équivalent numérique à l'aide du tableau ci-contre.

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23
Y	Z	.	;	?	!	espace	
24	25	26	27	28	29	30	

À chaque nombre B compris entre 0 et 30 (représenté par un bloc de deux chiffres : 00, 01, …, 30), on associe C, reste de la division euclidienne de B^7 par 31, c'est-à-dire vérifiant :
$C \equiv B^7\ (31)$.

1. Montrer qu'il existe des entiers d et v tels que $7d + 30v = 1$, avec $0 < d < 30$ et $v < 0$.

2. En utilisant la **partie A**, montrer que $B^{7d} \equiv B\ (31)$.

3. En déduire que $C^d \equiv B\ (31)$. *Dans ce cas, 7 est la clé de chiffrement et d la clé de déchiffrement.*

4. Chiffrer le mot MATH.

5. En utilisant un logiciel de calcul formel, déchiffrer le message suivant :
23 16 07 02 07 30 07 28 16 19 12 16 24 16 30 17 16 30 05 16 12 24 00 07 27.
(Avec le logiciel Xcas, **irem**(a,b) renvoie le reste de la division euclidienne de a par b.)

Cours 5

Plus petit commun multiple de deux entiers

Définition Le **plus petit commun multiple** des entiers naturels non nuls a et b est le plus petit élément de l'ensemble des multiples communs strictement positifs de a et de b.
On l'appelle aussi **PPCM** de a et b.

Notation
On note le plus petit commun multiple de a et b : PPCM $(a ; b)$.

Remarque : Le seul multiple de 0 est 0, donc le PPCM de a et de 0 est 0.
Le PPCM de a et b est un entier au moins égal à 1.
En particulier : PPCM $(a ; a) = a$ et PPCM $(1 ; a) = a$.

Avec la calculatrice :

Casio	Texas
Sélectionner OPTN puis NUM puis *ppcm* ou *lcm*.	Sélectionner math puis NUM puis *ppcm* ou *lcm*.

À noter
lcm est l'abréviation en anglais de *least common multiple*.

Généralisation Soit a et b des entiers.
PPCM $(a ; b)$ = PPCM $(|a| ; |b|)$.

Propriété Soit a et b des entiers naturels au moins égaux à 2.
Le PPCM de a et b est égal au produit de tous les facteurs premiers de a et de b avec, pour chacun d'eux, l'exposant le plus grand de ceux qu'il a dans a et dans b.

À noter
Cette propriété permet une détermination du PPCM lorsque les entiers ne sont pas trop grands.

Démonstration Soit m le PPCM de deux naturels a et b supérieurs ou égaux à 2.
Comme m est un multiple de a, sa décomposition en facteurs premiers comprend tous les facteurs premiers de a avec un exposant au moins égal à celui qu'ils ont dans la décomposition de a.
De même, elle comprend tous les facteurs premiers de b avec un exposant au moins égal à celui qu'ils ont dans la décomposition de b.
Ainsi, m comprend tous les facteurs premiers de a et de b, avec un exposant au moins égal au plus grand de ceux qu'il a dans a et dans b ; puisque m est le plus petit de ces multiples, l'exposant est dans chaque cas égal au plus grand de ceux qu'il a dans a et dans b.

Exemple : $75 = 3 \times 5^2$ et $45 = 3^2 \times 5$, donc : PPCM $(45 ; 75) = 3^2 \times 5^2 = 225$.

À noter
Si a et b sont premiers entre eux, le PPCM de a et b est égal au produit ab.

Propriétés
(1) L'ensemble des multiples communs de a et de b est l'ensemble des multiples de leur PPCM.
(2) Soit a et b des entiers. On a la relation :
PPCM $(a ; b) \times$ PGCD $(a ; b) = ab$.
(3) Si k est un entier naturel : PPCM $(ka ; kb) = k$ PPCM $(a ; b)$.

À noter
Cette relation (2) permet une détermination pratique du PPCM de deux entiers ; il suffit de déterminer le PGCD de ces entiers par l'algorithme d'Euclide puis d'utiliser cette relation.

Démonstration (1) et (2) On suppose a et b non nuls.
Soit d le PGCD de a et b : il existe des entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.
Soit m un multiple commun de a et de b : il existe alors des entiers k et k' tels que $\mu = ka = k'b$.
D'où : $kda' = k'db'$.
Comme d est non nul, on obtient : $ka' = k'b'$. Puisque a' divise $k'b'$ et que a' et b' sont premiers entre eux, on peut dire que a' divise k', d'après le théorème de Gauss. Il existe ainsi un entier q tel que $k' = qa'$.
On en déduit : $\mu = qa'b = qda'b'$.
Ainsi, tout multiple commun μ à a et b est un multiple de $da'b'$: le plus petit de ces multiples communs m est obtenu pour $q = 1$, ce qui fournit : $m = da'b'$. D'où : $md = (da')(db') = ab$.
Si a est nul et b non nul, l'égalité est vérifiée car $d = 0$.
(3) PPCM $(ka ; kb) \times$ PGCD $(ka ; kb) = k^2 ab$.
Or, PGCD $(ka ; kb) = k$ PGCD $(a ; b)$ et PPCM $(a ; b) \times$ PPGCD $(a ; b) = ab$.
PPCM $(ka ; kb) \times k \times$ PGCD $(a ; b) = k^2 \times$ PPCM $(a ; b) \times$ PGCD $(a ; b)$
d'où PPCM $(ka ; kb) = k \times$ PPCM $(a ; b)$.

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

Savoir-faire 12

➤ Voir l'exercice 42

Déterminer le PPCM de deux entiers

1. Déterminer le PPCM de 630 et de 588.

2. Déterminer le PPCM de 14 560 et 6 272.

Méthode
Pour déterminer le PPCM de deux entiers, on peut soit utiliser leur décomposition en facteurs premiers (si les nombres ne sont pas trop grands), soit calculer d'abord leur PGCD.

Solution

1. 630 et 588 n'étant pas trop grands, on peut utiliser la méthode de décomposition en facteurs premiers.
$630 = 2 \times 3^2 \times 5 \times 7$ et $588 = 2^2 \times 3 \times 7^2$, d'où PPCM $(630 ; 588) = 2^2 \times 3^2 \times 5 \times 7^2 = 8\,820$.

2. Dans ce cas, on peut déterminer d'abord le PGCD des deux nombres avec l'algorithme d'Euclide :
$14\,560 = 6\,272 \times 2 + 2\,016$; $6\,272 = 2\,016 \times 3 + 224$; $2\,016 = 224 \times 9$.
Le dernier reste non nul de la suite des divisions est 224, donc le PGCD de ces nombres est 224.
Soit m le PPCM de ces deux nombres.
Alors $m \times 224 = 14\,560 \times 6\,272 = 91\,884\,800$. D'où : $m = \dfrac{91\,884\,800}{224} = 407\,680$.
Remarque : On peut aussi utiliser la fonction *lcm* de la calculatrice.

Savoir-faire 13

➤ Voir l'exercice 97

Résoudre une équation avec le PPCM

Énoncé 1 Déterminer deux entiers naturels connaissant leur produit 1 792 et leur PPCM 224.

Solution

Soit a et b les entiers naturels cherchés. On a ainsi : $ab = 1\,792$.
Soit d le PGCD de a et b. La relation entre le PGCD et le PPCM permet d'écrire :
PGCD $(a ; b) \times$ PPCM $(a ; b) = ab$ soit $224d = 1\,792$.
On peut donc déterminer le PGCD de a et de b : $d = \dfrac{1\,792}{224} = 8$.
Il existe deux entiers a' et b' premiers entre eux tels que $a = 8a'$ et $b = 8b'$.
Alors, $ab = 64a'b'$, d'où $a'b' = 28 = 2^2 \times 7$.
On traite alors tous les cas où a' et b' prennent les valeurs des diviseurs positifs de 28, en étant premiers entre eux.

a'	b'	a	b
1	28	$8 \times 1 = 8$	$28 \times 8 = 224$
4	7	$4 \times 8 = 32$	$7 \times 8 = 56$
28	1	224	8
7	4	56	32

Les solutions sont les couples (8 ; 224), (32 ; 56), (224 ; 8) et (56 ; 32).

Méthode
Pour résoudre une équation faisant intervenir m, PPCM de a et b, et d, PGCD de a et b, on utilise les relations $md = ab$, $a = da'$ et $b = db'$.

Énoncé 2 Soit d et m le PGCD et le PPCM de deux entiers naturels a et b. Déterminer a et b tels que l'on ait : $m - 2d = 11$.

Solution

Soit a' et b' les entiers naturels premiers entre eux tels que $a = da'$ et $b = db'$.
Comme $md = ab$, on a : $md = d^2a'b'$, soit $m = da'b'$, car le PGCD d n'est pas nul.
La relation donnée s'écrit : $da'b' - 2d = 11$, soit $d(a'b' - 2) = 11$.
Ainsi, d divise 11, et d est positif, donc $d = 11$ ou $d = 1$.
Si $d = 11$, alors $a'b' - 2 = 1$, soit $a'b' = 3$. On en déduit que $(a' ; b')$ est égal à (1 ; 3) ou (3 ; 1).
D'où : $(a ; b)$ vaut (11 ; 33) ou (33 ; 11).
Si $d = 1$, alors $a'b' - 2 = 11$, soit $a'b' = 13$. On en déduit que $(a' ; b')$ est égal à (13 ; 1) ou (1 ; 13).
D'où : $(a ; b)$ vaut (13 ; 1) ou (1 ; 13).
Il y a quatre couples solutions : (11 ; 33), (33 ; 11), (13 ; 1) et (1 ; 13).

Cours 6

Petit théorème de Fermat

Le théorème suivant est surnommé « petit » théorème de Fermat, par opposition au grand théorème de Fermat qui dit que l'équation $x^n + y^n = z^n$ n'a pas de solution en nombres entiers pour n entier, $n \geqslant 3$.

À noter

On peut aussi énoncer que $n^{p-1} - 1$ est divisible par p.

Petit théorème de Fermat Soit n un entier.
Si p est un nombre premier ne divisant pas n, alors $n^{p-1} \equiv 1\ (p)$.

On peut aussi écrire que $n^{p-1} - 1 \equiv 0\ (p)$.

Démonstration p est un nombre premier, donc il est premier avec les entiers $1, 2, \ldots, p-1$ qui lui sont inférieurs.
Il est donc aussi premier avec leur produit $P = 1 \times 2 \times \ldots \times (p-1)$.
Pour k entier tel que $1 \leqslant k \leqslant p-1$, on appelle r_k le reste de la division euclidienne de kn par p.
Ce reste est non nul, puisque n n'est pas divisible par p.
Soit k et k' des entiers compris entre 1 et $p-1$ tels que $k < k'$.
Les restes r_k et $r_{k'}$ associés à k et k' sont distincts.
On raisonne par l'absurde.
Si $r_k = r_{k'}$, alors, puisque $r_k \equiv kn\ (p)$ et $r_{k'} \equiv k'n\ (p)$, on en déduit :
$$k'n - kn \equiv 0\ (p),$$
ce qui signifie que $(k'-k)n$ est un multiple de p.
Or, n n'est pas un multiple de p, et $1 \leqslant k' - k \leqslant p-1$. Il y a donc une contradiction.
Ainsi les restes r_k sont tous distincts et prennent les valeurs $1, 2, \ldots, p-1$.
On a alors : $r_1 \times r_2 \times \ldots \times r_{p-1} = 1 \times 2 \times \ldots \times (p-1)$.
Puisque, pour tout k, $r_k \equiv kn\ (p)$, on obtient :
$$1 \times 2 \times \ldots \times (p-1)\, n^{p-1} \equiv r_1 \times r_2 \times \ldots \times r_{p-1}\ (p)$$
$$1 \times 2 \times \ldots \times (p-1)\, n^{p-1} \equiv 1 \times 2 \times \ldots \times (p-1)\ (p)$$
D'où : $1 \times 2 \times \ldots \times (p-1)\,(n^{p-1} - 1) \equiv 0\ (p)$.
Ainsi p divise $1 \times 2 \times \ldots \times (p-1)\,(n^{p-1} - 1)$ et il est premier avec $1 \times 2 \times \ldots \times (p-1)$ donc, d'après le théorème de Gauss, il divise $n^{p-1} - 1$.
On conclut : $n^{p-1} - 1 \equiv 0\ (p)$, donc $n^{p-1} \equiv 1\ (p)$.

Point Histoire

Pierre de Fermat (1601–1665) a énoncé de très nombreux résultats d'arithmétique. Son « grand » théorème a résisté plus de trois siècles aux efforts des mathématiciens jusqu'à sa démonstration par **Wiles** en 1994.

Exemples :

- 5 ne divise pas 18, et 5 est premier. Donc $18^4 \equiv 1\ (5)$.
- 7 est premier, d'où $n^6 \equiv 1\ (7)$ pour tous les entiers n tels que 7 ne divise pas n, c'est-à-dire pour tous les entiers n non multiples de 7.
  Lorsque n est multiple de 7, on a $7^6 \equiv 0\ (7)$, et plus généralement $(7k)^6 \equiv 0\ (7)$, pour tout entier k.
- $7^{10} \equiv 1\ (11)$, car 11 est premier et ne divise pas 7.
  On a : $7^{2\,012} = (7^{10})^{201} \times 7^2$.
  Puisque $(7^{10})^{201} \equiv 1\ (11)$ et $7^2 \equiv 5\ (11)$, alors $7^{2\,012} \equiv 5\ (11)$: le reste de la division euclidienne de $7^{2\,012}$ par 11 est 5.

À noter

On peut aussi énoncer que $n^p - n$ est divisible par p pour tout entier n.

Corollaire Si p est un nombre premier et n un entier, alors $n^p \equiv n\ (p)$.

Démonstration On a : $n^p - n = n(n^{p-1} - 1)$.
Si n est divisible par p, alors $n^p - n$ est un multiple de p et $n^p - n \equiv 0\ (p)$.
Si n n'est pas divisible par p, d'après le petit théorème de Fermat, $n^{p-1} - 1$ est un multiple de p et par suite $n^p - n \equiv 0\ (p)$.
On a alors $n^p \equiv n\ (p)$.

Exemple : Pour montrer que $n^4 - n$ est un multiple de 5 pour toute valeur entière de n, on peut utiliser le corollaire du petit théorème de Fermat.
En effet, 5 étant un nombre premier ; on a alors pour tout entier n : $n^4 \equiv n\ (5)$, et par suite $n^4 - n \equiv 0\ (5)$.
$n^4 - n$ est bien un multiple de 5 pour tout entier n.

Savoir-faire 14

➤ Voir l'exercice 107

Montrer une divisibilité avec le petit théorème de Fermat

Montrer que, pour tout entier n, $n^{11} - n$ est divisible par 33.

Méthode
Dans un problème de divisibilité par le nombre premier p, on peut faire apparaître n^p.

Solution

11 étant un nombre premier, d'après le corollaire du petit théorème de Fermat, on a $n^{11} \equiv n\ (11)$.
$n^{11} - n \equiv 0\ (11)$, d'où $n^{11} - n$ est divisible par 11.
Comme 3 est un nombre premier, on a aussi $n^3 \equiv n\ (3)$.
$n^{11} = (n^3)^3 \times n^2$. On obtient $n^{11} \equiv n^3\ (3)$, et donc $n^{11} \equiv n\ (3)$: $n^{11} - n$ est aussi divisible par 3.
On en déduit que $n^{11} - n$ est divisible par 11 et par 3, qui sont des nombres premiers entre eux.
Le corollaire du théorème de Gauss assure que, pour tout entier n, $n^{11} - n$ est divisible par 33 (car $11 \times 3 = 33$).

Savoir-faire 15

➤ Voir l'exercice 151

Utiliser le petit théorème de Fermat pour un problème de cryptographie

On affecte à chaque entier compris entre 0 et 28 une lettre de l'alphabet ou un autre symbole (on affecte A à 0, B à 1, ..., Z à 25, α à 26, β à 27, γ à 28), puis on fait subir à chacun de ces entiers x la transformation f suivante : $x \mapsto y$, où y est le reste dans la division euclidienne par 29 de x^3.
On note $E = \{0 ; 1 ; 2 ; \ldots ; 28\}$.

1. **Chiffrer le mot MER.**

2. **Montrer que 3 et 28 sont premiers entre eux et écrire une relation de Bézout pour les entiers 3 et 28.**

3. **Montrer que si $f(x) = f(x')$, alors $x = x'$.**
En déduire que deux éléments différents de E ont deux images différentes par f.

4. **Soit x et y éléments de E tels que $y \equiv x^3\ (29)$. Montrer que $y^{19} \equiv x\ (29)$.**

5. **Décoder alors le mot INDICE.**

Conseil
Pour calculer à quoi est congru 13^{19} modulo 29, calculer d'abord à quoi sont congrus 13^{10} et 13^9 modulo 29, puis faire le produit.

Solution

1. MER se chiffre en : 12, 4, 17.
$f(12) = 17$ car $12^3 \equiv 17\ (29)$; $f(4) = 6$ car $43 \equiv 6\ (29)$ et $f(17) = 12$ car $173 \equiv 12\ (29)$.
17 correspond à R, 6 à G et 12 à M, donc le mot MER se code en RGM.

2. 3 est un nombre premier qui ne divise pas 28, donc 3 et 28 sont premiers entre eux.
On peut écrire : $3 \times 19 - 28 \times 2 = 1$.

3. Soit x et x' deux éléments de E tels que $f(x) = f(x')$.
Alors, on a : $x^3 \equiv x'^3\ (29)$, d'où : $(x^3)^{19} \equiv (x'^3)^{19}\ (29)$ et $x^{3\times19} \equiv x'^{3\times19}\ (29)$.
L'égalité de la question **2.** s'écrit : $3 \times 19 = 28 \times 2 + 1$.
Ceci donne $x^{28\times2+1} \equiv x'^{28\times2+1}\ (29)$ et $(x^{28})^2 x \equiv (x'^{28})^2 x'\ (29)$.
29 est premier et ne divise pas x et x', car x et x' sont strictement inférieurs à 29 : le petit théorème de Fermat montre alors que $x^{28} \equiv 1\ (29)$ et $x'^{28} \equiv 1\ (29)$.
On en déduit : $(x^{28})^2 \equiv 1\ (29)$ et $(x'^{28})^2 \equiv 1\ (29)$.
D'où : $x \equiv x'\ (29)$, et enfin $x = x'$ car x et x' sont compris entre 0 et 28.
Par contraposition, on en déduit que, si x est différent de x', leurs images $f(x)$ et $f(x')$ sont différentes.

4. Si $y \equiv x^3\ (29)$, alors $y^{19} \equiv (x^3)^{19}\ (29)$, d'où $y^{19} \equiv x\ (29)$ car on a vu que $x^{3\times19} \equiv x\ (29)$.

5. INDICE se chiffre en 8, 13, 3, 8, 3, 4. On calcule alors : $8^{19} \equiv 2\ (29)$,
$13^{19} \equiv 6\ (29)$, $3^{19} \equiv 18\ (29)$ et $4^{19} \equiv 9\ (29)$. On peut alors décoder le mot INDICE : on obtient CGSCSJ.

Exercices

Les exercices dont les numéros sont sur fond blanc sont corrigés à la fin du manuel.

POUR DÉMARRER

Diviseurs communs

Dans les exercices 1 à 6, on note $D(a)$ l'ensemble des diviseurs positifs de l'entier a.

1 Simplifier le plus possible la fraction $\frac{630}{546}$.
Que représente l'entier par lequel on a simplifié les deux termes de la fraction ?

2 1. Effectuer la division euclidienne de 456 par 58.
2. En déduire que les diviseurs communs de 456 et de 58 sont aussi des diviseurs de 50.

3 1. Vérifier que $123\,456 = 789 \times 156 + 372$.
2. Montrer que les diviseurs communs de 123 456 et de 789 sont aussi des diviseurs de 372.

4 Soit d un entier et soit a, b et c des entiers tels que :
$a = b + c$.
1. Montrer que si d divise a et b, alors d divise b et c.
2. Montrer que si d divise b et c, alors d divise a et b.
3. Quel résultat peut-on alors énoncer ?

5 1. Déterminer les diviseurs de 145 et les diviseurs de 30.
2. En déduire les diviseurs communs de 145 et de 30.
3. En remarquant que $870 = 145 \times 6$ et $180 = 30 \times 6$, déterminer les diviseurs communs de 870 et de 180.

6 Déterminer l'ensemble des diviseurs communs positifs de :
a. 56 et 72 ;
b. $56n$ et $72n$, où n est un entier naturel premier différent de 2.

Plus grand commun diviseur

7 1. Décomposer 140 et 154 en facteurs premiers.
2. En déduire le PGCD de 140 et de 154.

→ Pour vous aider Savoir-faire 1, p. 47

8 Déterminer le PGCD de 7 980 et 19 800 après avoir décomposé ces entiers en facteurs premiers.

9 Déterminer sans calcul le PGCD des nombres p et q suivants :
a. $p = 32 \times 10$ et $q = 32 \times 11$
b. $p = 3 \times 5 \times 17 \times 23$ et $q = 5 \times 23 \times 37$
c. $p = 15 \times (-12)$ et $q = 4 \times 11 \times (-3)$
d. $p = 7^3 \times 5^2$ et $q = 5^4 \times 7^2$

10 Déterminer l'ensemble des diviseurs communs de 656 et 321.

11 Déterminer le PGCD de 151 782 et de 698 394.
En déduire la forme simplifiée de la fraction $\frac{151\,782}{698\,394}$.

12 Déterminer, selon les valeurs de l'entier n, le PGCD de $n + 2$ et 2.

13 Déterminer, selon les valeurs de l'entier n, le PGCD de $n + 1$ et 3.

14 Déterminer, selon les valeurs de l'entier n, le PGCD de $2n + 1$ et de 5.

15 Soit n un entier naturel et $A = 2n$.
1. Quelles sont les valeurs possibles du PGCD de A et de 3 ?
2. Déterminer le PGCD de A et de 3 en fonction des valeurs prises par n.

16 Soit n un entier, $A = 3n + 5$ et $B = 2n - 1$.
1. Montrer que $2A - 3B = 13$.
2. En déduire les valeurs possibles du PGCD de A et B.

17 Soit a et b deux entiers naturels.
Le PGCD de a et de b est 9 et $a + b = 45$.
Déterminer les valeurs possibles de a et de b.

18 Soit a et b deux entiers naturels.
Le PGCD de a et de b est 26 et $a \times b = 6\,084$.
Déterminer les valeurs possibles de a et de b.

19 Le PGCD de deux entiers naturels non nuls est 12 et le plus grand de ces deux entiers est 240.
Déterminer les valeurs possibles de l'autre entier.

20 Déterminer tous les entiers naturels n tels que :
$n < 315$ et $\text{PGCD}(n ; 315) = 35$.

21 Soit p un entier naturel non nul tel que $252 \equiv 10\ (p)$ et $547 \equiv 8\ (p)$. Déterminer p.

22 Soit p un entier naturel non nul tel que $1\,234 \equiv 2\ (p)$ et $5\,678 \equiv 22\ (p)$. Déterminer p.

Entiers premiers entre eux

23 Dire si les nombres suivants sont ou non premiers entre eux :
a. 855 et 57
b. 171 et 99
c. 332 647 et 38 160
d. 1 259 et 535 075

24 Dans chaque cas, dire sans calcul si les entiers p et q sont premiers entre eux :
a. $p = 55 \times 4 \times 3$ et $q = 7 \times 9 \times 13$
b. $p = 3^4 \times 11^2$ et $q = 5^4 \times 12^2$
c. $p = 27 \times 5$ et $q = 34 \times 14$
d. $p = 12$ et $q = 13$

25 1. Soit n un entier.
Montrer que si $7n$ est divisible par 2, alors n est pair.
2. Montrer que si $7n$ est divisible par 3, alors n est un multiple de 3.

26 Déterminer le plus petit entier naturel strictement supérieur à 7 qui donne le même reste 7 quand on le divise par 52 et par 64.

27 Soit P le produit de trois entiers consécutifs.

1. Montrer P est divisible par 2 et par 3
2. En déduire que P est divisible par 6.

28 Logique

1. Soit n et m deux entiers. Montrer que si m est divisible par 5 et n par 3, alors le produit $m \times n$ est divisible par 15.
2. Étudier la réciproque de cette proposition.

29 On considère l'ensemble E des entiers naturels x inférieurs à 200 tels que $x \equiv 2\ (7)$ et $x \equiv 2\ (3)$.

1. Montrer que $x - 2$ est un multiple de 21.
2. En déduire les éléments de E.

30 Soit m et n deux entiers naturels non nuls tels que :
$$\text{PGCD}(m\,;n) = 7 \quad \text{et} \quad m \times n = 588.$$

1. Justifier l'existence de deux entiers m' et n' premiers entre eux et vérifiant $m' \times n' = 12$.
2. Quelles sont les valeurs possibles de m' et n' ?
En déduire les valeurs possibles de m et n.

31 Trouver les entiers m et n tels que :
$$\text{PGCD}(m\,;n) = 5 \quad \text{et} \quad \frac{m}{n} = \frac{4}{3}.$$

32 Déterminer deux entiers naturels x et y tels que :
a. $\text{PGCD}(x\,;y) = 3$ et $x + y = 27$
b. $\text{PGCD}(x\,;y) = 5$ et $xy = 50$
c. $\text{PGCD}(x\,;y) = 4$ et $x^2 - y^2 = 112$

Théorème de Bézout

33 Déterminer une solution particulière de l'équation $12x + 7y = 1$, où x et y sont des entiers.

34 Déterminer une solution particulière de l'équation $10x - 25y = 5$, où x et y sont des entiers.

35 1. Déterminer une solution particulière de l'équation $2x - 3y = 1$, où x et y sont des entiers.
2. Résoudre l'équation $2x - 3y = 1$, où x et y sont des entiers.

36 1. Déterminer une solution particulière de l'équation $21x + 13y = 1$, où x et y sont des entiers.
2. Résoudre l'équation $21x + 13y = 1$, où x et y sont des entiers.

37 1. Déterminer une solution particulière de l'équation $2x + 5y = 3$, où x et y sont des entiers.
2. Résoudre l'équation $2x + 5y = 3$ où x et y sont des entiers.

38 1. Déterminer le PGCD de 18 et de 27.
2. Déterminer les couples $(x\,;y)$ d'entiers solutions de l'équation :
$$18(5 - x) = 27(y + 3) \quad \textbf{(E)}.$$
3. Existe-t-il des couples de nombres entiers naturels solutions de **(E)** ?

39 1. Déterminer le PGCD de 2 045 et 64.
2. En déduire que l'équation :
$$2\,045x - 64y = 1 \quad \textbf{(1)}$$
d'inconnues les entiers x et y a au moins une solution.
Trouver une solution particulière de l'équation **(1)**.
3. Résoudre l'équation **(1)**.
4. En déduire les solutions de l'équation :
$$2\,045x - 64y = 7 \quad \textbf{(2)}.$$

40 1. Soit n un entier naturel, $A = 2n + 1$ et $B = n$.
Montrer que $A - 2B = 1$.
2. En déduire que A et B sont premiers entre eux.

41 1. Soit n un entier naturel, $A = 2n + 3$ et $B = 3n + 4$.
Montrer que $3A - 2B = 1$.
2. En déduire que A et B sont premiers entre eux.

PPCM de deux entiers

42 Calculer le PPCM des nombres suivants :
a. 108 et 144 **b.** 128 et 230 **c.** 1 848 et 1 950
d. 480 et 735 **e.** 876 et 1 028

→ Pour vous aider Savoir-faire 12, p. 59

43 Sans calcul, déterminer le PPCM des nombres entiers p et q suivants :
a. $p = 11$ et $q = 25$
b. $p = 2^2 \times 5^3 \times 7$ et $q = 4 \times 25 \times 49$
c. $p = 8 \times 13$ et $q = 8 \times 14$
d. $p = 12\,000$ et $q = 5\,000$

44 Déterminer le PGCD de 35 et 24.
En déduire le PPCM de 35 et 24.

45 Déterminer le PGCD de 24 et 36.
En déduire le PPCM de 24 et 36.

46 Déterminer tous les entiers naturels n tels que le PPCM de n et de 25 soit 75.

47 Déterminer tous les couples d'entiers naturels $(x\,;y)$ tels que $\text{PPCM}(x\,;y) = 130$ et $xy = 650$.

Petit théorème de Fermat

48 1. Montrer que 113 est un nombre premier.
2. Déterminer le reste de la division euclidienne de 7^{112} par 113.

49 Déterminer le reste de la division euclidienne de 123^{540} par 541.

50 1. Montrer que, pour tout n entier non nul, $n^{307} \equiv n\ (307)$.
2. À quelle condition sur n a-t-on $n^{306} \equiv 1\ (307)$?

51 1. Quels sont les entiers n qui vérifient $n^{10} \equiv 1\ (11)$?
2. Quels sont les entiers n qui vérifient $n^6 \equiv 1\ (7)$?
3. Quels sont les entiers n qui vérifient $n^{60} \equiv 1\ (77)$?

POUR S'ENTRAÎNER

PGCD de deux entiers

52 Déterminer, selon les valeurs de l'entier n, le PGCD de $A = 5n + 3$ et de $B = n - 4$.

→ Pour vous aider Savoir-faire 2, p. 47

53 Déterminer, selon les valeurs de l'entier n, le PGCD de $A = 4n + 19$ et de $B = 11 + 2n$.

→ Pour vous aider Savoir-faire 2, p. 47

54 Soit a et b deux entiers naturels non nuls.
Soit $x = 2a - 5b$ et $y = a - 2b$. Montrer que :
$$\text{PGCD}(x ; y) = \text{PGCD}(a ; b).$$

→ Pour vous aider Savoir-faire 3, p. 47

55 Soit a et b deux entiers naturels non nuls.
Soit $x = 7a + 5b$ et $y = 3a + 2b$. Montrer que :
$$\text{PGCD}(x ; y) = \text{PGCD}(a ; b).$$

→ Pour vous aider Savoir-faire 3, p. 47

56 ALGO

1. Déterminer le PGCD des nombres suivants à l'aide de l'algorithme d'Euclide :

a. 26 et 65 **b.** 84 et 27 **c.** 300 et 120
d. 6 652 et 924 **e.** 27 634 et 6 551

2. En déduire une écriture sous forme irréductible des fractions suivantes :
$$\frac{65}{26} ; \frac{84}{27} ; \frac{300}{120} ; \frac{6652}{924} ; \frac{27634}{6551}.$$

→ Pour vous aider Savoir-faire 4, p. 49

57 Le PGCD des entiers a et b est égal à d.
Déterminer le PGCD des entiers suivants :
a. a et $a + b$ **b.** $15a + 4b$ et $11a + 3b$

58 Soit n un entier naturel non nul, A l'entier $3n + 1$ et B l'entier $5n - 1$.

1. Montrer que le PGCD de A et B est un diviseur de 8.

2. Pour quelles valeurs de n ce PGCD est-il égal à 8 ?

59 TRAVAIL EN AUTONOMIE

Énoncé

Soit n un entier naturel. On définit :
$$A = n^2 + 7n + 6 \text{ et } B = n^2 + 5n - 6.$$
Après avoir factorisé A et B, déterminer le PGCD de A et B en fonction de n.

Solution

$A = (n + 6)(n + 1)$ et $B = (n + 6)(n - 1)$.
$\text{PGCD}(A ; B) = (n + 6)\,\text{PGCD}(n + 1 ; n - 1)$.
Soit $d = \text{PGCD}(n + 1 ; n - 1)$. d divise $n + 1$ et d divise $n - 1$, donc d divise $n + 1 - (n - 1)$, c'est-à-dire 2.
Comme d divise 2, alors d est égal à 1 ou 2.
Si $d = 2$, alors $n + 1$ et $n - 1$ sont pairs, donc n est impair.
Si $d = 1$, alors n est pair.
Donc, si n est pair : $\text{PGCD}(A ; B) = n + 6$.
Si n est impair : $\text{PGCD}(A ; B) = 2(n + 6)$.

60 Avec un tableur TICE

Soit n un entier naturel. On pose :
$$P(n) = 2n^2 - 10n + 3 \text{ et } Q(n) = n^2 - 5n.$$
À l'aide d'un tableur, conjecturer le PGCD de $P(n)$ et $Q(n)$ selon les valeurs de n. Démontrer cette conjecture.

AIDE : Utiliser la fonction PGCD du tableur.

61 On veut déterminer deux entiers naturels non nuls a et b inférieurs ou égaux à 150 tels que :
$$a + b = 210 \text{ et } \text{PGCD}(a ; b) = 15.$$

1. Montrer qu'il existe deux nombres entiers naturels premiers entre eux p et q tels que :
$$0 < p \leqslant 10,\ 0 < q \leqslant 10,\ a = 15p \text{ et } b = 15q.$$

2. Montrer que p et q vérifient $p + q = 14$.

3. Déterminer les couples $(a ; b)$ solutions du problème posé.

62 ALGO TICE

Programmer l'algorithme d'Euclide avec le logiciel AlgoBox ou le logiciel Xcas.

→ Pour vous aider Savoir-faire 5, p. 49

63 Algorithme d'Euclide étendu ALGO

On applique l'algorithme d'Euclide à un couple d'entiers $(a ; b)$.

Dividende	Diviseur	Reste	Quotient	u	v
				$u_0 = 1$	$v_0 = 0$
				$u_1 = 0$	$v_1 = 1$
a	b	r_1	q_1	u_2	v_2
b	r_1	r_2	q_2	u_3	v_3
r_1	r_2	r_3	q_3	u_4	v_4
....	...	...	...		

1. a. Vérifier que $a = u_0 a + v_0 b$ et $b = u_1 a + v_1 b$.
b. On veut définir u_2 et v_2 tels que $r_1 = u_2 a + v_2 b$.
Exprimer u_2 en fonction de u_0, de q_1 et de u_1, puis v_2 en fonction de v_0, q_1 et v_1.
c. On veut définir u_3 et v_3 tels que $r_2 = u_3 a + v_3 b$.
Exprimer u_3 en fonction de u_1, de q_2 et de u_2, puis v_3 en fonction de v_1, q_2 et v_2.

2. On présente l'algorithme d'Euclide de la façon suivante, où la colonne C1 contient les dividendes des divisions successives, la colonne C2 contient les diviseurs, la colonne C3 contient les restes et la colonne C4 contient les quotients.

C1	C2	C3	C4	u	v
				$u_0 = 1$	$v_0 = 0$
				$u_1 = 0$	$v_1 = 1$
a	b	r_1	q_1	$u_2 = u_0 - q_1 u_1$	$v_2 = v_0 - q_1 v_1$
b	r_1	r_2	q_2	$u_3 = u_1 - q_2 u_2$	$v_3 = v_1 - q_2 v_2$
r_1	r_2	r_3	q_3	$u_4 = u_2 - q_3 u_3$	$v_4 = v_2 - q_3 v_3$
...	...	...	...	...	...

a. Expliquer pourquoi la dernière étape fournit le PGCD de a et de b et les coefficients u et v tels que $au + bv = \text{PGCD}(a ; b)$.
b. Calculer les éléments de ce tableau avec :
$a = 1\,694$ et $b = 319$.

64 Logique

Soit m et n deux entiers naturels non nuls.

1. Montrer que si d est un diviseur commun de m et n, alors d est aussi un diviseur commun de $M = 3n + 4m$ et $N = 5n + 7m$.

2. Réciproquement, montrer que si d' est un diviseur de M et N, alors d' est aussi un diviseur de m et n.

3. En déduire que $\text{PGCD}(m ; n) = \text{PGCD}(M ; N)$.

VRAI – FAUX

Pour les exercices **65** à **68**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

65 $\text{PGCD}(2n + 2 ; 4n + 2) = 2$ pour tout entier n.

66 Si a et b sont deux entiers tels que $4a - 5b = 9$, alors $\text{PGCD}(a ; b) = 9$.

67 Soit n un entier, alors le PGCD de $2n + 5$ et $n + 1$ est un diviseur de 4.

68 Il existe deux entiers naturels x et y tels que :
$x + y = 450$ et $\text{PGCD}(x ; y) = 6$.

Nombres premiers entre eux Théorème de Gauss

69 Quel est le PGCD de deux entiers pairs consécutifs ?

→ Pour vous aider Savoir-faire 7, p. 53

70 Soit n un entier naturel non nul.
Montrer que la fraction $F = \dfrac{3n+1}{n}$ est irréductible.

→ Pour vous aider Savoir-faire 7, p. 53

71 Soit n un entier naturel non nul. Dire si les entiers p et q suivants sont premiers entre eux pour toute valeur de n.

1. $p = 12n$ et $q = 13n$
2. $p = 12n$ et $q = 13(n + 1)$
3. $p = n + 1$ et $q = 2n + 3$
4. $p = (n + 1)^2$ et $q = n^2$

72 Logique

1. Montrer que si a et b sont premiers entre eux, alors ab et $a + b$ sont premiers entre eux.

2. Étudier la réciproque de cet énoncé.

73 Logique

1. Montrer que si les entiers a et b^2 sont premiers entre eux, alors a et b sont premiers entre eux.

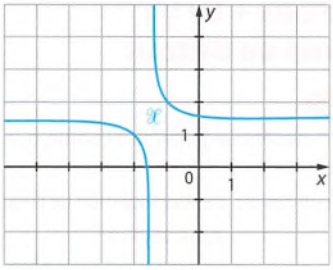
2. Étudier la réciproque de cet énoncé.

74 Montrer que si x et y sont deux entiers premiers entre eux, il en est de même des entiers $3x + 4y$ et $4x + 5y$.

75 Logique

Soit m et n deux entiers non nuls. On pose :
$M = 4m + 3n$ et $N = 5m + 4n$.
Démontrer que la fraction $\dfrac{m}{n}$ est irréductible si, et seulement si, la fraction $\dfrac{M}{N}$ est irréductible.

76 Soit $\mathcal{H}$ la représentation graphique dans un repère orthogonal de la fonction h définie pour tout $x \neq -\dfrac{3}{2}$ par :
$$h(x) = \frac{3x + 5}{2x + 3}.$$
Montrer que $\mathcal{H}$ a des points à coordonnées entières. Lesquels ?



77 1. Soit n un entier naturel strictement supérieur à 1. Montrer que n et $2n + 1$ sont premiers entre eux.

2. En déduire le PGCD de :
$n^2 - n$ et $2n^2 - n - 1$.

78 Théorème de Bézout ROC

1. Démontrer que s'il existe deux entiers relatifs u et v tel que $au + bv = 1$, alors les nombres entiers a et b sont premiers entre eux.

2. Soit m un entier naturel non nul.
Montrer que $5m + 1$ et m sont premiers entre eux.

3. Soit p un entier naturel.
Montrer que $pm + 1$ et m sont premiers entre eux.

4. Soit q un entier naturel premier avec m.
Montrer que $pm + q$ et m sont premiers entre eux.

79 Avec un logiciel TICE

On considère les polynômes $P(x)$ et $Q(x)$ définis pour tout réel x par :
$P(x) = 5x^3 + 30x^2 + 55x + 30$ et $Q(x) = 3x^2 + 9x + 6$.

1. À l'aide d'un tableur, conjecturer le PGCD de $P(n)$ et de $Q(n)$ lorsque n est un multiple de 3.

2. Montrer que le PGCD de 3 et $5n + 15$ est 1 ou 3.

3. Montrer que le PGCD de 3 et $5n + 15$ est égal à 3 si, et seulement si, $n \equiv 0\ (3)$.

4. À l'aide d'un logiciel de calcul formel, factoriser $P(x)$ et $Q(x)$.

5. En déduire la démonstration de la conjecture émise à la question 1.

AIDE : question 1. Utiliser la fonction PGCD du tableur.

Exercices

VRAI – FAUX

Pour les exercices **80** à **82**, indiquer si les affirmations sont vraies ou fausses puis justifier.

80 Pour tout entier n, n et $2n+1$ sont premiers entre eux.

81 La fraction $\frac{n+3}{2n+1}$ est irréductible pour tout entier n.

82 Pour tout entier naturel n, les entiers $3n+1$ et 11 sont premiers entre eux.

Équation $ax + by = c$ Théorème de Bézout

83 ALGO

1. Montrer, en utilisant l'algorithme d'Euclide, que 32 et 15 sont premiers entre eux.

2. En déduire un couple d'entiers solution de l'équation :

$$32x + 15y = 1.$$

→ Pour vous aider Savoir-faire 8, p. 53

84 1. À l'aide de la table de la calculatrice, déterminer un couple d'entiers solution de l'équation :

$$5x + 7y = 1.$$

2. En déduire un couple solution des équations suivantes, où x et y sont des entiers :

$5x - 7y = 1$ (E_1) $\quad -5x + 7y = 1$ (E_2)

$-5x - 7y = 1$ (E_3) $\quad 5x + 7y = 2$ (E_4)

$5x + 7y = -10$ (E_5) $\quad 5x - 7y = -10$ (E_6)

→ Pour vous aider Savoir-faire 9, p. 53

85 Déterminer les entiers x et y tels que $11x = 8y$.

→ Pour vous aider Savoir-faire 10, p. 55

86 1. Montrer que (9 ; 2) est une solution de l'équation :

$$3x - 13y = 1 \quad \textbf{(E)}.$$

2. Résoudre **(E)**.

3. En déduire :

a. l'ensemble des entiers x tels que $3x \equiv 1\ (13)$;

b. l'ensemble des entiers y tels que $13y \equiv 2\ (3)$.

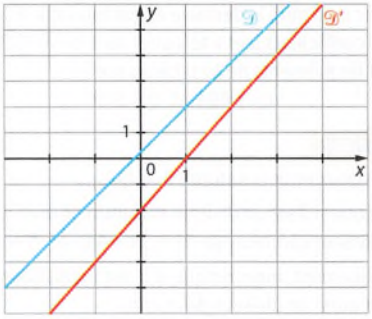
→ Pour vous aider Savoir-faire 10, p. 55

87 Démontrer que, quel que soit l'entier naturel n, l'entier $A = n^2(n^2 - 1)$ est divisible par 4, par 3 et par 12.

→ Pour vous aider Savoir-faire 11, p. 55

88 Trouver tous les entiers tels que les divisions euclidiennes de n par 11 et de n par 12 donnent le même reste égal à 5.

89 1. Dans le plan rapporté à un repère orthogonal, on appelle $\mathscr{D}$ la droite d'équation $-7x + 4y - 1 = 0$ et $\mathscr{D}'$ la droite d'équation $2x - y - 2 = 0$.
Déterminer deux points de $\mathscr{D}$ et deux points de $\mathscr{D}'$ à coordonnées entières.



2. Montrer que tous les points de $\mathscr{D}$ à coordonnées entières ont pour coordonnées $(1 + 4k ; 2 + 7k)$, où k est un entier.

3. Montrer que tous les points de $\mathscr{D}'$ à coordonnées entières ont pour coordonnées $(4 + k' ; 6 + 2k')$, où k' est un entier.

4. Résoudre le système d'équations suivant :

$$\begin{cases} 4k - k' = 3 \\ 7k - 2k' = 4 \end{cases}$$

5. En déduire qu'il existe un point d'intersection entre $\mathscr{D}$ et $\mathscr{D}'$ et que ce point a des coordonnées entières.

90 1. Justifier l'existence de couples d'entiers $(x ; y)$ solutions de l'équation **(1)** : $4x - 3y = 11$.

2. Déterminer tous les couples $(x ; y)$ d'entiers solutions de **(1)**.

3. Quelle est la valeur maximale d du PGCD des couples $(x ; y)$ ainsi obtenus ?

91 Théorème de Gauss ROC

1. En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

2. Déterminer, dans chaque cas, les entiers x et y qui vérifient les égalités suivantes :

a. $4x = 5y$ **b.** $44x = 55(y - 2)$ **c.** $44(x + 6) = 55(y - 2)$

92 Théorème de Bézout ROC

a et b sont deux entiers. Démontrer les équivalences ci-dessous.

1. Il existe un couple d'entiers $(u ; v)$ tel que $au + bv = 1$ si, et seulement si, a et b sont premiers entre eux.

2. L'équation $ax \equiv 1\ (b)$ admet des solutions dans $\mathbb{Z}$ si, et seulement si, a et b sont premiers entre eux.

93 1. Soit l'équation **(E)** $5x + 20y = n$ dont les inconnues sont les entiers naturels x, y et n.
À quelle condition **(E)** a-t-elle au moins une solution ?

2. Résoudre **(E)** lorsque $n = 165$.

3. On dispose de billets de 5 € et de billets de 20 €.
De combien de façons peut-on obtenir la somme de 165 € ?

VRAI – FAUX

Pour les exercices 94 à 96, indiquer si les affirmations sont vraies ou fausses, puis justifier.

94 L'équation $4x + 7y = 2$ a des solutions entières.

95 L'équation $3x \equiv 1\ (6)$ n'a pas de solution entière.

96 Soit x un entier, l'équation $3x \equiv 3\ (6)$ est équivalente à l'équation $x \equiv 1\ (2)$.

PPCM de deux entiers

97 Déterminer deux entiers naturels connaissant leur produit 720 et leur PPCM 120.

→ Pour vous aider Savoir-faire 13, p. 59

98 Soit n un entier naturel non nul.
Déterminer le PPCM des nombres p et q suivants :

a. $p = n + 1$ et $q = n$ **b.** $p = 2n + 2$ et $q = 4n + 2$
c. $p = n^2$ et $q = n^2 + 2n + 1$ **d.** $p = 4n^2$ et $q = 3n^2 + 3n$

99 Soit n un entier naturel tel que le PPCM de n et de 6 est 96. On appelle d le PGCD de n et de 6.

1. Déterminer les valeurs possibles de d.
2. Montrer que $n = 16d$.
3. En déduire les valeurs possibles de n.

100 **Relation entre PGCD et PPCM** ROC

1. Soit a et b deux entiers naturels, d leur PGCD et m leur PPCM. Montrer que $md = ab$.
2. Déterminer, en fonction de d, les couples $(a\,;b)$ d'entiers naturels dont le PGCD d et le PPCM m vérifient $m = 21d$.

101 **TRAVAIL EN AUTONOMIE**

Énoncé

1. Résoudre l'équation d'inconnue le réel X :
$$X^2 - 433X + 41\,616 = 0.$$
2. Déterminer deux entiers x et y premiers entre eux tels que :
$$x^2 + y^2 = 433 \text{ et } \text{PPCM}(x\,;y) = 204.$$

Solution

1. L'équation du second degré $X^2 - 433X + 41\,616 = 0$ admet deux solutions 144 et 289, obtenues en utilisant les formules de résolution ($\Delta = 21\,025 = 145^2$).
2. Comme x et y sont premiers entre eux, alors :
$$\text{PPCM}(x\,;y) = xy = 204.$$
On peut aussi écrire $x^2y^2 = 204^2 = 41\,616$.
x^2 et y^2 sont solutions de l'équation :
$$X^2 - 433X + 41\,616 = 0.$$
On en déduit que :
$$(x^2 = 144 \text{ et } y^2 = 289) \text{ ou } (x^2 = 289 \text{ et } y^2 = 144).$$
Les couples solutions sont donc :

x	12	12	−12	−12	17	17	−17	−17
y	17	−17	17	−17	12	−12	12	−12

102 ALGO

On donne l'algorithme suivant.

```
Saisir M, D
Q prend la valeur M/D
Pour K allant de 1 à Partie Entière de (√Q)
    Si Partie Entière de (Q/K) = Q/K
        Alors A prend la valeur Q/K
              B prend la valeur K
        Si PGCD (A ; B) = 1
            Alors X prend la valeur D × A
                  Y prend la valeur D × B
        Fin Si
    Fin Si
    Afficher X, Y
Fin Pour
```

1. Faire fonctionner cet algorithme avec $M = 30$ et $D = 3$, puis avec $M = 90$ et $D = 5$.
2. Que représentent alors les couples $(X\,;Y)$ obtenus ?
3. Qu'obtient-on si $D = 1$?
4. Programmer cet algorithme sur la calculatrice.

103 1. Soit a et b des entiers naturels non nuls tels que $\text{PGCD}(a + b\,;ab) = p$ où p est un nombre premier.
a. Démontrer que p divise a^2 et b^2.
b. En déduire que p divise a et b.
c. Démontrer que $\text{PGCD}(a\,;b) = p$.

2. Dans cette question, a et b désignent des entiers naturels non nuls tels que $a \leqslant b$.
a. Résoudre le système suivant :
$$\begin{cases} \text{PGCD}(a\,;b) = 5 \\ \text{PPCM}(a\,;b) = 170 \end{cases}$$
b. En déduire les solutions du système :
$$\begin{cases} \text{PGCD}(a+b\,;ab) = 5 \\ \text{PPCM}(a\,;b) = 170 \end{cases}$$

AIDE : question 1. a. On pourra écrire $a^2 = a(a + b) - ab$ et $b^2 = b(a + b) - ab$.

VRAI – FAUX

Pour les exercices 104 à 106, indiquer si les affirmations sont vraies ou fausses puis justifier.

104 Si x et y sont deux entiers premiers entre eux, alors le PPCM de x et y est xy.

105 Si a est un entier divisible par 7 *et* b un entier divisible par 5, alors le PPCM de a *et* b est divisible par 35.

106 Pour x et y entiers quelconques :
$$\text{PPCM}(x^2\,;y^2) = (\text{PPCM}(x\,;y))^2.$$

Exercices

Petit théorème de Fermat

107 1. Montrer que, pour tout entier n : $n^7 \equiv n\ (7)$.

2. Montrer que, pour tout entier n : $n^7 \equiv n\ (2)$.

3. Montrer que, pour tout entier n, $n^7 - n$ est divisible par 14.

→ Pour vous aider Savoir-faire 14, p. 61

108 Soit n un nombre entier et $A = n^5 - n$.

1. Montrer que, pour tout entier n, A est divisible par 5.

2. En utilisant les congruences modulo 3, montrer que A est divisible par 3.

3. En déduire que A est divisible par 15.

109 **TRAVAIL EN AUTONOMIE**

Énoncé

On considère la suite (U_n) d'entiers naturels définie par $3U_n = 10^{n+1} - 7$ pour tout entier naturel n.

1. Démontrer l'égalité $10^{16} \equiv 1\ (17)$.

2. En déduire que, pour tout entier naturel k, U_{16k+8} est divisible par 17.

Solution

1. 10 n'est pas divisible par 17 et 17 est un nombre premier donc, d'après le petit théorème de Fermat : $10^{16} \equiv 1\ (17)$.

2. $3U_{16k+8} = 10^{16k+9} - 7$.
$10^{16k+9} = (10^{16})^k \times 10^9$, $(10^{16})^k \equiv 1\ (17)$ et $10^9 \equiv 7\ (17)$,
d'où $3U_{16k+8} \equiv 0\ (17)$.
$3U_{16k+8}$ est donc divisible par 17.
Comme 3 et 17 sont premiers entre eux, U_{16k+8} est divisible par 17, pour tout entier naturel k.

110 Soit a un nombre entier.
On cherche le reste de la division euclidienne de a^6 par 7 suivant le reste de la division euclidienne de a par 7.

1. Recopier et compléter le tableau suivant :

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

2. Expliquer les résultats obtenus.

3. Déterminer le reste de la division euclidienne par 7 de $2\,012^{2\,012}$ et de $2\,016^{2\,016}$.

111 **Corollaire du théorème de Fermat** ROC

Prérequis : On suppose connu le petit théorème de Fermat.

1. Démontrer que, pour tout entier n, si p est premier alors $n^p \equiv n\ (p)$.

2. Soit n un entier naturel. On pose $A = n^7 - n$.
a. Montrer que A est divisible par 3 pour tout $n \in \mathbb{N}$.
b. Montrer que A est divisible par 7 pour tout $n \in \mathbb{N}$.
c. En déduire que A est divisible par 21 pour tout $n \in \mathbb{N}$.

112 Résoudre dans $\mathbb{Z}$ l'équation $x^5 \equiv x\ (30)$.

AIDE : Cela revient à déterminer les entiers tels que $x^5 - x$ soit divisible par 2, par 3, par 5. Utiliser le petit théorème de Fermat modulo 2, modulo 3 et modulo 5.

113 1. Décomposer 546 en produits de nombres premiers.

2. Démontrer que, pour tout entier x, on a :
a. $x^{13} \equiv x\ (13)$
b. $x^{13} \equiv x\ (7)$
c. $x^{13} \equiv x\ (3)$
d. $x^{13} \equiv x\ (2)$

3. En déduire que, pour tout entier x, $x^{13} \equiv x\ (546)$.

VRAI - FAUX

Pour les exercices 114 à 117, indiquer si les affirmations sont vraies ou fausses puis justifier.

114 $1\,234^{123} \equiv 1\ (123)$

115 Pour tout entier n, $n^{16} \equiv n\ (17)$.

116 Pour tout entier n, $n^{16} \equiv 1\ (17)$.

117 Pour tout entier n, $n^{17} \equiv n\ (17)$.

Top Chrono !

Résoudre chacun des exercices suivants en 10 minutes maximum.

118 Résoudre l'équation $5x + 9y = 7$, d'inconnues les entiers x et y.

119 Montrer que, pour tout entier n, les nombres $A = 4n + 5$ et $B = 3n + 4$ sont premiers entre eux.

120 Soit $A = 3n^2 + n$ et $B = 3n^2 + 4n + 1$, pour n entier naturel.

1. Montrer que $3n + 1$ divise A et B.

2. Est-ce que $3n + 1$ est le PGCD de A et de B ?

121 1. Montrer que 2 017 est un nombre premier.

2. Déterminer l'ensemble des couples $(a\ ;\ b)$ d'entiers naturels admettant 12 102 comme somme et 2 017 comme PGCD.

122 Déterminer tous les couples d'entiers naturels $(x\ ;\ y)$ tel que leur PGCD d et leur PPCM m vérifient $2m - 5d = 11$.

123 Soit n un entier naturel.
Démontrer que $n^5 - n$ est divisible par 10.

Pour faire le point

Choisir la (ou les) bonne(s) réponse(s).

Utiliser le PGCD de deux entiers

→ Pour vous aider Savoir-faire 2 et 7, p. 47 et 53

	A	B	C	D
124 Pour tout entier naturel n, le PGCD de $2n+1$ et n est	n	1	$n+1$	$2n+1$
125 Soit $F=\frac{n^2-1}{n}$, pour n entier non nul.	F est irréductible pour toute valeur de n.	F n'est jamais égal à un nombre entier.	F ne peut pas être égal à $\frac{3}{2}$.	Il existe des valeurs de n pour lesquelles F n'est pas irréductible.

Résoudre une équation du type $ax + by = c$

→ Pour vous aider Savoir-faire 8, 9 et 10, p. 53 et 55

126 L'équation $7x-6y=1$ d'inconnue le couple $(x\,;y)$ d'entiers	a pour seule solution $(1\,;1)$	n'a pas de solution	a pour solutions les couples $(6k+1\,;7k+1)$, avec k entier	a les mêmes solutions que le système $\begin{cases} x \equiv 1\,(6) \\ y \equiv 1\,(7) \end{cases}$
127 L'équation $ax+by=c$ (avec a, b et c entiers), d'inconnues les entiers x et y	n'a des solutions que pour $c=1$	a des solutions si, et seulement si, a et b sont premiers entre eux	n'a de solutions que si le PGCD de a et b divise c	n'a de solutions que si le PGCD de a et b est égal à c

Utiliser le PPCM de deux entiers

→ Pour vous aider Savoir-faire 13, p. 59

128 Soit x et y deux entiers dont le PGCD est d, alors	$\text{PPCM}(2x\,;3y)=\frac{6xy}{d}$	$\text{PPCM}(2x\,;3y)$ $=6\times\text{PPCM}(x\,;y)$	$\text{PPCM}(2x\,;3y)=6xy$	$d\times\text{PPCM}(2x\,;3y)=xy$
129 Soit x et y deux entiers non nuls dont le PGCD est d, alors	$\text{PPCM}(x\,;y)=\frac{xy}{d^2}$	$\text{PPCM}\left(\frac{x}{d}\,;\frac{y}{d}\right)$ $=\frac{1}{d^2}\text{PPCM}(x\,;y)$	$\text{PPCM}(dx\,;dy)=xy$	$\text{PPCM}(x\,;y)=dxy$

Déterminer une divisibilité

→ Pour vous aider Savoir-faire 11 et 14, p. 55 et 61

130 Si un entier a est divisible par b et c avec $\text{PGCD}(b\,;c)=6$, alors	a est divisible par bc	a est divisible par 6	a est divisible par $\frac{bc}{6}$	a est divisible par 36
131 Soit $N=25^{12}-1$.	N est divisible par 11.	N est divisible par 12.	N est divisible par 13.	N est divisible par 24.
132 Soit n un entier et $A=n(n^6-1)$.	A est divisible par 7 pour tout entier n.	A est divisible par 7 seulement pour n non multiple de 7.	A n'est jamais divisible par 7.	A est divisible par 7 seulement pour tout nombre premier n.

➤ **Voir les réponses, p. 140**

TP 1 Triplets pythagoriciens

TICE ALGO

→ Utiliser un tableur pour découvrir des triplets célèbres.

La propriété des triangles rectangles appelée propriété de Pythagore, était déjà connue des géomètres égyptiens de l'époque pharaonique. Ils l'appliquaient en architecture et en arpentage pour construire des angles droits.

On va s'intéresser aux triplets pythagoriciens, c'est-à-dire aux triplets d'entiers naturels non nuls $(a\,;b\,;c)$ vérifiant la relation de Pythagore $a^2+b^2=c^2$.
Cela revient à trouver les triangles rectangles dont tous les côtés sont des entiers.

A. Étude expérimentale

À l'aide d'un tableur, on va chercher les premiers triplets pythagoriciens.

1. Justifier que $\left(a\,;b\,;\sqrt{a^2+b^2}\right)$ est un triplet pythagoricien si, et seulement si, a, b et $\sqrt{a^2+b^2}$ sont des entiers.

2. Dans la première ligne et la première colonne d'une feuille de calcul d'un tableur, afficher les entiers naturels de 1 à 30.
Ils formeront les entiers a et b des triplets cherchés.

3. Entrer dans la cellule B2 une formule qui affiche 1 lorsqu'on obtient un triplet pythagoricien dont les deux premiers éléments sont a et b.

4. Combien a-t-on trouvé de tels triplets ?

B. Étude d'un cas particulier

On cherche les triangles rectangles pour lesquels l'hypoténuse c dépasse d'une unité seulement un des côtés b.

1. Montrer que $a^2=2b+1$.

2. En déduire que a est impair et peut s'écrire $a=2n+1$, avec n entier naturel.

3. Exprimer b et c en fonction de n et en déduire un triplet pythagoricien.

4. Montrer que si $(a\,;b\,;c)$ est un triplet pythagoricien, alors $(ka\,;kb\,;kc)$, avec k entier naturel non nul, est aussi un triplet pythagoricien. Donner alors quatre autres triplets pythagoriciens.

C. Étude mathématique

Soit $(a\,;b\,;c)$ un triplet pythagoricien et d le plus grand diviseur commun à a, b et c.
On note alors $a'=\frac{a}{d}$, $b'=\frac{b}{d}$ et $c'=\frac{c}{d}$.

1. Montrer que $(a'\,;b'\,;c')$ est un triplet pythagoricien.

2. Montrer, en raisonnant par l'absurde, que a' et b' ne peuvent pas être tous les deux pairs.

3. Montrer, en raisonnant par l'absurde, que a' et b' ne peuvent pas être tous les deux impairs.

4. On suppose que $a'=2n$ avec n entier naturel.
Montrer que $n^2=\alpha\times\beta$ avec $\alpha=\frac{c'-b'}{2}$ et $\beta=\frac{c'+b'}{2}$ où α et β sont des entiers.

5. Montrer que $b'=\beta-\alpha$, que $c'=\alpha+\beta$ et que α et β sont premiers entre eux. (On pourra raisonner par l'absurde en supposant que α et β ont un diviseur commun autre que 1.)

6. En déduire qu'il existe u et v entiers naturels non nuls tels que $\alpha=u^2$, $\beta=v^2$ et $u<v$.

7. Exprimer a, b et c en fonction de u, v et d.

8. Réciproquement, montrer que s'il existe des entiers naturels non nuls u, v et d avec $u<v$ tels que $a=2duv$, $b=d(v^2-u^2)$ et $c=d(u^2+v^2)$, alors $(a\,;b\,;c)$ est un triplet pythagoricien.

9. Donner la forme générale de tous les triplets pythagoriciens.

D. Algorithme de recherche

On donne l'algorithme suivant :

```
Saisir M
  Pour m prenant les valeurs de 2 à M
  |   Pour n prenant les valeurs 1 à m
  |   |   A prend la valeur 2mn
  |   |   B prend la valeur m² – n²
  |   |   C prend la valeur m² + n²
  |   Fin Pour
  Fin Pour
Afficher A, B, C
```

Justifier que cet algorithme affiche bien des triplets pythagoriciens.

Aides pour les logiciels

Excel ou Open Office

A. 3. Utiliser la fonction **ENT** du tableur pour tester si $\sqrt{a^2+b^2}$ est entier.
Utiliser ensuite la fonction **SI** pour afficher 1 ou 0 selon les cas.
On peut éventuellement colorer les cellules affichant un 1 à l'aide de l'outil Mise en forme conditionnelle (Excel) ou Formatage conditionnel (Open Office) du tableur.

TP 2 Équations polynomiales à coefficients entiers

→ Utiliser l'arithmétique pour résoudre des équations.

Une équation polynomiale à coefficients entiers est une équation de la forme :

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0 \quad (E),$$

où $a_n, a_{n-1}, \ldots, a_2, a_1$ et a_0 sont entiers avec $a_n \neq 0$. On va étudier un critère qui permet de trouver des solutions rationnelles ou entières des équations polynomiales, lorsqu'elles existent.

A. Étude d'un cas particulier

Soit (E_1) l'équation $x^7 - 6x^4 + 5x^3 - 3x^2 - 31x + 2 = 0$.

1. Montrer que si (E_1) a une solution entière m, alors m divise 2. En déduire les valeurs possibles de m.

2. (E_1) a-t-elle une solution entière ?

B. Étude mathématique

1. Montrer que, pour tout naturel n, si p et q sont deux entiers premiers entre eux, alors p et q^n sont aussi premiers entre eux.

2. a. On suppose que l'équation (E) admet une solution de la forme $\frac{p}{q}$, où p et q sont des entiers tels que la fraction $\frac{p}{q}$ soit irréductible. Montrer que $\frac{p}{q}$ est solution de (E) si, et seulement si, p et q vérifient l'équation (E') ci-après.

$$a_n p^n + a_{n-1}qp^{n-1} + a_{n-2}q^2p^{n-2} + \ldots + a_2 q^{n-2}p^2 + a_1 q^{n-1}p + a_0 q^n = 0.$$

b. Montrer que p divise a_0 et q divise a_n.

c. Énoncer un critère permettant de reconnaître les fractions irréductibles qui peuvent être solutions d'une équation polynomiale à coefficients entiers.

C. Une application

Soit (E_2) l'équation $15x^3 - 43x^2 - 7x + 3 = 0$.

1. Montrer que le critère énoncé dans la **partie B** montre qu'au plus 12 fractions irréductibles peuvent être solutions de l'équation (E_2).

2. En utilisant la calculatrice, en déduire les solutions exactes de cette équation.

TP 3 Exemple de codage par la méthode RSA

TICE → Utiliser un logiciel pour la méthode RSA.

Le système RSA est un système de codage à clés publiques, alors que les clés de décodage sont secrètes. Les clés de codage sont deux entiers e et n : n est le produit de deux nombres premiers p et q très grands, et e est un entier premier avec $(p-1)(q-1)$. On étudie ici un exemple très simplifié de cette méthode, afin d'avoir des calculs abordables : on choisit $e = 3$ et $n = 33 = 3 \times 11$.

Les clés de codage sont donc les entiers 3 et 33. On affecte à chaque entier de l'ensemble (E) = {0 ; 1 ; 2 ; … ; 32} une lettre de l'alphabet ou un autre symbole (on affecte A à 0, B à 1, …, Z à 25, [à 26, …, ^ à 29), puis on fait subir à chacun de ces entiers x la transformation f suivante : $x \mapsto y$, où y est le reste dans la division euclidienne de x^3 par 33.

1. Coder le mot PAIX.

2. a. Montrer que 3 et 20 sont premiers entre eux et écrire l'identité de Bézout associée.

b. Soit x un entier. Montrer que $x^{21} \equiv x\ (3)$ et $x^{21} \equiv x\ (11)$. En déduire que $x^{21} \equiv x\ (33)$.

3. a. Montrer que si $f(x) = f(x')$, alors $x = x'$. En déduire que deux éléments différents de (E) ont deux images différentes par f.

b. Soit x et y deux éléments de (E) tels que $y \equiv x^3\ (33)$. Montrer que $y^7 \equiv x\ (33)$. La clé de décodage est donc formée des entiers 7, 11 et 3.

c. Décoder le mot POU.

4. Le programme suivant a été réalisé avec le logiciel Xcas.

```
saisir (Nom) ; a : =asc (Nom) ; k : =dim (a) ;
b : =seq (0, t, 1, k) ;
pour j de 0 jusque k-1 faire
b[ j ] : =irem ( (a[ j ] - 65) ^7, 33) + 65 ;
fpour ;
décodage : =char (b) ; afficher (décodage)
```

a. Expliquer pourquoi il permet de décoder un mot donné.

b. Saisir ce programme avec Xcas, puis décoder les mots SAOYY, SALFT et FYLF.

c. Que fournit le décodage du mot INDICE ? Expliquer.

Aides pour les logiciels

Xcas

4. a. La fonction **asc** transforme un texte en une liste formée des codes ASCII de chaque lettre du texte. Par exemple, `asc("ABC")=[65,66,67]`. La fonction **char** renvoie un texte à partir d'une liste de codes ASCII. **irem(*a*,*b*)** donne le reste de la division euclidienne de l'entier a par l'entier b.

Sujet commenté BAC

➤ Énoncé

Thèmes
- Théorème de Gauss
- Nombres premiers entre eux
- Théorème de Bézout
- Congruences

1. Soit p et q deux entiers naturels tels que p et q soient premiers entre eux.
Déduire du théorème de Gauss que si a est un entier tel que $a \equiv 0\ (p)$ et $a \equiv 0\ (q)$, alors $a \equiv 0\ (pq)$.
On se propose de déterminer l'ensemble (S) des entiers naturels n vérifiant le système :

$$\begin{cases} n \equiv 9\ (17) \\ n \equiv 3\ (5) \end{cases}$$

2. On désigne par $(u\ ;\ v)$ un couple d'entiers tels que $17u + 5v = 1$.
a. Justifier l'existence d'un tel couple $(u\ ;\ v)$.
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).

3. a. Soit n un entier appartenant à (S). Démontrer que $n - n_0 \equiv 0\ (85)$.
b. En déduire qu'un entier n appartient à (S) si, et seulement si, il peut s'écrire sous la forme $n = 43 + 85k$, où k est un entier relatif.

D'après Bac, France métropolitaine, 2011

➤ Comprendre l'énoncé et choisir les méthodes

1. En premier lieu, il faut « traduire » les congruences en égalités.
Ainsi $a \equiv 0\ (p)$ revient à dire qu'il existe un entier naturel k tel que $a = kp$.
De même, $a \equiv 0\ (q)$ revient à dire qu'il existe un entier naturel k' tel que $a = k'q$.
L'égalité obtenue $kp = k'q$, avec p et q premiers entre eux, incite à appliquer le théorème de Gauss (➔ Savoir-faire 10, p. 55).

2. a. On demande de justifier l'existence d'un couple $(u\ ;\ v)$ d'entiers : on peut en donner un, mais ce n'est pas obligatoire puisque le théorème de Bézout assure son existence (➔ Savoir-faire 8, p. 53).
b. On trouve directement que $n_0 \equiv 9 \times 5v\ (17)$, mais pour arriver au résultat, soit $n_0 \equiv 9\ (17)$, il faut penser à isoler $5v$ dans l'identité de Bézout : $5v = 1 - 17u$.

c. La réponse se déduit de la question précédente.
Cette fois-ci, il faut trouver un couple $(u\ ;\ v)$, soit en faisant des essais, soit avec la calculatrice (➔ Savoir-faire 9, p. 53).

3. a. Il faut penser à traduire le fait que n et n_0 sont des éléments de (S) en termes de congruences modulo 5 et 17 : on peut alors faire la différence.
Comme 17 et 5 sont premiers entre eux, on peut appliquer la question **1**.
b. Il s'agit ici de démontrer une équivalence.
Il faut donc traiter la partie directe et sa réciproque.
Si $n \in$ (S), on doit prouver qu'il existe un entier k tel que $n = 43 + 85k$.
Réciproquement, si $n = 43 + 85k$, avec k entier, alors on doit prouver que n appartient à (S).

➤ Réponses

1. $a = kp$ et $a = k'q$, avec k et k' dans $\mathbb{N}$.
D'où : $kp = k'q$.
Comme p et q sont premiers entre eux alors, d'après le théorème de Gauss, p divise k' et q divise k.
Il existe donc un entier naturel m tel que $k = mq$.
D'où $a = mpq$ et $a \equiv 0\ (pq)$.

2. a. Puisque 5 et 17 sont premiers entre eux, d'après le théorème de Bézout il existe des entiers u et v tels que $17u + 5v = 1$.
b. (*) $n_0 = 3 \times 7u + 9 \times 5v$, donc $n_0 \equiv 9\ (17)$.
On a aussi $17u = 1 - 5v$, donc $17u \equiv 1\ (5)$.
(**) $n_0 = 3 \times 7u + 9 \times 5v$, donc $n_0 \equiv 3\ (5)$.
De (*) et (**), on déduit que n_0 appartient à (S).
c. $(-2\ ;\ 7)$ est un couple d'entiers tel que $17u + 5v = 1$, car $17 \times (-2) + 5 \times 7 = 1$.
Alors $n_0 = 3 \times 17 \times (-2) + 9 \times 5 \times 7 = 213$, donc 213 est un entier appartenant à (S).

3. a. Puisque n et n_0 appartiennent à (S), on a :
$n - n_0 \equiv 0\ (17)$ et $n - n_0 \equiv 0\ (5)$.
Comme 17 et 5 sont premiers entre eux et $17 \times 5 = 85$, d'après la question **1**, on obtient :

$$n - n_0 \equiv 0\ (85).$$

b. Grâce à la question précédente, on obtient :

$$n \in (S) \Rightarrow n = n_0 + 85k, \text{ avec } k \text{ entier.}$$

On remarque que $213 \equiv 43\ (85)$, donc on peut choisir $n_0 = 43$, d'où $n = 43 + 85k$.
Réciproquement, si $n = 43 + 85k$, avec k entier, n vérifie les deux équations caractérisant (S) car $n \equiv 3\ (5)$ et $n \equiv 9\ (17)$: ainsi, n appartient à (S).

Pour se préparer à l'écrit BAC

Sujet A

Capacités mises en œuvre

- *Résoudre une équation de la forme $ax + by = c$*
- *Utiliser les congruences*

Partie A

On considère l'équation **(E)** : $11x - 26y = 1$, où x et y désignent deux entiers relatifs.

1. Vérifier que le couple $(-7 ; -3)$ est solution de **(E)**.

2. Résoudre **(E)**. En déduire le couple d'entiers relatifs $(u ; v)$ solution de **(E)** tel que $0 \leqslant u \leqslant 25$.

Partie B

On assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

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 chiffre tout nombre entier x compris entre 0 et 25 en calculant $11x + 8$, puis en calculant le reste y de la division euclidienne de $11x + 8$ par 26. L'entier x est alors codé par y.

1. Coder la lettre W.

2. On cherche à déterminer la fonction de décodage.

a. À l'aide de la **partie A**, déterminer un entier x tel que :

$$11x \equiv 1\ (26).$$

b. En déduire un procédé de décodage, puis décoder la lettre W.

Savoir-faire

Question 1. ➤ Savoir-faire 10, p. 55

Sujet B

Capacités mises en œuvre

- *Utiliser le théorème de Bézout*
- *Utiliser le petit théorème de Fermat*

Pour tout entier naturel $n \geqslant 2$, on pose : $A(n) = n^4 + 1$.

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

b. Montrer que, quel que soit 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 $A(n)$, on a :

$$n^8 \equiv 1\ (d).$$

2. 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 $d - 1$.

3. Dans cette question, on suppose que n est pair.

Soit p un diviseur premier de $A(n)$. En examinant successivement les cas $s = 1$, $s = 2$ et $s = 4$, conclure que $p \equiv 1\ (8)$.

4. Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$. (La liste des nombres premiers congrus à 1 modulo 8 débute par 17, 41, 73, 89, 113, 137…)

Savoir-faire

Question 1. c. ➤ Savoir-faire 7, p. 53

Question 2. c. ➤ Savoir-faire 14, p. 61

Sujet C ROC

Capacités mises en œuvre

- *Démontrer le théorème de Gauss*
- *Résoudre une équation de la forme $ax + by = c$*
- *Utiliser le théorème de Gauss*
- *Utiliser les congruences*

Partie A. Restitution organisée de connaissances

Prérequis : On rappelle le théorème de Bézout : « Deux entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe un couple $(u ; v)$ d'entiers relatifs vérifiant $au + bv = 1$ ».

En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

Partie B

Soit A l'ensemble des entiers naturels de l'intervalle $[1 ; 46]$.

1. On considère l'équation **(E)** : $23x + 47y = 1$ où x et y sont des entiers relatifs.

a. Donner une solution particulière $(x_0 ; y_0)$ solution de **(E)**.

b. Déterminer l'ensemble des couples $(x ; y)$ solutions de **(E)**.

c. En déduire qu'il existe un unique entier x appartenant à A tel que $23x \equiv 1\ (47)$.

2. Soit a et b deux entiers relatifs.

a. Montrer que, si $ab \equiv 0\ (47)$, alors $a \equiv 0\ (47)$ ou $b \equiv 0\ (47)$.

b. En déduire que, si $a^2 \equiv 1\ (47)$, alors $a \equiv 1\ (47)$ ou $a \equiv -1\ (47)$.

3. a. Montrer que pour tout entier p de A, il existe un entier relatif q tel que $p \times q \equiv 1\ (47)$.

On admettra que pour tout entier p de A, il existe un unique entier, noté $\text{inv}(p)$, appartenant à A tel que $p \times \text{inv}(p) \equiv 1\ (47)$.

Par exemple $\text{inv}(1) = 1$ car $1 \times 1 \equiv 1\ (47)$, $\text{inv}(2) = 24$ car $2 \times 24 \equiv 1\ (47)$…

b. Quels sont les entiers p de A qui vérifient $p = \text{inv}(p)$?

Savoir-faire

Question B. 1. a. ➤ Savoir-faire 8 et 9, p. 53

Question B. 1. b. ➤ Savoir-faire 10, p. 55

Sujet D — VRAI – FAUX

Capacités mises en œuvre

- *Résoudre une équation de la forme $ax + by = c$*
- *Utiliser le PGCD et le PPCM*

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

1. On appelle (S) l'ensemble des couples $(x\,;y)$ d'entiers relatifs solutions de l'équation $3x - 5y = 2$.
Proposition 1 : L'ensemble (S) est l'ensemble des couples $(5k - 1\,;\,3k - 1)$ où k est un entier relatif.

2. On considère l'équation **(E)** : $x^2 + y^2 \equiv 0\ (3)$, où $(x\,;y)$ est un couple d'entiers relatifs.
Proposition 2 : Il existe des couples $(x\,;y)$ d'entiers relatifs solutions de **(E)** qui ne sont pas des couples de multiples de 3.

3. Soit n un entier naturel tel que $n \geqslant 3$. On considère l'équation **(E')** : $x^2 - 52x + 480 = 0$ où x est un entier naturel.
Proposition 3 : Il existe deux entiers naturels non nuls dont le PGCD et le PPCM sont solutions de l'équation **(E')**.

Savoir-faire
Question 1. ➤ Savoir-faire 10, p. 55
Question 3. ➤ Savoir-faire 13, p. 59

Sujet E

Capacités mises en œuvre

- *Résoudre une équation de la forme $ax + by = c$*
- *Utiliser les congruences*

1. On considère l'équation **(E)** : $11x - 7y = 5$ où x et y sont des entiers relatifs. Résoudre **(E)**.

2. Dans le plan rapporté à un repère orthonormé $(O\,;\vec{i}\,;\vec{j})$, on considère la droite $\mathscr{D}$ d'équation $11x - 7y - 5 = 0$.
On note $\mathscr{C}$ l'ensemble des points $M(x\,;y)$ du plan tels que :

$$0 \leqslant x \leqslant 50 \quad \text{et} \quad 0 \leqslant y \leqslant 50.$$

Déterminer le nombre de points de la droite $\mathscr{D}$ appartenant à l'ensemble $\mathscr{C}$ et dont les coordonnées sont des nombres entiers.

3. On considère l'équation **(F)** : $11x^2 - 7y^2 = 5$ où x et y sont des entiers relatifs.
a. Démontrer que si le couple $(x\,;y)$ est solution de **(F)**, alors $x^2 \equiv 2y^2\ (5)$.
b. Soit x et y des entiers relatifs.
Recopier et compléter les tableaux suivants :

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

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

Quelles sont les valeurs possibles du reste de la division euclidienne de x^2 et de $2y^2$ par 5 ?
c. En déduire que si $(x\,;y)$ est solution de **(F)**, alors x et y sont des multiples de 5.

4. Démontrer que si x et y sont des multiples de 5, alors le couple $(x\,;y)$ n'est pas solution de **(F)**.
Que peut-on en déduire pour l'équation **(F)** ?

Savoir-faire
Question 1. ➤ Savoir-faire 10, p. 55

Sujet F

Capacité mise en œuvre

- *Utiliser le théorème de Gauss*

Soit $(a\,;b)$ un couple d'entiers strictement positifs, tels que $a^2 = b^3$ 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. Démontrer que $a^2 = b^3$ si, et seulement si, a et b sont respectivement le cube et le carré d'un même entier.

4. Montrer que si n est le carré d'un nombre entier et le cube d'un autre entier, alors $n \equiv 0\ (7)$ ou $n \equiv 1\ (7)$.

Savoir-faire
Question 2. ➤ Savoir-faire 11, p. 55

Pour se préparer à l'oral — BAC

133 Résoudre l'équation $7x + 11y = 1$, où x et y sont des entiers.

134 Montrer que $A = n(n^4 - 1)$ est divisible par 15 pour tout entier n.

135 Pour quelles valeurs entières de n, les nombres $A = 2n + 5$ et $B = 5n - 1$ sont-ils premiers entre eux ?

136 Pour quelles valeurs entières de n, la fraction $\dfrac{6n+7}{2n+5}$ est-elle un nombre entier ?

137 Déterminer tous les couples d'entiers $(a\,;b)$ qui vérifient $\begin{cases} a + b = 350 \\ \text{PGCD}(a\,;b) = 14 \end{cases}$

POUR ALLER PLUS LOIN

138 PGCD de deux entiers dépendant d'un entier

1. Soit n un entier supérieur à 1, $A = n(n+1)$ et $B = (n-1)(n+2)$. Déterminer le PGCD de A et de B.

2. L'entier n étant supérieur à 2, on considère les nombres :

$$C = \frac{(n-1)(n+2)}{2} \quad \text{et} \quad D = \frac{(n-2)(n+3)}{2}.$$

Déterminer le PGCD de C et D, suivant la valeur du reste de la division de n par 4.

PISTE : On pourra former la différence de A et B, puis celle de C et D.

139 Équation du type $ax + by = c$ et PGCD

1. **a.** Résoudre pour x et y entiers l'équation :

$$3x - 2y = 1 \quad (E_1).$$

b. Résoudre pour x et y entiers l'équation :

$$3x - 2y = 4 \quad (E_2).$$

2. **a.** Soit n un entier naturel, $A = 2n + 2$ et $B = 3n + 1$.
Vérifier que A et B sont solutions de (E_2).
b. Quelles sont les valeurs possibles du PGCD de A et B ?
c. Montrer que si le PGCD de A et B est 4, alors n est impair.
d. À l'aide de la calculatrice, conjecturer pour quelles valeurs de n, on a $\text{PGCD}(A ; B) = 4$.

3. **a.** Si $n = 1 + 4q$, où q est un entier naturel montrer que A et B sont divisibles par 4.
b. En déduire le PGCD de A et B lorsque $n = 1 + 4q$, où q est un entier naturel.

140 Fraction irréductible

Déterminer l'ensemble des naturels n tels que la fraction $\frac{n^3 - n}{n+2}$ soit réductible.

PISTE : On pourra montrer que le PGCD de $n^3 - n$ et de $n + 2$ est aussi celui de $n + 2$ et de 6.

141 Nombres premiers entre eux

1. Montrer que l'on ne change pas le PGCD de deux entiers naturels lorsqu'on multiplie l'un d'eux par un nombre premier avec l'autre.

2. Soit x et y des entiers naturels non nuls.
On note $d = \text{PGCD}(x ; y)$, et $d' = \text{PGCD}(x^2 ; xy)$.
Montrer que $\text{PGCD}(d' ; y^2) = d^2$.

142 Suite numérique et PGCD

1. Étant donnés deux entiers naturels a et b non nuls, montrer que si $\text{PGCD}(a ; b) = 1$, alors $\text{PGCD}(a^2 ; b^2) = 1$.

2. Soit la suite (S_n) définie pour $n > 0$ par $\sum_{p=1}^{n} p^3$.

Démontrer par récurrence que, pour tout entier $n > 0$, on a :

$$S_n = \left(\frac{n(n+1)}{2}\right)^2.$$

3. Soit k un entier naturel non nul.
a. Démontrer que $\text{PGCD}(S_{2k} ; S_{2k+1}) = (2k+1)^2 \text{PGCD}(k^2 ; (k+1)^2)$.
b. Calculer $\text{PGCD}(k ; k+1)$.
c. Calculer $\text{PGCD}(S_{2k} ; S_{2k+1})$.

4. Soit k un entier naturel non nul.
a. Démontrer que $2k + 1$ et $2k + 3$ sont premiers entre eux.
b. Calculer $\text{PGCD}(S_{2k+1} ; S_{2k+2})$.

5. Déduire des questions précédentes qu'il existe une unique valeur de l'entier naturel n, que l'on déterminera, pour laquelle S_n et S_{n+1} sont premiers entre eux.

143 Le phare breton

1. Résoudre l'équation :

$$(E) \quad 15q - 28q' = 6,$$

où q et q' sont des nombres entiers.

2. En déduire les solutions du système suivant (S) :

$$\begin{cases} x \equiv 2 \ (15) \\ x \equiv 8 \ (28) \end{cases}$$

3. Un phare breton émet un signal jaune toutes les 15 minutes et un signal rouge toutes les 28 minutes. On aperçoit le signal jaune à 0 h 02 min et le signal rouge à 0 h 08 min.
À quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

144 PGCD et reste dans la division euclidienne

Le nombre n est un entier naturel non nul. On pose $a = 4n + 3$, $b = 5n + 2$ et on note d le PGCD de a et b.

1. Donner la valeur de d dans les trois cas suivants :
a. $n = 1$ **b.** $n = 11$ **c.** $n = 15$

2. Calculer $5a - 4b$ et en déduire les valeurs possibles de d.

3. **a.** Déterminer les entiers naturels n et k tels que $4n + 3 = 7k$.
b. Déterminer les entiers naturels n et k' tels que $5n + 2 = 7k'$.

4. Soit r le reste de la division euclidienne de n par 7.
Déduire des questions précédentes la valeur de r pour laquelle d vaut 7. Pour quelles valeurs de r, d est-il égal à 1 ?

145 Équation $au - bv = 1$

Soit a et b deux entiers premiers entre eux et supérieurs ou égaux à 2. On va montrer qu'on peut trouver un couple $(u_1 ; v_1)$ solution de l'équation (E) $au - bv = 1$ vérifiant $0 < u_1 < b$ et $0 < v_1 < a$.

1. Montrer que l'équation (E) admet au moins un couple solution, que l'on notera $(u_0 ; v_0)$.

2. La division euclidienne de u_0 par b donne pour quotient q et pour reste u_1. Montrer que u_1 n'est pas nul.

3. Soit l'entier $v_1 = v_0 - aq$.
Montrer que le couple $(u_1 ; v_1)$ est solution de (E).

4. Montrer que $v_1 < a$.

5. Montrer que v_1 est non nul.

6. Prouver l'unicité du couple $(u ; v)$ trouvé dans les questions précédentes et vérifiant les conditions du problème.

PISTE : **question 4.** On utilisera $u_1 \leqslant b - 1$.
question 6. Supposer qu'il y a deux couples $(u_1 ; v_1)$ et $(u_2 ; v_2)$ solutions, vérifiant $0 < u_1 < b$, $0 < u_2 < b$, $0 < v_1 < a$ et $0 < v_2 < a$, puis montrer que $u_1 = u_2$ et $v_1 = v_2$.

Exercices

146 PGCD et PPCM

Étant donné un entier naturel n, on considère les deux nombres a et b tels que $a = 2n^2$ et $b = n(2n+1)$.
On désigne par d le PGCD de a et b, et par m leur PPCM.
Montrer que l'on a $b - a = d$ et $b^2 - a^2 = m - d^2$.

147 Logique

1. Soit a et b des entiers naturels avec $a > b$.
Montrer que les propositions suivantes sont équivalentes :
(P_1) : $\frac{a}{b}$ est irréductible ; (P_2) : $\frac{a-b}{ab}$ est irréductible.

2. Soit deux entiers naturels x et y tels que $x > y$, de PGCD d et de PPCM m. Montrer que le PGCD de $x - y$ et de m est égal à d.

148 PPCM et congruences

1. Déterminer toutes les paires d'entiers naturels a et b tels que l'on ait : $\begin{cases} \text{PGCD}(a;b) = 42 \\ \text{PPCM}(a;b) = 1680 \end{cases}$

2. Déterminer l'ensemble des entiers x tels que $8x \equiv 7\ (5)$.

3. Résoudre l'équation $336x + 210y = 294$, avec x et y des entiers.

PISTE : question 3. On a une solution particulière de l'équation simplifiée.

149 Les jetons

On possède un certain nombre de jetons, ce nombre étant inférieur à 3 000. Qu'on les dispose en piles de 10, de 9, de 8, de 7, de 6, de 5, de 4, de 3 ou de 2 jetons, il en manque toujours un pour compléter la dernière pile.
Combien y a-t-il de jetons, sachant qu'on peut les disposer exactement en piles de 11 jetons ?

PISTE : Si $n+1$ est divisible par 8, il est aussi divisible par 2 et 4.

150 Chiffrement par transformation affine

Pour coder un message, on traduit tout d'abord chaque lettre en son équivalent numérique à l'aide du 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

Soit (E) l'ensemble des entiers naturels compris entre 0 et 25.
On définit un système de codage à l'aide de la transformation f suivante : si x appartient à (E), alors $x \mapsto y$, où y est le reste de la division euclidienne de $ax + b$ par 26, avec a et b entiers de (E), a étant non nul.

1. On suppose a premier avec 26.
Montrer que si $f(x) = f(x')$, alors $x = x'$.

2. On suppose que le PGCD de a et 26 est d, avec d différent de 1.
Montrer qu'il existe alors des lettres codées de la même façon.

3. En déduire quels sont les couples $(a\,;b)$ définissant un « bon » codage. Combien y a-t-il de tels couples ?
Combien y a-t-il de codages affines distincts ?

4. Montrer que si a est premier avec 26, alors il existe un entier a' de (E) tel que $aa' \equiv 1\ (26)$.

5. En déduire une formule de décodage, c'est-à-dire une expression de x en fonction de y, a, b et a' si on a $y = f(x)$.

151 Un chiffrement par exponentiation

On affecte à chaque entier compris entre 0 et 30 une lettre de l'alphabet ou un symbole (on affecte A à 0, B à 1, ..., Z à 25, α à 26, β à 27, γ à 28, δ à 29 et ε à 30).
Puis on fait subir à chacun de ces entiers x la transformation f suivante : $x \mapsto y$, où y est le reste dans la division euclidienne par 31 de x^7. On note $E = \{0\,;1\,;2\,;\ldots\,;30\}$. Les clés de ce codage sont 7 et 31.

1. Coder le mot CAMILLE.

2. Montrer que 7 et 30 sont premiers entre eux et écrire l'identité de Bézout correspondante.

3. En utilisant le petit théorème de Fermat, montrer que, si x et x' sont des éléments de E tels que $f(x) = f(x')$, alors $x = x'$.
En déduire que deux éléments différents de E ont des images différentes par f.

4. Soit x et y des éléments de E tels que $y \equiv x^7\ (31)$.
Montrer que $y^{13} \equiv x\ (31)$. La clé de décodage est donc 13.

5. Décoder alors le mot YCEγQN.

→ Pour vous aider Savoir-faire 15, p. 61

152 Méthode de Borel ALGO

1. Soit a et b deux naturels premiers entre eux.
Montrer que résoudre l'équation (E) : $au + bv = 1$ revient à résoudre l'équation $ax \equiv 1\ (b)$.

2. Expliquer pourquoi on peut alors calculer les multiples successifs de a et chercher ceux dont le reste dans la division euclidienne par b est 1.

3. Écrire un algorithme qui permet d'afficher des solutions de l'équation (E) en utilisant cette méthode.

4. Programmer cet algorithme sur la calculatrice.

153 Avec un tableur TICE

On affecte à chaque lettre de l'alphabet un entier compris entre 0 et 25. On note E l'ensemble de ces entiers. On se propose de réaliser le chiffrement d'un message à l'aide de la transformation suivante : si x appartient à E, alors $x \mapsto y$, où y est le reste de la division euclidienne de $3x + 11$ par 26.
Le message à coder est : LES INDICES SONT UTILES.

1. Ouvrir une feuille de calcul d'un tableur et écrire le message à coder sur la première ligne de cette feuille.

2. Transformer chaque lettre en un entier de E sur la deuxième ligne en utilisant la fonction **CODE** du tableur : **CODE(X)** fournit le code ASCII de la lettre X. Le code ASCII de A est 65, celui de B est 66, ..., celui de Z est 90.

3. À l'aide de la fonction **MODE**, effectuer la transformation sur la troisième ligne de la feuille de calcul.

4. Afficher le message codé sur la quatrième ligne, en utilisant la fonction **CAR** du tableur : **CAR(x)** fournit le caractère dont le code ASCII est x.

5. Décoder alors le message : LYQJRBYNQJQTQJBYYXSSXVXYQ.

154 Un entier divisible par 4

Soit n un entier naturel non nul.
On considère les entiers suivants : $N = 9n + 1$ et $M = 9n - 1$.

1. On suppose que n est un entier pair.
On pose $n = 2p$ avec p entier naturel non nul.
a. Montrer que M et N sont des entiers impairs.
b. Déterminer le PGCD de M et de N.

2. On suppose que n est impair.
On pose $n = 2p + 1$ avec p entier naturel.
a. Montrer que M et N sont pairs.
b. Déterminer le PGCD de M et de N.

3. Pour tout entier n naturel non nul, on considère l'entier $A = 81n^2 - 1$.
a. Exprimer A en fonction de M et de N.
b. Démontrer que si n est pair, alors A est impair.
c. Démontrer que A est divisible par 4 si, et seulement si, n est impair.

155 Chiffrement avec le système RSA

Le système RSA est un système de codage à clés publiques, alors que les clés de décodage sont secrètes. Les clés de codage sont deux entiers e et n. L'entier n est le produit de deux nombres premiers p et q très grands ; e est un entier premier avec $(p - 1)(q - 1)$.
On découpe le texte du message en blocs, puis on fait correspondre à chaque lettre son équivalent numérique. Ensuite, pour chaque bloc de chiffres B, on forme un bloc codé C, où C est le reste de la division euclidienne de B^e par n. Ainsi : $C \equiv B^e\ (n)$.

1. **a.** Montrer qu'il existe des entiers u et v tels que :
$$ue + v(p - 1)(q - 1) = 1.$$
b. Montrer qu'il existe des entiers k et d tels que :
$$u = k(p - 1)(q - 1) + d,$$
avec $0 < d < (p - 1)(q - 1)$.
c. En déduire qu'il existe un entier w tel que :
$$ed + w(p - 1)(q - 1) = 1.$$
d. Montrer que l'entier w est strictement négatif.

2. Soit x un entier. Montrer que $x^{ed} \equiv x\ (p)$ et que $x^{ed} \equiv x\ (q)$.
En déduire que $x^{ed} \equiv x\ (n)$.

3. Montrer que deux blocs de chiffres B et B′ distincts sont codés par deux blocs C et C′ distincts.

4. Montrer que, si $C \equiv B^e\ (n)$, alors $B \equiv C^d\ (n)$.
Cette formule permet donc un décodage du message chiffré C. Les clés de décodage sont ici d, p et q : en effet, le calcul de d nécessite la connaissance de p et q.

Point Histoire

Le système RSA, premier algorithme de chiffrement à clé publique, a été mis au point en 1977 par les américains **Rivest**, **Shamir** et **Adleman**.
La clé de codage, formée des entiers e et n, est publique : l'expéditeur du message lit les deux clés publiques e et n dans un annuaire. Il calcule alors B^e modulo n qu'il transmet au destinataire : celui-ci est le seul à connaître les entiers p et q qui permettent le calcul de d. Il calcule alors $(B^e)^d$ modulo n, ce qui lui permet de retrouver le message initial. La clé de décodage (privée) est formée des entiers d, p et q.
La force de ce système est que la connaissance de n ne permet pas de déterminer p et q, si n est suffisamment grand : en effet, la factorisation d'un nombre n de 600 chiffres nécessiterait, avec les meilleurs ordinateurs actuels, quelques millions d'années de temps de calcul !

156 PROBLÈME DE SYNTHÈSE

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 (U_n).

2. On appelle (E) l'ensemble des nombres premiers qui divisent au moins un des termes de la suite (U_n).
Montrer que 2, 3, 5 et 7 appartiennent à (E).

3. Soit p un nombre premier strictement supérieur à 3.
a. Montrer que :
$2^{p-1} \equiv 1\ (p)$, que $3^{p-1} \equiv 1\ (p)$ et que $6^{p-1} \equiv 1\ (p)$.
b. En déduire que $6 \times 2^{p-2} \equiv 3\ (p)$ et que $6 \times 3^{p-2} \equiv 2\ (p)$.
c. Montrer que $6U_{p-2} \equiv 0\ (p)$.
Le nombre p appartient-il à (E) ?

Prises d'initiatives

157 Soit a et b deux entiers premiers et distincts.
Démontrer que $a^{b-1} + b^{a-1} - 1$ est divisible par ab.

158 Trouver tous les couples d'entiers $(x ; y)$ dont le PGCD et le PPCM sont solutions de l'équation de l'équation :
$$X^2 - 91X + 588 = 0.$$

159 Soit p un nombre premier différent de 2.
Montrer que, pour tout entier n : $(n + 1)^p - (n^p + 1)$ est divisible par $2p$.

160 Résoudre le système $\begin{cases} 3x - 5y = 6 \\ y \equiv x^2\ (5) \end{cases}$

161 Soit n un entier, la fraction $\dfrac{n^3 + 4}{n^2 + 5}$ peut-elle être un nombre entier ?

162 On dispose de plus de 100 jetons et de moins de 500 jetons. Si on les distribue à 11 personnes, il en reste 4, si on les distribue à 13 personnes, il en reste 5.
De combien de jetons dispose-t-on ?

163 Déterminer toutes les solutions $(x ; y)$ entières de l'équation $x + y - 1 = \text{PGCD}(x ; y)$.

Avant de commencer, se tester avec...

...des QCM

Choisir la (ou les) bonne(s) réponse(s).

➤ Savoir déterminer le nombre de solutions d'un système

	A	B	C	D
1 Les droites d'équations $7x + 4y = 2$ et $9x - 11y = 1$ ont pour intersection	l'ensemble vide	un unique point	une droite	un point à coordonnées entières
2 Les plans d'équation $x + y + z = -3$ et $3x - y = -2$ ont pour intersection	l'ensemble vide	un ensemble constitué d'un unique point	une droite	un plan
3 Le nombre de solutions du système $\begin{cases} 3x - 4y = a \\ \frac{-\sqrt{2}}{3}x + \frac{\sqrt{32}}{9}y = b \end{cases}$ est égal à	1	0	une infinité	On ne peut pas répondre : cela dépend de a et b.

➤ Savoir calculer avec des taux d'évolution successifs

4 Un prix augmente de 3 % par an durant 15 ans. En 15 ans, il a été multiplié, à 10^{-3} près, par	1,558	51,186	0,450	15,450
5 Un prix augmente chaque année du même pourcentage p. En 10 ans, il a augmenté d'environ 22 %. p vaut environ	0,02	2	20	1,02

➤ Savoir utiliser les probabilités conditionnelles

6 Pour des événements A et B de probabilités non nulles, $P(B)$ est égal à	$P_A(B) + P_{\overline{A}}(B)$	$P(A)\,P_A(B) + P(\overline{A})P_{\overline{A}}(B)$	$P_A(B) + P_A(\overline{B})$	$\frac{P(B \cap A)}{P(A)}$
7 Soit des événements A et B tels que $P(A) = 0,2$, $P_A(B) = 0,3$ et $P_{\overline{A}}(\overline{B}) = 0,4$, alors $P(B)$ est égal à	0,9	0,7	0,54	0,38

➤ Voir les réponses, p. 140

...des exercices

8 60 % des participants à un congrès sont des hommes. 75 % des hommes se rendent au congrès avec leur voiture personnelle et 40 % des femmes ne viennent pas avec leur véhicule personnel. Recopier et compléter le tableau de fréquences ci-contre :

	Femmes	Hommes	Total
Véhicule personnel			
Train			
Total		60 %	100 %

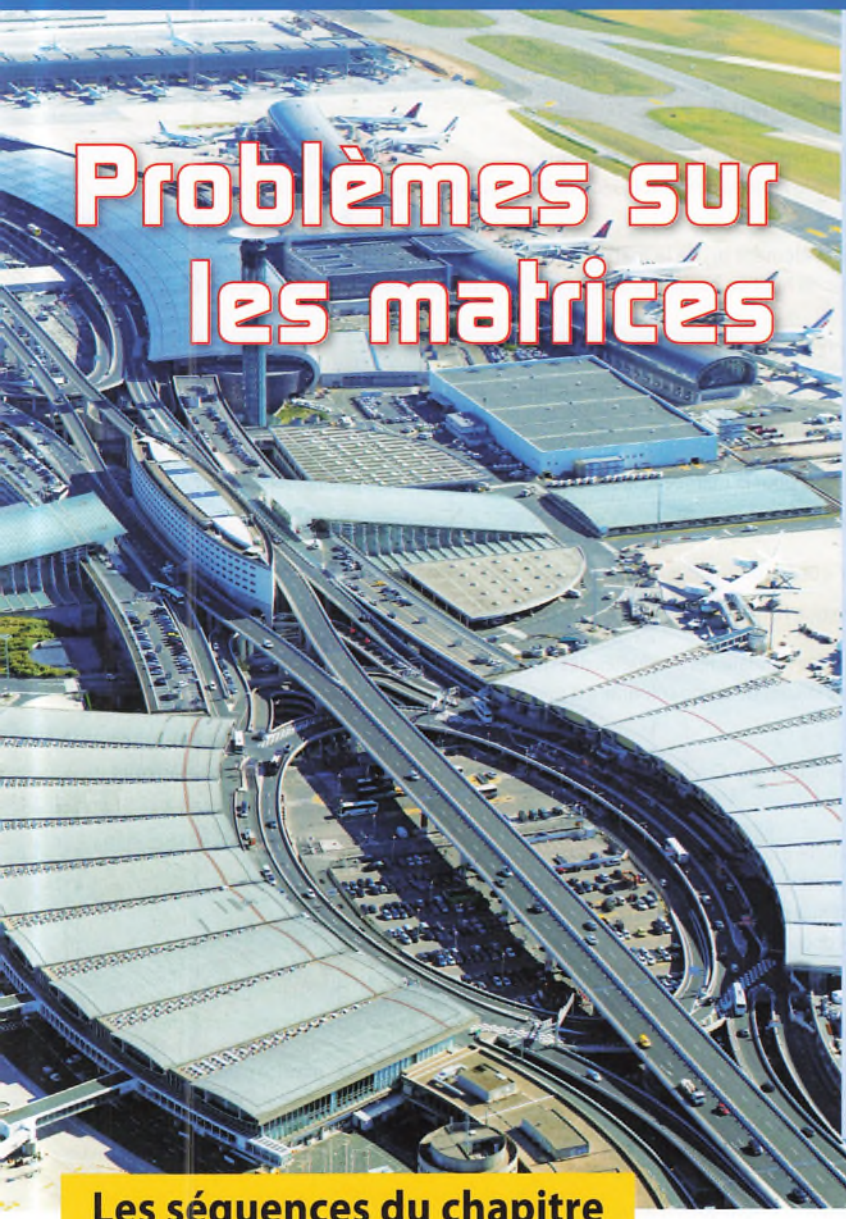
9 Dans une population, on étudie deux caractères génétiques A et B. 60 % des individus possèdent le caractère A et 40 % le caractère B, 18 % ne possèdent aucun des deux caractères.
On choisit un individu au hasard.
Quelle est la probabilité qu'il possède le caractère B sachant qu'il possède le caractère A ?

➤ Voir les réponses, p. 140

CHAPITRE

3

Problèmes sur les matrices



Les matrices sont des tableaux de nombres.

Elles constituent un élément essentiel de l'algèbre linéaire, branche très importante des mathématiques, et sont aujourd'hui à la base de nombreux calculs effectués par nos ordinateurs.

Elles permettent également de modéliser les réseaux, comme un réseau aérien.

Les séquences du chapitre

Le raisonnement logique Logique
p. 91, 92, 98 et 99

Les algorithmes ALGO
p. 97, 98, 99, 103 et 105

Utilisation de logiciels TICE
p. 90 et 103

Problème 1

Carré magique

Objectif
Découvrir la notion de matrice et les opérations usuelles.

Cours 1
Généralités sur les matrices

Point Histoire
On trouve des représentations de carrés magiques dans les civilisations indiennes et chinoises 2 000 ans av. J.-C. Le peintre allemand Dürer a représenté un de ces carrés dans sa célèbre gravure *Melancholia* en 1514.

Partie A. Définition d'une matrice magique

On considère le tableau de nombres (ou matrice) suivant : $A = \begin{pmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{pmatrix}$.

On appellera **élément $a_{i,j}$ de la matrice A** le nombre se trouvant ligne i, colonne j, les lignes étant numérotées de haut en bas de 1 à 3 et les colonnes numérotées de gauche à droite de 1 à 3.
On a ainsi $a_{1,2} = 9$.

1. Donner la valeur de $a_{1,1}$, $a_{3,2}$ et $a_{2,3}$.

2. a. Calculer la somme des éléments de la ligne 1 de la matrice A, c'est-à-dire :

$$\sum_{j=1}^{3} a_{1,j} = a_{1,1} + a_{1,2} + a_{1,3}.$$

b. Vérifier que, pour la matrice A, la somme des éléments d'une ligne ne dépend pas du numéro de cette ligne, c'est-à-dire que l'on a $\sum_{j=1}^{3} a_{1,j} = \sum_{j=1}^{3} a_{2,j} = \sum_{j=1}^{3} a_{3,j}$.

3. Vérifier que la somme des éléments d'une colonne ne dépend pas du numéro de la colonne, c'est-à-dire que l'on a $\sum_{i=1}^{3} a_{i,1} = \sum_{i=1}^{3} a_{i,2} = \sum_{i=1}^{3} a_{i,3}$.

4. Une matrice vérifiant les propriétés des questions **2.** et **3.** et dont la somme S d'une ligne est de plus égale à la somme d'une colonne, est dite semi-magique de somme S.

Vérifier que la matrice $C = \begin{pmatrix} 1 & 2 & 15 & 16 \\ 14 & 13 & 3 & 4 \\ 11 & 12 & 6 & 5 \\ 8 & 7 & 10 & 9 \end{pmatrix}$ est également une matrice semi-magique.

5. On appelle diagonale principale d'une matrice M carrée d'ordre p (c'est-à-dire ayant p lignes et p colonnes) la diagonale nord-ouest/sud-est joignant l'élément $m_{1,1}$ à l'élément $m_{p,p}$ et on appelle seconde diagonale de la matrice M la diagonale nord-est/sud-ouest joignant l'élément $m_{1,p}$ à l'élément $m_{p,1}$.

$\begin{pmatrix} m_{1,1} & * & * & m_{1,4} \\ * & m_{2,2} & m_{2,3} & * \\ * & m_{3,2} & m_{3,3} & * \\ m_{4,1} & * & * & m_{4,4} \end{pmatrix}$
diagonale principale et seconde diagonale d'une matrice carrée d'ordre 4

a. Soit $a_{i,j}$ un élément de la diagonale principale de la matrice A. Exprimer j en fonction de i.

b. Soit $a_{i,j}$ un élément de la seconde diagonale de la matrice A. Que vaut la somme $i + j$?

c. On dit qu'une matrice carrée semi-magique de somme S est magique lorsque la somme des éléments de la diagonale principale est égale à S et la somme des éléments de la seconde diagonale est égale à S.
Les matrices A et C sont-elles magiques ?

Partie B. Opérations sur les matrices magiques

1. Soit t un nombre réel et M une matrice.
On note tM la matrice obtenue en multipliant par t chacun des éléments de la matrice M.

a. Écrire la matrice 5A. Vérifier que cette matrice est magique.

b. Démontrer que, pour toute matrice magique M et tout nombre réel t, la matrice tM est magique.

2. Soit M et N deux matrices carrées de même ordre.
La matrice Q = M + N est la matrice dont l'élément $q_{i,j}$ est égal à la somme $m_{i,j} + n_{i,j}$.

Vérifier que la matrice A + B, où B est la matrice magique $\begin{pmatrix} 8 & 3 & 4 \\ 1 & 5 & 9 \\ 6 & 7 & 2 \end{pmatrix}$, est également magique.

3. M et N étant deux matrices carrées magiques de même ordre et t, s deux réels quelconques, la matrice tM + sN est-elle nécessairement magique ?

Cours 1

Généralités sur les matrices

Définition Une **matrice** A de dimension $n \times p$ (ou de format (n, p)) est un tableau de nombres comportant n lignes et p colonnes. Les nombres de ce tableau sont appelés les **éléments** ou les **coefficients** de la matrice. L'élément se trouvant à l'intersection de la ligne i et de la colonne j sera en général noté $a_{i,j}$. Lorsque $n = p$, on parle de **matrice carrée** et n est appelé l'**ordre** de la matrice.

Vocabulaire
Lorsque $n = 1$, on parle de **matrice ligne** ou **vecteur ligne.**
Lorsque $p = 1$, on parle de **matrice colonne** ou **vecteur colonne.**

Exemple : $A = \begin{pmatrix} 2 & \pi & -3 \\ 4 & 5 & \frac{1}{3} \end{pmatrix}$ est une matrice de dimension 2×3.

Une matrice carrée d'ordre 2 (de dimension 2×2) est une matrice de la forme : $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$.

Définition **Égalité de deux matrices**
Deux matrices A et B sont égales lorsqu'elles ont la même dimension et que pour chaque ligne i et chaque colonne j, l'élément $a_{i,j}$ de la matrice A est égal à l'élément $b_{i,j}$ de la matrice B.

Vocabulaire
On appelle **matrice nulle** la matrice dont tous les éléments sont égaux à 0.
On notera 0_n la matrice nulle d'ordre n.

Définition **Addition de deux matrices**
Soit A et B deux matrices ayant le même nombre de lignes et de colonnes.
La matrice $C = A + B$ est la matrice dont l'élément $c_{i,j}$ de la ligne i, colonne j est égal à la somme $a_{i,j} + b_{i,j}$ des éléments respectifs des lignes i et des colonnes j des matrices A et B.

Exemple : $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 7 & 8 \\ 9 & 12 \end{pmatrix} = \begin{pmatrix} 2+7 & 0+8 \\ 1+9 & 3+12 \end{pmatrix} = \begin{pmatrix} 9 & 8 \\ 10 & 15 \end{pmatrix}$.

Propriétés
(1) Pour deux matrices A et B ayant même nombre de lignes et de colonnes, on a $A + B = B + A$.
On dit que l'addition de deux matrices est commutative.
(2) Soit A, B et C des matrices ayant même nombre de lignes et de colonnes, on a $A + (B + C) = (A + B) + C$.
On dit que l'addition des matrices est associative.

Démonstration
(1) L'élément $s_{i,j}$ de la matrice $A + B$ est égal à $a_{i,j} + b_{i,j}$ et l'élément $s'_{i,j}$ de la matrice $B + A$ est égal à $b_{i,j} + a_{i,j}$.
Et ces nombres sont bien égaux.
(2) L'élément $s_{i,j}$ de la matrice $A + (B + C)$ est égal à $a_{i,j} + (b_{i,j} + c_{i,j})$ et l'élément $s''_{i,j}$ de la matrice $(A + B) + C$ est égal à $(a_{i,j} + b_{i,j}) + c_{i,j}$. Et ces nombres sont bien égaux.

À noter
On définit la différence $A - B$ de deux matrices par : $A - B = A + (-1)B$.

Définition **Multiplication par un réel**
Pour un réel k et une matrice A, on note kA la matrice M dont l'élément $m_{i,j}$ est égal à $k \times a_{i,j}$.

Exemple : $3\begin{pmatrix} 1 & -2 & 4 \\ 2 & \sqrt{2} & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 3\times 1 & 3\times(-2) & 3\times 4 \\ 3\times 2 & 3\times\sqrt{2} & 3\times\frac{1}{3} \end{pmatrix} = \begin{pmatrix} 3 & -6 & 12 \\ 6 & 3\sqrt{2} & 1 \end{pmatrix}$.

Propriétés Pour des réels k, k' et des matrices A et B, on a :
(1) $k(A + B) = kA + kB$ (2) $(k + k')A = kA + k'A$ (3) $k(k'A) = (kk')A$

On vérifie en effet, pour les trois cas, que chaque élément ligne i, colonne j du membre de gauche de l'égalité est égal à l'élément ligne i, colonne j du membre de droite.

Vocabulaire
La matrice $(-1)B$, notée $-B$, est appelée **matrice opposée** de B.

Propriété Soit A, B et C trois matrices de même dimension et k un réel.
L'égalité $A = B$ est équivalente à l'égalité $A + kC = B + kC$.
En particulier l'égalité $A + B = C$ équivaut à l'égalité $B = C - A$.

Démonstration
La première équivalence résulte de l'équivalence analogue sur les coefficients : l'égalité entre nombres réels $a_{i,j} + kc_{i,j} = b_{i,j} + kc_{i,j}$ est en effet équivalente à l'égalité $a_{i,j} = b_{i,j}$.
La seconde équivalence en résulte : on ajoute $-A$ ou A à chaque membre de l'égalité.

Savoir-faire 1 Lire et interpréter les coefficients d'une matrice

➤ Voir l'exercice 35

La matrice $M = \begin{pmatrix} 0,2 & 0,8 \\ 0,6 & 0,4 \end{pmatrix}$ donne la répartition des fréquences des votes dans la ville A (ligne 1) et dans la ville B (ligne 2) pour le candidat C1 (colonne 1) et le candidat C2 (colonne 2).
Ainsi le coefficient $m_{1,1}$ signifie que 20 % des votants de la ville A ont voté pour C1.
La ville A compte 10 000 votants et la ville B en compte 20 000. Donner une matrice ligne V donnant le nombre de voix obtenu par chaque candidat (colonne 1 : C1, colonne 2 : C2).

Conseil
Pour utiliser une matrice, il ne faut pas perdre de vue la signification des nombres qui y figurent.

Solution

$a_{1,1} \times 10\,000 = 0,2 \times 10\,000 = 2\,000$, donc 2 000 habitants de la ville A votent pour C1.
$a_{2,1} \times 20\,000 = 0,6 \times 20\,000 = 12\,000$, donc 12 000 habitants de la ville B votent pour C1.
Le candidat C1 a donc obtenu $2\,000 + 12\,000 = 14\,000$ voix.
$a_{1,2} \times 10\,000 = 0,8 \times 10\,000 = 8\,000$, donc 8 000 habitants de la ville A votent pour C2.
$a_{2,2} \times 20\,000 = 0,4 \times 20\,000 = 8\,000$, donc 8 000 habitants de la ville B votent pour C2.
Le candidat C2 a ainsi obtenu $8\,000 + 8\,000 = 16\,000$ voix.
On obtient la matrice ligne $V = (14\,000 \quad 16\,000)$, où $v_{1,1} = 14\,000$ est le nombre de voix obtenues par le candidat C1 et $v_{1,2} = 16\,000$ est le nombre de voix obtenues par le candidat C2.

	candidat C1	candidat C2
ville A	0,2	0,8
ville B	0,6	0,4

Savoir-faire 2 Créer une matrice sur une calculatrice

➤ Voir l'exercice 1

1. Définir la matrice $A = \begin{pmatrix} 2 & 1 & 3 \\ 9 & 8 & 7 \end{pmatrix}$ sur une calculatrice.

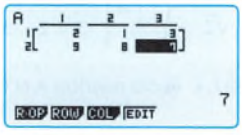
2. Calculer la somme des éléments de la ligne 1 de cette matrice dans l'écran de calcul.

Conseil
Pour certaines calculatrices Texas, il existe une touche matrice.

Solution

Casio

1. Chaque entrée se valide avec la touche EXE.
Entrer dans le menu **RUN-MAT**.
Sélectionner le menu ▶*MAT*, puis *Mat A*.
Il est alors demandé d'entrer *m* (nombre de lignes, ici 2), puis *n* (nombre de colonnes, ici 3).
Entrer ensuite chacun des coefficients et valider.

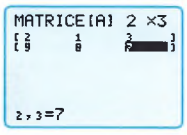


Pour utiliser cette matrice dans l'écran de calcul, sélectionner OPTN, *MAT* (touche F2), *MAT* (touche F1) puis entrer A.

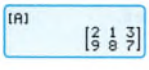
2. Calcul de la somme des éléments de la ligne 1 : Mat A[1,1]+Mat A[1,2]+Mat A[1,3].
Cette somme est égale à 6.

Texas

1. Entrer dans le menu matrice (2nde x^{-1}).
Sélectionner *EDIT* puis *1 : [A]*.
Le curseur se situe sur un chiffre représentant le nombre de lignes, entrer 2 et valider.
Puis entrer 3 (nombre de colonnes) et valider.
Entrer alors les coefficients de la matrice un à un.



Pour utiliser cette matrice dans l'écran de calcul, entrer à nouveau dans le menu matrice et sélectionner *NOMS* puis *1 : [A]*.

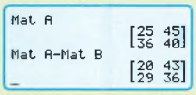


2. Calcul de la somme des éléments de la ligne 1 : [A](1,1)+[A](1,2)+[A](1,3).
Cette somme est égale à 6.

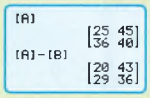
Savoir-faire 3 Calculer et interpréter la somme de deux matrices

➤ Voir l'exercice 39

Conseils
- Avant d'additionner des matrices, vérifier qu'elles ont même dimension.
- On peut vérifier le résultat à l'aide d'une calculatrice.



Casio



Texas

Un libraire possède deux magasins. Il relève les stocks de deux livres A (colonne 1) et B (colonne 2) dans le premier magasin (ligne 1) et le second magasin (ligne 2) : $S = \begin{pmatrix} 15 & 30 \\ 26 & 25 \end{pmatrix}$.

1. Prévoyant de plus fortes ventes, il décide d'augmenter les stocks en livrant 10 exemplaires du livre A et 15 exemplaires du livre B à chacun des deux magasins.
Traduire cette opération par une addition de matrices.

2. Les ventes de la première journée sont données par la matrice $V = \begin{pmatrix} 5 & 2 \\ 7 & 4 \end{pmatrix}$.
Donner la matrice des stocks en fin de première journée.

Solution

1. $\begin{pmatrix} 15 & 30 \\ 26 & 25 \end{pmatrix} + \begin{pmatrix} 10 & 15 \\ 10 & 15 \end{pmatrix} = \begin{pmatrix} 25 & 45 \\ 36 & 40 \end{pmatrix}$.

Exemple de lecture : après livraison, le premier magasin aura en stock 40 exemplaires du livre B.

2. À la fin de la première journée, la matrice des stocks est donnée par :

$$\begin{pmatrix} 25 & 45 \\ 36 & 40 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 20 & 43 \\ 29 & 36 \end{pmatrix}.$$

Savoir-faire 4 Multiplier une matrice par un réel

➤ Voir l'exercice 38

Après deux semaines de ventes des livres A et B cités dans le savoir-faire précédent, la matrice des stocks est $S = \begin{pmatrix} 4 & 2 \\ 6 & 8 \end{pmatrix}$. Le gérant décide d'augmenter de 50 % chacun des stocks.

Exprimer la nouvelle matrice S' des stocks en fonction de S.

Solution

Augmenter une quantité de 50 % revient à la multiplier par 1,5.
Multiplier chaque coefficient d'une matrice par 1,5 revient à multiplier la matrice par 1,5.
La nouvelle matrice des stocks est la matrice $S' = 1{,}5\,S$, c'est-à-dire :

$$S' = \begin{pmatrix} 1{,}5 \times 4 & 1{,}5 \times 2 \\ 1{,}5 \times 6 & 1{,}5 \times 8 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 9 & 12 \end{pmatrix}.$$

Méthode
Multiplier une matrice par un nombre t revient à multiplier chacun de ses éléments par t.

Savoir-faire 5 Utiliser l'égalité de deux matrices

➤ Voir les exercices 40 et 41

Soit t un réel, $A = \begin{pmatrix} 1 & 6 \\ 6 & 10 \end{pmatrix}$, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$.

Montrer que A peut s'écrire sous la forme $A = sI + tB$ où s et t sont des réels à déterminer.

Solution

Deux matrices sont égales si, et seulement si, elles ont les mêmes coefficients.

$A = sI + tB$ équivaut à : $\begin{cases} 1 = s + t \\ 6 = 2t \\ 6 = 2t \\ 10 = s + 4t \end{cases}$, ce qui équivaut à $\begin{cases} s + 3 = 1 \\ t = 3 \\ t = 3 \\ s + 12 = 10. \end{cases}$

Ce système équivaut à : $s = -2$ et $t = 3$. La matrice A peut donc s'écrire : $A = -2I + 3B$.

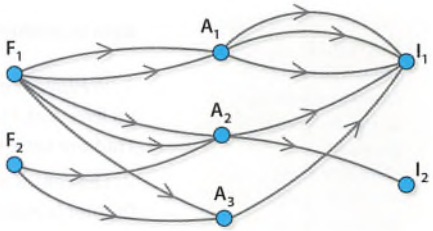
Méthode
Pour traduire l'égalité de deux matrices carrées d'ordre n, on écrit n^2 égalités entre nombres.

Problème 2 Liaisons aériennes

Objectif
Découvrir la notion de produit de deux matrices.

Cours 2
Multiplication de deux matrices

On représente le nombre de vols entre certaines grandes villes par le schéma ci-dessous.



Dans le tableau ci-après, on a indiqué les nombres de liaisons des villes F_1 et F_2 vers les villes A_1, A_2 et A_3 :

	A_1	A_2	A_3
F_1	2	2	1
F_2	0	1	1

Il y a, par exemple, deux liaisons de F_1 vers A_1.
On associe à ce tableau la matrice :

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

1. Définir de même la matrice Q des liaisons des villes A_1, A_2 et A_3 vers les villes I_1 et I_2.

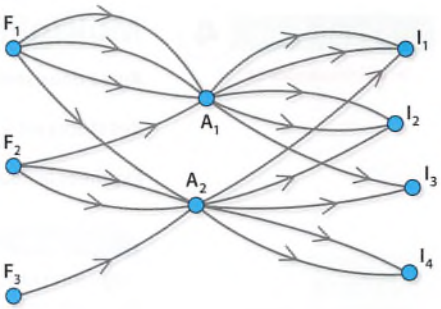
2. Vérifier que l'on peut se rendre de 9 façons distinctes de F_1 à I_1.

3. Définir la matrice R des nombres de liaisons des villes F_1 et F_2 vers les villes I_1 et I_2 : $R = \begin{pmatrix} 9 & \cdots \\ \cdots & \cdots \end{pmatrix}$.

4. Le lien entre les matrices obtenues se traduit par l'égalité $R = P \times Q$.
Expliquer comment on obtient le coefficient $r_{1,1}$ de R à partir des matrices P et Q.
Procéder de même pour les autres coefficients de R.

5. Sur le nouveau plan des vols ci-contre, on a :

$$P = \begin{pmatrix} 3 & 1 \\ 1 & 2 \\ 0 & 1 \end{pmatrix}.$$



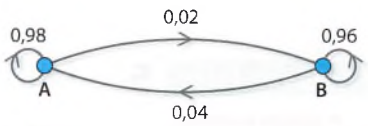
a. Identifier de même les matrices Q et R donnant les nombres de liaisons des villes A vers les villes I et des villes F vers les villes I.
b. Expliquer comment on obtient le coefficient $r_{1,1}$ de R à partir des matrices P et Q.

Problème 3 Évolution de sondages

Objectif
Utiliser les puissances d'une matrice pour étudier une évolution.

Cours 3
Puissances d'une matrice

Deux candidats se présentent à une élection.
En début de campagne, 25 % des personnes déclarent vouloir voter pour le candidat A et 75 % des personnes pour le candidat B.



On notera $R_1 = (0{,}25 \quad 0{,}75)$ la matrice ligne de cette distribution initiale des fréquences de vote. Chaque semaine, de nouveaux sondages sont réalisés. Les sondeurs relèvent une évolution constante : chaque semaine 98 % des personnes s'étant prononcées pour le candidat A la semaine précédente déclarent à nouveau une intention de vote pour A et 2 % de ces personnes se prononcent pour B.
Le candidat B conserve de semaine en semaine 96 % des intentions de vote, les 4 % restants changeant d'avis.

1. Calculer la matrice ligne R_2 de la distribution des fréquences des intentions de vote la deuxième semaine en vous aidant éventuellement d'un arbre pondéré, puis vérifier que $R_2 = R_1 E$, où E est la matrice traduisant les évolutions : $E = \begin{pmatrix} 0{,}98 & 0{,}02 \\ 0{,}04 & 0{,}96 \end{pmatrix}$.

2. Exprimer de même la matrice ligne R_3 de la distribution des intentions de vote la semaine 3 en fonction de R_2 et de la matrice E puis en fonction de R_1 et de la matrice E.

3. On suppose que la campagne électorale dure 12 semaines.

a. Exprimer la matrice ligne R_{12} de la répartition des intentions de vote la 12e semaine en fonction de la répartition initiale et de la matrice E.

b. À l'aide de la calculatrice, donner la distribution des intentions de vote en fin de campagne (on donnera les résultats en pourcentage, arrondis au point entier).

4. On suppose que la campagne dure 20 semaines. Quelle sera dans ce cas la répartition des intentions de vote en fin de campagne ? (On donnera les résultats en pourcentage, arrondis au point entier.)

5. Soit $P = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$ et $Q = \frac{1}{3}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$.

a. Calculer les matrices $D = QEP$ et QP.

b. Montrer par récurrence que pour tout entier naturel $n \geqslant 1$, on a $E^n = PD^nQ$.

c. Exprimer les éléments de la matrice E^n en fonction de n et en déduire que la matrice ligne R_n de la distribution des intentions de vote après n semaines est donnée par :

$$R_n = \frac{1}{12}(8 - 5 \times 0{,}94^{n-1} \quad 4 + 5 \times 0{,}94^{n-1}).$$

d. En déduire la durée de campagne nécessaire pour que les intentions de vote pour le candidat A dépassent 60 %.

Problème 4 Avec domiciles fixes

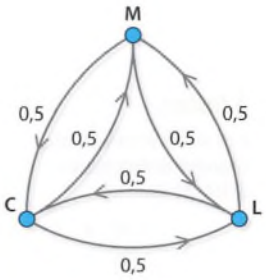
Objectif

Utiliser les puissances d'une matrice pour calculer des probabilités conditionnelles lors d'un grand nombre de répétitions.

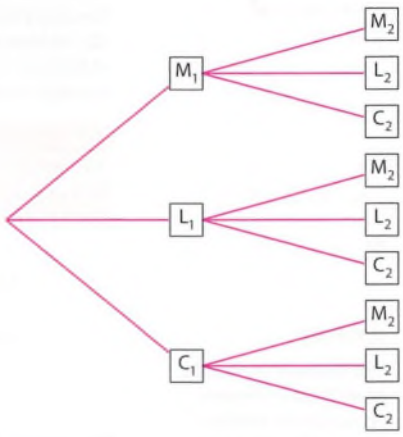
Cours 3 Puissances d'une matrice

Une personne retraitée possède trois maisons, une en bord de mer (M), une à Lille (L) et une à la campagne (C). Chaque mois, elle change de lieu en décidant à pile ou face l'endroit où elle passera le mois suivant. Cette personne choisit au hasard la maison où elle se trouvera en janvier 2012.

On note M_1 l'événement « cette personne passe le mois de janvier à la mer » et on définit de façon analogue les événements L_1, C_1 puis les événements M_j, L_j et C_j ($j \geqslant 2$) pour les mois suivants.



1. a. En recopiant et complétant l'arbre de probabilités conditionnelles ci-contre, déterminer la probabilité des événements M_2, L_2 et C_2.



b. On note $d_1 = \left(\frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{3}\right)$

et $A = \begin{pmatrix} 0 & 0{,}5 & 0{,}5 \\ 0{,}5 & 0 & 0{,}5 \\ 0{,}5 & 0{,}5 & 0 \end{pmatrix}$.

Interpréter les coefficients de d_1 et A en fonction de l'arbre précédent.

c. Interpréter les coefficients de la matrice ligne $d_2 = d_1A$.

2. a. Déterminer, à l'aide d'un arbre de probabilités, les probabilités des événements M_3, L_3 et C_3.

b. Vérifier que l'on retrouve ces probabilités en effectuant le calcul d_2A.

3. Démontrer par récurrence sur l'entier n que la matrice ligne $d_n = (P(M_n) \quad P(L_n) \quad P(C_n))$ est donnée par $d_n = d_1A^{n-1}$.

4. Déterminer la probabilité que cette personne passe Noël 2012 à Lille. Répondre à la même question si l'on sait qu'elle était à Lille en janvier 2012.

Cours 2

Multiplication de deux matrices

À noter
On peut retenir cette opération en remarquant l'analogie avec un produit scalaire.

Définition

Soit $A = (a_1\ a_2\ \dots\ a_p)$ une matrice ligne à p colonnes et $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_p \end{pmatrix}$ une matrice colonne à p lignes.

Le **produit A × B** est une matrice de dimension 1×1.
Son unique élément est égal à $a_1 b_1 + a_2 b_2 + \dots + a_p b_p$.

Exemple : $(2\ \ 3) \times \begin{pmatrix} 4 \\ 7 \end{pmatrix} = (2 \times 4 + 3 \times 7) = (29)$

Définition Soit A une matrice de dimension $n \times p$ et X une matrice colonne ayant p lignes.
La matrice produit $A \times X$, notée aussi AX, est une matrice colonne de n lignes.
L'élément de la ligne i de cette matrice est l'unique élément du produit L_iX où L_i est la ligne i de la matrice A.

Exemple : Soit $A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{pmatrix}$ et X la matrice colonne $X = \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$.

Pour $i = 1$ ou $i = 2$, on a :

$$L_iX = (a_{i,1}\ \ a_{i,2}\ \ a_{i,3}) \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = (2a_{i,1} + 3a_{i,2} + 4a_{i,3}),$$

d'où $AX = \begin{pmatrix} 2a_{1,1} + 3a_{1,2} + 4a_{1,3} \\ 2a_{2,1} + 3a_{2,2} + 4a_{2,3} \end{pmatrix}$.

Propriété Soit A une matrice de dimension $n \times p$, V et W des matrices colonnes de dimension $p \times 1$. Alors :
(1) $A(V + W) = AV + AW$ **(2)** pour tout réel k : $A(kV) = k(AV)$.

Démonstrations On le démontre pour une matrice à 2 colonnes.
(1) Soit L_1 la ligne 1 de la matrice A.
L'élément 1 de la matrice colonne de $A(V + W)$ est $L_1(V + W) = a_{1,1}(v_1 + w_1) + a_{1,2}(v_2 + w_2)$.
Et l'élément 1 de la matrice colonne $AV + AW$ est $(a_{1,1}v_1 + a_{1,2}v_2) + (a_{1,1}w_1 + a_{1,2}w_2)$.
Ces deux éléments sont égaux. On constate de même l'égalité des autres éléments.
(2) De façon analogue, l'élément 1 de la matrice colonne $A(kV)$ est $L_1(kV) = a_{1,1}(kv_1) + a_{1,2}(kv_2)$.
Et l'élément 1 de la matrice colonne $k(AV)$ est $k(a_{1,1}v_1 + a_{1,2}v_2)$.
Ces deux nombres sont bien égaux. Il en va de même pour les autres éléments de la matrice colonne.

Définition Soit A et B deux matrices carrées d'ordre n.
La matrice $A \times B$, notée aussi AB, est une matrice carrée d'ordre n.
Si $L_1, L_2, \dots, L_n$ sont les n lignes de A et $C_1, C_2, \dots, C_n$ les n colonnes de B, l'élément $p_{i,j}$ de la matrice produit AB est égal à l'unique élément de la matrice L_iC_j.

Exemple : $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} & a_{2,1}b_{1,2} + a_{2,2}b_{2,2} \end{pmatrix}$.

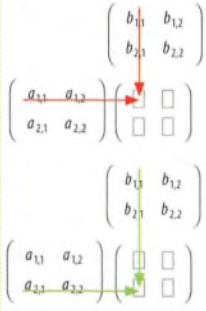
On a par exemple obtenu l'élément $p_{1,2}$ de la matrice produit avec le calcul :

$$L_1C_2 = (a_{1,1}\ \ a_{1,2}) \begin{pmatrix} b_{1,2} \\ b_{2,2} \end{pmatrix} = (a_{1,1}b_{1,2} + a_{1,2}b_{2,2}).$$

Remarque : On peut généraliser la notion de produit de A par B à certains cas de matrices non nécessairement carrées lorsque le nombre de colonnes de A est égal au nombre de lignes de B.

Propriétés Soit A, B et C des matrices carrées d'ordre n et k un réel. Alors :
(1) $A(BC) = (AB)C$ (associativité de la multiplication)
(2) $k(AB) = (kA)B = A(kB)$
(3) $A(B + C) = AB + AC$, $(A + B)C = AC + BC$ (distributivité)

À noter
Il est utile de poser le calcul du produit de deux matrices de la façon suivante :



etc...

À noter
Pour démontrer ces résultats, on vérifie que les éléments des matrices des membres droits sont les mêmes que ceux des matrices des membres gauches.

Savoir-faire 6

➤ Voir l'exercice 45

Multiplier une matrice par une matrice colonne

Une entreprise fabrique deux types de fauteuil nommés Qoänk et Tulska.
Le fauteuil Qoänk a un coût de 99 € l'unité, le fauteuil Tulska a un coût de 150 €.
L'état des stocks dans leurs deux magasins de la région PACA est donné par le tableau ci-dessous :

	Magasin de Marseille	Magasin de Toulon
Fauteuil Qoänk	52	45
Fauteuil Tulska	34	37

Donner la valeur des stocks (en €) de chaque magasin.

Méthode
Pour effectuer le produit d'une matrice A par une matrice colonne X on effectue le produit de chaque ligne de A par la matrice colonne X.

Solution

L'état des stocks est représenté par la matrice $S = \begin{pmatrix} 52 & 34 \\ 45 & 37 \end{pmatrix}$

et les prix des fauteuils par la matrice colonne $P = \begin{pmatrix} 99 \\ 150 \end{pmatrix}$.

$SP = \begin{pmatrix} 52 & 34 \\ 45 & 37 \end{pmatrix}\begin{pmatrix} 99 \\ 150 \end{pmatrix}$, soit $S = \begin{pmatrix} 52\times 99 + 34\times 150 \\ 45\times 99 + 37\times 150 \end{pmatrix} = \begin{pmatrix} 10248 \\ 10005 \end{pmatrix}$.

Le magasin de Marseille a un stock de valeur 10 248 €, celui de Toulon un stock de valeur 10 005 €.

Remarque : On peut effectuer un produit de matrices sur calculatrice comme indiqué ci-dessous ou en définissant au préalable les matrices comme indiqué dans le savoir-faire 2.

Casio	Texas
Entrer [[52,34][45,37]]×[[99][150]].	Entrer [[52,34][45,37]]*[[99][150]].
[[52,34][45,37]]×[[99] [10248] [10005]]	[52 34] [45 37] * [99] [150] = [10248] [10005]

Savoir-faire 7

➤ Voir les exercices 46 et 47

Multiplier des matrices

Soit $A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 5 & 6 \\ 8 & 11 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 2 \\ 5 & 10 \end{pmatrix}$ et $D = \begin{pmatrix} 2 & -10 \\ -1 & 5 \end{pmatrix}$.

1. A-t-on AB = BA ? AC = CA ?
2. Calculer la matrice CD.

Conseil
Lorsqu'on manipule des produits de matrices, il ne faut pas oublier que les règles de calculs ne sont pas nécessairement les mêmes que pour le produit de réels. Par exemple, l'égalité BA = AB n'est valable que dans des cas très particuliers.

Solution

1. $AB = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 8 & 11 \end{pmatrix} = \begin{pmatrix} 2\times 5+3\times 8 & 2\times 6+3\times 11 \\ 4\times 5+5\times 8 & 4\times 6+5\times 11 \end{pmatrix} = \begin{pmatrix} 34 & 45 \\ 60 & 79 \end{pmatrix}$.

et $BA = \begin{pmatrix} 5 & 6 \\ 8 & 11 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 5\times 2+6\times 4 & 5\times 3+6\times 5 \\ 8\times 2+11\times 4 & 8\times 3+11\times 5 \end{pmatrix} = \begin{pmatrix} 34 & 45 \\ 60 & 79 \end{pmatrix}$.

On a donc AB = BA.

$AC = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 5 & 10 \end{pmatrix} = \begin{pmatrix} 2\times 1+3\times 5 & 2\times 2+3\times 10 \\ 4\times 1+5\times 5 & 4\times 2+5\times 10 \end{pmatrix} = \begin{pmatrix} 17 & 34 \\ 29 & 58 \end{pmatrix}$.

et $CA = \begin{pmatrix} 1 & 2 \\ 5 & 10 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 1\times 2+2\times 4 & 1\times 3+2\times 5 \\ 5\times 2+10\times 4 & 5\times 3+10\times 5 \end{pmatrix} = \begin{pmatrix} 10 & 13 \\ 50 & 65 \end{pmatrix}$.

On a donc AC ≠ CA.

2. $CD = \begin{pmatrix} 1 & 2 \\ 5 & 10 \end{pmatrix}\begin{pmatrix} 2 & -10 \\ -1 & 5 \end{pmatrix} = \begin{pmatrix} 1\times 2+2\times(-1) & 1\times(-10)+2\times 5 \\ 5\times 2+10\times(-1) & 5\times(-10)+10\times 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Cours 3

Puissances d'une matrice

À noter

Un élément de la diagonale d'une matrice diagonale n'est pas nécessairement non nul.

Définitions

(1) On appelle **diagonale** (ou **diagonale principale**) d'une matrice A les éléments $a_{i,j}$ de la matrice ayant un indice de ligne égal à l'indice de colonne.

(2) On appelle **matrice diagonale** une matrice carrée dont les éléments non diagonaux sont tous égaux à 0.

Exemple : La matrice $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ est diagonale, ses éléments diagonaux sont $d_{1,1} = 2$, $d_{2,2} = 1$ et $d_{3,3} = 5$.

Définition La matrice carrée d'ordre n dont les éléments diagonaux sont égaux à 1 et dont tous les autres éléments sont égaux à 0 est appelée **matrice unité.** Elle est notée $\mathbf{I_n}$.

Exemple : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Si $D = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ où a et b sont des réels non nuls et si $T = \begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix}$, alors :

$$DT = TD = I_2.$$

Propriété Pour toute matrice carrée A d'ordre n, on a $AI_n = I_nA = A$.

À noter

Le produit de matrices étant associatif, dans le produit $A \times A \times \ldots \times A$, l'ordre dans lequel les multiplications sont effectuées n'a pas d'importance.

Définition A désignant une matrice carrée, on définit A^2 par $A^2 = A \times A$.
Et pour un entier naturel p, on définit A^p par $A^p = \underbrace{A \times A \times \ldots \times A}_{p \text{ fois}}$.

Exemple : Soit $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, alors $A^2 = AA = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

et $A^3 = AA^2 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} = \begin{pmatrix} 37 & 54 \\ 81 & 118 \end{pmatrix}$.

On peut aussi calculer A^3 ainsi : $A^3 = A^2A = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 37 & 54 \\ 81 & 118 \end{pmatrix}$.

À noter

Par convention, pour une matrice carrée A d'ordre n non nulle : $A^0 = I_n$.

Propriété Soit D une matrice diagonale d'ordre n d'éléments diagonaux $d_{1,1}, d_{2,2}, \ldots, d_{n,n}$.
Pour tout entier $p \geqslant 1$, la matrice D^p est la matrice diagonale dont les éléments diagonaux sont $(d_{1,1})^p, (d_{2,2})^p, \ldots, (d_{n,n})^p$.

Démonstration On établit par récurrence la propriété pour les matrices diagonales d'ordre 2.

- **Initialisation.** La propriété est vraie pour $p = 1$.
- **Hérédité.** Soit $p \geqslant 1$ un entier pour lequel $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^p = \begin{pmatrix} a^p & 0 \\ 0 & b^p \end{pmatrix}$. On a alors :

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{p+1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^p \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a^p & 0 \\ 0 & b^p \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

d'où $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{p+1} = \begin{pmatrix} a^p \times a + 0 \times 0 & a^p \times 0 + 0 \times b \\ 0 \times a + b^p \times 0 & 0 \times 0 + b^p \times b \end{pmatrix} = \begin{pmatrix} a^{p+1} & 0 \\ 0 & b^{p+1} \end{pmatrix}$.

L'hérédité est ainsi établie.

Conclusion : La propriété est ainsi établie pour tout entier $n \geqslant 1$.

Exemple : $D = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$, $D^2 = \begin{pmatrix} a^2 & 0 & 0 \\ 0 & b^2 & 0 \\ 0 & 0 & c^2 \end{pmatrix}$ et $D^3 = \begin{pmatrix} a^3 & 0 & 0 \\ 0 & b^3 & 0 \\ 0 & 0 & c^3 \end{pmatrix}$.

Savoir-faire 8

➤ Voir les exercices 51 à 52

Calculer les puissances d'une matrice carrée

Soit $A = \begin{pmatrix} 0,4 & 0,6 \\ 0,3 & 0,7 \end{pmatrix}$.

1. Calculer $3A^2$, $3A^3$, $3A^4$ et $3A^5$ à l'aide de la calculatrice.

2. Conjecturer une expression des éléments de la matrice $3A^n$ en fonction de n.

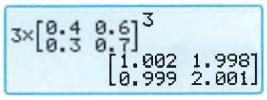
3. En déduire par récurrence les éléments de la matrice A^n pour tout entier naturel n.

Conseil
Pour déterminer les éléments de A^n, on peut calculer les premières puissances de A et dans certains cas conjecturer l'expression des éléments.

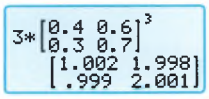
Solution

1. On trouve $3A^2 = \begin{pmatrix} 1,02 & 1,98 \\ 0,99 & 2,01 \end{pmatrix}$, $3A^3 = \begin{pmatrix} 1,002 & 1,998 \\ 0,999 & 2,001 \end{pmatrix}$,

$3A^4 = \begin{pmatrix} 1,0002 & 1,9998 \\ 0,9999 & 2,0001 \end{pmatrix}$ et $3A^5 = \begin{pmatrix} 1,00002 & 1,99998 \\ 0,99999 & 2,00001 \end{pmatrix}$.



Casio



Texas

2. Avec ce qui précède, on conjecture que pour tout entier $n \geqslant 2$, on a :

$$3A^n = \begin{pmatrix} 1+2\times10^{-n} & 2-2\times10^{-n} \\ 1-10^{-n} & 2+10^{-n} \end{pmatrix}.$$

3. **Initialisation.** L'initialisation est faite à la question précédente.

Hérédité. Soit $n \geqslant 2$ un entier pour lequel on suppose que $3A^n$ a la forme conjecturée.

On a alors $3A^{n+1} = 3A^n \times A = \begin{pmatrix} 1+2\times10^{-n} & 2-2\times10^{-n} \\ 1-10^{-n} & 2+10^{-n} \end{pmatrix}\begin{pmatrix} 0,4 & 0,6 \\ 0,3 & 0,7 \end{pmatrix}$.

Détaillons le calcul de l'élément ligne 1, colonne 1 :

$$(1+2\times10^{-n} \quad 2-2\times10^{-n})\begin{pmatrix} 0,4 \\ 0,3 \end{pmatrix} = \left((1+2\times10^{-n})\times0,4 + (2-2\times10^{-n})\times0,3\right).$$

Cet élément est donc égal à $1+0,2\times10^{-n} = 1+2\times10^{-n-1}$.

En procédant de même pour chaque élément, on prouve l'hérédité de la propriété.

Conclusion : La conjecture est ainsi établie par récurrence et :

$$A^n = \frac{1}{3}\begin{pmatrix} 1+2\times10^{-n} & 2-2\times10^{-n} \\ 1-10^{-n} & 2+10^{-n} \end{pmatrix} \text{ pour tout entier } n \geqslant 1.$$

Savoir-faire 9

➤ Voir les exercices 54 et 55

Utiliser la puissance n-ième d'une matrice

Deux suites (u_n) et (v_n) sont définies par $u_0 = a$, $v_0 = b$ et, pour tout entier $n \geqslant 1$, par :

$$u_n = 0,4\,u_{n-1} + 0,6\,v_{n-1} \text{ et } v_n = 0,3\,u_{n-1} + 0,7\,v_{n-1}.$$

Exprimer u_n et v_n en fonction de n lorsque $a = 2$ et $b = 3$.

Méthode
Pour exprimer en fonction de n les termes de suites définies par une relation de récurrence de la forme $\begin{pmatrix} u_n \\ v_n \end{pmatrix} = A\begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix}$, on peut utiliser les puissances de la matrice A.

Solution

Avec la matrice A du savoir-faire 8, on a : $\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} 0,4 & 0,6 \\ 0,3 & 0,7 \end{pmatrix}\begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix} = A \times \begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix}$.

On en déduit $\begin{pmatrix} u_n \\ v_n \end{pmatrix} = A \times A\begin{pmatrix} u_{n-2} \\ v_{n-2} \end{pmatrix} = A^2\begin{pmatrix} u_{n-2} \\ v_{n-2} \end{pmatrix}$ et de même :

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = A \times A^2\begin{pmatrix} u_{n-2} \\ v_{n-2} \end{pmatrix} = A^3\begin{pmatrix} u_{n-3} \\ v_{n-3} \end{pmatrix} = \ldots = A^n\begin{pmatrix} u_0 \\ v_0 \end{pmatrix}.$$

Soit $\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1+2\times10^{-n} & 2-2\times10^{-n} \\ 1-10^{-n} & 2+10^{-n} \end{pmatrix}\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ ou encore $\begin{cases} u_n = \frac{1}{3}(8-2\times0,1^n) \\ v_n = \frac{1}{3}(8+0,1^n) \end{cases}$, $n \in \mathbb{N}$.

Problème 5

Somme de puissances d'entiers

TICE

Objectif

Découvrir la notion d'inverse d'une matrice et son utilisation pour la résolution d'un système.

Cours 4
Matrice inverse

Partie A. Somme $1^3 + 2^3 + \ldots + n^3$

Sachant que $\sum_{j=1}^{n} j = \frac{1}{2}n(n+1)$ et $\sum_{j=1}^{n} j^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$, on conjecture que la suite $n \mapsto S(n) = 1^3 + 2^3 + \ldots + n^3$ est un polynôme de degré 4.

On cherche donc un polynôme de degré 4 $f : x \mapsto ax^4 + bx^3 + cx^2 + dx + e$ coïncidant avec S pour tout entier naturel n non nul.

Comme il y a cinq coefficients inconnus, on va chercher à imposer à ce polynôme 5 images :

$$f(1) = S(1), f(2) = S(2), \ldots, f(5) = S(5).$$

1. Vérifier que la recherche des réels a, b, c, d et e tels que les égalités précédentes soient satisfaites revient à chercher des nombres a, b, c, d et e tels que :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 16 & 8 & 4 & 2 & 1 \\ 81 & 27 & 9 & 3 & 1 \\ 256 & 64 & 16 & 4 & 1 \\ 625 & 125 & 25 & 5 & 1 \end{pmatrix} X = K \text{ où } X = \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} \text{ et } K = \begin{pmatrix} 1 \\ 9 \\ 36 \\ 100 \\ 225 \end{pmatrix}.$$

2. Avec le logiciel Xcas, on effectue les calculs ci-contre.

a. Expliquer pourquoi, avec ces résultats, on peut affirmer que l'équation $AX = K$ est équivalente à $X = BK$.

b. Vérifier que le produit BK est égal à la matrice colonne dont les éléments sont $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$, 0 et 0.

c. Quelle expression pour le polynôme f a-t-on ainsi obtenue ?

3. On effectue ensuite le calcul suivant avec Xcas :

f(x):=1/4*x^4+1/2*x^3+1/4*x^2;
x -> $(\frac{1}{4})*x^4+(\frac{1}{2})*x^3+(\frac{1}{4})*x^2$
simplifier(f(n)-f(n-1))
n^3

Montrer en quoi ce résultat permet de valider la conjecture :

« Pour tout naturel non nul n, $S(n) = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2$ ».

4. Pour tout entier naturel n non nul, on pose $T(n) = 1^3 + 3^3 + \ldots + (2n+1)^3$.

$T(n)$ est donc la somme des cubes des $n+1$ premiers entiers impairs.

a. Calculer $T(1)$, $T(2)$, $T(3)$, $T(4)$ et $T(5)$.

b. On conjecture que T est une fonction polynôme g de degré 4.

Expliquer pourquoi la matrice B précédente permet également de déterminer les coefficients de ce polynôme g et vérifier que :

$$g(n) = 2n^4 + 8n^3 + 11n^2 + 6n + 1.$$

c. Quel calcul peut-on effectuer avec Xcas pour établir rapidement que l'on a bien $T(n) = g(n)$ pour tout naturel non nul n ?

Fichier logiciel
03_TSspe_probleme5.xws
www. bordas-indice.fr

Partie B. Somme $1^2 + 3^2 + \ldots + (2n+1)^2$

Pour tout entier naturel n non nul, on pose $V(n) = 1^2 + 3^2 + \ldots + (2n+1)^2$.

Adapter la démarche précédente pour établir à l'aide du logiciel Xcas que V est une fonction polynôme de degré 3 que l'on explicitera.

Cours 4

Matrice inverse

Définition Soit A une matrice carrée d'ordre n.
S'il existe une matrice B telle que $AB = BA = I_n$, alors la matrice A est dite **inversible**.

Exemple : Soit $A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 0,8 & -0,2 \\ -0,6 & 0,4 \end{pmatrix}$.

On vérifie que $AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, donc A est inversible.

Propriété Il existe des matrices non nulles non inversibles.

Exemple : Soit $A = \begin{pmatrix} 2 & 10 \\ 4 & 20 \end{pmatrix}$. On a : $A\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ et $A\begin{pmatrix} 0 \\ 0,2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$.

S'il existait une matrice B telle que $BA = I_2$, on aurait $BA \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} = BA \times \begin{pmatrix} 0 \\ 0,2 \end{pmatrix}$,

soit $I_2\begin{pmatrix} 1 \\ 0 \end{pmatrix} = I_2\begin{pmatrix} 0 \\ 0,2 \end{pmatrix}$, soit $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0,2 \end{pmatrix}$.

Ceci est impossible, donc A n'est pas inversible.

Logique
On a raisonné par l'absurde pour montrer que A n'est pas inversible.

Propriété (admise) Soit A une matrice carrée d'ordre n.
Si B est une matrice carrée d'ordre n telle que $AB = I_n$, alors $BA = I_n$.
Et réciproquement si $BA = I_n$, alors $AB = I_n$.

À noter
La matrice inverse de A, lorsqu'elle existe, est nécessairement carrée et de même ordre que A.

Ce résultat n'a rien d'évident puisqu'en général, pour deux matrices A et B, on a $AB \neq BA$.

Propriété Soit A une matrice carrée d'ordre n.
Si B est une matrice telle que $AB = I_n$ et C une matrice telle que $CA = I_n$, alors $C = B$.
En particulier, une matrice inversible A a une unique matrice **inverse**, notée A^{-1} : $AA^{-1} = A^{-1}A = I_n$.

Démonstration Si $AB = I_n$, on a $C(AB) = CI_n$ en multipliant chaque membre par C, donc $C(AB) = C$.
Or $C(AB) = (CA)B = I_nB = B$ car pour toute matrice d'ordre n $I_nB = B$, d'où l'égalité $C = B$.

À noter
Pour vérifier que B est inverse de A, il suffit de vérifier que $AB = I_n$ ou de vérifier que $BA = I_n$.

Exemple : Soit A la matrice définie par $A = \begin{pmatrix} 11 & 2 \\ 16 & 3 \end{pmatrix}$ et x et y des réels.

Si $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$ alors pour toute matrice B : $BA\begin{pmatrix} x \\ y \end{pmatrix} = B\begin{pmatrix} u \\ v \end{pmatrix}$.

Si A admet une matrice inverse B, $BA = I_n$ et on aura donc $\begin{pmatrix} x \\ y \end{pmatrix} = B\begin{pmatrix} u \\ v \end{pmatrix}$.

L'égalité $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$ s'écrit : $\begin{cases} 11x + 2y = u \\ 16x + 3y = v \end{cases}$

En calculant x et y en fonction de u et v, on obtient : $\begin{cases} x = 3u - 2v \\ y = -16u + 11v \end{cases}$

On pose alors $B = \begin{pmatrix} 3 & -2 \\ -16 & 11 \end{pmatrix}$; A est donc inversible et la matrice B est son inverse.

À noter
La matrice nulle n'est pas inversible.

Propriété Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2, non nulle.
A est inversible si, et seulement si, le nombre $ad - bc$ est non nul.

Démonstration Soit $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Le calcul de AB donne $AB = \delta I_2$ où $\delta = ad - bc$.
Si $\delta \neq 0$, on a donc $A \times (\delta^{-1}B) = I_2$, donc A est inversible d'inverse $\delta^{-1}B$.
Si $\delta = 0$ alors $AB = 0_2$, donc A n'est pas inversible.
En effet si A était inversible d'inverse C, on aurait $CAB = I_2B = B$ et $CAB = C0_2 = 0_2$.
B serait donc la matrice nulle 0_2, ce qui n'est pas le cas.

Cours 5

Systèmes linéaires

Vocabulaire

L'écriture $AX = B$ est appelée **écriture matricielle du système.**

Définition Un système linéaire d'inconnues $x_1, x_2, \ldots, x_p$ est un système d'équations pouvant s'écrire sous la forme $AX = B$, où A est une matrice de dimension $n \times p$, B une matrice colonne de n lignes et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$.

Un système linéaire peut donc s'écrire sous la forme :

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,p}x_p = b_1 \\ \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,p}x_p = b_n \end{cases}$$

Exemple : Le système $\begin{cases} x + 2y = 6 \\ 3x + 2y = 5 \end{cases}$ s'écrit $AX = B$, avec $A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} 6 \\ 5 \end{pmatrix}$.

Logique

La contraposée de cette implication permet d'établir qu'une matrice n'est pas inversible : « Si un système linéaire ne possède aucune solution ou en possède plusieurs, alors la matrice associée n'est pas inversible ».

Propriété Si un système linéaire a pour écriture matricielle $AX = B$, où A est une matrice inversible d'ordre n et B une matrice colonne à n lignes, alors ce système possède une **solution unique**. Cette solution est donnée par $X = A^{-1}B$.

Démonstration Si $AX = B$ alors $A^{-1}AX = A^{-1}B$ d'où $X = A^{-1}B$: il y a donc au plus une solution.
Par ailleurs, $A(A^{-1}B) = (AA^{-1})B = B$: $A^{-1}B$ est donc bien solution.
$A^{-1}B$ est donc l'unique solution de l'équation $AX = B$.

Exemples :

- Reprenons les matrices $A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} 6 \\ 5 \end{pmatrix}$.

La matrice $A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$ est inversible avec $A^{-1} = \begin{pmatrix} -0{,}5 & 0{,}5 \\ 0{,}75 & -0{,}25 \end{pmatrix}$.

L'équation $AX = B$, d'inconnue X, est équivalente à $A^{-1}(AX) = A^{-1}B$, c'est-à-dire à $X = A^{-1}B = \begin{pmatrix} -0{,}5 \\ 3{,}25 \end{pmatrix}$. Le système $\begin{cases} x + 2y = 6 \\ 3x + 2y = 5 \end{cases}$, d'inconnue $(x\,;y)$, a donc une unique solution : le couple $(-0{,}5\,;3{,}25)$.

- Le système $\begin{cases} 2x + y = 4 \\ 6x + 3y = 12 \end{cases}$ admet une infinité de solutions : les couples $(t\,;4 - 2t)$ avec t réel quelconque. La matrice associée à ce système $A = \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix}$ n'est donc pas inversible.

- Considérons le système S $\begin{cases} x + 2y + 5z = 0 \\ 4x + 12y + 16z = 0 \\ 5x + 14y + 21z = 0 \end{cases}$ de matrice associée $A = \begin{pmatrix} 1 & 2 & 5 \\ 4 & 12 & 16 \\ 5 & 14 & 21 \end{pmatrix}$.

Les deux plans d'équations $x + 2y + 5z = 0$ et $4x + 12y + 16z = 0$ dans un repère de l'espace ont pour vecteurs normaux $\vec{n_{\mathscr{P}}}(1\,;2\,;5)$ et $\vec{n_{\mathscr{Q}}}(4\,;12\,;16)$. Ces deux vecteurs sont non colinéaires, les plans $\mathscr{P}$ et $\mathscr{Q}$ sont donc sécants suivant une droite (d).
On peut par ailleurs remarquer que la ligne L_3 de A s'écrit sous la forme : $L_3 = L_1 + L_2$.
Toute solution du système $\begin{cases} x + 2y + 5z = 0 \\ 4x + 12y + 16z = 0 \end{cases}$ est donc solution du système S.
En effet $x_0 + 2y_0 + 5z_0 = 0$ et $4x_0 + 12y_0 + 16z_0 = 0$ impliquent :

$$(x_0 + 2y_0 + 5z_0) + (4x_0 + 12y_0 + 16z_0) = 0 \text{ soit } 5x_0 + 14y_0 + 21z_0 = 0.$$

Le système S admet donc une infinité de solutions : la matrice A n'est pas inversible.

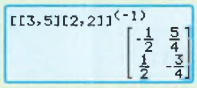
Propriété (admise) Si un système linéaire, d'écriture matricielle $AX = B$, où A est une matrice carrée, possède une solution unique, alors la matrice A est inversible.

Savoir-faire 10

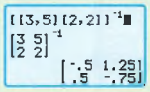
➤ Voir les exercices 65 et 66

Méthode
Pour déterminer l'inverse d'une matrice, on peut se ramener à la résolution d'un système.

Conseil
L'inverse d'une matrice peut être conjecturée à l'aide d'une calculatrice.



Casio



Texas

Déterminer l'inverse d'une matrice

Soit $A = \begin{pmatrix} 3 & 5 \\ 2 & 2 \end{pmatrix}$. Démontrer que A est inversible et déterminer sa matrice inverse.

Solution

On cherche une matrice $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telle que $AB = I_2$, c'est-à-dire telle que :

$$\begin{pmatrix} 3a+5c & 3b+5d \\ 2a+2c & 2b+2d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On cherche donc à déterminer quatre réels a, b, c et d tels que $\begin{cases} 3a+5c=1 \\ 3b+5d=0 \\ 2a+2c=0 \\ 2b+2d=1 \end{cases}$, c'est-à-dire tels que

$\begin{cases} 3a+5c=1 \\ a+c=0 \end{cases}$ et $\begin{cases} 3b+5d=0 \\ b+d=0,5 \end{cases}$.

Le premier système est équivalent à $\begin{cases} 3a-5a=1 \\ c=-a \end{cases}$, c'est-à-dire à $(a\,;c) = (-0,5\,;0,5)$.

Le second système est équivalent à $\begin{cases} 3b+5(0,5-b)=0 \\ d=0,5-b \end{cases}$, c'est-à-dire à $(b\,;d) = (1,25\,;-0,75)$.

La matrice inverse de A est donc la matrice $A^{-1} = \begin{pmatrix} -0,5 & 1,25 \\ 0,5 & -0,75 \end{pmatrix}$.

Savoir-faire 11

➤ Voir les exercices 33 et 34

Conseil
Lorsqu'on détermine l'inverse d'une matrice à l'aide de la calculatrice, veiller à contrôler l'exactitude de la réponse, des problèmes d'arrondis pouvant intervenir.

Résoudre un système à l'aide d'une matrice

Résoudre les systèmes S_1 $\begin{cases} x+2y=10 \\ 3x+y=20 \end{cases}$ et S_2 $\begin{cases} x+2y+3z=15 \\ 4x+5y+8z=22 \\ 12x+8y+14z=-7 \end{cases}$

Solution

Le système S_1 a pour écriture matricielle $AX = B$, avec $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$.

On peut utiliser les commandes de la calculatrice pour cette résolution.
On définit les matrices A et B comme indiqué au savoir-faire 2, puis on calcule $A^{-1}B$.

Casio	Texas
Mat A^-1×Mat B [6 2]	[A]^-1*[B] [6 2]

Le système S_2 a pour écriture matricielle $AX = B$ avec $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 8 \\ 12 & 8 & 14 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $B = \begin{pmatrix} 15 \\ 22 \\ -7 \end{pmatrix}$. En utilisant les commandes de la calculatrice, on obtient :

Casio	Texas
Mat A^-1×Mat B [-5/2 44 -47/2]	[A]^-1*[B] [-2.5 44 -23.5]

Exercices

Les exercices dont les numéros sont sur fond blanc sont corrigés à la fin du manuel.

POUR DÉMARRER

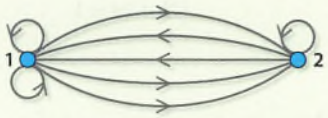
Définition d'une matrice

1 Soit $A = \begin{pmatrix} 0{,}7 & 0{,}2 & 0{,}1 \\ 0{,}8 & 0{,}15 & 0{,}05 \end{pmatrix}$.

1. Identifier les coefficients $a_{1,2}$, $a_{2,1}$ et $a_{2,3}$.
2. Entrer la matrice A dans la calculatrice.
3. Calculer la somme des éléments de la colonne 1 de cette matrice avec les outils de la calculatrice.

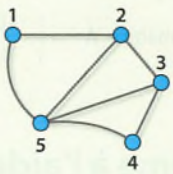
→ Pour vous aider Savoir-faire 2, p. 82

2 La figure ci-dessous schématise le nombre de liens internes à deux sites web ou reliant ces deux sites.



Définir la matrice A telle que l'élément $a_{i,j}$ de cette matrice est le nombre de liens du site i vers le site j.

3 Chaque matin, parmi cinq élèves d'une même classe de Terminale, certains se serrent la main, et d'autres non, selon le schéma ci-contre. On définit la matrice A des poignées de mains comme suit : l'élément $a_{i,j}$ de A vaut 1 si l'élève i a serré la main à l'élève j et 0 sinon.



1. Donner la matrice A.
2. Justifier l'égalité $a_{i,j} = a_{j,i}$ valable pour tous i et j entre 1 et 5.

4 Soit A la matrice carrée d'ordre 3 dont chaque élément $a_{i,j}$ est égal au reste de la division euclidienne de $i + j$ par 3. Donner la matrice A.

5 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$.

1. Identifier le nombre $a_{1,3}$ et le nombre $a_{3,1}$.
2. Calculer $\sum_{j=1}^{3} a_{j,j}$.
3. Calculer $\sum_{j=1}^{3} a_{2,j}$.
4. Calculer $\sum_{j=1}^{3} a_{4-j,j}$.

6 B est une matrice carrée d'ordre 3. Pour tous i et j compris entre 1 et 3, le coefficient $a_{i,j}$ de la matrice B est donné par $a_{i,j} = i + j$. Écrire la matrice B.

7 On appelle trace d'une matrice la somme des éléments de sa diagonale principale. Soit A une matrice carrée d'ordre n ($n \geqslant 2$), dont chacun des coefficients $a_{i,j}$ est donné par l'égalité :

$$a_{i,j} = \frac{1}{2}(i + j).$$

Exprimer la trace de A en fonction de n.

8 A est une matrice carrée d'ordre 4. Pour tous i et j compris entre 1 et 4, le coefficient $a_{i,j}$ de la matrice A est donné par $a_{i,j} = i - j$. Écrire la matrice A.

Additions de matrices et multiplication par un réel

9 Soit $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

Calculer la matrice $10I_2 - 7J$.

10 Soit $A = \begin{pmatrix} -1 & \sqrt{2} \\ 10 & 0{,}5 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & \frac{2}{3} \\ -5{,}1 & \pi \end{pmatrix}$.

Calculer les matrices $3A$ et $-2A - B$.

11 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 & 1 \\ 2 & -3 & 4 \\ -5 & 3 & 1 \end{pmatrix}$.

Calculer la matrice $2A - B$.

12 Soit a un réel strictement positif et :

$$A = \begin{pmatrix} \ln(a) & \ln(a^2) \\ \ln(a^3) & \ln(a^4) \end{pmatrix}.$$

Identifier la matrice carrée B telle que $A = \ln(a)\,B$.

13 Soit A la matrice carrée d'ordre 3 telle que pour tous i et j compris entre 1 et 3, on a $a_{i,j} = i$. Soit B la matrice carrée d'ordre 3 telle que pour tous i et j compris entre 1 et 3, on a $b_{i,j} = j^2$. Calculer la matrice $2A - 3B$.

14 Entrer les matrices :

$A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 6 \end{pmatrix}$ dans la calculatrice.

1. À l'aide de la calculatrice, ajouter ces deux matrices.
2. Quelle est la réponse de la calculatrice ? Expliquer.

Produit d'une matrice par une matrice colonne

15 Soit $A = \begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix}$ et $X = \begin{pmatrix} -2 \\ 4 \end{pmatrix}$.

Calculer la matrice produit AX, sans calculatrice.

16 À un point M $(x\,;y)$ du plan muni d'un repère, on associe le point M' $(x'\,;y')$ de coordonnées $(x'\,;y') = (x + 2y\,;-x + y)$.

Exprimer la matrice colonne $\begin{pmatrix} x' \\ y' \end{pmatrix}$ sous la forme $A\begin{pmatrix} x \\ y \end{pmatrix}$ où A est une matrice à identifier.

17 À tout point M $(x\,;y)$ du plan muni d'un repère, on associe le point M' $(x'\,;y')$ tel que :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Identifier la transformation ainsi définie.

18 Soit $A=\begin{pmatrix}1&2&3\\2&4&6\\-3&-6&-9\end{pmatrix}$ et $X=\begin{pmatrix}2\\2\\-2\end{pmatrix}$.

Calculer AX.

19 Un investisseur possède des titres en Bourse.
Les valeurs en euros de ces titres à différentes dates sont :

	Valeur du titre A	Valeur du titre B	Valeur du titre C
Date 1	2,48	11,51	22,22
Date 2	2,87	10,48	20,15

L'investisseur possède 500 titres A, 250 titres B et 320 titres C.
Déterminer la matrice colonne dont l'élément i est la valeur totale en euros détenue par l'investisseur à la date i.
Écrire cette matrice sous la forme d'un produit de la matrice des valeurs (à définir) et de la matrice colonne des effectifs détenus.

20 Le plan est muni d'un repère orthonormé.
À tout point M d'affixe $z=a+ib$, on associe le point M' d'affixe $z'=a'+ib'$ tel que $z'=2z$.
Donner la matrice carrée d'ordre 2, notée A, telle que :

$$\begin{pmatrix}a'\\b'\end{pmatrix}=A\times\begin{pmatrix}a\\b\end{pmatrix}.$$

21 Soit $T=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

1. Dans un repère orthonormé du plan, placer les points :
A(2 ; 3), B(−1 ; 2), C(0 ; 5) et D(2 ; 2).

2. Placer ensuite les points A', B', C', D' tels que les coordonnées du point M $(x\,;y)$ soient liées aux coordonnées du point M' $(x'\,;y')$ par la relation $\begin{pmatrix}x'\\y'\end{pmatrix}=T\begin{pmatrix}x\\y\end{pmatrix}$.

3. Émettre une conjecture sur la nature de la transformation ainsi définie.

Produit de deux matrices

22 Soit $A=\begin{pmatrix}-1&2\\3&-5\end{pmatrix}$ et $B=\begin{pmatrix}2{,}1&0{,}5\\11&4\end{pmatrix}$.

Déterminer, sans calculatrice, le produit AB et le produit BA.

23 Soit $A=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}$ et $B=\begin{pmatrix}0&-1&1\\2&-3&4\\-5&3&1\end{pmatrix}$.

Déterminer les produits AB et BA.

24 Soit $A=\begin{pmatrix}1&e^2\\e^3&e^5\end{pmatrix}$ et $B=\begin{pmatrix}e&1\\0&e^2\end{pmatrix}$.

Calculer le produit AB et le produit BA.

25 Soit $A=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ et $B=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ une matrice carrée d'ordre 2. Quel lien existe-t-il entre les matrices B et AB ?

26 Soit $A=\begin{pmatrix}3&4\\5&6\end{pmatrix}$ et $B=\begin{pmatrix}2&7\\8&9\end{pmatrix}$.

1. Vérifier par le calcul que l'on a bien $A+B=B+A$.

2. A-t-on $AB=BA$?

Puissances de matrices

27 Soit $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}$.

1. Calculer A^2.

2. En déduire A^n pour tout entier naturel n non nul.

28 Soit $A=\begin{pmatrix}\cos a&-\sin a\\\sin a&\cos a\end{pmatrix}$.

Vérifier que $A^2=\begin{pmatrix}\cos(2a)&-\sin(2a)\\\sin(2a)&\cos(2a)\end{pmatrix}$.

Inverse d'une matrice

29 La matrice $A=\begin{pmatrix}7&5\\3&2\end{pmatrix}$ est-elle inversible ?

30 Montrer que l'inverse de la matrice $A=\begin{pmatrix}2&3\\5&8\end{pmatrix}$ est la matrice $B=\begin{pmatrix}8&-3\\-5&2\end{pmatrix}$.

31 La matrice $A=\begin{pmatrix}2&-0{,}3333333333333333\\-2&\frac{1}{3}\end{pmatrix}$ est-elle inversible ?

On répondra sans calculatrice, puis on vérifiera la réponse de la calculatrice. Que peut-on en conclure ?

32 1. Déterminer l'inverse de la matrice $A=\begin{pmatrix}1&2\\3&5\end{pmatrix}$ à l'aide de la calculatrice.

2. Entrer la matrice $B=\begin{pmatrix}1&2+10^{-15}\\3&5\end{pmatrix}$ et chercher à déterminer son inverse avec la calculatrice.

3. Un enseignant affirme à ses élèves : « Attention, avec votre calculatrice, vous ne pourrez qu'établir des conjectures sur l'expression de la matrice inverse ». Justifier cet avertissement.

33 Déduire de l'exercice **32** la solution du système :

$$\begin{cases}x+2y=3\\3x+5y=9\end{cases}$$

→ Pour vous aider Savoir-faire 11, p. 93

34 Résoudre le système $\begin{cases}2x+3y+4z=5\\6x+7y+8z=9\\12x+11y+13z=14\end{cases}$ en utilisant l'inverse d'une matrice à déterminer, cette matrice inverse étant calculée à l'aide de la calculatrice.

→ Pour vous aider Savoir-faire 11, p. 93

POUR S'ENTRAÎNER

Définition d'une matrice

35 La matrice $A = \begin{pmatrix} 0,7 & 0,2 & 0,1 \\ 0,8 & 0,15 & 0,05 \end{pmatrix}$ donne la répartition des fréquences pour les choix de langue 1 (colonne 1 : anglais, colonne 2 : espagnol, colonne 3 : allemand) dans un lycée pour les filles (ligne 1) et les garçons (ligne 2).
Ainsi l'égalité $a_{1,2} = 0,2$ signifie que 20 % des filles ont choisi l'espagnol en langue 1. Le lycée compte 800 filles et 700 garçons.

1. Donner la matrice de dimension 2×3 correspondant aux effectifs.

2. Donner une matrice ligne à trois éléments donnant les fréquences d'élèves dans l'établissement pour chacune des langues.

→ Pour vous aider Savoir-faire 1, p. 82

36 Une matrice carrée d'ordre 4 est telle que $a_{i,j} = i(4 - j)$ pour tous i et j compris entre 1 et 4. Écrire cette matrice.

37 Sept personnes se réunissent.
Certains échangent des poignées de mains, et d'autres non.
Soit A la matrice carrée d'ordre 7 telle que $a_{i,j} = 1$ si la personne i a serré la main à la personne j et $a_{i,j} = 0$ sinon.
Peut-on organiser les rencontres de façon à ce que la somme des coefficients de la matrice soit un entier impair ?

AIDE : Comment pourrait-on interpréter cette somme ?

Additions de matrices, multiplication par un réel

38 Une personne possède deux magasins de jouets. Avant Noël, les stocks du magasin A (colonne 1) et du magasin B (colonne 2) de consoles PS Vita (ligne 1) et 3DS (ligne 2) sont donnés par la matrice :

$$S = \begin{pmatrix} 6 & 8 \\ 4 & 2 \end{pmatrix}.$$

Le propriétaire décide d'augmenter de 50 % chaque stock. Donner, en fonction de S, la nouvelle matrice des stocks.

→ Pour vous aider Savoir-faire 4, p. 83

39 Après réflexion, le propriétaire de l'exercice précédent décide d'augmenter d'une dizaine d'unités pour chaque type de console le stock de chacun des magasins.
Traduire cette décision à l'aide d'une opération sur les matrices.

→ Pour vous aider Savoir-faire 3, p. 83

40 Soit $A = \begin{pmatrix} 1 & 3 \\ 2 & 10 \end{pmatrix}$, $J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} -2 & 4 \\ 6 & 25 \end{pmatrix}$.
Déterminer deux réels s et t tels que $B = sJ + tA$.

→ Pour vous aider Savoir-faire 5, p. 83

41 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 8 & 7 & 6 \\ 15 & 16 & 17 \end{pmatrix}$ et $B = \begin{pmatrix} 8 & 10 & 15 \\ 40 & 38 & 30 \\ 75 & 80 & 88 \end{pmatrix}$.
Établir que la matrice B s'écrit sous la forme $sI_3 + tA$, où s et t sont des réels à déterminer.

→ Pour vous aider Savoir-faire 5, p. 83

42 Soit x un réel :

$$A = \begin{pmatrix} \frac{e^x + 3}{e^x} & \frac{4}{e^x} \\ \frac{5}{e^x} & \frac{e^x + 6}{e^x} \end{pmatrix} \text{ et } B = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Montrer que A peut s'écrire sous la forme $A = sI_2 + tB$, où s et t sont des réels à déterminer.

VRAI – FAUX

Pour les exercices 43 et 44, indiquer si les affirmations sont vraies ou fausses, puis justifier.

43 Si A et B sont deux matrices de même dimension à éléments tous entiers et s et t sont deux entiers premiers entre eux tels que $sA = tB$, alors la matrice B s'écrit sous la forme sM où M est une matrice à coefficients entiers.

44 Pour toute matrice A et tout réel s, si sA est la matrice nulle alors $s = 0$ ou A est la matrice nulle.

Produits et puissances de matrices

45 Trois élèves de Terminale S inscrits en spécialité mathématiques ont obtenu les notes suivantes :

	Mathématiques	Sciences Physiques	SVT
Candidat 1	$a_{1,1} = 17$	$a_{1,2} = 16$	$a_{1,3} = 12$
Candidat 2	$a_{2,1} = 19$	$a_{2,2} = 19$	$a_{2,3} = 15$
Candidat 3	$a_{3,1} = 14$	$a_{3,2} = 15$	$a_{3,3} = 18$

Les coefficients au baccalauréat pour ces disciplines sont donnés par le tableau :

Mathématiques	$c_1 = 9$
Sciences Physiques	$c_2 = 6$
SVT	$c_3 = 6$

Calculer la matrice colonne dont l'élément i est la moyenne du candidat i. Traduire ce calcul par le produit d'une matrice par une matrice colonne à définir.

→ Pour vous aider Savoir-faire 6, p. 87

46 Soit $A = \begin{pmatrix} 1 & 3 \\ -4 & 7 \end{pmatrix}$ et $B = \begin{pmatrix} 5 & 6 \\ 11 & 2 \end{pmatrix}$.
Est-ce que $AB = BA$?

→ Pour vous aider Savoir-faire 7, p. 87

47 Soit $A = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$ et $C = \begin{pmatrix} 29 & 36 \\ 45 & 56 \end{pmatrix}$.

1. Vérifier que $AC = CA$.

2. Vérifier que $C = A^2$.

En déduire une justification sans calcul de l'égalité $CA = AC$.

→ Pour vous aider Savoir-faire 7, p. 87

48 Soit $A = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$.

Déterminer toutes les matrices B de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $AB = BA$.

49 Soit $A = \begin{pmatrix} -2 & 8 \\ 1 & -4 \end{pmatrix}$.

Déterminer deux matrices non nulles B carrées d'ordre 2 telles que $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

50 TRAVAIL EN AUTONOMIE

Énoncé

Soit $A = \begin{pmatrix} 2 & 6 & 1 \\ 3 & 9 & 1{,}5 \\ 5 & 15 & 2{,}5 \end{pmatrix}$.

On note C_1, C_2 et C_3 les colonnes de A.

1. Vérifier qu'il existe des réels x et y tels que :
$$C_2 = xC_1 \text{ et } C_3 = yC_1.$$

2. En déduire une écriture de A sous la forme d'un produit d'une matrice colonne par une matrice ligne.

Solution

1. On a $C_2 = 3C_1$ et $C_3 = 0{,}5C_1$.

2. A est de la forme $\begin{pmatrix} a & 3a & 0{,}5a \\ b & 3b & 0{,}5b \\ c & 3c & 0{,}5c \end{pmatrix}$.

On a donc $A = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{pmatrix} 1 & 3 & 0{,}5 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0{,}5 \end{pmatrix}$.

51 Soit $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Calculer les matrices A^2, A^3 et A^4.

2. En déduire la matrice A^n pour tout entier naturel n non nul.

→ Pour vous aider Savoir-faire 8, p. 89

52 Soit $A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$.

1. À l'aide de la calculatrice, déterminer A^2 et A^3.

2. En déduire, pour tout entier $n \geqslant 1$, les éléments de la matrice A^n.

→ Pour vous aider Savoir-faire 8, p. 89

53 Soit $A = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$.

1. Calculer A^2, A^3, A^4 et A^5 à l'aide de la calculatrice.

2. En déduire les éléments de la matrice A^n en fonction de n pour tout entier $n \geqslant 1$.

AIDE : Raisonner suivant les valeurs de n modulo 4.

54 Soit a un réel. Soit (u_n) et (v_n) deux suites telles que $u_0 = 2$ et $v_0 = 1$, et pour tout entier $n \geqslant 1$:
$$u_n = a\,u_{n-1} + v_{n-1} \text{ et } v_n = a\,v_{n-1}.$$

1. Identifier la matrice A telle que pour tout entier $n \geqslant 1$:
$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = A \begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix}.$$

2. Calculer les matrices A^2, A^3, A^4 et A^5.

3. Émettre une conjecture sur l'expression des éléments de la matrice A^n pour n entier naturel non nul, puis démontrer cette conjecture.

4. En déduire une expression de u_n et v_n en fonction de n.

→ Pour vous aider Savoir-faire 9, p. 89

55 Soit $A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Calculer les matrices A^2, A^3 et A^4.

2. En déduire les éléments de la matrice A^n en fonction de n pour tout entier $n \geqslant 1$.

3. Soit (u_n) et (v_n) deux suites telles que $u_0 = \pi$ et $v_0 = \sqrt{3}$, et pour tout entier $n \geqslant 1$:
$$u_n = -u_{n-1} - v_{n-1} \text{ et } v_n = u_{n-1}.$$
Exprimer u_n et v_n en fonction de n.

→ Pour vous aider Savoir-faire 9, p. 89

56 ALGO

Soit $A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

1. Soit n un entier naturel au moins égal à 1.
Conjecturer puis démontrer une expression de J^n en fonction de n et de la matrice J.

2. Exprimer A, A^2 et A^3 en fonction des matrices I et J.

3. Vérifier que pour tout entier naturel $n \geqslant 1$, on a :
$$A^n = I + \frac{5^n - 1}{2} J.$$

4. Soit (u_n) et (v_n) deux suites telles que $u_0 = 2$ et $v_0 = 4$, et pour tout entier $n \geqslant 1$:
$$u_n = 3\,u_{n-1} + 2\,v_{n-1} \text{ et } v_n = 2\,u_{n-1} + 3\,v_{n-1}.$$
a. Écrire un programme pour la calculatrice dont l'entrée est un entier naturel non nul n et affichant des valeurs approchées de u_n et v_n.
b. Exprimer u_n et v_n en fonction de n.

AIDE : question 4. b. Faire le lien avec la matrice A.

Exercices

57 Logique

Soit A et B deux matrices carrées d'ordre 2.

1. Vérifier que si $A = 0_2$ ou $B = 0_2$, alors $AB = BA = 0_2$.

2. La réciproque de cette implication est-elle vraie ?

58 Soit A la matrice définie par $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Conjecturer puis démontrer une expression des éléments de A^n pour n entier naturel non nul.

AIDE : On partagera l'étude en deux cas : cas où n est pair, cas où n est impair.

59 **TRAVAIL EN AUTONOMIE**

Énoncé

Soit $A = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$.

1. Déterminer les puissances de la matrice $B = \frac{1}{3}A$.

2. En déduire les puissances de la matrice A.

Solution

1. $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $B^2 = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = 2B$, $B^3 = \begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix} = 4B$ et $B^4 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix} = 8B$. On conjecture l'égalité $B^n = 2^{n-1}B$.

On la démontre alors par récurrence.

- **Initialisation.** Elle a été établie ci-dessus.
- **Hérédité.** Soit n un entier naturel pour lequel $B^n = 2^{n-1}B$.

Alors $B^{n+1} = 2^{n-1}B \times B = 2^{n-1}B^2 = 2^{n-1} \times 2B = 2^nB$.

Conclusion : $B^n = 2^{n-1}B$ pour tout entier $n \geqslant 1$.

2. De $A = 3B$, on déduit $A^n = 3^nB^n = 3^n \times 2^{n-1}B$.

60 Dans les tablettes de chocolat ChocoBon, on trouve des représentations de tableaux.

La série comporte trois images.

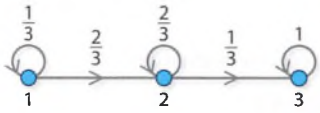
On considère que la probabilité d'obtenir une image lors de l'achat d'une tablette est égale à $\frac{1}{3}$.

1. Dresser un arbre de probabilités et déterminer la probabilité d'obtenir deux images différentes avec l'achat de deux tablettes.

2. À l'aide d'un arbre de probabilités, calculer la probabilité d'obtenir les trois images avec l'achat de trois tablettes.

3. Sur le schéma suivant, le nombre inscrit à côté d'un sommet correspond au nombre d'images distinctes obtenues.

Soit M la matrice dont l'élément $m_{i,j}$ est égal à la probabilité de passer de l'état i à l'état j lors de l'achat d'une nouvelle tablette. Cette probabilité est indiquée sur le schéma.



a. Justifier que le produit $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}M$ est égal à la matrice ligne dont les éléments sont les probabilités d'avoir 1, 2 ou 3 images distinctes après deux achats de tablettes.

b. Calculer et interpréter le produit $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}M^2$.

c. Quel calcul matriciel peut-on effectuer pour déterminer la probabilité d'avoir les trois images avec l'achat de six tablettes ? Effectuer ce calcul à l'aide de la calculatrice.

61 Soit $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ et $C = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$.

1. Calculer AC et CA.

2. Soit $M = A + C$. Démontrer que pour tout entier naturel non nul n, on a $M^n = A^n + C^n$.

3. Calculer les premières puissances de la matrice A à l'aide de la calculatrice et en déduire une expression de A^n en fonction de n.

4. Calculer les premières puissances de la matrice C à l'aide de la calculatrice. Conjecturer une expression de C^n en fonction de n (on séparera le cas n pair du cas n impair) et démontrer cette conjecture.

5. Déduire des questions précédentes une expression des éléments de M^n en fonction de l'entier naturel non nul n.

62 ALGO

Soit $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

1. Calculer A^2 et A^3 à l'aide de la calculatrice.

2. Vérifier que $A^3 = 2A + A^2$.

3. En déduire qu'il existe deux suites de nombres réels (a_n) et (b_n) telles que, pour tout entier $n \geqslant 3$, on a $A^n = a_nA + b_nA^2$ et établir que pour tout entier $n \geqslant 3$, on a $\begin{cases} a_{n+1} = 2b_n \\ b_{n+1} = a_n + b_n \end{cases}$

4. **a.** Démontrer que pour tout entier $n \geqslant 3$, on a :

$$b_{n+1} = b_n + 2b_{n-1}.$$

b. Déterminer b_3 et b_4.

c. Écrire un programme pour la calculatrice dont l'entrée est un entier naturel n non nul et calculant b_n.

d. On admet qu'il existe deux réels u et v tels que pour tout entier $n \geqslant 3$, on a $b_n = u \times (-1)^n + v \times 2^n$.

Déterminer les valeurs de u et v.

5. Exprimer, pour tout entier naturel $n \geqslant 3$, a_n en fonction de n.

VRAI – FAUX

Pour les exercices **63** et **64**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

63 Si A et B sont deux matrices carrées telles que le produit AB est la matrice nulle, alors A est la matrice nulle ou B est la matrice nulle.

64 Il existe des matrices A carrées d'ordre 2, distinctes de la matrice identité, telles qu'une puissance de A soit égale à la matrice identité.

Inverse d'une matrice

65 Soit $A = \begin{pmatrix} 3 & 11 \\ 2 & 5 \end{pmatrix}$.

Démontrer que A est inversible et déterminer l'inverse de la matrice A à l'aide de la résolution d'un système.

→ Pour vous aider Savoir-faire 10, p. 93

66 Soit $A = \begin{pmatrix} 5 & 7 \\ 12 & 3 \end{pmatrix}$.

Démontrer que A est inversible et déterminer l'inverse de la matrice A à l'aide de la résolution d'un système.

→ Pour vous aider Savoir-faire 10, p. 93

67 ALGO

Écrire un programme pour la calculatrice dont les entrées seront les quatre coefficients d'une matrice carrée d'ordre 2 et qui affichera en sortie le message « matrice inversible » ou « matrice non inversible » selon les cas.

68 Soit B une matrice de la forme :

$$B = \begin{pmatrix} -1 & 0 \\ m & 1 \end{pmatrix},$$

où m est un réel quelconque.

1. Calculer la matrice B^2.

2. En déduire que la matrice B est inversible et donner son inverse.

69 **TRAVAIL EN AUTONOMIE**

Énoncé

Soit $B = \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix}$.

1. Calculer B^2.

2. En déduire que B est inversible et donner sa matrice inverse.

Solution

1. On obtient $B^2 = I_3$.

2. On a $BB = I_3$. On en déduit que la matrice B est inversible et qu'elle est égale à son inverse.

70 Soit $A = \begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}$.

1. Déterminer les matrices A^2 et A^3.

2. En déduire que la matrice A est inversible et donner sa matrice inverse.

71 Logique

1. Démontrer l'implication : « Si la matrice A est inversible alors, pour tout entier naturel n, la matrice A^n est inversible ».

2. La réciproque est-elle vraie ?

72 Soit $A = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{pmatrix}$.

1. Vérifier qu'il existe deux réels a et b tels que $A^2 = aI_3 + bA$.

2. En déduire que la matrice A est inversible et donner son inverse.

73 Logique

Soit D une matrice diagonale d'ordre 3.

1. Montrer que si aucun des éléments de la diagonale de D n'est nul, alors D est inversible.
Expliciter les éléments de la matrice D^{-1} dans ce cas.

2. La réciproque de l'implication précédente est-elle vraie ?

74 Soit $A = \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 1 \\ -4 & 3 \end{pmatrix}$.

1. Déterminer la matrice P, inverse de Q, à l'aide de la calculatrice.

2. Calculer la matrice QAP.

3. En déduire, pour tout entier $n \geqslant 1$, les éléments de la matrice A^n.

AIDE : question 3. Exprimer A^n à l'aide de la matrice QAP.

VRAI – FAUX

Pour les exercices 75 et 76, indiquer si les affirmations sont vraies ou fausses, puis justifier.

75 Si A et B sont deux matrices inversibles, alors la matrice AB est inversible, d'inverse $A^{-1}B^{-1}$.

76 Si A et B sont deux matrices inversibles, alors la matrice $A + B$ est inversible.

Systèmes linéaires

77 On considère le système $\begin{cases} 5x + 4y = a \\ 10x + 7y = b \end{cases}$

1. Exprimer x et y en fonction de a et b en calculant, à l'aide de la calculatrice, l'inverse d'une matrice à identifier.

2. Dans un repère du plan, deux droites (d) et (d') ont pour équation $20x + 16y = 7$ et $10x + 7y = 15$.
Déterminer les coordonnées de leur point d'intersection à l'aide de la matrice inverse déterminée à la question précédente.

78 1. Résoudre le système linéaire $\begin{cases} 4x + 3y = 5 \\ 4x - 2y = 7 \end{cases}$

2. Soient x, y, a et b des réels tels que $\begin{cases} 4x + 3y = a \\ 4x - 2y = b \end{cases}$
Exprimer x et y en fonction de a et b.

3. Déterminer la matrice A de dimension 2×2 telle que :

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

4. Déduire des questions précédentes la matrice inverse de A.

79 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 3 & 1 & 0 \end{pmatrix}$.

1. À l'aide de la calculatrice, vérifier que A est inversible et obtenir son inverse.

2. Dans un repère orthonormé de l'espace, trois plans $\mathscr{P}$, $\mathscr{Q}$, $\mathscr{R}$ ont pour équations respectives :

$$x + 2y + 3z = 5, \quad x + y + 2z = 1 \quad \text{et} \quad 3x + y = 7.$$

Déduire de la question 1. l'intersection de ces trois plans.

Exercices

80 TRAVAIL EN AUTONOMIE

Énoncé

L'espace est muni d'un repère orthonormé.

Soit $\mathscr{P}$, $\mathscr{Q}$, $\mathscr{R}$ trois plans d'équations respectives :

$2x+3y+4z=5$, $x+2y+7z=1$ et $3x+5y+11z=6$.

1. Vérifier que la matrice $A=\begin{pmatrix}2&3\\1&2\end{pmatrix}$ est inversible et déterminer sa matrice inverse B.

2. En déduire la nature de l'intersection des deux plans $\mathscr{P}$ et $\mathscr{Q}$.

3. Soit C la matrice associée au système S_1 dont les trois équations sont celles des plans $\mathscr{P}$, $\mathscr{Q}$ et $\mathscr{R}$.
La matrice C est-elle inversible ?

Solution

1. Avec une calculatrice, on obtient $B=\begin{pmatrix}2&-3\\-1&2\end{pmatrix}$.

2. Le système S_2 $\begin{cases}2x+3y=5-4z\\x+2y=1-7z\end{cases}$ constitué des deux équations de plans $\mathscr{P}$ et $\mathscr{Q}$ s'écrit $A\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}5-4z\\1-7z\end{pmatrix}$, soit $\begin{pmatrix}x\\y\end{pmatrix}=B\begin{pmatrix}5-4z\\1-7z\end{pmatrix}$ ou encore $\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}13z+7\\-10z-3\end{pmatrix}$.

S_2 a donc pour solutions les triplets $(13t+7\,;-10t-3\,;t)$, avec t réel quelconque. L'intersection des plans $\mathscr{P}$ et $\mathscr{Q}$ est la droite (d) dont le triplet précédent constitue une représentation paramétrique, de paramètre t.

3. On remarque que l'équation de $\mathscr{R}$ est obtenue en ajoutant membre à membre les équations de $\mathscr{P}$ et $\mathscr{Q}$.
Les solutions du système S_1 sont donc celles du système S_2.
Le système de représentation matricielle $C\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}5\\1\\6\end{pmatrix}$ a une infinité de solutions.
La matrice C n'est donc pas inversible.

81

L'espace est muni d'un repère orthonormé.

1. Déterminer l'inverse de la matrice $A=\begin{pmatrix}5&10\\4&12\end{pmatrix}$.

2. Utiliser la matrice A pour déterminer une représentation paramétrique de la droite intersection des deux plans $\mathscr{P}$ et $\mathscr{Q}$ d'équations respectives $5x+10y+6z=1$ et $4x+12y+z=3$.

AIDE : Utiliser un système d'inconnues x et y, z étant considérée comme une « constante ».

82

Soit f une fonction polynôme de degré 2 définie sur $\mathbb{R}$ par $f(x)=ax^2+bx+c$ et $\mathscr{P}$ la parabole représentant f dans un repère du plan. On cherche à identifier f sachant que $\mathscr{P}$ passe par les points A (2 ; 26), B (4 ; 118) et C (6 ; 266).

1. Montrer que cela revient à résoudre le système, d'inconnues a, b et c, d'écriture matricielle $M\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}26\\118\\266\end{pmatrix}$ où M est une matrice à identifier.

2. En déduire l'expression de f à l'aide de la calculatrice.

3. Déterminer les fonctions g du second degré telles que :
$g(2)=g(6)$ et $g(4)=-2$.

VRAI - FAUX

Pour les exercices 83 et 84, indiquer si les affirmations sont vraies ou fausses, puis justifier.

83 Si le système $\begin{cases}ax+by=c\\a'x+b'y=c'\end{cases}$ d'inconnue $(x\,;y)$ n'a pas de solution, alors la matrice associée $\begin{pmatrix}a&b\\a'&b'\end{pmatrix}$ n'est pas inversible.

84 Si le système $\begin{cases}ax+by=c\\a'x+b'y=c'\end{cases}$ d'inconnue $(x\,;y)$ a au moins une solution, alors la matrice associée $\begin{pmatrix}a&b\\a'&b'\end{pmatrix}$ est inversible.

Top Chrono !

Résoudre chacun des exercices suivants en 10 minutes maximum.

85

On considère le système $\begin{cases}6x+5y=a\\8x+7y=b\end{cases}$ d'inconnue $(x\,;y)$. Exprimer x et y en fonction de a et b et en déduire la matrice inverse de la matrice :

$$A=\begin{pmatrix}6&5\\8&7\end{pmatrix}.$$

86

Soit $C=\begin{pmatrix}1&7\\-\frac{3}{7}&1\end{pmatrix}$.

Calculer C^3 et en déduire une résolution du système :

$$\begin{cases}x+7y=5\\-3x+7y=9\times 7\,.\end{cases}$$

87

Soit $A=\begin{pmatrix}2&1\\3&2\end{pmatrix}$ et $B=\begin{pmatrix}0&1\\5&6\end{pmatrix}$.

1. Déterminer une matrice $C=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ telle que $AC=B$.

2. Déterminer l'inverse de la matrice A à l'aide de la calculatrice et retrouver la matrice C obtenue précédemment à l'aide de cette matrice inverse.

88

Soit $A=\begin{pmatrix}2&2\\2&2\end{pmatrix}$.

1. Calculer les premières puissances de la matrice A.

2. Conjecturer une expression des éléments de A^n en fonction de n, puis la démontrer par récurrence.

Choisir la (ou les) bonne(s) réponse(s).

Connaître les propriétés des opérations sur les matrices

→ Pour vous aider Savoir-faire 5 et 7, p. 83 et 87

	A	B	C	D
89 Soit x, s, t et m des réels tels que, $\begin{pmatrix} 54 & 78 \\ x & 198 \end{pmatrix} = s\begin{pmatrix} 12 & 14 \\ 16 & 18 \end{pmatrix} + t\begin{pmatrix} 2 & 4 \\ 8 & m \end{pmatrix}$, alors	t est un entier multiple de s	$m = 16$	$tm = 12^2$	$x = 100$
90 A et B sont deux matrices carrées d'ordre 2. Si AB est la matrice nulle, alors	A ou B est la matrice nulle	BA est la matrice nulle	ni A, ni B n'est inversible	pour toute matrice colonne X à n lignes, les éléments de A(BX) sont tous nuls

Calculer des puissances de matrices

→ Pour vous aider Savoir-faire 8 et 9, p. 89

91 Soit $A = \begin{pmatrix} 1 & 3 \\ 5 & -1 \end{pmatrix}$, alors	$A^2 = 16\,I_2$	pour tout $n \geqslant 2$, $A^n = 16^n I_2$	le coefficient de la ligne 1, colonne 2 de A^5 est non nul	A^{200} a au moins un coefficient nul
92 Si $u_1 = u_2 = 1$ et pour tout entier $n \geqslant 3$, $\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A\begin{pmatrix} u_{n-1} \\ u_{n-2} \end{pmatrix}$ où $A = \begin{pmatrix} 5 & 5 \\ 1 & 0 \end{pmatrix}$, alors	$u_5 = 325$	$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A^{n-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	pour tout $n \geqslant 3$, $u_n = 10\,u_{n-2} + 5\,u_{n-3}$	$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A^{n-2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
93 Si, pour tout entier $n \geqslant 1$, on a $\begin{pmatrix} u_n \\ v_n \end{pmatrix} = A\begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix}$ où $A = \begin{pmatrix} 2 & 5 \\ 0 & 3 \end{pmatrix}$, $u_0 = 5$ et $v_0 = 1$, alors	la suite (v_n) est géométrique	la suite (u_n) n'est pas géométrique	pour tout entier $n \geqslant 0$, $u_n = 5 \times 3^n$	l'élément d'indices (1 ; 1) de A^n est 2^n

Utiliser l'inversion des matrices

→ Pour vous aider Savoir-faire 10 et 11, p. 93

94 Si $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ alors A^{-1} est égal à	$\begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1{,}5 & -0{,}5 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ -1{,}5 & 0{,}5 \end{pmatrix}$	aucune des trois matrices précédentes
95 La matrice associée au système $\begin{cases} 2x + 3y = a \\ 5x - 7y = b \end{cases}$	est inversible	n'est pas inversible	est inversible pour certaines valeurs de a et b et non inversible pour d'autres	a pour inverse une matrice de la forme $s\begin{pmatrix} 7 & 3 \\ 5 & -2 \end{pmatrix}, s \in \mathbb{R}$
96 Si A et B sont deux matrices carrées non nulles d'ordre n telles que $AB = t\,I_n$ où t est un nombre réel, alors	il existe une valeur de t telle que A n'est pas inversible	pour t non nul, la matrice B est inversible d'inverse $\frac{1}{t}$ A	l'inverse de la matrice A est la matrice B pour tout réel t non nul	$BA = t\,I_n$

➤ **Voir les réponses, p. 140**

TP 1 Chiffrement de Hill

→ Utiliser des matrices pour chiffrer et déchiffrer.

Point Histoire

C'est le mathématicien américain **Lester Hill** (1891-1961) qui a inventé cette méthode de chiffrement.

On va mettre en œuvre une méthode de chiffrement, appelée chiffrement de Hill, qui utilise une matrice et des raisonnements modulo *m* où *m* est le nombre de symboles de l'alphabet utilisé.

On associe à chaque lettre de l'alphabet un entier de l'ensemble E = {0 ; 1 ; 2 ; … ; 25} suivant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8

J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

A. Le principe du chiffrement de Hill

Dans cette partie, on se donne pour clé de chiffrement la matrice :

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}.$$

On va chiffrer dans la suite le mot INDICE. À l'aide de la grille ci-dessus, on code le mot INDICE, ce qui donne 8-13-3-8-2-4. On regroupe ensuite les lettres deux par deux et on forme les matrices colonnes $U_1 = \begin{pmatrix} 8 \\ 13 \end{pmatrix}$, $U_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$ et $U_3 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$.

1. a. Calculer les matrices $V_1 = AU_1$, $V_2 = AU_2$ et $V_3 = AU_3$.

b. En remplaçant chaque élément de ces matrices colonnes par son représentant dans E modulo 26, obtenir les matrices colonnes W_1, W_2 et W_3.

c. En associant les éléments de ces matrices W_1, W_2 et W_3 aux lettres selon le tableau précédent, on obtient le message sous sa forme chiffrée. Vérifier que ce message est DVUBYO.

2. Déterminer la matrice B, inverse de A, à l'aide d'une calculatrice. Vérifier que le principe de chiffrement de Hill, avec la clé B, appliqué au message DVUBYO redonne le message d'origine.

3. Déchiffrer le message YOWPEE.

B. Un autre exemple

On se donne maintenant pour clé la matrice $A = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}$.

1. Chiffrer le mot INDICE avec cette clé.

2. Soit la matrice $M = \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}$.

Calculer le produit MA et en déduire que A est inversible. On appelera B la matrice inverse de A.

3. Expliquer pourquoi l'utilisation de la clé B ne permet pas de déchiffrer le message HTPQMK.

4. Vérifier que l'utilisation de la clé définie par la matrice C = 23M permet le déchiffrage du message HTPQMK.

5. Cette clé C permet-elle de déchiffrer tous les messages chiffrés avec la clé A ?

C. Un troisième exemple

On se donne pour clé la matrice $A = \begin{pmatrix} 8 & 6 \\ 5 & 4 \end{pmatrix}$.

1. Déterminer deux mots de deux lettres, distincts, et dont le chiffrement par la méthode de Hill donnera le même message.

2. Une telle matrice est-elle une clé acceptable ?

D. Critère pour une clé acceptable

On utilise la clé $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c et d sont des entiers tels que l'entier $\delta = ad - bc$ soit un entier non nul premier avec 26.

1. Soit M la matrice $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Calculer le produit MA.

2. Déduire de la question précédente l'existence d'une matrice B à coefficients entiers telle que le produit BA soit égal à la matrice sI_2 où s est un entier tel que $s \equiv 1\ (26)$.

3. On reçoit un message chiffré par la méthode de Hill avec la clé A. Comment déchiffre-t-on ce message ?

E. Trigrammes

Le principe de chiffrement de Hill peut être appliqué avec des regroupements des lettres du message par groupe de 3 ou par groupe de 4, ou plus généralement par groupe de n (n entier naturel au moins égal à 2).

Avec la clé $A = \begin{pmatrix} 1 & 5 & 8 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix}$, on code en regroupant les lettres trois par trois.

1. Coder le mot INDICE avec la clé A.

2. Soit M la matrice $\begin{pmatrix} 23 & 13 & 22 \\ 6 & 19 & 12 \\ 23 & 19 & 19 \end{pmatrix}$.

a. Calculer la matrice produit MA.

b. Soit N la matrice obtenue en remplaçant chaque élément de la matrice MA par son représentant, modulo 26, dans E. Déterminer N.

c. En déduire une matrice B permettant le déchiffrement des messages chiffrés avec la clé A.

d. Vérifier que la matrice B permet effectivement de retrouver le mot INDICE à partir du mot obtenu à la question **1**.

TP 2 Algorithme de Smyrne

→ Utiliser une matrice et le calcul formel pour justifier un algorithme.

Point Histoire

Théon de Smyrne est un philosophe et mathématicien grec (vers 130 ap. J.-C.). Il est à l'origine de l'algorithme étudié ici, qui permet d'approcher des irrationnels par des suites d'entiers.

On étudie ci-dessous un algorithme permettant d'approcher $\sqrt{2}$ à l'aide de suites d'entiers.
On justifie ensuite cet algorithme à l'aide de suites et de matrices.

A. Un algorithme

On considère l'algorithme suivant :

Entrée : Un entier naturel n, non nul
Traitement : x prend la valeur 1 ; y prend la valeur 1
Pour j allant de 1 à n
  a prend la valeur $x + y$
  y prend la valeur $2x + y$
  x prend la valeur a
Fin Pour
Sortie : Afficher le rapport $\frac{y}{x}$

1. Traduire cet algorithme pour votre calculatrice.

2. Tester cet algorithme pour $n = 10$, $n = 15$ et $n = 20$.
Comparer le résultat obtenu avec le nombre $\sqrt{2}$.
Dans la suite, on va chercher à expliquer le phénomène observé.

B. Une matrice

Soit (x_n) et (y_n) deux suites définies par $x_0 = 1$ et $y_0 = 1$, et pour tout entier naturel n : $\begin{cases} x_{n+1} = x_n + y_n \\ y_{n+1} = 2x_n + y_n \end{cases}$

1. Déterminer x_1, y_1, x_2, y_2, x_3 et y_3.

2. Identifier la matrice A telle que, pour tout entier naturel n, on a $U_{n+1} = AU_n$ où, pour tout n, on a posé : $U_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

3. Justifier que, pour tout entier naturel n, on a :
$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

4. Exprimer la sortie de l'algorithme de la partie A pour l'entrée n à l'aide des suites (x_n) et (y_n).

5. a. Dans une ligne de commandes du logiciel Xcas, saisir les matrices A et U_0.

b. Définir ensuite les matrices U_1, U_2 et U_3 par une formule dans une ligne de commandes de Xcas.

c. Entrer les instructions :

`P:=jordan(A)[0];D:=jordan(A)[1];Q:=simplifier(inverse(P))`

dans une ligne de commandes de Xcas.
Quelle est la réponse du logiciel lorsqu'on entre maintenant la commande `simplifier(P*D*Q)` ?

d. Calculer avec Xcas : PD^2QU_0 et PD^3QU_0.
Quels résultats retrouve-t-on ? Expliquer.

6. a. On entre maintenant l'instruction

`F(n):=[[(sqrt(2)+1)^n,0],[0,(-(sqrt(2))+1)^n]]; factor(P*F(n)*Q*U0)`.

En déduire une expression, en fonction de n, du rapport r_n affiché par l'algorithme de la partie A.

b. Déterminer la limite de la suite (r_n) avec Xcas.

c. En factorisant le numérateur et le dénominateur par $\left(1+\sqrt{2}\right)^{n+1}$, déterminer cette limite sans logiciel.

C. Généralisation

On modifie l'algorithme de la partie A de la façon suivante :

Entrée : Un entier naturel n
Traitement : x prend la valeur 1 ; y prend la valeur 1
Pour j allant de 1 à n
  a prend la valeur $x + y$
  y prend la valeur $3x + y$
  x prend la valeur a
Fin Pour
Sortie : Afficher le rapport $\frac{y}{x}$

1. Que peut-on s'attendre à observer ?

2. Quelles sont les modifications à apporter à la feuille Xcas construite précédemment pour étudier ce cas ?

Aides pour les logiciels

Xcas

On consultera l'aide `aide/index` pour chaque instruction non connue.
B. 5. a. `A:=[[1,1],[2,1]];U0:=[[1],[1]]`.
B. 5. b. `U1:=A*U0`.
B. 5. c. La commande **jordan()** permet, comme l'indique la suite de la question, de déterminer une matrice inversible P et une matrice diagonale D telle que $A = PDP^{-1}$.
B. 5. d. Penser à la commande **simplifier()**.
B. 6. b. La syntaxe de l'instruction **limite()** est dans `aide/index`. Cette instruction demande trois arguments.

Sujet commenté BAC

➤ Énoncé

Thèmes
- *Calculs sur les matrices*
- *Inverse d'une matrice*
- *Puissances d'une matrice*

Deux enseignes concurrentes A et B se partagent l'intégralité d'un marché. En 2020, 92 % des clients se fournissent dans les magasins A et 8 % dans les magasins B. On suppose que, chaque année, 5 % des clients des magasins A décident de se fournir chez B et que 1 % des clients des magasins B changent de fournisseur et s'adressent aux magasins de l'enseigne A. Le nombre total de clients restant constant, on note a_n la probabilité de l'événement A_n : « un client choisi au hasard l'année $(2020 + n)$ se fournit dans les magasins A » et b_n la probabilité qu'il se fournisse dans les magasins B.

1. Justifier que, pour tout entier naturel $n \geqslant 1$, on peut écrire $\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-1} \end{pmatrix} M$ où M est une matrice carrée d'ordre 2 à déterminer.

2. a. Soit $Q = \frac{1}{6}\begin{pmatrix} 1 & 5 \\ -1 & 1 \end{pmatrix}$. Déterminer la matrice P inverse de la matrice Q.

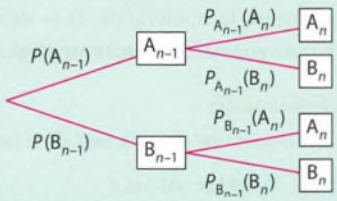
b. Calculer la matrice $D = QMP$.

c. En déduire les éléments de la matrice M^n pour n entier naturel.

d. En déduire une expression de a_n en fonction de l'entier naturel n.

➤ Comprendre l'énoncé et choisir les méthodes

1. Les données font intervenir des probabilités conditionnelles. On pensera donc à raisonner à partir d'un arbre :



2. a. On peut déterminer l'inverse P d'une matrice Q à l'aide de la résolution d'un système. Il est possible également d'émettre une conjecture à l'aide d'une calculatrice, cette conjecture devra ensuite être vérifiée par le calcul d'un produit de matrices.

→ Savoir-faire 10, p. 93

b. Pour calculer le produit QMP, on calcule d'abord QM puis (QM)P ou d'abord MP puis Q(MP). Une vérification avec la calculatrice peut permettre de corriger des erreurs.

→ Savoir-faire 7, p. 87

c. À partir de l'écriture PDP^{-1} d'une matrice, on calcule :

$$M^2 = (PDP^{-1})(PDP^{-1}) = PD(P^{-1}P)DP^{-1} = PDDP^{-1},$$

soit $M^2 = PD^2P^{-1}$.

Par récurrence, on établit dans ce cas l'égalité $M^n = PD^nQ$.

Il faut savoir par ailleurs calculer la puissance n-ième d'une matrice diagonale.

d. L'égalité $\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-1} \end{pmatrix} M$ définit les suites (a_n) et (b_n) par récurrence. Une récurrence permet d'en déduire l'égalité :

$$\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \end{pmatrix} M^n.$$

On utilise ensuite l'expression de M^n déterminée dans les questions précédentes.

→ Savoir-faire 9, p. 89

➤ Réponses

1. D'après la formule des probabilités totales, la probabilité $a_n = P(A_n)$ est égale à :

$$P(A_{n-1})P_{A_{n-1}}(A_n) + P(B_{n-1})P_{B_{n-1}}(B_n),$$

c'est-à-dire à $0{,}95\,a_{n-1} + 0{,}01\,b_{n-1}$.

De même, on a $b_n = 0{,}05\,a_{n-1} + 0{,}99\,b_{n-1}$.

On a donc $\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-1} \end{pmatrix} M$ où :

$$M = \begin{pmatrix} 0{,}95 & 0{,}05 \\ 0{,}01 & 0{,}99 \end{pmatrix}.$$

2. a. Avec une calculatrice, on conjecture que l'on a $P = \begin{pmatrix} 1 & -5 \\ 1 & 1 \end{pmatrix}$. On confirme cette conjecture par le calcul du produit RQ où $R = \begin{pmatrix} 1 & -5 \\ 1 & 1 \end{pmatrix}$. On a en effet $RQ = I_2$, donc la matrice R est bien égale à la matrice P inverse de Q.

b. On obtient $D = \begin{pmatrix} 1 & 0 \\ 0 & 0{,}94 \end{pmatrix}$.

c. De l'égalité $QMP = D$, on déduit $PQMPQ = PDQ$.

Or $PQ = I_2$, donc $M = PDQ$.

Si pour un entier naturel n on a $M^n = PD^nQ$, alors :

$$M^{n+1} = M^nM = PD^nQPDQ = PD^{n+1}Q.$$

On établit ainsi par récurrence que pour tout entier naturel n, on a $M^n = PD^nQ$, soit :

$$M^n = \frac{1}{6}\begin{pmatrix} 1 + 5 \times 0{,}94^n & 5 - 5 \times 0{,}94^n \\ 1 - 0{,}94^n & 5 + 0{,}94^n \end{pmatrix}.$$

d. De l'égalité $\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-1} \end{pmatrix} M$ valable pour tout entier n, on déduit $\begin{pmatrix} a_n & b_n \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \end{pmatrix} M^n$, d'où :

$$a_n = \frac{1}{6}(1 + 4{,}52 \times 0{,}94^n).$$

Pour se préparer à l'écrit BAC

Sujet A ALGO

Capacités mises en œuvre

- *Calculer un produit de matrices*
- *Calculer avec les puissances de matrices*

Pour tout entier naturel n non nul, on définit :

$$u_n = \left(3 + 2\sqrt{2}\right)^n.$$

1. Montrer que l'on peut écrire les premiers termes de la suite (u_n) sous la forme :

$u_1 = a_1 + b_1\sqrt{2}$, $u_2 = a_2 + b_2\sqrt{2}$ et $u_3 = a_3 + b_3\sqrt{2}$,

où les nombres a_j et b_j sont des entiers.

2. Montrer par récurrence sur n que u_n s'écrit sous la forme $u_n = a_n + b_n\sqrt{2}$ où a_n et b_n sont des entiers vérifiant les relations de récurrence :

$$a_n = 3a_{n-1} + 4b_{n-1} \text{ et } b_n = 2a_{n-1} + 3b_{n-1}.$$

3. On désire écrire un algorithme dont l'entrée est un entier naturel n non nul et dont la sortie est constituée des valeurs de a_n et b_n.

Un élève propose l'algorithme suivant :

Entrée : n entier naturel non nul
Traitement :
a prend la valeur 3
b prend la valeur 2
Pour j allant de 1 à n
  a prend la valeur $3a + 4b$
  b prend la valeur $2a + 3b$
Fin Pour
Sortie : Afficher a et b

Proposer une modification de cet algorithme permettant d'obtenir les valeurs annoncées.

4. Définir une matrice A telle que, pour tout entier naturel $n \geqslant 2$, on ait :

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = A\begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix}.$$

5. Soit $P = \begin{pmatrix} 2\sqrt{2} & -2\sqrt{2} \\ 2 & 2 \end{pmatrix}$ et $Q = \frac{1}{8}\begin{pmatrix} \sqrt{2} & 2 \\ -\sqrt{2} & 2 \end{pmatrix}$.

a. Établir que P et Q sont des matrices inverses l'une de l'autre.

b. Vérifier que la matrice QAP est une matrice diagonale D.

6. Déduire de ce qui précède une expression des éléments de la matrice A^n en fonction de l'entier naturel non nul n.

7. Soit n un entier naturel non nul.

Établir l'égalité $a_n = \frac{1}{2}\left(\left(3 - 2\sqrt{2}\right)^n + \left(3 + 2\sqrt{2}\right)^n\right)$.

Savoir-faire

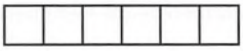
Question 7. ➤ Savoir-faire 9, p. 89

Sujet B ALGO

Capacités mises en œuvre

- *Utiliser l'inverse d'une matrice*
- *Calculer et utiliser les puissances d'une matrice*

On appelle planche de longueur n une planche découpée en n carrés unité. Exemple d'une planche de longueur 6 :



On veut paver les planches de longueur n avec des carrés unité bleus ou rouges et des dominos (constitués de deux carrés accolés) verts. On note u_n le nombre de façons différentes de paver une planche de longueur n. Les pavages de la planche de longueur 2 ci-dessous montrent que $u_2 = 5$.

1. Vérifier que $u_1 = 2$ et $u_3 = 12$.

2. Expliquer pourquoi, pour tout entier naturel $n \geqslant 2$, on a la relation $u_n = 2u_{n-1} + u_{n-2}$.

3. Reproduire et compléter l'algorithme suivant afin qu'il affiche u_n en sortie.

Saisir n
a prend la valeur 2
b prend la valeur 5
Pour i allant de 3 à n
  c prend la valeur b
  .....
  .....
Fin Pour
Afficher .....

4. Calculer les termes u_4 et u_5 à l'aide de la relation de récurrence précédente.

5. Établir que pour tout entier naturel $n \geqslant 2$, on a :

$$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A\begin{pmatrix} u_{n-1} \\ u_{n-2} \end{pmatrix},$$

où A est une matrice à identifier.

6. Soit $P = \begin{pmatrix} 1+\sqrt{2} & 1-\sqrt{2} \\ 1 & 1 \end{pmatrix}$ et $Q = \frac{1}{4}\begin{pmatrix} \sqrt{2} & 2-\sqrt{2} \\ -\sqrt{2} & 2+\sqrt{2} \end{pmatrix}$.

a. Vérifier que $Q = P^{-1}$.

b. Vérifier que la matrice $D = QAP$ est diagonale.

7. Établir que pour tout entier naturel non nul n, on a :

$$A^n = PD^nQ.$$

8. En déduire l'expression de u_n en fonction de l'entier naturel n ($n \geqslant 3$).

Savoir-faire

Question 8. ➤ Savoir-faire 9, p. 89

Sujet C

Capacités mises en œuvre

- *Déterminer une matrice inverse*
- *Résoudre un système à l'aide d'une matrice*
- *Calculer les puissances d'une matrice*

On définit la matrice $A = \begin{pmatrix} 2 & -1 & 3 \\ -3 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$.

1. Calculer la matrice $B = 4A - A^2$, puis le produit AB.

2. Déduire de ce qui précède que A est inversible et donner sa matrice inverse.

3. Dans l'espace muni d'un repère orthonormé $(O ; \vec{i}, \vec{j}, \vec{k})$, on considère les trois plans $\mathscr{P}$, $\mathscr{Q}$ et $\mathscr{R}$ d'équations respectives :

$2x - y + 3z = 1$, $-3x + y - z = 2$ et $x + y + z = 3$.

Déterminer l'intersection de ces trois plans à l'aide de la matrice B.

4. Vérifier que la matrice A^3 s'écrit sous la forme :

$$a_3 I_3 + b_3 A + c_3 A^2,$$

où a_3, b_3 et c_3 sont des réels à déterminer.

5. En déduire que la matrice A^4 s'écrit sous la forme :

$$a_4 I_3 + b_4 A + c_4 A^2,$$

où a_4, b_4 et c_4 sont des réels à déterminer.

6. Établir que pour tout entier naturel $n \geqslant 1$, la matrice A^n s'écrit sous la forme $a_n I_3 + b_n A + c_n A^2$ où les suites (a_n), (b_n) et (c_n) sont telles que, pour tout entier $n \geqslant 1$, on a :

$$a_{n+1} = -10c_n, \quad b_{n+1} = a_n \text{ et } c_{n+1} = b_n + 4c_n.$$

7. Déterminer a_n, b_n et c_n pour $n = 5$ puis pour $n = 6$.

Savoir-faire

Question 3. ➤ Savoir-faire 11, p. 93

Sujet D VRAI – FAUX

Capacités mises en œuvre

- *Multiplier des matrices*
- *Manipuler un système linéaire sous forme matricielle*
- *Calculer les puissances d'une matrice*

Pour chacune des propositions suivantes, indiquer si elle est vraie ou fausse et donner une justification.

1. Soit deux matrices carrées A et B non nulles.

Proposition A :

« La matrice AB ne peut pas être égale à la matrice nulle ».

Proposition B :

« La matrice AB ne peut pas être égale à la matrice BA ».

2. On considère une matrice carrée A telle qu'il existe un entier $n \geqslant 2$ tel que A^n est la matrice nulle.

Proposition C : « La matrice A est la matrice nulle ».

3. Soit A une matrice carrée d'ordre 2 non nulle telle que :

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

Proposition D : « Le système linéaire de représentation matricielle $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ a pour unique solution le couple $(x ; y) = (1 ; 2)$. »

4. Soit la matrice $A = \begin{pmatrix} 1 & 0 \\ 3 & 4 \end{pmatrix}$.

Proposition E : « Pour n entier naturel, A^n s'écrit $\begin{pmatrix} 1 & 0 \\ u_n - 1 & u_n \end{pmatrix}$, où (u_n) est une suite géométrique. »

Savoir-faire

Questions 1. et 2. ➤ Savoir-faire 7, p. 87

Pour se préparer à l'oral BAC

97 Les suites (a_n) et (b_n) sont telles que $\begin{pmatrix} a_n \\ b_n \end{pmatrix} = M\begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix}$ où $M = \begin{pmatrix} 0{,}96 & 0{,}02 \\ 0{,}04 & 0{,}98 \end{pmatrix}$ et $a_0 = 1$, $b_0 = 2$.

Calculer la matrice QMQ^{-1} où $Q = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}$ et en déduire une expression de a_n en fonction de l'entier naturel n.

98 L'espace est muni d'un repère orthonormé $(O ; \vec{i}, \vec{j}, \vec{k})$. $\mathscr{P}$ et $\mathscr{Q}$ sont deux plans d'équations respectives $7x + 8y + 2z = 1$ et $2x + 3y - 11z = 15$. Déterminer l'inverse de la matrice $A = \begin{pmatrix} 7 & 8 \\ 2 & 3 \end{pmatrix}$ à l'aide de la calculatrice. Utiliser cette matrice A^{-1} pour déterminer une représentation paramétrique de la droite intersection des deux plans $\mathscr{P}$ et $\mathscr{Q}$.

99 On considère le système $\begin{cases} 17x + 8y = a \\ 7x + 3y = b \end{cases}$

1. Exprimer x et y en fonction de a et b.

2. Écrire le système sous forme matricielle et déterminer l'inverse de la matrice du système.

POUR ALLER PLUS LOIN

100 Trigonométrie

Soit $A = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix}$ où a est un nombre réel.

1. Montrer, par récurrence, que l'on a :

$$A^n = \begin{pmatrix} \cos(na) & -\sin(na) \\ \sin(na) & \cos(na) \end{pmatrix}$$

pour tout entier naturel n non nul.

2. Le nombre a étant de la forme $a = \frac{\pi}{p}$, où p est un entier naturel non nul, déterminer les entiers naturels n tels que $A^n = A$.

101 Puissances d'une matrice stochastique

Soit a et b deux réels de l'intervalle $]0 ; 1[$ et $A = \begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}$.

1. Vérifier que $A = N + (1 - a - b)R$ où :

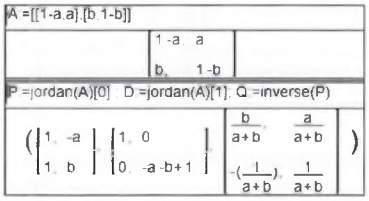
$$N = \frac{1}{a+b}\begin{pmatrix} b & a \\ b & a \end{pmatrix} \text{ et } R = \frac{1}{a+b}\begin{pmatrix} a & -a \\ -b & b \end{pmatrix}.$$

2. Vérifier que $NR = RN = 0_2$ où 0_2 est la matrice nulle d'ordre 2.

3. Déterminer les puissances des matrices N et R.

4. En déduire les éléments de la matrice A^n pour tout entier naturel n non nul.

5. Dans cette question, on va retrouver les résultats précédents à l'aide de certaines instructions du logiciel Xcas spécifiques à la théorie des matrices.



a. Vérifier que l'on a bien $Q = P^{-1}$.

b. Vérifier que la matrice PDQ est égale à A.

c. Retrouver avec ce qui précède les résultats obtenus à la question 4.

102 Les nombres de Fibonacci

On appelle nombre de Fibonacci l'entier f_n égal au nombre de façons d'écrire n comme somme de termes égaux à 1 ou à 2 (un ordre différent des termes comptant pour une écriture différente). Par exemple, l'entier $n = 4$ s'écrit :

$1 + 1 + 1 + 1$, $1 + 1 + 2$, $1 + 2 + 1$, $2 + 1 + 1$, $2 + 2$.

On a donc $f_4 = 5$. On pose par ailleurs $f_0 = 1$.

1. En séparant les sommes en sommes dont le premier terme vaut 1 ($n = 1 + \ldots$) et en sommes dont le premier terme vaut 2 ($n = 2 + \ldots$), montrer que pour tout entier naturel $n \geqslant 2$, on a : $f_n = f_{n-1} + f_{n-2}$.

2. Calculer les termes d'indices 2, 3, 4 et 5 de la suite de Fibonacci à l'aide de la récurrence précédente, puis en explicitant les décompositions d'entiers associées.

3. a. Vérifier que pour tout entier naturel $n \geqslant 2$, on a :

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A\begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix} \text{ où } A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

b. En déduire que pour tout entier naturel $n \geqslant 2$, on a :

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A^{n-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

4. Soit $P = \begin{pmatrix} 1+\sqrt{5} & 1-\sqrt{5} \\ 2 & 2 \end{pmatrix}$ et $Q = \frac{1}{20}\begin{pmatrix} 2\sqrt{5} & 5-\sqrt{5} \\ -2\sqrt{5} & 5+\sqrt{5} \end{pmatrix}$.

a. Vérifier que Q est la matrice inverse de P.

b. Calculer la matrice $D = QAP$.

c. En déduire que pour tout entier naturel n, on a $A^n = PD^nQ$.

5. Déduire des questions qui précèdent, une expression de f_n en fonction de n.

Point Histoire

Fibonacci (également connu sous le nom de Léonard de Pise) était un mathématicien italien (1175–1250). Il a introduit la suite étudiée dans cet exercice dans son livre *Liber Abaci*, paru en 1202.

103 Compter les mots

On écrit des mots avec l'alphabet $A = \{a ; b ; c ; d\}$. Par exemple, *abacdd* est un mot de longueur 6 écrit sur cet alphabet.

Pour tout entier naturel $n \geqslant 1$, on note p_n (respectivement i_n) le nombre de mots de longueur n écrit sur cet alphabet et comportant un nombre pair (respectivement impair) de lettres a.

1. Énoncer les mots de longueur 1 écrits sur l'alphabet A.
En déduire les valeurs de p_1 et i_1.

2. Énoncer les mots de longueur 2 écrits sur l'alphabet A.
En déduire les valeurs de p_2 et i_2.

3. On peut construire les mots de longueur n en ajoutant aux mots de longueur $(n - 1)$ l'une quelconque des 4 lettres de l'alphabet. En séparant les mots en deux groupes, ceux dont la première lettre est a et ceux dont la première lettre n'est pas a, montrer que l'on a la relation $\begin{pmatrix} p_n \\ i_n \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} p_{n-1} \\ i_{n-1} \end{pmatrix}$ pour tout entier naturel $n \geqslant 2$.

4. En déduire que, pour tout entier naturel $n \geqslant 2$, on a :

$$\begin{pmatrix} p_n \\ i_n \end{pmatrix} = B^{n-1}\begin{pmatrix} 3 \\ 1 \end{pmatrix} \text{ où } B = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

5. Soit $P = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

a. Déterminer la matrice Q, inverse de la matrice P, à l'aide de la calculatrice.

b. Calculer la matrice $D = QBP$.

c. En déduire les expressions de p_n et i_n en fonction de n.

104 Somme de termes en progression géométrique

Soit q un réel non nul et distinct de 1 et $A = \begin{pmatrix} 1 & 1 \\ 0 & q \end{pmatrix}$.

1. Calculer A^2, A^3, A^4 et A^5.

2. Démontrer que pour tout entier naturel $n \geqslant 1$, on a :

$$A^n = \begin{pmatrix} 1 & S_n \\ 0 & q^n \end{pmatrix} \text{ où } S_n = 1 + q + q^2 + \ldots + q^{n-1}.$$

3. Soit $P = \begin{pmatrix} -1 & 1 \\ 0 & q-1 \end{pmatrix}$. Vérifier que P est inversible avec :

$$P^{-1} = \begin{pmatrix} -1 & \frac{1}{q-1} \\ 0 & \frac{1}{q-1} \end{pmatrix}.$$

4. Vérifier que $A = PDP^{-1}$ avec $D = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$.

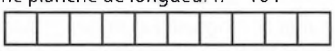
5. Pour n entier naturel non nul, calculer le produit de matrices PD^nP^{-1}.

6. Quelle formule du cours de la classe de Première a-t-on ainsi redémontrée ?

105 Un pavage

On appelle planche de longueur n une planche sur laquelle n carrés unité sont tracés.

Exemple d'une planche de longueur $n = 10$:



On dispose par ailleurs de carrés unité et de dominos constitués de deux carrés unité accolés. Les carrés unité sont rouges, les dominos sont bleus ou verts.

On note u_n le nombre de façons différentes de paver une planche de longueur n avec des carrés et des dominos.

Les pavages de la planche de longueur 3 ci-dessous montrent par exemple que $u_3 = 5$.

1. Vérifier que $u_1 = 1$, $u_2 = 3$ et $u_4 = 11$.

2. Expliquer pourquoi, pour tout entier naturel $n \geqslant 2$, on a la relation $u_n = u_{n-1} + 2u_{n-2}$.

3. Soit $A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$. Établir que pour tout entier naturel $n \geqslant 2$, on a $\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A \begin{pmatrix} u_{n-1} \\ u_{n-2} \end{pmatrix}$.

4. Soit $Q = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$.

Déterminer la matrice P inverse de Q à l'aide de la calculatrice.

5. Calculer la matrice $D = QAP$.

6. Déduire de ce qui précède une expression des éléments de la matrice A^n en fonction de l'entier naturel non nul n.

7. En déduire, pour tout entier naturel non nul n, une expression de u_n en fonction de n.

106 Une logique peu fondée

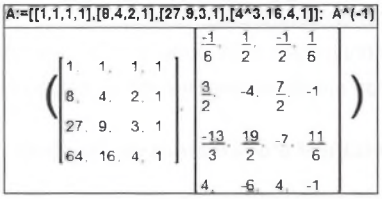
Partie A

On trouve dans un certain nombre de concours des épreuves dites de logique où il faut par exemple poursuivre une série de nombres comme la série suivante : 1 – 2 – 4 – 8.

1. Par quel nombre pourrait-on poursuivre cette série ?

2. Soit f un polynôme de la forme $f(x) = ax^3 + bx^2 + cx + d$ tel que $f(1) = 1$, $f(2) = 2$, $f(3) = 4$ et $f(4) = 8$.

a. À l'aide des résultats affichés ci-dessous par Xcas, identifier f.

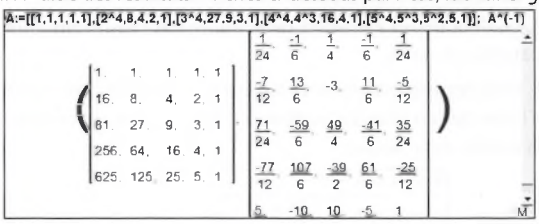


b. Par quel nombre pourrait-on maintenant poursuivre la série donnée ?

3. On donne maintenant la série 1 – 2 – 4 – 8 – 16 que les concepteurs d'une épreuve aimeraient voir complétée par le nombre 32.

Soit g un polynôme de la forme $g(x) = ax^4 + bx^3 + cx^2 + dx + k$ tel que $g(1) = 1$, $g(2) = 2$, $g(3) = 4$, $g(4) = 8$ et $g(5) = 16$.

a. À l'aide des résultats affichés ci-dessous par Xcas, identifier g.



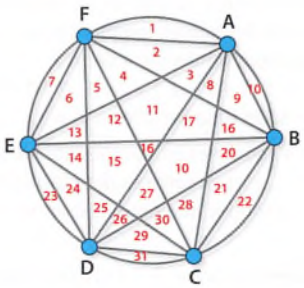
b. Par quel nombre peut-on maintenant poursuivre la série 1 – 2 – 4 – 8 – 16 ?

Partie B

On place des points sur un cercle de façon à ce que les segments joignant les points deux à deux ne se coupent jamais trois à trois. Lorsqu'on place deux points sur le cercle, on trace donc un seul segment, il partage l'intérieur du cercle en deux régions.

1. Lorsqu'on place trois points, vérifier que les segments partagent le cercle en quatre régions.

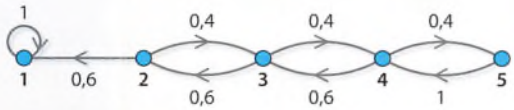
2. À l'aide de figures, compter le nombre de régions partageant l'intérieur du cercle avec quatre points, cinq points, six points sur le cercle.



3. Quel est le nombre le plus « logique » pour poursuivre la série 2 – 3 – 4 – 8 – 16 : est-ce 31 ou 32 ?

107 PROBLÈME DE SYNTHÈSE

Une personne part du point 3 du schéma ci-dessous et doit se rendre en deux pas au point 1. Son état d'ébriété le conduit à faire aléatoirement à chaque pas un déplacement à gauche avec une probabilité égale à 0,6 ou un pas à droite avec une probabilité égale à 0,4, sauf en 5 où la présence d'un mur le contraint à repartir vers la gauche.



1. À l'aide d'un arbre de probabilités :
a. déterminer la probabilité que cette personne soit arrivée à destination à son deuxième pas ;
b. déterminer la probabilité que cette personne se retrouve à son point de départ après deux pas.

2. On définit une matrice M carrée d'ordre 5 dont l'élément $m_{i,j}$ est égal à la probabilité de l'événement : « l'ivrogne se déplace de i en j (en un pas) ». On note R_n la matrice ligne à cinq éléments dont l'élément i est égal à la probabilité de l'événement : « l'ivrogne est en i après n pas ». En particulier, on a :

$$R_0 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

a. Donner les éléments des matrices R_1 et R_2.
b. Vérifier que l'on a $R_1 = R_0M$.
c. Justifier l'égalité $R_2 = R_0M^2$.
d. Exprimer R_n en fonction de R_0 et de M.

3. **a.** Soit n un entier impair.
Justifier que le troisième élément de la matrice ligne R_n est nul.
b. Pour n entier pair (non nul), certains éléments de R_n sont nuls. Lesquels ? Justifier.

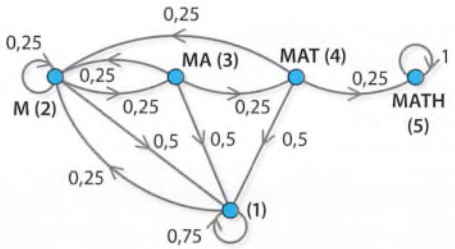
4. Notons p_n le premier élément de la matrice ligne R_n.
a. Que représente ce nombre pour l'ivrogne ?
b. Justifier que pour tout entier $n \geqslant 1$, on a $p_{2n} = p_{2n+1}$.

108 PROBLÈME DE SYNTHÈSE

Sur un jouet maltraité par des générations d'enfants, seules les lettres M, A, T, H du clavier sont encore fonctionnelles.
Tom frappe au hasard sur ces touches un grand nombre de fois.
À chaque frappe, on considère que chaque touche a une probabilité égale à 0,25 d'être choisie.
On s'intéresse à l'événement : « le mot MATH a été inscrit lors de la frappe ».

1. À l'aide d'un arbre, déterminer la probabilité d'avoir écrit le mot MATH à la quatrième frappe.

2. Pour étudier le processus, on dresse le schéma suivant :



et on définit la matrice B dont l'élément $b_{i,j}$ est égal à la probabilité de passer de l'état i à l'état j indiquée sur le schéma.
a. Donner les éléments de cette matrice.
b. Soit $\mu_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix}$.
Expliquer pourquoi le calcul μ_0B^4 permet de répondre à la question 1.

3. Tom a effectué une première frappe qui a donné la lettre M.
Il frappe ensuite encore quatre fois au hasard.
a. À l'aide d'arbres, déterminer la probabilité que le mot MATH soit obtenu (les quatre lettres étant consécutives).
b. Quel calcul utilisant la matrice B^4 peut-on effectuer pour retrouver le résultat de la question 3. **a.** ?

Prises d'initiatives

109 Soit la matrice $A = \begin{pmatrix} 1 & 1 & 2a \\ 2 & 1 & 1 \\ 1 & 1 & 3a \end{pmatrix}$ où a est un réel.
Quelles sont les valeurs de a pour lesquelles la matrice A est inversible ? Lorsque A est inversible, donner son inverse.

110 Lorsqu'on effectue le produit de deux matrices carrées d'ordre n, combien de multiplications et d'additions de nombres réels effectue-t-on ?

111 On appelle matrice triangulaire supérieure une matrice dont tous les éléments sous la diagonale sont nuls. On appelle déterminant d'une telle matrice X le produit de ses éléments diagonaux, noté det(X). A étant une matrice triangulaire supérieure, exprimer, pour tout entier naturel $n \geqslant 1$, $\det(A^n)$ en fonction des éléments diagonaux de A.

112 À un plan de n villes reliées par des routes, on associe une matrice M carrée d'ordre n dont l'élément $m_{i,j}$ est égal au nombre de routes reliant directement les villes i et j.
On appelle trace d'une matrice la somme des éléments de la diagonale principale de cette matrice.
Quel lien existe-t-il entre la trace de la matrice M^2 et le nombre de routes de ce plan ?

113 Chercher une formule générale donnant l'inverse d'une matrice carrée d'ordre 2.

114 Chercher sur Internet ce que l'on appelle la méthode de Gauss-Jordan pour le calcul d'inverses.
Utiliser cette méthode pour quelques matrices d'ordre 3 de votre choix.

Avant de commencer, se tester avec...

...des QCM

➤ Pour vous aider, voir le chapitre 3

Choisir la (ou les) bonne(s) réponse(s).

➤ Savoir utiliser des suites

	A	B	C	D
1 La suite (u_n) définie pour tout entier naturel n par $u_{n+1} = \frac{1}{2}u_n$ et $u_0 = 6$ vérifie	$u_n = \frac{1}{2^n}$	$u_n = \frac{1}{2^{n-1}}$	$\lim\limits_{n\to+\infty} u_n = 0$	$\lim\limits_{n\to+\infty} u_n = \frac{1}{2}$
2 Soit la suite (u_n) définie pour tout entier naturel n par $u_{n+1} = -3u_n + 4$. La suite (v_n) est géométrique avec	$v_n = u_n - 4$	$v_n = -3u_n$	$v_n = u_n - 1$	$v_n = u_n + 3$

➤ Savoir utiliser des probabilités

Soit A et B deux événements d'un univers. On sait que $P(A) = 0{,}6$, $P_A(B) = 0{,}5$ et $P_{\overline{A}}(\overline{B}) = 0{,}8$.

3 $P(B)$ est égal à	0,30	0,38	0,62	0,70
4 $P_B(A)$ est égal, à 10^{-2} près, à	0,30	0,50	0,63	0,79

➤ Savoir utiliser des matrices

On donne les matrices $A = \begin{pmatrix} 0{,}5 & -0{,}5 & 0 \\ -0{,}25 & 1 & -0{,}75 \\ -0{,}25 & -0{,}5 & 0{,}75 \end{pmatrix}$ et $B = I_3 - A$, où I_3 est la matrice unité d'ordre 3.

5 Le système $X \times A = X$, où X est une matrice ligne	n'a pas de solution	a pour unique solution (0 0 0)	est équivalent à $(X - I_3)A = 0$	a pour solutions toutes les matrices de la forme $(x\ x\ 2x)$
6 B est inversible et B^{-1} est égale à	$\begin{pmatrix} 1{,}5 & 1{,}5 & 0 \\ 2{,}5 & 1{,}5 & 0{,}5 \\ 2 & 0{,}5 & 0 \end{pmatrix}$	$\begin{pmatrix} -0{,}5 & -0{,}5 & 1 \\ -1{,}5 & -0{,}5 & 0{,}5 \\ -1 & 0{,}5 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & 1 & -3 \\ -1 & -1 & 3 \\ -1 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0{,}5 \\ -0{,}5 & 0 & 0{,}5 \end{pmatrix}$

➤ Voir les réponses, p. 140

...des exercices

7 Pendant les vacances, Maël a la possibilité de se baigner tous les jours.
S'il se baigne un jour, la probabilité qu'il se baigne le lendemain est 0,7 ; sinon, cette probabilité est 0,9.
Le premier jour de ses vacances, Maël se baigne. On note a_n (respectivement b_n) la probabilité que Maël se baigne (respectivement ne se baigne pas) le n-ième jour des vacances, pour n entier naturel non nul.

1. À l'aide d'un arbre de probabilités, déterminer a_1, b_1, a_2, b_2, a_3 et b_3.
2. Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

8 Soit les matrices $A = \begin{pmatrix} 4 & 0 \\ -2 & 5 \end{pmatrix}$ et $P = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$

1. Déterminer P^{-1}, puis la matrice $D = P^{-1} \times A \times P$.
2. Pour n entier naturel non nul, calculer D^n et en déduire A^n en fonction de n.

➤ Voir les réponses, p. 140

CHAPITRE

4

Problèmes d'évolution

Le Web est un réseau informatique mondial qui offre à ses utilisateurs une multitude de pages à consulter.

Pour nous aider sur la toile, des moteurs de recherche, comme Google et Yahoo, ont été créés. Ceux-ci effectuent un classement des pages quand on fait une requête, mais quels sont les critères qui guident les choix de ces moteurs ?

Google utilise un algorithme nommé *PageRank*, utilisant des suites de matrices, qui permet de proposer un classement des pages à l'utilisateur. C'est ce type de suites et de problèmes que nous allons aborder dans ce chapitre.

Les séquences du chapitre

Le raisonnement logique logique
p. 120 et 126

Les algorithmes ALGO
p. 126, 129, 133 et 136

Utilisation de logiciels TICE
p. 112, 113, 116, 117, 126, 132, 133 et 138

Problème 1 Évolution de populations de bactéries

Objectif
Découvrir la convergence de suites de matrices (U_n) telles que : $U_{n+1} = AU_n$.

Cours 1
Suites de matrices vérifiant : $U_{n+1} = AU_n + B$

Fichiers logiciels
04_TSspe_probleme1.xlsx
04_TSspe_probleme1.xls
04_TSspe_probleme1.ods
www. bordas-indice.fr

500 milliers de bactéries sont conservées dans une enceinte et peuvent prendre deux états physiologiques A et B. On désigne par a_n et b_n les effectifs, en milliers, de ces deux populations à l'instant n.

On estime que $\begin{cases} a_{n+1} = 0{,}95a_n + 0{,}2b_n \\ b_{n+1} = 0{,}05a_n + 0{,}8b_n \end{cases}$

À l'instant 0, on note a_0 et b_0 les effectifs de bactéries dans les états A et B.

1. On va étudier le comportement des suites (a_n) et (b_n) pour diverses conditions initiales.
Ouvrir une feuille de calcul d'un tableur. Saisir des valeurs de a_0 et de b_0 dans les cellules **B2** et **C2**, puis calculer les premiers termes de ces deux suites dans les colonnes **B** et **C**. Que constate-t-on ?

2. Soit (u_n) et (v_n) les suites telles que $u_n = a_n + b_n$ et $v_n = a_n - 4b_n$.
a. Montrer que la suite (u_n) est constante et la suite (v_n) géométrique.
b. Donner les expressions de u_n et de v_n en fonction de n, a_0 et b_0.
c. En déduire les expressions de a_n et de b_n en fonction de n, a_0 et b_0.
d. Déterminer la limite de chacune des suites (a_n) et (b_n). Que retrouve-t-on ?

3. Soit la matrice $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.
a. Montrer que $U_{n+1} = A \times U_n$, où A est une matrice à déterminer.
b. En déduire que $U_n = A^n \times U_0$. À quoi est égal A^n ?
c. En utilisant la question **2.**, déterminer la « limite » de la suite de matrices (U_n).

Problème 2 Reproduction des chamois dans un parc

Objectif
Étudier une suite de matrices (U_n) vérifiant : $U_{n+1} = AU_n + B$.

Cours 1
Suites de matrices vérifiant : $U_{n+1} = AU_n + B$

La population de chamois dans un parc se partage en deux classes d'âge, les « jeunes » et les « vieux ». On note u_n le nombre d'animaux « jeunes » l'année de rang n, et v_n le nombre d'animaux « vieux » l'année de rang n. On suppose que :
– 50 % des animaux « jeunes » passent dans la classe des « vieux » d'une année à l'autre ;
– le taux de mortalité est de 25 % dans la classe des « jeunes » et de 75 % dans la classe des « vieux » ;
– le taux de natalité est de 200 % pour la classe des « vieux », les « jeunes » n'étant pas encore en mesure de se reproduire.
Enfin, on introduit chaque année dans le parc 20 jeunes chamois supplémentaires.
Au début de l'étude, c'est-à-dire l'année de rang 0, il y a 400 jeunes chamois et 100 vieux chamois.

1. **a.** Vérifier que $u_1 = 320$ et $v_1 = 225$.
b. Exprimer u_{n+1} et v_{n+1} en fonction de u_n et de v_n.

2. On note $U_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. Déterminer la matrice carrée A et la matrice colonne B telles que :
$$U_{n+1} = A \times U_n + B.$$

3. **a.** Soit I_2 la matrice unité d'ordre 2.
Montrer que la matrice $E = I_2 - A$ est inversible et déterminer son inverse.
b. Montrer qu'il existe une unique matrice C telle que $C = AC + B$, et déterminer C.

4. Soit la matrice V_n telle que, pour tout entier naturel n : $V_n = U_n - C$. Montrer que $V_{n+1} = A \times V_n$.

5. Soit la matrice $P = \begin{pmatrix} 2 & 2 \\ 1 & -1 \end{pmatrix}$. Calculer P^{-1}, puis $D = P^{-1}AP$.

6. En déduire A^n en fonction de P^{-1}, D^n et P. Calculer la matrice A^n en fonction de n.

7. **a.** Déterminer alors les coefficients de la matrice V_n en fonction de n.
b. En déduire la matrice U_n en fonction de n.
c. Exprimer u_n et v_n en fonction de n.

8. **a.** Quelle est la limite de chacune des suites (u_n) et (v_n) ?
b. Quelle est la limite de la suite (w_n), où $w_n = \frac{u_n}{v_n}$? Interpréter ce résultat.

Problème 3 L'urne d'Ehrenfest

Objectif

Découvrir une suite de matrices de la forme $U_{n+1} = A\,U_n$ à travers un problème célèbre.

Cours 1

Suites de matrices vérifiant :

$U_{n+1} = AU_n + B$.

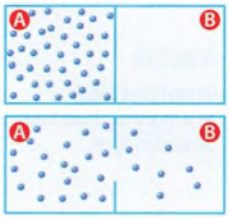
Point Histoire

Paul Ehrenfest (1880–1933) est un physicien autrichien.
Tatiana Ehrenfest (1876–1964) est une mathématicienne russo-néerlandaise.

Fichiers logiciels

04_TSspe_probleme3.xlsx
04_TSspe_probleme3.xls
04_TSspe_probleme3.ods
04_TSspe_probleme3.xws

www. bordas-indice.fr



En 1907, Paul et Tatiana Ehrenfest introduisent un modèle probabiliste qui permet de décrire l'évolution de la pression d'un gaz (évolution macroscopique irréversible dans le temps) par l'évolution microscopique réversible des molécules composant ce gaz.
On considère deux enceintes A et B de même volume.
Le vide est fait dans l'enceinte B, puis on fait un trou dans la paroi séparant les deux enceintes.
Comment évolue la répartition des molécules dans les deux enceintes ?
Pour étudier cette évolution, on utilise le modèle suivant :
– on dispose de deux urnes A et B, ainsi que de N boules ;
– à l'instant initial, toutes les boules sont dans l'urne A ;
– à intervalles réguliers, une boule est choisie au hasard et change d'urne : on effectue ainsi n tirages.

Partie A. Simulation avec un tableur

	A	B	C	D	E
1	Nombre de boules N			Urne A	Urne B
2	100		0	100	0
3			1	99	1
4			2	98	2
5			3	99	1

1. Saisir le nombre de boules de l'urne A dans la cellule **A2**.

2. Dans la colonne **C**, générer les numéros des étapes de 0 à 500.

3. Générer l'état initial des urnes dans les cellules **D2** et **E2**.

4. Dans la cellule **D3**, on simule le tirage d'une boule au hasard.
Soit N_k le nombre de boules de A à l'étape k. La probabilité de choisir une boule de A est $\frac{N_k}{N}$.
On choisit alors un nombre au hasard dans [0 ; 1] : si ce nombre est inférieur à $\frac{N_k}{N}$, alors une boule passe de A vers B, sinon c'est le contraire.
Saisir la formule adéquate dans la cellule **D3**, puis, par recopie, simuler 500 étapes.

5. Faire varier N et représenter graphiquement le nombre de boules dans l'urne A en fonction du temps. Que remarque-t-on ?

Partie B. Étude théorique dans le cas $N = 2$

Soit X_n la variable aléatoire donnant le nombre de boules dans l'urne A à l'issue des n tirages.
Soit E_n la matrice ligne $\begin{pmatrix} P(X_n=0) & P(X_n=1) & P(X_n=2) \end{pmatrix}$. L'état initial est donc $E_0 = (0 \;\; 0 \;\; 1)$.

1. Déterminer E_1, E_2, E_3 et E_4.

2. Déterminer E_n selon la parité de n. Est-ce que le nombre de molécules se stabilise dans les urnes ?

Partie C. Étude théorique dans le cas $N = 4$

Soit E_n la matrice $\begin{pmatrix} P(X_n=0) & P(X_n=1) & P(X_n=2) & P(X_n=3) & P(X_n=4) \end{pmatrix}$.
L'état initial est donc $E_0 = (0 \;\; 0 \;\; 0 \;\; 0 \;\; 1)$.

1. Calculer $P(X_1=0)$, $P(X_1=1)$, $P(X_1=2)$, $P(X_1=3)$ et $P(X_1=4)$.

2. Calculer $P(X_2=0)$, $P(X_2=1)$, $P(X_2=2)$, $P(X_2=3)$ et $P(X_2=4)$.

3. a. En utilisant un arbre de probabilités, exprimer $P(X_{n+1}=0)$ en fonction des probabilités $P(X_n=j)$, où $j \in \{0, 1, 2, 3, 4\}$.

b. Faire de même pour $P(X_{n+1}=1)$, $P(X_{n+1}=2)$, $P(X_{n+1}=3)$ et $P(X_{n+1}=4)$.

4. Écrire la matrice A telle que $E_{n+1} = E_n \times A$. En déduire E_n en fonction de E_0 et A.

5. À l'aide de la calculatrice ou d'un logiciel, déterminer E_3, E_{10} et E_{50}. Que peut-on en conclure ?

6. a. Montrer par récurrence que $E_n = \begin{pmatrix} \frac{1}{8} - \frac{1}{2^{n+1}} & 0 & \frac{3}{4} & 0 & \frac{1}{8} + \frac{1}{2^{n+1}} \end{pmatrix}$ pour n entier naturel pair non nul et que, si n est impair, alors : $E_n = \begin{pmatrix} 0 & \frac{1}{2} - \frac{1}{2^n} & 0 & \frac{1}{2} + \frac{1}{2^n} & 0 \end{pmatrix}$.

b. La suite de matrices (E_n) semble-t-elle avoir une « limite » en $+\infty$?

7. Déterminer l'espérance mathématique de X_n, ainsi que sa limite en $+\infty$.

Cours 1

Suites telles que $U_{n+1} = AU_n + B$

Suites de matrices

Définition Une suite de matrices colonnes de taille p (p entier, $p \geqslant 2$) est une fonction de $\mathbb{N}$ dans l'ensemble des matrices colonnes de taille p.

Si (U_n) est une suite de matrices colonnes, tous les coefficients de la matrice U_n sont des termes de suites numériques.

Exemple : La suite (U_n) définie par $U_n = \begin{pmatrix} n+2 \\ n^2 \end{pmatrix}$ est une suite de matrices dont les termes sont les suites numériques (u_n) et (v_n) telles que $u_n = n + 2$ et $v_n = n^2$.

À noter
On peut aussi définir de la même façon une suite de matrices lignes.

Définition Une suite de matrices converge si, et seulement si, toutes les suites formant les éléments de cette matrice convergent.

Exemple : La suite (U_n) telle que $U_n = \begin{pmatrix} e^{-n} \\ 1 - e^{-2n} \end{pmatrix}$ converge vers la matrice $U^* = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

À noter
Si une suite de matrices (U_n) converge, sa limite est la matrice ayant pour éléments les limites de chaque suite composant (U_n).

Suites de la forme $U_{n+1} = AU_n + B$

Propriété Soit une suite de matrices colonnes (U_n) de taille p vérifiant, pour tout entier naturel n : $U_{n+1} = AU_n$, où A est une matrice carrée d'ordre p.
Alors, pour tout entier naturel n : $U_n = A^n U_0$.

Vocabulaire
Une suite de matrices colonnes est **constante** si cette suite est formée de matrices égales entre elles.

Démonstration Soit la propriété $P(n)$ dépendant de l'entier naturel n : $U_n = A^n U_0$.
- **Initialisation** : $P(0)$ est vraie, car $A^0 = I_p$ et $I_p U_0 = U_0$.
- **Hérédité** : On suppose $P(n)$ vraie pour un entier naturel n.

Alors, $U_n = A^n U_0$, d'où $U_{n+1} = A \times A^n U_0 = A^{n+1} U_0$: $P(n+1)$ est vraie.
Conclusion : $P(0)$ est vraie et P est héréditaire, $P(n)$ est donc vraie pour toute valeur de n.

Propriété Soit une suite de matrices colonnes (U_n) de taille p vérifiant, pour tout entier naturel n : $U_{n+1} = AU_n + B$, où A est une matrice carrée non nulle d'ordre p et B une matrice colonne de taille p. S'il existe une matrice C telle que $C = AC + B$, alors le terme général de cette suite peut s'écrire : $U_n = A^n(U_0 - C) + C$.

À noter
On cherche une suite constante égale à C vérifiant la relation de récurrence.

Remarque : Si $I_p - A$ est inversible, alors $C = (I_p - A)^{-1} B$.

Démonstration Puisque $C = AC + B$, et $U_{n+1} = AU_n + B$, on obtient par différence :
$U_{n+1} - C = AU_n - AC = A(U_n - C)$.
La suite (V_n) telle que $V_n = U_n - C$ vérifie $V_{n+1} = AV_n$, donc $V_n = A^n V_0$.
On en déduit $U_n - C = A^n(U_0 - C)$, soit $U_n = A^n(U_0 - C) + C$.

Vocabulaire
Les suites numériques définies par la relation de récurrence $u_{n+1} = au_n + b$ sont appelées suites **arithmético-géométriques**.

Cas particulier : Si U_n, A et B sont des matrices de format $(1, 1)$, que l'on peut identifier à des réels, on a $u_{n+1} = au_n + b$. Le réel c existe si $1 - a$ est inversible, soit pour $a \neq 1$, et alors, $u_n = (u_0 - c)a^n + c$, où $c = \dfrac{b}{1-a}$. Pour $a = 1$, (u_n) est une suite arithmétique et $u_n = u_0 + nb$.

Convergence des suites vérifiant $U_{n+1} = AU_n + B$

Propriété Soit une suite de matrices colonnes vérifiant $U_{n+1} = AU_n + B$.
On suppose qu'il existe une matrice C telle que $C = AC + B$.
(1) Si $U_0 = C$, la suite converge vers C.
(2) Si $U_0 \neq C$ et si la suite (A^n) converge, alors la suite (U_n) converge.

Démonstration Si $U_0 = C$, alors pour tout naturel n, $U_n = C$, donc (U_n) converge vers C. Sinon, puisque $U_n = A^n(U_0 - C) + C$ et (A^n) converge vers A', on en déduit que (U_n) converge vers : $A'(U_0 - C) + C$.

Savoir-faire 1 Étudier une suite vérifiant $U_{n+1} = AU_n$

➤ Voir les exercices 29 et 30

Soit la suite de matrices colonnes (U_n) définies par $U_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et par la relation de récurrence $U_{n+1} = AU_n$, avec $A = \begin{pmatrix} 0,3 & -0,1 \\ 0,2 & 0 \end{pmatrix}$.

1. Montrer que $A^n = 0,1^n \begin{pmatrix} 2^{n+1}-1 & 1-2^n \\ 2^{n+1}-2 & 2-2^n \end{pmatrix}$. En déduire l'expression de U_n en fonction de n.

2. La suite (U_n) est-elle convergente ?

Méthode
Pour déterminer la limite d'une suite de matrices, on détermine la limite de chaque élément de la matrice.

Solution

1. On fait un raisonnement par récurrence. Soit $P(n)$ la propriété : « $A^n = 0,1^n \begin{pmatrix} 2^{n+1}-1 & 1-2^n \\ 2^{n+1}-2 & 2-2^n \end{pmatrix}$ ».

• **Initialisation.** On vérifie que $P(0)$ est vraie : $0,1^0 \begin{pmatrix} 2^{0+1}-1 & 1-2^0 \\ 2^{0+1}-2 & 2-2^0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = A^0$.

• **Hérédité.** On suppose $P(n)$ vraie pour un entier naturel n. Alors :

$A^{n+1} = 0,1^n \begin{pmatrix} 2^{n+1}-1 & 1-2^n \\ 2^{n+1}-2 & 2-2^n \end{pmatrix} \times 0,1 \begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix} = 0,1^{n+1} \begin{pmatrix} 2 \times 2^{n+1} - 1 & 1-2^{n+1} \\ 2 \times 2^{n+1} - 2 & 2-2^{n+1} \end{pmatrix}$, donc $P(n+1)$ est vraie.

On en déduit que $U_n = 0,1^n \begin{pmatrix} 2^{n+1}-1+1-2^n \\ 2^{n+1}-2+2-2^n \end{pmatrix} = 0,1^n \begin{pmatrix} 2^n \\ 2^n \end{pmatrix} = \begin{pmatrix} 0,2^n \\ 0,2^n \end{pmatrix}$.

2. La suite (U_n) converge vers la matrice $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, car $\lim\limits_{n \to +\infty} (0,2^n) = 0$.

Savoir-faire 2 Étudier une suite de matrices vérifiant $U_{n+1} = AU_n + B$

➤ Voir les exercices 39 et 40

Soit la matrice $A = \begin{pmatrix} 0,3 & 0,2 \\ 0,1 & 0,4 \end{pmatrix}$ et $B = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$. On définit la suite de matrices (U_n) par $U_0 = \begin{pmatrix} 24 \\ 3 \end{pmatrix}$ et, pour tout entier naturel n : $U_{n+1} = AU_n + B$.

1. Montrer que $A = PDQ$, avec $P = \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 0,5 & 0 \\ 0 & 0,2 \end{pmatrix}$ et $Q = \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} \end{pmatrix}$.
Calculer QP et en déduire A^n en fonction de n.

2. Exprimer U_n en fonction de n, puis étudier la convergence de la suite (U_n).

Méthode
Pour déterminer le terme général d'une suite telle que $U_{n+1} = AU_n + B$, on commence par trouver une suite constante solution.

Solution

1. On calcule d'abord $PD = \begin{pmatrix} 0,5 & -0,4 \\ 0,5 & 0,2 \end{pmatrix}$, puis $(PD)Q = \begin{pmatrix} 0,3 & 0,2 \\ 0,1 & 0,4 \end{pmatrix} = A$.

Alors $A^n = (PDQ)(PDQ) \dots (PDQ) = PD^nQ$, car $QP = I_2$. D'où :

$$A^n = \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0,5^n & 0 \\ 0 & 0,2^n \end{pmatrix} \times \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 0,5^n + 2 \times 0,2^n & 2 \times 0,5^n - 2 \times 0,2^n \\ 0,5^n - 0,2^n & 2 \times 0,5^n + 0,2^n \end{pmatrix}.$$

2. Si $U_n = C$ pour tout entier naturel n, alors $C = AC + B$, soit $(I_2 - A)C = B$.

$I_2 - A = \begin{pmatrix} 0,7 & -0,2 \\ -0,1 & 0,6 \end{pmatrix}$: cette matrice est inversible et la calculatrice donne $(I_2 - A)^{-1} = \begin{pmatrix} 1,5 & 0,5 \\ 0,25 & 1,75 \end{pmatrix}$.

On vérifie que c'est bien l'inverse. D'où $C = (I_2 - A)^{-1} \times B = \begin{pmatrix} 1,5 & 0,5 \\ 0,25 & 1,75 \end{pmatrix} \times \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 3 \end{pmatrix}$.

On en déduit : $U_{n+1} - C = A(U_n - C)$, et ainsi $U_n - C = A^n(U_0 - C)$.

D'où $U_n = \begin{pmatrix} 18 \\ 3 \end{pmatrix} + \frac{1}{3} \begin{pmatrix} 0,5^n + 2 \times 0,2^n & 2 \times 0,5^n - 2 \times 0,2^n \\ 0,5^n - 0,2^n & 2 \times 0,5^n + 0,2^n \end{pmatrix} \times \begin{pmatrix} 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 + 2 \times 0,5^n + 4 \times 0,2^n \\ 3 + 2 \times 0,5^n - 2 \times 0,2^n \end{pmatrix}$.

La limite de $0,5^n$ est 0, comme celle de $0,2^n$. On en déduit que $\lim\limits_{n \to +\infty} (18 + 2 \times 0,5^n + 4 \times 0,2^n) = 18$ et $\lim\limits_{n \to +\infty} (3 + 2 \times 0,5^n - 2 \times 0,2^n) = 3$: la suite (U_n) converge vers la matrice $U^* = \begin{pmatrix} 18 \\ 3 \end{pmatrix}$.

Problème 4

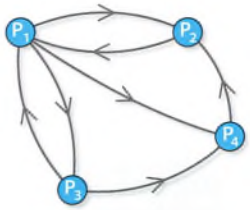
Un Web en miniature

Objectif
Découvrir une marche aléatoire.

Cours 2
Étude des marches aléatoires

Comment les moteurs de recherche s'y prennent-ils pour classer les millions de pages qui contiennent le mot sur lequel on cherche des informations sur Internet ? On va étudier, dans un cas simple, le fonctionnement de l'algorithme de calcul du « *PageRank* » d'une page Web, utilisé par Google.

On considère quatre pages Web reliées entre elles par des liens « hypertexte » permettant de passer de l'une à l'autre.



On notera $j \mapsto i$ un lien de la page P_j vers la page P_i.
Un surfeur passe d'une page à l'autre.
On va étudier la position du surfeur au bout de n étapes.
Pour cela, on considère la variable aléatoire X_n égale respectivement à 1, 2, 3 ou 4 selon que le surfeur est en P_1, P_2, P_3 ou P_4.

Partie A. Premier modèle

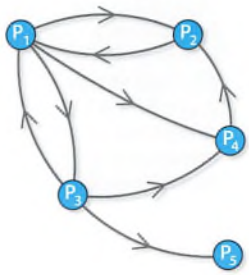
Le surfeur est un promeneur impartial qui navigue sur cette toile en cliquant sans préférence sur les liens qui lui sont offerts.

1. On suppose que le surfeur part de la page P_1.
On a donc $P(X_0 = 1) = 1$, $P(X_0 = 2) = 0$, $P(X_0 = 3) = 0$ et $P(X_0 = 4) = 0$.
a. Déterminer $P(X_1 = 1)$, $P(X_1 = 2)$, $P(X_1 = 3)$ et $P(X_1 = 4)$.
b. À l'aide d'un arbre de probabilités, déterminer $P(X_2 = 1)$, $P(X_2 = 2)$, $P(X_2 = 3)$ et $P(X_2 = 4)$.

2. Le surfeur commence sa navigation à une page quelconque.
a. Montrer que $P(X_{n+1} = 1) = P(X_n = 2) + \frac{1}{2}P(X_n = 3)$.
b. Exprimer de la même façon $P(X_{n+1} = k)$, pour $k \in \{2, 3, 4\}$, en fonction de $P(X_n = 1)$, $P(X_n = 2)$, $P(X_n = 3)$ et $P(X_n = 4)$.
c. Soit U_n la matrice ligne $\begin{pmatrix} P(X_n = 1) & P(X_n = 2) & P(X_n = 3) & P(X_n = 4) \end{pmatrix}$.
Déterminer la matrice A telle que $U_{n+1} = U_n \times A$.
A est appelée matrice de transition de cette promenade aléatoire.
d. Préciser la position du surfeur au bout de 20 étapes si celui-ci part de P_1.
Quelle est cette position si le surfeur part de P_2 ? de P_3 ? de P_4 ?
e. À l'aide de la calculatrice ou d'un logiciel, calculer A^{10}, A^{20} et A^{80} (on arrondira les coefficients des matrices à 10^{-3} près). Émettre une conjecture sur la position limite du surfeur.
f. Déterminer la matrice ligne X telle que $X \times A = X$. Que remarque-t-on ?
La matrice solution dont la somme des éléments est 1 s'appelle le régime stationnaire.

Partie B. Second modèle

Le modèle précédent va être amélioré afin de corriger un défaut.



1. Supposons qu'on ajoute à cette toile une page P_5 n'ayant aucun lien « hypertexte » la reliant à une autre page. Que va-t-il se passer pour le surfeur au bout d'un certain nombre d'étapes ?

2. On définit une nouvelle matrice de transition A' en ajoutant à la matrice A une matrice B qui représente les goûts du promeneur, avec un coefficient c élément de [0 ; 1] tel que $A' = cA + (1 - c)B$ (A représente la structure des liens de la toile et B représente les goûts du promeneur).
Puisque Google ne peut deviner les goûts de l'internaute, on choisit pour B la matrice dont tous les éléments sont $\frac{1}{n}$, où n est le nombre de pages de la toile. Que se passe-t-il si on choisit $c = 0$? $c = 1$?

3. On choisit à présent, comme les concepteurs de cet algorithme : $c = 0{,}85$.
On reprend la toile formée des quatre pages Web de la **partie A**.
a. Déterminer la nouvelle matrice de transition A'.
b. À l'aide de la calculatrice ou d'un logiciel, calculer A'^{10}, A'^{20} et A'^{80} (on arrondira les coefficients des matrices à 10^{-3} près). Quel est le nouvel état stationnaire ?

Point Histoire
Larry Page (né en 1973) est un informaticien américain, cofondateur du moteur de recherche Google avec Sergey Brin. Le premier brevet relatif au *PageRank* a été déposé en 1997.

Problème 5 Les émissions concurrentes

Objectif
Découvrir le comportement asymptotique d'une marche aléatoire à deux états.

Cours 3
Étude asymptotique des marches aléatoires

Deux chaînes de télévision A et B programment chaque semaine, à la même heure, deux émissions concurrentes. On suppose que le nombre global de téléspectateurs de ces émissions reste constant. Au début de l'étude, 70 % de ces téléspectateurs regardent la chaîne A. Une étude statistique a montré que 15 % des téléspectateurs qui ont regardé la chaîne A une semaine, regardent la chaîne B la semaine suivante. On a aussi noté que 10 % des téléspectateurs qui ont regardé la chaîne B une semaine, regardent la chaîne A la semaine suivante.

1. a. On note respectivement a_n et b_n les proportions de téléspectateurs des chaînes A et B au bout de n semaines et X_n la matrice ligne $(a_n \ \ b_n)$. On pose $X_0 = (a_0 \ \ b_0)$. Que vaut a_0 ?
b. Utiliser un arbre de probabilités pour déterminer l'expression de a_{n+1} en fonction de a_n et b_n, ainsi que l'expression de b_{n+1} en fonction de a_n et b_n.

2. Déterminer la matrice A telle que $X_{n+1} = X_n \times A$. Que peut-on dire des lignes de la matrice A ?

3. a. Calculer A^2 et A^3. En déduire X_2 et X_3.
b. Quelle est la proportion de téléspectateurs regardant la chaîne A au bout de 3 semaines ?

4. Soit la matrice $P = \begin{pmatrix} 1 & -1,5 \\ 1 & 1 \end{pmatrix}$. Déterminer P^{-1}, puis $D = P^{-1} \times A \times P$.

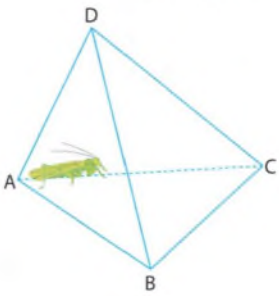
5. Calculer D^n, puis en déduire la matrice A^n en fonction de n.

6. a. Calculer la matrice X_n en fonction de n, a_0 et b_0.
b. Quelle est l'influence des proportions initiales sur une éventuelle convergence de la suite (X_n) ?

Problème 6 Une sauterelle dans une cage tétraédrique

Objectif
Découvrir le comportement asymptotique d'une marche aléatoire à quatre états.

Cours 3
Étude asymptotique des marches aléatoires



Une sauterelle se déplace toutes les minutes d'un sommet à l'autre de sa cage qui a la forme d'un tétraèdre.
Elle reste exactement une minute au même endroit.
Quand elle est au sommet A, elle a autant de chances d'aller sur les trois autres sommets.
Quand elle est au sommet B, elle ne se rend que sur les sommets A et D, de façon équiprobable.
Quand elle est au sommet C, elle ne se rend que sur les sommets A et B, et elle choisit A avec une probabilité égale à $\frac{1}{3}$.
Quand elle est au sommet D, elle choisit A, B ou C avec les probabilités respectives $\frac{1}{2}$, $\frac{1}{4}$ et $\frac{1}{4}$. À l'instant 0 où on met la sauterelle dans sa cage, celle-ci se trouve en A.

1. Quelle est la probabilité que la sauterelle se trouve en B après une minute ? après deux minutes ?

2. On note A_n l'événement « la sauterelle est au sommet A au bout de n minutes ».
Les événements B_n, C_n et D_n sont définis de façon similaire.
a. À l'aide d'un arbre de probabilités, exprimer $P(A_{n+1})$ en fonction de $P(A_n)$, $P(B_n)$, $P(C_n)$ et $P(D_n)$.
b. Exprimer de même $P(B_{n+1})$, $P(C_{n+1})$ et $P(D_{n+1})$ en fonction de $P(A_n)$, $P(B_n)$, $P(C_n)$ et $P(D_n)$.

3. On note X_n la matrice ligne $(P(A_n) \ \ P(B_n) \ \ P(C_n) \ \ P(D_n))$.
Déterminer la matrice carrée M telle que $X_{n+1} = X_n \times M$.

4. Avec une calculatrice ou un logiciel, calculer M^2, M^{10} et M^{60}.

5. Quelle est la probabilité que la sauterelle soit en A au bout de dix minutes ? au bout d'une heure ?

6. Que constate-t-on ? Interpréter ce résultat.

7. Résoudre l'équation $X = XM$, dont l'inconnue est $X = (x \ \ y \ \ z \ \ t)$, avec $x + y + z + t = 1$.

Cours 2

Étude des marches aléatoires

Généralités sur les marches aléatoires

À noter

Les suites matricielles étudiées dans cette partie sont liées à des processus aléatoires : on parle de marche aléatoire à deux ou plusieurs états.

Définition Soit une expérience aléatoire ayant N issues possibles $S_1, S_2, \dots S_N$.

X_n	S_1	S_2	...	...	S_N
$P(X_n = S_i)$	a_1	a_2			a_N

Une **marche aléatoire** sur $E = \{S_1, S_2, \dots, S_N\}$ est une suite de variables aléatoires (X_n), prenant chacune pour valeurs les différents états possibles, telle que l'état du processus à l'instant $(n + 1)$ ne dépend que de celui à l'instant n précédent, mais non de ses états antérieurs, et ceci indépendamment de n.

À noter

$S_1, S_2, \dots, S_N$ sont les **états** du processus.
Le processus prend un nombre fini d'états et évolue par étapes successives d'un état à l'autre.

La loi de probabilité de X_n, qui donne la probabilité de chaque état à l'étape n, est appelée l'**état probabiliste à l'étape n**. On note U_n la matrice ligne : $U_n = \big(P(X_n = S_1)\ \ P(X_n = S_2) \dots P(X_n = S_N)\big)$. Cette suite de matrices (U_n) décrit l'évolution du système. Ce processus est « sans mémoire ».

Définition La **probabilité de passage** (ou de transition) de l'état i à l'état j en une étape (ou une transition) est la probabilité $P_{X_n = i}(X_{n+1} = j)$. On la note $p_{i,j}$.

Définition La matrice dont le coefficient situé à la ligne i et à la colonne j est $p_{i,j}$ est la **matrice de transition de la marche aléatoire**.

Vocabulaire

Une matrice possédant ces deux propriétés est appelée une matrice **stochastique**.

Propriétés Soit une matrice de transition formée des éléments $p_{i,j}$.

(1) Tous ses éléments sont compris entre 0 et 1 : $0 \leqslant p_{i,j} \leqslant 1$.

(2) La somme des éléments de chaque ligne est 1 : $\sum_{j=1}^{N} p_{i,j} = 1$.

À noter

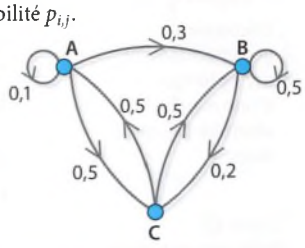
$$\begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{ccc} S_1 & S_2 & S_3 \end{array} \\ \begin{pmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,2} \\ p_{3,2} & p_{3,2} & p_{3,3} \end{pmatrix} \end{array}$$

Graphe associé à une matrice de transition

À toute marche aléatoire, on peut associer un graphe. Ce graphe est construit de la façon suivante :
– les états sont représentés par des points : ce sont les sommets du graphe ;
– le passage d'un état à un autre est symbolisé par un arc orienté reliant deux sommets (un sommet pouvant être relié à lui-même) : ce sont les arêtes du graphe ;
– sur chaque arc orienté de l'état i vers l'état j est noté la probabilité $p_{i,j}$.

Exemple : Soit la matrice de transition d'une marche aléatoire à trois états : $M = \begin{pmatrix} 0{,}1 & 0{,}3 & 0{,}5 \\ 0 & 0{,}5 & 0{,}2 \\ 0{,}5 & 0{,}5 & 0 \end{pmatrix}$

Le graphe de cette marche aléatoire est ci-contre.



Marche aléatoire à deux états

Propriété Toute matrice de transition d'une marche aléatoire à deux états est de la forme $\begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}$, où $a = P_{X_n = S_1}(X_{n+1} = S_2)$ et $b = P_{X_n = S_2}(X_{n+1} = S_1)$.

Démonstration La matrice est de cette forme, car la somme des éléments de chaque ligne est 1.

Propriété Soit U_n la matrice ligne associée à une marche aléatoire à l'instant n.
Si M est sa matrice de transition, alors $U_{n+1} = U_n M$. De plus : $U_n = U_0 M^n$.

Démonstration (dans le cas de deux états)

Le premier élément de U_{n+1} est $P(X_{n+1} = S_1)$. La formule des probabilités totales donne :

$P(X_{n+1} = S_1) = P_{X_n = S_1}(X_{n+1} = S_1) \times P(X_n = S_1) + P_{X_n = S_2}(X_{n+1} = S_1) \times P(X_n = S_2)$

$= p_{1,1} \times P(X_n = S_1) + p_{1,2} \times P(X_n = S_2)$

De même : $P(X_{n+1} = S_2) = p_{2,1} \times P(X_n = S_1) + p_{2,2} \times P(X_n = S_2)$.

On en déduit : $U_{n+1} = U_n M$, et ainsi $U_n = U_0 M^n$, d'après les résultats du cours 1.

Savoir-faire 3

➤ Voir l'exercice 53

Modéliser une marche aléatoire

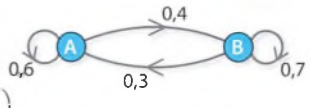
Un couple part en voyage chaque année. S'il est resté en France une année donnée, la probabilité que ce couple voyage à l'étranger l'année suivante est 0,4. Dans le cas contraire, la probabilité qu'il voyage à nouveau à l'étranger est 0,7. En 2012, ce couple est allé à l'étranger.

1. Représenter cette marche aléatoire à l'aide d'un graphe.
2. Écrire la matrice de transition M de cette marche aléatoire.
3. Quelle est la probabilité que ce couple parte à l'étranger en 2017 ?

Méthode
Pour déterminer l'état probabiliste à l'étape n d'une marche aléatoire de matrice de transition M, on calcule d'abord M^n.

Solution

1. On note A l'état « le couple reste en France » et B l'état « le couple part à l'étranger ».



2. $P_{X_n=A}(X_{n+1}=B)=0,4$ et $P_{X_n=B}(X_{n+1}=B)=0,7$; $M=\begin{pmatrix}0,6 & 0,4\\ 0,3 & 0,7\end{pmatrix}$, avec comme ordre des états : A, B.
3. L'état initial est modélisé par $U_0=(0\ \ 1)$. L'état en 2017 est donné par la matrice U_5, avec $U_5=U_0M^5$. Avec la calculatrice, on trouve à 10^{-3} près : $M^5=\begin{pmatrix}0,430 & 0,570\\ 0,428 & 0,572\end{pmatrix}$ et $U_5=(0,428\ \ 0,572)$.

La probabilité cherchée est donc 0,572 (à 10^{-3} près).

Savoir-faire 4

➤ Voir l'exercice 60

Étudier une marche aléatoire

Une puce saute d'un sommet d'un triangle ABC à un autre : elle choisit indifféremment l'un ou l'autre des sommets restants. Elle part du sommet A à l'instant 0.

1. Écrire la matrice de transition M de cette marche aléatoire.
2. Soit la matrice $P=\begin{pmatrix}1 & 2 & -1\\ 1 & 0 & 2\\ 1 & -2 & -1\end{pmatrix}$. Déterminer P^{-1}, puis $D=P^{-1}MP$.

En déduire M^n en fonction de n, où n est un entier naturel.

3. Quelle est la probabilité que la puce soit à nouveau en A à l'instant n ?

Conseil
Pour écrire la matrice de transition d'une marche aléatoire, faire attention à l'ordre des états.

Solution

1. La probabilité pour la puce de sauter sur un autre sommet est $\frac{1}{2}$, donc on obtient :

$$M=\begin{pmatrix}0 & \frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & 0 & \frac{1}{2}\\ \frac{1}{2} & \frac{1}{2} & 0\end{pmatrix}$$, l'ordre des états étant A, B, C.

2. On trouve après calculs : $D=\begin{pmatrix}1 & 0 & 0\\ 0 & -\frac{1}{2} & 0\\ 0 & 1 & -\frac{1}{2}\end{pmatrix}$ et $M^n=\begin{pmatrix}\frac{1}{3}+\frac{2}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n\\ \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}+\frac{2}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n\\ \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n & \frac{1}{3}+\frac{2}{3}\left(-\frac{1}{2}\right)^n\end{pmatrix}$

3. $U_0=(1\ 0\ 0)$ et $U_n=U_0\times M^n$, d'où $U_n=\left(\frac{1}{3}+\frac{2}{3}\left(-\frac{1}{2}\right)^n\ \ \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n\ \ \frac{1}{3}-\frac{1}{3}\left(-\frac{1}{2}\right)^n\right)$.

Donc la probabilité que la puce soit en A à l'instant n est $\frac{1}{3}+\frac{2}{3}\left(-\frac{1}{2}\right)^n$.

Cours 3

Étude asymptotique des marches aléatoires

Étude asymptotique d'une marche aléatoire à deux états

Vocabulaire
On parle d'état stable ou d'état **stationnaire**.

Propriété Soit une marche aléatoire à deux états, de matrice de transition $M=\begin{pmatrix}1-a & a\\ b & 1-b\end{pmatrix}$.
Pour (a, b) différent de $(0, 0)$ et $(1, 1)$, la suite des états probabilistes converge vers un état indépendant de la distribution initiale. Cet état probabiliste est l'**état stable** : $\pi=\left(\frac{b}{a+b}\quad\frac{a}{a+b}\right)$.
L'état stable π est solution de l'équation $\pi M=\pi$.

À noter
L'état stable $(x\ y)$ est tel que $x+y=1$.

Démonstration Soit U_n la matrice ligne associée à cette marche aléatoire, et $U_0=(x_0\ \ y_0)$ avec $x_0+y_0=1$.

Soit la matrice $S=\begin{pmatrix}1 & a\\ 1 & -b\end{pmatrix}$ et (a, b) différent de $(0, 0)$ et $(1, 1)$.

Alors, puisque $a+b\neq 0$, S est inversible et $S^{-1}=\frac{1}{a+b}\begin{pmatrix}b & a\\ 1 & -1\end{pmatrix}$.

D'où : $S^{-1}MS=S^{-1}\times\begin{pmatrix}1 & a(1-a-b)\\ 1 & -b(1-a-b)\end{pmatrix}$ et $S^{-1}MS=\begin{pmatrix}1 & 0\\ 0 & 1-a-b\end{pmatrix}$.

En notant $D=\begin{pmatrix}1 & 0\\ 0 & 1-a-b\end{pmatrix}$, on a $M=SDS^{-1}$. D'où $M^n=(SDS^{-1})\dots(SDS^{-1})=SD^nS^{-1}$.

Puisque $D^n=\begin{pmatrix}1 & 0\\ 0 & (1-a-b)^n\end{pmatrix}$, on obtient : $M^n=\frac{1}{a+b}\begin{pmatrix}b+a(1-a-b)^n & a-a(1-a-b)^n\\ b-b(1-a-b)^n & a+b(1-a-b)^n\end{pmatrix}$.

$0\leqslant a+b\leqslant 2$, donc $-1\leqslant 1-a-b\leqslant 1$.
Puisque $a+b$ n'est égal ni à 0, ni à 2, $(1-a-b)^n$ a pour limite 0 et M^n a pour limite $\frac{1}{a+b}\begin{pmatrix}b & a\\ b & a\end{pmatrix}$.

Puisque $U^n=U_0M^n$, alors la suite U_n converge vers $\frac{1}{a+b}(x_0\ \ y_0)\times\begin{pmatrix}b & a\\ b & a\end{pmatrix}$,

soit $\frac{1}{a+b}(bx_0+by_0\quad ax_0+ay_0)=\left(\frac{b}{a+b}\quad\frac{a}{a+b}\right)=\pi$.

On peut remarquer que cette matrice π est la solution de l'équation $U=UM$.

En effet : $\pi M=\left(\frac{b}{a+b}\quad\frac{a}{a+b}\right)\times\begin{pmatrix}1-a & a\\ b & 1-b\end{pmatrix}=\left(\frac{b(1-a)+ab}{a+b}\quad\frac{ab+a(1-b)}{a+b}\right)$,

soit $\pi M=\left(\frac{b}{a+b}\quad\frac{a}{a+b}\right)=\pi$.

Point Histoire
Andrei Markov (1856 – 1922) est un mathématicien russe. Ses travaux en probabilités l'ont amené à définir les chaînes de Markov, dont les marches aléatoires étudiées ici sont un cas particulier.

Remarques :
- Si $a=0$ et $b=0$, la matrice de transition est la matrice unité. La suite des états est constante, donc elle converge, mais la limite dépend de la distribution initiale : il n'y a pas d'état stable.
- Si $a=1$ et $b=1$, alors $P^2=I_2$, $P^3=P\dots$ donc la suite ne converge pas car elle prend successivement deux valeurs différentes : il n'y a pas d'état stable.

Étude asymptotique d'une marche aléatoire à *N* états

Logique
Cette condition est suffisante, mais elle n'est pas nécessaire.

Propriété Soit une marche aléatoire à N états ($N\geqslant 3$) dont la matrice de transition est M.
S'il existe un entier naturel n tel que la matrice M^n n'a aucun élément égal à 0, alors la suite (U_n) décrivant l'état probabiliste de cette marche aléatoire converge.
La limite de cette suite définit un **état stable** : celui-ci est solution de l'équation $U=U\times M$.

Ceci est réalisé en particulier si la matrice M ne comporte aucun zéro.

Exemple : Soit la marche aléatoire à trois états dont la matrice de transition est

$M=\begin{pmatrix}0,8 & 0 & 0,2\\ 0 & 0,1 & 0,9\\ 0,5 & 0,5 & 0\end{pmatrix}$. Alors $M^2=\begin{pmatrix}0,64 & 0,34 & 0,02\\ 0,05 & 0,81 & 0,14\\ 0,65 & 0,10 & 0,25\end{pmatrix}$.

M^2 ne contient pas de 0, donc la suite décrivant l'état probabiliste de cette marche aléatoire converge vers un état stable.

Savoir-faire 5

➤ Voir l'exercice 67

Étudier la convergence d'une marche aléatoire à deux états

Deux joueurs de tennis A et B décident de jouer une partie toutes les semaines.
La probabilité que A gagne la partie de la première semaine est 0,7. Si A gagne la partie de la semaine n, la probabilité qu'il gagne la semaine suivante est seulement de 0,4. Si A perd la partie de la semaine n, il change de stratégie et la probabilité qu'il gagne la semaine suivante est de 0,9. On note S_1 l'état « A gagne la semaine n » et S_2 l'état « B gagne la semaine n ».

1. Écrire la matrice de transition associée à cette marche aléatoire, en considérant les états dans l'ordre S_1, S_2.

2. Déterminer l'état stable de cette marche aléatoire. Conclure.

Méthode
Pour déterminer l'état stable $(x \ \ y)$ d'une marche aléatoire de matrice M, on résout l'équation :
$(x \ \ y) \times M = (x \ \ y)$, avec $x + y = 1$.

Solution

1. La matrice de transition est $M = \begin{pmatrix} 0,4 & 0,6 \\ 0,9 & 0,1 \end{pmatrix}$.

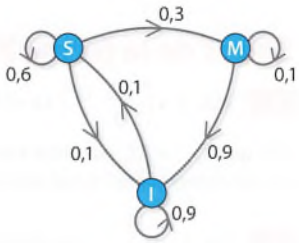
2. L'état stable de cette marche aléatoire existe, car la matrice A ne contient pas de 0. Cet état stable est défini par la matrice $\pi = (x \ \ y)$ telle que $\pi M = \pi$, soit $\begin{cases} 0,4x + 0,9y = x \\ 0,6x + 0,1y = y \end{cases}$ qui équivaut à $2x = 3y$.
Or $x + y = 1$, donc $2x = 3(1 - x)$, soit $5x = 3$ et $x = \frac{3}{5}$. L'état stable est donc $\left(\frac{3}{5} \ \ \frac{2}{5}\right)$: lorsque n tend vers l'infini, la probabilité que A gagne se stabilise à 0,6.

Savoir-faire 6

➤ Voir l'exercice 69

Étudier la convergence d'une marche aléatoire à plusieurs états

Un individu susceptible de contracter une maladie peut être dans un des trois états suivants : S (susceptible de tomber malade), M (infecté par la maladie) et I (immunisé).
Son état peut changer tous les trois mois selon certaines probabilités données dans le graphe ci-contre.



1. Déterminer la matrice de transition de cette marche aléatoire, en considérant les états dans l'ordre S, M, I.

2. Faire une étude asymptotique de cette marche aléatoire.

Méthode
Pour assurer l'existence d'un état stable, il suffit qu'une puissance de la matrice de transition soit sans 0.

Solution

1. $P_{X_n=S}(X_{n+1} = S) = 0,6$; $P_{X_n=S}(X_{n+1} = M) = 0,3$ et $P_{X_n=S}(X_{n+1} = I) = 0,1$. La première ligne de la matrice de transition est donc : 0,6 0,3 0,1. On a aussi $P_{X_n=M}(X_{n+1} = M) = 0,1$ et $P_{X_n=M}(X_{n+1} = I) = 0,9$.
Enfin $P_{X_n=I}(X_{n+1} = S) = 0,1$ et $P_{X_n=I}(X_{n+1} = I) = 0,9$. D'où la matrice de transition : $P = \begin{pmatrix} 0,6 & 0,3 & 0,1 \\ 0 & 0,1 & 0,9 \\ 0,1 & 0 & 0,9 \end{pmatrix}$.

2. $P^2 = \begin{pmatrix} 0,37 & 0,21 & 0,42 \\ 0,09 & 0,01 & 0,9 \\ 0,15 & 0,03 & 0,82 \end{pmatrix}$. Puisque la matrice P^2 ne contient pas de 0, il existe un état stationnaire.
Pour le déterminer, on résout :
$(x \ \ y \ \ z) \times P = (x \ \ y \ \ z)$, soit $\begin{cases} 0,6x + 0,1z = x \\ 0,3x + 0,1y = y \\ 0,1x + 0,9y + 0,9z = z \end{cases}$, soit $\begin{cases} z = 4x \\ x = 3y \\ 4x = z \end{cases}$, soit $z = 4x$ et $y = \frac{1}{3}x$.
Comme $x + y + z = 1$, on en déduit : $x + \frac{1}{3}x + 4x = 1$, soit $x = \frac{3}{16}$. Enfin : $y = \frac{1}{16}$ et $z = \frac{3}{4}$.
Quand le nombre de mois tend vers l'infini, la population tend vers la répartition $\left(\frac{3}{16} \ \ \frac{1}{16} \ \ \frac{3}{4}\right)$: à terme, la proportion de personnes immunisées tend vers 75 %.

Exercices

Les exercices dont les numéros sont sur fond blanc sont corrigés à la fin du manuel.

POUR DÉMARRER

Suites de matrices

1 Soit la suite de matrices colonnes (X_n) telle que, pour tout entier naturel n : $X_n = \begin{pmatrix} n^2-4 \\ 3n+1 \end{pmatrix}$.

Déterminer X_0, X_1, X_2 et X_{20}.

2 Soit la suite de matrices colonnes (X_n) telle que, pour tout entier naturel n : $X_n = \begin{pmatrix} \dfrac{1}{n+1} \\ 0{,}6^n \end{pmatrix}$.

Étudier la convergence de cette suite de matrices.

3 Soit la suite de matrices colonnes (X_n) telle que, pour tout entier naturel n : $X_{n+1} = X_n + B$, où $B = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ et $X_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

1. Calculer X_1, X_2 et X_3.
2. Déterminer l'expression de X_n en fonction de n.
3. La suite (X_n) converge-t-elle ?

4 Soit la suite de matrices colonnes (X_n) telle que, pour tout entier naturel n : $X_{n+1} = \frac{1}{2}X_n$, avec $X_0 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

1. Calculer X_1, X_2 et X_3.
2. Déterminer l'expression de X_n en fonction de n.
3. La suite (X_n) converge-t-elle ?

Suites de la forme $X_{n+1} = AX_n$

5 Soit $A = \begin{pmatrix} 0{,}5 & 0 \\ 0 & 1 \end{pmatrix}$. La suite de matrices colonnes (X_n) telle que $X_{n+1} = AX_n$ pour tout entier naturel n, avec $X_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, est-elle convergente ? Si oui, préciser sa limite.

6 Soit $A = \begin{pmatrix} \dfrac{1}{2} & 1 \\ 0 & 1 \end{pmatrix}$. On définit la suite de matrices colonnes (X_n) telle que $X_{n+1} = AX_n$ pour tout entier naturel n, et $X_0 = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$.

1. Montrer que $A^n = \begin{pmatrix} \dfrac{1}{2^n} & 2 - \dfrac{1}{2^{n-1}} \\ 0 & 1 \end{pmatrix}$.
2. Étudier la convergence de la suite (X_n).

7 Soit les suites (x_n) et (y_n) définies pour tout entier naturel n par : $\begin{cases} x_{n+1} = x_n + y_n \\ y_{n+1} = -2x_n + 4y_n \end{cases}$, avec $x_0 = 1$ et $y_0 = 0$.

1. On note $X_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

Déterminer la matrice A telle que $X_{n+1} = AX_n$.

2. On admet que $A^n = \begin{pmatrix} 2^{n+1} - 3^n & 3^n - 2^n \\ 2^{n+1} - 2 \times 3^n & 2 \times 3^n - 2^n \end{pmatrix}$.

En déduire x_n et y_n en fonction de n.

3. Étudier la convergence des suites (x_n) et (y_n).

Suites arithmético-géométriques

8 Soit la suite (u_n) telle que $u_0 = 0$, et pour tout entier naturel n : $u_{n+1} = 2u_n + 3$ **(R)**.

1. Montrer que la suite (c_n) telle que $c_n = -3$ vérifie la relation **(R)**.
2. Montrer que la suite de terme général $v_n = u_n - c_n$ est géométrique, puis exprimer u_n en fonction de n.

9 Soit la suite (u_n) telle que $u_0 = 2$, et pour tout entier naturel n : $u_{n+1} = 3u_n - 2$.

1. Déterminer la suite constante égale à c, solution de cette relation.
2. Montrer que la suite de terme général $v_n = u_n - c$ est géométrique, puis exprimer u_n en fonction de n.

10 Soit la suite (u_n) telle que $u_0 = 2$, et pour tout entier naturel n : $u_{n+1} = \frac{1}{4}u_n - 3$.

1. Déterminer la suite constante égale à c, solution de cette relation.
2. Montrer que la suite de terme général $v_n = u_n - c$ est géométrique, puis exprimer u_n en fonction de n.
3. Étudier la convergence de la suite (u_n).

Suites de la forme $X_{n+1} = AX_n + B$

11 Soit la suite de matrices colonnes (X_n) telle que :

$$X_{n+1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix} X_n + \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ et } X_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

1. Montrer que la suite constante (C_n) définie pour tout entier naturel n par $C_n = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ vérifie cette relation.
2. Déterminer X_n en fonction de n.
3. La suite (X_n) est-elle convergente ?

12 Soit la suite de matrices colonnes (X_n) telle que :

$$X_{n+1} = \begin{pmatrix} 0{,}2 & 0 \\ 0 & 2 \end{pmatrix} X_n + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } X_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

1. Déterminer la suite constante vérifiant cette relation.
2. Pourquoi la suite (X_n) n'est-elle pas convergente ?

13 Soit $A = \begin{pmatrix} 0{,}25 & 0 \\ 0 & 0{,}4 \end{pmatrix}$. La suite de matrices colonnes (X_n) telle que $X_{n+1} = AX_n + B$, avec $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $X_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ est-elle convergente ? Si oui, préciser sa limite.

14 Soit $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$. On définit la suite de matrices colonnes (X_n) par la relation $X_{n+1} = AX_n + B$ pour tout entier naturel n, et $X_0 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$.

1. Montrer que la matrice $C = \begin{pmatrix} -1 \\ -2 \end{pmatrix}$ vérifie la relation de récurrence $X_{n+1} = AX_n + B$.

2. **a.** Soit $D = \frac{1}{2}A$. Déterminer la matrice N telle que $D = I_2 + N$.

b. Calculer N^2, puis D^2, D^3, D^4 en fonction de I_2 et N.

c. En déduire D^n, puis A^n.

3. La suite (X_n) est-elle convergente ?

Marches aléatoires

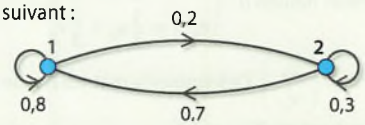
15 La matrice de transition d'une marche aléatoire à deux états est $A = \begin{pmatrix} 0{,}25 & a \\ b & 0{,}4 \end{pmatrix}$. Déterminer les réels a et b.

16 La matrice de transition d'une marche aléatoire à deux états A et B est $M = \begin{pmatrix} 0{,}1 & 0{,}9 \\ 0{,}4 & 0{,}6 \end{pmatrix}$, en considérant les états dans l'ordre alphabétique.

1. Quelle est la probabilité de transition de l'état A vers l'état B ?

2. Quelle est la probabilité de transition de l'état B vers l'état B ?

17 Une marche aléatoire à deux états 1 et 2 est donnée par le graphe suivant :



Écrire sa matrice de transition, en considérant les états dans l'ordre naturel.

18 La matrice de transition d'une marche aléatoire à deux états A et B est $M = \begin{pmatrix} 0{,}45 & 0{,}55 \\ 0{,}65 & 0{,}35 \end{pmatrix}$, en considérant les états dans l'ordre alphabétique.

1. Représenter le graphe de cette marche aléatoire.

2. On part de l'état A. Quelle est la probabilité que les deux états suivants du système soient A ?

19 La matrice de transition d'une marche aléatoire à deux états est $M = \begin{pmatrix} 0{,}4 & 0{,}6 \\ 0{,}2 & 0{,}8 \end{pmatrix}$.

L'état initial est donné par $E_0 = (1 \ 0)$.

Calculer M^2. En déduire la probabilité de retour à l'état initial après deux étapes.

20 Déterminer les réels a, b et c afin que la matrice M suivante soit la matrice de transition d'une marche aléatoire à trois états :

$$M = \begin{pmatrix} a & 0{,}1 & 0{,}6 \\ 0{,}2 & 0{,}7 & b \\ 0{,}5 & c & 0{,}3 \end{pmatrix}.$$

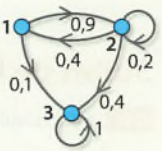
21 La matrice de transition d'une marche aléatoire à trois états A, B et C est $M = \begin{pmatrix} 0{,}5 & 0{,}1 & 0{,}4 \\ 0{,}6 & 0{,}3 & 0{,}1 \\ 0 & 0{,}3 & 0{,}7 \end{pmatrix}$, les états étant considérés dans l'ordre alphabétique.

1. Quelle est la probabilité de transition de l'état A vers l'état B ?

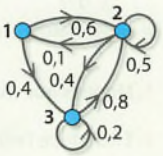
2. Quelle est la probabilité de transition de l'état C vers l'état B ?

22 Une marche aléatoire est donnée par le graphe ci-contre.

Écrire sa matrice de transition, en considérant les états dans l'ordre naturel.



23 Une marche aléatoire est donnée par le graphe ci-contre.



1. Écrire sa matrice de transition M, les états étant considérés dans l'ordre 1, 2, 3.

2. Calculer M^2 et interpréter les éléments de la première ligne de M^2.

24 Une puce saute d'un sommet d'un carré ABCD à un autre sommet de ce carré en choisissant le sommet de façon équiprobable, sauf lorsqu'elle est en A où elle choisit au hasard entre B et C.

1. Écrire la matrice de transition de cette promenade aléatoire, en considérant les états dans l'ordre alphabétique.

2. La puce part de A. Quelle est la probabilité qu'elle revienne en A au bout de trois sauts ?

Étude asymptotique des marches aléatoires

25 La matrice de transition d'une marche aléatoire à deux états est $M = \begin{pmatrix} 0{,}1 & 0{,}9 \\ 0{,}7 & 0{,}3 \end{pmatrix}$.

Montrer que cette marche aléatoire admet un état stable, puis le déterminer.

26 Soit la marche aléatoire à deux états A et B dont la matrice de transition est $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

1. Décrire cette marche aléatoire.

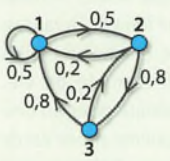
2. Admet-elle un état stable ?

27 Une marche aléatoire à deux états A et B est telle que la probabilité de transition de l'état A vers lui-même est 0,5 et celle de l'état B vers lui-même est 0,75.

1. Écrire sa matrice de transition, les états étant pris dans l'ordre A, B.

2. Montrer que cette marche aléatoire admet un état stable, et le déterminer.

28 Une marche aléatoire est donnée par le graphe ci-dessous :



1. Écrire sa matrice de transition M, les états étant considérés dans l'ordre 1, 2, 3.

2. Cette marche aléatoire admet-elle un état stable ? Si oui, le déterminer.

POUR S'ENTRAÎNER

Suites de la forme $X_{n+1} = AX_n$

29 Soit la suite de matrices colonnes (U_n) définies par $U_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, et par la relation de récurrence $U_{n+1} = AU_n$ (pour n entier naturel), où $A = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix}$.

1. Montrer que $A^n = \begin{pmatrix} 2^{n+1} - 1 & 2 - 2^{n+1} \\ 2^n - 1 & 2 - 2^n \end{pmatrix}$.
2. En déduire l'expression de U_n en fonction de n.
3. La suite (U_n) est-elle convergente ?

→ Pour vous aider Savoir-faire 1, p. 115

30 Soit la suite de matrices colonnes (V_n) définies par $V_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, et par la relation de récurrence $V_{n+1} = AV_n$ (pour n entier naturel), où $A = \begin{pmatrix} 1 & -\frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{pmatrix}$.

1. Soit P la matrice $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$. Calculer sa matrice inverse P^{-1}, puis la matrice D définie par $D = P^{-1}AP$.
2. Calculer D^n, puis A^n en fonction de n.
3. Déterminer V_n en fonction de n.
4. La suite (V_n) est-elle convergente ?

→ Pour vous aider Savoir-faire 1, p. 115

31 Soit la suite de matrices colonnes (X_n) définies par $X_0 = \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix}$, et par la relation $X_{n+1} = AX_n$ (pour n entier naturel), où $A = \begin{pmatrix} 1 & -2 & 2 \\ -1 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}$.

1. Soit la matrice $P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. Calculer sa matrice inverse P^{-1}, puis la matrice D définie par $D = P^{-1}AP$.
2. Calculer D^n, puis A^n.
3. En déduire l'expression de X_n en fonction de n.
4. La suite (X_n) est-elle convergente ?

32 Dans une population de souris femelles, chaque souris femelle donne naissance à une femelle durant sa première année de vie, et à huit femelles pendant sa deuxième année de vie. D'autre part, la probabilité pour qu'une souris survive une deuxième année est de 0,25, et il n'y a aucune chance qu'elle survive au-delà de la deuxième année. On note a_n le nombre de souris juvéniles (âgées de moins d'un an), b_n le nombre de souris adultes (âgées entre un et deux ans) et c_n le nombre total de souris femelles dans la population étudiée à l'instant n (supposé entier).

On suppose qu'il y a 20 souris femelles juvéniles et aucune souris femelle adulte à l'instant 0.

1. Si on note X_n la matrice colonne $\begin{pmatrix} a_n \\ b_n \end{pmatrix}$, montrer que, pour n entier naturel, on a : $X_{n+1} = AX_n$, où $A = \begin{pmatrix} 1 & 8 \\ 0{,}25 & 0 \end{pmatrix}$.
2. Soit P la matrice $\begin{pmatrix} 2 & -1 \\ 0{,}25 & 0{,}25 \end{pmatrix}$.

Déterminer P^{-1}, puis calculer $D = P^{-1}AP$.

3. Pour n entier naturel, calculer D^n, puis A^n.
4. **a.** En déduire les expressions de a_n et de b_n en fonction de n.
b. Déterminer l'expression de c_n en fonction de n.
5. Quelle est la limite des suites (a_n), (b_n) et (c_n) ?
6. Déterminer la limite quand n tend vers l'infini de $\frac{a_n}{c_n}$, puis de $\frac{b_n}{c_n}$ et de $\frac{c_{n+1}}{c_n}$. Interpréter ces résultats.

33 Soit les suites (u_n) et (v_n) telles que $u_0 = a$ et $v_0 = b$, et pour tout entier naturel n : $\begin{cases} u_{n+1} = \frac{2}{3}u_n + \frac{1}{3}v_n \\ v_{n+1} = \frac{1}{3}u_n + \frac{2}{3}v_n \end{cases}$

1. On note $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. Déterminer la matrice A telle que, pour tout entier naturel n : $X_{n+1} = AX_n$.
2. Montrer que $A^n = \frac{1}{2}\begin{pmatrix} 1 + \frac{1}{3^n} & 1 - \frac{1}{3^n} \\ 1 - \frac{1}{3^n} & 1 + \frac{1}{3^n} \end{pmatrix}$.
3. En déduire la matrice X_n en fonction de n, a et b.
4. En déduire les expressions de u_n et de v_n en fonction de n, a et b.
5. Étudier la convergence des suites (u_n) et (v_n).

34 Soit les suites (u_n), (v_n) et (w_n) définies, pour tout entier naturel n, par : $\begin{cases} u_{n+1} = 5u_n - 5v_n + 2w_n \\ v_{n+1} = -u_n + 7v_n - 4w_n \\ w_{n+1} = 2u_n - 5v_n + 5w_n \end{cases}$

avec $u_0 = 0$, $v_0 = 1$ et $w_0 = 0$.

1. Soit $X_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$. Déterminer la matrice A telle que $X_{n+1} = AX_n$.
2. Soit la matrice $P = \begin{pmatrix} 1 & 4 & 1 \\ -1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Calculer sa matrice inverse P^{-1}, puis la matrice D définie par $D = P^{-1}AP$.
3. Calculer D^n.
4. Pourquoi suffit-il de calculer une seule colonne de la matrice A^n pour obtenir X_n ?
5. Déterminer l'expression de X_n en fonction de n.
6. Quelle est la limite de la suite (X_n) ?

35 Des chercheurs étudient une population d'oiseaux dans un écosystème. On sait que ces oiseaux sont adultes au bout d'un an et que le sex-ratio est équilibré à la naissance. Chaque année, 80 % des femelles de plus d'un an pondent en moyenne un œuf. De plus, le taux de survie entre 0 et un an est de 30 %, et il est de 40 % après un an. Au début de l'étude, il y a 200 juvéniles et 400 adultes.

Soit t un entier naturel.
On note $N(t)$ la matrice colonne $\begin{pmatrix} x(t) \\ y(t) \end{pmatrix}$, où $x(t)$ et $y(t)$ sont les effectifs d'oiseaux juvéniles et adultes à la date t (exprimés en années).

1. Montrer que l'on a $\begin{cases} x(t+1) = 0{,}4\,y(t) \\ y(t+1) = 0{,}3\,x(t) + 0{,}4\,y(t) \end{cases}$

2. Déterminer la matrice A telle que : $N(t+1) = A \times N(t)$.

3. Soit la matrice $P = \begin{pmatrix} 2 & -2 \\ 3 & 1 \end{pmatrix}$. Calculer sa matrice inverse P^{-1}, puis $D = P^{-1}AP$.

4. Calculer D^t, puis A^t.

5. **a.** Étudier la convergence de la suite de matrices $(N(t))_{t\in\mathbb{N}}$.
b. Que peut-on en conclure pour cette population ?

36 On considère des nombres décimaux a et b, appartenant à l'intervalle $]0\,;\,1[$, vérifiant $a - b = 0{,}5$ et tels que $10a$ et $10b$ soient des nombres entiers.
Deux urnes contiennent chacune 10 boules : une urne rouge contient $10a$ boules rouges et une urne noire contient $10b$ boules rouges. Les boules étant indiscernables les unes des autres, on effectue une suite de tirages au hasard d'une boule dans l'une des deux urnes, selon les règles suivantes :
– le premier tirage a lieu dans l'une des deux urnes tirée au hasard (avec équiprobabilité) ;
– après chaque tirage dans une urne, la boule est remise dans la même urne ;
– pour tout entier naturel n, le $(n+1)$-ième tirage a lieu dans l'urne de la couleur de la boule tirée au n-ième tirage.
Pour tout entier naturel n supérieur ou égal à 1, on désigne par R_n l'événement « on tire une boule rouge au n-ième tirage » et par N_n l'événement « on tire une boule noire au n-ième tirage ».

1. **a.** Calculer les probabilités $P(R_1)$ et $P(N_1)$.
b. Soit X_n la matrice $\begin{pmatrix} P(R_n) \\ P(N_n) \end{pmatrix}$. Montrer qu'il existe une matrice A telle que, pour tout entier n supérieur ou égal à 1, on ait :
$$X_{n+1} = AX_n.$$

2. On pose $P = \begin{pmatrix} b & -1 \\ 1-a & 1 \end{pmatrix}$ et $Q = 2\begin{pmatrix} 1 & 1 \\ a-1 & b \end{pmatrix}$.
a. Prouver que $Q^{-1} = P$.
b. Déterminer la matrice D telle que $D = P^{-1}AP$.
c. Exprimer D^n, puis A^n en fonction de a, b et n.

3. **a.** Calculer X_n en fonction de a, b et n.
b. La suite (X_n) est-elle convergente ?
c. Interpréter le résultat précédent.

VRAI – FAUX

Pour les exercices **37** et **38**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

37 Quand elles sont convergentes, les suites de matrices colonnes (X_n) définies pour tout entier naturel n par la relation $X_{n+1} = AX_n$ et la donnée de X_0 convergent vers la matrice $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

38 Si $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, alors la suite de matrices colonnes (X_n) définie par $X_{n+1} = AX_n$ et $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ n'est pas convergente.

Suites de la forme $X_{n+1} = AX_n + B$

39 Soit les matrices $A = \begin{pmatrix} 1 & -\frac{3}{2} \\ \frac{1}{4} & -\frac{1}{4} \end{pmatrix}$ et $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Soit la suite de matrices (X_n) telle que $X_0 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ et, pour tout entier naturel n : $X_{n+1} = AX_n + B$.

1. Soit la matrice $P = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$.
Calculer sa matrice inverse P^{-1}, puis la matrice $D = P^{-1}AP$.

2. Calculer D^n, puis A^n.

3. Calculer la matrice C telle que $C = AC + B$.

4. Exprimer X_n en fonction de n.

5. Étudier la convergence de la suite (X_n).

→ Pour vous aider Savoir-faire 2, p. 115

40 Soit les matrices $A = \begin{pmatrix} \frac{1}{2} & 0 \\ -1 & -\frac{1}{3} \end{pmatrix}$ et $B = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$.

Soit la suite de matrices (X_n) telle que $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et, pour tout entier naturel n : $X_{n+1} = AX_n + B$.

1. Soit la matrice $P = \begin{pmatrix} 5 & 0 \\ -6 & -1 \end{pmatrix}$.
Calculer sa matrice inverse P^{-1}, puis la matrice $D = P^{-1}AP$.

2. Calculer D^n, puis A^n.

3. Exprimer X_n en fonction de n.

4. Étudier la convergence de la suite (X_n).

→ Pour vous aider Savoir-faire 2, p. 115

41 Soit les matrices $A = \begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Soit la suite de matrices (X_n) telle que $X_0 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$ et, pour tout entier naturel n : $X_{n+1} = AX_n + B$.

1. Montrer que $A^n = (-1)^n \begin{pmatrix} 1 & -3n \\ 0 & 1 \end{pmatrix}$.

2. Exprimer X_n en fonction de n.

3. La suite (X_n) est-elle convergente ?

Exercices

42 Soit les suites (x_n) et (y_n) telles que $x_0 = \frac{7}{8}$ et $y_0 = \frac{3}{8}$, et pour tout entier naturel n : $\begin{cases} x_{n+1} = 6x_n + 3y_n + 4 \\ y_{n+1} = -x_n + 2y_n - 1 \end{cases}$

1. On note $U_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$. Déterminer les matrices A et B telles que, pour tout entier naturel n : $U_{n+1} = AU_n + B$.
2. Soit $P = \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix}$. Calculer P^{-1}, puis $D = P^{-1}AP$.
3. En déduire D^n, puis A^n.
4. Déterminer la matrice U_n en fonction de n.
5. En déduire les expressions de x_n et de y_n en fonction de n.
6. Étudier la convergence des suites (x_n) et (y_n).

43 ALGO TICE

Soit la suite (u_n) définie par la donnée de ses deux premiers termes $u_0 = 0$ et $u_1 = 1$, et par la relation :

$u_{n+1} = \frac{3}{2}u_n - \frac{1}{2}u_{n-1}$, pour n entier supérieur ou égal à 1.

1. Élaborer un algorithme permettant le calcul du terme de rang n de cette suite. Programmer cet algorithme.
2. On note $X_n = \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}$, pour $n \geqslant 1$.

Déterminer la matrice A telle que $X_{n+1} = AX_n$.

3. Soit $P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Calculer P^{-1}, puis $D = P^{-1}AP$.
4. En déduire D^n, puis A^n.
5. Exprimer u_n en fonction de n. La suite (u_n) est-elle convergente ?

AIDE : question 1. Utiliser une variable auxiliaire c pour y stocker u_n avant le calcul de u_{n+1} dans la boucle **POUR**.

44 **TRAVAIL EN AUTONOMIE**

Énoncé

Soit la suite $(u_n)_{n\in\mathbb{N}}$ définie par son premier terme $u_0 = 2$ et par $u_{n+1} = 3u_n + 4$ pour tout entier naturel n.

1. Exprimer u_n en fonction de n.
2. En déduire la limite de la suite (u_n).

Solution

1. On cherche une suite constante vérifiant la relation de récurrence, c'est-à-dire un réel c tel que $c = 3c + 4$.
On trouve $2c = -4$, soit $c = -2$.
Ainsi : $u_{n+1} - (-2) = 3u_n + 4 + 2 = 3u_n + 6 = 3(u_n + 2)$.
La suite de terme général $u_n + 2$ est une suite géométrique de raison 3, donc $u_n + 2 = 3^n(u_0 + 2)$, soit $u_n + 2 = 4 \times 3^n$, et ainsi : $u_n = 4 \times 3^n - 2$.
2. Puisque $\lim\limits_{n\to\infty} (3^n) = +\infty$, on en déduit que la limite de la suite (u_n) est $+\infty$.

45 Soit la suite (u_n) définie par son premier terme $u_0 = 1$ et par $u_{n+1} = \frac{1}{4}u_n - 7$, pour tout entier naturel n.

1. Déterminer u_n en fonction de n.
2. En déduire la limite de la suite (u_n).

46 Soit la suite (u_n) définie par son premier terme $u_0 = 3$ et par $u_{n+1} = \frac{1}{10}u_n + 18$, pour tout entier naturel n.

1. Déterminer u_n en fonction de n.
2. En déduire la limite de la suite (u_n).

47 Soit la suite (u_n) définie par son premier terme $u_0 = 2$ et par $u_{n+1} = 5u_n - 8$, pour tout entier naturel n.

1. Déterminer u_n en fonction de n.
2. En déduire la limite de la suite (u_n).

48 ALGO

Soit a, b et α des réels donnés, avec $a > 0$.
Élaborer un algorithme permettant d'obtenir la limite de la suite $(u_n)_{n\in\mathbb{N}}$ telle que $u_{n+1} = au_n + b$ et $u_0 = \alpha$.

49 Logique

Soit l'énoncé : « Si A est une matrice diagonale dont les éléments sont compris entre 0 et 1, alors la suite (X_n) définie par la relation $X_{n+1} = AX_n + B$ converge ».

1. Cet énoncé est-il vrai ?
2. Écrire l'énoncé réciproque. Est-il vrai ?

VRAI – FAUX

Pour les exercices 50 à 52, indiquer si les affirmations sont vraies ou fausses, puis justifier.

50 La suite de matrices colonnes vérifiant $X_{n+1} = 2X_n + B$ et $X_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, avec $B = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, converge.

51 Une suite arithmétique est une suite arithmético-géométrique.

52 Les suites définies par la relation de récurrence $u_{n+1} = au_n + b$ convergent si et seulement si $-1 < a < 1$.

Marches aléatoires à deux états

53 Un coucou annonce l'heure en sortant de sa maison. Celui-ci, un peu vieillissant, est capricieux :
– s'il est sorti de sa maison à l'heure exacte, il en sort à nouveau une heure plus tard avec la probabilité 0,9 ;
– s'il n'est pas sorti à l'heure exacte, il sort une heure plus tard avec la probabilité 0,8.
Ces probabilités sont indépendantes de l'heure.
À huit heures, le coucou a chanté. On note S l'état « le coucou est sorti » et N l'état « le coucou n'est pas sorti ».

1. Représenter cette marche aléatoire à l'aide d'un graphe.
2. Écrire la matrice de transition de cette marche aléatoire, les états étant dans l'ordre S, N.
3. Quelle est, à 10^{-3} près, la probabilité que le coucou chante à midi ?

→ Pour vous aider Savoir-faire 3, p. 119

54 TRAVAIL EN AUTONOMIE

Énoncé

Par suite d'une forte augmentation du prix des carburants de 2010 à 2011, certains salariés d'une entreprise changent de mode de déplacement pour se rendre sur leur lieu de travail.
En 2010, 80 % des salariés utilisaient leur voiture personnelle.
En 2011, 30 % des salariés utilisant leur voiture en 2010 ne l'utilisaient plus et 10 % des personnes ne l'utilisant pas en 2010 l'utilisaient en 2011.
On suppose que ces proportions restent constantes d'une année à l'autre. On note A l'état « un salarié utilise sa voiture personnelle » et B l'état « un salarié n'utilise pas sa voiture personnelle ».

1. Écrire la matrice de transition associée à cette marche aléatoire, les états étant pris dans l'ordre A, B.

2. On suppose que cette évolution se poursuit.
Quelle est la probabilité qu'un salarié de cette entreprise utilise sa voiture personnelle en 2012 ? en 2015 ?

3. **a.** Soit x_n la probabilité qu'un salarié utilise sa voiture personnelle au cours de l'année $(2010 + n)$.
Exprimer x_{n+1} en fonction de x_n.
b. En déduire l'expression de x_n en fonction de n.
c. En supposant que cette évolution se poursuive, est-il possible d'envisager qu'à terme, aucun des salariés n'utilise sa voiture personnelle pour aller au travail ?

Solution

1. La matrice de transition est :

$$M = \begin{pmatrix} 0,7 & 0,3 \\ 0,1 & 0,9 \end{pmatrix}.$$

2. L'état initial en 2010 est $E_0 = \begin{pmatrix} 0,8 & 0,2 \end{pmatrix}$.

L'état probabiliste en 2012 est E_2.

Or $E_2 = E_0 \times M^2 = \begin{pmatrix} 0,448 & 0,552 \end{pmatrix}$.

Donc, la probabilité qu'un salarié utilise sa voiture personnelle en 2012 est 0,448.
On a aussi : $E_5 = E_0 \times M^5 \approx \begin{pmatrix} 0,293 & 0,707 \end{pmatrix}$, à 10^{-3} près, donc la probabilité de l'état A en 2015 est 0,293.

3. **a.** On a :

$$\begin{pmatrix} x_{n+1} & y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & y_n \end{pmatrix} M$$
$$= \begin{pmatrix} 0,7x_n + 0,1y_n & 0,3x_n + 0,9y_n \end{pmatrix}$$

avec $x_n + y_n = 1$.
D'où : $x_{n+1} = 0,7x_n + 0,1(1 - x_n) = 0,1 + 0,6x_n$.
b. (x_n) est une suite arithmético-géométrique. On cherche d'abord le réel c tel que $c = 0,1 + 0,6c$, soit $0,4c = 0,1$, ce qui donne $c = 0,25$.
Ainsi : $x_{n+1} - 0,25 = 0,6\,(x_n - 0,25)$.
D'où : $x_n - 0,25 = 0,6^n\,(x_0 - 0,25) = 0,6^n \times 0,55$.
On en déduit : $x_n = 0,25 + 0,55 \times 0,6^n$.
c. C'est impossible, car d'après la formule précédente :

$$x_n > 0,25 \text{ pour toute valeur de } n.$$

55

Les clients d'une banque nationale se répartissent en deux catégories :
– la catégorie A, formée des clients d'agence (état A) ;
– la catégorie I, composée des clients d'Internet (état I).
En 2012, 92 % des clients sont des clients d'agence et 8 % sont des clients d'Internet. On admet que, chaque année, 5 % des clients d'agence deviennent clients d'Internet et inversement, 1 % des clients d'Internet deviennent clients d'agence.
On suppose que le nombre de clients reste constant au cours du temps et qu'un client ne peut pas faire partie des deux catégories. On s'intéresse à l'évolution de la répartition des clients de cette banque dans les années à venir.

1. Déterminer la matrice de transition de cette marche aléatoire, les états étant pris dans l'ordre A, I.

2. Déterminer, à 10^{-3} près, la répartition prévisible des clients de la banque en 2016.

56

Dans une résidence de vacances, les touristes vont tous les jours à la plage. Ils disposent pour se déplacer de deux moyens : un minibus ou des quads. Chaque jour, ils peuvent modifier leur choix de transport.

Le premier jour, 80 % des touristes choisissent le minibus.
On considère qu'ensuite, chaque jour, 30 % de ceux qui ont pris le minibus la veille choisissent le quad et 15 % des vacanciers qui avaient emprunté le quad la veille choisissent le minibus.
On note M l'état « choix du minibus » et B l'état « choix du quad ».

1. Écrire la matrice de transition associée à cette situation, les états étant pris dans l'ordre M, B.

2. Déterminer la répartition prévisible le sixième jour.

3. **a.** Soit a_n la proportion de vacanciers choisissant le minibus le jour n. Exprimer a_{n+1} en fonction de a_n.
b. En déduire a_n en fonction de n.

VRAI – FAUX

Pour les exercices 57 à 59, indiquer si les affirmations sont vraies ou fausses, puis justifier.

57 La somme des éléments d'une colonne de la matrice de transition d'une marche aléatoire à deux états n'est jamais égale à 1.

58 La somme des éléments diagonaux d'une marche aléatoire à deux états est toujours supérieure ou égale à 1.

59 La matrice de transition d'une marche aléatoire à deux états est toujours inversible.

Marches aléatoires à plusieurs états

60 Trois enfants jouent avec une balle.
Lorsqu'Alexis a la balle, il l'envoie à Boris dans $\frac{3}{4}$ des cas et à Camille dans $\frac{1}{4}$ des cas. Quand c'est Boris qui a la balle, il l'envoie à Alexis dans $\frac{3}{4}$ des cas et à Camille sinon. Enfin, Camille envoie toujours la balle à Boris.
Au début du jeu, c'est Alexis qui a la balle.
On note respectivement A, B, C les états « Alexis a la balle », « Boris a la balle », « Camille a la balle ».

1. Écrire la matrice de transition M de cette marche aléatoire, les états étant pris dans l'ordre A, B, C.

2. Quelle est la probabilité que Boris ait la balle après le 4e lancer ?

3. Soit P la matrice $\begin{pmatrix} 1 & 1 & 5 \\ 1 & 1 & -9 \\ 1 & -4 & 12 \end{pmatrix}$.
Déterminer P^{-1}, puis la matrice $D = P^{-1}MP$.

4. Pour n entier naturel non nul, calculer D^n, puis M^n.

5. En déduire, en fonction de n, la probabilité qu'Alexis ait la balle au n-ième lancer.

→ Pour vous aider Savoir-faire 4, p. 119

61 Un éditeur de jeu vidéo en ligne multi-joueurs ouvre trois serveurs pour son dernier jeu :
– le serveur A pour les joueurs débutants ;
– le serveur B pour les joueurs de niveau intermédiaire ;
– le serveur C pour les joueurs confirmés.
Il s'avère que chaque année, au terme de leur abonnement :
– 40 % des joueurs du serveur A y restent, et 60 % passent sur le serveur B ;
– 70 % des joueurs du serveur B y restent, 20 % passent sur le serveur A, et le reste passe sur le serveur C ;
– 85 % des joueurs du serveur C y restent, les autres passant sur le serveur B.
On note A l'état « le joueur est sur le serveur A », B l'état « le joueur est sur le serveur B »et C l'état « le joueur est sur le serveur C ».

1. Représenter le graphe associé à cette situation.

2. Écrire la matrice de transition de cette marche aléatoire, les états étant pris dans l'ordre A, B, C.

3. Lors de la première année de fonctionnement, la répartition est la suivante : 40 % sont sur le serveur A, 50 % sur le serveur B et 10 % sur le serveur C.
a. Quelle est la répartition prévisible au bout de 4 ans ?
b. Quelle est la répartition prévisible au bout de 8 ans ?

62 Trois sortes d'images sont réparties en proportions égales dans des boîtes de céréales. Un inspecteur des fraudes, ayant observé ce qui se passait pour 1 000 personnes achetant chaque semaine une boîte de céréales et voyant qu'au bout de 12 semaines, 15 personnes n'avaient que deux des trois images, a déclaré mensongère la publicité : « les images sont également réparties dans les paquets ».
On se propose de vérifier si cette affirmation est vraie.
On considère donc 1 000 personnes qui, chaque semaine, achètent exactement une boîte. Au bout d'une semaine, elles auront toutes une image. L'état E_n du système la n-ième semaine est une matrice ligne $X_n = \begin{pmatrix} a_n & b_n & c_n \end{pmatrix}$, où a_n est le nombre de personnes ayant une seule sorte d'images, b_n est le nombre de personnes ayant exactement deux images distinctes et c_n est le nombre de personnes ayant les trois images.
Quand on a une seule image, la probabilité d'en tirer une nouvelle est $\frac{2}{3}$; quand on a deux sortes d'images, la probabilité de tirer la troisième sorte est $\frac{1}{3}$.

1. À quoi est égale la matrice X_1 ?

2. Écrire la matrice de transition M de cette marche aléatoire.

3. Soit la matrice $P = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.
Calculer P^{-1}, puis la matrice $D = P^{-1}AP$.

4. Déterminer D^n, puis M^n en fonction de n.

5. En déduire X_n en fonction de n.

6. Quelle est la limite de la suite (X_n) ? L'interpréter.

7. Au bout de combien de semaines peut-on considérer que toutes les personnes ont les trois images ?

63 Dans une région, on considère trois types de temps : beau, variable, pluvieux. On sait que :
– s'il fait beau un jour donné, la probabilité qu'il fasse beau le lendemain est $\frac{1}{3}$et celle qu'il pleuve est $\frac{1}{6}$;
– si le temps est variable, la probabilité qu'il soit variable le lendemain est $\frac{1}{4}$ et celle qu'il pleuve est $\frac{1}{2}$;
– s'il pleut, la probabilité qu'il pleuve le lendemain est $\frac{1}{4}$ et la probabilité qu'il fasse beau est $\frac{1}{2}$.
On note B, V, P les états associés à ces types de temps.

1. Écrire la matrice de transition associée à cette marche aléatoire, les états étant pris dans l'ordre B, V, P.

2. Le 1er juillet, il fait beau.
a. Quelle est la probabilité qu'il fasse beau le 8 juillet ?
b. Quelle est la probabilité qu'il fasse beau tous les jours du 1er au 8 juillet ?

64 Un jeu de l'oie simple est constitué de cinq cases numérotées de 1 à 5 et disposées comme ci-dessous :

La case 1 est la case de départ, et la case 5 est la case d'arrivée.
Pour faire avancer le pion, on lance un dé à quatre faces numérotées de 1 à 4 et on avance le pion d'un nombre de cases égal au nombre obtenu avec le dé.
Le jeu s'arrête lorsque le pion tombe sur la case 5 ; sinon le pion recule d'un nombre de cases égal à ce qu'il reste à compter (par exemple, si le pion est en 4 et que le dé donne 3, le pion avance d'une case jusqu'à 5, puis recule de deux cases jusqu'à 3).
Les différents états de ce processus sont les cases 1, 2, 3, 4 et 5.

1. Écrire la matrice de transition de cette marche aléatoire, les états étant pris dans l'ordre naturel.

2. Quelle est, à 10^{-3} près, la probabilité d'avoir terminé le jeu après quatre coups ?

3. Combien faut-il jouer de coups pour que la probabilité de gagner dépasse 95 % ?

VRAI – FAUX

Pour les exercices 65 et 66, indiquer si les affirmations sont vraies ou fausses, puis justifier.

65 Le coefficient $p_{3,2}$ d'une matrice de transition est la probabilité de passer de l'état 2 à l'état 3.

66 Soit M une matrice de transition d'une marche aléatoire. L'élément $a_{1,1}$ de la matrice M^4 est la probabilité d'être resté 4 fois dans l'état 1.

Étude asymptotique des marches aléatoires

67 Dans une île, on considère que, chaque année, 40 % des habitants de la capitale vont vivre dans le reste de l'île, tandis que 20 % des habitants du reste de l'île viennent habiter dans la capitale. On néglige les autres échanges de population. On suppose qu'en janvier 2012, il y a 5 000 habitants dans l'île, dont 2 000 dans la capitale. On note A l'état « les habitants habitent la capitale » et B l'état « les habitants n'habitent pas dans la capitale ».

1. Écrire la matrice de transition associée à cette marche aléatoire, les états étant pris dans l'ordre A, B.

2. Déterminer l'état stable de cette marche aléatoire.
Que peut-on en conclure ?

→ Pour vous aider Savoir-faire 5, p. 121

68 ALGO TICE

Une compagnie aérienne étudie la réservation sur l'un de ses vols. Une place donnée est libre le jour d'ouverture de la réservation et son état évolue jusqu'à la fermeture de la réservation :
– si la place est réservée un jour donné, elle le sera encore le jour suivant avec la probabilité 0,9 ;
– si la place est libre un jour donné (état L), elle sera réservée (état R) le jour suivant avec la probabilité 0,4.
On s'intéresse à l'évolution de la réservation de cette place.

1. Écrire la matrice de transition associée à cette marche aléatoire, les états étant pris dans l'ordre L, R.

2. Déterminer l'état stable de cette marche aléatoire.
Que peut-on en conclure ?

3. Une place, libre un jour donné, est réservée le lendemain.
On veut déterminer, à l'aide d'un programme, au bout de combien de jours elle va être à nouveau libre.

a. Compléter l'algorithme ci-contre afin d'effectuer une simulation donnant en sortie le nombre de jours au bout duquel la place redevient libre.

```
n prend la valeur 2.
Tant que .....
    n prend la valeur n + 1
Fin Tant que
Afficher n.
```

b. On veut afficher en sortie le temps moyen (en jours) pour qu'une place redevienne libre.
Compléter cet algorithme afin d'effectuer N simulations.

c. Programmer cet algorithme.

69 Les agences de notation évaluent les capacités des pays à emprunter. On considère, pour simplifier, que ces agences décernent chaque année une note entière comprise entre 1 et 3, correspondant au degré de confiance qu'on peut accorder à ce pays sur ses capacités à rembourser un prêt.
Pour tout entier naturel n, on appelle Z_n la variable aléatoire égale à la note obtenue par un pays donné l'année n.
On suppose qu'un pays conserve sa note avec la probabilité 0,9 ; on suppose aussi que, pour $i \neq j$, la probabilité que la note Z_{n+1} soit égale à j sachant que la note l'année d'avant est i est proportionnelle à : $\frac{1}{|i-j|}$.
Au 1er janvier 2012, la note de ce pays est 3.

1. Montrer que la matrice de transition est :

$$\begin{pmatrix} \frac{9}{10} & \frac{1}{15} & \frac{1}{30} \\ \frac{1}{20} & \frac{9}{10} & \frac{1}{20} \\ \frac{1}{30} & \frac{1}{15} & \frac{9}{10} \end{pmatrix}$$

avec les états dans l'ordre : « la note est 1 », « la note est 2 » et « la note est 3 ».

2. Quelle est la probabilité que ce pays voit sa note abaissée d'un cran au 1er janvier 2014 ?

3. Cette marche aléatoire possède-t-elle un état stable ?
Interpréter le résultat obtenu.

→ Pour vous aider Savoir-faire 6, p. 121

70 ALGO

Soit une marche aléatoire à deux états, dont les coefficients a et b de la matrice de transition sont donnés.
Écrire un algorithme qui affiche en sortie s'il existe un état stable ; si cet état existe, l'afficher aussi en sortie.

71 À l'instant initial, trois cartes à jouer, le roi de trèfle, le roi de pique et la dame de cœur sont posées sur une table, faces cachées.
À chaque instant n ($n \geqslant 1$), le maître du jeu (le bonneteur) échange la carte centrale et la carte de droite avec la probabilité 0,4 ou bien il échange la carte centrale et celle de gauche avec la probabilité 0,6.
On s'intéresse à l'évolution du roi de trèfle.
Les états sont pris dans l'ordre :
– G : « la carte de gauche est le roi de trèfle » ;
– C : « la carte du centre est le roi de trèfle » ;
– D : « la carte de droite est le roi de trèfle ».

1. Représenter cette situation par un graphe.

2. Quelle est la matrice de transition de cette marche aléatoire ?

3. Cette marche aléatoire possède-t-elle un état stable ?
Interpréter le résultat obtenu.

Exercices

72 Chaque année, une association de cyclotouristes prépare de nouveaux circuits. Elle élabore des circuits de différents niveaux : facile, moyen et difficile. Au 1er janvier 2012, l'association a fait un bilan : 20 % de ses adhérents ont choisi le niveau facile (noté A), 70 % de ses adhérents ont choisi le niveau moyen (noté B) et 10 % de ses adhérents ont choisi le niveau difficile (noté C).
Pour répondre aux attentes des adhérents et les fidéliser sur le long terme, une enquête est effectuée :
– parmi les adhérents ayant choisi le niveau A, 40 % restent à ce niveau et 60 % passent au niveau B ;
– parmi les adhérents ayant choisi le niveau B, 70 % restent à ce niveau et 20 % reviennent au niveau A, les autres passant au niveau C ;
– parmi les adhérents ayant choisi le niveau C, 85 % restent à ce niveau et les autres reviennent au niveau B.
On s'intéresse à l'évolution de la répartition des adhérents à partir du 1er janvier 2012 (on néglige les nouveaux abonnés et les départs).

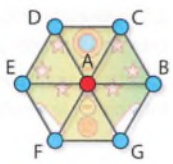
1. Représenter le graphe de cette marche aléatoire.

2. Déterminer la matrice de transition de cette marche aléatoire.

3. Cette marche aléatoire possède-t-elle un état stable ? Interpréter le résultat obtenu.

4. Le président de l'association affirme que 50 % des adhérents choisiront après un certain nombre d'années le niveau B. Cette affirmation est-elle correcte ?

73 Un flipper est schématisé ci-contre. Si la boule se trouve au centre A, elle prend toutes les directions de manière uniforme.



Si la boule est sur un bord du flipper, elle a deux fois moins de chances d'aller au centre que dans chacune des deux autres voies. Les états sont pris dans l'ordre alphabétique.

1. Déterminer la matrice de transition de cette marche aléatoire.

2. La boule part du centre. Quelle est la probabilité qu'elle soit à nouveau au centre après six coups de flipper ?

3. Montrer que cette marche aléatoire possède un état stable. Le déterminer.

AIDE : question 3. Soit $P = (p_1 \ p_2 \ p_3 \ p_4 \ p_5 \ p_6 \ p_7)$ l'état stable. Par symétrie : $p_2 = \ldots = p_7$.

74 En 1903, A. Markov lut le poème « Eugène Onéguine » de Pouchkine. Il remarqua que les consonnes et les voyelles se succédaient dans les proportions suivantes : la probabilité d'avoir deux voyelles qui se suivent est de $\frac{1}{8}$ et la probabilité d'avoir deux consonnes consécutives est de $\frac{1}{3}$.

1. Représenter le graphe de cette marche aléatoire.

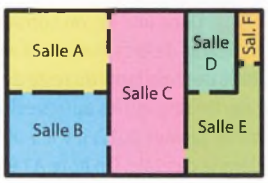
2. Déterminer la matrice de transition de cette marche aléatoire, les états étant pris dans l'ordre « voyelle – consonne ».

3. Quel est le pourcentage de voyelles et de consonnes dans cet ouvrage ?

Point Histoire

Andreï Markov, mathématicien russe, a formalisé l'étude des probabilités de succession de différents états en se basant pour ses premiers travaux sur le roman *Eugène Onéguine*, d'Alexandre Pouchkine.

75 Un musée est formé de six salles. Le gardien surveille ces salles en passant de l'une à l'autre toutes les dix minutes : il choisit de façon équiprobable une des portes de la pièce où il se trouve.



Le gardien commence sa journée à 8 h dans la salle A.

1. Déterminer la matrice de transition de cette marche aléatoire.

2. Quelle est la probabilité qu'il soit dans la salle A au bout d'une heure ?

3. Cette marche aléatoire admet-elle un état stable ?

4. Un voleur connaît les habitudes du gardien. Dans quelle(s) salle(s) et à partir de quelle heure doit-il agir afin que la probabilité qu'il soit surpris par le gardien soit inférieure à 0,1 ?

VRAI – FAUX

Pour les exercices **76** et **77**, indiquer si les affirmations sont vraies ou fausses, puis justifier.

76 Toute marche aléatoire possède un état stable.

77 Si la suite des états probabilistes d'une marche aléatoire converge, la limite est nécessairement un état stable.

Top Chrono !

Résoudre chacun des exercices suivants en 10 minutes maximum.

78 Étudier la convergence de la suite $(u_n)_{n\in\mathbb{N}}$ telle que :

$$u_{n+1} = \frac{1}{5}u_n - 8 \text{ et } u_0 = 3.$$

79 La matrice de transition d'une marche aléatoire à deux états est $\begin{pmatrix} 0{,}4 & 0{,}6 \\ 0{,}1 & 0{,}9 \end{pmatrix}$. L'état initial est $\begin{pmatrix} 0{,}4 & 0{,}6 \end{pmatrix}$.

1. Quel est l'état probabiliste après 5 étapes ?

2. Déterminer l'état stable de cette marche aléatoire.

80 Soit la suite de matrices colonnes $(X_n)_{n\in\mathbb{N}}$ telle que $X_{n+1} = AX_n$, avec :

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ et } X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La suite de matrices $(U_n)_{n\in\mathbb{N}}$ telle que $U_n = \frac{1}{n+1}X_n$ est-elle convergente ?

Choisir la (ou les) bonne(s) réponse(s).

Étudier une suite de matrices de la forme $U_{n+1} = AU_n + B$

→ Pour vous aider Savoir-faire 1 et 2, p. 115

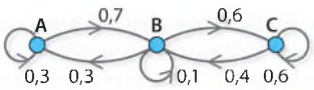
Soit les matrices $A = \begin{pmatrix} 1 & \frac{1}{3} \\ -1 & -\frac{1}{6} \end{pmatrix}$ et $B = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$. Pour n entier naturel, $A^n = \begin{pmatrix} 4\left(\frac{1}{2}\right)^n - 3\left(\frac{1}{3}\right)^n & 2\left(\frac{1}{2}\right)^n - 2\left(\frac{1}{3}\right)^n \\ -6\left(\frac{1}{2}\right)^n + 6\left(\frac{1}{3}\right)^n & -3\left(\frac{1}{2}\right)^n + 4\left(\frac{1}{3}\right)^n \end{pmatrix}$.

	A	B	C	D
81 La suite de matrices définie par $X_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$ avec $X_{n+1} = AX_n$ et $X_0 = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ est telle que	sa limite est $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$X_n = \begin{pmatrix} \frac{6}{2^n} - \frac{5}{3^n} \\ \frac{10}{3^n} - \frac{9}{2^n} \end{pmatrix}$	$X_n = \begin{pmatrix} \frac{1}{2^{n-1}} \\ -\frac{3}{2^n} \end{pmatrix}$	$\lim\limits_{n\to+\infty} \frac{x_n}{y_n} = -\frac{2}{3}$
82 La suite de matrices colonnes (U_n) telles que $U_{n+1} = AU_n + B$ et $U_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	a pour limite $\begin{pmatrix} 4 \\ -6 \end{pmatrix}$	a pour limite $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	n'est pas convergente	a pour limite $\begin{pmatrix} 2 \\ -3 \end{pmatrix}$
83 La suite de matrices colonnes (U_n) vérifiant $U_{n+1} = AU_n + B$ et $U_0 = \begin{pmatrix} 5 \\ -8 \end{pmatrix}$ est telle que U_n est égale à	$\begin{pmatrix} 4 + \frac{1}{2^{n-2}} + \frac{1}{3^n} \\ -6 - \frac{3}{2^{n-1}} - \frac{2}{3^n} \end{pmatrix}$	$\begin{pmatrix} 4 + \frac{1}{3^n} \\ -6 - \frac{2}{3^n} \end{pmatrix}$	$\begin{pmatrix} 2 + \frac{3}{2^{n-1}} - \frac{5}{3^n} \\ -3 - \frac{9}{2^n} + \frac{10}{3^n} \end{pmatrix}$	$\begin{pmatrix} 2 + \frac{1}{3^n} \\ -3 - \frac{2}{3^n} \end{pmatrix}$

Étudier une marche aléatoire

→ Pour vous aider Savoir-faire 3 et 4, p. 119

Une marche aléatoire à trois états A, B et C est donnée par le graphe ci-contre. Pour les calculs, les états sont considérés dans l'ordre alphabétique. L'état probabiliste initial est donné par la matrice ligne $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$.



84 La matrice de transition de cette marche aléatoire est	$\begin{pmatrix} 0,3 & 0,3 & 0 \\ 0,7 & 0,1 & 0,4 \\ 0 & 0,6 & 0,6 \end{pmatrix}$	$\begin{pmatrix} 0,3 & 0,7 & 0 \\ 0,3 & 0,1 & 0,6 \\ 0 & 0,4 & 0,6 \end{pmatrix}$	$\begin{pmatrix} 0,3 & 0,7 & 0,3 \\ 0,3 & 0,1 & 0,6 \\ 0,6 & 0,4 & 0,6 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0,7 & 0,6 & 0,6 \\ 0,3 & 0,3 & 0,4 \end{pmatrix}$
85 À l'étape 5, la probabilité de l'état B est égale, à 10^{-3} près, à	0,151	0,334	0,343	0,353

Étudier asymptotiquement une marche aléatoire

→ Pour vous aider Savoir-faire 5 et 6, p. 121

86 La marche aléatoire de matrice de transition $\begin{pmatrix} 0,25 & 0,75 \\ 0,15 & 0,85 \end{pmatrix}$ a pour état stable	$\begin{pmatrix} \frac{5}{6} & \frac{1}{6} \end{pmatrix}$	$\begin{pmatrix} \frac{17}{22} & \frac{5}{22} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{6} & \frac{5}{6} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix}$
87 La marche aléatoire de matrice de transition $\begin{pmatrix} 0,2 & 0 & 0,8 \\ 0,4 & 0 & 0,6 \\ 0 & 0,7 & 0,3 \end{pmatrix}$ et d'état initial $\begin{pmatrix} 0,5 & 0,4 & 0,1 \end{pmatrix}$	ne converge pas	converge vers $\begin{pmatrix} \frac{1}{2} & \frac{2}{5} & \frac{9}{10} \end{pmatrix}$	converge vers $\begin{pmatrix} \frac{7}{41} & \frac{14}{41} & \frac{20}{41} \end{pmatrix}$	converge vers $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$

➤ Voir les réponses, p. 140

TP 1 Proies et prédateurs

TICE → Utiliser un tableur pour prévoir l'évolution de deux espèces.

On va étudier les évolutions des populations de proies (lièvres variables) et de prédateurs (lynx du Canada) dans la baie d'Hudson, au Canada. Suite à un grand nombre d'observations, on fait les hypothèses suivantes :

– La population de proies a tendance à augmenter naturellement de 5 % d'une année sur l'autre.

– L'interaction des prédateurs se traduit par une baisse de la population de proies d'une année sur l'autre : cette diminution est proportionnelle au nombre de proies et au nombre de prédateurs avec un coefficient de 0,1 %.

– Le nombre de naissances de prédateurs au cours d'une année dépend pratiquement uniquement de la capacité des prédateurs à trouver de la nourriture et il est proportionnel au nombre de prédateurs et au nombre de proies avec un coefficient de 0,002 %.

– Sur une année, le nombre de prédateurs diminue par décès de 3 %.

On suppose qu'à l'instant t, l'effectif des proies est $x(t)$ et celui des prédateurs est $y(t)$, où x et y sont des fonctions dérivables sur $\mathbb{R}$. Les hypothèses de l'énoncé conduisent au système suivant : $\begin{cases} x'(t) = 0{,}05\,x(t) - 0{,}001x(t)y(t) \\ y'(t) = -0{,}03\,y(t) + 0{,}0002\,x(t)y(t) \end{cases}$

A. Première étude du problème

1. Discrétisation du problème : on va décrire les populations de proies et de prédateurs à l'aide de deux suites (x_n) et (y_n) associées aux populations de lièvres et de lynx une année donnée. Montrer que, pour tout entier naturel n :

$$\begin{cases} x_{n+1} = 1{,}05x_n - 0{,}001x_n y_n \\ y_{n+1} = 0{,}97y_n + 0{,}0002x_n y_n \end{cases}$$

2. Que se passerait-il en l'absence de prédateurs ?

3. Que se passerait-il en l'absence de proies ?

4. On suppose à présent que, pour tout entier naturel n, $x_n \neq 0$ et $y_n \neq 0$. Montrer qu'il existe des conditions initiales x_0 et y_0 pour lesquelles le nombre de lièvres et de lynx resterait constant.

B. Utilisation d'un tableur

On suppose qu'il y a au départ 200 lièvres et 50 lynx dans la baie d'Hudson. On va étudier avec un tableur l'évolution du nombre de lièvres et de lynx sur 500 ans.

1. Saisir les effectifs initiaux dans les cellules A2 et B2, les valeurs de n dans la colonne C et calculer les effectifs de lièvres et de lynx dans les colonnes E et F.

	A	B	C	D	E	F
1	x0	yo		n	xn	yn
2	200	50		0	200	50
3				1	200	50,5

2. Représenter l'évolution du nombre de proies en fonction du temps : que constate-t-on ?

3. Représenter l'évolution du nombre de prédateurs en fonction du temps : que constate-t-on en le comparant au graphique précédent ?

4. Représenter l'ensemble des points de coordonnées $(x_n ; y_n)$. Mettre en évidence le **point d'équilibre** du système, de coordonnées $(x_0 ; y_0)$.

5. Faire varier les effectifs initiaux des deux populations. Commenter les différences.

C. Linéarisation du problème

On se propose de faire une étude algébrique de ce problème. Pour cela, on définit les nouvelles suites (X_n) et (Y_n), où :

$$X_n = x_n - 150 \quad \text{et} \quad Y_n = y_n - 50.$$

1. Exprimer X_{n+1} et Y_{n+1} en fonction de X_n et Y_n.

2. Les termes contenant les produits X_nY_n étant « petits », on les néglige. Montrer que, si on pose $U_n = \begin{pmatrix} X_n \\ Y_n \end{pmatrix}$, alors les égalités précédentes peuvent s'écrire matriciellement : $U_{n+1} = A \times U_n$, avec $A = \begin{pmatrix} 1 & -0{,}15 \\ 0{,}01 & 1 \end{pmatrix}$.

3. Exprimer alors U_n en fonction de A et de n.

4. En déduire une méthode de calcul des effectifs de ces populations.

D. Retour aux fonctions

Comme dans la **partie C**, on peut définir de nouvelles fonctions X et Y telles que :

$$X(t) = x(t) - 150 \quad \text{et} \quad Y(t) = y(t) - 50.$$

1. Montrer qu'en « négligeant » les produits $x(t)y(t)$, on obtient les équations :

$$X'(t) = -0{,}15Y(t) \quad \text{et} \quad Y'(t) = 0{,}01X(t).$$

2. a. En déduire que $X''(t) = -0{,}0015X(t)$, en notant X'' la dérivée de X'.

b. Que valent $X(0)$ et $X'(0)$?

3. À l'aide d'un logiciel de calcul formel, résoudre cette équation différentielle (on pourra tenir compte des conditions initiales).

```
desolve([x''=-0,0015x,x(0)=50,x'(0)=0],x)
```

Pourquoi ceci confirme-t-il les résultats vus dans la **partie B** ?

TP 2 Le collectionneur d'images

→ Utiliser un algorithme pour estimer le temps d'attente pour gagner à un jeu.

Dans chaque paquet de guimauves Bambi, on trouve une image de collection. La série complète comprend quatre images différentes. On se propose d'étudier l'évolution du nombre d'images dans la collection d'un enfant, et de déterminer le nombre moyen de paquets qu'il va devoir acheter pour avoir la collection complète.

A. Étude de la marche aléatoire

On va étudier la marche aléatoire associée au processus d'obtention de ces images. On suppose qu'il y a une répartition uniforme des diverses images dans les paquets mis en vente. On note A_1, A_2, A_3 et A_4 les états correspondant respectivement à la possession d'une image, deux images, trois images et quatre images. Après l'achat du premier paquet, le premier état probabiliste est : $E_1 = (1\ 0\ 0\ 0)$.

1. Écrire la matrice de transition M de cette marche aléatoire, les états étant pris dans l'ordre A_1, A_2, A_3, A_4.

2. Quelle est, à 10^{-3} près, la probabilité d'avoir les quatre images après 5 achats ? après 10 achats ?

3. Soit la matrice $P = \begin{pmatrix} 1 & 3 & 3 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

a. Déterminer P^{-1}, puis $D = P^{-1}MP$.

b. Pour n entier naturel non nul, calculer D^n, et en déduire l'expression de M^n en fonction de n.

4. a. Déterminer E_n en fonction de n.

b. Quelle est la limite de la suite (E_n) ? Interpréter.

B. Étude expérimentale

On va réaliser un algorithme simulant les achats d'un enfant jusqu'à ce qu'il obtienne les quatre images. Pour cela, on définit une liste de quatre éléments telle que chaque élément représente le nombre d'images de chaque type collectionnées.
On veut afficher en sortie le nombre m de paquets achetés.

1. Recopier et compléter l'algorithme ci-contre.
(Rand (1, 4) désigne un entier aléatoire compris entre 1 et 4.)

2. Programmer cet algorithme.

```
L prend la valeur {0, 0, 0, 0}.
m prend la valeur 0.
  Tant que .....
    a prend la valeur Rand (1, 4)
    L[a] prend la valeur ...
    m prend la valeur ...
  Fin Tant que
Afficher m
```

3. a. Modifier cet algorithme afin de simuler n expériences de ce type, et d'obtenir en sortie le nombre moyen de paquets à acheter pour avoir la collection complète.

b. Programmer cet algorithme.
Qu'obtient-on en simulant 100 expériences ? 1 000 expériences ?

C. Nombre moyen de paquets à acheter

1. Soit la somme $S_n(x) = \sum_{k=1}^{n} k \times x^{k-1}$, où n est un entier supérieur ou égal à 1 et x un réel de $]0\,;1[$.

a. Soit f la fonction définie sur $]0\,;1[$ par $f(x) = \sum_{k=1}^{n} x^k$.

On note f' la dérivée de f.
Quelle relation existe-t-il entre $f'(x)$ et $S_n(x)$?

b. Exprimer $f(x)$ en fonction de n et de x.

c. En utilisant l'expression trouvée à la question précédente, calculer $f'(x)$ en fonction de n et de x.

d. En déduire $S_n(x)$ en fonction de n et de x.

e. Déterminer la limite de la suite $(S_n(x))_{n\in\mathbb{N}^*}$ (on admet que $\lim\limits_{n\to+\infty} nx^n = 0$).

2. Soit T la variable aléatoire égale au nombre de paquets à acheter pour avoir toute la collection, après le premier achat.
Soit X_i le nombre de paquets à acheter pour passer de l'état A_i à l'état A_{i+1}. On a : $T = X_1 + X_2 + X_3$, et on admet que :

$$E(T) = E(X_1) + E(X_2) + E(X_3).$$

a. Montrer que $P(X_1 = k) = \frac{3}{4} \times \left(\frac{1}{4}\right)^{k-1}$.

b. Calculer $P(X_2 = k)$ et $P(X_3 = k)$ en fonction de k.

3. Comme les variables aléatoires X_i prennent leurs valeurs dans $\mathbb{N}^*$, on définit $E(X_i)$ comme la limite lorsque n tend vers $+\infty$ de :

$$\sum_{k=1}^{n} k \times P(X_i = k).$$

a. Montrer que l'on a : $\sum_{k=1}^{n} k \times P(X_1 = k) = \frac{3}{4} S_n\left(\frac{1}{4}\right)$.

b. En déduire $E(X_1)$, $E(X_2)$ et $E(X_3)$.

c. En déduire $E(T)$. Comparer avec la **partie B**.

Aides pour les logiciels

AlgoBox

B. 2. Pour définir une liste L, lui donner un nom L et entrer le rang du premier terme.
Puis, quand il est demandé « entrer le terme de rang 1 de la liste », saisir tous les termes séparés par : (deux points). Par exemple : 0:0:0:0.

Sujet commenté BAC

➤ Énoncé

Thèmes
- *Marche aléatoire*
- *Étude asymptotique*

À la Bourse, un titre donné peut monter (état M), rester stable (état S) ou baisser (état B).
Si ce titre monte un jour n, on a constaté qu'il monte le jour suivant $(n+1)$ avec la probabilité 0,4 et reste stable avec la probabilité 0,6.
S'il reste stable un jour n, on a constaté qu'il monte le lendemain avec la probabilité 0,2, reste stable avec la probabilité 0,5 et baisse avec la probabilité 0,3. S'il baisse le jour n, on a constaté qu'il reste stable le lendemain avec la probabilité 0,4 et baisse à nouveau avec la probabilité 0,6.
Ces probabilités sont indépendantes de n. Le premier jour de cotation (appelé le jour 1), le titre est stable.

1. Déterminer la matrice de transition A de cette marche aléatoire, en considérant les états dans l'ordre M, S, B.

2. a. Quelle est, à 10^{-3} près, la probabilité que le titre reste stable pendant la première semaine de cotation ?
b. Quelle est, à 10^{-3} près, la probabilité que le titre soit stable le septième jour de cotation ?

3. Montrer que cette marche aléatoire admet un état stationnaire. Le déterminer et l'interpréter.

4. On suppose à présent que, le premier jour de cotation, le titre est en hausse.
Quelle est la probabilité qu'il soit stable le septième jour de cotation ? Quel est l'état stationnaire ?

➤ Comprendre l'énoncé et choisir les méthodes

1. La probabilité de passer de M (état 1) à S (état 2) est l'élément $m_{1,2}$ de la matrice, c'est-à-dire 0,6.

→ Savoir-faire 3, p. 119

2. a. La probabilité que le titre reste stable le premier jour est 1, et donc le second jour, elle est de 0,5 (d'après l'énoncé), et encore 0,5 le troisième jour, puisque le titre est stable le second jour : on peut faire un arbre de probabilités pour le visualiser.
b. Le calcul d'une probabilité à une étape donnée du processus nécessite le calcul de l'état probabiliste à cette étape.
L'état probabiliste à l'étape n est égal à $E_0 \times A^n$, si A est la matrice de transition. Ici, le premier état est E_1, ce qui modifie la formule.

→ Savoir-faire 4, p. 119

3. On doit d'abord prouver l'existence d'un état stable : puisque A contient des zéros, on calcule A^2, et on conclut.
L'état stable est alors solution du système :

$$\begin{pmatrix} x & y & z \end{pmatrix} \times A = \begin{pmatrix} x & y & z \end{pmatrix}.$$

Ne pas oublier en le résolvant d'ajouter l'équation supplémentaire $x+y+z=1$.

→ Savoir-faire 6, p. 121

4. On calcule $E'_7 = E'_1 \times A^6$ avec $E'_1 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$. L'état stationnaire est indépendant de l'état probabiliste initial : il ne change pas.

➤ Réponses

1. La matrice de transition est $A = \begin{pmatrix} 0,4 & 0,6 & 0 \\ 0,2 & 0,5 & 0,3 \\ 0 & 0,4 & 0,6 \end{pmatrix}$.

2. a. La probabilité que le titre reste stable pendant les sept premiers jours est : $1 \times 0,5^6 \approx 0,016$.
b. On calcule l'état probabiliste au jour 7.
Si on note $E_1 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$ l'état probabiliste au jour 1, alors l'état probabiliste le jour 7 est donné par $E_7 = E_1 \times A^6$.
On calcule A^6, à 10^{-3} près, avec la calculatrice :

$$A^6 \approx \begin{pmatrix} 0,167 & 0,484 & 0,349 \\ 0,161 & 0,481 & 0,358 \\ 0,155 & 0,477 & 0,367 \end{pmatrix}.$$

D'où $E_7 \approx \begin{pmatrix} 0,161 & 0,481 & 0,358 \end{pmatrix}$ à 10^{-3} près ; la probabilité cherchée est donc 0,481.

3. $A^2 = \begin{pmatrix} 0,28 & 0,54 & 0,18 \\ 0,18 & 0,49 & 0,33 \\ 0,08 & 0,44 & 0,48 \end{pmatrix}$: la matrice A^2 ne contient pas de zéro, donc il existe un état stable. On résout

$$\begin{cases} 0,4x + 0,2y = x \\ 0,6x + 0,5y + 0,4z = y, \text{ avec } x+y+z=1. \text{ On a : } \\ 0,3y + 0,6z = z \end{cases} \begin{cases} y = 3x \\ 4z = 9x \\ 3y = 4z \end{cases}$$

Puisque $x+y+z=1$, on obtient $x + 3x + \frac{9}{4}x = 1$, soit $\frac{25}{4}x = 1$ et $x = \frac{4}{25}$. On en déduit : $y = \frac{12}{25}$ et $z = \frac{9}{25}$.
L'état stable est donc $\begin{pmatrix} 0,16 & 0,48 & 0,36 \end{pmatrix}$. Au bout d'un grand nombre de jours de cotation, il y aura environ 16 % des jours où le titre est en hausse, 48 % des jours où le titre est stable et 36 % des jours où le titre est en baisse.

4. On obtient, à 10^{-3} près, $E'_7 \approx \begin{pmatrix} 0,167 & 0,484 & 0,349 \end{pmatrix}$.
La probabilité cherchée est donc 0,484.

Pour se préparer à l'écrit BAC

Sujet A

Capacités mises en œuvre

- *Étudier une marche aléatoire à trois états*
- *Étudier une suite de matrices vérifiant $X_{n+1} = AX_n + B$*

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 l'état « la marque X est utilisée un mois donné », Y l'état « la marque Y est utilisée un mois donné » et Z l'état « la marque Z est utilisée un mois donné ».
Au cours du mois d'essai ($n = 0$), on a observé l'état initial de ce processus : $E_0 = \begin{pmatrix} 0{,}1 & 0{,}2 & 0{,}7 \end{pmatrix}$.
Les probabilités des événements X, Y et Z le mois n sont respectivement notées x_n, y_n et z_n.
On suppose le processus sans mémoire.
D'autre part, en déterminant par sondage les intentions des consommateurs que l'on supposera constantes, on a obtenu la matrice de transition de cette marche aléatoire :

$$M = \begin{pmatrix} 0{,}4 & 0{,}3 & 0{,}3 \\ 0{,}3 & 0{,}4 & 0{,}3 \\ 0{,}2 & 0{,}1 & 0{,}7 \end{pmatrix}.$$

1. a. Exprimer x_{n+1}, y_{n+1} et z_{n+1} en fonction de x_n, y_n et z_n.
b. À quoi est égal $x_n + y_n + z_n$?

2. Soit les matrices colonnes $U_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$ et $B = \begin{pmatrix} 0{,}2 \\ 0{,}1 \end{pmatrix}$.
Déterminer la matrice A telle que $U_{n+1} = AU_n + B$.

3. Soit la matrice $P = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$.
a. Montrer que P est inversible et calculer P^{-1}.
b. Calculer $D = P^{-1}AP$.
c. En déduire, pour n entier naturel, la matrice D^n, puis la matrice A^n en fonction de n.

4. a. Montrer qu'il existe une matrice C telle que $C = AC + B$. Calculer C.
b. En déduire l'expression de U_n en fonction de n.

5. a. Exprimer x_n, y_n et z_n en fonction de n.
b. Que conclure de l'utilisation, à long terme, des marques X, Y et Z ?

Savoir-faire
Question 1. ➤ Savoir-faire 3, p. 119
Question 4. ➤ Savoir-faire 2, p. 115

Sujet B

Capacités mises en œuvre

- *Étudier une suite de matrices vérifiant $X_{n+1} = AX_n$*
- *Étudier la convergence d'une suite de matrices colonnes*

Un biologiste souhaite déterminer, sur une durée assez longue, l'évolution de la population d'une famille d'insectes insulaires.
Des observations ont montré que l'espèce possède trois stades de développement : les larves, les adultes et les insectes âgés.
On a observé que, sur une unité de temps, seuls les adultes se reproduisaient et que leur taux de natalité est de 225 %.
On sait aussi que le taux de mortalité des larves et des adultes est de 25 % et que celui des individus âgés est de 75 %.
On sait enfin que le temps moyen passé au stade de larves est de 4 unités de temps, comme le temps moyen passé au stade d'adultes (on peut supposer donc qu'au bout d'un an, 25 % des larves deviennent adultes).
À l'instant initial de l'étude, les effectifs (en milliers) des populations de larves, d'adultes et d'insectes âgés sont respectivement égaux à a, b et c.

On note $N(t)$ la matrice colonne $\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix}$ donnant la population de larves, d'adultes et d'insectes à l'instant t, où t est un entier naturel.

1. Montrer que $N(t+1) = A \times N(t)$, où A est la matrice :

$$A = \begin{pmatrix} 0{,}5 & 2{,}25 & 0 \\ 0{,}25 & 0{,}5 & 0 \\ 0 & 0{,}25 & 0{,}25 \end{pmatrix}.$$

2. On suppose dans cette question $a = 100$, $b = 200$ et $c = 50$. Combien y a-t-il d'adultes au bout de 10 unités de temps (à une unité près) ?

3. Soit la matrice $P = \begin{pmatrix} 6 & 12 & 0 \\ -2 & 4 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.
a. Calculer P^{-1}, puis la matrice $D = P^{-1}AP$.
b. Pour t entier naturel, déterminer D^t, puis A^t.

4. Exprimer $x(t)$, $y(t)$ et $z(t)$ en fonction de a, b, c et t.

5. a. Ce modèle prédit-il la pérennité de l'espèce ?
b. Déterminer $\lim\limits_{t \to +\infty} \left(\dfrac{x(t)}{y(t)} \right)$. Interpréter ce résultat.

Savoir-faire
Question 3. ➤ Savoir-faire 1, p. 115

Sujet C

Capacités mises en œuvre

- *Étudier une suite de matrices vérifiant $X_{n+1} = AX_n$*
- *Étudier asymptotiquement une marche aléatoire*

Un appartement est formé de deux pièces A et B reliées entre elles par une porte ouverte ; seule la pièce B possède une fenêtre ouverte.
Une guêpe qui s'était endormie dans la pièce A se réveille à l'instant 0.
On estime que :
– quand la guêpe est dans la pièce A à l'instant n (exprimé en minutes), elle est encore dans la pièce A une minute après avec une probabilité égale à $\frac{1}{3}$.
– quand la guêpe est dans la pièce B à l'instant n, alors une minute après, elle est retournée dans la pièce A avec la probabilité $\frac{1}{4}$ et elle est restée dans la pièce B avec la probabilité $\frac{1}{2}$.

1. Dans cette question, quand la guêpe est sortie, elle ne revient plus.

a. Déterminer la matrice de transition M de cette marche aléatoire, les états A « la guêpe est en A », B « la guêpe est en B » et E « la guêpe est sortie » étant pris dans l'ordre alphabétique.

b. Soit $\begin{pmatrix} a_n & b_n & c_n \end{pmatrix}$ l'état probabiliste de cette marche aléatoire à l'instant n. On note : $X_n = \begin{pmatrix} a_n & b_n \end{pmatrix}$.
Déterminer la matrice Q telle que $X_{n+1} = X_n \times Q$.

c. Montrer que pour n entier supérieur ou égal à 1 :

$$Q^n = \begin{pmatrix} \frac{2}{5}\left(\frac{5}{6}\right)^n & \frac{4}{5}\left(\frac{5}{6}\right)^n \\ \frac{3}{10}\left(\frac{5}{6}\right)^n & \frac{3}{5}\left(\frac{5}{6}\right)^n \end{pmatrix}.$$

d. En déduire la probabilité que la guêpe soit sortie de l'appartement n minutes après son réveil.

e. Au bout de combien de temps cette probabilité est-elle supérieure à 0,999 ?

2. Dans cette question, quand la guêpe est sortie, elle revient dans la pièce B avec la probabilité 0,1.

a. Que devient la matrice de transition ?

b. Montrer que cette marche aléatoire possède un état stable. Le déterminer, puis l'interpréter.

Savoir-faire
Question 1. ➤ Savoir-faire 4, p. 119
Question 2. ➤ Savoir-faire 6, p. 121

Sujet D ALGO

Capacités mises en œuvre

- *Étudier une suite de matrices vérifiant $X_{n+1} = AX_n$*
- *Écrire un algorithme de recherche d'un terme d'une suite récurrente*

Corentin a trouvé dans son grenier un plan conduisant à un trésor. Il est dit ceci :

« Plante un bâton A au pied du puits et un bâton B au pied du figuier, puis plante un bâton C au milieu du chemin reliant ces deux bâtons, puis un bâton D au milieu du chemin reliant B et C, et ainsi de suite… Tu trouveras le trésor au bout de tes efforts ».

Le figuier est à 200 mètres du puits. Peut-on aider Corentin à trouver le trésor ?
Pour tout entier naturel n, on note u_n la distance du n-ième bâton planté au puits. Ainsi $u_0 = 0$ et $u_1 = 200$.

1. Montrer que pour $n \geqslant 1$: $u_{n+1} = \frac{1}{2}u_n + \frac{1}{2}u_{n-1}$.

2. Écrire un algorithme permettant le calcul du terme u_n de cette suite, avec comme entrée l'entier n.

3. On note $X_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$. Montrer que $X_{n+1} = AX_n$, où A est une matrice que l'on déterminera.

4. a. Soit $P = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$. Calculer P^{-1}, puis $D = P^{-1}AP$.

b. Calculer D^n, puis A^n en fonction de n.

5. a. En déduire l'expression de u_n en fonction de n.

b. Déterminer la limite de la suite (u_n). Conclure.

Savoir-faire
Question 4. ➤ Savoir-faire 1, p. 115

Pour se préparer à l'oral BAC

88 Soit la suite de matrices colonnes $(X_n)_{n\in\mathbb{N}}$ telle que $X_{n+1} = AX_n + B$, avec $A = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ et $X_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

1. Déterminer l'expression de X_n en fonction de n.

2. La suite (X_n) est-elle convergente ?

89 Dans une ville donnée, si une année, un habitant pratique le covoiturage, l'année suivante il se déplace seul dans sa voiture avec une probabilité de 0,6 ; si une année, il se déplace seul dans sa voiture, il pratique le covoiturage l'année suivante avec une probabilité de 0,35.
Déterminer, s'il existe, l'état stable de cette marche aléatoire.

POUR ALLER PLUS LOIN

90 Convergence d'une marche aléatoire à trois états

Partie A. Matrice de transition sans zéros

On se propose de démontrer le théorème du cours sur la convergence des marches aléatoires dans le cas de trois états : « Soit une marche aléatoire à trois états dont la matrice de transition est P. Si P n'a aucun élément égal à 0, alors la suite (U_n) décrivant l'état probabiliste de cette marche aléatoire converge ».

On note P la matrice de transition d'une marche aléatoire à trois états et $p_{i,j}$ les éléments de P.

Pour n entier supérieur ou égal à 1, on note $p_{i,j}(n)$ les éléments de P^n.

Soit M_n le plus grand élément de la première colonne de P^n et m_n le plus petit élément de cette colonne.

On note d le plus petit élément de la matrice P.

1. a. Montrer que :

$$p_{i,1}(n+1) = p_{i,1}\,p_{1,1}(n) + p_{i,2}\,p_{2,1}(n) + p_{i,3}\,p_{3,1}(n).$$

b. On suppose que $m_n = p_{2,1}(n)$. Montrer que M_{n+1} est le plus grand des nombres $p_{i,1}\,p_{1,1}(n) + p_{i,2}\,m_n + p_{i,3}\,p_{3,1}(n)$ quand i varie de 1 à 3.

c. Montrer que :

$$p_{i,1}\,p_{1,1}(n) + p_{i,2}\,m_n + p_{i,3}\,p_{3,1}(n) \leqslant (1 - p_{i,2})\,M_n + p_{i,2}\,m_n.$$

d. En déduire que : $M_{n+1} \leqslant M_n - d\,(M_n - m_n)$.

2. Un calcul similaire à celui fait à la question **1.** montre que l'on a aussi : $m_{n+1} \geqslant m_n + d\,(M_n - m_n)$.

a. Montrer que la suite (M_n) est décroissante.

En déduire qu'elle converge.

b. Montrer que la suite (m_n) est croissante.

En déduire qu'elle converge.

3. a. Montrer que, pour tout entier naturel n, $n \geqslant 1$:

$$M_{n+1} - m_{n+1} \leqslant (1 - 2d)\,(M_n - m_n).$$

b. Montrer par récurrence que $0 \leqslant M_n - m_n \leqslant k^{n-1}$, où k est un réel appartenant à $]0\,;\,1[$.

c. Montrer que la suite $(p_{i,1}(n))_{n\in\mathbb{N}^*}$ converge vers un réel indépendant de i.

d. Expliquer pourquoi le raisonnement fait est aussi valable pour les suites $(p_{i,2}(n))_{n\in\mathbb{N}^*}$ et $(p_{i,3}(n))_{n\in\mathbb{N}^*}$.

e. En déduire la convergence de la suite de matrices (P^n), puis celle de la suite de matrices (U_n).

Partie B. Cas général

Dans cette partie, on suppose seulement que la matrice P^2 est telle que tous ses coefficients soient strictement positifs.

1. La suite (u_{2n}) est formée des termes $u_0, u_2, u_4 \ldots$

Soit (u_n) une suite décroissante et telle que la suite (u_{2n}) converge vers 0.

Montrer que la suite (u_n) converge aussi vers 0.

2. En utilisant la **partie A** (avec les mêmes notations), montrer que $\lim\limits_{n\to\infty} (M_{2n} - m_{2n}) = 0$.

3. a. En déduire que la suite $(p_{i,j}(n))$ converge.

b. Conclure comme dans la **partie A.**

4. Vérifier que le raisonnement ne change pas si on suppose que P^r est à coefficients strictement positifs, avec r entier supérieur ou égal à 3.

PISTE : **partie A. 1. c.** $p_{i,1}(n) \leqslant M$ pour tout i.
partie A. 3. c. Utiliser un encadrement de $p_{i,j}(n)$.
partie B. 1. Utiliser la définition de la convergence d'une suite vers 0.

91 Les double-pile dans le jeu de PILE ou FACE

On effectue des lancers successifs et indépendants d'une pièce de monnaie pour laquelle la probabilité d'apparition de PILE (P) est $\frac{2}{3}$.

On dit qu'il y a apparition d'un double PILE au rang n ($n \geqslant 2$) s'il y a un PILE au rang n et au rang $n-1$, mais qu'il n'y a pas un double PILE au rang $n-1$.

1. Étude d'un exemple.

On considère les 13 lancers suivants :

1	2	3	4	5	6	7	8	9	10	11	12	13
P	F	P	P	P	P	P	P	F	F	P	P	P
SP	F	SP	DP	SP	DP	SP						

Recopier ce tableau et compléter la dernière ligne par les indications (F : face, SP : simple PILE, DP : double PILE).

2. Pour n entier naturel non nul, on note B_n l'événement « la première apparition d'un double PILE se situe au rang n », et b_n sa probabilité.

a. Déterminer b_1, b_2, b_3 et b_4.

b. On note P_n l'événement « il y a apparition d'un PILE au rang n », et F_n l'événement « il y a apparition d'un FACE au rang n ».

Exprimer $P_{F_1}(B_{n+2})$ en fonction de $P(B_{n+1})$.

Exprimer $P_{P_1\cap F_2}(B_{n+2})$ en fonction de $P(B_n)$, puis $P_{P_1}(B_{n+2})$ en fonction de $P(B_n)$.

c. En déduire que pour tout entier naturel non nul n :

$$b_{n+2} = \frac{1}{3}\,b_{n+1} + \frac{2}{9}\,b_n.$$

3. Pour tout entier naturel non nul n, on définit U_n la matrice colonne $\begin{pmatrix} b_n \\ b_{n+1} \end{pmatrix}$.

a. Déterminer la matrice A telle que $U_{n+1} = AU_n$.

b. Exprimer U_n en fonction de n, A et U_1.

c. On pose $P = \begin{pmatrix} 3 & -3 \\ 2 & 1 \end{pmatrix}$.

Déterminer la matrice P^{-1}, puis la matrice $D = P^{-1}AP$.

d. Calculer D^n en fonction de n, puis A^n en fonction de n.

e. En déduire l'expression de b_n en fonction de n.

4. Soit C_n l'événement « il n'y a aucune apparition d'un double PILE au cours des n premiers lancers », et c_n sa probabilité.

a. Exprimer $\overline{C_n}$ à l'aide des événements $B_1, B_2, \ldots B_n$.

b. Déterminer la probabilité c_n.

c. Quelle est la limite de la suite (c_n) ?

Interpréter le résultat.

92 Télé-péage

Une société d'autoroute veut tester un nouveau dispositif de « télé-péage » en simulant des passages de véhicules à la barrière de péage.
Ces simulations ne prennent pas en compte l'usure du dispositif et sont indépendantes les unes des autres.
Une simulation de passage d'un véhicule comporte deux étapes.
– Étape 1 : déclenchement d'ouverture de la barrière à l'arrivée du véhicule.
– Étape 2 : si l'étape 1 fonctionne, déclenchement de la fermeture de la barrière après le passage du véhicule.
On note a la probabilité qu'une panne apparaisse à l'étape 1 ($a \in]0\,;1[$).
Dans le cas où il n'y a pas eu de panne lors de l'étape 1, la probabilité qu'une panne apparaisse à l'étape 2 sera notée b ($b \in]0\,;1[$).
Le test consiste à enchaîner des simulations de passages de véhicules tant que le système fonctionne sans avoir de panne.
Pour n entier naturel non nul, on définit trois événements :
– A_n « une panne se produit lors de la première étape de la n-ième simulation » ;
– B_n « la première étape de la n-ième simulation se déroule normalement, mais une panne se produit lors de la seconde étape » ;
– C_n « la n-ième simulation s'est déroulée sans aucune panne ».

1. Calculer en fonction de a et b la probabilité des événements A_1, B_1 et C_1.

2. Représenter tous les événements pouvant survenir à l'issue d'au plus deux simulations de passage.
Calculer la probabilité de ces événements.

3. Calculer, en fonction de n, a et b, la probabilité de chacun des événements A_n, B_n et C_n.

4. **a.** On considère la suite (u_n) définie pour tout entier naturel non nul n par $u_n = (1-\alpha)^n(1-\beta)^n$, où α et β sont deux nombres réels de l'intervalle $]0\,;1[$.
Montrer que la suite (u_n) est convergente et calculer sa limite.
b. Quelle conclusion peut-on en tirer sur le test étudié ?

93 Temps d'attente pour gagner à un jeu de dé

On lance indéfiniment un dé à quatre faces bien équilibré dont les faces sont numérotées 1, 2, 3, 4. On s'intéresse au maximum obtenu après un certain nombre de lancers du dé.

Partie A. Simulation du lancer avec un tableur

1. Saisir la liste des entiers de 1 à 100 sur la première ligne d'une feuille de calcul à partir de **B1**.

2. On simule une première série de lancers sur la seconde ligne de la feuille de calcul.
a. Simuler en **B2** le premier lancer.
b. Simuler en cellule **C2** le second lancer, en tenant compte du fait que l'on ne garde que le résultat maximal obtenu.
c. Recopier cette formule vers la droite afin de générer 100 lancers successifs de ce dé.

3. Simuler à présent 500 séries de lancers.

4. Pour chaque série de lancers, on va déterminer le numéro du premier lancer de la série qui atteint le 4.
a. Avec la fonction **EQUIV** du tableur, saisir la formule voulue en cellule **CY2** pour la première série de lancers.
b. Opérer de même pour les 500 séries.

5. En déduire le nombre de moyen de lancers nécessaires pour atteindre 4 sur ces 500 séries de lancers.

Partie B. Étude de la marche aléatoire

1. Écrire la matrice de transition A de cette marche aléatoire à quatre états.
On convient que l'état probabiliste initial est :

$$E_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}.$$

2. Quelle est la probabilité de gagner en un coup ? en deux coups ? en trois coups ? en quatre coups ?

3. On considère la matrice $B = 4A$.
Soit n entier supérieur ou égal à 1. Montrer que :

$$B^n = \begin{pmatrix} 1 & a_n & b_n & c_n \\ 0 & 2^n & d_n & e_n \\ 0 & 0 & 3^n & f_n \\ 0 & 0 & 0 & 4^n \end{pmatrix}$$

où les suites (a_n), (b_n), (c_n), (d_n), (e_n) et (f_n) satisfont à des relations de récurrence que l'on donnera.

4. **a.** Reconnaître la suite (a_n), et exprimer a_n en fonction de n.
b. Exprimer $b_{n+1} + 2^{n+1}$ en fonction de $b_n + 2^n$.
En déduire l'expression de b_n en fonction de n.
c. En calculant $c_{n+1} + 3^{n+1}$, déterminer l'expression de c_n en fonction de n.
d. En déduire l'expression de B^n, puis celle de A^n en fonction de n.

5. En déduire l'expression de l'état probabiliste E_n en fonction de n. Quelle est sa limite ?

6. À partir de combien de lancers la probabilité d'atteindre 4 dépasse 0,999 ?

Partie C. Calcul du temps d'attente

Soit T la variable aléatoire égale au temps d'attente pour gagner une partie.

1. Calculer $P(T=1)$ et $P(T=2)$.

2. Calculer $P(T=k)$, pour $k \geqslant 1$.

3. T prenant ses valeurs dans $\mathbb{N}^*$, son espérance mathématique est définie comme la limite lorsque n tend vers $+\infty$ de :

$$\sum_{k=1}^{n} k \times P(T=k).$$

On admet que la limite de $\sum_{k=1}^{n} k \times \left(\frac{3}{4}\right)^{k-1}$ quand n tend vers $+\infty$ est égale à 16.
Déterminer $E(T)$ et comparer avec la **partie A**.

PISTE : partie A. 2. a. Utiliser **ALEA.ENTRE.BORNES**.
partie A. 4. a. EQUIV(*n*;zone de cellules;0) renvoie le rang de la première occurrence de n dans la zone de cellules définie.

94 **Concours de tir au pistolet**

Un concours de tir au pistolet entre deux compétiteurs A et B est constitué d'une suite d'épreuves consistant, pour chacun des compétiteurs, en un tir visant à atteindre une cible.
Les deux compétiteurs tirent simultanément, chacun d'eux disposant de sa cible personnelle.
On associe à ce concours une expérience aléatoire.
À chaque épreuve, la probabilité que A touche sa cible est $\frac{2}{3}$ et elle est de $\frac{1}{2}$ pour B. De plus, les résultats obtenus par A et B sont indépendants les uns des autres.
Enfin, toutes les épreuves sont indépendantes entre elles.
À l'issue de l'épreuve, il faut avoir touché sa cible pour être autorisé à poursuivre le concours, sinon on est éliminé. Le concours cesse lorsque les deux compétiteurs ont été éliminés.
Pour n entier supérieur ou égal à 1, on considère les événements suivants, définis à l'issue de la n-ième épreuve :
– A_n : « seul A n'est pas éliminé » ;
– B_n : « seul B n'est pas éliminé » ;
– C_n : « aucun compétiteur n'est éliminé » ;
– D_n : « les deux compétiteurs sont éliminés ».

Partie A. Comportement asymptotique

1. Calculer les probabilités conditionnelles suivantes :
a. $P_{A_n}(A_{n+1})$, $P_{A_n}(B_{n+1})$, $P_{A_n}(C_{n+1})$ et $P_{A_n}(D_{n+1})$;
b. $P_{B_n}(A_{n+1})$, $P_{B_n}(B_{n+1})$, $P_{B_n}(C_{n+1})$ et $P_{B_n}(D_{n+1})$;
c. $P_{C_n}(A_{n+1})$, $P_{C_n}(B_{n+1})$, $P_{C_n}(C_{n+1})$ et $P_{C_n}(D_{n+1})$;
d. $P_{D_n}(A_{n+1})$, $P_{D_n}(B_{n+1})$, $P_{D_n}(C_{n+1})$ et $P_{D_n}(D_{n+1})$.

2. En déduire la matrice de transition M de cette marche aléatoire.

3. Soit P la matrice $\begin{pmatrix} 1 & 0 & -1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.
a. Calculer la matrice $D = P^{-1}MP$.
b. En déduire D^n, puis M^n, pour n entier supérieur ou égal à 1.

4. On note X_n la matrice $\begin{pmatrix} P(A_n) & P(B_n) & P(C_n) & P(D_n) \end{pmatrix}$.
a. Exprimer X_n en fonction de n.
b. Étudier la convergence de la suite (X_n).
c. Pouvait-on prévoir ces résultats ?

Partie B. Temps moyen de première élimination

On note T la variable aléatoire qui prend pour valeur le numéro de l'épreuve à l'issue de laquelle a lieu la première élimination.

1. Déterminer $P(T = 1)$.

2. Soit n un entier supérieur ou égal à 2.
a. Déterminer $P(C_1 \cap C_2 \cap \ldots \cap C_n)$.
b. Calculer $P(T > n)$, puis $P(T = n)$.
Vérifier que cette formule reste valable pour $n = 1$.

3. Calculer $\lim\limits_{n \to +\infty} \sum\limits_{k=1}^{n} P(T = k)$. Pouvait-on prévoir ce résultat ?

4. On suppose $n \geqslant 2$.
a. Montrer que $P(T > n-1) = P(T = n) + P(T > n)$.
b. Vérifier l'égalité suivante :
$$n P(T > n) + \sum_{k=1}^{n} k P(T = k) = \sum_{k=0}^{n-1} P(T > k).$$
c. En déduire la limite quand n tend vers $+\infty$ de $\sum\limits_{k=1}^{n} k P(T = k)$.
d. Quelle interprétation peut-on en donner ?

95 **PROBLÈME DE SYNTHÈSE**

Soit p, q et r trois réels positifs ou nuls tels que $p + q + r = 1$, et n un entier naturel. Un point mobile M parcourt aléatoirement le triangle ABC de la façon suivante : si, à l'instant n, le point M se trouve en un sommet donné du triangle ABC, alors, à l'instant $n + 1$, M se trouvera au sommet suivant avec la probabilité p, il se trouvera au sommet précédent avec la probabilité q, ou il restera au même sommet avec la probabilité r (on convient que B suit A, C suit B et A suit C).
On suppose ces probabilités indépendantes de n.
À l'instant 0, le point M se trouve en A.
On note A l'état « le mobile est en A », B l'état « le mobile est en B » et C l'état « le mobile est en C » l'ordre des états étant A, B, C.

1. Écrire la matrice de transition T de cette marche aléatoire.

2. Étudier le comportement du point M dans les cas suivants :
a. $r = 1$ **b.** $p = 1$ **c.** $p = q = r$

3. Dans la suite, on suppose $p = q$, et p élément de $\left]0 ; \frac{1}{2}\right]$.
Soit P la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$.
a. Montrer que P est inversible et calculer P^{-1}.
b. Calculer la matrice : $D = P^{-1}TP$.
c. Pour n entier naturel, déterminer D^n, puis T^n.
d. En déduire la probabilité que M soit en A à l'instant n. Calculer de même les probabilités que M soit en B ou en C à l'instant n.
e. Conclure sur le comportement asymptotique du point M.
f. Les résultats sont-ils modifiés si M part de B ou de C ?

Prises d'initiatives

96 Une rumeur court comme quoi les calculatrices ne seront pas autorisées au bac. Cette information est transmise à travers n intermédiaires. On suppose que chaque lycéen transmet le message correctement avec une probabilité p telle que $0 < p < 1$ ou le déforme en son contraire avec la probabilité $1 - p$. Modéliser cette situation par une marche aléatoire à deux états. Déterminer alors la probabilité que l'information transmise par le n-ième intermédiaire soit conforme à l'information initiale, lorsque le nombre d'intermédiaires devient très important.

97 Un message codé de façon binaire est transmis à travers un réseau. À chaque étape du réseau, la probabilité que le chiffre (0 ou 1) soit inchangé est p. Quelle est la probabilité pour qu'un mot de 5 chiffres soit transmis sans erreur ?

Corrigés

Retrouvez les corrigés détaillés des pages Avant de commencer et Pour faire le point sur www. bordas-indice.fr

Chapitre 1 Divisibilité et nombres premiers

Avant de commencer

1 A et C ; 2 A et C ; 3 B ; 4 A et C ; 5 B ; 6 B et C ; 7 C ; 8 B, C et D ; 9 C et D.

10 $737 = 700 + 30 + 7 = 7 \times 100 + (7 \times 4 + 2) + 7$
$= 7 \times 100 + 7 \times 4 + 7 \times 1 + 2 = 105 \times 7 + 2.$
737 est le dividende, 7 est le diviseur, 105 est le quotient, 2 est le reste.

11 On divise l'entier par 2.
Si le reste est 0, l'entier est pair. Si le reste est 1, l'entier est impair.

12 Les entiers s'écrivant sous la forme $3k$, avec $k \in \mathbb{Z}$, sont les multiples de 3. D'après un critère de divisibilité souvent rencontré dans les classes antérieures, ce sont les entiers dont la somme des chiffres (en écriture décimale) est également un multiple de 3.
On peut également caractériser ces entiers par le fait que leur reste dans la division euclidienne par 3 est 0.

13 La liste des entiers naturels diviseurs de 30 est :
1 ; 2 ; 3 ; 6 ; 5 ; 10 ; 15 ; 30.

14 Les couples $(x ; y)$ solutions vérifient $y = 1 - 2x$.
En donnant à x une valeur entière, $1 - 2x$ sera entier.
On trouve ainsi facilement dix couples d'entiers solutions.

Exercices

4 On peut utiliser la feuille de calcul ci-dessous :

	A	B	C
1	1	36	=SI(MOD(B$1;A1)=0;"diviseur";"")
2	2		=SI(MOD(B$1;A2)=0;"diviseur";"")
3	3		=SI(MOD(B$1;A3)=0;"diviseur";"")
4	4		=SI(MOD(B$1;A4)=0;"diviseur";"")
5	5		=SI(MOD(B$1;A5)=0;"diviseur";"")
6	6		=SI(MOD(B$1;A6)=0;"diviseur";"")

6 On cherche les entiers de la forme $17k$ (k entier relatif) tels que $-50 \leqslant 17k \leqslant 75$, donc tels que $-2 \leqslant k \leqslant 4$.
Il y a donc 7 entiers multiples de 17 compris entre –50 et 75.

12 $\sqrt{n}$ n'est pas nécessairement entier.

17 $\overline{aa} = 11a$. 1 et 11 sont donc diviseurs de chacun des entiers $\overline{aa}$.

27 On pourra par exemple consulter le site ChronoMath :
http://serge.mehl.free.fr/anx/crible_era.html.

41 L'écriture en base 10 d'un entier n est tel que celui-ci s'écrit sous la forme $10A + u$ où u, chiffre des unités, est compris entre 0 et 9.
Cet encadrement de u permet d'affirmer que u est aussi le reste de la division de n par 10.

60 1. $(x - 5)(y - 3) = xy - 5y - 3x + 15$.
2. $xy = 3x + 5y$ équivaut à $(x - 5)(y - 3) = 15$.
D'où les couples $(x ; y)$ solutions :
(6 ; 18), (4 ; –12), (20 ; 4), (–10 ; 2), (0 ; 0), (8 ; 8), (10 ; 6) et (2 ; –2).

71 Soit b un tel entier naturel. L'égalité $12 = bq + q$ ou encore $12 = q(b + 1)$ montre que b est diviseur de 12.
On cherche les couples $(q ; b)$ avec $b > q$ et $12 = q(b + 1)$.
Les solutions sont les couples (1 ; 11) et (2 ; 5). b peut valoir 11 ou 5.

83 Soit n un entier naturel.
1. $(n^2 + 8)^2 = n^4 + 16n^2 + 64$.
D'où $g(n) = (n^2 + 8)^2 - 16n^2 = (n^2 + 8 - 4n)(n^2 + 8 + 4n)$.
2. Pour tout entier naturel n : $n^2 + 8 - 4n \geqslant 4$ et $n^2 + 8 + 4n \geqslant 8$, les deux facteurs sont distincts de 1 donc l'entier $g(n)$ n'est pas premier.

91 $d_{(a,b)}$ a pour équation $y = -abx + ab$.
$f(a ; b) = ab$. D'où le résultat.

102 De $(x - y)(x + y) = p$ et x, y positifs, on déduit $x - y = 1$ et $x + y = p$.
D'où $x = \frac{1}{2}(p + 1)$ et $x = \frac{1}{2}(p - 1)$. On en déduit qu'il n'y a pas de solution pour $p = 2$ et un unique couple solution donné ci-dessus pour $p > 2$.

113 $2\,018 = 403 \times 5 + 3$. On a donc $2\,018 \equiv 3\ (5)$, d'où :
$2\,018^{2\,018} \equiv 3^{2\,018}\ (5)$.
Par ailleurs $3^4 = 16 \times 5 + 1$. On a donc $3^4 \equiv 1\ (5)$, d'où $(3^4)^{504} \equiv 1^{504}\ (5)$, soit $3^{2016} \equiv 1\ (5)$ et $3^{2016} \times 3^2 \equiv 1 \times 3^2\ (5)$ ou encore $3^{2018} \equiv 9\ (5)$.
Comme $9 \equiv 4\ (5)$, le reste cherché est 4.

115 1. Les sorties de l'algorithme pour les entrées $N = 0$, $N = 1$, $N = 2$, …, $N = 16$ sont :
0 ; 1 ; 2 ; 3 ; 4 ; –3 ; –2 ; –1 ; 0 ; 1 ; 2 ; 3 ; 4, –3 ; –2 ; –1 ; 0.
2. S est obtenu en enlevant à N un multiple de 8.
3. $7 \equiv -1\ (8)$ d'où $7^k + 1 \equiv (-1)^k + 1\ (8)$.
Si k est impair, le reste est 0. Si k est pair, le reste est 2.

127 On note respectivement u et d le chiffre des unités et celui des dizaines d'un entier naturel N.
1. N s'écrit $100A + 10d + u$.
Comme $100 \equiv 0\ (4)$ et $10 \equiv 2\ (4)$, on a le résultat.
2. N est divisible par 4 si, et seulement si, $2d + u$ est divisible par 4.

Pour faire le point

141 B ; **142** A ; **143** C ; **144** D ; **145** A et B ; **146** B (si on avait éliminé la valeur 2 pour p, A et C seraient des réponses également correctes) ; **147** A ; **148** A ; **149** B ; **150** C ; **151** A ; **152** B, C et D.

Chapitre 2 Problèmes de chiffrement

Avant de commencer

1 A, B et C ; 2 B ; 3 C ; 4 B ; 5 B et C ; 6 A, B, C et D.

7 d divise toutes les combinaisons linéaires de 182 et de 21 donc en particulier $182 - 8 \times 21 = 14$. Les valeurs positives possibles de d sont 1 ; 2 ; 7 ; 14 mais 21 n'est pas divisible par 2 et par 14.
Donc $d \in \{-1 ; 1 ; -7 ; 7\}$.

8 De $a = bq + r$, on déduit l'égalité $r = a - bq$ qui est une combinaison linéaire de a et de b.
Donc tout diviseur commun de a et de b divise r.

9 $3x \equiv 3\ (6) \Leftrightarrow 3x = 3 + 6q$ avec $q \in \mathbb{Z}$
$\Leftrightarrow x = 1 + 2q$ avec $q \in \mathbb{Z} \Leftrightarrow x \equiv 1\ (2)$

10 $y = -\frac{x}{3} + \frac{11}{12} \Leftrightarrow 12y + 4x = 11 \Leftrightarrow 4(3y + x) = 11$.
Pour tout x et tout y dans $\mathbb{Z}$, $4(3y + x)$ est un entier divisible par 4.
Or 11 n'est pas divisible par 4. L'équation est donc sans solution.

11 Si $n = 2p$ avec p entier naturel, $A_{2p} = 3^{2p} = 9^p$ et $9 \equiv 1\ (4)$
d'où $A_{2p} \equiv 1\ (4)$. Le reste est alors 1.
Si $n = 2p + 1$, avec p entier naturel, alors $A_{2p+1} = 3 \times A_{2p}$ et $A_{2p+1} \equiv 3\ (4)$.
Le reste est alors 3.

Exercices

4 1. Si d divise a et b, alors il divise $a - b$.
Or $a - b = c$, donc d divise b et c.
2. Si d divise b et c, alors il divise $b + c$. Or $b + c = a$, donc d divise a et b.
3. Si $a + b = c$, alors les diviseurs communs de a et de b sont les diviseurs communs de b et de c.

9 **a.** PGCD $(p\,;q) = 32$; **b.** PGCD $(p\,;q) = 5\times 23 = 115$;
c. PGCD $(p\,;q) = 12$; **d.** PGCD $(p\,;q) = 5^2\times 7^2 = 1\,225$.

14 Soit d le PGCD de $2n+1$ et de 5, avec n entier.
Alors d est un diviseur de 5 et prend les valeurs 1 ou 5.
Si $d = 5$ alors $2n+1$ est un multiple de 5 et n est de la forme $2+5q$, avec q entier. $d = 1$ dans les autres cas.

17 Il existe deux nombres entiers premiers entre eux a' et b' tels que $a = 9a'$, $b = 9b'$ et $a'+b' = 5$. a' prend les valeurs 1, 2, 3 et 4.
On obtient les couples (9 ; 36), (18 ; 27), (27 ; 18) et (36 ; 9).

25 1. Si $7n$ est divisible par 2, alors il existe k entier tel que $7n = 2k$.
Comme 7 et 2 sont premiers entre eux alors 2 divise n et n est pair.
2. De même avec 7 et 3 premiers entre eux.

28 1. Si m est divisible par 5 et n par 3, il existe k et k' entiers tels que $m = 5k$ et $n = 3k'$; alors $m\times n = 15kk'$. Il existe donc un entier $q = kk'$ tel que $m\times n = 15q$ et le produit est divisible par 15.
2. Si $m\times n$ est divisible par 15, alors m est divisible par 5 et n.
Cette réciproque est fausse, $m = 15$ et $n = 2$ fournit un contre-exemple.

38 1. PGCD (18 ; 27) = 9.
2. **(E)** $\Leftrightarrow 2(5-x) = 3(y+3)$. Comme 2 et 3 sont premiers entre eux alors, d'après le théorème de Gauss, 2 divise $y+3$ et 3 divise $5-x$. Il existe q et q' entiers tels que $y+3 = 2q$ et $5-x = 3q'$ et en remplaçant dans **(E)**, on trouve $q = q'$. D'où $x = 5-3q$ et $y = -3+2q$, q entier.
3. $x\in\mathbb{N} \Leftrightarrow 5-3q\geqslant 0 \Leftrightarrow q\leqslant \frac{5}{3}$; $y\in\mathbb{N} \Leftrightarrow -3+2q\geqslant 0 \Leftrightarrow q\geqslant \frac{3}{2}$.
Pour qu'il existe un couple d'entiers naturels solutions de **(E)**, il faut que $\frac{3}{2}\leqslant q\leqslant \frac{5}{3}$. Or il n'existe pas d'entier q vérifiant cette double inégalité.
Il n'existe pas d'entiers naturels solutions de **(E)**.

43 **a.** PPCM $(p\,;q) = 11\times 25$; **b.** PPCM $(p\,;q) = 4\times 5^3\times 49$;
c. PPCM $(p\,;q) = 8\times 13\times 14$; **d.** PPCM $(p\,;q) = 12\times 5\times 1\,000$.

48 1. 113 n'a pas de diviseurs positifs autre que 1 et lui-même.
113 n'a pas de diviseurs entre 2 et 10 et $\sqrt{113} < 11$.
2. 113 est premier et 7 n'est pas divisible par 113. D'après le petit théorème de Fermat, $7^{112}\equiv 1\ (113)$ donc le reste cherché est 1.

58 1. Soit d = PGCD $(A\,;B)$, d divise A et B donc d divise $5A-3B = 8$.
d est un diviseur de 8.
2. Si PGCD $(A\,;B) = 8$ alors il existe q et q' entiers tels que $A = 8q$ et $B = 8q'$, soit $3n\equiv 7\ (8)$ et $5n\equiv 1\ (8)$.
Par disjonction des cas, en utilisant les congruences modulo 8, on trouve que les entiers n cherchés sont tels que $n\equiv 5\ (8)$.

64 1. Si d est un diviseur commun de m et n, alors d divise toute combinaison linéaire de m et n et en particulier M et N.
2. Si d' est un diviseur commun de M et de N, alors il divise toute combinaison linéaire de M et de N et en particulier $5M-3N = -m$ et $7M-4N = n$. Donc d' divise m et n.
3. Les diviseurs communs de n et m sont les diviseurs communs de M et N : l'ensemble des diviseurs communs à n et m et à M et N ont donc le même plus grand élément. Alors PGCD $(m\,;n)$ = PGCD $(M\,;N)$.

71 1. Pour $n = 1$, p et q sont premiers entre eux. Pour $n\geqslant 2$: p et q ont pour PGCD n, et ils ne sont pas premiers entre eux.
2. Pour $n = 13$ ou $n = 11$, par exemple, p et q ne sont pas premiers entre eux.
3. p et q sont premiers entre eux pour toute valeur de n, car $-2p+q = 1$ (théorème de Bézout).
4. p et q sont premiers entre eux pour toute valeur de n. En effet, n est premier avec $n+1$, donc avec $(n+1)^2$. Ainsi, n^2 est premier avec $(n+1)^2$.

77 1. Comme $2n+1-2\times n = 1$, d'après le théorème de Bézout, n et $2n+1$ sont premiers entre eux.
2. En factorisant : $n^2-n = n(n-1)$ et $2n^2-n-1 = (2n+1)(n-1)$.
PGCD $(n^2-n\,;2n^2-n-1) = (n-1)$ PGCD $(n\,;2n+1) = n-1$.

88 $n = 11q+5$ et $n = 12q'+5$ avec q et q' entiers. D'où $11q = 12q'$.
Comme 11 et 12 sont premiers entre eux, d'après le théorème de Gauss : $q = 12k$ et $q' = 11k$ d'où $n = 132k+5$ ou $n\equiv 5\ (132)$.

91 1. Voir le cours 4, p. 54.
2. **a.** $x = 5k$ et $y = 4k$ avec k entier.
b. $x = 5k$ et $y = 2+4k$ avec k entier.
c. $x = 4+5k$ et $y = 2+4k$ avec k entier.

98 **a.** PGCD $(n\,;n+1) = 1$: PPCM $(p\,;q) = n(n+1)$.
b. $p = 2(n+1)$ et $q = 2(2n+1)$; PGCD $(n+1\,;2n+1) = 1$:
PPCM $(p\,;q) = 4(n+1)(2n+1)$.
c. $q = (n+1)^2$ et PGCD $(n\,;n+1) = 1$: PPCM $(p\,;q) = n^2(n+1)^2$.
d. $p = 4n\times n$ et $q = 3n(n+1)$: PPCM $(p\,;q) = 12n^2(n+1)$.

113 1. $546 = 2\times 3\times 7\times 13$.
2. **a.** 13 est premier donc, d'après le corollaire du petit théorème de Fermat : $x^{13}\equiv x\ (13)$.
b. 7 est premier, $x^7\equiv x\ (7)$ et $x^{13} = x^7\times x^6$ d'où $x^{13}\equiv x^7\ (7)$ et $x^{13}\equiv x\ (7)$.
c. On a toujours $x\equiv 0\ (3)$ ou $x\equiv 1\ (3)$ ou $x\equiv 2\ (3)$.
Dans les trois cas $x^{13}-x\equiv 0\ (3)$ d'où $x^{13}\equiv x\ (3)$.
d. On a toujours $x\equiv 0\ (2)$ ou $x\equiv 1\ (2)$.
Dans les deux cas $x^{13}-x\equiv 0\ (2)$ et $x^{13}\equiv x\ (2)$.
3. $x^{13}-x$ est divisible par 13, 7, 3 et 2 qui sont des entiers premiers entre eux, donc $x^{13}-x$ est divisible par le produit $13\times 7\times 3\times 2 = 546$.
D'où $x^{13}\equiv x\ (546)$.

Pour faire le point

124 B ; **125** A ; **126** C ; **127** C ; **128** A et B ; **129** C ; **130** B et C ; **131** B, C et D ; **132** A.

Chapitre 3 Problèmes sur les matrices

Avant de commencer

1 B ; 2 C ; 3 D ; 4 A ; 5 A ; 6 B ; 7 C.

8

	Femmes	Hommes	Total
Véhicule personnel	0,24	$0,45 = 0,75\times 0,6$	0,69
Train	$0,16 = 0,4\times 0,4$	0,15	0,31
Total	0,4	0,6	1

9 Notons a l'événement « l'individu possède le caractère A » et b l'événement « l'individu possède le caractère B ».
D'après l'énoncé, on a $p(\overline{a \text{ ou } b}) = 0,18$; d'où $p(a \text{ ou } b) = 0,82$ et $p(a \text{ et } b) = p(a)+p(b)-p(a \text{ ou } b) = 0,18$.
D'où $p_a(b) = \dfrac{p(a \text{ et } b)}{p(a)} = \dfrac{0,18}{0,6} = 0,3$.

Exercices

8 $A = \begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$.

12 $A = \begin{pmatrix} \ln a & 2\ln a \\ 3\ln a & 4\ln a \end{pmatrix}$, d'où $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

14 La calculatrice indique que l'on ne peut pas additionner deux matrices n'ayant pas les mêmes dimensions.

20 $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.

25 On a $AB = -B$.

28 $A^2 = \begin{pmatrix} \cos^2 a - \sin^2 a & -2\sin a \cos a \\ 2\sin a \cos a & \cos^2 a - \sin^2 a \end{pmatrix}$.

Les formules de trigonométrie usuelles permettent alors de conclure.

31 Le réel $a_{1,1}\,a_{2,2} - a_{2,1}\,a_{1,2}$ est non nul : la matrice est inversible. Pourtant la plupart des calculatrices signalent une matrice non inversible. Le problème est dû au fait que ces calculatrices remplacent $\frac{1}{3}$ par une valeur approchée de ce nombre.

37 Dans la ligne 1 de la matrice, on place un 1 en face du numéro de chaque personne ayant serré la main à la personne numéro 1 et un 0 partout ailleurs : la somme des éléments de cette ligne est donc égale au nombre de mains serrées par la personne numéro 1.
De même, la somme des éléments de la ligne 2 est égale au nombre de mains serrées par la personne numéro 2.
Mais si la personne numéro 2 a serré la main à la personne numéro 1, on voit que cette poignée de mains est comptée deux fois : une fois dans la somme des éléments de la ligne 1 et une fois dans la somme des éléments de la ligne 2.
En raisonnant de la même façon pour chaque ligne, on constate que la somme des coefficients de la matrice est égale au double du nombre de poignées de mains (c'est-à-dire, si l'on préfère, au nombre total de mains serrées, chaque poignée de mains faisant intervenir deux mains). Cette somme est donc nécessairement paire.

48 On cherche des réels a, b, c et d tels que :

$$\begin{pmatrix} a-2c & b-2d \\ c+2a & d+2b \end{pmatrix} = \begin{pmatrix} a+2b & b-2a \\ c+2d & d-2c \end{pmatrix}.$$

Ce qui est équivalent à $c = -b$ et $d = a$. Les matrices B qui conviennent sont les matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ où a et b sont des réels quelconques.

58 Après quelques calculs de puissances de A, on conjecture que pour tout entier $n \geqslant 1$, on a :

$$A^{2n} = \begin{pmatrix} 2^{n-1} & 0 & 2^{n-1} \\ 0 & 2^n & 0 \\ 2^{n-1} & 0 & 2^{n-1} \end{pmatrix} \text{ et } A^{2n+1} = \begin{pmatrix} 0 & 2^n & 0 \\ 2^n & 0 & 2^n \\ 0 & 2^n & 0 \end{pmatrix}.$$

On confirme ensuite cette conjecture à l'aide d'une démonstration par récurrence.

72 1. On vérifie que $A^2 = \begin{pmatrix} -2 & 3 & -3 \\ -3 & 4 & -3 \\ 3 & -3 & 4 \end{pmatrix}$.

On cherche ensuite deux réels a et b tels que $A^2 = aI_3 + bA$, soit :

$$\begin{pmatrix} -2 & 3 & -3 \\ -3 & 4 & -3 \\ 3 & -3 & 4 \end{pmatrix} = \begin{pmatrix} a & b & -b \\ -b & a+2b & -b \\ b & -b & a+2b \end{pmatrix}$$

On a $A^2 = -2I_3 + 3A$.

2. L'égalité $A^2 = -2I_3 + 3A$ s'écrit aussi $A(A - 3I_3) = -2I_3$.

A est donc inversible, d'inverse $B = \frac{-1}{2}(A - 3I_3)$.

79 1. La calculatrice affiche pour l'inverse de A la matrice :

$$\begin{pmatrix} -0{,}5 & 0{,}75 & 0{,}25 \\ 1{,}5 & -2{,}25 & 0{,}25 \\ -0{,}5 & 1{,}25 & -0{,}25 \end{pmatrix}.$$

On vérifie que B est bien l'inverse de A en calculant le produit AB ou le produit BA.

2. Le système constitué des trois équations de plan s'écrit aussi sous la forme $A\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \\ 7 \end{pmatrix}$ ou encore $B\begin{pmatrix} 5 \\ 1 \\ 7 \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

Or $B\begin{pmatrix} 5 \\ 1 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ -3 \end{pmatrix}$, l'intersection des trois plans $\mathscr{P}$, $\mathscr{Q}$, $\mathscr{R}$ est donc constituée du point M de coordonnées (0 ; 7 ; −3).

Pour faire le point

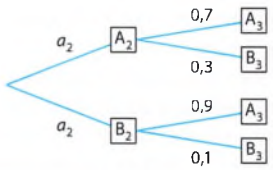
89 A, B et C ; **90** D ; **91** A, C et D ; **92** A et D ; **93** A, C et D ; **94** B ; **95** A et D ; **96** A et B.

Chapitre 4 Problèmes d'évolution

Avant de commencer

1 C ; 2 C ; 3 B ; 4 D ; 5 B ; 6 C.

7 1. $a_1 = 1$ et $b_1 = 0$.
D'après l'énoncé, $a_2 = 0{,}7$ et $b_2 = 0{,}3$.
Pour déterminer a_3 et b_3, on peut faire un arbre de probabilités, en nommant A_n l'événement « Maël se baigne » et B_n l'événement « Maël ne se baigne pas ». $a_3 = 0{,}7a_2 + 0{,}9b_2 = 0{,}76$ et $b_3 = 0{,}3a_2 + 0{,}1b_2 = 0{,}24$.



2. À l'aide d'un arbre de probabilités similaire avec A_n, A_{n+1}, B_n et B_{n+1}, on trouve :

$$a_{n+1} = 0{,}7a_n + 0{,}9b_n \text{ et } b_{n+1} = 0{,}3a_n + 0{,}1b_n.$$

8 1. $P^{-1} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$, puis $D = \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}$.

2. D est une matrice diagonale, donc $D^n = \begin{pmatrix} 5^n & 0 \\ 0 & 4^n \end{pmatrix}$.

$D = P^{-1}AP \Leftrightarrow A = PDP^{-1}$, d'où :

$$A^n = (PDP^{-1})(PDP^{-1}) \ldots (PDP^{-1}) = PD^nP^{-1}.$$

D'où $A^n = \begin{pmatrix} 4^n & 0 \\ 2 \times 4^n - 2 \times 5^n & 5^n \end{pmatrix}$.

Exercices

7 1. $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$.

2. D'après le cours : $X_n = A^n X_0$, avec $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

D'où : $\begin{cases} x_n = 2^{n+1} - 3^n \\ y_n = 2^{n+1} - 2 \times 3^n \end{cases}$

3. On écrit : $x_n = 3^n\left(2 \times \left(\frac{2}{3}\right)^n - 1\right)$ et $y_n = 3^n\left(2 \times \left(\frac{2}{3}\right)^n - 2\right)$.

Puisque la limite de la suite de terme général $\left(\frac{2}{3}\right)^n$ est 0, et celle de la suite de terme général 3^n est $+\infty$, on en déduit que les suites (x_n) et (y_n) ont pour limite $-\infty$: elles sont divergentes.

9 1. Si une suite constante, égale à c, est solution, alors $c = 3c - 2$, soit $c = 1$.
La suite (t_n) de terme général $t_n = 1$ est solution de cette relation de récurrence.

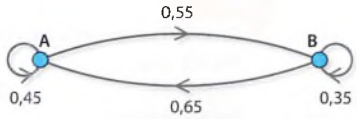
2. $v_{n+1} = u_{n+1} - 1 = (3u_n - 2) - 1 = 3(u_n - 1) = 3v_n$.
(v_n) est une suite géométrique de raison 3, avec $v_0 = 1$.

D'où $v_n = 3^n$. Et ainsi : $u_n = v_{n+1} = 3^n + 1$.

18 1. La matrice de transition donne les valeurs suivantes :

$$p_{A,A} = 0{,}45 \; ; \; p_{A,B} = 0{,}55 \; ; \; p_{B,A} = 0{,}65 \; ; \; p_{B,B} = 0{,}35.$$

D'où le graphe de cette marche aléatoire :



2. $p_{A,A} = 0{,}45$ pour chacune des deux étapes : puisqu'il y a indépendance, la probabilité que les deux états suivants du système soient A est $0{,}45^2 = 0{,}2025$.

25 La matrice de transition M ne contient pas de 0, donc il existe un état stable. Pour le déterminer, on résout :

$$\begin{pmatrix} x & y \end{pmatrix} \times M = \begin{pmatrix} x & y \end{pmatrix}, \text{ avec } x + y = 1.$$

On a : $0{,}1x + 0{,}7y = x$, soit $0{,}9x = 0{,}7y$, ou $9x = 7y$.
Comme $y = 1 - x$, on obtient : $9x = 7 - 7x$, soit $x = \frac{7}{16}$.
L'état stable est donc : $\begin{pmatrix} \frac{7}{16} & \frac{9}{16} \end{pmatrix}$.

31 1. $P^{-1} = \begin{pmatrix} 0{,}5 & 0{,}5 & -0{,}5 \\ 0{,}5 & -0{,}5 & 0{,}5 \\ -0{,}5 & 0{,}5 & 0{,}5 \end{pmatrix}$. On calcule : $D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

2. $D^n = \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & 3^n & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

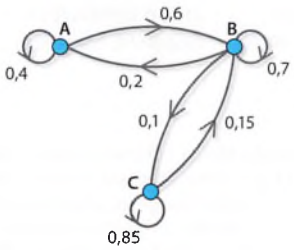
Puisque $A = PDP^{-1}$, on a :

$$A^n = PD^nP^{-1} = \frac{1}{2}\begin{pmatrix} (-1)^n + 3^n & (-1)^n - 3^n & (-1)^{n+1} + 3^n \\ (-1)^n - 1 & (-1)^n + 1 & (-1)^{n+1} + 1 \\ 3^n - 1 & -3^n + 1 & 3^n + 1 \end{pmatrix}.$$

3. $X_n = A^nX_0 = \begin{pmatrix} 2 \times (-1)^n \\ 2 \times (-1)^n - 2 \\ -2 \end{pmatrix}$.

4. La suite de terme général $(-1)^n$ n'a pas de limite, donc la suite de matrices (X_n) n'est pas convergente.

61 1. Graphe associé :



2. Matrice de transition :

$$M = \begin{pmatrix} 0{,}4 & 0{,}6 & 0 \\ 0{,}2 & 0{,}7 & 0{,}1 \\ 0 & 0{,}15 & 0{,}85 \end{pmatrix}.$$

3. **a.** La répartition prévisible au bout de 4 ans est donnée par :

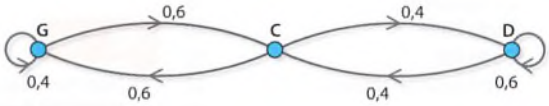
$$P_4 = \begin{pmatrix} 0{,}4 & 0{,}5 & 0{,}1 \end{pmatrix} \times M^4.$$

Or $M_4 \approx \begin{pmatrix} 0{,}225 & 0{,}611 & 0{,}163 \\ 0{,}204 & 0{,}572 & 0{,}224 \\ 0{,}082 & 0{,}337 & 0{,}582 \end{pmatrix}$, à 10^{-3} près, donc :

$$P_4 \approx \begin{pmatrix} 0{,}200 & 0{,}564 & 0{,}236 \end{pmatrix}.$$

b. $M_8 \approx \begin{pmatrix} 0{,}189 & 0{,}542 & 0{,}269 \\ 0{,}181 & 0{,}527 & 0{,}292 \\ 0{,}135 & 0{,}438 & 0{,}427 \end{pmatrix}$, à 10^{-3} près, donc au bout de 8 ans : $M_8 \approx \begin{pmatrix} 0{,}179 & 0{,}524 & 0{,}296 \end{pmatrix}$.

71 1. Graphe associé :



2. Matrice de transition :

$$M = \begin{pmatrix} 0{,}4 & 0{,}6 & 0 \\ 0{,}6 & 0 & 0{,}4 \\ 0 & 0{,}4 & 0{,}6 \end{pmatrix}.$$

3. $M^2 = \begin{pmatrix} 0{,}52 & 0{,}24 & 0{,}24 \\ 0{,}24 & 0{,}52 & 0{,}24 \\ 0{,}24 & 0{,}24 & 0{,}52 \end{pmatrix}$: M^2 ne contient pas de 0, donc il existe un état stable.
Pour le déterminer, on résout :

$$\begin{pmatrix} x & y & z \end{pmatrix} \times M = M, \text{ avec } x + y + z = 1.$$

On a :

$$\begin{cases} 0{,}4x + 0{,}6y = x \\ 0{,}6x + 0{,}4z = y \\ 0{,}4y + 0{,}6z = z \end{cases} \text{ soit } \begin{cases} x = y \\ 3x + 2z = 5y \\ y = z \end{cases}, \text{ soit } x = y = z.$$

Puisque $x + y + z = 1$, l'état stable est $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$.

Au bout d'un nombre important d'échanges, le roi de trèfle a autant de chances d'être à gauche, au centre ou à droite.

Pour faire le point

81 A, C et D ; **82** A ; **83** B ; **84** B ; **85** D ; **86** C ; **87** C.

Index

Crédits photographiques

6 et 7 : DR ; **9** ph © photlook - Fotolia ; **14** Ph coll Archives Sejer ; **16 et 45** ph © Rabatti Marco / Domingie Serge/Akg-images/T ; **18 et 54** BIS / Ph. J.L. Charmet © Archives Larbor ; **27** BIS / Ph. Coll. Archives Nathan ; **31** ph © Prod. Numérik - Fotolia ; **39** et p 60 BIS / Ph. © Archives Bordas ; **41** BIS / Ph. Coll. Archives Larbor ; **42 et 43** ph © SPL/COSMOS ; **44** ph © Radius Images/Corbis ; **51** ph © akg-images ; **52** © Jacques Boyer / Roger-Viollet ; **57** The Mathematical Association of America, 2011 ; **66** BIS / © Banque centrale européenne ; **75** ph © Philippe Roy/Hemis/Corbis ; **76** ph © Nikolai Tsvetkov - Fotolia ; **78 et 79** ph © ph.guignard/air-images.net ; **80** BIS/ Ph coll Archives Sejer ; **96** DR ; **102** Ph Coll Archives Sejer ; **107** ph © AKG-images/T ; **110 et 111** ph © ktsdesign - Fotolia ; **113 g & dt :** Ph coll Archives Sejer ; **116** ph © Jason DeCrow/AP/SIPA ; **120 et p 130 :** ph © Science Photo Library/AKG-Images ; **124** ph © kontur-vid – Fotolia ; **125** ph © Christian Maurer - Fotolia ; **127** ph © 4 R. Peterkin - Fotolia ; **138** ph ©Gilles ROLLE/REA

Édition : Julien Barret
Conception graphique : Oxygène
Couverture : Mecano
Composition et schémas : Soft Office
Recherche iconographique : Clémence Zagorsky
Fabrication : Jean-Philippe Dore

Imprimé en Espagne par GRAFICAS ESTELLA
No de Projet : 10216844- Dépôt legal : juin 2015

Une table de nombres premiers

Voici la liste des nombres premiers compris entre 1 et 5 000.

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
1 009	1 013	1 019	1 021	1 031	1 033	1 039	1 049	1 051	1 061	1 063	1 069	1 087	1 091
1 093	1 097	1 103	1 109	1 117	1 123	1 129	1 151	1 153	1 163	1 171	1 181	1 187	1 193
1 201	1 213	1 217	1 223	1 229	1 231	1 237	1 249	1 259	1 277	1 279	1 283	1 289	1 291
1 297	1 301	1 303	1 307	1 319	1 321	1 327	1 361	1 367	1 373	1 381	1 399	1 409	1 423
1 427	1 429	1 433	1 439	1 447	1 451	1 453	1 459	1 471	1 481	1 483	1 487	1 489	1 493
1 499	1 511	1 523	1 531	1 543	1 549	1 553	1 159	1 567	1 571	1 579	1 583	1 597	1 601
1 607	1 609	1 613	1 619	1 621	1 627	1 637	1 657	1 663	1 667	1 669	1 693	1 697	1 699
1 709	1 721	1 723	1 733	1 741	1 747	1 753	1 759	1 777	1 783	1 787	1 789	1 801	1 811
1 823	1 831	1 847	1 861	1 867	1 871	1 873	1 877	1 879	1 889	1 901	1 907	1 913	1 931
1 933	1 949	1 951	1 973	1 979	1 987	1 993	1 997	1 999	2 003	2 011	2 017	2 027	2 029
2 039	2 053	2 063	2 069	2 081	2 083	2 087	2 089	2 099	2 111	2 113	2 129	2 131	2 137
2 141	2 143	2 153	2 161	2 179	2 203	2 207	2 213	2 221	2 237	2 239	2 243	2 251	2 267
2 269	2 273	2 281	2 287	2 293	2 297	2 309	2 311	2 333	2 339	2 341	2 347	2 351	2 357
2 371	2 377	2 381	2 383	2 389	2 393	2 399	2 411	2 417	2 423	2 437	2 441	2 447	2 459
2 467	2 473	2 477	2 503	2 521	2 531	2 539	2 543	2 549	2 551	2 557	2 579	2 591	2 593
2 609	2 617	2 621	2 633	2 647	2 657	2 659	2 663	2 671	2 677	2 683	2 687	2 689	2 693
2 699	2 707	2 711	2 713	2 719	2 729	2 731	2 741	2 749	2 753	2 767	2 777	2 789	2 791
2 797	2 801	2 803	2 819	2 833	2 837	2 843	2 851	2 857	2 861	2 879	2 887	2 897	2 903
2 909	2 917	2 927	2 939	2 953	2 957	2 963	2 969	2 971	2 999	3 001	3 011	3 019	3 023
3 037	3 041	3 049	3 061	3 067	3 079	3 083	3 089	3 109	3 119	3 121	3 137	3 163	3 167
3 169	3 181	3 187	3 191	3 203	3 209	3 217	3 221	3 229	3 251	3 253	3 257	3 259	3 271
3 299	3 301	3 307	3 313	3 319	3 323	3 329	3 331	3 343	3 347	3 359	3 361	3 371	3 373
3 389	3 391	3 407	3 413	3 433	3 449	3 457	3 461	3 463	3 467	3 469	3 491	3 499	3 511
3 517	3 527	3 529	3 533	3 539	3 541	3 547	3 557	3 559	3 571	3 581	3 583	3 593	3 607
3 613	3 617	3 623	3 631	3 637	3 643	3 659	3 671	3 673	3 677	3 691	3 697	3 701	3 709
3 719	3 727	3 733	3 739	3 761	3 767	3 769	3 779	3 793	3 797	3 803	3 821	3 823	3 833
3 847	3 851	3 853	3 863	3 877	3 881	3 889	3 907	3 911	3 917	3 919	3 923	3 929	3 931
3 943	3 947	3 967	3 989	4 001	4 003	4 007	4 013	4 019	4 021	4 027	4 049	4 051	4 057
4 073	4 079	4 091	4 093	4 099	4 111	4 127	4 129	4 133	4 139	4 153	4 157	4 159	4 177
4 201	4 211	4 217	4 219	4 229	4 231	4 241	4 243	4 253	4 259	4 261	4 271	4 273	4 283
4 289	4 297	4 327	4 337	4 339	4 349	4 357	4 363	4 373	4 391	4 397	4 409	4 421	4 423
4 441	4 447	4 451	4 457	4 463	4 481	4 483	4 493	4 507	4 513	4 517	4 519	4 523	4 547
4 549	4 561	4 567	4 583	4 591	4 597	4 603	4 621	4 637	4 639	4 643	4 649	4 651	4 657
4 663	4 673	4 679	4 691	4 703	4 721	4 723	4 729	4 733	4 751	4 759	4 783	4 787	4 789
4 793	4 799	4 801	4 813	4 817	4 831	4 861	4 871	4 877	4 889	4 903	4 909	4 919	4 931
4 933	4 937	4 943	4 951	4 957	4 967	4 969	4 973	4 987	4 993	4 999			