MANUEL LIBRE

Term S

MATRICES et SUITES • ARITHMÉTIQUE

Delphine ARNAUD
Lycée Dominique Savio,
Douala

Bruno CASAVECCHIA
Lycée Dominique Savio,
Douala

Paul MILAN
Lycée d'adultes de la Ville
de Paris

Environnement numérique et
relectures réalisés par l'association
Sésamath

MAGNARD

SOMMAIRE

ARITHMÉTIQUE

PRÉPARER LE BACCALAURÉAT

Dans cette partie, les notions des différents chapitres de ce manuel sont regroupées dans un ensemble d'activités : problèmes ouverts, problèmes de synthèse et QCM. Le but est de développer les compétences utiles pour le bac : organiser ses connaissances, mener un raisonnement, rédiger clairement la résolution d'un problème.

MATRICES ET SUITES

LOGOS ET INDICATIONS

19	Exercice corrigé en fin de manuel
INFO	Exercice avec l'ordinateur
CALC	Exercice avec la calculatrice
ALGO	Exercice d'algorithmique

TRAVAILLER UN CHAPITRE

Manuel et **manuel numérique**, deux outils complémentaires

1 VÉRIFIER SES PRÉREQUIS

1 Réalisez le test de début de chapitre.

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 Montrer que les nombres suivants sont des nombres premiers :

1) 31 2) 47 3) 53 4) 61 5) 83

2 Sans calculatrice, à l'aide des critères de divisibilité par 3, 5 et 11 ou de la division par 7, montrer que les nombres suivants ne sont pas premiers :

1) 57 3) 143 5) 341 7) 319
2) 91 4) 265 6) 427 8) 1581

3 Sans calculatrice, donner tous les diviseurs des nombres suivants :

1) 16 3) 24 5) 45 7) 63
2) 15 4) 36 6) 51 8) 91

4 Traduire avec une seule égalité de congruence les propositions suivantes :

1) n est divisible par 6.
2) n est divisible par 3 et par 5.
3) n est divisible par 4 et par 6.
4) n est divisible par 8 et par 9.

5 Traduire par une phrase les propositions suivantes sans utiliser le mot « congruence » :

1) $n \equiv 0\ (5)$.
2) si $n \equiv 0\ (4)$ et $n \equiv 0\ (5)$, alors $n \equiv 0\ (20)$.
3) Si $n \leqslant 25$ et si $n \not\equiv 0\ (2)$, $n \not\equiv 0\ (3)$, $n \not\equiv 0\ (5)$ alors n est premier.
4) Si p est premier et si $ab \equiv 0\ (p)$, alors $a \equiv 0\ (p)$ ou $b \equiv 0\ (p)$.

Voir solutions p. 151

2 Vérifiez vos réponses en fin de manuel.

Chapitre AR3
Les nombres premiers

Auto-évaluation

1 Ils ne comptent aucun diviseur autre que 1 et eux-même.

2 1) divisible par 3 5) divisible par 11
2) divisible par 7 6) divisible par 7
3) divisible par 11 7) divisible par 11
4) divisible par 5 8) divisible par 3

2 APPRENDRE UNE LEÇON

1 Apprenez les définitions et les propriétés.

2 Refaites les exercices corrigés des méthodes du cours.

Renvoi

MÉTHODE 1 **Multiplier deux matrices**

Ex. 30 p. 97

Pour calculer la matrice C égale à AB, on vérifie que le nombre de colonnes de A est égal au nombre de lignes de B, puis on dispose les matrices suivant le schéma $\begin{array}{c|c} & B \\ \hline A & C \end{array}$ de sorte que c_{ij} soit à l'intersection du prolongement de la i-ème ligne de A et de la j-ième colonne de B.

Exercice d'application Soit $A = \begin{pmatrix} 1 & 3 & 5 & -2 \\ -2 & 0 & -3 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 & -3 \\ 3 & -1 & 0 \\ 0 & -2 & 2 \\ 2 & -3 & -4 \end{pmatrix}$. Calculer AB.

Correction

A est de taille 2×4 et B de taille 4×3.
A a autant de colonnes que B a de lignes, donc $C = AB$ existe et sa taille est 2×3.
On dispose les matrices comme ci-contre.

$$\begin{pmatrix} 2 & 1 & -3 \\ 3 & -1 & 0 \\ 0 & -2 & 2 \\ 2 & -3 & -4 \end{pmatrix}$$

3 Faites l'exercice d'entraînement lié à la méthode.

30 MÉTHODE 1 p. 90

Effectuer les produits des matrices suivantes :

1) $\begin{pmatrix} 2 & 1 & -1 \\ -3 & 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ -1 \\ 1 \end{pmatrix}$

2) $\begin{pmatrix} 5 & 2 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -3 & 1 \end{pmatrix}$

3) $\begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}\begin{pmatrix} 2 & -1 & 1 \end{pmatrix}$

4) $\begin{pmatrix} -1 & 2 & 1 \\ 0 & 2 & 2 \\ -2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$

4 Vérifiez vos réponses en fin de manuel

30 1) $\begin{pmatrix} 6 \\ -13 \end{pmatrix}$

2) $\begin{pmatrix} 4 & -3 \\ -8 & 3 \end{pmatrix}$

3) $\begin{pmatrix} 8 & -4 & 4 \\ 2 & -1 & 1 \\ 4 & -2 & 2 \end{pmatrix}$

4) $\begin{pmatrix} -4 \\ -2 \\ -7 \end{pmatrix}$

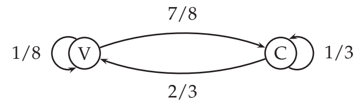
3 S'ENTRAÎNER POUR LE BAC

1. Repérez les éléments importants de la consigne, comme les verbes d'action à l'infinitif.

2. Vérifiez votre compréhension du vocabulaire.
→ utilisez le lexique à la fin du manuel ou sur le manuel numérique.

3. Réalisez un schéma si nécessaire ou utilisez un tableur, une calculatrice, un logiciel de géométrie dynamique…

28 Le graphe probabiliste suivant décrit la succession des voyelles (V) et des consonnes (C) dans le roman *Eugène Onéguine* de Pouchkine (voir 6 page 115) :

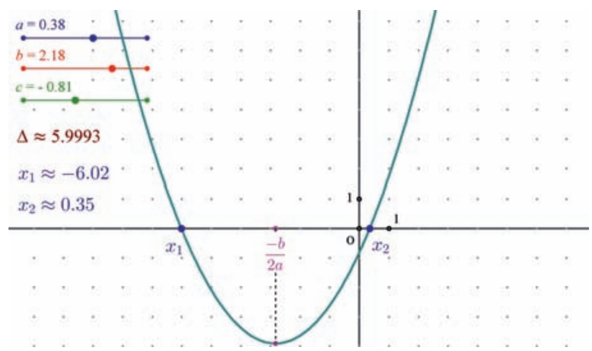


On note par une matrice ligne P_n la répartition de probabilité à la n-ième lettre du livre.

1) Déterminer la matrice de transition T telle que $P_{n+1} = P_n T$.

2) Déterminer un réel λ et une matrice Q tels que :
$$P_{n+1} = \lambda P_n + Q.$$

4. Réalisez les parcours pédagogiques personnalisés (J3P) pour vous entraîner et éventuellement approfondir les notions étudiées.



4 PRÉPARER LE BAC

1. Faites les exercices d'activités mentales.
Sans difficultés calculatoires, ils permettent de vérifier que les raisonnements sont compris.

2. Vérifiez vos réponses en fin de manuel.

3. Réalisez le QCM de fin de chapitre.

4. Vérifiez vos réponses en fin de manuel.

5. Consultez les compléments proposés dans le manuel numérique.

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Au moins une réponse est exacte. Déterminer la (ou les) bonne(s) réponse(s).

53 Lequel parmi ces nombres n'est pas premier ?
a) 227 b) 379 c) 221 d) 313

54 Pour établir la liste des nombres premiers inférieurs à 4 000 à l'aide du crible d'Ératosthène, on raye les multiples des nombres premiers jusqu'à :
a) 61 b) 67 c) 100 d) 4 000

55 On considère le nombre $N = n + (n+2) + n(n+2)$ avec $n \in \mathbb{N}$. Le nombre N est premier :
a) si n est impair.
b) pour aucune valeur de n.
c) pour les 4 premières valeurs impaires de n.
d) si n est premier.

56 Parmi les phrases suivantes, quelles sont celles qui sont vraies ?
a) Si n est un nombre premier, alors n est impair.
b) Si p et q sont deux nombres premiers distincts, alors p et q sont premiers entre eux.
c) Si p est premier et divise le produit ab, alors p divise a ou p divise b.
d) Soit p un nombre premier. Si $a \equiv p\ (p)$, alors a est premier.

57 Parmi les phrases suivantes, quelles sont celles qui sont vraies ?
a) Si n est un nombre impair, alors n est un nombre premier.
b) Si p et q sont premiers entre eux, alors p et q sont des nombres premiers.
c) Si p divise a ou p divise b, alors p divise le produit ab.
d) Soit p un nombre premier. Si a est premier alors $a \equiv p\ (p)$.

MÉTHODES DE L'ANNÉE

Arithmétique

Matrices

ARITHMÉTIQUE

1

Multiples. Division euclidienne. Congruence

Connaissances nécessaires à ce chapitre

- Connaître les critères de divisibilité
- Déterminer les diviseurs d'un nombre
- Déterminer les restes d'une division par 3, 4, 5 et 9
- Maîtriser le vocabulaire de la division : dividende, diviseur, quotient et reste.
- Effectuer des opérations sur la parité

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 Sans l'aide de la calculatrice, déterminer si les nombres suivants sont divisibles par 4.

1) 136 **2)** 514 **3)** 1 352 **4)** 9 894

2 Sans l'aide de la calculatrice, déterminer si les nombres suivants sont des multiples de 3 ou de 9.

1) 129 **2)** 567 **3)** 5 634 **4)** 21 573

3 Parmi les entiers suivants, indiquer sans effectuer de division ceux qui sont divisibles par 6 :

456, 251, 512, 645, 842, 50 106

4 Déterminer tous les diviseurs des nombres suivants (on pourra s'aider des critères de divisibilité) :

1) 36 (9 diviseurs) **2)** 48 (10 diviseurs) **3)** 96 (12 diviseurs) **4)** 240 (20 diviseurs)

5 Sans l'aide de la calculatrice, trouver les restes des divisions suivantes :

1) 1 951 par 3 **2)** 165 par 3 **3)** 1 945 par 9 **4)** 457 par 9 **5)** 1 542 par 5 **6)** 788 par 5

6 On divise 7 entiers naturels successifs par 7. Quels sont les restes obtenus ?

7 On donne : $117 = 6 \times 17 + 15$.

1) Dans la division de 117 par 17, donner le dividende, le quotient et le reste.

2) Quel est le reste de la division de 117 par 6 ?

8 Un nombre n est la somme de deux entiers a et b.

1) n est pair. Quelle peut être la parité de a et de b ?

2) n est impair. Quelle peut être la parité de a et de b ?

3) Énoncer une règle sur la parité de la somme de deux entiers.

9 Un nombre n est le produit de deux entiers a et b.

1) n est pair. Quelle peut être la parité de a et de b ?

2) n est impair. Quelle peut être la parité de a et de b ?

3) Énoncer une règle sur la parité du produit de deux entiers.

10 Un nombre n est le carré d'un entier a.

1) n est pair. Quelle peut être la parité de a ?

2) n est impair. Quelle peut être la parité de a ?

3) Énoncer une règle sur la parité d'un entier et de son carré.

Voir solutions p. 151

Activités d'approche

ACTIVITÉ 1 Nombres parfaits et nombres amiables

1) Un diviseur strict d'un entier naturel n est un entier naturel, distinct de n, qui divise n.

a) Déterminer les 12 diviseurs de 220. Quels sont ses diviseurs stricts ?

b) Déterminer les 10 diviseurs de 496. Quels sont ses diviseurs stricts ?

2) Un nombre parfait est un nombre égal à la somme de ses diviseurs stricts.
496 est-il un nombre parfait ?

3) Deux entiers sont dits amiables si chacun d'eux est égal à la somme de tous les diviseurs stricts de l'autre. Faire la somme des diviseurs stricts de 220. En déduire avec quel entier n, le nombre 220 peut être amiable. Vérifier alors que n et 220 sont amiables.

ACTIVITÉ 2 Un problème de calendrier

Sachant que le 1er janvier 2015 était un jeudi, le but de cette activité est de déterminer le jour de la semaine correspondant au 1er janvier 2040.
On rappelle qu'une année normale contient 365 jours et qu'une année bissextile en contient 366. Une année n est bissextile si n est divisible par 4 mais pas par 100, ou si n est divisible par 400 (1900 n'était pas bissextile, mais 2000 l'était).

1) Déterminer le nombre de jours N séparant le 1er janvier 2015 et le 1er janvier 2040.

2) Pour déterminer le jour de la semaine du 1er janvier 2040, on s'intéresse au reste r de la division euclidienne de N par 7. On dit que r et N sont congrus modulo 7 car ils ont le même reste dans la division par 7. À quelle valeur est alors congru N modulo 7 ?

3) En déduire le jour de la semaine du 1er janvier 2040.

ACTIVITÉ 3 Clés des numéros ISBN

L'*International Standard Book Number* permet de coder tous les ouvrages édités dans le monde entier. Il est composé de 13 chiffres.

Étudions le **numéro ISBN** : 978-2-86889-006-1. Il est décomposé en :

- une première partie N de 12 chiffres commençant par 978 ou 979. Ici, en enlevant les tirets, on a $N = 978\,286\,889\,006$;
- une seconde partie K, qui représente la clé, composée de 1 chiffre (de 1 à 9). Ici $K = 1$.

On détermine la clé K de la façon suivante :

- on forme un nombre n en additionnant les chiffres du numéro ISBN après avoir multiplié par 3 les chiffres de rang pair :
$n = 9+3\times7+8+3\times2+8+3\times6+8+3\times8+9+3\times0+0+3\times6 = 129$;
- on détermine le reste r dans la division euclidienne de n par 10 :
$129 = 10\times12+9$, on obtient alors $r = 9$.
- on soustrait ce reste à 10 : $K = 10 - r = 10 - 9 = 1$.

1) Vérifier la clé sur le code ISBN de l'image ci-contre.

2) Quelle doit être la valeur de a pour que le code 978-2-84225-01a-1 soit un code ISBN ?

ISBN : 978-2-210-10467-9
9 782210 104679

1. Avant-propos

L'arithmétique a pour objet l'étude des nombres entiers.
Ces entiers peuvent être naturels ($\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \dots\}$) ou relatifs ($\mathbb{Z} = \{\dots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\dots\}$).

> « L'arithmétique [...] a le privilège d'avoir passionné les mathématiciens les plus éminents en même temps qu'elle n'a cessé d'attirer les amateurs. Cette séduction tient, pour beaucoup, dans ce dernier cas, au fait que des problèmes très difficiles, parfois non résolus, ont souvent des énoncés simples qui peuvent être compris à partir d'une formation mathématique élémentaire. Gauss tenait l'arithmétique pour la "la reine des mathématiques" et on a pu dire que la théorie des nombres était "la plus pure des mathématiques pures". »

François Le Lionnais (1901-1984), dans *Dictionnaire des mathématiques*, Éditions Puf, 1979

On admettra les propriétés suivantes :

PROPRIÉTÉS

- **Principe du bon ordre** : toute partie **non vide** de $\mathbb{N}$ admet un plus petit élément.
- **Principe de descente infinie** : toute suite dans $\mathbb{N}$ strictement décroissante est stationnaire à partir d'un certain rang.
- **Principe des tiroirs** : si on range $(n+1)$ chaussettes dans n tiroirs, alors au moins un tiroir contiendra au moins 2 chaussettes.

Les deux premières propriétés seront utilisées dans les deux prochains chapitres.
Lorsqu'on s'intéresse à la partie décimale du résultat de la division d'un entier par n, on est sûr qu'à partir de la $(n+1)$-ième décimale, on obtiendra un reste déjà obtenu (principe des tiroirs). Cela explique la partie décimale périodique d'un nombre rationnel non décimal.

2. Multiples et diviseurs dans $\mathbb{Z}$

A. Définition et propriétés

DÉFINITION

Soit a et b deux entiers relatifs.
a est un **multiple** de b si, et seulement si, il existe un entier relatif k tel que : $a = kb$.

REMARQUES :

- D'autres formulations sont possibles : « a est divisible par b », « b divise a », « b est un **diviseur** de a » pour décrire la relation $a = kb$.
- On utilise aussi la notation $b|a$ pour signifier que b divise a.

Exemples

1) $6 = 2 \times 3$ donc 2 et 3 sont des diviseurs de 6.
   Les diviseurs dans $\mathbb{N}$ de 6 sont : 1, 2, 3, 6.
2) $-52 = (-4) \times 13$ donc $-4,\ 4,\ -13$ et 13 sont des diviseurs de -52.
   Les diviseurs dans $\mathbb{Z}$ de -52 sont : $-52,\ -26,\ -13,\ -4,\ -2,\ -1,\ 1,\ 2,\ 4,\ 13,\ 26,\ 52$.

PROPRIÉTÉS

1) 0 est **multiple** de tout entier a car $0 = 0 \times a$.
2) 1 **divise** tout entier a car $a = a \times 1$.
3) Si a est un **multiple** de b et si $a \neq 0$, alors : $|a| \geqslant |b|$.
4) Soit a et b non nuls, si a **divise** b et si b **divise** a, alors $a = b$ ou $a = -b$.

MÉTHODE 1 Utiliser la divisibilité pour résoudre un problème

► Ex. 13 p. 16

Comme un entier ne possède qu'un nombre restreint de diviseurs, on cherchera à factoriser et à reconnaître les diviseurs pour résoudre une équation ou un problème de divisibilité.

Exercice d'application Déterminer tous les couples d'entiers naturels $(x;y)$ tels que : $x^2 - 2xy = 15$.

Correction On factorise par x : $x^2 - 2xy = 15 \quad \Leftrightarrow \quad x(x-2y) = 15$.
On détermine les diviseurs positifs de 15 : $D_{15} = \{1\ ,\ 3\ ,\ 5\ ,\ 15\}$.
Puisque $x > 0$ et $y > 0$, on a $x > x - 2y$. On obtient les décompositions suivantes :

$$\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \text{ ou } \begin{cases} x = 5 \\ x - 2y = 3 \end{cases} \quad \Leftrightarrow \quad \begin{cases} x = 15 \\ y = \dfrac{x-1}{2} = 7 \end{cases} \text{ ou } \begin{cases} x = 5 \\ y = \dfrac{x-3}{2} = 1 \end{cases}$$

Les couples solutions sont donc : $(15\,;7)$ et $(5\,;1)$.

Exercice d'application Déterminer tous les entiers relatifs n tels que $(n-3)$ divise $(n+5)$.

Correction Si $(n-3)$ divise $(n+5)$, alors il existe un entier k tel que : $n + 5 = k(n-3)$.
De l'astuce $5 = -3 + 8$, on obtient :

$$(n-3) + 8 = k(n-3) \quad \Leftrightarrow \quad k(n-3) - (n-3) = 8 \quad \Leftrightarrow \quad (n-3)(k-1) = 8$$

Donc $(n-3)$ est un diviseur de 8.
Les diviseurs relatifs de 8 sont : $D_8 = \{-8\,;-4\,;-2\,;-1\,;\,1\,;\,2\,;\,4\,;\,8\}$.
On a donc le tableau suivant correspondant aux valeurs possibles de n :

$n-3$	-8	-4	-2	-1	1	2	4	8
n	-5	-1	1	2	4	5	7	11

On vérifie que $(n-3)$ divise bien $(n+5)$ pour toutes ces valeurs de n.

B. Opérations sur les multiples

PROPRIÉTÉ

Soit trois entiers relatifs a, b et c.
Si a **divise** b et c, alors a **divise** $b + c$; $b - c$ ou toute **combinaison linéaire** de b et de c : $\alpha b + \beta c$, où α et β sont deux entiers relatifs.

PREUVE On sait que a divise b et c, donc il existe deux entiers relatifs k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a.$$

On a alors : $b + c = (k + k')a$; $b - c = (k - k')a$ et $\alpha b + \beta c = (\alpha k + \beta k')a$.

Donc a divise $b + c$; $b - c$ et $\alpha b + \beta c$.

Exemple k étant un entier naturel, on pose $a = 9k + 2$ et $b = 12k + 1$.
Pour déterminer une condition sur les diviseurs positifs communs à a et b, on cherche à éliminer k par une combinaison linéaire. La combinaison linéaire qui permet d'éliminer k consiste à trouver le plus petit multiple commun à 9 et 12, soit 36.
Soit d un diviseur commun à a et b.
Comme d divise a et b, il divise aussi $c = 4a - 3b$, soit

$$c = 4(9k + 2) - 3(12k + 1) = 36k + 8 - 36k - 3 = 5.$$

Donc d doit diviser 5. Comme 5 n'a que deux diviseurs positifs 1 et 5, les diviseurs positifs communs à a et b sont à chercher dans $\{1 ; 5\}$.

3. La division euclidienne

DÉFINITION ET THÉORÈME

Soit a un entier relatif et b un entier naturel non nul.
On appelle **division euclidienne** de a par b, l'opération qui, au couple $(a ; b)$, associe l'unique couple $(q ; r)$ tel que :

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

a s'appelle le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

PREUVE L'existence et l'unicité du couple $(q ; r)$ sont à démontrer : exercice 19, p. 16.

Exemples
1) La division euclidienne de 114 par 8 correspond à : $114 = 8 \times 14 + 2$.
   Ainsi $q = 14$ et $r = 2$.
2) Pour avoir un reste positif dans la division euclidienne de -114 par 8, on écrit : $-2 = 6 - 8$.
   On obtient alors : $-114 = 8 \times (-14) - 2 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6$.
   Ainsi $q = -15$ et $r = 6$.

REMARQUES :
- Le reste est toujours un entier naturel inférieur au diviseur. Par conséquent, dans la division par 7, par exemple, il existe 7 restes possibles : 0, 1, 2, 3, 4, 5, 6.
- On peut schématiser la division euclidienne comme on pose une division : $\begin{array}{c|c} a & b \\ \hline r & q \end{array}$

  Ainsi, en reprenant l'exemple de la division de 114 par 8, on a : $\begin{array}{c|c} 114 & 8 \\ \hline \mathbf{2} & \mathbf{14} \end{array}$

MÉTHODE 2 Utiliser la définition de la division euclidienne

► Ex. 20 p. 17

Exercice d'application Trouver tous les entiers dont le quotient dans la division euclidienne par 5 donne un quotient égal à 3 fois le reste.

Correction Soit a un entier qui vérifie la condition de l'énoncé. On divise a par 5, on a alors : $a = 5q + r$ avec $0 \leqslant r < 5$.
Comme $q = 3r$, on a : $a = 15r + r = 16r$ avec $0 \leqslant r < 5$.

On trouve toutes les valeurs de a en faisant varier r de 0 à 4 compris, on a alors l'ensemble solution : $S = \{0\ ;\ 16\ ;\ 32\ ;\ 48\ ;\ 64\}$.

Exercice d'application Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise $2a$ par b, le reste est 5. Déterminer le diviseur b.

Correction Écrivons chacune des deux divisions euclidiennes, en notant q et q' les quotients respectifs :

$$\begin{cases} a = bq + 8 \quad \text{avec} \quad b > 8 \\ 2a = bq' + 5 \quad \text{avec} \quad b > 5 \end{cases}$$

En multipliant la première division par 2 et en égalisant avec la deuxième, on obtient :

$$\begin{aligned} 2bq + 16 &= bq' + 5 \quad \text{avec} \quad b > 8 \\ b(2q - q') &= -11 \\ b(q' - 2q) &= 11 \end{aligned}$$

b est donc un multiple positif non nul de 11, supérieur à 8, donc : $b = 11$.

4. Congruence

A. Entiers congrus à n

DÉFINITION

Soit n un entier naturel ($n \geqslant 2$), a et b deux entiers relatifs.
On dit que deux entiers a et b sont **congrus modulo n** si, et seulement si, a et b ont le même reste dans la division euclidienne par n. On note alors :

$$a \equiv b \mod n \quad \text{ou} \quad a \equiv b\ (n) \quad \text{ou} \quad a \equiv b\ [n].$$

Exemples

1) $57 \equiv 15\ (7)$ car : $57 = 7 \times 8 + \mathbf{1}$ et $15 = 7 \times 2 + \mathbf{1}$
$41 \equiv -4\ (9)$ car : $41 = 9 \times 4 + \mathbf{5}$ et $-4 = 9 \times (-1) + \mathbf{5}$
2) Un nombre est congru à son reste modulo n dans la division euclidienne par n.
$2\,008 \equiv 8\ (10)$ car $2\,008 = 10 \times 200 + 8$; $17 \equiv 1\ (4)$; $75 \equiv 3\ (9)$.
3) Si $x \equiv 0\ (2)$, alors x est pair.
Si $x \equiv 1\ (2)$, x est impair.

PROPRIÉTÉS

- $a \equiv 0\ (n) \quad \Leftrightarrow \quad a$ est un multiple de n ou n est un diviseur de a.
- La congruence est une relation d'équivalence, c'est-à-dire, pour tous entiers a, b, c, on a :
  1) $a \equiv a\ (n)$ **(réflexivité)**
  2) Si $a \equiv b\ (n)$, alors $b \equiv a\ (n)$ **(symétrie)**
  3) Si $a \equiv b\ (n)$ et si $b \equiv c\ (n)$, alors $a \equiv c\ (n)$ **(transitivité)**

REMARQUE : La démonstration est laissée à l'initiative de l'élève.

THÉORÈME

Soit n un entier naturel ($n \geqslant 2$), a et b deux entiers relatifs.

$$a \equiv b\ (n) \quad \Leftrightarrow \quad a - b \equiv 0\ (n)$$

PREUVE Comme il s'agit d'une équivalence, il faut démontrer la propriété dans les deux sens.

- *Dans le sens direct* : On sait que $a \equiv b\ (n)$. Il existe donc des entiers q, q' et r tels que :

$$a = nq + r \quad \text{et} \quad b = nq' + r \quad \text{avec} \quad 0 \leqslant r < n.$$

  On obtient : $a - b = n(q - q')$.

  $a-b$ est alors un multiple de n, et son reste dans la division par n est nul, d'où : $a - b \equiv 0\ (n)$.

- *Réciproquement* : On sait que $a - b \equiv 0\ (n)$. Il existe k tel que : $a - b = kn \quad (1)$.

  Si l'on effectue la division de a par n, on a : $a = nq + r \quad$ avec $0 \leqslant r < n \quad (2)$.

  De (1) et (2), on obtient :

$$\begin{aligned} nq + r - b &= kn \\ -b &= kn - nq - r \\ b &= (q-k)n + r \end{aligned}$$

  a et b ont le même reste dans la division par n, donc : $a \equiv b\ (n)$.

B. Compatibilité de la congruence avec l'addition et la multiplication

THÉORÈME

Soit n un entier naturel $(n \geqslant 2)$ et a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b\ (n) \quad \text{et} \quad c \equiv d\ (n).$$

La relation de congruence est compatible :

1) avec l'addition : $a + c \equiv b + d\ (n)$
2) avec la multiplication : $ac \equiv bd\ (n)$
3) avec les puissances : pour tout entier naturel k, $\quad a^k \equiv b^k\ (n)$

PREUVE

1) **Compatibilité avec l'addition**

On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a-b)$ et $(c-d)$ sont des multiples de n.
Il existe donc deux entiers relatifs k et k' tels que : $a-b = kn$ et $c-d = k'n$.
En additionnant ces deux égalités, on obtient :

$$a-b+c-d = kn+k'n \quad \Leftrightarrow \quad (a+c)-(b+d) = (k+k')n.$$

Donc $(a+c)-(b-d)$ est un multiple de n, d'où : $a+c \equiv b+d\ (n)$.

2) **Compatibilité avec la multiplication**

On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe deux entiers relatifs k et k' tels que : $a = b+kn$ et $c = d+k'n$.
En multipliant ces deux égalités, on obtient :

$$\begin{aligned}
ac &= (b+kn)(d+k'n) \\
ac &= bd+k'bn+kdn+kk'n^2 \\
ac &= bd+(k'b+kd+kk'n)n \\
ac-bd &= (k'b+kd+kk'n)n
\end{aligned}$$

Donc $(ac-bd)$ est un multiple de n, d'où : $ac \equiv bd\ (n)$.

3) La compatibilité avec les puissances est à prouver dans l'exercice **24**, p. 17.

MÉTHODE 3 Déterminer un reste dans une division euclidienne

► Ex. 26 p. 17

Exercice d'application Déterminer les restes dans la division euclidienne par 7 des nombres :

1) 50^{100} 2) 100 3) 100^3 4) $50^{100}+100^{100}$

Correction

1) On a $50 \equiv 1\ (7)$ car $50 = 7 \times 7 + 1$.
D'après la compatibilité avec les puissances, on a : $50^{100} \equiv 1^{100} \equiv 1\ (7)$.
Le reste est 1.

2) $100 = 50 \times 2$, comme $50 \equiv 1\ (7)$, d'après la compatibilité avec la multiplication, on a : $100 \equiv 2\ (7)$. Le reste est 2.

3) Comme $100 \equiv 2\ (7)$, d'après la compatibilité avec les puissances, on a :
$100^3 \equiv 2^3 \equiv 8 \equiv 1\ (7)$. Le reste est 1.

4) $100^{100} = 100^{3\times 33+1} = \left(100^3\right)^{33} \times 100$, donc d'après la compatibilité avec les puissances et la multiplication, on a : $100^{100} \equiv 1^{33} \times 2 \equiv 2\ (7)$.
D'après la compatibilité avec l'addition, on a alors : $50^{100}+100^{100} \equiv 1+2 \equiv 3\ (7)$.
Le reste est 3.

REMARQUE : La notion de congruence prend ici tout son intérêt. Par exemple, bien que l'on ne puisse calculer $50^{100}+100^{100}$, on peut connaître son reste dans la division par 7 de façon simple et rapide.

MÉTHODE 4 Démontrer qu'un nombre est divisible par un autre nombre

► Ex. 29 p. 17

Exercice d'application Montrer que : $\forall n \in \mathbb{N}, \quad 3^{n+3} - 4^{4n+2}$ est divisible par 11.

Correction On a : $3^{n+3} = 3^n \times 3^3 = 27 \times 3^n$.
Or $27 \equiv 5\ (11)$, donc d'après la compatibilité avec la multiplication, on a :

$$\forall n \in \mathbb{N}, \quad 3^{n+3} \equiv 5 \times 3^n\ (11)$$

On a : $4^{4n+2} = \left(4^4\right)^n \times 4^2$, or $4^2 \equiv 5\ (11)$ donc $4^4 \equiv 5^2 \equiv 3\ (11)$, donc :

$$\forall n \in \mathbb{N}, \quad 4^{4n+2} \equiv 3^n \times 5\ (11)$$

On en déduit donc que :

$$3^{n+3} - 4^{4n+2} \equiv 0\ (11)$$

La proposition est donc vérifiée pour tout entier naturel n.

MÉTHODE 5 Construire un tableau de congruence

► Ex. 31 p. 17

Un tableau de congruence est un tableau permettant de présenter des résultats de manière exhaustive en se référant aux restes possibles dans une division euclidienne.

Exercice d'application

1) Déterminer suivant les valeurs de l'entier relatif n, le reste de la division de n^2 par 7.
2) En déduire alors les solutions de l'équation $x^2 \equiv 2\ (7)$.

Correction

1) On détermine les restes suivant une méthode exhaustive, c'est-à-dire on détermine les restes de n^2 à partir de chaque reste possible de la division de n par 7.
   On peut construire un tableau de congruence pour présenter les résultats :

Reste de la division de n par 7	0	1	2	3	4	5	6
Reste de la division de n^2 par 7	0	1	4	2	2	4	1

   Par exemple si $n \equiv 3\ (7)$, alors $n^2 \equiv 9 \equiv 2\ (7)$.
   Les restes possibles de n^2 par 7 sont donc : 0, 1, 2 et 4.
2) Pour résoudre $x^2 \equiv 2\ (7)$, on recherche dans le tableau les valeurs de n pour lesquelles on obtient un reste de 2 quand n est au carré. Il est obtenu pour les restes 3 et 4 dans la division de n par 7.
   Les solutions de l'équation sont donc : $x \equiv 3\ (7)$ et $x \equiv 4\ (7)$.

Activités mentales

1 Dresser la listes des diviseurs de : 150, 230 et 810.

2 À quelle condition un nombre est-il divisible par 6 ? À l'aide d'une factorisation, montrer que $a(a^2-1)$ est divisible par 6 pour tout entier relatif a.

3 Soit k un entier naturel. On pose $a = 5k+4$ et $b = 3k+1$.

1) Montrer que, si d est un diviseur commun à a et b, alors d divise 7.
2) Dans quel ensemble les valeurs de d sont-elles à rechercher ?

4 Dans chaque cas, écrire la division euclidienne de a par b.

1) $a = 193$ et $b = 16$.
2) $a = 18$ et $b = 50$.
3) $a = -20$ et $b = 7$.
4) $a = -354$ et $b = 17$.

5 Dans la division euclidienne de deux entiers naturels, le dividende est 63 et le reste 17. Donner toutes les valeurs possibles du quotient et du diviseur.

6 Dans une division euclidienne, le quotient d'un entier relatif x par 3 est 7. Quels sont les restes possibles ? En déduire toutes les valeurs de x.

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

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

9 Pour chaque valeur de a donnée, trouver un entier relatif x tel que : $a \equiv x \pmod 9$ et $-4 \leqslant x < 5$.

1) $a = 11$
2) $a = 24$
3) $a = 62$
4) $a = 85$
5) $a = -12$
6) $a = 32$

10 Trouver les restes de la division euclidienne par 11 des nombres suivants : 12^{15} ; 78^{15} ; 10^7.

11 Montrer que $2^5 \equiv -1$ (11). Quels sont alors les restes de la division par 11 de 13^{12} et $(-2)^{19}$?

12 Démontrer que pour tout naturel n, $6^n - 1$ est divisible par 5.

Multiples et diviseurs

13 ► MÉTHODE 1 p. 10
Déterminer les couples $(x;y)$ d'entiers naturels qui vérifient :

1) $x^2 = y^2 + 21$.
2) $x^2 - 7xy = 17$.

14 Déterminer les entiers relatifs n qui vérifient :

1) $n^2 + n = 20$.
2) $n^2 + 2n = 35$.

15 Déterminer les entiers relatifs n tel que :

1) $n+3$ divise $n+10$.
2) $n+1$ divise $3n-4$.

16 L'exercice consiste à trouver les valeurs du naturel $n > 4$ pour lesquelles la fraction $\dfrac{n+17}{n-4}$ est un entier.

1) Démontrer que $n-4$ divise $n+17$ équivaut à $n-4$ divise 21.
2) Déterminer alors toutes les valeurs de n correspondant au problème.

17 Soit l'équation (E) : $xy - 5x - 5y - 7 = 0$.

1) Montrer que :
   $xy - 5x - 5y - 7 = 0 \iff (x-5)(y-5) = 32$.
2) Déterminer les couples d'entiers naturels $(x;y)$ qui vérifient (E).

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

Division euclidienne

19 Le but de cet exercice est de montrer la validité de la définition de la division euclidienne.

1) Démontrer le **lemme d'Archimède** :
   soit deux entiers naturels a et b $(b \neq 0)$, alors il existe un entier naturel n tel que : $nb > a$.
2) **Existence** d'un couple $(q;r)$ tel que :
   $a = bq + r$ avec $0 \leqslant r < b$.
   Soit S l'ensemble des entiers s tels que : $bs > a$.
   a) Montrer que S admet un plus petit élément t.
   b) En déduire alors qu'il existe un entier q tel que : $bq \leqslant a < b(q+1)$.
3) **Unicité** du couple (q,r).
   On suppose qu'il existe deux couples $(q\,;r)$ et $(q'\,;r')$ tels que : $a=bq+r=bq'+r'$ avec
   $0 \leqslant r<b$ et $0 \leqslant r'<b'$.
   Montrer alors que nécessairement $q = q'$ et $r = r'$.

20 ► MÉTHODE 2 p. 12

Trouver les entiers naturels n qui, dans la division euclidienne par 4, donnent un quotient égal au reste.

21 Trouver un entier naturel qui, dans la division euclidienne par 23, a pour reste 1 et, dans la division euclidienne par 17, a le même quotient et pour reste 13.

22 On divise un entier naturel n par 152, puis par 147. Les quotients sont égaux et les restes respectifs sont 13 et 98. Quel est cet entier naturel n ?

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

Congruence

24 Soit un entier naturel $n \geqslant 2$ et a, b des entiers relatifs vérifiant : $a \equiv b\ (n)$.

Démontrer, en vous appuyant sur les preuves du théorème de compatibilité, que : $\forall\, k \in \mathbb{N}, \quad a^k \equiv b^k\ (n)$.

25 Résoudre dans $\mathbb{Z}$ les systèmes suivants :

1) $\begin{cases} x \equiv -2\ (5) \\ x > 0 \end{cases}$ **2)** $\begin{cases} x + 2 \equiv -1\ (7) \\ 100 \leqslant x < 125 \end{cases}$

26 ► MÉTHODE 3 p. 14

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

27 Vérifier que $2^4 \equiv -1\ (17)$ et $6^2 \equiv 2\ (17)$.

Quel est le reste de la division par 17 des nombres $1\,532^{20}$ et 346^{12} ?

28 Vérifier que 999 est divisible par 27, puis que $10^{3n} \equiv 1\ (27)$, avec $n \in \mathbb{N}$.

Quel est alors le reste dans la division de $10^{100} + 100^{10}$ par 27 ?

29 ► MÉTHODE 4 p. 15

Démontrer que pour tout entier naturel k, on a :

$5^{4k} - 1$ divisible par 13.

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

31 ► MÉTHODE 5 p. 15

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

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

32 Démontrer que pour tout entier n, n^2 est congru soit à 0, soit à 1, soit à 4, modulo 8.

Résoudre alors dans $\mathbb{Z}$ l'équation :

$(n+3)^2 - 1 \equiv 0\ (8)$.

33 Déterminer les restes de la division euclidienne de 5^n par 11 suivant les valeurs de n. On donnera les résultats sous forme d'un tableau.

34

1) Compléter cette table des restes dans la congruence modulo 4.

$x \equiv$	0	1	2	3
$x^2 \equiv$				

2) Prouver que l'équation $7x^2 - 4y^2 = 1$, d'inconnues x et y entiers relatifs, n'a pas de solution.

3) Résoudre dans $\mathbb{Z}$ l'équation $(x+3)^2 \equiv 1 \pmod 4$.

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

36

1) Déterminer l'ensemble E_1, des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 7.

2) Déterminer l'ensemble E_2 des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 3.

3) k est un entier relatif.

Vérifier que si, $x = 1 + 21k$ ou $x = -2 + 21k$, alors $n = x^2 + x - 2$ est divisible par 42.

37 Déterminer le reste dans la division euclidienne de $11^{2\,011}$ par 7.

38 Soit n un entier naturel, on sépare son nombre de dizaines a et le chiffre des unités b. On a alors : $n = 10\,a + b$.

1) Prouver que n est divisible par 17 si, et seulement si, $a - 5b$ est divisible par 17.

2) Montrer par ce procédé (que l'on peut réitérer) que les nombres : 816 et 16 983 sont divisibles par 17.

39 On pose $A_n = n^5 - n$, $n \in \mathbb{N}$.

1) Montrer que A_n est pair.

2) Montrer que A_n est divisible par 3.

3) En utilisant les congruences modulo 5, démontrer que A_n est divisible par 5.

4) Pourquoi A_n est-il divisible par 30 ?

40 **D'après Bac (Antilles Guyane - 2011)**

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 $x^2 \equiv 2y^2 \pmod 5$.

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

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

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

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

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

41 **D'après Bac (Nouvelle-Calédonie - 2009)**

On considère l'équation notée (G) :

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

1) Montrer que $100 \equiv 2$ (modulo 7).

Démontrer que si $(x ; y)$ est solution de (G) alors $3x^2 \equiv 2^n$ (modulo 7).

2) Reproduire et compléter le tableau suivant :

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

3) Démontrer que 2^n est congru à 1, 2 ou 4 modulo 7.

En déduire que l'équation (G) n'admet pas de solution.

42 **D'après Bac (Polynésie - 2014)** ALGO

Dans cet exercice, on appelle numéro du jour de naissance j le rang de ce jour dans le mois et numéro du mois de naissance m, le rang du mois dans l'année.

Par exemple, pour une personne née le 14 mai, alors $j = 14$ et $m = 5$.

Partie A

Lors d'une représentation, un magicien demande aux spectateurs d'effectuer le programme de calcul (A) suivant :

« Prenez le numéro de votre jour de naissance et multipliez-le par 12. Prenez le numéro de votre mois de naissance et multipliez-le par 37. Ajoutez les deux nombres obtenus. Je pourrai alors vous donner la date de votre anniversaire »

Un spectateur annonce 308 et en quelques secondes, le magicien déclare : « Votre anniversaire tombe le 1er août ! ».

1) Vérifier que pour une personne née le 1er août, le programme de calcul (A) donne effectivement le nombre 308.

2) **a)** Pour un spectateur donné, on note z le résultat obtenu en appliquant le programme de calcul (A). Exprimer z en fonction de j et de m et démontrer que $z \equiv m$ (12).

b) Retrouver alors la date de l'anniversaire d'un spectateur ayant obtenu le nombre 455 en appliquant le programme de calcul (A).

Partie B

Lors d'une autre représentation, le magicien décide de changer son programme de calcul. Pour un spectateur dont le numéro du jour de naissance est j et le numéro du mois de naissance est m, le magicien demande de calculer le nombre z défini par $z = 12j + 31m$.

On considère l'algorithme ci-dessous :

```
Liste des variables utilisées
  j, m, z : entiers
Traitement et affichage
  Pour m variant de ... à ... faire
    Pour j variant de ... à ... faire
      Donner à z la valeur de 12j + 31m
      Si ... Alors
        Afficher la valeur de j, m
      Fin Si
    Fin Pour
  Fin Pour
```

1) Compléter cet algorithme afin qu'il affiche toutes les valeurs de j et de m telles que :

$$12j + 31m = 503.$$

2) Quelle est alors la date d'anniversaire correspondante ?

43 **D'après Bac (Antilles-Guyane - 2012)** ALGO

On considère l'algorithme suivant où Ent$\left(\dfrac{A}{N}\right)$ désigne la partie entière de $\dfrac{A}{N}$.

> *Liste des variables utilisées*
> A, N : *entiers*
> *Entrées*
>   Donner à N la valeur de 1
> *Traitements et affichage*
>   **Tant que** ($N \leqslant \sqrt{A}$) **faire**
>   **Si** $\dfrac{A}{N} = \text{Ent}\left(\dfrac{A}{N}\right)$ **Alors**
>   Afficher la valeur de N et $\dfrac{A}{N}$
>   **Fin Si**
>   **Fin Tant que**

Quels résultats affiche cet algorithme pour $A = 12$?
Que donne cet algorithme dans le cas général ?

44 **D'après Bac (Liban - 2009)**

Le but de l'exercice est de montrer qu'il existe un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009\ (10\,000)$.

Partie A

1) Déterminer le reste de la division euclidienne de $2\,009^2$ par 16.
2) En déduire que $2\,009^{8\,001} \equiv 2009\ (16)$.

Partie B

On considère la suite (u_n) définie sur $\mathbb{N}$ par :
$u_0 = 2\,009^2 - 1$ et $\forall n \in \mathbb{N},\ u_{n+1} = (u_n + 1)^5 - 1$.

1) a) Démontrer que u_0 est divisible par 5.
   b) On rappelle le binôme de Newton à l'ordre 5 :
   $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$
   Démontrer que pour tout entier naturel n,
   $$u_{n+1} = u_n\left[u_n^4 + 5\left(u_n^3 + 2u_n^2 + 2u_n + 1\right)\right]$$
   c) Démontrer par récurrence que, $\forall n \in \mathbb{N}$, u_n est divisible par 5^{n+1}.
2) a) Vérifier que $u_3 = 2\,009^{250} - 1$ puis en déduire que $2\,009^{250} \equiv 1\ (625)$.
   b) Démontrer alors que $2\,009^{8\,001} \equiv 2\,009\ (625)$.

Partie C

On admet que l'on peut montrer que $2\,009^{8\,001} - 2\,009$ est divisible par $10\,000$.

Conclure, c'est-à-dire déterminer un entier naturel dont l'écriture décimale du cube se termine par 2 009.

45 **D'après Bac (Asie - 2004)**

On appelle (E) l'ensemble des entiers naturels qui peuvent s'écrire sous la forme $9 + a^2$ où a est un entier naturel non nul ;
par exemple : $10 = 9 + 1^2$, $13 = 9 + 2^2$, etc.
On se propose dans cet exercice d'étudier l'existence d'éléments de (E) qui sont des puissances de 2, 3 ou 5.

1) Étude de l'équation d'inconnue a : $a^2 + 9 = 2^n$ où $a \in \mathbb{N}$, et $n \geqslant 4$.
   a) Montrer que si a existe, a est impair.
   b) En raisonnant modulo 4, montrer que l'équation proposée n'a pas de solution.
2) Étude de l'équation d'inconnue a : $a^2 + 9 = 3^n$ où $a \in \mathbb{N}$, et $n \geqslant 3$.
   a) Montrer que si $n \geqslant 3$, 3^n est congru à 1 ou à 3 modulo 4.
   b) Montrer que si a existe, il est pair et en déduire que nécessairement n est pair.
   c) On pose $n = 2p$ où p est un entier naturel, avec $p \geqslant 2$. Déduire d'une factorisation de $3^n - a^2$, que l'équation proposée n'a pas de solution.
3) Étude de l'équation d'inconnue a : $a^2 + 9 = 5^n$ où $a \in \mathbb{N}$, et $n \geqslant 2$.
   a) En raisonnant modulo 3, montrer que l'équation est impossible si n est impair.
   b) On pose $n = 2p$, en s'inspirant de 2) c) démontrer qu'il existe un unique entier naturel a tel que $a^2 + 9$ soit une puissance entière de 5.

46 **D'après Bac (Polynésie - 2006)**

Pour chacune des trois propositions suivantes, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie.

- **Proposition 1** : « Pour tout entier naturel n, 3 divise le nombre $2^{2n} - 1$ ».
- **Proposition 2** : « Si un entier relatif x est solution de l'équation $x^2 + x \equiv 0\ (6)$, alors $x \equiv 0\ (3)$ ».
- Deux entiers naturels M et N sont tels que M a pour écriture abc en base dix et N a pour écriture bca en base dix.
  Proposition 3 : « Si l'entier M est divisible par 27 alors l'entier $M - N$ est aussi divisible par 27. »

47 **Congruences**

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

1) Étudier la parité de l'entier $A(n)$.
2) Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.
3) Montrer que, pour tout entier d diviseur de $A(n)$: $n^8 \equiv 1\ (d)$.

48 **Vrai-Faux**

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

- **Proposition 1 :** Le reste de la division euclidienne de 2011^{2011} par 7 est 2.
- **Proposition 2 :** 11^{2011} est congru à 4 modulo 7.
- **Proposition 3 :** « $x^2 + x + 3 \equiv 0$ (modulo 5) si, et seulement si, $x \equiv 1$ (modulo 5). »

49 **Le phare des baleines**

À la pointe ouest de l'île de Ré se situe le grand phare des baleines. L'escalier qui mène au sommet a un nombre de marches compris entre 246 et 260.
Ted et Laure sont deux sportifs. Laure qui est plus jeune monte les marches 4 par 4 et à la fin il lui reste 1 marche. Ted, lui, monte les marches 3 par 3 et à la fin il lui reste 2 marches.
Combien l'escalier compte-t-il de marches ?

50 **Bouteilles**

Un super marché reçoit une livraison de bouteilles. Si l'on compte les bouteilles par 3, 5 ou 7, il en reste toujours 2.
Sachant que le nombre de bouteilles est compris entre 1500 et 1600, combien de bouteilles le supermarché a-t-il reçues ?

51 **Critères de divisibilité usuels**

1) a) Énoncer un critère de divisibilité par 3 et par 9.
   b) Énoncer un critère de divisibilité par 4.
2) Soit un entier $N = \overline{a_n a_{n-1} \dots a_1 a_0}$ dans notre système de notation. On a donc : $N = \sum_{i=0}^{n} 10^i a_i$.
   a) Montrer que : $\forall n \in \mathbb{N},\ 10^n \equiv 1$ modulo 3 et modulo 9.
   b) Démontrer le critère de divisibilité par 3 et par 9.
   c) Montrer que : $10^2 \equiv 0\ \ (4)$.
   Démontrer alors le critère de divisibilité par 4.
3) En observant les nombres 297, 880 et 242, un élève a formulé la conjecture :
   « tout nombre à trois chiffres dans lequel le chiffre des dizaines est la somme du chiffre des centaines et du chiffre des unités est divisible par 11 ».
   a) Cette conjecture s'applique-t-elle au nombre 473 ?
   b) Démontrer cette conjecture en prenant un nombre de 3 chiffres $N = \overline{abc}$.
   c) La réciproque est-elle vraie ?
4) D'une manière générale, un entier naturel N est divisible par 11 si, et seulement si, la somme des chiffres de rang impair diminuée de la somme des chiffres de rang pair est divisible par 11.
   Exemples :
   6 **4**5**7** est divisible par 11 car $(7+4) - (5+6) = 0$.
   1**9** 3**4**6 **7**0**1** est divisible par 11 car
   $(1+7+4+9) - (0+6+3+1) = 11$.
   98**7** 6**5**4 **3**2**1** n'est pas divisible par 11 car
   $(1+3+5+7+9) - (2+4+6+8) = 5$.
   a) Soit les nombres entiers naturels de quatre chiffres différents écrits avec les chiffres 2, 5, 6 et 9. Parmi ces nombres déterminer tous les nombres qui sont divisibles par 11.
   b) Montrer que : $\forall n \in \mathbb{N},\ 10^n \equiv -1\ \ (11)$.
   Démontrer ce critère de divisibilité par 11 en posant : $N = \overline{a_n a_{n-1} \dots a_1 a_0}$.

52 **Critères de divisibilité par 7 et 13**

Soit un entier naturel n. On décompose n de la façon suivante : $n = 10a + b$ avec $0 \leqslant b \leqslant 9$. Les coefficients a et b correspondent respectivement au nombre de dizaines et au chiffre des unités de l'entier n.

1) **Divisibilité par 7**
   a) Établir la liste des multiples de 7 inférieurs à 100 dans $\mathbb{N}$.
   b) Montrer que n est divisible par 7 si, et seulement si, $a - 2b$ est divisible par 7.
   c) En déduire, sans utiliser une calculatrice, les multiples de 7 parmi les entiers suivants :
   574 ; 827 ; 3 906 ; 31 729 ; 172 011.
   Aide : penser à réitérer le processus si nécessaire.
2) **Divisibilité par 13**
   a) Établir la liste des multiples de 13 inférieurs à 100 dans $\mathbb{N}$.
   b) Montrer que n est divisible par 13 si, et seulement si, $a + 4b$ est divisible par 13.
   c) En déduire, sans utiliser une calculatrice, les multiples de 13 parmi les entiers suivants :
   676 ; 943 ; 4 652 ; 156 556.
   Aide : penser à réitérer le processus si nécessaire.

53 Deux méthodes pour trouver un reste

1) a) Déterminer, suivant les valeurs de l'entier naturel non nul n, le reste dans la division euclidienne par 9 de 7^n.
   b) Démontrer alors que $(2\,005)^{2\,005} \equiv 7\ (9)$.
2) a) Démontrer que pour tout entier naturel n non nul : $(10)^n \equiv 1\ (9)$.
   b) On désigne par N un entier naturel écrit en base dix, on appelle S la somme de ses chiffres.
   Démontrer la relation suivante : $N \equiv S\ (9)$.
   c) En déduire que N est divisible par 9 si, et seulement si, S est divisible par 9.
3) On suppose que $A = (2\,005)^{2\,005}$.
   On désigne par :
   - B la somme des chiffres de A ;
   - C la somme des chiffres de B ;
   - D la somme des chiffres de C.

   a) Démontrer la relation suivante : $A \equiv D\ (9)$.
   b) Sachant que $2\,005 < 10\,000$, démontrer que A s'écrit en numération décimale avec au plus 8 020 chiffres. En déduire que $B \leqslant 72\,180$.
   c) Démontrer que $C \leqslant 45$.
   d) En étudiant la liste des entiers inférieurs à 45, déterminer un majorant de D plus petit que 15.
   e) Démontrer que $D = 7$.

54 Suite et terminaison

On considère la suite (u_n) d'entiers définie par :

$$\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6 \end{cases}$$

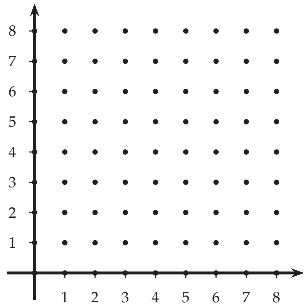
1) Calculer u_1, u_2, u_3 et u_4.
   Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?
2) Montrer que, $\forall n \in \mathbb{N},\ u_{n+2} \equiv u_n\ (4)$.
   En déduire que :
   $\forall k \in \mathbb{N},\ u_{2k} \equiv 2\ (4)$ et $u_{2k+1} \equiv 0\ (4)$.
3) a) Montrer par récurrence que, pour tout entier naturel n, $2u_n = 5^{n+2} + 3$.
   b) En déduire que, pour tout entier naturel n, $2u_n \equiv 28\ (100)$.
4) Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

55 Réseau

Soit a et b deux entiers naturels non nuls. On appelle « réseau » associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthogonal, dont les coordonnées $(x ; y)$ sont des entiers vérifiant les conditions : $0 \leqslant x \leqslant a$ et $0 \leqslant y \leqslant b$. On note $R_{a,b}$ ce réseau.
Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriétés géométriques des points correspondants du réseau.

Les réponses sont attendues sans explication, et seront données sous la forme d'un graphique pour chaque cas.

Représenter graphiquement les points $M(x ; y)$ du réseau $R_{8,8}$ vérifiant :
1) $x \equiv 2$ (3) et $y \equiv 1$ (3) sur un premier graphique.
2) $x + y \equiv 1$ (3) sur un deuxième graphique.
3) $x \equiv y$ (3) sur un troisième graphique.



Je teste mes connaissances

À la fin de ce chapitre, je dois être capable de :

- Trouver tous les diviseurs d'un entier
- Résoudre une équation grâce à la divisibilité
- Utiliser les propriétés des diviseurs
- Déterminer un quotient et un reste dans une division euclidienne
- Appliquer les propriétés de la congruence pour déterminer un reste ou simplifier une équation

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Déterminer la réponse exacte.

56 Le nombre de diviseurs positifs de 700 est :

(a) 16 (b) 18 (c) 20 (d) 22

57 Le nombre de couples d'entiers naturels vérifiant l'équation $5x^2 - 7xy = 17$ est :

(a) 0 (b) 2 (c) 1 (d) 4

58 Il existe un entier k pour lequel $9k + 2$ et $7k + 3$ ont pour diviseur commun d tel que :

(a) $d = 13$ (b) $d = 2$ (c) $d = 3$ (d) $d = 6$

On donne : $17\,648 = 17 \times 1\,037 + 19$.

59 Le reste de la division euclidienne de 17 648 par 17 est :

(a) 19 (b) 2 (c) 17 (d) 1 037

60 Le quotient de la division de 17 648 par 1 037 est :

(a) 19 (b) 18 (c) 17 (d) 2

61 Le reste de la division de $-17\,648$ par 17 est :

(a) 2 (b) 19 (c) -2 (d) 15

62 L'ensemble des solutions de l'équation $3x \equiv 6\ (9)$ est :

(a) $x \equiv 2\ (9)$ (b) $x \equiv 5\ (9)$ (c) $x \equiv 8\ (9)$ (d) $x \equiv 2\ (3)$

63 Le reste de la division de $2\,016^{2\,016}$ par 5 est :

(a) 1 (b) 2 (c) 3 (d) 4

64 Le reste de la division de $2\,015^{2\,015}$ par 7 est :

(a) 1 (b) 2 (c) 5 (d) 6

TP 1 Trouver les diviseurs d'un entier

ALGO

Pour trouver tous les diviseurs d'un entier $N \geqslant 2$, on commence par écrire dans deux colonnes 1 et N puis on teste si les nombres à partir de 2 sont diviseurs de N en s'arrêtant lorsque le nombre de la colonne de droite est plus petit que celui la colonne de gauche.

1) On cherche tous les diviseurs de 120.
Compléter le tableau ci-contre :

Diviseur d	Quotient k
1	120
2	60

2) Que doit vérifier le dernier nombre de la colonne de gauche ?

3) On cherche à automatiser la recherche des diviseurs de N. La colonne de gauche se termine lorsque le diviseur d est supérieur à $\sqrt{N}$.

```
1.  Liste des variables utilisées
2.    N, K, I : entiers
3.    L1, L2 : listes
4.  Entrées
5.    Saisir N
6.    Donner à K la valeur de 0
7.    Donner à I la valeur de 1
8.  Traitements
9.    Tant que (......) faire
10.     Si ...... Alors
11.       Donner à K la valeur de K + 1
12.       Donner à L1(K) la valeur de I
13.       Donner à L2(K) la valeur de ......
14.     Fin Si
15.     Donner à I la valeur de I + 1
16.   Fin Tant que
17.   Pour I variant de 1 à K faire
18.     Donner à L1(K + I) la valeur de L2(K − I + 1)
19.   Fin Pour
20. Affichage
21.   Afficher la valeur de L1
```

a) Compléter les lignes 9, 10 et 13 de l'algorithme.

b) Quel est le rôle de la ligne 18 ?

c) Écrire cet algorithme sur AlgoBox et le tester avec les diviseurs de 120, 96 et 700.

TP 2 Division euclidienne

Pour faire comprendre la division d'un entier naturel par un entier naturel non nul à l'école primaire, on procède par soustractions successives, c'est-à-dire que, si l'on veut diviser 32 par 5, on soustrait 5 à 32 autant de fois que cela est possible.

$$32 - 5 = 27$$
$$27 - 5 = 22$$
$$22 - 5 = 17$$
$$17 - 5 = 12$$
$$12 - 5 = 7$$
$$7 - 5 = 2$$

On a ainsi enlevé 6 fois 5 et il reste 2, on peut donc écrire : $32 = 5 \times 6 + 2$.

1) Écrire un algorithme permettant de trouver le quotient q et le reste r de la division dans $\mathbb{N}$ de a par b ($b \neq 0$) par cette méthode. Tester cet algorithme pour les divisions suivantes : 32 par 5 ; 12 par 13 et 1 412 par 13.

2) Améliorer cet algorithme de façon à ce qu'il puisse trouver le quotient q et le reste r de la division d'un entier relatif a par un entier naturel b non nul. Tester cet algorithme pour la division -114 par 8.

TP 3 Notion de base

Notre système de numération est un système décimal de position. Il est constitué de 10 chiffres dont la position indique le nombre d'unités de la puissance de 10 correspondante.

$$3\,405 = 3 \times 10^3 + 4 \times 10^2 + 0 \times 10^1 + 5 \times 10^0$$

Dans un système de position en base b, on note un nombre N par $\overline{a_n a_{n-1} \dots a_1 a_0}^{\,b}$.
Ce nombre N s'écrit dans notre système décimal de position par :

$$N = \overline{a_n a_{n-1} \dots a_1 a_0}^{\,b} = a_n \times b^n + a_{n-1} \times b^{n-1} + \dots + a_1 \times b^1 + a_n \times b^0$$

$$\text{avec } i \in \{0, 1, \dots, n\},\ 0 \leqslant a_i < b.$$

En base b, il y a b chiffres : 0, 1, 2, ..., $b-1$.

1) Conversion de la base b vers la base 10

- En base 2, il n'y a que 2 chiffres : 0 et 1.
  $\overline{1011}^{\,2} = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$
  $= 8 + 0 + 2 + 1 = 11$
- En base 5, il y a 5 chiffres : 0, 1, 2, 3 et 4
  $\overline{231}^{\,5} = 2 \times 5^2 + 3 \times 5^1 + 1 \times 5^0$
  $= 50 + 15 + 1 = 66$

a) Convertir en base 10, le nombre écrit en base deux suivant : $\overline{10\,000\,111\,011}^{2}$.

b) Convertir en base 10, le nombre écrit en base 5 suivant : $\overline{4\,323}^{5}$.

c) Convertir en base 10, le nombre écrit en base 7 suivant : $\overline{31\,652}^{7}$.

d) En base 12, il y a 12 chiffres. On ajoute aux 10 chiffres de notre système décimal les chiffres $\alpha = 10$ et $\beta = 11$.
Convertir en base 10, les nombres écrits en base 12 suivants : $\overline{1\alpha 6}^{12}$ et $\overline{10\alpha\beta}^{12}$.

2) Conversion de la base 10 vers la base b

- Pour convertir l'écriture de 496 en base 7, on effectue les divisions euclidiennes suivantes :

$$\begin{array}{r|l} 496 & 7 \\ \hline 6 & 70 \end{array} \qquad \begin{array}{r|l} 70 & 7 \\ \hline 0 & 10 \end{array} \qquad \begin{array}{r|l} 10 & 7 \\ \hline 3 & 1 \end{array}$$

$$\text{donc } 496 = 1 \times 7^3 + 3 \times 7^2 + 0 \times 7^1 + 6 \times 7^0 = \overline{1\,306}^7$$

a) En prenant exemple sur la conversion de 496 dans le base 7, convertir le nombre 2 016 dans la base 2.

b) Convertir, par la même méthode, le nombre 68 425 dans la base 8.

c) Convertir, par la même méthode, le nombre 2 278 dans la base 12.

d) Démontrer que les divisions euclidiennes successives d'un nombre N, puis des quotients par la base b finissent par s'arrêter à partir d'un certain rang n.
Exprimer alors le nombre N dans la base b à l'aide des restes successifs $r_1, r_2, \ldots, r_n$.

3) Q représente l'écriture d'un nombre en base B et N l'écriture décimale.

a) Conversion dans le système décimal

Soit l'algorithme suivant :

1. *Liste des variables utilisées*
2. Q, B, N, I, R : *entiers*
3. *Entrées*
4. Saisir Q, B
5. Donner à N la valeur de 0
6. Donner à I la valeur de 0
7. *Traitements*
8. **Tant que** $(Q \neq 0)$ **faire**
9. Donner à R la valeur de $Q - 10 \times \mathrm{E}\left(\dfrac{Q}{10}\right)$
10. Donner à Q la valeur de $\mathrm{E}\left(\dfrac{Q}{10}\right)$
11. Donner à N la valeur de $N + R \times B^I$
12. Donner à $I + 1$ la valeur de I
13. **Fin Tant que**
14. *Affichage*
15. Afficher N

- Que fait-on aux lignes 8, 9 et 10 ?
- Que fait-on à la ligne 11 ?
- Rentrer ce programme dans la calculatrice : $Q = 2\,013$ et $B = 7$.
  Que renvoie le programme ? Vérifier ce résultat à la main.
- Pourquoi dans ce programme B ne peut être supérieur à 10 ?
- On cherche à améliorer cet algorithme pour qu'il puisse convertir un nombre dans une base supérieure à 10. Il faut alors rentrer les différents chiffres de Q dans une liste L_1 (10 pour α et 11 pour β). Modifier cet algorithme afin qu'il convertisse un nombre dans une base supérieure à 10.
  Tester cet algorithme en donnant la conversion de $\overline{\alpha\,\beta 29}^{12}$ dans notre système décimal. Vérifier ce résultat à la main.

b) Conversion en base B.

Soit l'algorithme suivant :

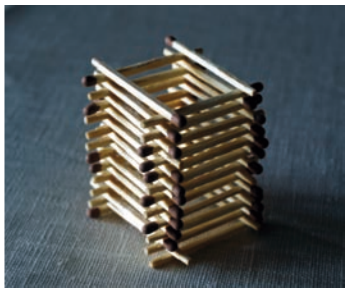
```
1.  Liste des variables utilisées
2.     Q, B, N, I, R : entiers
3.  Entrées
4.     Saisir N, B
5.     Donner à Q la valeur de 0
6.     Donner à I la valeur de 0
7.  Traitements
8.     Tant que (......) faire
9.        Donner à R la valeur de .........
10.       Donner à N la valeur de ......
11.       Donner à Q la valeur de .........
12.       Donner à I + 1 la valeur de I
13.    Fin Tant que
14. Affichage
15.    Afficher Q
```

- Compléter les lignes 8, 9, 10 et 11 de cet algorithme.
- Rentrer ce programme dans votre calculatrice. On saisit $N = 2013$ et $B = 5$. Que renvoie le programme ? Vérifier ce résultat à la main.

Récréation, énigmes

Jeu de Nim

On a disposé 40 allumettes sur un tapis.
Deux joueurs prennent chacun, à tour de rôle, une, deux trois ou quatre allumettes. Celui qui prend la dernière allumettes perd la partie.
Il existe une stratégie gagnante pour le joueur qui commence.
Exposer cette stratégie. Généraliser ensuite à un nombre n d'allumettes.



Pièces d'un puzzle

En rangeant les n pièces de son puzzle, Claudia constate que :

- si elle les range par groupe de 5, il lui reste 3 pièces ;
- si elle les range par groupe de 7, il lui reste 2 pièces ;
- si elle les range par groupe de 9, il lui reste 1 pièce ;
- et si elle les range par groupe de 11, il ne lui reste plus de pièce.

Combien ce puzzle contient de pièces sachant que ce nombre est inférieur à 2 000 ?
(On pourra étudier la quantité $2n - 11$.)

ARITHMÉTIQUE

2

PGCD. Théorèmes de Bézout et de Gauss

Connaissances nécessaires à ce chapitre

- Déterminer le PGCD de deux entiers
- Savoir reconnaître deux nombres premiers entre eux
- Connaître les congruences
- Trouver un couple d'entiers vérifiant l'équation : $ax + by = c$

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 « PGCD » signifie : « plus grand commun diviseur ».

1) Calculer le PGCD de 26 et 65, puis simplifier $\frac{26}{65}$.

2) Calculer le PGCD de 72 et 54, puis simplifier $\frac{72}{54}$.

3) Calculer le PGCD de 255 et 35, puis simplifier $\frac{255}{35}$.

2 Soit n un entier naturel. Le PGCD de n et de 72 vaut 8. Parmi les valeurs suivantes quelles sont celles que peut prendre n ?

9, 16, 18, 24, 32, 40, 48

3 Deux nombres sont premiers entre eux si leur PGCD est égal à 1.

1) 9 et 16 sont-ils premiers entre eux ?

2) 35 et 91 sont-ils premiers entre eux ?

3) 31 et 67 sont-ils premiers entre eux ?

4 Les phrases suivantes sont-elles vraies ou fausses ? Justifier.

1) Un nombre entier a est divisible par 6 et 9, donc a est divisible par 54.

2) Un nombre entier a est divisible par 8 et 9, donc a est divisible par 72.

3) Un nombre entier a est divisible par 4 et 18, donc $a \equiv 36\ (36)$.

4) Un nombre entier a est divisible par 10 et 15, donc $a \equiv 0\ (150)$.

5 Soit x et y des nombres entiers. Les phrases suivantes sont-elles vraies ou fausses ? Justifier.

1) Si $x \equiv 0\ (81)$, alors $x \equiv 0\ (9)$.

2) L'équation $x^2 + 2y^2 \equiv 3\ (4)$ admet des solutions.

6 Trouver un couple d'entiers $(x\ ;\ y)$ vérifiant les équations suivantes :

1) $7x - 10y = 1$

2) $4x + 5y = 1$

3) $3x + 4y = 3$

4) $7x - 12y = 3$

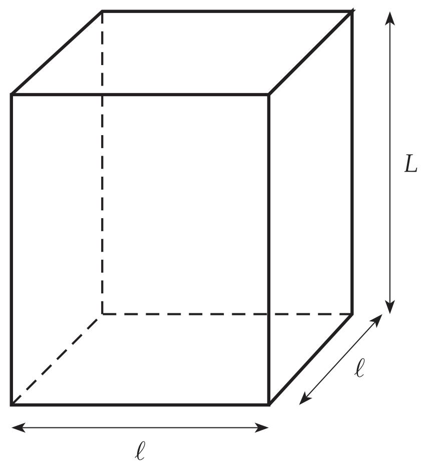
7 Pierre a des jetons d'une valeur de 3 points et Jean a des jetons d'une valeur de 7 points.
Pierre doit donner 34 points à Jean.
Comment Pierre et Jean peuvent-il procéder ? Donner une solution.

Voir solutions p. 151

ACTIVITÉ 1 Boîtes dans une caisse

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).



1) Dans cette question, $\ell = 882$ et $L = 945$.

a) Quelle est la plus grande valeur possible pour a ?
On appelle d cette valeur. d est appelé le PGCD de a et de b.

b) Démontrer que tous les diviseurs de d conviennent comme valeur de a.

c) Existe-t-il d'autres valeurs possibles pour a ?

2) 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.
On pose : $\ell = a\ell'$ et $L = aL'$.

a) Que peut-on dire de PGCD$(\ell'; L')$ si $a = 12$? Pourquoi ?

b) Vérifier, dans le cas $a = 12$, que $\ell'^2 L' = 45$.

c) Montrer qu'il y a exactement deux boîtes B possibles dont on donnera les dimensions.

ACTIVITÉ 2 Algorithme pour une solution particulière

Le but de cette activité est de déterminer un algorithme permettant de déterminer un couple d'entiers relatifs $(x_0 \,;\, y_0)$ solution de l'équation (E) : $59x + 27y = 1$.
On suppose que cette équation admet des solutions entières.

1) Pourquoi peut-on trouver un entier naturel $x_0 > 0$ tel que le couple $(x_0 \,;\, y_0)$ soit solution de (E) ?

2) On s'intéresse à la quantité $59u + 27v$ où u et v varient sur $\mathbb{Z}$.
On propose l'algorithme de la page suivante pour calculer les valeurs de x_0 et y_0.
E(x) signifie la partie entière de x.

a) Que fait-on à la ligne 8 ?

b) Que calcule-t-on à la ligne 9 ?

c) Expliquer la condition $(r \neq 1)$ dans la boucle conditionnelle.

d) Déterminer la valeur à donner à la variable v à la ligne 11, pour que v donne la valeur y_0.

e) Rentrer le programme dans la calculatrice et donner une solution $(x_0 \,;\, y_0)$ de (E).

Liste des variables utilisées
u, v, r : *entiers*
Entrées
Donner à r la valeur de 0
Donner à u la valeur de 0
Traitements
Tant que $(r \neq 1)$ **faire**
Donner à u la valeur de $u + 1$
Donner à r la valeur de $59u - 27 \times \mathrm{E}\left(\dfrac{59u}{27}\right)$
Fin Tant que
Donner à v la valeur de ...
Affichage
Afficher u, v

ACTIVITÉ 3 Chiffrement affine

Le **chiffrement** ou cryptage consiste à transformer un message en message codé (ou chiffré). Le **déchiffrement** est le procédé inverse, il consiste à décoder un message codé.

Partie A : Un premier exemple

Afin de **coder** un message, 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

Un chiffrement élémentaire est le chiffrement affine. On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.
À une lettre du message :

- on associe un entier x entre 0 et 25 suivant le tableau ci-dessus ;
- on calcule $f(x) = 11x + 8$ et l'on détermine le reste y de la division de $f(x)$ par 26 ;
- on traduit y par une lettre d'après le tableau ci-dessus.

Exemple : Si l'on veut coder la lettre G par la fonction $f(x) = 11x + 8$, on passe par les étapes suivantes : G $\Rightarrow$ $x = 6$ $\Rightarrow$ $11 \times 6 + 8 = 74$ $\Rightarrow$ $74 \equiv 22\ (26)$ $\Rightarrow$ $y = 22$ $\Rightarrow$ W

La lettre G est donc codée par la lettre W.

1) Coder la lettre W.

2) Existence d'une fonction de décodage.

Théorème de Bézout : a et b sont deux entiers naturels. « a et b sont premiers entre eux » équivaut à « il existe deux entiers relatifs u et v tels que $au + bv = 1$ ».

a) Pourquoi le théorème de Bézout permet-il d'affirmer qu'il existe un entier relatif u tel que : $11u + 26v = 1$?
b) Montrer alors que l'équation $11x \equiv 1\ (26)$, puis que l'équation $11x \equiv j\ (26)$, j étant un entier naturel, admettent une solution.

3) Déterminer la fonction de décodage.
a) Montrer que pour tous entiers relatifs x et j, on a : $11x \equiv j\ (26) \quad \Leftrightarrow \quad x \equiv 19j\ (26)$.
b) En déduire que la fonction f^{-1} de décodage est $f^{-1}(y) = 19y + 4$.
c) Décoder la lettre L.

Partie B : Codage et décodage

La fonction de codage est définie par la fonction f telle que : $f(x) = 21x + 11$.

1) Coder le mot : ENIGME.
On pourra éventuellement remplir le tableau ci-contre.

Lettre	E	N	I	G	M	E
x	4					
$f(x)$	95					
y	17					
Code	R					

2) On cherche la fonction de déchiffrage f^{-1}.

a) Démontrer que, pour tous relatifs x et z, on a : $21x \equiv z\ (26) \quad \Leftrightarrow \quad x \equiv 5z\ (26)$.
b) En déduire que la fonction de décodage est définie par : $f^{-1}(y) = 5y + 23$.
c) Décoder le message RPERNL.
On pourra éventuellement remplir le tableau ci-contre.

Code	R	P	E	R	N	L
y	17					
$f^{-1}(y)$	108					
x						
Lettre						

Partie C : Casser une fonction de cryptage

On a reçu le message suivant : FMEYSEPGCB.

Par une étude statistique de la fréquence d'apparition des lettres sur un passage plus important, on déduit que le chiffrement est affine, que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f(x) = ax + b$ où a et b sont des entiers naturels compris entre 0 et 25.

1) Démontrer que a et b vérifient le système suivant : $\begin{cases} 4a + b \equiv 4\ (26) \\ 9a + b \equiv 13\ (26) \end{cases}$

2) a) Démontrer que $5a \equiv 9\ (26)$, puis que $a \equiv 7\ (26)$.
b) En déduire que $b \equiv 2\ (26)$ et que f est définie par $f(x) = 7x + 2$.
c) Démontrer que, pour tous relatifs x et z, on a : $7x \equiv z\ (26) \quad \Leftrightarrow \quad x \equiv 15z\ (26)$.
d) En déduire que la fonction de décodage f^{-1} est définie par $f^{-1}(y) = 15y + 22$.
e) Décoder le message.

1. Plus grand commun diviseur

A. Définition et propriétés

DÉFINITION

Soit a et b deux entiers relatifs non tous nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément d, appelé **plus grand commun diviseur**. On le note : $\textbf{PGCD}(a, b)$.

PREUVE *Existence*

L'ensemble des diviseurs communs à a et b est un ensemble fini car c'est l'intersection de deux ensembles finis.
De plus, 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.
Or tout ensemble fini non vide dans $\mathbb{Z}$ admet un plus grand et unique élément, donc d existe.

Exemples $\text{PGCD}(24, 18) = 6$, $\text{PGCD}(60, 84) = 12$, $\text{PGCD}(150, 240) = 30$.

PROPRIÉTÉ

- $\text{PGCD}(a, b) = \text{PGCD}(b, a)$
- $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$
- $\text{PGCD}(a, 0) = a$ car 0 est multiple de tout entier.
- Si b divise a, alors $\text{PGCD}(a, b) = |b|$.
- Pour tout entier naturel k non nul, on a : $\text{PGCD}(ka, kb) = k\,\text{PGCD}(a, b)$.

REMARQUE : Les preuves de ces propriétés sont laissées à l'initiative de l'élève.

Exemples

- $\text{PGCD}(82, 0) = 82$.
- $\text{PGCD}(-24, -18) = \text{PGCD}(24, 18) = 6$.
- $\text{PGCD}(30, 5) = 5$ car 30 est un multiple de 5.
- $\text{PGCD}(240, 180) = 10\text{PGCD}(24, 18) = 60$.

B. Nombres premiers entre eux

DÉFINITION

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

Exemples

- $\text{PGCD}(15, 8) = 1$ donc 15 et 8 sont premiers entre eux.
- $\text{PGCD}(a, 1) = 1$. Le nombre 1 est premier avec tout entier.

ATTENTION : Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers. 15 et 8 ne sont pas premiers et pourtant ils sont premiers entre eux.
Par contre, deux nombres premiers distincts sont nécessairement premiers entre eux.

C. Algorithme d'Euclide

THÉORÈME

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

Division de a par b	$a = b\,q_0 + r_0$	avec $b > r_0 \geqslant 0$
Division de b par r_0	$b = r_0\,q_1 + r_1$	avec $r_0 > r_1 \geqslant 0$
Division de r_0 par r_1	$r_0 = r_1\,q_2 + r_2$	avec $r_1 > r_2 \geqslant 0$
$\vdots$	$\vdots$	
Division de r_{n-2} par r_{n-1}	$r_{n-2} = r_{n-1}\,q_n + r_n$	avec $r_{n-1} > r_n \geqslant 0$
Division de r_{n-1} par r_n	$r_{n-1} = r_n\,q_{n+1} + 0$	

On a alors $\text{PGCD}(a,b) = r_n$.

PREUVE

- Montrons que $\text{PGCD}(a,b) = \text{PGCD}(b,r_0)$.

  Soit $D = \text{PGCD}(a,b)$ et $d = \text{PGCD}(b,r_0)$.

  D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0. Par conséquent $D \leqslant d$.
  d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b. Par conséquent $d \leqslant D$.

  On déduit de ces deux inégalités que $D = d$, d'où $\text{PGCD}(a,b) = \text{PGCD}(b,r_0)$.

- La suite des restes : $r_0, r_1, r_2, \ldots, r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car :
  $r_0 > r_1 > r_2 > \cdots > r_n$.
  D'après le principe de descente infinie, il existe alors n tel que $r_{n+1} = 0$.

- De proche en proche, on en déduit que :

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_0) = \cdots = \text{PGCD}(r_{n-2},r_{n-1}) = \text{PGCD}(r_{n-1},r_n).$$

  Or r_n divise r_{n-1}, donc $\text{PGCD}(r_{n-1},r_n) = r_n$.

- Conclusion : $\text{PGCD}(a,b) = r_n$. Le dernier reste non nul est le PGCD.

MÉTHODE 1 Calculer le PGCD de deux nombres

► Ex. 13 p. 38

Exercice d'application Calculer $\text{PGCD}(4\,539, 1\,958)$.

Correction On effectue les divisions euclidiennes suivantes :

$$4\,539 = 1\,958 \times 2 + 623$$
$$1\,958 = 623 \times 3 + 89$$
$$623 = 89 \times 7$$

Conclusion : $\text{PGCD}(4\,539, 1\,958) = 89$.

Remarque : Le petit nombre d'étapes de cet exemple montre la performance de cet algorithme à comparer avec la décomposition en facteurs premiers (voir chapitre A3).
ALGO Voir TP 1 pour la performance de l'algorithme.

2. Théorème de Bézout

Sur la pierre tombale d'Étienne Bézout (né à Nemours, le 31 mars 1730 et mort aux Basses-Loges, le 27 septembre 1783), dans l'église Saint-Pierre à Avon (en Seine-et-Marne), on peut lire cette épitaphe :

« Géomètre savant, philosophe paisible.
Père, époux, citoyen, ami tendre et sensible.
Son savoir fut profond, son esprit pénétrant.
Il connut les plaisirs que donne la sagesse ;
il vécut pour les siens, cultiva leur tendresse
et fit de leur bonheur, son bonheur le plus grand.
Pour sauver de l'oubli son nom et sa mémoire
ce marbre était sans doute un témoin superflu ;
mais des regrets que laisse après lui sa vertu
l'amitié se console en parlant de sa gloire. »

A. Identité de Bézout

PROPRIÉTÉ

Soit a et b deux entiers non nuls et $D = \text{PGCD}(a, b)$.
Il existe alors un couple (u, v) d'entiers relatifs telle que : $au + bv = D$.

PREUVE

Soit G l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs.
G est une partie de $\mathbb{N}$ non vide : on vérifie facilement que $|a| \in G$.

D'après le principe du bon ordre, G admet donc un plus petit élément d tel que $d = au + bv$.

- $D = \text{PGCD}(a, b)$ divise a et b donc D divise $au + bv = d$ et donc $D \leqslant d$.

- Montrons que d divise a.
  Divisons a par d, on a alors $a = dq + r$ avec $0 \leqslant r < d$.
  On isole le reste et on remplace d par $au + bv$:
  $$r = a - dq = a - auq - bvq = a(1 - uq) + b(-vq)$$
  Si $r \neq 0$ alors $r \in G$, or $r < d$ et d est le plus petit élément de G, cela est contradictoire.
  Donc $r = 0$ par conséquent d divise a.
- En faisant le même raisonnement, on montre que d divise aussi b.

  d divise a et b, donc $d \leqslant D$.
- Conclusion : $D \leqslant d$ et $d \leqslant D$ donc $D = d$.

Conséquence : Tout diviseur commun à a et b divise leur PGCD.

B. Théorème de Bézout

THÉORÈME

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

$$au + bv = 1$$

CONSÉQUENCE : Si $\text{PGCD}(a\,;\,b) = D$, alors $a = Da'$ et $b = Db'$ avec $\text{PGCD}(a'\,;\,b') = 1$

REMARQUE : La preuve du théorème de Bézout et de sa conséquence fait l'objet de l'exercice 21 p. 39.

MÉTHODE 2 Montrer que deux nombres sont premiers entre eux

► Ex. 22 p. 39

Exercice d'application

Montrer que $(2n+1)$ et $(3n+2)$ sont premiers entre eux, $n \in \mathbb{N}$.

Correction Il faut prouver qu'il existe des coefficients u et v tels que $u(2n+1) + v(3n+2) = 1$.

$$-3(2n+1) + 2(3n+2) = -6n - 3 + 6n + 4 = 1$$

$\forall n \in \mathbb{N}$, il existe $u = -3$ et $v = 2$ tels que $u(2n+1) + v(3n+2) = 1$.

Les entiers $(2n+1)$ et $(3n+2)$ sont donc premiers entre eux.

MÉTHODE 3 Déterminer un couple $(u\,;\,v)$ tel que $au + bv = 1$

► Ex. 28 p. 39

Exercice d'application

Montrer que 59 et 27 sont premiers entre eux, puis déterminer un couple d'entiers relatifs (x, y) tel que : $59x + 27y = 1$.

Correction

Pour montrer que 59 et 27 sont premiers entre eux, on effectue l'algorithme d'Euclide.

$$59 = 27 \times 2 + 5 \qquad (1)$$

$$27 = 5 \times 5 + 2 \qquad (2)$$

$$5 = 2 \times 2 + 1 \qquad (3)$$

Le dernier reste est 1. Donc $\text{PGCD}(59, 27) = 1$ et 59 et 27 sont premiers entre eux.

Pour déterminer un couple $(x\,;\,y)$, on remonte l'algorithme d'Euclide :

de (3) on obtient :

$$2 \times 2 = 5 - 1$$

On multiplie l'égalité (2) par 2

$$27 \times 2 = 5 \times 10 + 2 \times 2$$

$$27 \times 2 = 5 \times 10 + 5 - 1$$

$$27 \times 2 = 5 \times 11 - 1$$

$$5 \times 11 = 27 \times 2 + 1$$

On multiplie l'égalité (1) par 11

$$59 \times 11 = 27 \times 22 + 5 \times 11$$

$$59 \times 11 = 27 \times 22 + 27 \times 2 + 1$$

$$59 \times 11 = 27 \times 24 + 1$$

On a donc :

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

C. Corollaire de Bézout

PROPRIÉTÉ

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

PREUVE

- *Dans le sens direct* : Supposons que l'équation $ax + by = c$ admette une solution $(x_0\ ;\ y_0)$.
  Soit $D = \text{PGCD}(a, b)$ alors, comme D divise a et b, il divise $ax_0 + by_0$.
  D divise donc c.
- *Réciproquement* : Soit c un multiple de $D = \text{PGCD}(a, b)$.
  Donc il existe un entier relatif k tel que : $c = kD$.
  De l'égalité de Bézout, il existe deux entiers relatifs u et v tels que : $au + bv = D$.
  En multipliant par k, on obtient : $auk + bvk = kD \Leftrightarrow a(uk) + b(vk) = c$.
  Donc il existe $x_0 = uk$ et $y_0 = vk$ tels que $ax_0 + by_0 = c$.

Exemple

- L'équation $4x + 9y = 2$ admet des solutions car $\text{PGCD}(4, 9) = 1$ et 2 est multiple de 1.
  En effet, si $x = -4$ et $y = 2$, on a : $4(-4) + 9(2) = -16 + 18 = 2$.
- L'équation $9x - 15y = 2$ n'admet pas de solution car $\text{PGCD}(9, 15) = 3$ et 2 n'est pas multiple de 3.

3. Le théorème de Gauss et son corollaire

A. Théorème de Gauss

THÉORÈME

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

PREUVE Si a divise le produit bc, alors il existe un entier k tel que : $bc = ka$.

Si a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$.

En multipliant par c, on a :

$$\begin{aligned} acu + bcv &= c \qquad \text{or } bc = ka, \text{ donc :} \\ acu + kav &= c \\ a(cu + kv) &= c \end{aligned}$$

Donc a divise c.

Exemple Pour trouver les solutions dans $\mathbb{Z}^2$ de l'équation $5(x-1) = 7y$, on sait que :

5 divise $7y$. Or $\text{PGCD}(5,7) = 1$, donc, d'après le théorème de Gauss, 5 divise y.
On a donc : $y = 5k$.

En remplaçant dans l'équation, on a :

$$5(x-1) = 7 \times 5k \quad \Leftrightarrow \quad x-1 = 7k \quad \Leftrightarrow \quad x = 7k+1$$

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

Réciproquement, ces solutions vérifient effectivement l'équation.

B. Corollaire de Gauss

PROPRIÉTÉ

Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a.

PREUVE Si b et c divisent a, alors il existe deux entiers relatifs k et k' tels que :

$$a = kb \quad \text{et} \quad a = k'c \quad \text{donc :} \quad kb = k'c.$$

b divise $k'c$, or $\text{PGCD}(b,c) = 1$ donc, d'après le théorème de Gauss, b divise k' donc : $k' = k''b$.

$$a = k'c = k''bc$$

Donc bc divise a.

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

4. Équation diophantienne *ax + by = c*

A. Définition et existence

DÉFINITION

Une **équation diophantienne** est une équation à coefficients entiers dont on cherche les solutions entières. Soit a, b et c trois entiers relatifs, les équations diophantiennes du premier degré sont du type : $ax + by = c$.

REMARQUE : Diophante d'Alexandrie est un mathématicien grec du III^{e} siècle de notre ère.

PROPRIÉTÉ

Une équation diophantienne du premier degré, de la forme $ax + by = c$, où a, b et c sont des entiers relatifs, admet des solutions si, et seulement si, c est un multiple du $\text{PGCD}(a,b)$.

PREUVE Cela découle directement du corollaire du théorème de Bézout.

Exemple L'équation $17x - 33y = 1$ admet des solutions car $\text{PGCD}(17,33) = 1$.

B. Résolution

MÉTHODE 4 Résoudre une équation du type *ax + by = c*

► Ex. 42 p. 40

- On cherche une solution particulière à l'équation.
- On recherche ensuite l'ensemble des solutions en soustrayant termes à termes l'équation et l'égalité de la solution particulière.
- On applique le théorème de Gauss, puis l'on vérifie que les solutions trouvées vérifient bien l'équation.

Exercice d'application Déterminer l'ensemble des solutions de l'équation (E) $17x - 33y = 1$.

Correction

1) On cherche une solution particulière de (E). Ici, il existe une solution évidente : le couple (2 ;1), car $17 \times 2 - 33 \times 1 = 34 - 33 = 1$.

2) On recherche ensuite la solution générale de (E). On a : $\begin{cases} 17x - 33y = 1 \\ 17 \times 2 - 33 \times 1 = 1 \end{cases}$.

   Par soustraction termes à termes des deux égalités, on obtient :

$$17(x-2) - 33(y-1) = 0 \quad \Leftrightarrow \quad 17(x-2) = 33(y-1) \quad (\text{E}')$$

   33 divise $17(x-2)$. Or $\text{PGCD}(17, 33) = 1$, donc d'après le théorème de Gauss, 33 divise $(x-2)$. On a donc : $x - 2 = 33\,k$, $k \in \mathbb{Z}$. En remplaçant dans (E'), on trouve $y - 1 = 17\,k$.

3) Les solutions de (E) sont de la forme : $\begin{cases} x = 2 + 33\,k \\ y = 1 + 17\,k \end{cases}$, $k \in \mathbb{Z}$.

4) Ces solutions vérifient effectivement l'équation.

Exercice d'application Déterminer l'ensemble des solutions de l'équation (E_1) $15x + 8y = 5$.

Correction

1) L'équation (E_1) admet des solutions car 15 et 8 sont premiers entre eux.
2) On cherche une solution particulière à l'équation (E_2) : $15x + 8y = 1$.
   $(-1\,;\,2)$ est solution évidente à (E_2) car : $15 \times (-1) + 8 \times 2 = -15 + 16 = 1$.
3) En multipliant par 5, on trouve alors une solution particulière à (E_1). Le couple $(-5\,;\,10)$ est solution de (E_1).
4) On recherche ensuite la solution générale de (E_1). On a : $\begin{cases} 15x + 8y = 5 \\ 15(-5) + 8(10) = 5 \end{cases}$.

   Par soustraction termes à termes des deux égalités on obtient :

$$15(x+5) + 8(y-10) = 0 \quad \Leftrightarrow \quad 15(x+5) = 8(10-y) \quad (\text{E}_2)$$

   8 divise $15(x+5)$. Or $\text{PGCD}(15, 8) = 1$, donc d'après le théorème de Gauss, 8 divise $(x+5)$.
   On a donc : $x + 5 = 8\,k$, $k \in \mathbb{Z}$.
   En remplaçant dans l'équation (E_2), on trouve $10 - y = 15\,k$.
5) Les solutions de (E_1) sont de la forme : $\begin{cases} x = -5 + 8\,k \\ y = 10 - 15\,k \end{cases}$, $k \in \mathbb{Z}$.
6) Ces solutions vérifient effectivement l'équation.

S'entraîner

Activités mentales

1 Déterminer de tête et à l'aide des règles de divisibilité, les PGCD des entiers suivants :

1) 12 et 42.
2) 45 et 105.
3) 92 et 69.
4) 72 et 108.

2 Sur un vélodrome, deux cyclistes partent en même temps d'un point M et roulent à vitesse constante.
Le coureur A boucle le tour en 35 secondes ; le coureur B en 42 secondes.
Au bout de combien de temps le coureur A aura-t-il un tour d'avance sur le coureur B ?

3

1) On veut découper un rectangle de 24 cm sur 40 cm en carrés dont le côté est le plus grand possible, sans perte.
Combien doit mesurer le côté du carré ?

2) On dispose d'un grand nombre de rectangles du type précédent que l'on veut assembler bord à bord pour former le carré le plus petit possible.
Combien doit mesurer le côté du carré ?

4 Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1) 78 et 108.
2) 144 et 840.
3) 202 et 138.

5 Montrer que deux entiers naturels consécutifs non nuls sont premiers entre eux.

6 En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(x\ ;\ y)$ qui vérifient les équations suivantes :

1) $5(x+3) = 4y$
2) $41x + 9y = 0$

7 Trouver un couple d'entiers relatifs $(x;y)$ qui vérifie l'équation : $7x + 5y = 1$.

8 Existe-il des couples d'entiers $(x\ ;\ y)$ solutions de chacune des équations suivantes ?

1) $37x + 25y = 1$
2) $51x + 39y = 1$
3) $51x + 39y = 2016$

PGCD

9 Dresser la liste des diviseurs positifs de 72 et de 60. En déduire leur PGCD.

10 Si, en un point donné du ciel, un astre A apparaît tous les 28 jours et un astre B tous les 77 jours, avec quelle périodicité les verra-t-on simultanément en ce point ?

11 Déterminer tous les entiers naturels n inférieurs à 200 tels que : $\text{PGCD}(n;324) = 12$.

12 ALGO

a et b sont deux entiers naturels non nuls tels que $a > b$.

1) Démontrer que : $\text{PGCD}(a;b) = \text{PGCD}(a-b;b)$.

2) Calculer les PGCD des entiers suivants par cette méthode, répétée autant de fois que nécessaire :
a) 308 et 165.
b) 1 008 et 308.
c) 735 et 210.

3) a) Recopier et compléter l'algorithme correspondant à cette méthode.

1. *Liste des variables utilisées*
2. a, b, c : entiers naturels
3. *Entrées*
4. Saisir a, b
5. *Traitements*
6. **Tant que** $(a \neq b)$ **faire**
7. Donner à . . . la valeur de $|a-b|$
8. Donner à . . . la valeur de b
9. Donner à . . . la valeur de c
10. **Fin Tant que**
11. *Affichage*
12. Afficher la valeur de . . .

b) Expliquer la condition de la ligne 6.

c) Rentrer cet algorithme dans la calculatrice puis la tester à l'aide des valeurs de la question 2.

Algorithme d'Euclide

13 ► MÉTHODE 1 p. 32

Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1) 441 et 777.
2) 2004 et 9185.

14 Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1) 2 012 et 7 545. **2)** 1 386 et 546.

15 Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1) 4 935 et 517. **2)** 1 064 et 700.

16 Les entiers suivants sont-ils premiers entre eux ?

1) 4 847 et 5 633. **2)** 5 617 et 813.

17 Si on divise 4 294 et 3 521 par un même entier positif, on obtient respectivement 10 et 11 comme reste.

Quel est cet entier ?

18 En divisant 1 809 et 2 527 par un même entier naturel, les restes sont respectivement 9 et 7.

Quel est le plus grand nombre que l'on peut obtenir comme diviseur ?

19 On note n un naturel non nul, $a = 3n+1$ et $b = 5n-1$.

1) Montrer que le $\mathrm{PGCD}(a,b)$ est un diviseur de 8.
2) Pour quelles valeurs de n, $\mathrm{PGCD}(a,b)$ est-il égal à 8 ?

20 n est un entier relatif quelconque. On pose :

$$A = n-1 \text{ et } B = n^2 - 3n + 6.$$

1) a) Démontrer que le PGCD de A et de B est égal au PGCD de A et de 4.
b) Déterminer, selon les valeurs de l'entier n, le PGCD de A et de B.
2) Pour quelles valeurs de l'entier relatif n, $n \neq 1$, $\dfrac{n^2-3n+6}{n-1}$ est-il un entier relatif ?

Théorème de Bézout

21 Soit l'égalité de Bézout : « Soit a et b deux entiers non nuls et D leur PGCD. Il existe un couple d'entiers relatifs telle que $au + bv = D$ ».

1) Démontrer le théorème de Bézout « a et b sont premiers entre eux si, et seulement si, il existe un couple d'entiers relatifs $(u;v)$ tel que $au + bv = 1$ ».
2) En déduire que si $\mathrm{PGCD}(a;b) = D$, alors $a = Da'$ et $b = Db'$ avec $\mathrm{PGCD}(a';b') = 1$.

22 ▶ MÉTHODE 2 p. 34

Démontrer que, pour tout relatif k,

$(7k+3)$ et $(2k+1)$ sont premiers entre eux.

23 n est un entier naturel , $a = 7n+4$ et $b = 5n+3$.

Montrer, pour tout n, que a et b sont premiers entre eux.

24 Démontrer que pour tout relatif n, les entiers $(14n+3)$ et $(5n+1)$ sont premiers entre eux. En déduire $\mathrm{PGCD}(87;31)$.

25 Prouver que la fraction $\dfrac{n}{2n+1}$ est irréductible pour tout entier naturel n.

26 Prouver que la fraction $\dfrac{2n+1}{n(n+1)}$ est irréductible pour tout entier naturel n.

27 La fraction $\dfrac{n^3+n}{2n+1}$ est-elle irréductible pour tout entier naturel n ?

28 ▶ MÉTHODE 3 p. 34

Montrer que 17 et 40 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $17x - 40y = 1$.

29 Montrer que 23 et 26 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $23x + 26y = 1$.

30 L'équation $6x + 3y = 1$ admet-elle des solutions entières ? Et l'équation $7x + 5y = 1$?

31 Montrer que 221 et 331 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $221x - 331y = 1$.

32 **Vrai ou faux ?**

S'il existe deux entiers relatifs u et v tel que $au + bv = 3$, alors le PGCD de a et de b est égal à 3. Justifier.

33 Résoudre dans $\mathbb{N}^2$ les systèmes suivants.

On donnera la réponse sous forme d'un tableau.

1) $\begin{cases} xy = 1512 \\ \mathrm{PGCD}(x,y) = 6 \end{cases}$ **2)** $\begin{cases} xy = 300 \\ \mathrm{PGCD}(x,y) = 5 \end{cases}$

Théorème de Gauss

34 En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(a; b)$ qui vérifient :

$$33a - 45b = 0.$$

35

1) En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(x; y)$ qui vérifient :

$$7(x-3) = 5(y-2).$$

2) De la question précédente, déterminer les entiers naturels x tels que : $7x \equiv 1\ (5)$.

36 En utilisant le théorème de de Gauss, démontrer le corollaire du théorème de Gauss :« Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a ».

37 Montrer que si $n \equiv 0\ (8)$ et $n \equiv 0\ (9)$, alors $n \equiv 0\ (72)$.

PPCM

38 Soit deux entiers relatifs a et b.
On appelle $\text{PPCM}(a; b)$ le plus petit multiple strictement positif de a et de b.

1) Calculer $\text{PPCM}(18; 12)$ et $\text{PPCM}(24\ ;\ 40)$.
2) Calculer $\frac{7}{6} + \frac{11}{15}$. Que représente $\text{PPCM}(6\ ;\ 15)$?

39 On appelle $D = \text{PGCD}(a\ ;\ b)$ et $M = \text{PPCM}(a\ ;\ b)$.

1) Montrer que si $a = Da'$ et $b = Db'$, alors $M = Da'b'$.
2) En déduire que : $D \times M = ab$.

40 Soit a et b deux naturels tels que $a < b$.
En utilisant les propriétés de l'exercice **39**, déterminer a et b tels que : $\text{PGCD}(a\ ;\ b) = 6$ et $\text{PPCM}(a\ ;\ b) = 102$.

Équation du type *ax* + *by* = *c*

41 Soit l'identité de Bézout : « Soit a et b deux entiers non nuls et D leur PGCD. Il existe un couple d'entiers relatifs tel que $au + bv = D$ ».
Démontrer le corollaire du théorème de Bézout : « L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple du $\text{PGCD}(a\ ;\ b)$ ».

42 ▶ MÉTHODE 4 p. 37
Soit l'équation (E) : $4x - 3y = 2$.

1) Déterminer une solution particulière entière à (E).
2) Déterminer l'ensemble des solutions entières.

43 Soit l'équation (F) : $3x - 4y = 6$.

1) Déterminer une solution particulière entière à (F).
2) Déterminer l'ensemble des solutions entières.

44 Soit l'équation (G) : $5x + 8y = 2$.

1) Déterminer une solution particulière entière à (G).
2) Déterminer l'ensemble des solutions entières.

45 Soit l'équation $13x - 23y = 1$.

1) Déterminer une solution particulière entière, à l'aide de l'algorithme d'Euclide, à cette équation.
2) Déterminer l'ensemble des solutions entières.

46

1) Déterminer l'ensemble des couples $(x; y)$ des nombres entiers relatifs, solutions de l'équation :
$$\text{(E)}\ :\ 8x - 5y = 3.$$
2) Soit m un nombre entier relatif tel qu'il existe un couple $(p; q)$ de nombres entiers vérifiant :
$m = 8p + 1$ et $m = 5q + 4$.
Montrer que le couple (p, q) est solution de l'équation (E).
3) Déterminer le plus petit de ces nombres entiers m supérieur à 2 000.

47

1) On considère l'équation (E) à résoudre dans $\mathbb{Z}$:
$$7x - 5y = 1.$$
   a) Vérifier que le couple (3 ; 4) est solution de (E).
   b) Montrer que le couple d'entiers $(x; y)$ est solution de (E) si, et seulement si, $7(x-3) = 5(y-4)$.
   c) Montrer que les solutions entières de l'équation (E) sont exactement les couples $(x; y)$ d'entiers relatifs tels que :
$$\begin{cases} x = 5k + 3 \\ y = 7k + 4 \end{cases} \quad \text{où } k \in \mathbb{Z}.$$
2) Une boîte contient 25 jetons, des rouges, des verts et des blancs. Sur les 25 jetons, il y a x jetons rouges et y jetons verts.
Sachant que $7x - 5y = 1$, quels peuvent être les nombres de jetons rouges, verts et blancs ?

48 D'après Bac (Antilles-Guyane - 2014)

En montagne, un randonneur a effectué des réservations dans deux types de gîte : l'hébergement A et l'hébergement B.

Une nuit en hébergement A coûte 24 € et une nuit en hébergement B coûte 45 €.

Il se rappelle que le coût total de sa réservation est de 438 €.

On souhaite retrouver les nombres x et y de nuitées passées respectivement en hébergement A et en hébergement B.

1) a) Montrer que les nombres x et y sont respectivement inférieurs ou égaux à 18 et 9.

b) Recopier et compléter les pointillés de l'algorithme suivant afin qu'il affiche les couples $(x\,;\,y)$ possibles.

```
Liste des variables utilisées
  x, y : entiers
Traitements et affichage
  Pour x variant de 0 à ... faire
    Pour y variant de 0 à ... faire
      Si ... Alors
        Afficher la valeur de x, y
      Fin Si
    Fin Pour
  Fin Pour
```

2) Justifier que le coût total de la réservation est un multiple de 3.

3) a) Justifier que l'équation $8x + 15y = 1$ admet pour solution au moins un couple d'entiers relatifs.

b) Déterminer une telle solution.

c) Résoudre l'équation (E) : $8x + 15y = 146$ où x et y sont des nombres entiers relatifs.

4) Le randonneur se souvient avoir passé au maximum 13 nuits en hébergement A.
Montrer alors qu'il peut retrouver le nombre exact de nuits passées en hébergement A et celui des nuits passées en hébergement B.
Calculer ces nombres.

49 D'après Bac (Métropole - 2011)

Partie A : Restitution organisée des connaissances

On rappelle ci-dessous le théorème de Bézout et le théorème de Gauss.
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 $au + bv = 1$. »
Théorème de Gauss :
« Soient a, b, c des entiers relatifs. Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c. »

1) En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

2) Soient p et q deux entiers naturels tels que p et q sont premiers entre eux.
Déduire du théorème de Gauss que, si a est un entier relatif, tel que $a \equiv 0\ (p)$ et $a \equiv 0\ (q)$, alors $a \equiv 0\ (pq)$.

Partie B

On se propose de déterminer l'ensemble $\mathscr{S}$ des entiers relatifs n vérifiant le système :

$$\begin{cases} n \equiv 9\ (17) \\ n \equiv 3\ (5) \end{cases}$$

1) Recherche d'un élément de $\mathscr{S}$.
On désigne par $(u\,;\,v)$ un couple d'entiers relatifs tel 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 $\mathscr{S}$.

c) Donner un exemple d'entier n_0 appartenant à $\mathscr{S}$.

2) Caractérisation des éléments de $\mathscr{S}$.

a) Soit n un entier relatif appartenant à $\mathscr{S}$.
Démontrer que $n - n_0 \equiv 0\ (85)$.

b) En déduire qu'un entier relatif n appartient à $\mathscr{S}$ si, et seulement si, n peut s'écrire sous 1a forme $n = 43 + 85k$ où k est un entier relatif.

3) Application
Zoé sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9.
Si elle fait des tas de 5 jetons, il lui en reste 3.
Combien a-t-elle de jetons ?

50 D'après Bac (Nouvelle-Calédonie - 2007)

1) Dans cette question x et y désignent des entiers relatifs.

a) Montrer que l'équation $(E)\ :\ 65x - 40y = 1$ n'a pas de solution.

b) Montrer que l'équation $(E')\ :\ 17x - 40y = 1$ admet au moins une solution.

c) Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E').

d) Résoudre l'équation (E').
En déduire qu'il existe un unique naturel $x_0 < 40$ tel que : $17x_0 \equiv 1\ (40)$.

2) Pour tout naturel a, démontrer que si $a^{17} \equiv b\ (55)$ et si $a^{40} \equiv 1\ (55)$, alors $b^{33} \equiv a\ (55)$.

51 D'après Bac (Antilles-Guyane - 2015)

Partie A

Pour deux entiers naturels non nuls a et b, on note $r(a,\ b)$ le reste dans la division euclidienne de a par b.
On considère l'algorithme suivant :

```
Liste des variables utilisées
   c : entier naturel
   a, b : entiers naturels non nuls
Entrées
   Saisir a
   Saisir b
Traitements
   Donner à c la valeur de r(a, b)
   Tant que (c ≠ 0) faire
      Donner à a la valeur de b
      Donner à b la valeur de c
      Donner à c la valeur de r(a, b)
   Fin Tant que
Affichage
   Afficher la valeur de b
```

1) Faire fonctionner cet algorithme avec $a = 26$ et $b = 9$ en indiquant les valeurs de a, b et c à chaque étape.

2) Cet algorithme donne en sortie le PGCD des entiers naturels non nuls a et b.
Le modifier pour qu'il indique si deux entiers naturels non nuls a et b sont premiers entre eux ou non.

Partie B

À chaque lettre de l'alphabet on associe grâce au tableau ci-dessous un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :
Étape 1 : on choisit deux entiers naturels p et q compris entre 0 et 25.
Étape 2 : à la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau ci-dessus.
Étape 3 : on calcule l'entier x' défini par les relations

$$x' \equiv px + q\ (26) \quad \text{et} \quad 0 \leqslant x' \leqslant 25.$$

Étape 4 : à l'entier x', on associe la lettre correspondante dans le tableau.

1) Dans cette question, on choisit $p = 9$ et $q = 2$.

a) Démontrer que la lettre V est codée par la lettre J.

b) Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que : $9u + 26v = 1$. Donner sans justifier un couple $(u\ ;\ v)$ qui convient.

c) Démontrer que $x' \equiv 9x + 2\ (26)$ équivaut à : $x \equiv 3x' + 20\ (26)$.

d) Décoder la lettre R.

2) Dans cette question, on choisit $q = 2$ et p est inconnu.
On sait que J est codé par D.
Déterminer la valeur de p (on admettra que p est unique).

3) Dans cette question, on choisit $p = 13$ et $q = 2$.
Coder les lettres B et D.
Que peut-on dire de ce codage ?

52 Carrelage d'une pièce

Pour carreler une pièce rectangulaire mesurant 4,18 m sur 5,67 m, un carreleur propose à des propriétaires le choix entre deux modèles de dalles carrées.

1) Le premier modèle a 29 cm de côté et coûte 2,30 € l'unité.
Avec ce modèle, il n'utilise que des dalles entières et il complète avec du joint autour de chaque dalle.
  a) Calculer le nombre maximal de dalles que l'on peut poser dans la largeur de la pièce.
  b) Calculer le nombre maximal de dalles que l'on peut poser dans la longueur de la pièce.
  c) Les joints autour des dalles auront-ils tous la même largeur ?
  Si oui, quelle est cette largeur ?

2) Le second modèle a 36 cm de côté et coûte 3,10 € l'unité.
Avec ce modèle-là, il est préconisé d'utiliser des joints de 0,6 cm et le carreleur est alors dans l'obligation de couper des dalles. Les découpes ne sont pas réutilisées. Calculer le nombre de dalles nécessaires.

3) Quel sera le choix le moins coûteux pour l'achat des dalles ?

53 Vrai ou faux ?

Pour chacune des quatre propositions, indiquer si elle est vraie ou fausse, et donner une démonstration de la réponse choisie.

1) **Proposition 1 :** $\forall n \in \mathbb{N}^*$, $3n$ et $2n+1$ sont premiers entre eux.

2) On appelle S l'ensemble des couples $(x;y)$ d'entiers relatifs solutions de l'équation $3x - 5y = 2$.
Proposition 2 : « L'ensemble S est l'ensemble des couples $(5k-1\ ;\ 3k-1)$ où k est un entier relatif. »

3) Soit a et b deux entiers naturels.
Proposition 3 : « S'il existe deux entiers relatifs u et v tels que $au + bv = 2$, alors le PGCD de a et b est égal à 2 ».

4) On considère l'équation (E) : $x^2 - 52x + 480 = 0$, où x est un entier naturel.
Proposition 4 : « Il existe deux entiers naturels non nuls dont le PGCD et le PPCM sont solutions de l'équation (E). »

54 Conjonction de comètes

Le but est de déterminer l'ensemble $\mathscr{S}$ des entiers relatifs n vérifiant le système :

$$\begin{cases} n \equiv 13\ [19] \\ n \equiv 6\ [12] \end{cases}$$

1) Recherche d'un élément de $\mathscr{S}$.
On désigne par $(u\ ;\ v)$ un couple d'entiers relatifs tel que $19u + 12v = 1$.
  a) Justifier l'existence d'un tel couple $(u\ ;\ v)$.
  b) On pose $n_0 = 6 \times 19u + 13 \times 12v$.
  Démontrer que n_0 appartient à $\mathscr{S}$.
  c) Donner un exemple d'entier n_0 appartenant à $\mathscr{S}$.

2) Caractérisation des éléments de $\mathscr{S}$.
  a) Soit n un entier relatif appartenant à $\mathscr{S}$.
  Démontrer que $n - n_0 \equiv 0\ (228)$.
  b) En déduire qu'un entier relatif n appartient à $\mathscr{S}$ si, et seulement si, n peut s'écrire sous la forme $n = -6 + 228k$ où k est un entier relatif.

3) Application.
La comète A passe tous les 19 ans et apparaîtra la prochaine fois dans 13 ans.
La comète B passe tous les 12 ans et apparaîtra la prochaine fois dans 6 ans.
Dans combien d'années pourra-t-on observer les deux comètes la même année ?

55 Restes chinois

On se propose de résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} N \equiv 5\ [13] \\ N \equiv 1\ [17] \end{cases}$$

1) Vérifier que 239 est solution de ce système.

2) Soit N un entier relatif solution de ce système.
Démontrer que N peut s'écrire sous la forme :
$N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.

3) Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.

4) En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.

56 Un problème du VIIIᵉ siècle

1) On considère l'équation (E) : $8x + 5y = 1$, où $(x\,;\,y)$ est un couple de nombres entiers relatifs.

a) Donner une solution particulière de l'équation (E).

b) Résoudre l'équation (E).

2) Soit N un nombre naturel tel qu'il existe un couple $(a\,;\,b)$ de nombres entiers vérifiant :

$$\begin{cases} N = 8a + 1 \\ N = 5b + 2. \end{cases}$$

a) Montrer que le couple $(a\,;\,-b)$ est solution de (E).

b) Quel est le reste dans la division de N par 40 ?

3) a) Résoudre l'équation $8x + 5y = 100$, où $(x\,;\,y)$ est un couple de nombres entiers relatifs.

b) Au VIIIᵉ siècle, un groupe composé d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune.
Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

57 Algorithme et équation diophantienne ALGO

On considère l'algorithme suivant, où A et B sont des entiers naturels tels que $A < B$:

```
Liste des variables utilisées
  A, B, C, D : entiers
Entrées
  Saisir A, B tels que A < B
Traitements
  Donner à D la valeur de B − A
  Tant que (D > 0) faire
    Donner à B la valeur de A
    Donner à A la valeur de D
    Si B > A Alors
      Donner à D la valeur de B − A
    Sinon
      Donner à D la valeur de A − B
    Fin Si
  Fin Tant que
Affichage
  Afficher la valeur de A
```

1) On entre $A = 12$ et $B = 14$.
En remplissant le tableau suivant, déterminer la valeur affichée par l'algorithme.

A	B	D
12	14	

2) Que calcule cet algorithme ?

3) a) Montrer que 221 et 331 sont premiers entre eux.

b) Justifier que l'équation (E) : $221x - 331y = 1$ admet des solutions entières.

c) Déterminer une solution particulière de l'équation (E).
(On pourra éventuellement remonter l'algorithme d'Euclide.)

d) Déterminer l'ensemble des couples $(x\,;\,y)$ d'entiers relatifs solutions de l'équation (E).

4) On considère les suites d'entiers naturels (u_n) et (v_n) définies pour tout entier naturel n par

$$u_n = 2 + 221n \qquad \text{et} \qquad \begin{cases} v_0 = 3 \\ v_{n+1} = v_n + 331 \end{cases}$$

a) Quelle est la nature de la suite (v_n) ?
En déduire l'expression de v_n en fonction de l'entier naturel n.

b) Déterminer tous les couples d'entiers naturels $(p\,;\,q)$ tels que :
$u_p = v_q$, $\quad 0 \leqslant p \leqslant 500 \quad$ et $\quad 0 \leqslant q \leqslant 500$.

À la fin de ce chapitre, je dois être capable de :

- Calculer un PGCD grâce à l'algorithme d'Euclide
- Connaître l'énoncé de l'identité de Bézout
- Connaître le théorème et le corollaire de Bézout
- Connaître le théorème et le corollaire de Gauss
- Trouver toutes les solutions dans $\mathbb{Z}^2$ de l'équation : $ax + by = c$

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Déterminer la réponse exacte en la justifiant.

58 On a $\text{PGCD}(25\,176\ ,\ 42\,722) = 2$. Combien de divisions, à l'aide de l'algorithme d'Euclide, sont-elles nécessaires jusqu'à obtenir un reste nul ?

a) 12 b) 11 c) 10 d) 9

59 a et b sont deux entiers naturels tels que : $\text{PGCD}(a, b) = 7$.
Dans l'algorithme d'Euclide, les quotients successifs sont 3, 1, 1, 2 (comprenant la dernière division de reste nul). Alors :

a) $(a\ ;\ b) = (35, 63)$ b) $(a\ ;\ b) = (35, 126)$ c) $(a\ ;\ b) = (25, 126)$ d) $(a\ ;\ b) = (14, 35)$

60 Le nombre de couples d'entiers naturels vérifiant $\text{PGCD}(a; b) = 42$ et $a + 2b = 336$ est :

a) 4 b) 3 c) 2 d) 1

61 Pour tout entier n, on pose $a = 3n - 5$ et $b = 2n - 7$. Alors :

a) a et b sont premiers entre eux.
b) $\text{PGCD}(a, b) = 11$.
c) Tout diviseur commun à a et b divise 11.
d) a et b ne sont pas premiers entre eux.

62 Soit n un entier naturel.
Quelle fraction est irréductible pour tout n ?

a) $\dfrac{3n}{2n+1}$ b) $\dfrac{n+8}{2n+5}$ c) $\dfrac{3n^2}{2n^2+n}$ d) $\dfrac{n}{(2n+1)(3n+1)}$

63 L'équation diophantienne $5x - 8y = 1$ admet comme solutions des couples d'entiers relatifs qui sont :

a) toujours premiers entre eux.
b) parfois premiers entre eux.
c) jamais premiers entre eux.
d) On ne peut pas déterminer si les entiers sont premiers entre eux ou non.

64 Un nombre est divisible par 15 et par 24, alors ce nombre est divisible par :

(a) 360 (b) 120 (c) 90 (d) 72

65 Soit k un entier relatif. L'équation $5(x-2) = 7k$ d'inconnue x a pour solution :

(a) $x \equiv 2\ (5)$ (b) $x \equiv 5\ (7)$ (c) $x \equiv 2\ (7)$ (d) $x \equiv 0\ (7)$

66 Soit a, b, c trois entiers relatifs et n un entier naturel ($n \geqslant 2$).
La proposition : « Si $ac \equiv bc\ (n)$ alors $a \equiv b\ (n)$ » :

(a) est toujours vraie.
(b) est vraie si c et n sont premiers entre eux.
(c) est vraie si a et b sont premiers entre eux.
(d) n'est jamais vraie.

67 Soit l'équation diophantienne (E) : $27x + 25y = 1$.

(a) $(63\ ;\ -68)$ est solution de (E).
(b) (E) admet un couple d'entiers naturels comme solution.
(c) $(25\ ;\ 37)$ est solution de (E).
(d) (E) n'admet pas de solution.

68 L'équation diophantienne : $17x - 13y = 2$ admet :

(a) aucune solution.
(b) comme solutions : $\begin{cases} x = -6 + 13k \\ y = -8 + 17k \end{cases}$, $k \in \mathbb{Z}$.
(c) comme solutions : $\begin{cases} x = 7 + 26k \\ y = 9 + 34k \end{cases}$, $k \in \mathbb{Z}$.
(d) comme solutions : $\begin{cases} x = 7 + 13k \\ y = 9 - 17k \end{cases}$, $k \in \mathbb{Z}$.

Dans les exercices suivants, plusieurs réponses sont proposées. Déterminer celles qui sont exactes. Justifier.

69 Relever les affirmations vraies.

(a) Si le $\text{PGCD}(a, b) = 1$, alors $\text{PGCD}(a + b\ ;\ b) = 1$.
(b) Il existe deux naturels a et b tels que la somme vaut 150 et $\text{PGCD}(a, b) = 8$.
(c) Deux nombres impairs consécutifs sont premiers entre eux.
(d) L'équation $51x + 39y = 2016$ admet des solutions entières.

70 Dans un chiffrement affine, la fonction de codage est définie par la fonction $f(x) = 17x + 22$ (voir tableau de codage de l'activité 3 p. 29).

(a) Le codage de « HUIT » est « LYCA ».
(b) Le message « PZWC » veut dire « VRAI ».
(c) La seule solution dans $\mathbb{Z}^2$ de l'équation $17x - 26y = 1$ est $(23\ ;\ 15)$.
(d) La fonction de décodage est : $f^{-1}(y) = 23y + 14$.

TP 1 Performance d'un algorithme

1) Recopier et compléter l'algorithme suivant pour qu'il calcule PGCD$(a;b)$.
E(x) signifie la partie entière du nombre x.
Comment s'appelle-t-il ?

Liste des variables utilisées
  a, b, q, r : entiers naturels
Entrées
  Saisir a, b
  Donner à q la valeur de $\mathrm{E}\left(\frac{a}{b}\right)$
  Donner à r la valeur de $a - bq$
Traitements
  Tant que (...) **faire**
    Donner à ... la valeur de b
    Donner à ... la valeur de r
    Donner à q la valeur de ...
    Donner à r la valeur de ...
  Fin Tant que
Affichage
  Afficher la valeur de ...

2) On saisit $a = 391$ et $b = 221$.

a) Remplir ce tableau, en calculant à la main les différentes étapes du programme :

	a	b	q	r
Étape 0	391	221	1	170
Étape 1				
Étape 2				
Étape 3				

b) Rentrer cet algorithme dans la calculatrice et vérifier le résultat trouvé.

3) Modifier cet algorithme pour qu'il affiche le nombre d'étapes nécessaires pour calculer PGCD$(a;b)$. Combien d'étapes sont nécessaires pour calculer le PGCD de $a = 87\,724$ et $b = 23\,296$?

4) On voudrait connaître le nombre maximum m d'étapes nécessaires pour calculer le PGCD de deux nombres de n chiffres pour $n \in \{5, 6, 7, 8\}$. Pour cela, on modifie le programme pour qu'il calcule 100 fois le PGCD de deux nombres de n chiffres et qu'il affiche le nombre maximum d'étapes m.

a) Quelle instruction peut-on utiliser pour générer un nombre au hasard de n chiffres ?

b) Écrire un algorithme permettant de répondre au problème posé.

c) Rentrer ce programme dans la calculatrice, puis remplir le tableau suivant :

n	5	6	7	8
m				

TP 2 Conjonction de corps célestes

Un astronome a observé au jour J_0 le corps céleste A, qui apparaît périodiquement tous les 105 jours. Six jours plus tard ($J_0 + 6$), il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome.
Le but de cet exercice est de déterminer la date de ce jour J_1.

1) Soit u et v le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1.
Montrer que le couple $(u\ ;\ v)$ est solution de l'équation $(E_1)\ :\ 35x - 27y = 2$.

2) **a)** Déterminer un couple d'entiers relatifs $(x_0\ ;\ y_0)$ solution particulière de l'équation (E_2) : $35x - 27y = 1$.
b) En déduire une solution particulière $(u_0\ ;\ v_0)$ de (E_1).
c) Déterminer toutes les solutions de l'équation (E_1).
d) Déterminer la solution $(u\ ;\ v)$ permettant de déterminer J_1.

3) **a)** Combien de jours s'écouleront entre J_0 et J_1 ?
b) Le jour J_0 était le mardi 7 décembre 1999, quelle est la date exacte du jour J_1 ?
(L'année 2000 était bissextile.)
c) Si l'astronome manque ce futur rendez-vous, combien de jours devra-t-il attendre jusqu'à la prochaine conjonction des deux astres ?


Portrait imaginaire d'Hypatie d'Alexandrie

Hypatie d'Alexandrie (vers 370 - 415)
Seule mathématicienne connue de l'Antiquité. Elle écrit notamment des commentaires sur l'arithmétique de Diophante et sur les tables de Ptolémée. Elle meurt lapidée par des moines chrétiens fanatiques.

TP 3 Chiffrement de Hill

A Partie A : Inverse de 23 modulo 26

Soit l'équation : (E) : $23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1) Vérifier que le couple $(-9\ ;\ -8)$ est solution de l'équation (E).
2) Résoudre alors l'équation (E).
3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1 \pmod{26}$.

B Codage et décodage

Le chiffrement de Hill publié en 1929, est un chiffre polygraphique, c'est-à-dire qu'on ne chiffre pas les lettres les unes après les autres, mais par « paquets ».
Voici un exemple « bigraphique », c'est-à-dire où les lettres sont regroupées deux à deux.

Étape 1 : On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant 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 obtient des couples d'entiers $(x_1\ ;\ x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

Étape 2 : Chaque couple $(x_1\ ;\ x_2)$ est transformé en $(y_1\ ;\ y_2)$ tel que :

$$(S_1)\quad \begin{cases} y_1 \equiv 11x_1 + 3x_2 \ (26) \\ y_2 \equiv 7x_1 + 4x_2 \ (26) \end{cases} \quad \text{avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 : Chaque couple $(y_1\ ;\ y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres.

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape 1}}{\Longrightarrow} (19,4) \overset{\text{étape 2}}{\Longrightarrow} (13,19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1) Coder le mot ST.

2) On décide de construire un algorithme permettant d'aller plus vite.
On propose l'algorithme à compléter suivant où $\mathrm{E}(x)$ désigne la partie entière de x :

> *Liste des variables utilisées*
> X, Y, Z, T : entiers
> *Entrées*
> Saisir X, Y
> *Traitements*
> Donner à Z la valeur de ...
> Donner à T la valeur de ...
> Donner à Z la valeur de $Z - 26 \times \mathrm{E}\left(\dfrac{Z}{26}\right)$
> Donner à T la valeur de $T - 26 \times \mathrm{E}\left(\dfrac{T}{26}\right)$
> *Affichage*
> Afficher les valeurs de Z, T

a) Coder PALACE et RAPACE.

b) Que constatez-vous ?

3) On veut maintenant déterminer la procédure de décodage.

a) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_1) vérifie aussi les équations du système :

$$(S_2)\quad \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \ (26) \\ 23x_2 \equiv 19y_1 + 11y_2 \ (26) \end{cases}$$

b) À l'aide de la partie A, montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_2) vérifie aussi les équations du système :

$$(S_3)\quad \begin{cases} x_1 \equiv 16y_1 + y_2\ (26) \\ x_2 \equiv 11y_1 + 5y_2\ (26) \end{cases}$$

c) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_3) vérifie aussi les équations du système (S_1).

d) Écrire un algorithme sur le même principe que l'algorithme de chiffrage pour décoder un mot.

e) Décoder le mot : PFXXKNU.
Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, on supprimera la lettre dont le code est W.

Récréation, énigmes

Repas gastronomique

28 personnes participent à un repas gastronomique. Le prix normal est de 26 € sauf pour les étudiants et les enfants. Ces derniers paient respectivement 17 € et 13 €. La somme totale recueillie est de 613 €.
Calculer le nombre d'étudiants et d'enfants ayant participé au repas.
Proposer trois méthodes dont une algorithmique pour résoudre ce problème.

Jour et mois de naissance

En multipliant mon jour de naissance par 12 et mon mois de naissance par 31, j'obtiens 442.
Quelle est ma date de naissance ? On proposera deux méthodes dont une algorithmique à ce problème.
(On ne demande pas l'année, ouf !)

Théorème des restes chinois

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager de manière égale, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

ARITHMÉTIQUE

3

Les nombres premiers

Connaissances nécessaires à ce chapitre

- Connaître les règles de divisibilité par 3, 5, 11
- Trouver tous les diviseurs d'un nombre
- Déterminer si des nombres sont congruents
- Utiliser les règles de calcul avec la congruence
- Utiliser le théorème de Gauss

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 Montrer que les nombres suivants sont des nombres premiers :

1) 31 **2)** 47 **3)** 53 **4)** 61 **5)** 83

2 Sans calculatrice, à l'aide des critères de divisibilité par 3, 5 et 11 ou de la division par 7, montrer que les nombres suivants ne sont pas premiers :

1) 57 **3)** 143 **5)** 341 **7)** 319
2) 91 **4)** 265 **6)** 427 **8)** 1581

3 Sans calculatrice, donner tous les diviseurs des nombres suivants :

1) 16 **3)** 24 **5)** 45 **7)** 63
2) 15 **4)** 36 **6)** 51 **8)** 91

4 Traduire avec une seule égalité de congruence les propositions suivantes :

1) n est divisible par 6.
2) n est divisible par 3 et par 5.
3) n est divisible par 4 et par 6.
4) n est divisible par 8 et par 9.

5 Traduire par une phrase les propositions suivantes sans utiliser le mot « congruence » :

1) $n \equiv 0\ (5)$.
2) si $n \equiv 0\ (4)$ et $n \equiv 0\ (5)$, alors $n \equiv 0\ (20)$.
3) Si $n \leqslant 25$ et si $n \not\equiv 0\ (2)$, $n \not\equiv 0\ (3)$, $n \not\equiv 0\ (5)$ alors n est premier.
4) Si p est premier et si $ab \equiv 0\ (p)$, alors $a \equiv 0\ (p)$ ou $b \equiv 0\ (p)$.

Voir solutions p. 151

ACTIVITÉ 1 Table des nombres premiers inférieurs à 150

On donne ci-dessous la liste des entiers naturels non nuls inférieurs ou égaux à 150.

Rappeler la définition d'un nombre premier.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Partie A : Élaboration de la liste à la main

On se propose de déterminer la liste des nombres premiers inférieurs ou égaux à 150 à la main. Cette méthode s'appelle le **crible d'Ératosthène**. Un « crible » est une sorte de tamis qui, ici, retient uniquement les nombres premiers.

1) On raye 1 et on entoure 2. Rayer tous les multiples de 2 supérieurs à 2.

2) On entoure 3. Rayer tous les multiples de 3 à partir de 9 qui ne sont pas déjà rayés.

3) On entoure 5. Rayer tous les multiples de 5 à partir de 25 qui ne sont pas déjà rayés.

4) On entoure 7. Rayer tous les multiples de 7 à partir de 49 qui ne sont pas déjà rayés.

5) On entoure 11. Rayer tous les multiples de 11 à partir de 121 qui ne sont pas déjà rayés.

6) Entourer tous les nombres de la liste qui ne sont pas rayés. Vérifier qu'il y a 35 nombres entourés et qu'ils correspondent aux nombres premiers inférieurs à 150.

Partie B : Justification

1) Pourquoi est-on sûr lorsqu'on entoure 7 que les multiples de 7 inférieurs à 49 sont déjà rayés de la liste ?

2) On donne la propriété :

> « Si n n'est pas premier, alors il admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$ ».

Parmi les entiers naturels jusqu'à 150, pourquoi est-on sûr qu'une fois rayés tous les multiples de 2 à 11, tous les nombres non rayés sont premiers ?

Partie C : Algorithme

On désire automatiser ce procédé par un programme avec la calculatrice. On utilise pour cela deux listes. À chaque fois que l'on « entoure » un nombre, dans le programme, on le transfère de la liste L_1 dans une liste L_2. La fonction E(x) correspond à la partie entière du nombre *re*.

On écrit l'algorithme ci-contre.

- I est un compteur ;
- les entiers A correspondent aux nombres premiers de la liste des entiers de 1 à 150 ;
- les entiers M correspondent aux multiples de A inférieurs à 150 ;
- les entiers P correspondent aux rangs des nombres premiers A ;
- les entiers Q correspondent au nombre de multiples de A inférieurs ou égaux à 150 ;
- la liste L_1 correspond à la liste des entiers de 1 à 151 ;
- la liste L_2 correspond à la liste des nombres premiers inférieurs ou égaux à 150.

1. *Liste des variables utilisées*
2. I, A, M, P, Q : entiers
3. L_1, L_2 : listes
4. *Entrées*
5. Effacer L_1, L_2
6. **Pour** I **variant de** 1 **à** 151 **faire**
7. Donner à $L_1(I)$ la valeur de I
8. **Fin Pour**
9. Donner à A la valeur de 2
10. Donner à P la valeur de 0
11. *Traitements*
12. **Tant que** $(A \leqslant 150)$ **faire**
13. **Tant que** $(L_1(A) = 0)$ **faire**
14. Donner à A la valeur de $A + 1$
15. **Fin Tant que**
16. **Si** $A \neq 151$ **Alors**
17. Donner à P la valeur de $P + 1$
18. Donner à $L_2(P)$ la valeur de $L_1(A)$
19. Donner à Q la valeur de $\mathrm{E}\left(\frac{150}{A}\right)$
20. **Fin Si**
21. **Pour** I **variant de** 1 **à** Q **faire**
22. Donner à M la valeur de $A \times I$
23. Donner à $L_1(M)$ la valeur de 0
24. **Fin Pour**
25. **Fin Tant que**
26. *Affichage*
27. Afficher P, L_2

1) Pourquoi rentre-t-on dans la liste L_1 les nombres de 1 à 151 ?

2) Quel procédé dans le programme utilise-t-on pour « rayer » un nombre ?

3) Que fait-on aux lignes 22 et 23 ?

4) À la ligne 27, à quoi correspondent P et L_2 ?

5) Rentrer ce programme dans la calculatrice et comparer le résultat avec celui obtenu dans la partie A.

6) Que devrait-on ajouter et modifier dans ce programme pour qu'il puisse afficher la liste des nombres premiers inférieurs ou égaux à un entier N donné ?

7) Donner alors la liste des nombres premiers inférieurs ou égaux à 400. Combien y en a-t-il ?

ACTIVITÉ 2 Nombre de diviseurs

Le but de cette activité est de déterminer tous les diviseurs de 567 à l'aide d'une décomposition en produit de facteurs premiers.

1) Décomposer 567 en produit de facteurs premiers et vérifier qu'il existe deux entiers p et q tels que : $567 = p^4 \times q$.

2) Pourquoi un diviseur de 567 est-il de la forme $p^\alpha q^\beta$ avec $0 \leqslant \alpha \leqslant 4$ et $0 \leqslant \beta \leqslant 1$?

3) Remplir le tableau suivant :

$\times$	p^0	p^1	p^2	p^3	p^4
q^0					
q^1					

4) Donner alors l'ensemble des diviseurs de 567.
Combien y en a-t-il ? Pouvait-on prévoir ce résultat ?

5) Proposer une autre méthode à partir de la décomposition en facteurs premiers permettant de déterminer tous les diviseurs de 567.

6) Proposer un algorithme permettant de trouver tous les diviseurs de 567.

7) **a)** Décomposer 735 en produit de facteurs premiers.
Peut-on prévoir le nombre de diviseurs de 735 ?

b) Vérifier ce résultat par la méthode de votre choix.

ACTIVITÉ 3

Cette activité a pour objectif d'exploiter la décomposition en facteurs premiers à travers le problème classique de « l'âge du capitaine ».

Le capitaine dit à son fils :
« La cabine n° 1 abrite M. Dupont et ses deux filles. Le produit de leurs trois âges est 2 450 et la somme de leurs trois âges est égale à 4 fois le tien. Peux-tu trouver les âges des trois passagers ? »
Après un instant, le fils répond : « Non, il me manque une donnée. »
Le capitaine ajoute alors : « Je suis plus âgé que M. Dupont. »
Le fils du capitaine en déduit alors les trois réponses.

Partie A : L'âge de M. Dupont

1) Décomposer 2 450 en produit de facteurs premiers.

2) Déterminer tous les diviseurs inférieurs à 100 (il y en a 12).

3) Quels sont les âges possibles pour M. Dupont (il y en a 4) ?

Partie B : L'âge de ses deux filles

1) Donner les possibilités des âges des deux filles de M. Dupont pour ces 4 possibilités.

2) Sachant que la somme des trois âges est un multiple de 4, combien reste t-il de possibilités ?

Partie C : L'âge du capitaine

1) Le fils du capitaine connaît l'âge de son père, en quoi cette indication donne-t-elle les trois âges ?

2) Déterminer l'âge du capitaine, celui de M. Dupont et de ses filles.

1. Définition et propriétés

A. Définition

DÉFINITION

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

CONSÉQUENCES :

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur).
- Un nombre premier p est un entier naturel supérieur ou égal à 2, soit : $p \geqslant 2$.
- Les nombres premiers inférieurs à 100 sont :
  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.
- Si un entier naturel n n'est pas premier, il admet un diviseur d tel que : $2 \leqslant d < n$.

REMARQUE : Un entier naturel non premier est parfois appelé un **nombre composé**.

B. Critère d'arrêt ou test de primalité

PROPRIÉTÉ : Critère d'arrêt

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

PREUVE

- Si n est premier, il admet un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble D des diviseurs d de n tels que : $2 \leqslant d < n$ n'est pas vide. D'après le principe du bon ordre, il admet donc un plus petit élément p.
  Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leqslant d' < p$ qui diviserait aussi n.
  Ceci est impossible car p est le plus petit élément de D. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leqslant q$. En multipliant cette inégalité par p, on obtient :

$$p^2 \leqslant pq \quad \Leftrightarrow \quad p^2 \leqslant n, \quad \text{soit} \quad p \leqslant \sqrt{n}$$

MÉTHODE 1 Montrer qu'un nombre est premier

► Ex. 13 p. 62

Pour montrer qu'un naturel n est premier, on utilise la contraposée du critère d'arrêt :
« Si n n'admet pas de diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier. »

Exercice d'application

Montrer que 109 est un nombre premier.

Correction On a $10 < \sqrt{109} < 11$. Donc si 109 n'est pas premier, il admet un diviseur premier inférieur à 11.

On teste tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.

- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- En effectuant la division euclidienne de 109 par 7, on obtient : $109 = 7 \times 15 + 4$.
  109 n'est donc pas divisible par 7.
- Conclusion : 109 n'est pas divisible par 2, 3, 5, et 7 donc 109 est premier.

Exemple ALGO

Le programme ci-contre détermine si un nombre N est premier.
N'ayant pas à notre disposition la liste des nombres premiers :

- on teste si N est divisible par 2 ;
- puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieurs à $\sqrt{N}$.

On obtient alors pour les nombres 527, 719, 11 111 et 37 589 que :

- 527 est divisible par 17 ;
- 719 est premier ;
- 11 111 est divisible par 41 ;
- 37 589 est premier.

```
Liste des variables utilisées
  N, I : entiers
Entrées
  Saisir N
  Donner à I la valeur 2
Traitements
  Si E(N/I) = N/I Alors
    Afficher N "divisible par" I
  Fin Si
  Donner à I la valeur de I+1
  Tant que (I ⩽ √N) faire
    Si E(N/I) = N/I Alors
      Afficher N "divisible par" I
    Fin Si
    Donner à I la valeur de I+2
  Fin Tant que
Affichage
  Afficher N "est premier"
```

C. Infinité des nombres premiers

PROPRIÉTÉ

Il existe une infinité de nombres premiers.

PREUVE

Cette preuve, par l'absurde ou par contradiction est celle proposée au IIIe siècle av. J.-C., par Euclide, dans son ouvrage « *Les Éléments* ».
Il en existe bien évidemment d'autres.
Supposons qu'il existe un nombre fini n de nombres premiers : $p_1, p_2, \ldots, p_i, \ldots, p_n$.
Soit N un nombre entier non premier, supérieur à 2, tel que :
$N = p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n + 1$.

D'après le critère d'arrêt, N admet un diviseur premier.
Soit p_i, $i \in \{1, 2, \ldots, n\}$, ce diviseur premier.
p_i divise donc $p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n) = 1$.
Ceci est impossible car $P_i \geqslant 2$, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est contradictoire.

D. Crible d'Ératosthène

ALGORITHME : Crible d'Ératosthène

Pour dresser la liste des nombres premiers inférieurs ou égaux à N :
- Écrire la liste des entiers de 2 à N.
  D'après le critère d'arrêt, tous les nombres composés (non premiers) plus petits que N ont un facteur premier inférieur ou égal à $\sqrt{N}$.
- Éliminer de la liste tous les multiples de 2 sauf 2.
  Le nombre suivant non éliminé est alors premier. Ici on trouve 3.
- Éliminer de la liste tous les multiples de 3 sauf 3.
  Le nombre suivant non éliminé est alors premier. Ici on trouve 5.
- Réitérer l'étape ci-dessus tant qu'il existe des multiples de nombres premiers inférieurs ou égaux à $\sqrt{N}$.

Remarques :
1) Pour éliminer les multiples de a supérieurs à a, commencer à a^2, car les multiples inférieurs à a ont déjà été éliminés. En effet, les multiples de a inférieurs à a^2 sont aussi des multiples de nombres inférieurs à a. Par exemple lorsqu'on élimine les multiples de 7, on commence à partir de 49.
2) Si $N = 150$, comme $\sqrt{150} \approx 12,25$, alors tout nombre composé sera éliminé en tant que multiple de 2, 3, 5, 7 et 11.

Exemple Pour $N = 100$, on obtient le tableau suivant. Les nombres premiers sont colorés en jaune :

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Remarque : On appelle fonction de compte des nombres premiers, la fonction notée $\pi(x)$ qui compte les nombres premiers inférieurs ou égaux à x.
On a par exemple : $\pi(100) = 25$, $\pi(200) = 46$, $\pi(500) = 95$, $\pi(1000) = 168$.

E. Théorème de Gauss et nombres premiers

PROPRIÉTÉ

Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs. Soit p un nombre premier et a, b deux entiers :

$$\text{Si } p \text{ divise } ab \quad \Leftrightarrow \quad p \text{ divise } a \text{ ou } p \text{ divise } b.$$

PREUVE Comme p est premier, on a : $\text{PGCD}(p, a) = p$ ou $\text{PGCD}(p, a) = 1$.

- Si $\text{PGCD}(p, a) = p$, alors p divise a.
- Si $\text{PGCD}(p, a) = 1$, alors p et a sont premiers entre eux. D'après le théorème de Gauss (voir chapitre 2), p divise b.

Remarque : En particulier, si p est premier et divise une puissance a^k, alors nécessairement p divise a. De cela découle que p^k divise a^k.

Conséquences :

- Si un nombre premier p divise un produit de facteurs premiers, alors p est l'un de ces facteurs premiers.
- Si un nombre n est un carré, alors toutes les puissances des facteurs de sa décomposition en facteurs premiers sont paires.
- Soit $p_1, p_2, \ldots, p_k$ des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_k$ des entiers naturels non nuls. Si, pour tout $i \in \{1, 2, \ldots, k\}$, $p_i^{\alpha_i}$ divise un entier n, alors le produit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ divise aussi l'entier n.

2. Décomposition, diviseurs d'un entier

A. Théorème fondamental de l'arithmétique

THÉORÈME

Tout entier $n \geqslant 2$ peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers. Soit $p_1, p_2 \ldots p_m$ des nombres entiers premiers distincts et $\alpha_1, \alpha_2, \ldots \alpha_m$ des entiers naturels non nuls :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}$$

MÉTHODE 2 Décomposer un nombre en produit de facteurs premiers

► Ex. 25 p. 63

Exercice d'application Décomposer 16 758 en produit de facteurs premiers.

Correction

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

On présente la décomposition avec une barre verticale où l'on écrit à droite, les diviseurs premiers et, à gauche, le quotient des divisions successives par ces diviseurs premiers pris dans l'ordre croissant.

On a donc $16\,758 = 2 \times 3^2 \times 7^2 \times 19$.

PREUVE

Soit n un entier naturel supérieur ou égal à 2.

- Si n est premier, alors n se décompose en lui-même.

  Sinon $n = p_1 \times q_1$ avec $p_1 \leqslant q_1$ et p_1 premier car, d'après le critère d'arrêt, n admet un diviseur premier p_1 tel que $2 \leqslant p_1 \leqslant \sqrt{n}$.

- Si q_1 est premier, alors n se décompose en $n = p_1 \times q_1$.

  Sinon $q_1 = p_2 \times q_2$ avec $p_2 \leqslant q_2$ et p_2 premier car, d'après le critère d'arrêt, q_1 admet un diviseur premier p_2 tel que $2 \leqslant p_2 \leqslant \sqrt{q_1}$. On a alors $q_2 < q_1$.

- Si q_2 est premier, alors n se décompose en $n = p_1 \times p_2 \times q_2$.

  Sinon on réitère le processus, obtenant $q_3,\ q_4, \ldots,\ q_n$ avec $q_3 > q_4 > \cdots > q_n \geqslant 2$.
  Toute suite strictement décroissante dans $\mathbb{N}$ est stationnaire à partir d'un certain rang n donc q_n est premier.

  n se décompose en produit de facteurs premiers : $n = p_1 \times p_2 \times \cdots \times p_n \times q_n$.

  Les facteurs premiers $p_1,\ p_2, \ldots,\ p_n$ et q_n peuvent être éventuellement identiques. On les regroupe alors sous la forme $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}$, avec $\alpha_1, \alpha_2, \ldots, \alpha_m$ des entiers naturels non nuls.

L'**existence** de la décomposition est alors démontrée. L'**unicité** de la décomposition est admise.

MÉTHODE 3 Déterminer le PGCD de deux nombres à partir d'une décomposition en produit de facteurs premiers

► Ex. 27 p. 63

Exercice d'application

Déterminer PGCD(126 ; 735) à l'aide d'une décomposition en produit de facteurs premiers.

Correction

- On décompose les deux nombres en produit de facteurs premiers.

$$\begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array} \qquad \begin{array}{r|l} 735 & 3 \\ 245 & 5 \\ 49 & 7 \\ 7 & 7 \\ 1 & \end{array}$$

On a donc :
$126 = 2 \times 3^2 \times 7$
$735 = 3 \times 5 \times 7^2$

- On détermine les facteurs premiers communs pour trouver le PGCD de ces deux nombres.

$$\text{PGCD}(126\ ;\ 735) = 3 \times 7 = 21.$$

Remarque : L'algorithme d'Euclide est à préférer pour la recherche du PGCD à la méthode par décomposition car il est plus économe en opérations :

$$735 = 126 \times 5 + 105$$
$$126 = 105 \times 1 + 21$$
$$105 = 21 \times 5$$

On obtient PGCD(735 ; 126) en trois étapes.

B. Diviseurs d'un entier

PROPRIÉTÉ

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

$$n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \cdots \times p_m^{\alpha m}.$$

Alors tout diviseur d de n a pour décomposition :

$$d = p_1^{\beta 1} \times p_2^{\beta 2} \times \cdots \times p_m^{\beta m} \quad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i \text{ et } i \in \{1, 2, \ldots, m\}$$

Le nombre N de diviseurs est alors : $N = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)$.

Remarques :

- Le nombre de diviseurs d'un entier se calcule facilement car la puissance d'un facteur premier p_i peut varier de 0 à α_i, ce qui fait $(\alpha_i + 1)$ possibilités.
- Pour qu'un entier n admette un nombre impair de diviseurs, les $(\alpha_i + 1)$ doivent être impairs, donc toutes les puissances α_i doivent être paires. Le nombre n est alors un carré.

MÉTHODE 4 Trouver le nombre de diviseurs d'un entier

► Ex. 30 p. 63

Exercice d'application

Trouver le nombre de diviseurs de 120, puis déterminer tous ses diviseurs.

Correction

- On décompose 120 en facteurs premiers : $120 = 2^3 \times 3 \times 5$.

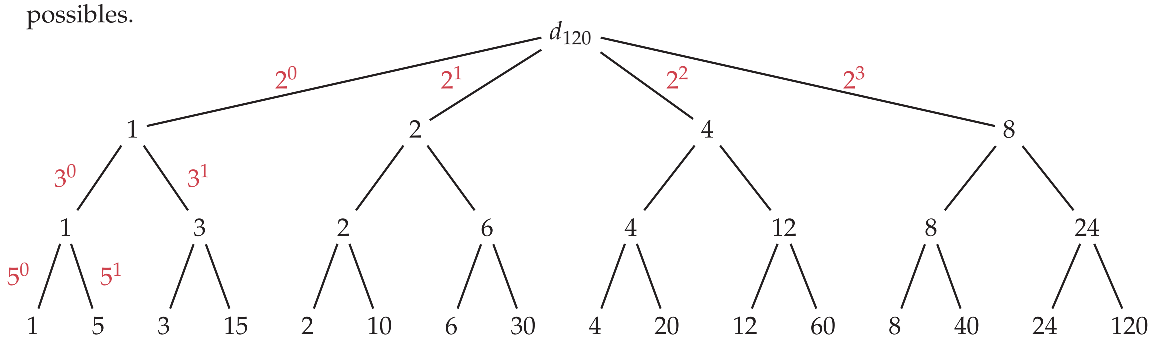
  On alors : $(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16$. Il y a 16 diviseurs pour 120.

- Pour déterminer tous ses diviseurs, on peut utiliser un tableau à double entrée en séparant les puissances de 2 et les puissances de 3 et 5. On obtient alors :

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

  Les 16 diviseurs de 120 sont donc : $D_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$.

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



MÉTHODE 5 Déterminer un entier conditionné par ses diviseurs

► Ex. 36 p. 63

Exercice d'application

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

Correction

- L'entier n a 15 diviseurs. Il faut donc connaître toutes les décompositions de 15 en facteurs supérieurs à 1. Il n'y a que deux décompositions possibles soit en un seul facteur 15, soit en deux facteurs 3×5.
- On sait que n est divisible par 6, il est donc divisible par 2 et par 3. Donc n admet au moins deux facteurs premiers. Comme 15 ne peut se décomposer en plus de deux facteurs, alors n ne peut admettre que deux facteurs premiers : 2 et 3. On a donc : $n = 2^{\alpha}3^{\beta}$.
- Comme on a $15 = 3 \times 5$ diviseurs, alors : $(1+\alpha)(1+\beta) = 3 \times 5$.
- On trouve alors deux solutions : $\alpha = 2$ et $\beta = 4$ ou $\alpha = 4$ et $\beta = 2$.
- On sait de plus que n n'est pas divisible par $8 = 2^3$, donc α est inférieur à 3. n est donc :

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

Exercice d'application

Déterminer le plus petit entier naturel possédant 28 diviseurs.

Correction Soit n l'entier cherché.

Trouvons toutes les décompositions de 28 en produit de facteurs supérieurs à 1. On peut décomposer 28 en 1, 2 ou 3 facteurs : 28 ou 2×14 ou 4×7 ou $2 \times 2 \times 7$.

- En un facteur.
  Le plus petit entier n est alors $n = 2^{\alpha}$ avec $\alpha + 1 = 28$, soit $\alpha = 27$.
  Donc $n = 2^{27} = 134\,217\,728$.
- En deux facteurs : $28 = 2 \times 14$.
  Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta}$ avec $\alpha + 1 = 14$ et $\beta + 1 = 2$.
  On trouve : $\alpha = 13$ et $\beta = 1$, donc $n = 2^{13} \times 3 = 24\,576$.
- En deux facteurs : $28 = 4 \times 7$.
  Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta}$ avec $\alpha + 1 = 7$ et $\beta + 1 = 4$.
  On trouve : $\alpha = 6$ et $\beta = 3$, donc $n = 2^6 \times 3^3 = 1\,728$.
- En trois facteurs : $28 = 2 \times 2 \times 7$.
  Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta} \times 5^{\gamma}$ avec $\alpha + 1 = 7$, $\beta + 1 = 2$ et $\gamma + 1 = 2$.
  On trouve : $\alpha = 6$, $\beta = 1$ et $\gamma = 1$, donc $n = 2^6 \times 3 \times 5 = 960$.

Conclusion, le plus petit entier naturel ayant 28 diviseurs est 960.

S'entraîner

Activités mentales

1 Déterminer les nombres premiers parmi les entiers suivants : 39, 47, 51, 67, 77, 83, 91.

2 Citer tous les nombres premiers compris entre 30 et 60.

3 Soit a et b deux entiers naturels inférieurs ou égaux à 20. Le produit ab est divisible par 5. Quelles sont les valeurs possibles pour a et b ?

4 Soit p un nombre premier et n en entier naturel.

Montrer que si p divise n^2, alors p^2 divise n^2.

5 Soit a un entier naturel. 13 divise a^5.

Montrer que 13^4 divise $\dfrac{a^5}{13}$.

6 Décomposer mentalement les nombres suivants en produits de facteurs premiers : 30, 40, 64, 70, 120, 800, 2 000, 60 000.

7 On considère le nombre 6! (factoriel 6) défini par : $6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6$.

Décomposer n en produit de facteurs premiers.

8 Déterminer la décomposition en facteurs premiers de : $29^2 - 4$ et $85^2 - 16$.

9 Déterminer le nombre de diviseurs de 48.

10 Déterminer le nombre de diviseurs de 60.

11 En optimisant la décomposition en produit de facteurs premiers, déterminer les entiers naturels, compris entre 2 et 50, qui possèdent le plus de diviseurs.

12 En optimisant la décomposition en produit de facteurs premiers : déterminer les entiers naturels, compris entre 2 et 100, qui possèdent le plus de diviseurs.

Généralité sur les nombres premiers

13 ► MÉTHODE 1 p. 55

Sans calculatrice, à l'aide de divisions successives et du critère d'arrêt, déterminer si les entiers suivants sont premiers ou non.

97 ; 117 ; 271 ; 323 ; 401 ; 527 ; 719

14 Montrer que 271 est premier. On expliquera clairement la méthode utilisée.

15 Donner la liste des nombres premiers inférieurs à 50. Les nombres 577 et 689 sont-ils premiers ?

16 p est premier et $p \geqslant 5$.

1) Démontrer que $p^2 - 1$ est divisible par 3.
2) Démontrer que $p^2 - 1$ est divisible par 8.
3) En déduire que $p^2 - 1$ est divisible par 24.

17 Soit p soit un nombre premier tel que $p > 3$.

1) Quels sont les restes possibles dans la division de p par 12 ?
2) Prouver que $p^2 + 11$ est divisible par 12.

18 Démontrer que pour tout n entier ($n \geqslant 1$), $30n + 7$ n'est jamais la somme de deux nombres premiers.

19 Soit le nombre $N = 2n^2 + n - 10$ avec $n \in \mathbb{N}$.

1) Factoriser N.
2) Pour quelles valeurs de n, le nombre N est-il premier ?

20 **Vrai ou faux ?**

Soit le nombre $N = 2n^2 + 7n + 6$ avec $n \in \mathbb{N}$.
La proposition suivante est-elle vraie ou fausse ?
Justifier.
« Il existe une valeur de n telle que N soit premier. »

21 On considère un entier n tel que $n^2 = 17p + 1$, où p est premier.

1) Écrire $17p$ comme le produit de deux facteurs.
2) Citer le théorème de Gauss appliqué aux nombres premiers.
3) En déduire n, puis p.

22 On considère un entier n tel que $n^2 = 29p + 1$, où p est premier.

1) Écrire $29p$ comme le produit de deux facteurs en fonction de n.

2) Citer le théorème de Gauss appliqué aux nombres premiers.
3) En déduire n, puis p.

23 Est-il possible de trouver un nombre premier p tel que $p + 1\,000$ et $p + 2\,000$ soient aussi premiers ?

Aide : On pourra raisonner modulo 3, c'est-à-dire que l'on analysera successivement les cas $p \equiv 0$, $p \equiv 1$ et $p \equiv 2$ modulo 3.

24 **Nombres de Mersenne**

On appelle nombres de Mersenne, les nombres M_n de la forme : $M_n = 2^n - 1$, avec $n \in \mathbb{N}^*$.

1) Calculer les six premiers nombres de Mersenne. Quels sont ceux qui sont des nombres premiers ?
2) Soit n un entier naturel non nul et a un entier. Montrer la factorisation standard : $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$.
3) En déduire que, si d est un diviseur de n, M_n est divisible par $2^d - 1$.
4) Montrer que, si M_n est premier, alors n est premier. La réciproque est-elle vraie ? (On pourra calculer M_{11}.)
5) Soit a et n deux entiers tels que : $a \geqslant 2$ et $n \geqslant 2$. Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Décomposition. Nombre de diviseurs

25 ► MÉTHODE 2 p. 58

Décomposer 960 en produit de facteurs premiers. Quel est le nombre de diviseurs de 960 ?

26 Décomposer en produit de facteurs premiers 221 122. Quel est le nombre de diviseurs de 221 122 ?

27 ► MÉTHODE 3 p. 59

1) Déterminer le PGCD de 2 650 et 1 272 :
   a) à l'aide de l'algorithme d'Euclide ;
   b) à l'aide de la décomposition en produit de facteurs premiers de 2 650 et 1 272.
2) Quelle est la méthode la plus efficace ? Pourquoi ?

28 Déterminer PGCD$(a\,;\,b)$ à l'aide d'une décomposition en facteurs premiers, puis à l'aide de l'algorithme d'Euclide des couples $(a\,;\,b)$ suivants :

1) $a = 1\,188$ et $b = 1\,485$ 2) $a = 3\,780$ et $b = 3\,528$

29

1) Déterminer le PGCD de 428 904 et 306 360 :
   a) à l'aide de l'algorithme d'Euclide ;
   b) à l'aide de la décomposition en facteurs premiers de 428 904 et 306 360.
2) Quelle est la méthode la plus efficace ? Pourquoi ?

30 ► MÉTHODE 4 p. 60

Décomposer 792 en produit de facteurs premiers. Quel est le nombre de diviseurs de 792 ? À l'aide d'un tableau ou d'un arbre déterminer tous les diviseurs de 792.

31 Décomposer 8 316 en produit de facteurs premiers. Quel est le nombre de diviseur de 8 316 ?
À l'aide d'un tableau ou d'un arbre déterminer tous les diviseurs de 8 316.

32 Trouver un nombre de trois chiffres qui soit un carré parfait divisible par 56.

33

1) Décomposer 2 016 en produit de facteurs premiers.
2) Déterminer, en expliquant la méthode choisie, la plus petite valeur de l'entier naturel k pour laquelle k^2 est un multiple de 2 016.

34 Trouver tous les diviseurs de 84, puis résoudre dans $\mathbb{N}$ l'équation : $x(x+1)(2x+1) = 84$.

35 Le produit de deux entiers naturels a et b ($a < b$) est 11 340. On note d leur PGCD.

1) a) Pourquoi d^2 divise-t-il 11 340 ?
   b) Pourquoi $d = 2^\alpha \times 3^\beta$, avec $0 \leqslant \alpha \leqslant 1$ et $0 \leqslant \beta \leqslant 2$?
2) On sait de plus que a et b ont six diviseurs communs et a est un multiple de 5.
   a) Démontrer que $d = 18$.
   b) En déduire a et b.

36 ► MÉTHODE 5 p. 61

α et β sont deux entiers naturels et $n = 2^\alpha 3^\beta$.
Le nombre de diviseurs de n^2 est le triple du nombre de diviseurs de n.

1) Prouver que $(\alpha - 1)(\beta - 1) = 3$.
2) En déduire n.

37 Un nombre n s'écrit $2^\alpha 3^\beta$ où α et β sont deux entiers naturels. Le nombre de diviseurs de $12n$ est le double du nombre de diviseurs de n.

1) Montrer que l'on a : $\beta(\alpha - 1) = 4$.
2) En déduire les trois valeurs possibles pour n.

38 Un entier n a 5 diviseurs et $n - 16$ est le produit de deux nombres premiers.

1) Prouver que $n = p^4$, avec p premier.
2) Écrire $n - 16$ sous forme d'un produit de trois facteurs dépendant de p.
3) En déduire la valeur de n.

39 Un détaillant de matériel audiovisuel effectue trois remises successives sur un article qui coûtait 300 € et qu'il vend 222,87 €.
Quels sont les pourcentages (nombres entiers) des trois remises ?

40 **Les zéros de 1 000 !**

L'exercice a pour but de déterminer par combien de zéros se termine le nombre 1 000 ! (factorielle mille et non « mille points d'exclamation »)

On rappelle que : $1\,000! = 1 \times 2 \times 3 \times \cdots \times 1\,000$.

1) Montrer qu'il existe des entiers p et q ($p \geqslant 1$ et $q \geqslant 1$) et un entier N premier avec 10 tels que :
$$1\,000! = 2^p \times 5^q \times N.$$
2) On justifiera clairement les questions suivantes :
   a) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5 ?
   b) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^2 ?
   c) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^3 ?
   d) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^4 ?
   e) En déduire alors que $q = 249$.
3) Établir que $p > q$ et que le nombre cherché est q.

41 **Triplets pythagoriciens**

Soit p un nombre premier donné. On se propose d'étudier l'existence de couples $(x; y)$ d'entiers naturels strictement positifs vérifiant l'équation :
$$\text{(E)} \quad x^2 + y^2 = p^2.$$

1) On pose $p = 2$. Montrer que l'équation (E) est sans solution.
2) On suppose désormais que $p \neq 2$ et que le couple $(x; y)$ est solution de l'équation (E). Le but des questions suivantes est de prouver que x et y sont premiers entre eux.
   a) Montrer que x et y sont de parités différentes.
   b) Montrer que x et y ne sont pas divisibles par p.
   c) En déduire que x et y sont premiers entre eux.
3) On suppose maintenant que p est une somme de deux carrés non nuls, c'est-à-dire que :
   $p = u^2 + v^2$,
   où u et v sont deux entiers naturels strictement positifs.
   a) Vérifier que le couple $\left(|u^2 - v^2| \; ; \; 2uv\right)$ est solution de (E).
   b) Donner une solution de l'équation (E) lorsque : $p = 5$, puis lorsque $p = 13$.
4) On se propose enfin de vérifier, sur deux exemples, que l'équation (E) est impossible lorsque p n'est pas la somme de deux carrés.
   a) $p = 3$ et $p = 7$ sont-ils la somme de deux carrés ?
   b) Démontrer que les équations : $x^2 + y^2 = 9$ et $x^2 + y^2 = 49$ n'admettent pas de couples solutions d'entiers strictement positifs.

42 **Théorème d'Euclide**

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

1) Euclide donne la règle suivante pour trouver des nombres parfaits :
   « Si un nombre a s'écrit $2^n(2^{n+1} - 1)$ et si $2^{n+1} - 1$ est premier, alors a est parfait ».
   Exemples : Trouver les quatre premiers nombres parfaits.
2) **Démonstration**. On pose $a = 2^n(2^{n+1} - 1)$ et supposons que $2^{n+1} - 1$ est premier.
   a) Quelle est la décomposition de a en produit de facteurs premiers ?
   b) En déduire la liste des diviseurs de a.
   c) Démontrer alors que la somme des diviseurs stricts est égale à ce nombre a.

43 D'après Bac (Centre Étrangers - 2015)

Dans cet exercice, on s'intéresse aux triplets d'entiers naturels non nuls $(x,\ y,\ z)$ tels que :

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

Ces triplets seront nommés « triplets pythagoriciens » en référence aux triangles rectangles dont ils mesurent les côtés, et notés en abrégé « TP ».
Ainsi (3, 4, 5) est un TP car $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

Partie A : Généralités

1) Démontrer que, si $(x,\ y,\ z)$ est un TP, et p un entier naturel non nul, alors le triplet $(px,\ py,\ pz)$ est lui aussi un TP.
2) Démontrer que, si $(x,\ y,\ z)$ est un TP, alors les entiers naturels x, y et z ne peuvent pas être tous les trois impairs.
3) Pour cette question, on admet que tout entier naturel non nul n peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair :

$$n = 2^{\alpha} \times k$$

où α est un entier naturel (éventuellement nul) et k un entier naturel impair.
L'écriture $n = 2^{\alpha} \times k$ est nommée « décomposition » de n.
Voici, par exemple, les « décompositions » des entiers 9 et 120 : $9 = 2^0 \times 9$, et $120 = 2^3 \times 15$.
   a) Donner la décomposition de l'entier 192.
   b) Soit x et z deux entiers naturels non nuls, dont les décompositions sont $x = 2^{\alpha} \times k$ et $z = 2^{\beta} \times m$.
   Écrire la décomposition des entiers naturels $2x^2$ et z^2.
   c) En examinant l'exposant de 2 dans la décomposition de $2x^2$ et dans celle de z^2 , montrer qu'il n'existe pas de couple d'entiers naturels non nuls $(x,\ z)$ tels que $2x^2 = z^2$.

On admet que la question **3a** permet d'établir que les trois entiers naturels x, y et z sont deux à deux distincts. Comme de plus, les entiers naturels x, y jouent un rôle symétrique, dans la suite, pour tout TP $(x,\ y,\ z)$, les trois entiers naturels x, y et z seront rangés dans l'ordre suivant :

$$x < y < z.$$

Partie B : Recherche de triplets pythagoriciens contenant l'entier 2015

1) Décomposer en produit de facteurs premiers l'entier 2 015 puis, en utilisant le TP donné dans le préambule, déterminer un TP de la forme $(x,\ y,\ 2\,015)$.
2) On admet que, pour tout entier naturel n,
$(2n+1)^2 + \left(2n^2+2n\right)^2 = \left(2n^2+2n+1\right)^2$.
Déterminer un TP de la forme $(2\,015,\ y,\ z)$.
3) a) En remarquant que $403^2 = 169 \times 961$, déterminer un couple d'entiers naturels non nuls $(x,\ z)$ tels que : $z^2 - x^2 = 403^2$, avec $x < 403$.
   b) En déduire un TP de la forme $(x,\ 2\,015,\ z)$.

44 D'après Bac (Pondichéry - 2015)

Les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés **nombres de Mersenne**.

1) On désigne par a, b et c trois entiers naturels non nuls tels que : $\text{PGCD}(b\ ,\ c) = 1$.
Prouver, à l'aide du théorème de Gauss, que :
« Si b divise a et c divise a,
alors le produit bc divise a. »
2) On considère le nombre de Mersenne $2^{33} - 1$.
Un élève utilise sa calculatrice et obtient les résultats ci-dessous.

$\left(2^{33}-1\right) \div 3$	2863311530
$\left(2^{33}-1\right) \div 4$	2147483648
$\left(2^{33}-1\right) \div 12$	715827882,6

Il affirme que 3 divise $\left(2^{33}-1\right)$ et 4 divise $\left(2^{33}-1\right)$ et 12 ne divise pas $\left(2^{33}-1\right)$.
   a) En quoi cette affirmation contredit-elle le résultat démontré à la question **1** ?
   b) Justifier que, en réalité, 4 ne divise pas $\left(2^{33}-1\right)$.
   c) En remarquant que $2 \equiv -1\ (3)$, montrer que, en réalité, 3 ne divise pas $2^{33} - 1$.
   d) Calculer la somme :
   $S = 1 + 2^3 + \left(2^3\right)^2 + \left(2^3\right)^3 + \cdots + \left(2^3\right)^{10}$.
   e) En déduire que 7 divise $2^{33} - 1$.
3) On considère le nombre de Mersenne $2^7 - 1$.
Est-il premier ? Justifier.

4) Soit l'algorithme suivant où $\mathrm{MOD}(N,\ k)$ représente le reste de la division euclidienne de N par k.

```
Liste des variables utilisées
   n : entier supérieur ou égal à 3
   k : entier supérieur ou égal à 2
Entrées
   Saisir n
   Donner à k la valeur de 2
Traitements
   Tant que (MOD(2^n − 1 , k) ≠ 0 et
            k ⩽ √(2^n − 1)) faire
      Donner à k la valeur de k + 1
   Fin Tant que
Affichage
   Afficher k
   Si k > √(2^n − 1) Alors
      Afficher "Cas 1"
   Sinon
      Afficher "Cas 2"
   Fin Si
```

a) Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?

b) Que représente le Cas 2 pour le nombre de Mersenne étudié ? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié ?

c) Que représente le Cas 1 pour le nombre de Mersenne étudié ?

45 D'après Bac (Asie - 2014)

Partie A

Pour tout entier naturel $k \geqslant 2$, on pose $M_k = 2^k - 1$.

On dit que M_k est le k-ième nombre de Mersenne.

1) a) Reproduire et compléter le tableau suivant, qui donne quelques valeurs de M_k :

k	2	3	4	5	6	7	8	9	10
M_k	3								

b) D'après le tableau précédent, si k est un nombre premier, peut-on conjecturer que le nombre M_k est premier ?

2) Soient p et q deux entiers naturels non nuls.

a) En déduire que $2^{pq} - 1$ est divisible par $2^p - 1$.

b) En déduire que si un entier k supérieur ou égal à 2 n'est pas premier, alors M_k ne l'est pas non plus.

3) a) Prouver que le nombre de Mersenne M_{11} n'est pas premier.

b) Que peut-on en déduire concernant la conjecture de la question **1b** ?

Partie B

Le test de Lucas-Lehmer permet de déterminer si un nombre de Mersenne donné est premier. Ce test utilise la suite numérique (u_n) définie par $u_0 = 4$ et pour tout entier naturel n :

$$u_{n+1} = u_n^2 - 2.$$

Si n est un entier naturel supérieur ou égal à 2, le test permet d'affirmer que le nombre M_n est premier si, et seulement si, $u_{n-2} \equiv 0\ (M_n)$. Cette propriété est admise dans la suite.

1) Utiliser le test de Lucas-Lehmer pour vérifier que le nombre de Mersenne M_5 est premier.

2) Soit n un entier naturel supérieur ou égal à 3.

L'algorithme suivant, qui est incomplet, doit permettre de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer.

```
Liste des variables utilisées
   u, M, n, i : entiers naturels
Entrées
   Saisir n ⩾ 3
   Donner à u la valeur de 4
Traitements
   Donner à M la valeur de . . .
   Pour i variant de 1 à . . . faire
      Donner à u la valeur de . . .
   Fin Pour
   Si M divise u Alors
      Afficher M . . .
   Sinon
      Afficher M . . .
   Fin Si
```

Recopier et compléter cet algorithme de façon à ce qu'il remplisse la condition voulue.

46 **Nombre d'éléments**

Soit (E) l'ensemble des entiers naturels écrits, en base 10, sous la forme $\overline{abba}$ où a est un chiffre supérieur ou égal à 2 et b est un chiffre quelconque.

Exemples d'éléments de (E) : 2 002 ; 3 773 ; 9 119.

On cherche le nombre d'éléments de (E) ayant 11 comme plus petit facteur premier.

1) a) Décomposer 1 001 en produit de facteurs premiers.
   b) Montrer que tout élément de (E) est divisible par 11.
2) a) Quel est le nombre d'éléments de (E) ?
   b) Quel est le nombre d'éléments de (E) qui ne sont ni divisibles par 2 ni par 5 ?
3) Soit n un élément de (E) s'écrivant sous la forme $\overline{abba}$.
   a) Montrer que : « n est divisible par 3 » équivaut à « $a + b$ » est divisible par 3.
   b) Montrer que : « n est divisible par 7 » équivaut à « b est divisible par 7 ».
4) Déduire des questions précédentes le nombre d'éléments de (E) qui admettent 11 comme plus petit facteur premier.

47 **Vrai ou faux ?**

1) Soit n un entier naturel supérieur à 5.
   Proposition 1 : $n^2 - 3n - 10$ n'est jamais un nombre premier.
2) Soit n un entier naturel supérieur ou égal à 3.
   Proposition 2 : Pour tout entier k ($2 \leqslant k \leqslant n$), le nombre $n! + k$ n'est pas premier.

48 **Rep-unit**

Un rep-unit (ou répunit) est un entier naturel dont l'écriture ne comporte que des 1. Le nom provient de *repated unit* en anglais.

On se propose dans cet exercice d'étudier le problème suivant :

« Les nombres dont l'écriture décimale n'utilise que le seul chiffre 1 peuvent-ils être premiers ? »

Pour tout entier naturel p tel que $p \geqslant 2$, on pose :

$N_p = 1\ldots1$ où 1 apparaît p fois.

On a alors : $N_p = 10^{p-1} + 10^{p-2} + \cdots + 10^1 + 1$.

1) Les nombres N_2, N_3, N_4 sont-ils premiers ?
2) Prouver que $N_p = \dfrac{10^p - 1}{9}$.
3) On se propose de démontrer que si p n'est pas premier, alors N_p n'est pas premier.
   On rappelle que pour tout nombre réel x et pour tout entier naturel n non nul :
   $$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$
   a) On suppose que p est pair et on pose $p = 2q$, où q est un entier naturel plus grand que 1.
      Montrer que N_p est divisible par $N_2 = 11$.
   b) On suppose p non premier et on pose $p = kq$ où k et q sont des entiers naturels plus grands que 1.
      En déduire que N_p est divisible par N_k.
   c) Énoncer une condition nécessaire pour que N_p soit premier.
      Cette condition est-elle suffisante ?

49 **Divisibilité par 240**

p est un nombre premier supérieur ou égal à 7.

Le but de cet exercice est de montrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.

1) Peut-on avoir $p \equiv 0\ (3)$?
   En analysant les autres cas modulo 3, démontrer que n est divisible par 3.
2) En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que :
   $$p^2 - 1 = 4k(k+1).$$
   En déduire que $p^2 - 1$ est divisible par 8 puis que n est divisible par 16.
3) En raisonnant comme à la question 1) modulo 5, démontrer que 5 divise n.
4) a) Que peut-on dire si a et b divise c et que $\mathrm{PGCD}(a, b) = 1$?
   b) Déduire des questions précédentes que 240 divise n.
5) Existe-t-il 15 nombres premiers $p_1, p_2, \ldots, p_{15}$ supérieurs à 7, tels que l'entier A ci-dessous soit un nombre premier ?
   $$A = p_1^4 + p_2^4 + \cdots + p_{15}^4$$

50 Nombres de Fermat

Soit n un entier naturel, on appelle nombre de Fermat le nombre F_n tel que : $F_n = 2^{2^n} + 1$.

1) Soit k un entier naturel non nul.

a) Montrer pour tout entier naturel x que :

$$x^{2k+1} + 1 = (x+1)(x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1).$$

b) Montrer que si m est un entier naturel impair, $2^m + 1$ n'est pas premier.

c) Montrer que si m est un entier naturel qui possède un diviseur impair, $2^m + 1$ n'est pas premier.

d) En déduire que les seuls entiers naturels de la forme $2^m + 1$ sont les nombres de Fermat.

2) Calculer les cinq premiers nombres de Fermat : F_0, F_1, F_2, F_3 et F_4 puis vérifier qu'ils sont premiers.

3) Vérifier que pour tout entier naturel n :
$F_{n+1} = (F_n - 1)^2 + 1$.
En déduire $\text{PGCD}(F_n\,;\,F_{n+1})$.

4) Montrer que, pour tout entier naturel n tel que $n \geqslant 2$, $F_n \equiv 7\ (10)$.

51 Petit théorème de Fermat

Le but de l'exercice est d'étudier certaines propriétés de divisibilité de l'entier $4^n - 1$, lorsque n est un entier naturel.

On rappelle la propriété connue sous le nom de petit théorème de Fermat :

« Si p est un nombre premier et a un entier naturel premier avec p, alors $a^{p-1} - 1 \equiv 0\ (p)$ ».

Partie A : Quelques exemples

1) Démontrer que, pour tout entier naturel n, 4^n est congru à 1 modulo 3.

2) Prouver à l'aide du petit théorème de Fermat, que $4^{28} - 1$ est divisible par 29.

3) Pour $1 \leqslant n \leqslant 4$, déterminer le reste de la division de 4^n par 17. En déduire que, pour tout entier k, le nombre $4^{4k} - 1$ est divisible par 17.

4) Pour quels entiers naturels n le nombre $4^n - 1$ est-il divisible par 5 ?

5) À l'aide des questions précédentes, déterminer quatre diviseurs premiers de $4^{28} - 1$.

Partie B : Divisibilité par un nombre premier

Soit p un nombre premier différent de 2.

1) Démontrer qu'il existe un entier $n \geqslant 1$ tel que $4^n \equiv 1\ (p)$.

2) Soit $n \geqslant 1$ un entier naturel tel que $4^n \equiv 1\ (p)$. On note b le plus petit entier strictement positif tel que $4^b \equiv 1\ (p)$ et r le reste de la division euclidienne de n par b.

a) Démontrer que $4^r \equiv 1\ (p)$. En déduire que $r = 0$.

b) Prouver l'équivalence : $4^n - 1$ est divisible par p si, et seulement si, n est multiple de b.

c) En déduire que b divise $p - 1$.

52 Fonctions modulo 227

1) On considère l'équation (E) : $109x - 226y = 1$, où x et y sont des entiers relatifs.

a) Déterminer le PGCD de 109 et 226. Que peut-on en conclure pour l'équation (E) ?

b) Montrer que l'ensemble des solutions de (E) est l'ensemble des couples de la forme :
$(141 + 226k\,;\,68 + 109k)$, où k appartient à $\mathbb{Z}$.
En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109d = 1 + 226e$.
(On précisera les valeurs des entiers d et e.)

2) Démontrer que 227 est un nombre premier.

3) On note A l'ensemble des 227 entiers naturels a tels que $a \leqslant 226$.
On considère les deux fonctions f et g de A dans A définies de la manière suivante :

- à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227.
- à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

a) Vérifier que $g[f(0)] = 0$.
On donne le théorème suivant appelé petit théorème de Fermat :
« Si p est un nombre premier et a un entier non divisible par p, alors $a^{p-1} \equiv 1\ (p)$. »

b) Montrer que, quel que soit l'entier non nul a de A, $a^{226} \equiv 1\ (227)$.

c) En utilisant **1b**, en déduire que, quel que soit l'entier non nul a de A, on a : $g[f(a)] = a$.
Que peut-on dire de $f[(g(a)] = a$?

À la fin de ce chapitre, je dois être capable de :

- Connaître la définition exacte d'un nombre premier
- Déterminer si un nombre est premier ou non à l'aide du critère d'arrêt
- Utiliser le crible d'Ératosthène
- Utiliser le théorème de Gauss dans le cas d'un nombre premier
- Décomposer un nombre en produit de facteurs premiers
- Exprimer les diviseurs d'un nombre à partir de sa décomposition en facteurs premiers
- Calculer le nombre de diviseurs d'un nombre à partir de sa décomposition en produit de facteurs premiers

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Au moins une réponse est exacte. Déterminer la (ou les) bonne(s) réponse(s).

53 Lequel parmi ces nombres n'est pas premier ?

(a) 227 (b) 379 (c) 221 (d) 313

54 Pour établir la liste des nombres premiers inférieurs à 4 000 à l'aide du crible d'Ératosthène, on raye les multiples des nombres premiers jusqu'à :

(a) 61 (b) 67 (c) 100 (d) 4 000

55 On considère le nombre $N = n + (n+2) + n(n+2)$ avec $n \in \mathbb{N}$. Le nombre N est premier :

(a) si n est impair.
(b) pour aucune valeur de n.
(c) pour les 4 premières valeurs impaires de n.
(d) si n est premier.

56 Parmi les phrases suivantes, quelles sont celles qui sont vraies ?

(a) Si n est un nombre premier, alors n est impair.
(b) Si p et q sont deux nombres premiers distincts, alors p et q sont premiers entre eux.
(c) Si p est premier et divise le produit ab, alors p divise a ou p divise b.
(d) Soit p un nombre premier. Si $a \equiv p\ (p)$, alors a est premier.

57 Parmi les phrases suivantes, quelles sont celles qui sont vraies ?

(a) Si n est un nombre impair, alors n est un nombre premier.
(b) Si p et q sont premiers entre eux, alors p et q sont des nombres premiers.
(c) Si p divise a ou p divise b, alors p divise le produit ab.
(d) Soit p un nombre premier. Si a est premier alors $a \equiv p\ (p)$.

58 Soit p un nombre premier, k et a deux entiers supérieurs à 1.
Si p divise a^k, alors :

(a) p divise a.
(b) p^k divise a^k.
(c) $p = a^k$ si a est premier.
(d) p divise tout diviseur de a^k.
(e) Il y a un diviseur de a qui divise p.

59 Le nombre 10 920 possède :

(a) 144 diviseurs
(b) 64 diviseurs
(c) 72 diviseurs
(d) 48 diviseurs

60 Soit p, q et r trois nombres premiers.
La décomposition en produit de facteurs premiers d'un entier n est : $n = p^2 \times q \times r^3$. Alors

(a) n possède 6 diviseurs.
(b) n possède 12 diviseurs.
(c) n possède 18 diviseurs.
(d) n possède 24 diviseurs.

61 Un nombre n possède 15 diviseurs.

(a) n possède exactement deux facteurs premiers.
(b) n peut ne posséder qu'un seul facteur premier.
(c) n n'est pas nécessairement un carré.
(d) n est un carré.

62 On donne l'algorithme suivant dans lequel $\mathrm{E}(x)$ désigne la partie entière du nombre x :

Liste des variables utilisées
  A, N : entiers naturels
Entrées
  Saisir A
  Donner à N la valeur de 1
Traitements et affichage
  Tant que $(N \leqslant \sqrt{A})$ **faire**
    Si $\dfrac{A}{N} = \mathrm{E}\left(\dfrac{A}{N}\right)$ **Alors**
      Afficher N, $\dfrac{A}{N}$
    Fin Si
  Fin Tant que
  Donner à N la valeur de $N+1$

(a) Cet algorithme affiche le nombre de diviseurs de A.
(b) Cet algorithme affiche tous les multiples de N.
(c) Cet algorithme affiche les diviseurs premiers de A.
(d) Cet algorithme affiche tous les diviseurs de A.

TP 1 Nombres premiers et théorème de Sophie Germain

1) On donne les définitions suivantes :

- Un nombre premier p de Sophie Germain est tel que p et $2p+1$ sont premiers.
- Le nombre $2p+1$ est alors appelé nombre premier sûr.
- Une suite $(p, 2p+1, 2(2p+1)+1, \dots)$ de nombres premiers de Sophie Germain est appelée une chaîne de Cunningham. Chaque terme d'une telle suite, à l'exception du premier et du dernier, est à la fois un nombre premier de Sophie Germain et un nombre premier sûr. Le premier est un nombre de Sophie Germain, le dernier un nombre premier sûr.

a) Déterminer les premiers de Sophie Germain inférieurs à 100.

b) Démontrer, à l'aide du critère d'arrêt, que 239 est un premier de Sophie Germain et que 227 est un nombre premier sûr.

c) Déterminer une chaîne de Cunningham de 5 termes.

2) On donne le théorème suivant :

Pour tout entier $n > 1$, on a : $n^4 + 4$ n'est pas premier.

a) Montrer que, pour tout entier, on a l'égalité dite de « Sophie Germain » :

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

b) n est un entier naturel. Pour quelle(s) valeur(s) de n, $n^4 + 4$ est-il premier ?
En déduire la véracité du théorème.

c) Démontrer que $4^{545} + 545^4$ n'est pas premier.

3) Factoriser $n^4 + n^2 + 1$. Pour quelle(s) valeur(s) de n, $n^4 + n^2 + 1$ est-il premier ?

Marie-Sophie Germain (1776-1831)

À l'âge de treize ans, Sophie Germain lut l'histoire d'Archimède et décida de devenir mathématicienne. Luttant contre la volonté de ses parents, elle apprit les mathématiques en cachette en lisant Newton et Euler, puis s'intéressa à la théorie des nombres à travers les ouvrages de Legendre et Gauss. Redoutant que son travail ne soit ignoré parce qu'elle était une femme, elle leur écrivit sous le pseudonyme de M. Le Blanc et entretint avec eux des correspondances mathématiques durant plusieurs années.

Elle apporta une importante avancée sur le grand théorème de Fermat dans le cas où la puissance est un nombre premier de Sophie Germain, c'est-à-dire qu'il n'existe pas d'entiers naturels x, y, z, tels que :
$x^p + y^p = z^p$ si $p > 2$ est un nombre premier de Sophie Germain.

Lorsque Gauss apprit la supercherie, il lui écrivit : « Mais comment vous décrire mon admiration et mon étonnement à voir mon estimé correspondant Monsieur Le Blanc se métamorphoser en cet illustre personnage qui donne un si brillant exemple de ce que j'aurais trouvé difficile à croire. »

TP 2 Le système cryptographique RSA

Le nom du système RSA., provient des initiales des noms de ses inventeurs américains en 1977 : Ronald **R**ivest (informaticien), Adi **S**hamir (informaticien) et Leonard **A**dleman (mathématicien).

A Arithmétique du système RSA

Soit p et q deux nombres premiers impairs distincts. On pose $n = pq$ et on désigne par e un entier tel que : $1 < e < (p-1)(q-1)$ et e premier avec $(p-1)(q-1)$.

1) Montrer qu'il existe d unique tel que : $1 \leqslant d < (p-1)(q-1)$ et $ed \equiv 1\ [(p-1)(q-1)]$.

2) On rappelle le petit théorème de Fermat :

« Soit un nombre premier p et un entier naturel a non multiple de p, alors : $a^{p-1} \equiv 1\ (p)$. »

Prouver que, pour tout $m \in \mathbb{N}$, $m^{ed} \equiv m\ (n)$.

3) On choisit $p = 5$, $q = 7$ et $e = 7$. Calculer d.

B Envoi d'un message

Alice veut transmettre un message à Bob.
Pour cela, Bob diffuse à tout le monde (donc à Alice) les nombres n et e. Il garde pour lui les nombres p et q qui lui permettent de calculer d pour déchiffrer un message.
Bob rend publique : $n = 33$ et $e = 7$.

Alice voudrait transmettre le mot « SALUT ».
Alice traduit chaque lettre : elle obtient pour la première $m_1 = 18$.

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

Alice code ensuite ces nombres avec la fonction « *trappe* » de Bob : $f_B(m) = m^e\ (n)$.
Pour le premier nombre : $m_1^e \equiv c_1\ (n) \quad \Leftrightarrow \quad 18^7 \equiv 6\ (33) \quad$ d'où $\quad c_1 = 6$.

1) Vérifier qu'Alice envoie à Bob les nombres suivants : 06 - 00 - 11 - 26 - 13.

2) Bob décode alors ces nombres avec sa fonction « *trappe inverse* » : $f_B^{-1}(c) = c^d\ (n)$.
Expliquer pourquoi cette fonction inverse permet de déchiffrer le message ?

3) Pour le premier nombre : $c_1^d \equiv m_1\ (n) \quad \Leftrightarrow \quad 6^3 \equiv 18\ (33) \quad$ d'où $\quad m_1 = 18$.
Bob reçoit un deuxième message avec les nombres suivants :
$14 - 20 - 08 - 12 - 02 - 09 - 00 - 01 - 11 - 16$.
Que lui dit Alice ?

4) **Authentification** : Bob est-il sûr de recevoir ce message d'Alice ?
Alice dispose également d'une fonction trappe f_A (f_A publique et f_A^{-1} connue d'Alice uniquement).
Alice envoie à Bob un message contenant :
- ce qu'elle avait à lui dire ;
- une double signature : A, $f_A^{-1}(A)$.

Comment Bob peut-il s'assurer que le message reçu vient bien d'Alice ?

Commentaires

1) Un système à clef publique :
le couple $(n\ ;\ e)$ connu de tout un chacun permet à « tout public » de transmettre un message à Bob ;
le couple $(p\ ;\ q)$ n'est connu que de Bob et lui permet d'être le seul à pouvoir déchiffrer le message en calculant d.

2) La sécurité du système tient pour l'essentiel dans :
- la construction de nombres premiers « grands » (on sait le faire) ;
- la difficulté de décomposer un nombre grand (300 chiffres par exemple) en produit de deux nombres premiers.
  Mais personne ne sait si une attaque du RSA qui éviterait la factorisation est impossible !

3) Les fonctions à sens unique : un système asymétrique
La fonction *one-way*, de Bob, f_B est connue de tout le monde.
En revanche, la fonction réciproque $f_B^{-1}(m) \mapsto m^d\ \ (n)$, n'est connue que de Bob et est pratiquement impossible à calculer, sauf si l'on dispose d'une information supplémentaire (*trap-door information*), d'où le nom donné à une telle fonction : **fonction trappe**.

C Avec des nombres plus grands

On choisit deux nombres premiers plus grand : $p = 41$ et $q = 53$.

1) a) Calculer n et $(p-1)(q-1)$.

b) On choisit $e = 1\,427$. Montrer que e est premier avec $(p-1)(q-1)$ à l'aide de l'algorithme d'Euclide. En remontant cet algorithme, en déduire d.

2) Bob rend publique $n = 2\,173$ et $e = 1\,427$.
Alice voudrait transmettre le message « Help ! ».
Alice traduit chaque lettre à l'aide du code ASCII (prononcé « aski ») obtenant les nombres de trois chiffres suivants :

H	e	l	p	espace	!
072	101	108	112	032	033

Alice code ensuite ces nombres avec la fonction « *trappe* » de Bob : $f_B(m) = m^e\ (n)$.
Pour H, elle recherche $m_1^e \equiv c_1\ (n) \quad \Leftrightarrow \quad 72^{1\,427} \equiv ?\ (2\,173)$.
Inutile de s'acharner avec la calculatrice, elle se montrera incapable du calcul de $72^{1\,427}$ modulo 2 173. On a recours alors à une méthode dite **d'exponentiation modulaire rapide**.

a) Montrer que $e = 1\,427$ s'écrit $2^{10} + 2^8 + 2^7 + 2^4 + 2 + 1$.

b) Montrer alors que : $m^{1\,427} = m^{2^{10}} \times m^{2^8} \times m^{2^7} \times m^{2^4} \times m^2 \times m$.

c) On calcule ensuite les restes successifs $a_1, a_2, \ldots, a_{10}$ par la division par 2 173 de :
$m, m^2, m^{2^2}, m^{2^3}, m^{2^4}, \ldots, m^{2^{10}}$.
Montrer alors que $a_{10} \times a_8 \times a_7 \times a_4 \times a_1 \times a_0 \equiv c_1\ (2\,173)$.

d) On propose le programme suivant pour coder le message d'Alice.
Ce programme calcule successivement les restes $a_1, a_2, \ldots, a_{10}$.
On range alors les dix restes dans une liste L_1.
Avant de lancer le programme, on a rentré dans une liste L_2 les coefficients des puissances de 2 de 1 427 : $L_2 = (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$.
On cherche ensuite le reste du produit S des a_i où le rang i dans L_2 n'est pas nul.

Liste des variables utilisées
  m, A, n, I, S : entiers
  L_1, L_2 : listes
Entrées
  Saisir n, m
  Effacer L_1
  Donner à A la valeur de reste de m par n
  Donner à $L_1(1)$ la valeur de A
Traitements
  Pour I **variant de** 2 **à** 11 **faire**
    Donner à A la valeur de reste de A^2 par n
    Donner à $L_1(I)$ la valeur de A
  Fin Pour
  Donner à S la valeur de $L_1(1) \times L_2(1)$
  Pour I **variant de** 2 **à** 11 **faire**
    Si $L_2(I) \neq 0$ **Alors**
      Donner à S la valeur de $S \times L_1(I)$
      Donner à S la valeur de reste de S par n
    Fin Si
  Fin Pour
Affichage
  Afficher S

Montrer que si l'on rentre $n = 2\,173$ et $m = 72$, on trouve : $c_1 = 966$.
Coder alors l'ensemble du message d'Alice.

Système d'authentification, fabriqué par la société RSA Security.

Récréation, énigmes

Recherche d'un PGCD

Trouver le PGCD de $3^{37} - 3$ et de $1\,221$.
(Note : il y a du Fermat dans l'air ! !)

PRÉPARER LE BACCALAURÉAT

Présentation de l'épreuve

Durée : 4 heures **Coefficient :** 9. L'épreuve comporte **3 à 5 exercices indépendants**, notés sur 3 à 10 points. Ces exercices abordent les connaissances envisagées dans le programme. Certains vous demanderont une **restitution organisée de connaissances** (la rédaction d'une démonstration figurant au programme), d'autres l'**application directe** de résultats ou de méthodes. Enfin, certaines **questions ouvertes** pourront amener à l'étude d'une situation conduisant à choisir un modèle simple, à émettre une conjecture, à expérimenter, à formuler un raisonnement.

Conseils

La veille de l'épreuve

Pensez à préparer : votre calculatrice (piles neuves et en mode Examen – à partir de 2018), une règle, un compas, plusieurs stylos de couleurs différentes (attention à ne pas utiliser le rouge) et une bouteille d'eau.

Les 5 premières minutes

Quand vous recevez le sujet, lisez bien les indications de la première page et vérifiez le nombre de pages, la quantité d'exercices et les points associés. L'exercice portera la mention « obligatoire » ou « spécialité ». Lisez une première fois les énoncés et choisissez dans quel ordre vous allez faire les exercices : par ordre croissant de difficulté (pour vous).

Au cours de l'épreuve

Lisez attentivement les énoncés. Si vous n'arrivez pas à résoudre la question, ne perdez pas de temps : allez à la question suivante ou à un autre exercice. Vous pourrez revenir à cette question plus tard. Changer de page pour un nouvel exercice et laisser de l'espace pour revenir à une question non traitée.

Les 10 dernières minutes

Quand vous avez terminé, relisez votre copie. La qualité de la rédaction, la clarté et la précision de votre raisonnement seront prises en compte dans l'appréciation de votre copie. Soignez votre écriture. Encadrez les résultats. Vérifiez que vous avez bien indiqué votre nom dans le cartouche et que toutes vos pages sont dans la chemise.

Des problèmes et QCM pour préparer le bac

Ce chapitre regroupe un ensemble d'activités qui utilisent les notions de différents chapitres et permettent de développer les compétences utiles pour le bac :

- consolider vos connaissances et les organiser ;
- mettre en œuvre une recherche de façon autonome ;
- mener des raisonnements ;
- avoir une attitude critique vis-à-vis des résultats obtenus ;
- communiquer à l'écrit.

Problèmes ouverts

Les **problèmes ouverts** se définissent comme des « énoncés courts qui n'induisent ni la méthode, ni la solution ». Il est possible de s'engager dans des essais, des conjectures, des projets de résolution, des contre-exemples.

Problèmes de synthèse

Ils font appel à des notions étudiées dans différents chapitres avec des questions qui s'enchaînent. Ils permettent de réactiver un ensemble de connaissances et d'établir des liens entre les chapitres.

QCM de synthèse

Ils permettent de vérifier l'acquisition des connaissances et des raisonnements en s'affranchissant de la rédaction.

PROBLÈMES OUVERTS

1 **D'après Irem Lyon**

On distribue des bonbons à n enfants placés en cercle en tournant toujours dans le même sens : on donne un bonbon à un enfant, on passe le suivant, on donne un bonbon au troisième, on passe les deux suivants, on donne un bonbon au sixième, etc.

Pour quelles valeurs de n les enfants auront-ils tous au moins un bonbon ?

2 Dans le vivarium d'un zoo, vivent des caméléons de couleurs unies : 13 oranges, 15 verts et 17 bruns. Lors d'une visite à ces grands lézards, Ali observe un curieux phénomène : lorsque deux caméléons de couleurs distinctes se croisent, ils prennent la troisième couleur.

Comment organiser les rencontres pour que la population de caméléons soit unicolore ?

3 En choisissant cinq entiers distincts au hasard, est-on sûr qu'à chaque fois la somme de trois d'entre eux est un multiple de 3 ?

4 Soit la fonction $f : x \mapsto \dfrac{3x+1}{x+1}$.

Sa courbe représentative a-t-elle des points à coordonnées entières ? Si oui, les caractériser.

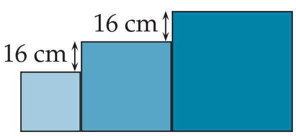
5 Les entiers naturels non nuls x, y, z sont les longueurs des côtés d'un triangle ABC.

Démontrer que si le triangle ABC est rectangle en A alors l'une au moins des longueurs de l'un des côtés est un multiple de 5.

6 Un théâtre pratique deux tarifs : 19 € pour les abonnés et 29 € pour les autres.

À la fin d'une représentation, la caissière a égaré les souches des billets mais elle est sûre d'avoir fait 818 € de recette. Aider la caissière à retrouver la répartition des tickets vendus pour rendre compte au gérant.

7 La figure ci-dessous est formée de trois carrés. L'unité de mesure est le cm et les mesures des côtés des carrés sont des entiers naturels.



Quelles sont les mesures des côtés des carrés sachant que l'aire de la figure est divisible par 10 et inférieure à 5 000 cm^2 ?

8 Est-il vrai qu'un entier naturel qui a un nombre impair de diviseurs est un carré parfait ?

9 Soit a, b et c trois nombres premiers strictement supérieurs à 3.

Le nombre $a^2 + b^2 + c^2$ peut-il être premier ?

10 Les côtés d'un terrain triangulaire mesurent 132 m, 156 m et 204 m. On veut planter des choux sur son pourtour de façon qu'il y ait un chou à chaque sommet du triangle et que les choux soient régulièrement espacés d'un nombre entier de mètres.

Combien de choux au minimum doit-on planter ?

11 Trois navires partent régulièrement d'un même port : l'un tous les huit jours, l'autre tous les dix jours et le dernier tous les quinze jours.

Sachant qu'ils ont quitté le port ensemble un 11 mai, quelle est la date du prochain départ commun ?

12 Soit un entier dont l'écriture a entre 4 et 6 chiffres parmi 1, 3, 7 et 9 présents chacun au moins une fois.

Cet entier peut-il être divisible par 7 ?

13 Existe-t-il un couple d'entiers naturels $(a\ ;\ b)$ tel que le quotient $\dfrac{a^3+1}{ab-1}$ soit un entier naturel ?

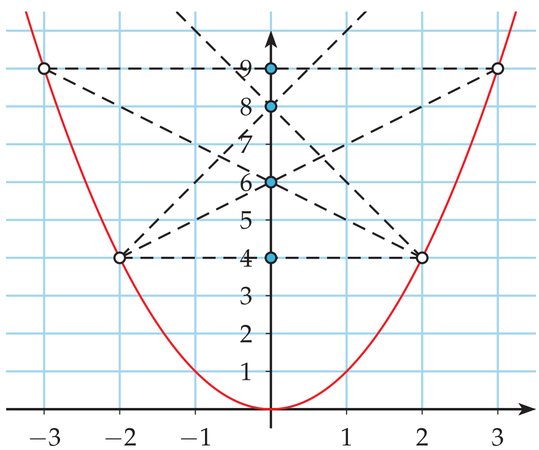
14 **Crible de Matiassevitch**

Soit a et b deux entiers naturels supérieurs à 2.

Dans un repère orhogonal, on place les points $A(-a\ ;a^2)$, $B(b\ ;\ b^2)$ et $M(0\ ;\ m)$ le point d'intersection de la droite (AB) avec l'axe des ordonnées.

Conjecturer l'ensemble des valeurs que m ne peut pas prendre, à l'exception de 0 et de 1.

Démontrer cette conjecture.



15 L'ADN est une séquence de nucléotides dont les quatre bases essentielles sont l'adénine (1), la thymine (2), la guanine (3) et la cytosine (4).
La matrice de transition suivante représente les probabilités de successions des quatre bases :

$$\begin{pmatrix} 0,3 & 0,21 & 0,29 & 0,2 \\ 0,17 & 0,3 & 0,3 & 0,23 \\ 0,25 & 0,2 & 0,3 & 0,25 \\ 0,32 & 0,3 & 0,08 & 0,3 \end{pmatrix}$$

Donner les successions la moins et la plus probables.

16 Un agent fait sa ronde autour d'un parc de forme hexagonale. À chaque angle, il lance un dé : si c'est pair, il continue dans le même sens ; sinon, il change de sens. Un être mal intentionné, qui connaît la combine, a-t-il plutôt intérêt à vouloir entrer dans le parc par un endroit plutôt qu'un autre ?

17 Soit deux suites de matrices (U_n) et (V_n) définies, pour tout $n \in \mathbb{N}$, par :

$$U_{n+1} = 0,8U_n + 3 \quad \text{et} \quad V_{n+1} = -0,6U_n + 1,25V_n + 4$$

Les suites (U_n) et (V_n) sont-elles convergentes ? Si oui, déterminer à quelles conditions, exprimées en fonction des matrices initiales U_0 et V_0.

18 Après le débat de l'entre-deux-tours, un candidat à la présidence voit sa cote de popularité évoluer chaque jour de la façon suivante :

- 3 % de ses partisans deviennent ses détracteurs ;
- 3,5 % de ses détracteurs deviennent ses partisans.

Le candidat a recueilli 41 % des suffrages au premier tour. Peut-il espérer l'emporter dans une semaine ?

19 Chococam, une entreprise de barres chocolatées, lance une opération commerciale en glissant dans chaque paquet le poster d'une équipe ayant fini sur le podium de la coupe d'Afrique des Nations.
On admet qu'il y a assez de paquets sur le marché pour considérer que les posters sont toujours équirépartis.

1) Chococam matraque qu'en achetant six paquets, on a trois chances sur quatre d'avoir les trois posters. Chococam fait-elle de la publicité mensongère ?
2) Un client peut-il être sûr d'obtenir les trois posters ? Si oui, déterminer le nombre de paquets qu'il doit acheter au minimum.

20 Un message codé en binaire est transmis via un réseau. À chaque étape du réseau, la probabilité qu'un bit (0 ou 1) soit transmis sans erreur est $0,01$.
Quelle est la probabilité qu'un octet (huit bits consécutifs) soit transmis sans erreur ?

21 En temps normal, l'équilibre de deux substances A et B présentes dans le corps d'un koala garantit sa bonne santé. Mais chez un koala malade, les quantités de A et B fluctuent et l'on doit injecter chaque mois une quantité q en mg par litre de sang de substance A.
Ainsi, d'un mois n à l'autre, les quantités en mg par litre de sang, a_n (A) et b_n (B), sont régies par l'égalité :

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 0,3 & 0,7 \\ -0,2 & 1,3 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix} + \begin{pmatrix} q \\ 0 \end{pmatrix}.$$

Pour guérir le koala, il faut stabiliser la quantité de substance B autour de 1 000 mg par litre de sang.
Quelle quantité q de substance A faut-il injecter chaque mois au koala pour y parvenir ?

22 Un réseau de lignes de bus qui relie cinq villages A, B, C, D et E est représenté par un graphe dont la matrice est, avec les villes dans l'ordre alphabétique :

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Par exemple, $m_{12} = m_{21} = 1$ signifie que les villages A et B sont directement reliés et $m_{13} = m_{31} = 0$ que les villages A et C ne sont pas directement reliés.
Quels villages ne sont pas reliés en au plus cinq arrêts ?

23 La firme FEZ lance une campagne de publicité pour augmenter les ventes d'un produit qu'elle commercialise et que seulement 30 % des clients lui achètent. Elle apprend qu'au bout d'une semaine :

- 20 % des clients qui achetaient à la concurrence achètent maintenant chez FEZ ;
- 10 % des clients qui achetaient chez FEZ achètent maintenant à la concurrence.

On suppose que le comportement des clients ne change pas. La campagne de FEZ fonctionnera-t-elle ? Si oui, déterminer à partir de combien de semaines.

PROBLÈMES DE SYNTHÈSE

Pour les exercices **1** et **2** relatifs au **chiffrement de Hill**, on utilisera la table de correspondance suivante.

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

1 D'après Bac (Antilles-Guyane - septembre 2013)

Partie A

On considère l'algorithme suivant :

```
1.  A et X sont des entiers
2.  Saisir un entier positif A
3.  Affecter à X la valeur de A
4.  Tant que X supérieur ou égal à 26
5.     Affecter à X la valeur X - 26
6.  Fin du tant que
7.  Afficher X
```

1) Qu'affiche l'algorithme si on saisit : **a)** 3 ? **b)** 55 ?

2) Pour un entier saisi quelconque, que représente le résultat fourni par l'algorithme ?

Partie B

On code un bloc de deux lettres selon la procédure suivante où x_1, x_2, y_1, y_2, z_1 et z_2 sont **toujours des entiers naturels inférieurs à 25**.

- On associe au bloc la matrice $\begin{pmatrix} x_1 & x_2 \end{pmatrix}$ où x_1 et x_2 sont fournis par la table de correspondance.
- On calcule $\begin{pmatrix} y_1 & y_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \times C$ où $C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$ est appelée la matrice de codage.
- $\begin{pmatrix} y_1 & y_2 \end{pmatrix}$ donne $\begin{pmatrix} z_1 & z_2 \end{pmatrix}$ telle que $\begin{cases} z_1 \equiv y_1 & [26] \\ z_2 \equiv y_2 & [26] \end{cases}$.
- $\begin{pmatrix} z_1 & z_2 \end{pmatrix}$ est transformée en un bloc de deux lettres en utilisant la table de correspondance.

1) Soit l'exemple suivant où le bloc RE est codé en DP :
RE $\mapsto \begin{pmatrix} 17 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 55 & 93 \end{pmatrix} \mapsto \begin{pmatrix} 3 & 15 \end{pmatrix} \mapsto$ DP
Justifier l'obtention de $\begin{pmatrix} 55 & 93 \end{pmatrix}$ puis $\begin{pmatrix} 3 & 15 \end{pmatrix}$.

2) Soit $\begin{pmatrix} x_1 & x_2 \end{pmatrix}$ et $\begin{pmatrix} x'_1 & x'_2 \end{pmatrix}$ deux matrices qui donnent $\begin{pmatrix} z_1 & z_2 \end{pmatrix}$ par la procédure de codage.

a) Montrer que $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 & [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & [26] \end{cases}$.

b) En déduire que $\begin{cases} x_1 \equiv x'_1 & [26] \\ x_2 \equiv x'_2 & [26] \end{cases}$ puis $\begin{cases} x_1 = x'_1 \\ x_2 = x'_2 \end{cases}$.

3) On souhaite décoder DP pour revenir à DP.

a) Vérifier que $C^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

b) Calculer $\begin{pmatrix} y_1 & y_2 \end{pmatrix} = \begin{pmatrix} 3 & 15 \end{pmatrix} C^{-1}$.

c) Calculer $\begin{pmatrix} x_1 & x_2 \end{pmatrix}$ tels que $\begin{cases} x_1 \equiv y_1 & [26] \\ x_2 \equiv y_2 & [26] \end{cases}$.

4) On cherche à généraliser une procédure de décodage pour passer de $\begin{pmatrix} z_1 & z_2 \end{pmatrix}$ à $\begin{pmatrix} x_1 & x_2 \end{pmatrix}$.
Soit $\begin{pmatrix} y'_1 & y'_2 \end{pmatrix} = \begin{pmatrix} z_1 & z_2 \end{pmatrix} C^{-1}$.
Soit $\begin{pmatrix} x_1 & x_2 \end{pmatrix}$ telle que $\begin{cases} x_1 \equiv y'_1 & [26] \\ x_2 \equiv y'_2 & [26] \end{cases}$.
Montrer que $\begin{cases} 3x_1 + x_2 \equiv z_1 & [26] \\ 5x_1 + 2x_2 \equiv z_2 & [26] \end{cases}$.

5) Conclure et décoder QC.

2 D'après Bac (Centres Étrangers - 2014)

Partie A

On donne les matrices :

$$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}, X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ et } Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

1) Calculer la matrice $6A - A^2$.

2) En déduire que A est inversible et déterminer les réels α et β tels que $A^{-1} = \alpha I + \beta A$.

3) Vérifier que : $B = 5A^{-1}$.

4) Démontrer que si $AX = Y$, alors $5X = BY$.

Partie B

On code deux lettres selon la procédure suivante :

- On associe aux deux lettres la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 et x_2 sont fournis par la table de correspondance.
- X donne $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que $Y = AX$.
- Y donne $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ où r_1 et r_2 sont les restes de la division euclidienne par 26 de y_1 et y_2.
- Les entiers r_1 et r_2 donnent alors les deux lettres codées par la table de correspondance.

Exemple : OU $\mapsto \begin{pmatrix} 14 \\ 20 \end{pmatrix} \mapsto \begin{pmatrix} 76 \\ 82 \end{pmatrix} \mapsto \begin{pmatrix} 24 \\ 4 \end{pmatrix} \mapsto$ YE

On admet que 21 est l'unique entier k tel que :

$$0 \leqslant k \leqslant 25 \quad \text{et} \quad 5k \equiv 1 \ [26].$$

1) Coder le mot `ET`.
2) Démontrer que : $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$.
3) En utilisant la question 3 de la partie A, établir que :
$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \ [26] \\ x_2 \equiv 15y_1 + 6y_2 \ [26] \end{cases}.$$
4) Décoder le mot `QP`.

3 Arbre de Stern-Brocot

L'arbre de Stern-Brocot est une représentation de tous les rationnels strictement positifs, sous forme de fractions irréductibles.

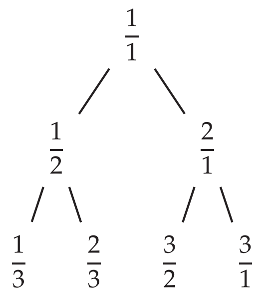
Il a été découvert presque simultanément par le mathématicien allemand Moritz Stern et l'horloger français Achille Brocot.

Initialement, on pose $\dfrac{a}{b} = \dfrac{0}{1} = 0$ et $\dfrac{a'}{b'} = \dfrac{1}{0} = +\infty$.

Ensuite, on répète à l'infini le procédé suivant :

« Insérer $\dfrac{a+a'}{b+b'}$ entre $\dfrac{a}{b}$ et $\dfrac{a'}{b'}$. »

Ainsi, après trois étapes, l'arbre est :



Partie A : Irréductibilité et unicité

1) a) Construire l'arbre jusqu'à l'étape 4.
   b) Écrire dans l'ordre croissant toutes les fractions obtenues de l'étape 0 à l'étape 4.
2) Rappeler la définition d'une fraction irréductible.
3) On souhaite démontrer par récurrence que si $\dfrac{a}{b}$ et $\dfrac{a'}{b'}$ sont deux fractions consécutives à la n-ième étape, alors $a'b - ab' = 1$.
   a) Vérifier la propriété au rang 0.
   b) Supposons la propriété vraie au rang p. Calculer :
   $$a(b+b') - b(a+a') \text{ et } (a+a')b' - (b+b')a'.$$
   En déduire que la propriété est héréditaire.
   c) Utiliser le théorème de Bézout pour conclure.
4) On admet l'existence, c'est-à-dire que toute fraction irréductible existe dans l'arbre.
   On veut montrer l'unicité, c'est-à-dire montrer qu'aucune fraction n'apparaît plus d'une fois dans l'arbre.
   a) Soit deux fractions $\dfrac{a}{b}$ et $\dfrac{a'}{b'}$ de l'arbre.
   Démontrer que $\dfrac{a}{b} < \dfrac{a+a'}{b+b'} < \dfrac{a'}{b'}$.
   b) En déduire l'unicité.

Partie B : Représentation matricielle

Étant donné que l'arbre représente chaque nombre de manière unique, il existe un seul chemin qui mène à une fraction irréductible donnée. Si on appelle G et D les branches de l'arbre qui vont respectivement à gauche et à droite, on peut traduire tout chemin par un mot.

1) a) Déterminer la fraction associée au mot GDG.
   b) Déterminer le mot associé à la fraction $\dfrac{5}{3}$.
2) Soit deux fractions de l'arbre $\dfrac{a}{b}$ et $\dfrac{a'}{b'}$ et les matrices
   $M = \begin{pmatrix} a & a' \\ b & b' \end{pmatrix}$ et $U = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.
   Déterminer les matrices $\hat{G}$ et $\hat{D}$ telles que :
   $$M\hat{G} = \begin{pmatrix} a & a+a' \\ b & b+b' \end{pmatrix} \text{ et } M\hat{D} = \begin{pmatrix} a+a' & a' \\ b+b' & b' \end{pmatrix}.$$
3) On identifie la fraction $\dfrac{a}{b}$ à la matrice $\begin{pmatrix} a \\ b \end{pmatrix}$.
   a) Calculer $\hat{G}\hat{D}\hat{G}U$. À quoi cela correspond-il ?
   b) D'après le résultat de la question 1b, exprimer $\begin{pmatrix} 5 \\ 3 \end{pmatrix}$ comme produit de facteurs $\hat{G}$, $\hat{D}$ et U.
4) Démontrer que, pour tout $n \in \mathbb{N}$:
   a) $\hat{D}^n U$ est associée à $n+1$;
   b) $\hat{G}^n U$ est associée à l'inverse de $n+1$.

4 D'après Bac (Asie - 2015)

On dit qu'un entier naturel non nul N est un nombre triangulaire s'il existe un entier naturel n tel que : $N = 1 + 2 + \ldots + n$.

Par exemple, 10 est triangulaire car $10 = 1 + 2 + 3 + 4$.

Le but de ce problème est de déterminer des nombres triangulaires qui sont les carrés d'un entier.

On rappelle que, pour tout entier naturel non nul n :

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Partie A : Nombres triangulaires carrés

1) Montrer que 36 est un nombre triangulaire, et qu'il est aussi le carré d'un entier.

2) a) Montrer que le nombre $1+2+\ldots+n$ est le carré d'un entier si, et seulement si, il existe un entier naturel p tel que : $n^2+n-2p^2=0$.

b) En déduire que le nombre $1+2+\ldots+n$ est le carré d'un entier si, et seulement si, il existe un entier naturel p tel que : $(2n+1)^2-8p^2=1$.

Partie B : Étude d'une équation diophantienne

On considère (E) l'équation diophantienne :

$$x^2-8y^2=1$$

où x et y désignent deux entiers relatifs.

1) Donner deux couples d'entiers naturels inférieurs à 10 qui sont solution de (E).

2) Démontrer que, si $(x\,;\,y)$ est solution de (E), alors x et y sont premiers entre eux.

Partie C : Lien avec le calcul matriciel

Soit deux entiers relatifs x et y, la matrice $A=\begin{pmatrix}3&8\\1&3\end{pmatrix}$ et deux entiers relatifs x' et y' tels que $\begin{pmatrix}x'\\y'\end{pmatrix}=A\begin{pmatrix}x\\y\end{pmatrix}$.

1) Exprimer x' et y' en fonction de x et de y.

2) Déterminer la matrice A^{-1}, puis exprimer x et y en fonction de x' et y'.

3) Démontrer que $(x\,;\,y)$ est solution de (E) si et seulement si $(x'\,;\,y')$ est solution de (E).

4) On définit les suites (x_n) et (y_n) par $x_0=3$ et $y_0=1$ et, pour tout entier naturel n, $\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=A\begin{pmatrix}x_n\\y_n\end{pmatrix}$.

On admet que, pour tout $n\in\mathbb{N}$, x_n et y_n sont des entiers naturels.

Démontrer par récurrence que, pour tout $n\in\mathbb{N}$, le couple $(x_n\,;\,y_n)$ est solution de (E).

Partie D : Retour au problème initial

À l'aide des parties précédentes, déterminer un nombre triangulaire supérieur à 2 015 qui est le carré d'un entier.

5 Un code d'entrée d'immeuble noté $\overline{abcdk}$ est constitué de cinq chiffres décimaux :

- les quatre premiers chiffres a, b, c, d forment l'identifiant de chaque locataire ;
- le cinquième chiffre k est une clé de contrôle.

Lorsqu'un code est tapé au clavier, un ordinateur fait un test puis un autre si le premier est réussi :

- **TEST1** : vérification de la validité du code.
- **TEST2** : authentification d'un locataire.

Voici l'algorithme de TEST 1 (où `a%b` donne le reste de la division euclidienne de a par b).

`A est une matrice carrée d'ordre 2`
`U est une matrice ligne de taille 2`
`V est une matrice colonne de taille 2`
`a, b, c, d, r, k sont entiers naturels`
`U prend la valeur` $\begin{pmatrix}2\\3\end{pmatrix}$
`V prend la valeur` $\begin{pmatrix}1&2\end{pmatrix}$
`Afficher "Entrez votre code :"`
`Saisir a, b, c, d, k`
`A prend la valeur` $\begin{pmatrix}\mathtt{a}&\mathtt{b}\\\mathtt{c}&\mathtt{d}\end{pmatrix}$
`r prend la valeur V*A*U+k`
`Si R%7=0 alors TEST2`

1) Tester l'algorithme avec le code 49173.
Est-ce un code valide ?

2) Soit un code $\overline{abcdk}$ et $n=2a+3b+4c+6d+k$.
Démontrer que si le code est valide, alors $n\equiv 0\ [7]$.

3) Un locataire entre le code 14135 qui est refusé.
Cependant, il n'est pas sûr du premier chiffre.
a) Déterminer un chiffre z tel que $2z\equiv 3\ [7]$.
b) Retrouver le premier chiffre du code du locataire.

4) Un autre locataire intervertit les 2e et 3e chiffres de son code. Pourra-t-il entrer ?

5) Un troisième locataire entre un code en se trompant sur le premier chiffre mais la porte s'ouvre quand même.
Expliquer comment cela est possible.

QCM BILAN

Pour chaque question, déterminer la ou les réponse(s) exacte(s). Justifier.

1 On considère dans l'ensemble des entiers relatifs l'équation : $x^2 - x + 4 \equiv 0 \ [6]$.

a) Toutes les solutions sont des entiers pairs.
b) Il n'y a aucune solution.
c) Les solutions vérifient $x \equiv 2 \ [6]$.
d) Les solutions vérifient $x \equiv 2 \ [6]$ ou $x \equiv 5 \ [6]$.

2 On se propose de résoudre l'équation (E) : $\text{PGCD}(3n + 4 \ ; \ 4n + 3) = 7$.

a) Les solutions de (E) sont de la forme $n \equiv 0 \ [7]$.
b) Les solutions de (E) sont de la forme $n \equiv 1 \ [7]$.
c) Les solutions de (E) sont de la forme $n \not\equiv 1 \ [7]$.
d) L'équation (E) n'a pas de solution.

3 On se propose de résoudre l'équation (E) : $24x + 34y = 2$, où x et y sont des entiers relatifs.

a) Les solutions de (E) sont toutes de la forme : $(x \ ; \ y) = (34k - 7 \ ; \ 5 - 24k)$, pour $k \in \mathbb{Z}$.
b) L'équation (E) n'a aucune solution.
c) Les solutions de (E) sont toutes de la forme : $(x \ ; \ y) = (17k - 7 \ ; \ 5 - 12k)$, pour $k \in \mathbb{Z}$.
d) Les solutions de (E) sont toutes de la forme : $(x \ ; \ y) = (-7k \ ; \ 5k)$, pour $k \in \mathbb{Z}$.

4 On considère les deux nombres $n = 1\,789$ et $p = 1\,789^{2\,017}$. On a alors :

a) $n \equiv 4 \ [17]$ et $p \equiv 0 \ [17]$.
b) p est un nombre premier.
c) $p \equiv 4 \ [17]$.
d) $p \equiv 1 \ [17]$.

5 Soit le nombre $A_n = 2^n + 3^n + 4^n + 5^n + 6^n$ pour $n \in \mathbb{N}$. On a alors :

a) $A_{2\,017} \equiv 3 \ [17]$.
b) $A_{2\,017} \equiv 4 \ [17]$.
c) $A_{2\,017} \equiv 5 \ [17]$.
d) $A_{2\,017} \equiv 6 \ [17]$.

6 Laquelle, parmi les phrases suivantes, est incorrecte.

a) Si $\text{PGCD}(a; b) = 1$ alors, $\text{PGCD}(a^2; b^2) = 1$.
b) Si $(a^2 + ab - b^2)^2 = 1$ alors, a et b sont premiers entre eux.
c) 25 037 n'est pas un nombre premier.
d) $x^2 + x + 1 \equiv 0 \ [7]$ si, et seulement si $x \equiv 2 \ [7]$.

7 Soit a et b deux nombres premiers entre eux.

a) $a + b$ et $2ab$ sont premiers entre eux.
b) a^2 et b^2 sont premiers entre eux.
c) $a + b$ et $a^2 - ab + b^2$ sont premiers entre eux ou divisibles par 3.
d) Il existe un couple $(a \ ; \ b)$ tel que $a + b$ et $a^2 - ab + b^2$ sont divisibles par 6.

8 On lance une pièce équilibrée et on veut obtenir au moins quatre fois consécutives le même résultat. On a plus d'une chance sur deux d'y parvenir à partir d'un nombre de lancers égal à :

(a) 5 (b) 11 (c) 17 (d) 23

9 Une matrice de transition M vérifie : $M\begin{pmatrix}0,5\\0,5\end{pmatrix} = \begin{pmatrix}0,45\\0,55\end{pmatrix}$ et $M\begin{pmatrix}0,2\\0,8\end{pmatrix} = \begin{pmatrix}0,24\\0,76\end{pmatrix}$.

Alors M^2 est égale à :

(a) $\begin{pmatrix}2/3 & 1/6\\1/3 & 5/6\end{pmatrix}$ (b) $\begin{pmatrix}0,64 & 0,0784\\0,36 & 0,9216\end{pmatrix}$ (c) $\begin{pmatrix}4/9 & 3/7\\5/9 & 4/7\end{pmatrix}$ (d) $\begin{pmatrix}0,66 & 0,17\\0,34 & 0,83\end{pmatrix}$

10 Dans un repère orthonormé de l'espace, soit deux plans $\mathscr{P} : 2x+3y+4z=5$ et $\mathscr{Q} : x+2y+7z=1$. Soit la matrice $A = \begin{pmatrix}2 & 3\\1 & 2\end{pmatrix}$ et son inverse $A^{-1} = \begin{pmatrix}2 & -3\\-1 & 2\end{pmatrix}$. L'intersection des deux plans est :

(a) vide

(b) une droite d'équation cartésienne :
$$\begin{cases}x=2t-1\\y=-3t+2 \quad \text{pour } t\in\mathbb{R}\\z=t\end{cases}$$

(c) une droite d'équation cartésienne :
$$\begin{cases}x=-2t+1\\y=3t-2 \quad \text{pour } t\in\mathbb{R}\\z=t\end{cases}$$

(d) une droite d'équation cartésienne :
$$\begin{cases}x=13t+7\\y=-10t-3 \quad \text{pour } t\in\mathbb{R}\\z=t\end{cases}$$

11 Si A et B sont deux matrices carrées non nulles d'ordre n telles que $AB=\lambda I_n$ où $\lambda\in\mathbb{R}$, alors :

(a) il existe λ tel que A n'est pas inversible

(b) pour tout $\lambda\neq 0$, $B^{-1}=\dfrac{1}{\lambda}A$

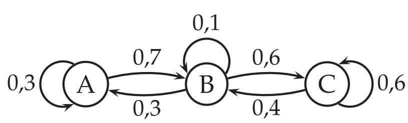
(c) pour tout $\lambda\neq 0$, $A^{-1}=B$

(d) pour tout λ, $BA=\lambda I_n$

12 Soit la matrice $A=\begin{pmatrix}1 & 1 & 2a\\2 & 1 & 1\\1 & 1 & 3a\end{pmatrix}$. Déterminer la valeur de a pour laquelle la matrice n'est pas inversible.

(a) $a=1$ (b) $a=0,5$ (c) $a=\dfrac{1}{3}$ (d) $a=0$

13 Une marche aléatoire entre trois états A, B et C est définie par le graphe suivant :



L'état initial est l'état A. La probabilité d'être dans l'état B à l'étape 5 vaut à 10^{-3} :

(a) 0,151 (b) 0,334 (c) 0,343 (d) 0,353

14 A et B sont deux usines. Chaque année, 44 % des ouvriers de A rejoignent B et 4 % des ouvriers de B rejoignent A. Aujourd'hui, A et B ont 3 000 ouvriers chacune mais dans un futur lointain :

(a) A n'aura plus d'ouvriers

(b) la répartition sera la même

(c) B comptera environ 2 750 ouvriers

(d) A comptera environ 11 ouvriers

Matrices : opérations

Connaissances nécessaires à ce chapitre

- ▶ Utiliser la notation indicielle
- ▶ Résoudre un système linéaire d'équations

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Auto-évaluation

1 Dans la gravure *La Melancolia* d'Albrecht Dürer, on peut voir le tableau de 4 lignes et de 4 colonnes suivant :

On écrit un système correspondant à ce tableau où le second membre est toujours égal à 34 :

$$\begin{cases} 16x+3y+2z+13t &= 34 \\ 5x+10y+11z+8t &= 34 \\ 9x+6y+7z+12t &= 34 \\ 4x+15y+14z+t &= 34 \end{cases}$$

1) Vérifier que $(1\,;\,1\,;\,1\,;\,1)$ est solution de ce système.

2) Soit $a_{i,j}$ le coefficient situé dans la i-ième ligne et la j-ième colonne. Montrer que $\displaystyle\sum_{i=1}^{4} a_{i,i} = \sum_{i=1}^{4} a_{5-i,i}$.

3) La i-ième ligne du tableau devient la i-ième colonne d'un nouveau tableau.
Écrire le nouveau système correspondant où le second membre est toujours égal à 34.

2

1) Résoudre les systèmes linéaires suivants :

a) $\begin{cases} 5x+2y=-4 \\ 7x+3y=6 \end{cases}$ **c)** $\begin{cases} 12x+15y=112,5 \\ 8x+10y=75 \end{cases}$

b) $\begin{cases} 3x-9y=-1 \\ -2x+6y=1 \end{cases}$ **d)** $\begin{cases} 2x+y=5 \\ 3x+2y=7 \end{cases}$

2) Que peut-on dire des tableaux suivants ?

5	2
7	3

3	−9
−2	6

12	15
8	10

2	1
3	2

3 On se place dans un repère du plan.

1) Démontrer que les droites (d') : $x+y=3$, (d) : $x=2$ et (d'') : $y=2x-3$ sont concourantes.

2) Soit trois points $A(1\,;\,1)$, $B(7\,;\,1)$ et $C(3\,;\,3)$.
Déterminer les coordonnées du centre de gravité du triangle ABC.

4 Déterminer le polynôme P de degré 2 vérifiant les conditions données.

1) $P(0)=-1$, $P(0,5)=1$ et $P(-2)=1$.

2) $P(1)=1$, $P'(1)=1$ et $P(-1)=0$.

➤➤➤ Voir solutions p. 151

Activités d'approche

ACTIVITÉ 1 Notion de matrice

Dans le tableau à double entrée ci-dessous figurent les quantités de quatre types de produits (sandwichs, burgers, pizzas, kebabs) commandées quotidiennement par le gérant d'un snack chez trois fournisseurs (Macrofood, Producoin et Oresto) au cours du premier trimestre.

	sandwichs	burgers	pizzas	kebabs
Macrofood	25	20	20	45
Producoin	10	10	0	20
Oresto	5	5	10	15

Partie A : Former une matrice

En plaçant les nombres tels qu'ils sont disposés dans le tableau entre deux grandes parenthèses, on forme un objet mathématique qu'on appelle **matrice**. On nomme cette matrice A.

$$A = \begin{pmatrix} 25 & 20 & 10 & 45 \\ 10 & 10 & 0 & 20 \\ 5 & 5 & 20 & 15 \end{pmatrix}$$

1) La **taille** d'une matrice est donnée sous la forme : nombre de lignes $\times$ nombre de colonnes. Déterminer la taille de la matrice A.

2) On note a_{ij} et on appelle **coefficient** le nombre situé dans la i-ième ligne et la j-ième colonne. Quel est le coefficient a_{21} ? À quoi correspond t-il ?

3) Faire un second tableau qui présente les mêmes informations que le premier en permutant les lignes et les colonnes. Écrire la matrice A' correspondante.
A' est appelée **transposée** de A et on la note A^{T}.

4) À quel coefficient de A le coefficient a'_{ij} de A' est-il égal ?

Partie B : Opérer avec les matrices

Dans toute la suite, on considère que les lignes des matrices sont associées aux fournisseurs et les colonnes aux produits.

1) Au 2^{e} trimestre, le gérant augmente de 40 % les quantités commandées au 1er trimestre.

- **a)** Sur le modèle de la matrice A, écrire la matrice B correspondante aux nouvelles données.
- **b)** Écrire la matrice donnant le nombre de produits commandés chez Macrofood.
  Donner sa taille.
- **c)** Écrire la matrice donnant le nombre de sandwichs commandés chez chaque fournisseur.
  Donner sa taille.

2) Écrire la matrice C représentant les quantités commandées au 1er semestre.
Comment peut-on obtenir C à partir de A et B ?

3) Au 3^{e} trimestre, le gérant diminue de 20 % les quantités commandées au 1er trimestre.

- **a)** Écrire la matrice D correspondant aux nouvelles données.
- **b)** Déterminer la matrice E représentant la quantité moyenne de produits commandés par mois chez chaque fournisseur.
  Comment peut-on obtenir cette matrice E à partir des matrices C et D ?

ACTIVITÉ 2 Produit de deux matrices

Pour rejoindre leur spot de surf à Lacanau, trois amis (Ulrich, Manolo et Jules) passent chacun un certain temps (en heures) dans différents moyens de transports conformément au tableau ci-contre.

	Avion	Train	Voiture
Ulrich	0	6	1,5
Manolo	1,5	0	0,3
Jules	1	1	0,1

Ci-après, la matrice T représente les temps du tableau et la matrice colonne V la vitesse moyenne (en $\text{km} \cdot \text{h}^{-1}$) de chaque moyen de transport (de haut en bas : avion, train, voiture).

$$T = \begin{pmatrix} 0 & 6 & 1,5 \\ 1,5 & 0 & 0,3 \\ 1 & 1 & 0,1 \end{pmatrix} \qquad V = \begin{pmatrix} 750 \\ 210 \\ 90 \end{pmatrix}$$

1) a) Déterminer la distance totale parcourue par chaque ami et inscrire les résultats dans une matrice colonne D (de haut en bas, Ulrich, Manolo et Jules).

b) Exprimer le coefficient d_{ij} de D en fonction des coefficients des matrices T et V.
On dit que la matrice D est le produit de la matrice T par la matrice V. On note $D = TV$.

2) À partir du tableau ci-contre qui donne l'impact CO_2 (en kg) et le prix (en €) pour une heure passée dans chaque moyen de transport, on souhaite calculer l'impact et le prix du trajet de chacun des amis.

	Impact CO_2	Prix
Avion	111	172,5
Train	0,546	33,6
Voiture	1,035	5,4

a) Écrire la matrice M de taille 3×2 correspondant au tableau ci-dessus.

b) Calculer la matrice produit TM en fusionnant le produit de T par la première colonne de M, puis le produit de T par la deuxième colonne de M.

c) Qui a fait le trajet le plus économique ? le plus écologique ?

3) a) On utilise un tableur (voir ci-dessous). Quelle formule doit-on inscrire dans la cellule D4 et étendre dans la plage de couleur bleu pour retrouver les résultats précédents ?

	A	B	C	D	E	F
1				750	111	172,5
2				210	0,546	33,6
3				90	1,035	5,4
4	0	6	1,5			
5	1,5	0	0,3			
6	1	1	0,1			

b) Écrire l'égalité de matrices relative à la feuille de calcul sous la forme $\begin{pmatrix} \cdots \\ \cdots \end{pmatrix}\begin{pmatrix} \cdots \\ \cdots \end{pmatrix}=\begin{pmatrix} \cdots \\ \cdots \end{pmatrix}$.

4) L'an prochain, Ulrich, Manolo et Jules partiront à Honolulu avec Hermine, une surfeuse rencontrée à Lacanau. Le tableau ci-contre fournit les temps (en heures) qu'ils passeront dans les transports pour rejoindre leur destination.

	Avion	Train	Voiture
Ulrich	15,25	0	5,8
Manolo	15	0	3
Jules	15	3	0,8
Hermine	15,5	0,5	0,1

a) Utiliser un tableur pour déterminer qui a fait le trajet le moins long, qui a fait le trajet le moins écologique et qui a fait le trajet le moins économique.

b) Écrire l'égalité de matrices relative au calcul précédent.

ACTIVITÉ 3 Inverse d'une matrice

ALGO

Un professeur a donné à ses élèves l'énoncé suivant :

> Alix demande à son ami grec Enak de penser à deux nombres et de lui donner dans l'ordre les résultats de :
> - la somme du triple de son premier et du quintuple de son second ;
> - la somme de son premier et du double de son second.
>
> Après quelques calculs, Alix étonne Enak en lui révélant les nombres qu'il a choisis !
> Écrire un algorithme et le programmer pour aider Alix à ne plus se fatiguer.

Élise a réussi l'exercice. Elle met son amie Lilou dans la peau d'Enak qui vérifie que cela fonctionne. « Passe-moi ton programme ! » dit-elle. Mais Élise, qui ne veut pas trop l'aider, ne lui montre que l'algorithme ci-contre.

```
1.  x, y, r, s sont des réels
2.  Saisir r, s
3.  Affecter à x la valeur 2r-5s
4.  Affecter à y la valeur -r+3s
5.  Afficher x, y
```

Partie A : Inverser les rôles

1) Se mettre dans la peau d'Enak et tester si l'algorithme fonctionne.

2) Soit les matrices colonnes $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $R = \begin{pmatrix} r \\ s \end{pmatrix}$.

a) Déterminer la matrice carrée M d'ordre 2 (*i. e.* de taille 2×2) telle que $MX = R$.

b) En s'aidant de l'algorithme, déterminer la matrice carrée N d'ordre 2 telle que $NR = X$.

c) On dit que A et B, deux matrices carrées d'ordre 2, sont **inverses** l'une de l'autre si $AB = BA = I_2$ où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est la matrice **identité** d'ordre 2.

Démontrer que M et N sont inverses l'une de l'autre.

Partie B : Existence de l'inverse

1) Soit deux matrices $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$ telles que $AB = I_2$.

a) Montrer qu'on peut écrire deux systèmes linéaires de deux équations à deux inconnues, x et y pour l'un, x' et y' pour l'autre.

b) Expliquer pourquoi ces deux systèmes admettent une unique solution.

c) Déterminer les valeurs de x, x', y et y' en résolvant les systèmes d'équations.

d) Vérifier alors que $BA = I_2$. En déduire que B est l'inverse de A.

2) Soit les matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$ telles que $AB = I_2$.

a) Montrer qu'on peut écrire deux systèmes linéaires de deux équations à deux inconnues, x et y pour l'un, x' et y' pour l'autre.

b) Déterminer une condition nécessaire et suffisante portant sur a, b, c et d pour que les deux systèmes précédents admettent chacun une solution unique.

c) Dans le cas où la condition établie précédemment est réalisée, résoudre les deux systèmes.

En déduire que la matrice $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est l'inverse de A.

1. Définitions et vocabulaire

DÉFINITION : Matrice

Une **matrice** de **taille** $m \times n$ est un tableau de nombres formé de m lignes et n colonnes qui s'écrit sous la forme :

$$\begin{array}{cc} & n \text{ colonnes} \\ m \text{ lignes} & \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \end{array}$$

Le nombre a_{ij} (avec $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$) est situé dans la i-ième ligne et la j-ième colonne. Il est appelé un **coefficient** de la matrice.

REMARQUE : En général, on note une matrice avec une lettre majuscule ou avec le coefficient général entre parenthèses, par exemple (a_{ij}).
Si $i > 9$ ou $j > 9$, on écrira par exemple $a_{1,11}$ et pas a_{111} pour éviter la confusion avec $a_{11,1}$.

Exemple Soit $A = (a_{ij})$ la matrice de taille 2×3 égale à $\begin{pmatrix} 4 & 7 & -5 \\ 3 & -1 & 8 \end{pmatrix}$.
Le coefficient a_{12} vaut 7. Le coefficient a_{21} vaut 3.

DÉFINITION : Matrice ligne, matrice colonne, matrice carrée

- Une matrice de taille $1 \times n$ est appelée **matrice ligne** de taille n.
- Une matrice de taille $n \times 1$ est appelée **matrice colonne** de taille n.
- Une matrice de taille $n \times n$ est appelée **matrice carrée** d'**ordre** n.

Exemple $A = \begin{pmatrix} 4 & -2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 4 \\ -2 \end{pmatrix}$ et $C = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ sont respectivement une matrice ligne de taille 3, une matrice colonne de taille 2 et une matrice carrée d'ordre 2.

DÉFINITION : Matrices égales

Deux matrices $A = (a_{ij})$ et $B = (b_{ij})$ sont **égales** si elles ont la même taille $m \times n$ et si, pour tout couple $(i\,;\,j)$ tel que $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$, on a $a_{ij} = b_{ij}$.

DÉFINITION : Matrice diagonale

Une **matrice diagonale** (a_{ij}) est une matrice carrée dont les coefficients à l'extérieur de la **diagonale principale** sont nuls, c'est-à-dire tels que $a_{ij} = 0$ pour $i \neq j$.

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix}$$

REMARQUE : Une matrice diagonale se note aussi $\mathbf{diag}(a_1, a_2, \ldots, a_n)$.
Dans une matrice diagonale, un ou plusieurs coefficients a_i peuvent être nuls.

DÉFINITION : Matrice identité

La **matrice identité d'ordre n** est la matrice diagonale d'ordre n, notée I_n, dont la diagonale principale ne contient que des 1.

Exemple L'identité d'ordre 3 est $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On peut aussi la noter $\text{diag}(1,1,1)$.

REMARQUE : S'il n'y a pas d'ambiguïté, on note l'identité I sans préciser son ordre en indice.

DÉFINITION : Matrice transposée

La **matrice transposée** d'une matrice A de taille $m \times n$ est la matrice notée A^{T}, de taille $n \times m$, obtenue en échangeant les lignes et les colonnes de A.

Exemple $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$; $\begin{pmatrix} 0{,}3 & 0{,}7 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} 0{,}3 \\ 0{,}7 \end{pmatrix}$.

2. Opérations sur les matrices

A. Somme de deux matrices

DÉFINITION : Somme de deux matrices

Soit $A = (a_{ij})$ et $B = (b_{ij})$ deux matrices de même taille $m \times n$.
La **somme** des matrices A et B est la matrice notée $A + B$ définie par :
$A + B = (c_{ij})$ avec $c_{ij} = a_{ij} + b_{ij}$ pour tout couple $(i\ ;\ j)$ tel que $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$.

Exemple Soit $A = \begin{pmatrix} -3 & 5 \\ -1 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -5 \\ 4 & 0 \end{pmatrix}$. $A + B = \begin{pmatrix} -3+2 & 5-5 \\ -1+4 & 3+0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 3 & 3 \end{pmatrix}$.

PROPRIÉTÉ

Soit A, B, C trois matrices de même taille.
- $A + B = B + A$ (commutativité)
- $(A + B) + C = A + (B + C)$ (associativité)

DÉFINITION : Différence de deux matrices

Soit A et B deux matrices de même taille.
La **différence** des matrices A et B est la matrice notée $A - B$ égale à la somme $A + (-B)$ où $-B$ est la matrice **opposée** de B dont les coefficients sont les opposés des coefficients de B.

Exemple Soit $A = \begin{pmatrix} -3 & 5 \\ -1 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -5 \\ 4 & 0 \end{pmatrix}$.
$A - B = A + (-B) = \begin{pmatrix} -3 & 5 \\ -1 & 3 \end{pmatrix} + \begin{pmatrix} -2 & 5 \\ -4 & 0 \end{pmatrix} = \begin{pmatrix} -3-2 & 5+5 \\ -1-4 & 3+0 \end{pmatrix} = \begin{pmatrix} -5 & 10 \\ -5 & 3 \end{pmatrix}$.

B. Produit d'une matrice par un réel

DÉFINITION : Produit d'une matrice par un réel

Soit A une matrice et k un nombre réel.
Le **produit** de A par le réel k est la matrice notée kA dont les coefficients sont obtenus en multipliant tous les coefficients de A par k.

Exemple $A = \begin{pmatrix} 3,5 & -5 & 2,5 \\ -1 & 0,5 & -5,5 \end{pmatrix}$.
Alors, $-2A = \begin{pmatrix} -2\times 3,5 & -2\times(-5) & -2\times 2,5 \\ -2\times(-1) & -2\times 0,5 & -2\times(-5,5) \end{pmatrix} = \begin{pmatrix} -7 & 10 & -5 \\ 2 & -1 & 11 \end{pmatrix}$.

PROPRIÉTÉ

Soit A et B deux matrices de même taille et deux réels k et k'.

- $0A = 0$ et $1A = A$
- $k(A+B) = kA + kB$
- $(k+k')A = kA + k'A$
- $(kk')A = k(k'A)$

Remarque : Dans l'égalité $0A = 0$, le 0 de gauche est un réel mais celui de droite désigne la **matrice nulle**, matrice ayant la même taille que A et dont tous les coefficients sont nuls.

C. Produit de deux matrices

DÉFINITION : Produit d'une matrice ligne par une matrice colonne

Le **Produit d'une matrice ligne par une matrice colonne** de la matrice ligne $A = \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}$ par la matrice colonne $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ est noté AB et est égal au réel $\sum_{i=1}^{n} a_i b_i = a_1b_1 + a_2b_2 + \cdots + a_nb_n$.

Exemple Soit $A = \begin{pmatrix} 3 & 0 & -2 \end{pmatrix}$ et $B = \begin{pmatrix} -1 \\ -4 \\ -2 \end{pmatrix}$. $AB = 3\times(-1) + 0\times(-4) - 2\times(-2) = 1$.

DÉFINITION : Produit de deux matrices

Soit A une matrice de taille $m \times n$ et B une matrice de taille $n \times p$.
Le **produit** de A par B, noté AB, est la matrice $C = (c_{ij})$ de taille $m \times p$ telle que c_{ij} est égal au produit de la i-ième ligne de A par la j-ième colonne de B.

Remarques :

- Le produit d'une matrice A par une matrice B n'existe qu'à condition que le nombre de colonnes de A soit égale au nombre de lignes de B.
- Si le produit d'une matrice A par une matrice B existe, en général, il n'est pas commutatif : en premier lieu, BA n'existe pas toujours (il n'existe que si A et B sont des matrices carrées) et, même si c'est le cas, généralement on n'a pas $AB = BA$.

MÉTHODE 1 Multiplier deux matrices

► Ex. 30 p. 97

Pour calculer la matrice C égale à AB, on vérifie que le nombre de colonnes de A est égal au nombre de lignes de B, puis on dispose les matrices suivant le schéma $\begin{array}{c|c} & B \\ \hline A & C \end{array}$ de sorte que c_{ij} soit à l'intersection du prolongement de la i-ème ligne de A et de la j-ième colonne de B.

Exercice d'application Soit $A = \begin{pmatrix} 1 & 3 & 5 & -2 \\ -2 & 0 & -3 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 & -3 \\ 3 & -1 & 0 \\ 0 & -2 & 2 \\ 2 & -3 & -4 \end{pmatrix}$. Calculer AB.

Correction

A est de taille 2×4 et B de taille 4×3.
A a autant de colonnes que B a de lignes, donc
$C = AB$ existe et sa taille est 2×3.
On dispose les matrices comme ci-contre.
On calcule alors, par exemple :
$c_{11} = 1 \times 2 + 3 \times 3 + 5 \times 0 - 2 \times 2 = 7$.

$$\begin{array}{cc} & \begin{pmatrix} 2 & 1 & -3 \\ 3 & -1 & 0 \\ 0 & -2 & 2 \\ 2 & -3 & -4 \end{pmatrix} \\ \begin{pmatrix} 1 & 3 & 5 & -2 \\ -2 & 0 & -3 & 2 \end{pmatrix} & \begin{pmatrix} 7 & -6 & 15 \\ 0 & -2 & -8 \end{pmatrix} \end{array}$$

REMARQUE : Il n'est pas nécessaire que l'une des matrices A ou B soit nulle pour que AB=0.

Exemple Soit $A = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Alors, $AB = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

PROPRIÉTÉS

Soit A, B et C trois matrices compatibles avec les produits écrits ci-après et soit k un réel.

- $(AB)C = A(BC) = ABC$ (associativité)
- $A(B + C) = AB + AC$ et $(A + B)C = AC + BC$ (distributivité)
- $(kA)B = A(kB) = k(AB)$
- $AI = IA = A$ et $A0 = 0A = 0$

D. Puissance d'une matrice carrée

DÉFINITION

Soit A une matrice carrée et n un entier naturel.
La puissance n-ième de A est la matrice notée A^n égale :

- au produit de n facteurs A si $n \neq 0$;
- à la matrice identité I de même ordre que celui de A si $n = 0$.

Exemple Soit $A = \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}$. Alors, $A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $A^2 = \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}$.

On peut démontrer par récurrence que, pout tout $n \in \mathbb{N}$, $A^n = \begin{pmatrix} 2^n & 0 \\ 0 & (-3)^n \end{pmatrix}$.

MÉTHODE 2 Effectuer un calcul matriciel avec la calculatrice

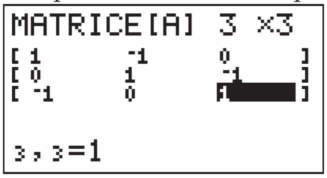
► Ex. 37 p. 98

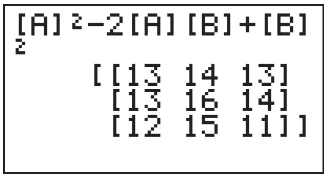
Exercice d'application Soit $A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}$. Calculer $A^2 - 2AB + B^2$.

Correction

Avec une calculatrice TI

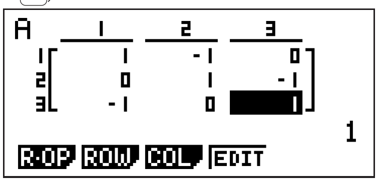
- Entrer dans le mode "Matrice" puis le menu "EDIT".
- Saisir la taille de la matrice A puis ses coefficients. Pour les coefficients négatifs, utiliser la touche "(-)". Faire de même pour B.
- Quitter le mode "Matrice" puis y entrer à nouveau et, dans le menu "NOMS", sélectionner la matrice [A]. Compléter la formule et taper "Entrer".

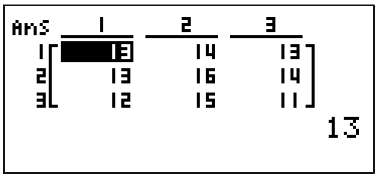




Avec une calculatrice CASIO

- Entrer dans le menu "RUN-MAT" puis choisir ▸MAT (touche F3).
- Saisir la taille de la matrice A puis ses coefficients. Faire de même pour B.
- Quitter ▸MAT, taper la formule en faisant précéder chaque nom de matrice par "Mat" (touches SHIFT puis 2) : Mat A²-2Mat AMat B+Mat B². Exécuter.





3. Matrices inversibles

A. Inverse d'une matrice carrée

DÉFINITION : Inverse d'une matrice carrée

Une matrice carrée A d'ordre n est **inversible** s'il existe une matrice carrée B d'ordre n telle que $AB = BA = I$.
La matrice B, notée A^{-1}, est appelée la **matrice inverse** de A.

Exemple Soit $A = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$ et $B = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$. $AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ donc B est l'inverse de A.

PROPRIÉTÉ

Si une matrice est inversible, alors son inverse est unique.

PREUVE Soit A une matrice inversible ayant deux inverses B et C.
On a $B = BI = B(AC) = (BA)C = IC = C$. Ainsi, $B = C$. Donc, l'inverse de A est unique.

PROPRIÉTÉ

Si $AB = I$, alors A est inversible et $B = A^{-1}$.

Remarque : Il suffit donc seulement de vérifier l'une des égalités $AB = I$ ou $BA = I$ pour montrer que A et B sont inverses l'une de l'autre.

Exemple Soit $A = \begin{pmatrix} 1 & 1 & 0 \\ -2 & -1 & 0 \\ 3 & -2 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & -1 & 0 \\ 2 & 1 & 0 \\ 7 & 5 & 1 \end{pmatrix}$. Alors, $AB = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I$.
Donc A et B sont inverses l'une de l'autre et on a les égalités $A^{-1} = B$ et $B^{-1} = A$.

B. Inverse d'une matrice carrée d'ordre 2

DÉFINITION : Déterminant d'une matrice carrée d'ordre 2

Le **déterminant** de la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est le réel noté $\det(M)$ ou $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ égal à $ad - bc$.

THÉORÈME : Inverse d'une matrice carrée d'ordre 2

- La matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si, et seulement si, $ad - bc \neq 0$.
- Si A est inversible, alors $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

PREUVE Soit $N = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Alors, $MN = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$.

- Si $ad - bc \neq 0$, alors $\dfrac{1}{ad-bc}MN = I \Leftrightarrow M\left(\dfrac{1}{ad-bc}N\right) = I$.
  Donc M est inversible et son inverse est $\dfrac{1}{ad-bc}N = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
- Si $ad - bc = 0$, alors $MN = 0$. Supposons alors que M soit inversible, d'inverse P.
  Alors, on aurait $PMN = IN = N$ et $PMN = P0 = 0$ et donc $N = 0$, ce qui est absurde.

Remarques :

- Toute matrice carrée admet un déterminant et un seul, mais pour un ordre strictement supérieur à 2, il n'existe pas de formule simple pour le calculer et on utilisera une calculatrice ou un logiciel de calcul formel (voir Méthode 4 p. 94).
- Le déterminant non nul est un critère d'inversibilité d'une matrice carrée de tout ordre.

Exemple $A = \begin{pmatrix} 3 & 8 \\ 2 & 6 \end{pmatrix}$. Alors, $\det(A) = \begin{vmatrix} 3 & 8 \\ 2 & 6 \end{vmatrix} = 3 \times 6 - 2 \times 8 = 18 - 16 = 2 \neq 0$.
Ainsi, A est inversible et $A^{-1} = \dfrac{1}{2}\begin{pmatrix} 6 & -8 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & -4 \\ -1 & 1{,}5 \end{pmatrix}$.

4. Résolution d'un système linéaire

PROPRIÉTÉ : Écriture matricielle d'un système

Le système linéaire $\begin{cases} ax+by &= c \\ a'x+b'y &= c' \end{cases}$ a pour écriture matricielle $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ c' \end{pmatrix}$.

PREUVE $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ c' \end{pmatrix} \Leftrightarrow \begin{pmatrix} ax+by \\ a'x+b'y \end{pmatrix} = \begin{pmatrix} c \\ c' \end{pmatrix} \Leftrightarrow \begin{cases} ax+by &= c \\ a'x+b'y &= c' \end{cases}$.

Remarque : Cette propriété se généralise à un système de dimension quelconque.

Exemple $\begin{pmatrix} 2 & -3 & 1 \\ 3 & -2 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 7 \\ -5 \end{pmatrix}$ correspond au système $\begin{cases} 2x-3y+z &= 7 \\ 3x-2y-z &= -5 \end{cases}$.

PROPRIÉTÉ

Soit A une matrice carrée inversible d'ordre n et B une matrice colonne de taille n.
Alors, le système linéaire d'écriture matricielle $AX = B$ admet une unique solution :
le n-uplet correspondant à la matrice colonne $A^{-1}B$.

PREUVE Soit un système linéaire d'écriture matricielle $AX = B$ où A est inversible.
Alors, on a : $AX = B \Leftrightarrow A^{-1}AX = A^{-1}B \Leftrightarrow IX = A^{-1}B \Leftrightarrow X = A^{-1}B$.

MÉTHODE 3 Résoudre un système de deux équations à deux inconnues

► Ex. 68 p. 101

Exercice d'application Résoudre le système linéaire $\begin{cases} 2x+5y &= 8 \\ 3x-4y &= 15 \end{cases}$.

Correction On résout l'équation $AX = B$ où $A = \begin{pmatrix} 2 & 5 \\ 3 & -4 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} 8 \\ 15 \end{pmatrix}$.
On calcule $\det(A) = -4\times 2 - 3\times 5 = -23$. Comme $\det(A) \neq 0$, alors A est inversible.
Donc, l'équation $AX = B$ a pour unique solution $X = A^{-1}B$.
On calcule $X = \dfrac{-1}{23}\begin{pmatrix} -4 & -5 \\ -3 & 2 \end{pmatrix}\begin{pmatrix} 8 \\ 15 \end{pmatrix} = \dfrac{-1}{23}\begin{pmatrix} -4\times 8-5\times 15 \\ -3\times 8+2\times 15 \end{pmatrix} = \begin{pmatrix} 107/23 \\ -6/23 \end{pmatrix}$.
Le système admet donc pour unique solution le couple $\left(\dfrac{107}{23} ; \dfrac{-6}{23}\right)$.

Remarque : Un système linéaire d'écriture matricielle $AX = B$ où A n'est pas inversible a soit une infinité de solutions, soit aucune.

Exemple Le système $\begin{cases} 3x+6y &= a \\ 4x+8y &= b \end{cases}$ s'écrit matriciellement $AX = B$ où $A = \begin{pmatrix} 3 & 6 \\ 4 & 8 \end{pmatrix}$.
Or, $\det(A) = 0$ donc A n'est pas inversible.
Dans le système, multiplions l'équation du haut par 4 et celle du bas par 3. On obtient :
$\begin{cases} 12x+24y &= 4a \\ 12x+24y &= 3b \end{cases}$ ce qui entraîne que $4a = 3b$ toujours vrai, ou jamais.

MÉTHODE 4 Résoudre un système linéaire avec la calculatrice ou un logiciel

► Ex. 70 p. 101

- On passe à l'écriture matricielle du système : $AX = B$.
- On vérifie que le déterminant de A est non nul, pour vérifier l'inversibilité de A.
- On détermine alors A^{-1}, puis le produit $A^{-1}B$ pour obtenir la solution.

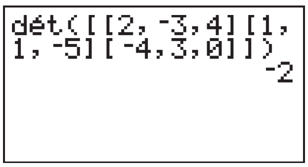
Exercice d'application Résoudre le système linéaire $\begin{cases} 2x - 3y + 4z & = & -1 \\ x + y - 5z & = & 2 \\ -4x + 3y & = & 6 \end{cases}$.

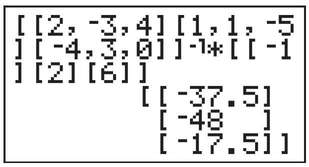
Correction Le système a pour écriture matricielle $AX = B$ avec :

$$A = \begin{pmatrix} 2 & -3 & 4 \\ 1 & 1 & -5 \\ -4 & 3 & 0 \end{pmatrix},\ X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ et } B = \begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}$$

Avec une calculatrice TI

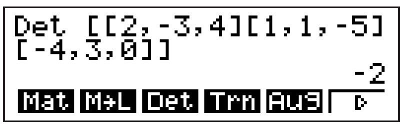
- Entrer dans le mode MATRICE puis dans le menu MATH et choisir la commande dét(.
  Saisir la matrice en utilisant les crochets "[" (touches 2nde ×) et "]" (touches 2nde −). Pour les coefficients négatifs, utiliser la touche (−).
- Faire "préced" (touches 2nde entrer) pour revenir dans l'instruction précédente.
  Supprimer dét(et la parenthèse finale.
  À la suite, appuyer sur la touche x^{-1}, saisir la matrice colonne B et appuyer sur "entrer".

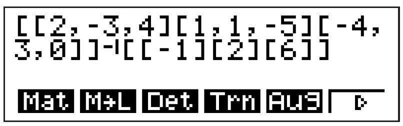


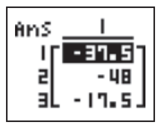


Avec une calculatrice CASIO

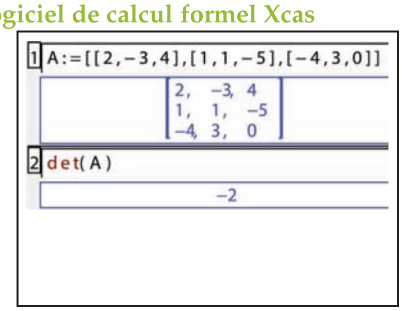
- Appuyer sur la touche OPTN, choisir MAT puis la commande Det.
  Saisir la matrice en utilisant les crochets "[" (touches 2nde +) et "]" (touches 2nde −).
- Appuyer sur la flèche gauche pour revenir dans l'instruction précédente. Supprimer Det.
  À la suite, faire "x^{-1}" (touches SHIFT)), saisir la matrice colonne B et appuyer sur EXE.

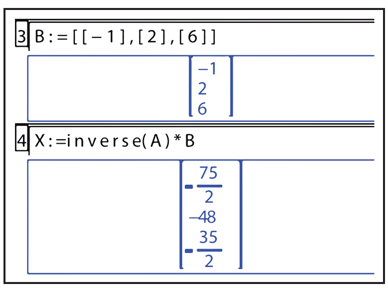






Avec le logiciel de calcul formel Xcas





► Ainsi, $\det(A) = -2 \neq 0$ donc A est inversible et le système admet une unique solution : le triplet $(-37{,}5\ ;\ -48\ ;\ -17{,}5)$.

Activités mentales

Pour les exercices **1** à **6**, déterminer si chaque proposition est vraie ou fausse.

1

1) Une matrice de taille 2×3 a 2 colonnes et 3 lignes.

2) Soit $A = (a_{ij}) = \begin{pmatrix} 3 & 7 & 8 \\ 4 & 1 & 2 \\ 6 & 5 & 9 \end{pmatrix}$. Alors $a_{21} = 7$.

3) Dans la matrice précédente, le coefficient a_{13} vaut 8.

4) $\begin{pmatrix} \frac{1}{3} & 7 \\ 4 & 1 \end{pmatrix}$ est l'inverse de $\begin{pmatrix} 3 & \frac{1}{7} \\ \frac{1}{4} & 1 \end{pmatrix}$.

2 Soit deux matrices de tailles différentes.

1) On peut faire leur somme.

2) On peut faire leur produit.

3) L'une peut être l'inverse de l'autre.

4) L'une peut être la transposée de l'autre.

3 Soit deux matrices de même taille.

1) On peut faire leur somme.

2) On peut faire leur produit.

3) L'une peut être l'inverse de l'autre.

4) L'une peut être la transposée de l'autre.

4 Soit A et B deux matrices carrées de même ordre et non nulles.

1) A peut être l'inverse de B.

2) Le produit AB peut être nul.

3) Le produit AB est une matrice carrée de même ordre.

4) Le produit AB est égal au produit BA.

5

1) La matrice associée à un système linéaire de n équations à p inconnues est une matrice de taille $p \times n$.

2) La matrice représentant les inconnues d'un système linéaire de n équations à p inconnues peut être :

- **a)** une matrice ligne comportant n colonnes ;
- **b)** une matrice ligne comportant p colonnes ;
- **c)** une matrice colonne comportant n lignes ;
- **d)** une matrice colonne comportant p lignes.

6

1) Soit A et B deux matrices. $AB=0 \Rightarrow A=0$ ou $B=0$.

2) $A = \begin{pmatrix} 4 & 21 \\ 6 & 12 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 7 \\ 2 & 4 \end{pmatrix}$. Alors, $A - 3B = 4I_2$.

7 Soit $A = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $B = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ et $C = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$.

Donner la taille des produits suivants, s'ils existent.

1) AB^T **2)** CA **3)** BC **4)** $A^\mathsf{T}C$

8 Soit deux matrices : C carrée, N non carrée.

À quelle condition les matrices suivantes existent-elles ?

1) C^{-1} **3)** CC^T **5)** C^2 **7)** CN

2) N^{-1} **4)** NN^T **6)** N^2 **8)** NC

9 Soit $A = \begin{pmatrix} 11 & 9 & 18 \\ 8 & -23 & 17 \\ 12 & 17 & 80 \end{pmatrix}$.

1) Écrire les coefficients a_{13} et a_{31}.

2) Calculer les sommes :

a) $\displaystyle\sum_{i=1}^{3} a_{ii}$ **b)** $\displaystyle\sum_{i=1}^{3} a_{i2}$ **c)** $\displaystyle\sum_{j=1}^{3} a_{j,4-j}$

10 Sur un stand, on inventorie des T-shirts selon le modèle et la taille. A est la matrice de leurs effectifs où les lignes correspondent aux modèles (dans l'ordre T_1, T_2, T_3) et les colonnes aux tailles (dans l'ordre S, M, L).

$$A = \begin{pmatrix} 5 & 3 & 7 \\ 3 & 9 & 2 \\ 1 & 5 & 4 \end{pmatrix}$$

1) Combien y-a t-il de T-shirts modèle T_3 en taille M ?

2) Que représente la somme $\displaystyle\sum_{i=1}^{3} a_{2i}$? La somme $\displaystyle\sum_{i=1}^{3} a_{i3}$?

Taille et coefficients d'une matrice

11 Dans les matrices schématisées suivantes, chaque point représente un nombre.

$$A=\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad B=\begin{pmatrix} \cdot & \cdot & \cdot \end{pmatrix} \quad C=\begin{pmatrix} \cdot \\ \cdot \\ \cdot \end{pmatrix}$$

$$D=\begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad E=\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} \quad F=\begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

1) Déterminer la taille de chaque matrice.

2) Schématiser les matrices étant données leurs tailles :

- $J : 4 \times 7$
- $K : 1 \times 6$
- $L : 5 \times 1$

12 Soit $A = (a_{ij})$ une matrice carrée d'ordre 4.

Écrire la matrice A dans chacun des cas suivants :

1) $a_{ij} = i + j$ **3)** $a_{ij} = i^3 + 3j$

2) $a_{ij} = 2i - j$ **4)** $a_{ij} = |i - 2j|$

13 Soit $B = (b_{ij})$ une matrice carrée d'ordre 5.
Écrire la matrice B dans chacun des cas suivants :

1) $b_{ij} = \begin{cases} 1 \text{ si } i = j \\ i+1 \text{ si } i < j \\ j-2 \text{ si } i > j \end{cases}$ **2)** $b_{ij} = \begin{cases} i \text{ si } i = j \\ 3 \text{ si } i < j \\ -2 \text{ si } i > j \end{cases}$

14 Soit $M = (m_{ij})$ une matrice carrée d'ordre n.
Déterminer l'ensemble des coefficients vérifiant chaque égalité donnée.

1) $i = j$ **3)** $i = j+1$
2) $i = j-1$ **4)** $i + j = n$

15 Trois dépôts (D_1, D_2, D_3) vendent des bouteilles de sirop aux mêmes prix : 1 € la grenadine (G), 1,50 € la menthe (M) et 2,2 € l'orgeat (O). Ci-après, les tableaux de gauche à droite rendent compte :

- des stocks au début de l'été ;
- des quantités commandées pour l'été ;
- des ventes pour la saison estivale.

	Stocks			Commandes			Ventes		
	G	M	O	G	M	O	G	M	O
D_1	75	45	45	165	85	40	185	95	80
D_2	85	20	25	120	70	85	165	55	95
D_3	50	45	35	60	25	60	65	60	40

1) Calculer le stock de chaque dépôt après commande.
2) Calculer la recette de la vente des sirops cet été.
3) Le gérant pense que ses ventes auraient augmenté de 20 % s'il avait diminué de 15 % les prix des sirops. La recette aurait-elle été meilleure dans ce cas ?

16 Soit l'algorithme suivant :

```
n, i, j sont des entiers
A est une matrice carrée de taille n
Traitement
Saisir n et A
Pour i allant de 1 à n
    Pour j allant de 1 à n
        Si i+j=n+1 alors aij=1 sinon aij=0
    Fin Pour
Fin Pour
```

1) Faire tourner l'algorithme pour $n = 4$.
2) Quel type de matrice l'algorithme fabrique-t-il ?
3) Modifier l'algorithme pour qu'il fabrique l'identité.

Transposée d'une matrice

17 Soit la matrice $A = \begin{pmatrix} 5 & \dots & 8 & 7 \\ \dots & 9 & \dots & 1 \\ 7 & \dots & 0 & 3 \end{pmatrix}$.
On sait que $a_{32} = 5$, $a_{23} = -4$, $a_{21} = 8$ et $a_{12} = 11$.
Compléter A et écrire A^T, la transposée de A.

18 **Produit scalaire**

1) Calculer le produit scalaire $\vec{u} \cdot \vec{v}$ dans les cas suivants :

a) $\vec{u} \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}$ et $\vec{v} \begin{pmatrix} -5 \\ -4 \\ 2 \end{pmatrix}$ **b)** $\vec{u} \begin{pmatrix} 1\sqrt{2} \\ 3\sqrt{4} \\ 5\sqrt{6} \end{pmatrix}$ et $\vec{v} \begin{pmatrix} 3\sqrt{1} \\ 2\sqrt{2} \\ 1\sqrt{3} \end{pmatrix}$

2) Soit U et V les matrices colonnes représentant $\vec{u}$ et $\vec{v}$. Exprimer $\vec{u} \cdot \vec{v}$ en fonction de U et V.

19 Une matrice carrée A est dite **symétrique** si $M = M^\mathsf{T}$ et **antisymétrique** si $M = -M^\mathsf{T}$.

1) Soit $K = \begin{pmatrix} 6 & 1 & 8 \\ 7 & 5 & 3 \\ 2 & 9 & 4 \end{pmatrix}$, $X = K + K^\mathsf{T}$ et $Y = 2K - X$.

a) Montrer que X est symétrique, Y antisymétrique.
b) Qu'ont en commun les trois matrices K, X et Y ?

2) Soit S, A et Q trois matrices carrées d'ordre 3 respectivement symétrique, antisymétrique et quelconque. Montrer que :

a) Les éléments diagonaux de A sont nuls.
b) $Q + Q^\mathsf{T}$ est symétrique ; $Q - Q^\mathsf{T}$ antisymétrique.
c) S^n est symétrique pour tout $n \in \mathbb{N}$.

Combinaison linéaire de matrices

20 Calculer $A + B$ en écrivant ses coefficients sous la forme la plus simple possible.

1) $A = \begin{pmatrix} -5 & 0 & 8 \\ 1/4 & 1/10 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 2/3 & 3 & 1/5 \\ 1/4 & 1/5 & -2 \end{pmatrix}$

2) $A = \begin{pmatrix} \sqrt{2} & -\sqrt{3} \\ -\sqrt{50} & \sqrt{20} \end{pmatrix}$ et $B = \begin{pmatrix} -\sqrt{8} & \sqrt{18} \\ -\sqrt{75} & \sqrt{45} \end{pmatrix}$

21 Soit $A = \begin{pmatrix} 3 & -8 & 5 \\ 6 & -2 & 1 \\ 0 & 4 & 7 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 9 \\ 2 & -4 & -7 \\ 3 & 5 & 1 \end{pmatrix}$.

Calculer :

1) $A + B$ **2)** $3A$ **3)** $-5B$ **4)** $2A - 3B$

22 Déterminer la valeur de a telle que :

$$\begin{pmatrix} 8 & 7 \\ 5a & -2a \end{pmatrix} + \begin{pmatrix} 3a & 1 \\ 11 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 8 \\ -19 & 18 \end{pmatrix}$$

23 Soit $A = \begin{pmatrix} \ln 3 & \ln 5 \\ \sqrt{2} & \pi \end{pmatrix}$ et $C = \begin{pmatrix} \ln 6 & \ln 30 \\ 3\sqrt{2}-1 & 1 \end{pmatrix}$.
Déterminer la matrice B telle que $A + B = C$.

24 Déterminer les réels x et y tels que :

$$x\begin{pmatrix} 11 & 7 \\ -4 & 3 \end{pmatrix} + y\begin{pmatrix} 8 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -17 & -23 \\ 16 & -7 \end{pmatrix}$$

25 Soit $A = \begin{pmatrix} 3 & 8 & 1 \\ 0 & 7 & 11 \\ a & b & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 15 & c & d \\ e & 35 & f \\ 6 & 5 & g \end{pmatrix}$.
Déterminer les réels a, b, c, d, e, f, g et k tels que $A = kB$.

26 Déterminer les réels α, β et γ tels que :

$$\begin{pmatrix} \alpha^2 & 3 \\ \alpha+\beta & 10 \end{pmatrix} = 2\begin{pmatrix} 8 & \gamma \\ 1,5\alpha - 0,5 & 5 \end{pmatrix}$$

27 ALGO
Écrire un algorithme calculant la somme de deux matrices. Il testera d'abord si la somme est possible, si ce n'est pas le cas, il enverra un message d'erreur.

Produit de matrices

28 Dans les matrices schématisées suivantes, chaque point représente un nombre.

$A = \begin{pmatrix} \cdot & \cdot & \cdot \end{pmatrix}$ $\quad B = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$ $\quad C = \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}$ $\quad D = \begin{pmatrix} \cdot \\ \cdot \\ \cdot \end{pmatrix}$

$E = \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}$ $\quad F = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$ $\quad G = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix}$ $\quad H = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$

1) Quels produits peut-on effectuer avec :
   a) deux matrices ? b) trois matrices ?
2) Quel produit peut-on effectuer en utilisant le plus grand nombre de matrices distinctes ?

29 Soit A une matrice de taille $m \times n$ et B une matrice de taille $p \times q$.
Déterminer à quelle condition chacun des produits suivants existe et donner sa taille si c'est le cas.
1) AB 2) BA 3) $BABA$ 4) A^3

30 ► MÉTHODE 1 p. 90
Effectuer les produits des matrices suivantes :

1) $\begin{pmatrix} 2 & 1 & -1 \\ -3 & 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ -1 \\ 1 \end{pmatrix}$ 3) $\begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}\begin{pmatrix} 2 & -1 & 1 \end{pmatrix}$

2) $\begin{pmatrix} 5 & 2 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -3 & 1 \end{pmatrix}$ 4) $\begin{pmatrix} -1 & 2 & 1 \\ 0 & 2 & 2 \\ -2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$

31 Soit les matrices $A = \begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix}$.
Vérifier que $AB = 0$, puis calculer BA.

32 Dans chaque cas, montrer que le produit des matrices A et B est commutatif.

1) $A = \begin{pmatrix} -4 & -2 \\ -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} -3 & -2 \\ -1 & 1 \end{pmatrix}$

2) $A = \begin{pmatrix} -4 & -2 \\ 2 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} -2 & -1 \\ 1 & 2 \end{pmatrix}$

3) $A = \begin{pmatrix} -2 & -1 \\ 1 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} -3 & -1 \\ 1 & 2 \end{pmatrix}$

4) $A = \begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix}$

33 Soit $A = \begin{pmatrix} -1 & 1 & 3 \\ 1 & -2 & -5 \\ -1 & 2 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} -2 & -2 & -1 \\ -1 & 1 & 2 \\ 0 & -1 & -1 \end{pmatrix}$.
1) Déterminer AB et BA.
2) Que peut-on dire des matrices A et B ?

34 Soit $A = \begin{pmatrix} 2 & 1 & -7 \\ 4 & 3 & 1 \\ 8 & -5 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 7 & 8 & 2 \\ 4 & 3 & 1 \\ -3 & 0 & 5 \end{pmatrix}$
et M la matrice carrée d'ordre 3 telle que $a_{12} = 2$, $a_{22} = -3$, $a_{32} = 1$ et $a_{ij} = 0$ partout ailleurs.
1) Calculer MA et MB.
2) Expliquer le résultat obtenu.

35 $A = \begin{pmatrix} 3 & 4 \\ -2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}$ et $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$.
1) Les matrices A et B commutent-elles ?
2) a) Montrer que A et M commutent si, et seulement si, $\begin{cases} y = -2z \\ t = x + z \end{cases}$.
   b) Montrer que les coefficients de A, B et de l'identité d'ordre 2 vérifient ce système.
3) Soit C une matrice qui commute avec A.
   Démontrer que $ABC = CBA$.

36 Une entreprise doit fabriquer 80 ordinateurs α et 50 ordinateurs ω à partir d'unités de ressources.

Le tableau suivant fournit le nombre d'unités nécessaires à la fabrication de chaque modèle et le coût de chaque unité.

Ressources	α	ω	Coût
Bureau d'étude	1	2	60 €
Main d'œuvre	2	2,5	25 €
Composants	3	6	35 €

Soit $A = \begin{pmatrix} 60 & 25 & 35 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 2 & 2{,}5 \\ 3 & 6 \end{pmatrix}$ et $C = \begin{pmatrix} 80 \\ 50 \end{pmatrix}$.

Calculer les produits matriciels suivants et interpréter :

1) AB **2)** BC **3)** ABC

Puissance d'une matrice

37 ► MÉTHODE 2 p. 91

Calculer A^2, puis A^3 :

1) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ **3)** $A = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$

2) $A = \begin{pmatrix} 1 & 3 \\ -1 & 1 \end{pmatrix}$ **4)** $A = \begin{pmatrix} -2 & 1 \\ -3 & 1 \end{pmatrix}$

38 Déterminer le carré des matrices suivantes :

1) $A = \begin{pmatrix} 2 & -2 & 4 \\ -2 & 2 & -4 \\ -2 & 2 & -4 \end{pmatrix}$ **3)** $C = \begin{pmatrix} 1 & -3 & -3 \\ -2 & 2 & 3 \\ 2 & -3 & -4 \end{pmatrix}$

2) $B = \begin{pmatrix} 1 & -3 & -4 \\ -1 & 3 & 4 \\ 1 & -3 & -4 \end{pmatrix}$ **4)** $D = \begin{pmatrix} 1 & -3 & -4 \\ 0 & 3 & 0 \\ -2 & -3 & -1 \end{pmatrix}$

39 Soit les matrices $A = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$ et $B = \dfrac{1}{3}A$.

Déterminer B^n. En déduire A^n.

40 Soit $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ et $B = kA$ où $k \in \mathbb{R}$.

Pour quelles valeurs de k a-t-on $B^2 = B$?

41 Soit $A=\begin{pmatrix} 4 & -4 \\ 3 & -3 \end{pmatrix}$, $B=\begin{pmatrix} 2 & 3 \\ -2 & -3 \end{pmatrix}$ et $C=\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}$.

Montrer que, pour tout entier naturel non nul n :

1) $A^n = A$ **2)** $B^{2n} = -B$ **3)** $4C^n = 4^n C$

42 Soit $A = \begin{pmatrix} 0 & 2 & 5 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix}$ et I l'identité d'ordre 3.

1) Calculer I^n et A^n.

2) En déduire l'expression de la matrice $(I + A)^5$.

43 Déterminer, pour tout n entier naturel non nul, la puissance n-ième de chaque matrice.

1) $A=\begin{pmatrix} 3 & -2 \\ 4 & -3 \end{pmatrix}$ **2)** $B=\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$ **3)** $C=\begin{pmatrix} -3 & 1 \\ 3 & 3 \end{pmatrix}$

44 Soit la matrice $A = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$.

1) Calculer A^2.

2) Démontrer par récurrence que, pour tout entier naturel n, $A^{2n} = 5^n I$.

3) Calculer A^{2016}.

45 Soit la matrice $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

En écrivant $A = I + J$, où I est l'identité d'ordre 3 et J une matrice à déterminer, calculer A^n pour $n \in \mathbb{N}$.

46 Soit $M = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ avec a réel strictement positif.

Le but est de déterminer $M^{1\,000}$ de trois façons.

1) a) Calculer M^2, M^3 et M^4.

b) Conjecturer puis démontrer l'expression de M^n en fonction de n. En déduire $M^{1\,000}$.

2) a) Vérifier que $M^2 = 2M - I$.

b) En déduire M^3 et M^4 en fonction de M et I.

c) Conclure.

3) a) Déterminer la matrice A telle que $M = I + A$.

b) Calculer A^2.

c) En déduire M^2, M^3 et M^4 en fonction de A et I.

d) Exprimer $M^{1\,000}$ en fonction de A et I.

e) Conclure.

47 Soit les matrices $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = A - I$.

1) Calculer B^2 et B^3.

2) a) Peut-on utiliser la formule du binôme de Newton pour développer l'expression $(I + B)^n$? Justifier.

b) Démontrer que, pour tout entier naturel $n \geqslant 3$:

$$A^n = \binom{n}{0} I + \binom{n}{1} B + \binom{n}{2} B^2.$$

48 Soit $A=\begin{pmatrix} -1 & 1 & 2 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$ et $D=\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

1) Soit la matrice $B = A - D$. Calculer B^2 et B^3.

2) Démontrer que, pour tout entier naturel $n \geqslant 3$, on a :

$$A^n = (-1)^n \left(I_3 - nB + \frac{n(n-1)}{2} B^2 \right).$$

49 Soit la matrice $A = \begin{pmatrix} 3 & 1 & 2 \\ 0 & 3 & -1 \\ 0 & 0 & 3 \end{pmatrix}$.

1) Déterminer une matrice diagonale B et une autre matrice C telle que $A = B + C$.

2) a) Pour tout entier n, donner l'expression de B^n.

b) Vérifier que B et C sont commutatives.

c) Démontrer que, pour tout $n \in \mathbb{N}^*$:

$$A^n = B^n + nCB^n + \binom{n}{2} C^2 B^{n-2}.$$

50 Soit A la matrice carrée d'ordre 4 telle que $a_{ij} = 0$ si $i \geqslant j$ et $a_{ij} = i + j$ si $i < j$.

1) Écrire A. Quelle particularité a-t-elle ?

2) Déterminer A^n pour tout entier naturel n.

Calculs matriciels divers

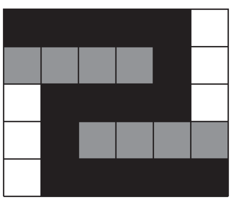
51 Soit $A = \begin{pmatrix} 4 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -2 \\ -3 & -5 \end{pmatrix}$, $C = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$.

1) Parmi les calculs suivants, déterminer ceux qu'on peut effectuer et donner la taille du résultat.

a) AB	**e)** CA	**i)** ABC
b) $A - B$	**f)** CB	**j)** A^2
c) AC	**g)** $B + C$	**k)** B^2
d) $A + 2C$	**h)** BAC	**l)** C^2

2) Effectuer les calculs possibles.

52 Une image numérique en nuances de gris est représentée par une matrice où le coefficient situé dans la i-ème ligne et la j-ème colonne est égal au niveau de gris, entre 0 (blanc) et 1 (noir), du pixel correspondant.



1) Écrire la matrice A des niveaux de gris de l'image précédente où les trois couleurs sont noir, blanc et gris moyen (niveau 0,5).

2) a) Écrire la matrice B du négatif de cette image.

b) Exprimer b_{ij} en fonction de a_{ij}.

c) Représenter l'image correspondante à B^{T}.

3) Soit $C = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$.

a) Décrire l'influence du facteur k sur l'image représentée par kC pour $k \in]0 ; 1[$.

b) Déterminer la matrice D telle que $D = 2A - C$.

c) Représenter l'image correspondante à D.

53 Soit la matrice triangulaire $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

1) a) A est triangulaire supérieure. Que dire de A^{T} ?

b) Calculer $A + A^{\mathsf{T}} - I$.

2) a) Calculer A^2, A^3, A^4 et conjecturer A^n.

b) Démontrer la conjecture par récurrence.

54 Soit $A = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 6 \\ -1 & 2 \end{pmatrix}$ et $C = A + B$.

1) Calculer C^2.

2) Calculer $A^2 + 2AB + B^2$.

3) Pourquoi n'a-t-on pas $C^2 = A^2 + 2AB + B^2$?

55 Soit A et B deux matrices carrées commutatives. Développer les expressions suivantes :

1) $(2A + I)(I - A)$

2) $(A + 2I)^2$

3) $(A + 2B)(B - A)$

4) $(2A - B)^2$

56 Soit $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec a, b, c et d réels.

On souhaite résoudre l'équation $X^2 = I$.

1) Montrer que, si $b = 0$, les solutions de l'équation ne dépendent que de c.

2) Montrer que, si $b \neq 0$, les solutions sont telles que :

$$c = \frac{1 - a^2}{b} \text{ et } d = -a.$$

57 Soit la matrice $A = \begin{pmatrix} 1 & -3 & -2 \\ -1 & 1 & -4 \\ -1 & 2 & -2 \end{pmatrix}$.

1) Calculer A^2, puis vérifier que $A^3 = 2I$.

2) En déduire A^{3n}, A^{3n+1} et A^{3n+2} pour tout $n \in \mathbb{N}$.

58 Soit la suite (u_n) telle que $u_0=0$ et $u_{n+1}=u_n+2^n$.

Prouver que, pour $n \neq 0$, $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & u_n \\ 0 & 1 & 0 \\ 0 & 0 & 2^n \end{pmatrix}$.

59 INFO

À l'aide d'un logiciel de calcul formel, déterminer A^n pour tout n entier naturel non nul.

1) $A = \begin{pmatrix} 1 & -4 & -4 \\ -1 & 1 & 2 \\ 1 & -2 & -3 \end{pmatrix}$ **2)** $A = \begin{pmatrix} 1 & -3 & -2 \\ -3 & 1 & 2 \\ 3 & -3 & -4 \end{pmatrix}$

60 On pose $A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ pour $\theta \in \mathbb{R}$.

1) Démontrer que $A(\theta)A(\theta') = A(\theta+\theta')$.

2) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n(\theta) = A(n\theta)$.

Inverse d'une matrice

61 Pour chaque matrice, déterminer si elle est inversible et, si oui, calculer son inverse.

1) $\begin{pmatrix} -3 & 2 \\ -2 & 2 \end{pmatrix}$ **5)** $\begin{pmatrix} -3 & 4 \\ 6 & -8 \end{pmatrix}$

2) $\begin{pmatrix} 4 & 2 \\ 3 & 6 \end{pmatrix}$ **6)** $\begin{pmatrix} -2 & -1 \\ -1 & -1 \end{pmatrix}$

3) $\begin{pmatrix} 8 & 4 \\ -4 & -2 \end{pmatrix}$ **7)** $\begin{pmatrix} \sqrt{3}+1 & 2 \\ 1 & \sqrt{3}-1 \end{pmatrix}$

4) $\begin{pmatrix} 0 & 2 \\ 3 & 6 \end{pmatrix}$ **8)** $\begin{pmatrix} 1 & 0 \\ -4 & -4 \end{pmatrix}$

62 Soit la matrice $A = \begin{pmatrix} 1 & -2 & -2 \\ -1 & 0 & -2 \\ -1 & -2 & 0 \end{pmatrix}$.

1) Calculer $A^2 + A$.

2) En déduire que A est inversible et déterminer A^{-1}.

63 Soit la matrice $A = \begin{pmatrix} 1 & -2 & -1 \\ -2 & 1 & 1 \\ -2 & 2 & 0 \end{pmatrix}$.

1) Calculer $A^2 - 3A$.

2) En déduire que A est inversible et déterminer A^{-1}.

64 Soit la matrice $A = \begin{pmatrix} 0 & -2 & -1 \\ 1 & 3 & 1 \\ -1 & -2 & 0 \end{pmatrix}$.

1) Démontrer que $2A - A^2 = I$.

2) En déduire que A est inversible et calculer A^{-1}.

65 ALGO

Soit M la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et l'algorithme suivant.

```
a, b, c, d, det sont des nombres
L1 et L2 sont des listes
Traitement
Saisir a, b, c, d
det prend la valeur ad - bc
Si det=0 alors Afficher "Impossible"
Sinon
    L1[1] prend la valeur d/det
    L1[2] prend la valeur -b/det
    L2[1] prend la valeur -c/det
    L2[2] prend la valeur a/det
    Afficher L1, L2
Fin Si
```

1) Préciser la signification de l'affichage « Impossible ».

2) Que dire de la matrice obtenue par l'affichage des listes L1 et L2 ? Vérifier la réponse par un calcul.

3) Programmer l'algorithme dans AlgoBox et le tester pour $a = 3$, $b = 2$, $c = 2$, $d = 3$.

4) On suppose que M est inversible.
Démontrer que M^{T} est inversible et que :

$$\left(M^{\mathsf{T}}\right)^{-1} = \left(M^{-1}\right)^{\mathsf{T}}.$$

5) En déduire comment modifier simplement l'algorithme pour qu'il calcule, si possible, l'inverse de la transposée de M.

66 Soit les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$.

Pour toute matrice carrée inversible M et tout entier naturel n, on note $M^{-n} = \left(M^{-1}\right)^n$.

1) Démontrer que, pour tout $n \in \mathbb{Z}$:

a) $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ **b)** $B^n = \begin{pmatrix} 2^n & 0 \\ 2^n-1 & 1 \end{pmatrix}$

2) Peut-on en déduire $(AB)^n$ pour tout $n \in \mathbb{Z}$?

67 **Inverse d'un produit**

Soit A et B deux matrices inversibles et $\lambda \in \mathbb{R}^*$.

1) Prouver que AB est inversible et déterminer $(AB)^{-1}$.

2) Prouver que λA est inversible et déterminer $(\lambda A)^{-1}$.

Résolution d'un système linéaire

68 ► MÉTHODE 3 p. 93

À l'aide des matrices mais sans l'aide de la calculatrice ou d'un logiciel, résoudre les systèmes suivants :

1) $\begin{cases} -4x+3y=2 \\ -x+y=5 \end{cases}$ **3)** $\begin{cases} 3\sqrt{3}x+3y=\sqrt{3} \\ -3x-\sqrt{3}y=1 \end{cases}$

2) $\begin{cases} 9x-4y=2 \\ -1,8x+0,8y=-9 \end{cases}$ **4)** $\begin{cases} 6x+8y=8\,400 \\ x+1,5y=1\,450 \end{cases}$

69 À l'aide des matrices mais sans l'aide d'un logiciel, résoudre les systèmes suivants (on discutera des solutions selon les valeurs de θ) :

1) $\begin{cases} \cos\theta x-\sin\theta y = \cos\theta+\sin\theta \\ \cos\theta x+\sin\theta y = -\cos\theta+\sin\theta \end{cases}$

2) $\begin{cases} \cos\theta x-\sin\theta y = \dfrac{\sqrt{3}}{2} \\ \cos\theta y+\sin\theta x = -\dfrac{1}{2} \end{cases}$

70 ► MÉTHODE 4 p. 94

Résoudre chacun des systèmes d'équations suivants avec la calculatrice ou un logiciel de calcul formel :

1) $\begin{cases} 3x-3y-2z=0 \\ 3x+y+z=-2 \\ -2x+3y+2y=-1 \end{cases}$ **3)** $\begin{cases} -x-3y-2z=-1 \\ -3x-2y+2z=0 \\ 3x+3y-z=-1 \end{cases}$

2) $\begin{cases} 2x-3y+z=-8 \\ -3x+2y-3z=3 \\ x-y+z=-1 \end{cases}$ **4)** $\begin{cases} -2x-3y-2z=2 \\ -3x-3y+2z=1 \\ x+2y+3z=-2 \end{cases}$

71 Déterminer, si c'est possible, deux réels a et b vérifiant l'égalité donnée.

1) $\begin{pmatrix} 5 & 2 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} 4 \\ 9 \end{pmatrix}$ **2)** $\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} -2 \\ 11 \end{pmatrix}$

72 Déterminer, si c'est possible, trois réels a, b et c vérifiant l'égalité donnée.

1) $\begin{pmatrix} 3 & 1 & 4 \\ 2 & -1 & 0 \\ 1 & -1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} 5 \\ 0 \\ -1 \end{pmatrix}$

2) $\begin{pmatrix} 4 & -2 & 1 \\ 1 & 2 & 3 \\ 2 & -6 & -5 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} 7 \\ 7 \\ -7 \end{pmatrix}$

3) $\begin{pmatrix} 2 & -1 & 1 \\ 3 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} 2 \\ 8 \\ 2 \end{pmatrix}$

73 Soit $A=\begin{pmatrix} 1 & -2 & -2 \\ 2 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$ et $B=\begin{pmatrix} 1 & 2 & -2 \\ 2 & 5 & -6 \\ -2 & -4 & 5 \end{pmatrix}$.

1) Montrer que A et B sont inverses l'une de l'autre.

2) Résoudre les systèmes d'équations suivants :

a) $\begin{cases} x-2y-2z=0 \\ 2x+y+2z=-9 \\ 2x+z=-8 \end{cases}$ **b)** $\begin{cases} x+2y-2z=-2 \\ 2x+5y-6z=-7 \\ -2x-4y+5z=8 \end{cases}$

74 Soit le système linéaire (S) $\begin{cases} 2x+5y=8 \\ 3x-4y=15 \end{cases}$.

On pose $X=\begin{pmatrix} x \\ y \end{pmatrix}$ et $X'=\begin{pmatrix} x & y \end{pmatrix}$.

1) a) Écrire (S) sous la forme matricielle $AX=B$.

b) Vérifier que A est inversible et calculer A^{-1}.

c) En déduire les solutions du système.

2) a) Écrire (S) sous la forme matricielle $X'A'=B'$.

b) Que peut-on dire de A et A' ? de B et B' ?

c) Exprimer X' en fonction de A et B.

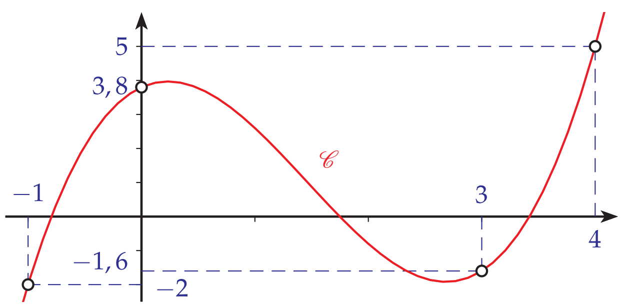
75 Soit a et b deux réels.

1) Résoudre le système linéaire $\begin{cases} 4x+3y=a \\ 8x+7y=b \end{cases}$.

2) Déterminer les coordonnées du point d'intersection des droites d'équations $12x+9y=4$ et $8x+7y=1$ dans un repère donné.

76 Déterminer la fonction polynôme du second degré dont la courbe représentative est la parabole passant par les points $A(-1\,;-3)$, $B(3\,;-5)$ et $C(4\,;-13)$.

77 Soit la fonction polynôme de degré 3 définie par $f(x)=ax^3+bx^2+cx+d$ représentée ci-dessous.



1) Justifier que $d=3,8$.

2) Soit la matrice ligne $X=\begin{pmatrix} a & b & c \end{pmatrix}$.

Déterminer deux matrices A et B telles que $AX^{\mathsf{T}}=B$.

3) Résoudre l'équation précédente avec la calculatrice.

En déduire l'expression de $f(x)$.

78 **D'après Bac S (Asie - 2015)**

Le but est de résoudre l'équation (E) : $x^2 - 8y^2 = 1$ où x, y sont deux entiers relatifs.

Soit $(a;b)$ un couple solution de (E) et soit a' et b' deux entiers relatifs tels que :

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix} \text{ où } A = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}.$$

1) Exprimer a' et b' en fonction de a et de b.

2) Déterminer la matrice M^{-1}, puis exprimer a et b en fonction de a' et b'.

3) Démontrer que $(a;b)$ est solution de (E) si, et seulement si, $(a';b')$ est solution de (E).

4) Soit les suites (a_n) et (b_n) définies par $a_0 = 3$, $b_0 = 1$ et, pour tout entier naturel n, $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = M \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

Démontrer par récurrence que, pour tout entier naturel n, le couple $(a_n ; b_n)$ est solution de (E).

79 **D'après Bac S (Amérique du Nord - 2015)**

Soit $M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix}$ et $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Partie A

1) Déterminer la matrice M^2.

2) On donne $M^3 = \begin{pmatrix} 20 & 10 & 11 \\ 12 & 2 & 9 \\ 42 & 20 & 21 \end{pmatrix}$.

Vérifier que $M^3 = M^2 + 8M + 6I$.

3) En déduire que M est inversible et que :

$$M^{-1} = \frac{1}{6}\left(M^2 - M - 8I\right)$$

Partie B

On cherche à déterminer trois nombres entiers a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A(1 ; 1), B(−1 ; −1) et C(2 ; 5).

1) Démontrer que le problème revient à chercher trois entiers a, b et c tels que

$$M \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}.$$

2) Calculer les nombres a, b et c et vérifier que ces nombres sont des entiers.

80 **D'après Bac ES (Pondichéry - 2014)**

Deux sociétés, Fontana (F) et Boumbouno (B), se partagent le marché des fontaines d'eau à bonbonnes dans les entreprises d'une grande ville. L'entreprise F fournit ses clients en recharges pour les fontaines à eau et dispose des résultats antérieurs suivants :

Nombre de recharges	Coût total de production
1 000	1 100 €
3 000	2 740 €
5 000	8 300 €

Soit f la fonction polynôme de degré 3, définie pour tout nombre réel x de l'intervalle [0 ; 10] par :

$$f(x) = \alpha x^3 + \beta x^2 + \gamma x + 10.$$

Lorsque le nombre x désigne le nombre de milliers de recharges produites, $f(x)$ est égale au coût total de production en centaines d'euros.

1) Démontrer que le triplet $(\alpha ; \beta ; \gamma)$ est solution du système suivant :

$$(S) \quad \begin{cases} \alpha + \beta + \gamma = 1 \\ 27\alpha + 9\beta + 3\gamma = 17,4 \\ 125\alpha + 25\beta + 5\gamma = 73 \end{cases}$$

2) On pose $X = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$.

a) Écrire le système (S) sous la forme $MX = Y$ où M et Y sont des matrices que l'on précisera.

b) À l'aide de la calculatrice, vérifier que la matrice M est inversible.

Déterminer le triplet solution du système (S).

3) Quel serait alors le coût total annuel de production pour 8 000 recharges d'eau produites ?

4) Un espion d'entreprise de chez Fontana a dérobé la fonction donnant le coût de production en centaines d'euros $b(x)$ de chez Boumbouno, en fonction de x le nombre de milliers de recharges produites :

$$b : x \mapsto 0,6x^3 + 0,9x^2 + 0,2x + 7$$

a) Déterminer pour combien de milliers de recharges produites, les entreprises Fontana et Boumbouno produisent au même coût.

b) Étudier quelle entreprise a le plus faible coût de production en fonction du nombre de milliers de recharges produites.

81 ALGO

Soit l'algorithme suivant dans lequel `A[i][j]` est un nombre correspond au coefficient a_{ij} de la matrice A.

```
1.  n, p, i, j sont des nombres entiers
2.  A est une matrice
3.  Traitement
4.  Pour i allant de 1 à n
5.      Pour j allant de 1 à p
6.          Saisir A[i][j]
7.      Fin Pour
8.  Fin Pour
9.  Pour i allant de 2 à n
10.    Pour j allant de 2 à p
11.        A[i][j]=A[i-1][j]+A[i][j-1]
12.    Fin Pour
13. Fin Pour
14. Afficher la matrice A
```

1) Expliquer à quoi servent les lignes 4 à 8.

2) Quelle matrice s'affiche en sortie si on saisit

$$A = \begin{pmatrix} 1 & 3 & 6 & 0 \\ -1 & 1 & 2 & 3 \\ 2 & 4 & 5 & 6 \end{pmatrix} \text{ ?}$$

3) Lignes 9 et 10 : pourquoi i et j commencent-ils à 2 ?

4) Un élève a testé l'algorithme mais il n'a noté que partiellement la matrice qui s'est affichée à la fin :

$$\begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & 4 & 7 & 16 & 15 \\ \dots & 9 & 16 & 32 & 47 \end{pmatrix}$$

a) Peut-il reconstituer cette matrice ? Expliquer.

b) Retrouver le maximum de coefficients en décrivant brièvement la méthode.

c) Si on sait que $a_{11} = -5$, peut-on reconstituer complètement la matrice ? Si oui, l'écrire.

d) Même question si on sait que $a_{12} = 4$.

82 On cherche une fonction polynôme f vérifiant :

$$(x^2-2)f''(x)+(1-3x)f'(x)+f(x) = x^3+6x^2-2x+4$$

1) Justifier que $f(x)$ est un polynôme de degré 3.

2) Soit $f(x) = ax^3+bx^2+cx+d$.
Écrire un système qui régit les coefficients a, b, c et d.

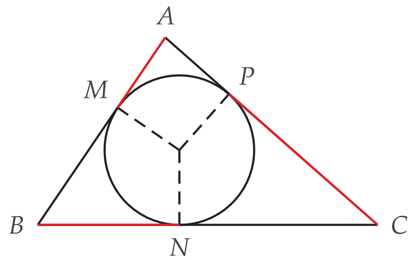
3) À l'aide des matrices, résoudre ce système.

83 Soit $A = \begin{pmatrix} 1 & -3 & 6 \\ 6 & -8 & 12 \\ 3 & -3 & 4 \end{pmatrix}$ et I l'identité d'ordre 3.

1) Déterminer les réels a et b tels que $aA + bI = A^2$.

2) En déduire que A est inversible et exprimer A^{-1} en fonction de A et I.

84 Soit ABC un triangle tel que $[AB]$, $[BC]$, $[AC]$ sont respectivement de longueurs 4 cm, 6 cm, 5 cm et tangents à son cercle inscrit en M, N, P.
Le but est de calculer $x = AM$, $y = BN$, $z = CP$.



1) Démontrer que le problème revient à résoudre l'équation matricielle :

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$$

2) Résoudre cette équation et en déduire les longueurs cherchées.

85 Une usine fabrique deux articles A et B à partir de composants X, Y et Z produits grâce à trois ressources : du travail, des matières premières et de l'énergie.

Le tableau ci-contre donne le nombre de composants utilisés pour fabriquer chaque article.

	X	Y	Z
A	1	3	2
B	2	3	3

Le tableau ci-dessous indique les coûts (en €) des ressources requises pour produire chaque composant.

	Travail	Matières premières	Énergie
X	8	12	3
Y	7	18	4
Z	1	8	5

À l'aide de produits de matrices, calculer :

- la matrice donnant les coûts de chaque ressource intervenant dans la fabrication de chaque article ;
- les coûts de production de chaque article ;
- le coût total pour produire 9 articles A et 7 articles B.

86 Soit le système $\begin{cases} 3x + \ \ 7y = \ \ 4 \\ 12x + 28y = 16 \end{cases}$.

1) Sa matrice associée est-elle inversible ?

2) Déterminer une relation entre les deux équations.

3) En déduire que les solutions du système sont les couples $\left(t\ ;\ \dfrac{4-3t}{7}\right)$ pour $t \in \mathbb{R}$.

87 Soit le système (S) : $\begin{cases} x + \ \ y - \ \ z = \ \ 1 \\ 2x - 3y + \ \ z = -5 \\ x - 4y + 2z = -6 \end{cases}$.

1) Sa matrice associée est-elle inversible ?

2) Montrer que la troisième équation est une combinaison linéaire des deux autres.

3) Montrer que (S) $\Leftrightarrow \begin{cases} x + \ \ y - \ \ z = \ \ 1 \\ \ \ \ \ -5y + 3z = -7 \end{cases}$.

4) En déduire que les solutions de (S) sont les triplets $\left(\dfrac{-2+2t}{5}\ ;\ \dfrac{7+3t}{5}\ ;\ t\right)$ pour $t \in \mathbb{R}$.

5) Vérifier à l'aide du logiciel Xcas.

88 **Système paramétré**

Soit le système $\begin{cases} (3-\lambda)x - \quad 2y \quad\ \ = -4 \\ \quad 5x \quad - (4+\lambda)y = \ \ 5 \end{cases}$ où $\lambda \in \mathbb{R}$.

1) a) Démontrer que, si λ vérifie $\lambda^2 + \lambda - 2 \neq 0$, alors le système admet un unique couple solution.

b) À l'aide du calcul matriciel, déterminer le couple solution du système en fonction de λ.

2) a) Résoudre l'équation $\lambda^2 + \lambda - 2 = 0$.

b) Résoudre le système pour les racines obtenues à la question précédente.

89 **Équation de Pell-Fermat** ALGO

Soit l'équation $(E)\ :\ x^2 - 7y^2 = 1$ où x et y sont des entiers naturels.

1) a) Exprimer x en fonction de y.

b) Écrire un algorithme qui, pour y entier de 0 à 1 000, calcule x, teste s'il est entier et affiche les couples solutions.

c) Le programmer sur la calculatrice ou un logiciel et donner les solutions.

2) a) Montrer que si $(x\ ;\ y)$ est solution de (E), alors $(x'\ ;\ y')$ tel que $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 8 & 21 \\ 3 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ l'est aussi.

b) En déduire un algorithme qui, à partir de la solution triviale $(1\ ;\ 0)$, donne de proche en proche 9 autres solutions.

c) Le programmer et donner les solutions.

90 ALGO

Soit la partie traitement d'un algorithme destiné à calculer, si possible, le produit C de deux matrices A et B.

```
1.  Saisir A, B
2.  ...................
3.  ...................
4.  Si .... alors
5.     Afficher "Erreur de dimension"
6.  Sinon
7.     n égale le nombre de .... de A
8.     m égale le nombre de .... de B
9.     Pour i allant de 1 à n faire
10.       Pour k allant de 1 à m faire
11.          ...................
12.       Fin Pour
13.    Fin Pour
14. Fin Si
```

1) Compléter les lignes 2, 3 et 4 destinées à tester si le produit AB est possible ou non.

2) Exprimer c_{ik} en fonction de a_{ij} et b_{jk}.

3) Écrire une procédure qui calcule c_{ik}.

4) Compléter l'algorithme et le tester avec un logiciel.

5) On s'intéresse à la complexité de l'algorithme.

a) Quel est le nombre de multiplications nécessaires au calcul de c_{ik} ? Le nombre d'additions ?

b) En déduire le nombre total d'opérations nécessaires au calcul de AB.

c) Expliciter le résultat pour deux matrices carrées d'ordre n.

91 Soit $A = \begin{pmatrix} 2 & -1 & 3 \\ -3 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ et $B = 4A - A^2$.

1) Calculer B puis AB.

2) En déduire que A est inversible et déterminer A^{-1}.

3) Dans un repère orthonormé de l'espace, soit trois plans et leurs équations :

- $\mathcal{P} : 2x - y + 3z = 1$
- $\mathcal{Q} : -3x + y - z = 2$
- $\mathcal{R} : x + y + z = 3$

Déterminer les coordonnées de l'intersection de ces trois plans à l'aide de la matrice B.

92 **Vous avez dit logique ?** INFO

Partie A

1) Quel nombre prolonge le plus logiquement la série 1, 2, 4, 8 ?

2) Soit le polynôme $f : x \mapsto ax^3 + bx^2 + cx + d$ tel que $f(1) = 1$, $f(2) = 2$, $f(3) = 4$ et $f(4) = 8$.

a) Identifier f à l'aide d'un logiciel de calcul formel.

b) En déduire un nombre qui prolonge la série 1, 2, 4, 8.

3) Soit maintenant la série 1, 2, 4, 8, 16 conçue pour être logiquement prolongée par 32.

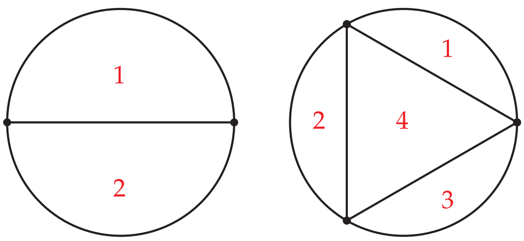
Soit le polynôme $g : x \mapsto ax^4 + bx^3 + cx^2 + dx + e$ tel que $g(1) = 1$, $g(2) = 2$, $g(3) = 4$, $g(4) = 8$ et $g(5) = 16$.

a) Identifier g à l'aide d'un logiciel de calcul formel.

b) En déduire un nombre qui prolonge la série 1, 2, 4, 8, 16.

Partie B

En plaçant des points distincts sur un cercle et en les reliant deux à deux par des segments, on partage en régions l'intérieur du cercle.



1) Déterminer le nombre de régions partageant l'intérieur du cercle avec quatre points sur le cercle.

Même chose avec cinq points, puis six.

2) Quel nombre poursuit le plus logiquement la série 2, 4, 8, 16 ? Est-ce 31 ou 32 ?

93 Dans le plan muni d'un repère orthonormé, soit trois points non alignés A, B et C. On note $(a\ ;\ a')$ les coordonnées de A, $(b\ ;\ b')$ celles de B, etc.

1) On veut placer trois points M, N, P tels que A, B, C soient les milieux respectifs de $[MN]$, $[NP]$, $[MP]$.

Proposer une solution par construction.

2) Cherchons une autre solution en exprimant les coordonnées de M, N, P à partir de celles de A, B, C.

a) Déterminer R la matrice carrée d'ordre 3 telle que :

$$\begin{pmatrix} a & b & c \end{pmatrix} = \begin{pmatrix} m & n & p \end{pmatrix} R.$$

b) Avec la calculatrice ou un logiciel de calcul formel, en déduire m, n, p en fonction de a, b, c.

c) Exprimer de même m', n', p' avec a', b', c'.

3) Vérifions les résultats dans CaRMetal.

a) Placer trois points A, B et C non alignés, puis le point D d'abscisse `x(A)+x(B)-x(C)` et d'ordonnée `y(A)+y(B)-y(C)`.

b) Que semble-t-on pourvoir dire du point D ?

c) Définir M, N et P à l'aide de formules similaires et vérifier qu'ils sont solutions du problème posé.

4) Démontrer que, si quatre points A, B, C, D non alignés sont les milieux des côtés d'un quadrilatère $MNPQ$, alors $ABCD$ est un parallélogramme.

5) Cherchons par une méthode analytique à déterminer M, N, P, Q tels que A, B, C, D soient les milieux respectifs de $[MN]$, $[NP]$, $[PQ]$, $[MQ]$.

a) Déterminer R la matrice carrée d'ordre 4 telle que :

$$\begin{pmatrix} a & b & c & d \end{pmatrix} = \begin{pmatrix} m & n & p & q \end{pmatrix} R.$$

b) Soit S la matrice carrée d'ordre 4 dont les lignes sont toutes égales à la ligne $\begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$.

Calculer SR et en déduire que R n'est pas inversible (on pourra raisonner par l'absurde).

c) On suppose que $ABCD$ est un parallélogramme. Montrer géométriquement qu'il existe une infinité de solutions au problème posé.

94 Le stère (de symbole st) est une unité de mesure des volumes de stockage de bois de chauffage ou de charpente. Il équivaut à 1 m^3 apparent pour des bûches d'1 m de long. Mais si les bûches rangées sont plus courtes, l'espace entre elles diminue et le volume aussi.

- pour des bûches de 0,5 m, 1 st équivaut à 0,8 m^3 ;
- pour des bûches de 0,33 m, 1 st équivaut à 0,68 m^3.

Pour une longueur de bûche L donnée, il y a proportionnalité entre le nombre de stères n et le volume V occupé par le bois rangé. On a ainsi l'égalité $n = k_L \times V$.

Pour $0,20 \text{ m} < L < 1 \text{ m}$, on a $k_L = aL^3 + bL^2 + cL + d$ où a, b, c et d sont des réels à déterminer.

1) Calculer k_1 et $k_{0,5}$.

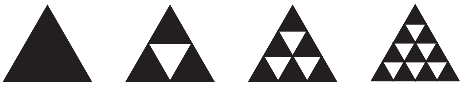
2) On sait que $k_{0,8} = 1,1$ et $k_{0,2} = 1,76$.

Déterminer a, b, c et d par un calcul matriciel.

3) En déduire le volume occupé par un stère de bois coupé en bûches de 0,60 m.

95 **Nombres carrés triangulaires**

Un triangle équilatéral est pavé en éléments semblables en fonction de n, nombre de divisions régulières d'un côté. On colorie alors en noir les éléments orientés comme le triangle pavé. Soit la suite $(t_n)_{n\geqslant 1}$ des nombres dits « triangulaires » d'éléments noirs.



$t_1 = 1$ $t_2 = 3$ $t_3 = 6$ $t_4 = 10$

1) a) Exprimer t_n en fonction de n.

b) Avec une calculatrice ou un tableur, déterminer deux couples d'entiers $(p\ ;\ q)$ tels que $p^2 = t_q$ et les nombres « carrés triangulaires » correspondants.

c) Vérifier que 41 616 est carré triangulaire.

2) a) On pose $x = 2q+1$ et $y = 2p$. Démontrer que $p^2 = t_q$ si, et seulement si, $x^2 - 2y^2 = 1$.

b) Montrer que, si les entiers naturels x et y vérifient l'égalité $x^2 - 2y^2 = 1$, alors x' et y' définis par $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ la vérifient aussi.

c) Vérifier que si x est impair, alors x' l'est aussi.

d) En déduire un algorithme qui donne 10 nombres carrés triangulaires. Le programmer sur un logiciel et donner ces 10 nombres.

96 Soit $A = \begin{pmatrix} a+b & 0 & b \\ b & a & b \\ b & 0 & a+b \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

1) Exprimer A en fonction de l'identité I, J, a et b.

2) Calculer J^n (on pourra d'abord calculer les premières puissances de J, émettre une conjecture et la démontrer par récurrence).

3) Calculer A^2.

4) Démontrer l'égalité $A^n = a^n I + \dfrac{(a+2b)^n - a^n}{2} J$.

5) Soit $C = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{pmatrix}$. Calculer le produit CJ.

6) Démontrer par l'absurde que :

a) si $a = 0$, alors A n'est pas inversible.

b) si $a + 2b = 0$, alors A n'est pas inversible.

7) Pour $a \neq 0$ et $a + 2b \neq 0$, on pose $B = \dfrac{1}{a} I - \dfrac{b}{a(a+2b)} J$.
Montrer que B est l'inverse de A.

97 Une usine fabrique trois articles A, B et C à partir de quatre produits différents P_1, P_2, P_3 et P_4 obtenus grâce à trois ressources : du travail (T), des matières premières (M) et de l'énergie (E).
Ci-dessous, le tableau de gauche donne les quantités de produits utilisés pour fabriquer chaque article et celui de droite, les coûts (en €) des ressources nécessaires pour obtenir chaque produit.

	P_1	P_2	P_3	P_4
A	3	2	2	1
B	4	3	0	2
C	0	5	3	2

	T	M	E
P_1	10	15	3
P_2	12	8	2
P_3	4	12	4
P_4	3	5	1

1) Soit $F = \begin{pmatrix} 3 & 2 & 2 & 1 \\ 4 & 3 & 0 & 2 \\ 0 & 5 & 3 & 2 \end{pmatrix}$ et $R = \begin{pmatrix} 10 & 15 & 3 \\ 12 & 8 & 2 \\ 4 & 12 & 4 \\ 3 & 5 & 1 \end{pmatrix}$.

a) Calculer le produit $P = FR$.

b) En déduire le coût de l'énergie nécessaire à la fabrication d'un article B.

2) Calculer le produit $U = P \times \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.
Donner une interprétation du résultat.

3) Calculer le produit $V = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \times P$.
Donner une interprétation du résultat.

4) À l'aide d'un produit matriciel, calculer le coût total pour produire 4 articles A, 3 articles B et 8 articles C.

5) À la fin d'une journée, on a constaté que la fabrication de ces trois articles a coûté 14 800 € en travail, 18 000 € en matières premières et 4 400 € en énergie. Déterminer le nombre d'articles A, B et C qui ont été fabriqués au cours de cette journée.

98 **Méthode de Cayley-Hamilton**

Soit la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c, d sont des réels.

1) Démontrer que $M^2 = (a+d)M - (ad - bc)I$.

2) En déduire que si $ad - bc \neq 0$, alors M est inversible. Retrouver dans ce cas l'inverse de M en fonction de a, b, c et d.

99 Montrer que l'équation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ a des solutions si, et seulement si, les réels a, b, c suivent dans cet ordre une progression arithmétique.

100 INFO

Avec un logiciel de calcul formel, étudier l'existence de solutions des systèmes en fonction des paramètres :

1) $\begin{cases} x + y + (1-m)z = m+2 \\ (1+m)x - y + 2z = 0 \\ 2x - my + 3z = m+2 \end{cases}$

2) $\begin{cases} x - my + m^2z = m \\ mx - m^2y + mz = 1 \\ mx + y - m^3z = -1 \end{cases}$

3) $\begin{cases} x + my + z = 1 \\ (m+1)x + 2y + (m-3)z = -1 \\ (m-1)x - 3z = -1 \end{cases}$

4) $\begin{cases} x + y + z + t = a \\ x - y - z + t = b \\ -x - y + z + t = c \\ -3x + y - 3z - 7t = d \end{cases}$

5) $\begin{cases} ax + by + z = 1 \\ x + aby + z = b \\ x + by + az = 1 \end{cases}$

6) $\begin{cases} \frac{x}{1+a} + \frac{y}{1+2a} + \frac{z}{1+3a} = 1 \\ \frac{x}{2+a} + \frac{y}{2+2a} + \frac{z}{2+3a} = 1 \\ \frac{x}{3+a} + \frac{y}{3+2a} + \frac{z}{3+3a} = 1 \end{cases}$

101 **Système non linéaire**

Le but est de résoudre le système $\begin{cases} x^3y^2z^6 = 1 \\ x^4y^5z^{12} = 2 \\ x^2y^2z^5 = 3 \end{cases}$

lorsque x, y, z sont des réels strictement positifs.

1) On pose $X = \ln x$, $Y = \ln y$ et $Z = \ln z$.
Montrer que la résolution du système revient à déterminer X, Y et Z tels que :

$$\begin{pmatrix} 3 & 2 & 6 \\ 4 & 5 & 12 \\ 2 & 2 & 5 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 \\ \ln 2 \\ \ln 3 \end{pmatrix}$$

2) À l'aide de la calculatrice, déterminer le triplet solution $(X\,;\,Y\,;\,Z)$.
En déduire le triplet $(x\,;\,y\,;\,z)$ solution du système.

102 **Matrice nilpotente**

Une matrice carrée A est dite **nilpotente** s'il existe un entier positif p tel que $A^p = 0$.

1) Montrer que si A est nilpotente, alors $I - A$ est inversible et préciser son inverse.

2) Montrer que la somme de deux matrices nilpotentes qui commutent est une matrice nilpotente.

103 Soit la matrice $A = \begin{pmatrix} 2 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ et la suite (u_n) définie par $u_0 = 0$ et $u_{n+1} = 2u_n + 3 \times 2^n$.

1) Démontrer que $A^n = \begin{pmatrix} 2^n & 0 & u_n \\ 0 & 1 & 0 \\ 0 & 0 & 2^n \end{pmatrix}$.

2) Soit $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

a) Vérifier que $DS = SD$.

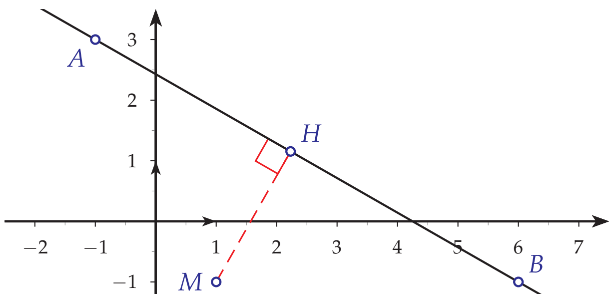
b) Montrer que, pour tout $k \geqslant 2$, on a $S^k = 0$.

c) Utiliser le formule du binôme de Newton pour calculer A^n.

3) En déduire (u_n) sous forme explicite.

104 **Matrice de Gram**

Dans un repère orthonormé $(O\,;\,\vec{\imath}, \vec{\jmath})$ du plan, soit (AB) une droite, M un point quelconque du plan et H le projeté orthogonal de M sur (AB).



On appelle **matrice de Gram**, associée aux vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AM}$, la matrice $G = \begin{pmatrix} \overrightarrow{AB} \cdot \overrightarrow{AB} & \overrightarrow{AB} \cdot \overrightarrow{AM} \\ \overrightarrow{AM} \cdot \overrightarrow{AB} & \overrightarrow{AM} \cdot \overrightarrow{AM} \end{pmatrix}$.

1) a) Justifier que la distance du point M à la droite (AB) est égale à MH.

b) Démontrer que $MH = \dfrac{\sqrt{\det(G)}}{AB}$.

2) Soit les points $A(-1\,;\,3)$, $B(6\,;\,-1)$ et $M(1\,;\,-1)$.

a) Déterminer la matrice de Gram associée aux vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AM}$.

b) En déduire la distance de M à (AB).

105 **Matrice idempotente**

Une matrice carrée A est dite **idempotente** si $A^2 = A$.

1) Soit une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Traduire par un système que A est idempotente.

2) Résoudre ce système en considérant deux cas :

- $b = 0$
- $b \neq 0$.

106 Produit nul

Le but est de prouver de deux façons, algébriquement puis par l'absurde, que : « si un produit de deux matrices carrées d'ordre 2 non nulles est nul, alors les deux matrices ne sont pas inversibles ».

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$.

1) a) Calculer le produit AB et exprimer un premier système qui traduit l'égalité $AB = 0$.

b) Démontrer que ce système équivaut à un système de huit produits nuls dans lesquels interviennent les déterminants de A et B.

c) Conclure.

2) a) Si A était inversible, que vaudrait B ?

b) Rédiger une démonstration par l'absurde sur la base de la constatation précédente.

107 Coefficients stœchiométriques

La combustion du butane (C_4H_{10}) en présence de dioxygène (O_2) produit du dioxyde de carbone (CO_2) et de la vapeur d'eau (H_2O).

L'équation-bilan de cette réaction est de la forme :

$$x\mathrm{C_4H_{10}} + y\mathrm{O_2} \to z\mathrm{CO_2} + t\mathrm{H_2O}$$

où x, y, z et t sont des entiers naturels.

1) a) Écrire le système linéaire qui traduit l'équilibre de cette équation-bilan.

b) En déduire une égalité matricielle de la forme $AX = B$ où A est une matrice carrée d'ordre 3, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et B est une matrice colonne dont les coefficients ne dépendent que de t.

c) Résoudre l'équation obtenue précédemment pour déterminer x, y et z en fonction de t.

d) En déduire les coefficients qui équilibrent l'équation-bilan.

2) Équilibrer les équations-bilans des réactions suivantes en procédant comme au **1**.

a) L'oxyde d'aluminium (Al_2O_3) réagit avec le carbone (C) et le dichlore (Cl_2) pour donner du chlorure d'aluminium ($AlCl_3$) et du monoxyde de carbone (CO).

b) Au cours de la photosynthèse, du dioxyde de carbone et de l'eau sont transformés en glucose ($C_6H_{12}O_6$) et en dioxygène.

c) Le permanganate de potassium ($KMnO_4$), l'acide sulfurique (H_2SO_4) et le sulfate ferreux ($FeSO_4$) réagissent pour donner du sulfate de potassium (K_2SO_4), du sulfate de manganèse ($MnSO_4$), du sulfate ferrique ($Fe_2(SO_4)_3$) et de l'eau (H_2O).

108 Fonctions homographiques

Soit deux fonctions : f définie pour $c \neq 0$ et $x \neq -\frac{d}{c}$, et g définie pour $c' \neq 0$ et $x \neq -\frac{d'}{c'}$ par :

$$f(x) = \frac{ax+b}{cx+d} \quad \text{et} \quad g(x) = \frac{a'x+b'}{c'x+d'}.$$

1) À quelles conditions f et g sont-elles des fonctions homographiques ?

2) Soit $h = f \circ g$ la fonction composée de g suivie de f c'est-à-dire telle que $h(x) = f[g(x)]$.

On admet que h est définie sur un ensemble $\mathcal{D}$, égal à $\mathbb{R}$ privé de $-\frac{d'}{c'}$ et éventuellement d'un autre réel.

a) Déterminer $h(x)$ et $\mathcal{D}$ lorsque :

$$f(x) = \frac{3x+4}{5x+6} \quad \text{et} \quad g(x) = \frac{4x-6}{-3x+5}.$$

b) Montrer qu'on peut écrire $h(x) = \frac{\alpha x + \beta}{\gamma x + \delta}$ avec :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

3) On appelle H, F et G les trois matrices ci-dessus dans l'ordre de gauche à droite.

a) Démontrer que la matrice H est inversible.

b) À quelle condition h est-elle une fonction homographique restreinte à $\mathcal{D}$?

4) a) Déterminer $h(x)$ et $\mathcal{D}$ lorsque :

$$f(x) = \frac{3x+5}{2x-1} \quad \text{et} \quad g(x) = \frac{x+5}{2x-3}.$$

b) Démontrer que, si F est l'inverse de G, alors h est la fonction identité $x \mapsto x$ restreinte à $\mathcal{D}$.

c) Peut-on déterminer une fonction f telle que $f \circ f$ soit la fonction identité $x \mapsto x$ restreinte à $\mathcal{D}$?

5) Démontrer que h ne peut pas être la fonction nulle.

6) En général, la composée de fonctions n'est pas commutative, c'est-à-dire que pour toutes fonctions r et s qu'on peut composer dans un sens ou dans l'autre, on n'a pas $r \circ s = s \circ r$.

a) Montrer que si f et g sont commutatives relativement à la composition, alors $FG = GF$.

b) Expliciter une condition nécessaire et suffisante pour qu'on ait $f \circ g = g \circ f$.

À la fin de ce chapitre, je dois être capable de :

Calculer sans calculatrice :
- une combinaison linéaire de matrices
- un produit de matrices
- une puissance de matrice
- l'inverse d'une matrice carrée d'ordre 2

Me servir d'une calculatrice pour :
- affecter une matrice à une variable
- effectuer des opérations sur les matrices
- calculer le déterminant, l'inverse d'une matrice carrée

Résoudre un système linéaire à l'aide des matrices

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Déterminer celles qui sont correctes.

Soit les matrices $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 & -1 \\ 3 & 0 & 2 \end{pmatrix}$.

109 Que vaut $A + B$?

a) $\begin{pmatrix} 2 & 2 & 0 \\ 3 & 1 & 2 \end{pmatrix}$

b) $\begin{pmatrix} 2 & 2 & 0 \\ 3 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix}$

c) $A + B$ n'existe pas

d) Aucune des trois propositions précédentes

110 Que vaut A^2 ?

a) $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 2 & 0 \end{pmatrix}$

c) $A^2 = A$

d) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$

111 Que vaut le produit AB ?

a) $\begin{pmatrix} 1 & 1 & 1 \\ 3 & 2 & 3 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 3 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & -1 \\ 3 & 0 & 2 \\ 3 & 0 & 2 \end{pmatrix}$

d) AB n'existe pas

112 Que vaut le produit BA ?

a) BA n'existe pas

b) $\begin{pmatrix} 1 & 1 & 1 \\ 3 & 2 & 3 \end{pmatrix}$

c) $BA = AB$

d) $\begin{pmatrix} 1 & 3 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}$

113 L'inverse de A :

a) est une matrice carrée d'ordre 3

b) n'existe pas

c) a un déterminant nul

d) égale $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

114 Pour tout entier naturel n non nul, on peut écrire $A^n = A + J$ avec J égale à :

a) $\begin{pmatrix} 0 & 0 & 0 \\ n-1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

b) $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & n-1 \\ 0 & 0 & 0 \end{pmatrix}$

c) $\begin{pmatrix} 0 & n-1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

d) $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & n-1 & 0 \end{pmatrix}$

115 Le produit de matrices AB est calculable si, et seulement si :

(a) A a autant de colonnes que B

(b) A a autant de colonnes que B a de lignes

(c) A a autant de lignes que B a de colonnes

(d) A a autant de lignes que B

116 Si le produit de matrices AB existe, alors c'est une matrice carrée si :

(a) A a autant de colonnes que B

(b) A a autant de colonnes que B a de lignes

(c) A a autant de lignes que B a de colonnes

(d) A a autant de lignes que B

117 Si le produit de la matrice A par la matrice B existe, alors on le calcule en multipliant :

(a) toute ligne de A par toute ligne de B

(b) toute colonne de A par toute ligne de B

(c) toute colonne de A par toute colonne de B

(d) toute ligne de A par toute colonne de B

118 La matrice $\begin{pmatrix} d & b \\ a & c \end{pmatrix}$ est inversible si :

(a) $ac - bd \neq 0$ (b) $ad - bc \neq 0$ (c) $cd - ab \neq 0$ (d) $bc - ad \neq 0$

119 Quelles que soient les matrices carrées de même ordre A, B, C et D, on a :

(a) $B^2 + B = B(B+1)$

(b) $A(BC) = (AB)C$

(c) $(A-B)(A+B) = A^2 - BA + AB - B^2$

(d) $(A+B)^2 = A^2 + 2AB + B^2$

120 Si A est une matrice carrée dont le carré est la matrice nulle 0, alors :

(a) A est inversible (b) $A = 0$ (c) $A^3 = 0$ (d) $(I-A)^{-1} = I + A$

121 Soit la matrice $H = \begin{pmatrix} k & 0 \\ 0 & -k \end{pmatrix}$ où $k \in \mathbb{R}^*$ et A une matrice carrée d'ordre 2. Alors :

(a) $AH = HA$ (b) $H^2 = k^2 I$ (c) $H^3 = -k^3 I$ (d) $k^2 H^{-1} = H$

122 Un **système de Cramer** est un système d'équations linéaires dont la matrice des coefficients est inversible. Parmi les systèmes linéaires suivants, lesquels sont des systèmes de Cramer ?

(a) $\begin{cases} x + 3y = 1 \\ 2x - y = 3 \end{cases}$ (b) $\begin{cases} 6x + 3y = 1 \\ 4x - 2y = 3 \end{cases}$ (c) $\begin{cases} x + 2y = 1 \\ -2x - 4y = 3 \end{cases}$ (d) $\begin{cases} 6x + 3y = 1 \\ 4x + 2y = 3 \end{cases}$

123 Le système $\begin{cases} 5x - 3y = 3 \\ 3x - 2y = 2 \end{cases}$ a pour solution le couple de réels $(x\ ;\ y)$ tels que :

(a) $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 & -3 \\ 3 & -2 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ (b) $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ -3 & 5 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ (c) $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2 & -3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ (d) $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ 3 & -5 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$

124 Pour quelle(s) valeur(s) de m, le système $\begin{cases} 2x + my = 4 \\ mx + y = 5 \end{cases}$ admet-il une unique solution ?

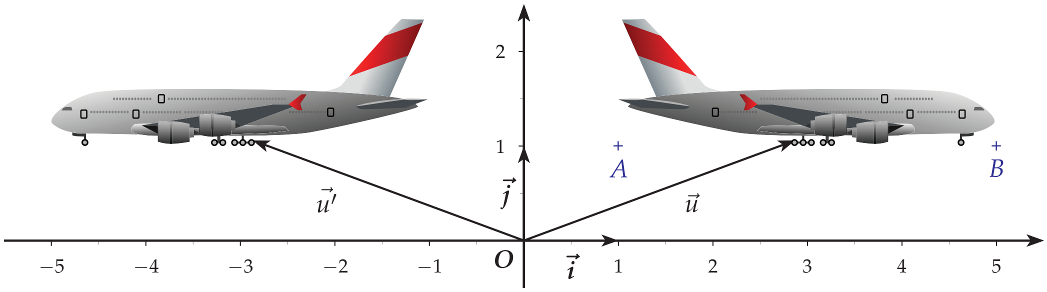
(a) $m = -\sqrt{2}$ (b) $m = 0$ (c) $m = \sqrt{2}$ (d) $m = 2$

TP 1 Traitement d'image

INFO

A Un peu de réflexions

1) À l'aide d'un logiciel de géométrie dynamique, réaliser la construction suivante :
- Insérer une image au choix (`Image1` et deux points A et B sont créés).
- Repositionner `Image1` telle que A soit en $(1\,;\,1)$.
- Créer la matrice $M = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Appliquer la matrice M à l'image `Image1` (l'image `Image1'` est créée).



Dans toute la suite, on se place dans un repère orthonormé direct $(O\,;\,\vec{i}\,,\,\vec{j})$.

2) Soit deux vecteurs $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\vec{u}'\begin{pmatrix} x' \\ y' \end{pmatrix}$ tels que $\begin{pmatrix} x' \\ y' \end{pmatrix} = M\begin{pmatrix} x \\ y \end{pmatrix}$.

a) Exprimer x' et y' en fonction de x et y.

b) En déduire que M est la matrice associée à la symétrie d'axe $(O\,;\,\vec{j})$.

3) Déterminer la matrice N associée à la symétrie d'axe $(O\,;\,\vec{i})$. Vérifier avec le logiciel.

4) Déterminer la matrice P associée à la symétrie de centre O. Vérifier avec le logiciel.

5) Exprimer P en fonction de M et N.

B Ça tourne !

Dans le plan complexe, soit deux points $M\begin{pmatrix} x \\ y \end{pmatrix}$ et $M'\begin{pmatrix} x' \\ y' \end{pmatrix}$ d'affixes $z = x + \mathrm{i}y$ et $z' = x' + \mathrm{i}y'$.

Soit la rotation de centre O et d'angle θ qui transforme M en M'.

1) Exprimer z' en fonction de z et θ.

2) En déduire les coordonnées de $\overrightarrow{OM'}$ en fonction de celles de $\overrightarrow{OM}$.

3) Déterminer alors la matrice R telle que $\begin{pmatrix} x' \\ y' \end{pmatrix} = R\begin{pmatrix} x \\ y \end{pmatrix}$.

4) Vérifier que la matrice R est inversible et déterminer son inverse.

5) a) Pour $\theta = \dfrac{\pi}{3}$, calculer R et R^{-1}.

b) À quel angle de rotation est associée la matrice R^{-1} ? Vérifier avec le logiciel.

TP 2 C'est du propre !

INFO

Soit une matrice carrée M et un vecteur colonne U non nul.
On dit que U est un **vecteur propre** de M s'il existe un réel λ tel que $MU = \lambda U$.
Le réel λ est alors appelé **valeur propre** de M, associée au vecteur propre U.

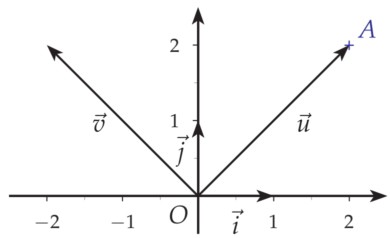
Dans le repère du plan $(O\,;\vec{i},\vec{j})$, on désignera par $\vec{u}$ un représentant du vecteur colonne U.

A Cas d'une matrice diagonale

Soit $D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et U un vecteur colonne de taille 2 non nul. On pose $V = DU$.

1) À l'aide d'un logiciel de géométrie dynamique, réaliser la construction suivante :

- Créer la matrice D.
- Placer un point A, puis créer le vecteur $\vec{u}$ tel que $\vec{u} = \overrightarrow{OA}$.
- Construire le représentant du vecteur $\vec{v}$ d'origine O en multipliant la matrice D par le vecteur $\vec{u}$.



2) Dans cette question, on cherche s'il existe $\lambda \in \mathbb{R}$ tel que $V = DU = \lambda U$.

a) Quelle condition doivent vérifier les vecteurs $\vec{u}$ et $\vec{v}$?

b) Dans le logiciel, déplacer $\vec{u}$ afin de satisfaire la condition établie précédemment.
Quelles semblent être les valeurs propres de D ?

c) Calculer les deux valeurs propres de D et donner un vecteur propre associé à chacune.

B Généralisation à une matrice carrée d'ordre 2

Soit la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

1) Démontrer l'équivalence : λ valeur propre de $M \Leftrightarrow M - \lambda I$ non inversible.

2) En déduire l'équivalence : λ valeur propre de $M \Leftrightarrow \lambda^2 - (a+d)\lambda + ad - bc = 0$.

3) En déduire une condition sur a, b, c et d pour que M ait deux valeurs propres.

C Application

Soit la matrice $M = \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix}$.

1) a) Vérifier la condition établie à la question **3** de la partie **B**.

b) Calculer les valeurs propres de M. On les note dans l'ordre croissant λ_1 et λ_2.

c) Vérifier que $U_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ et $U_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ sont des vecteurs propres associés respectivement à λ_1 et λ_2.

2) Soit les matrices $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$.

a) Montrer que $MP = PD$, puis que $M = PDP^{-1}$.

b) En déduire que, pour tout entier naturel n, on a $M^n = PD^nP^{-1}$.

c) Calculer M^n.

TP 3 Hill cipher

ALGO INFO

En cryptographie symétrique, le chiffrement de Hill est un système de chiffrement par bloc qui utilise les propriétés de l'arithmétique modulaire et des matrices. Inventé par Lester S. Hill en 1929, il consiste à substituer les lettres du message **clair**, non pas l'une après l'autre, mais par « paquets ». On obtient ainsi un message **chiffré** plus difficile à casser.
Chaque lettre est codée par son rang diminué de 1 dans l'alphabet latin.

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

Avant qu'il ne soit traité, on formate d'abord le message clair : on supprime accents, espaces et ponctuation, on regroupe les lettres par bloc de 2 (si une lettre reste orpheline à la fin, on ajoute arbitrairement une lettre), puis on remplace chaque lettre par le nombre correspondant dans le tableau. On forme ainsi une matrice à 2 lignes qu'on note X.

> Exemple `DE L'OR` $\mapsto \begin{array}{c|c|c} \mathtt{D} & \mathtt{L} & \mathtt{R} \\ \mathtt{E} & \mathtt{O} & \mathtt{A} \end{array} \mapsto \begin{pmatrix} 3 & 11 & 17 \\ 4 & 14 & 0 \end{pmatrix} = X$

Ensuite, on calcule AX, où A est une matrice carrée d'ordre 2 fixée, appelée **clé du chiffrement**. On obtient une matrice Y où chaque coefficient est remplacé par le plus petit entier naturel qui lui est congru modulo 26. Enfin, on convertit en lettres grâce au tableau.

> Exemple Appliquons la clé de chiffrement $A = \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix}$.
>
> $\begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix} \begin{pmatrix} 3 & 11 & 17 \\ 4 & 14 & 0 \end{pmatrix} = \begin{pmatrix} 33 & 119 & 119 \\ 47 & 167 & 85 \end{pmatrix} \mapsto \begin{pmatrix} 7 & 15 & 15 \\ 21 & 11 & 7 \end{pmatrix} = Y \mapsto \begin{array}{c|c|c} \mathtt{H} & \mathtt{P} & \mathtt{P} \\ \mathtt{V} & \mathtt{L} & \mathtt{H} \end{array} \mapsto$ `HVPLPH`

A Késako ?

On souhaite déchiffrer le message `KYBNSY` qui a été obtenu avec la clé précédente.

1) Déterminer la matrice chiffrée associée à ce message.

D'ordinaire, si A est inversible : $AX = Y \Leftrightarrow X = A^{-1}Y$. Mais ici : $AX \equiv Y \Leftrightarrow X \equiv A^{-1}Y$ [26].
Il faut donc **inverser A modulo 26** : c'est la **clé du déchiffrement**.

2) a) Écrire A^{-1} sous la forme $k^{-1}B$ avec B à coefficients entiers et k le déterminant de A.

b) Il existe des algorithmes efficaces pour déterminer l'inverse de k modulo n mais pour $n = 26$, la « force brute » est sans doute la manière la plus simple. Voici l'algorithme :

```
1. Multiplier successivement k par m ∈ {1,3,5,7,9,11,15,17,19,21,23,25}
2. Arrêter quand le produit km ≡ 1 [26]. Alors k⁻¹ ≡ m [26].
```

Déterminer par ce procédé l'inverse de k modulo 26. En déduire la clé du déchiffrement.

c) Déterminer sans calculatrice les deux premières lettres du message clair.

3) Dans un tableur, élaborer un déchiffrement automatique. Voici quelques formules utiles :

- `= CODE(lettre)-65` donne le nombre associé à la `lettre` dans le tableau précédent.
- `= MOD(n;26)` donne le reste de la division euclidienne de `n` par 26.
- `= CAR(nombre+65)` donne la lettre associée au `nombre` dans le tableau précédent.

B La clé pour bien choisir

1) On se donne maintenant pour clé de chiffrement la matrice $A = \begin{pmatrix} 9 & 4 \\ 8 & 5 \end{pmatrix}$.

a) Chiffrer le message « `L'EX GANG : BYE !` » avec cette clé.

b) Peut-on affirmer que les clés de chiffrement et de déchiffrement sont les mêmes ?

2) a) Montrer que deux mots de deux lettres, toutes différentes, peuvent donner deux mots chiffrés identiques.

b) Déterminer la condition pour qu'on ait $A\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x' \\ y' \end{pmatrix}$.

3) La matrice A est-elle inversible modulo 26 ? Pourquoi ?

4) On veut construire une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ inversible modulo 26.

a) Expliquer pourquoi les coefficients d'une même ligne ou d'une même colonne ne doivent être divisibles ni par 2 ni par 13.

b) a étant un entier fixé, expliquer comment choisir b et c.

C Casser le code

Un agent du KGB a intercepté un bout de message codé par un chiffrement de Hill (`FYIR`) et sa transcription en message clair (`VLAD`). Montrer que cela suffit à retrouver la clé du chiffrement.

Récréation, énigmes

Une **matrice magique** est une matrice carrée d'ordre $n \in \mathbb{N}^*$ dont les sommes des n coefficients de chaque ligne, colonne et diagonale sont égales à un même nombre, appelé alors **constante magique**. Si, en plus, les coefficients de la matrice sont les entiers de 1 à n^2, alors elle est dite **normale**.

1) Démontrer qu'il n'existe pas de matrice magique normale d'ordre 2.

2) Démontrer que le double de la constante magique est $n^3 + n$.

3) Soit une matrice magique normale $M = \begin{pmatrix} a & b & \maltese \\ c & d & \maltese \\ \maltese & \maltese & \maltese \end{pmatrix}$.

a) Réécrire cette matrice en remplaçant les croix maltaises $\maltese$ par des expressions qui dépendent de a, b, c et d.

b) Montrer que a, b, c et d vérifient un système de deux équations.

c) Résoudre ce système et en déduire une matrice magique normale d'ordre 3.

4) En 1956, dans les ruines du palais d'Anxi en banlieue de l'actuelle X'ian, ancienne capitale de la Chine, on a retrouvé une plaque métallique datant de la dynastie Yuan (1271-1368) où figure une grille de 36 cases remplies de chiffres arabes orientaux.

a) Vérifier que la matrice d'ordre 6 correspondant à cette grille est une matrice magique normale.

b) Vérifier que la matrice d'ordre 4 composée des coefficients encadrés en rouge est une matrice magique.

$$\begin{pmatrix} \text{۲۸} & \text{۴} & \text{۳} & \text{۳۱} & \text{۳۵} & \text{۱۰} \\ \text{۳۶} & \text{۱۸} & \text{۲۱} & \text{۲۴} & \text{۱۱} & \text{۱} \\ \text{۷} & \text{۲۳} & \text{۱۲} & \text{۱۷} & \text{۲۲} & \text{۳۰} \\ \text{۸} & \text{۱۳} & \text{۲۶} & \text{۱۹} & \text{۱۶} & \text{۲۹} \\ \text{۵} & \text{۲۰} & \text{۱۵} & \text{۱۴} & \text{۲۵} & \text{۳۲} \\ \text{۲۷} & \text{۳۳} & \text{۳۴} & \text{۶} & \text{۲} & \text{۹} \end{pmatrix}$$

MATRICES

2

Suites de matrices et marches aléatoires

Connaissances nécessaires à ce chapitre

- Connaître le calcul matriciel
- Utiliser les résultats sur les suites géométriques
- Utiliser les résultats sur les probabilités discrètes
- Démontrer par récurrence

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 Soit la suite (u_n) telle que $u_{n+1} = \dfrac{u_n}{3}$ et $u_0 = 27$.

1) Exprimer u_n en fonction de n.

2) Montrer que (u_n) converge et donner sa limite.

2 Soit la suite $(a_n)_{n\geqslant 0}$ telle que $a_{n+1} = -3a_n + 4$.

1) Montrer qu'il existe une valeur de a_0 pour laquelle (a_n) est une suite constante. On note k cette valeur.

2) Montrer que la suite (b_n) telle que $b_n = a_n - k$ est géométrique. En déduire a_n en fonction de n.

3 Soit $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & 2 \end{pmatrix}$ et $T = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$.

1) a) Avec la calculatrice, calculer D^2 et D^3.

b) Conjecturer l'expression de D^n.

c) Démontrer cette conjecture par récurrence.

2) Démontrer que $T^n = 0$ pour $n \geqslant 3$.

4 Soit $a = \dfrac{1+\sqrt{5}}{2}$, $b = \dfrac{1-\sqrt{5}}{2}$ et les matrices :

$$P = \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix} \text{ et } D = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

1) Vérifier que P est inversible et calculer P^{-1}.

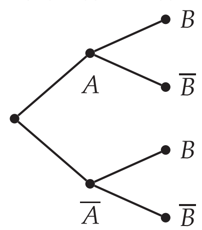
2) Calculer le produit PDP^{-1}.

5 Soit A et B deux événements d'un univers tels que $P(A) = \dfrac{3}{5}$, $P_A(B) = \dfrac{1}{2}$ et $P_{\overline{A}}(\overline{B}) = \dfrac{4}{5}$.

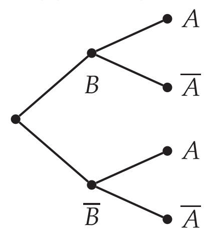
1) Calculer $P(B)$ puis $P_B(A)$.

2) Pondérer les arbres de probabilité suivants.

a)



b)



6 Le mathématicien Andreï Markov remarqua qu'en moyenne, sur les 20 000 premières lettres d'un roman de Pouchkine, une voyelle sur huit suit une voyelle et une consonne sur trois suit une consonne.

1) Donner les probabilités qu'une consonne suive une voyelle et vice-versa.

2) Soit $(X_n)_{n\geqslant 1}$ la suite de variables aléatoires valant 0 si la n-ième lettre est une voyelle et 1 sinon.

a) Pour tous i et j valant 0 ou 1, déterminer les probabilités $P_{\{X_n=i\}}(\{X_{n+1}=j\})$.

b) Exprimer $P(\{X_{n+1}=0\})$ et $P(\{X_{n+1}=1\})$ en fonction de $P(\{X_n=0\})$ et $P(\{X_n=1\})$.

Voir solutions p. 151

ACTIVITÉ 1 Des bactéries stratégiques

On étudie l'évolution d'une population de 500 000 bactéries confinées dans une enceinte.
On observe que ces micro-organismes unicellulaires peuvent opérer une mutation génétique dans le but de mieux assurer leur survie.
Ainsi, une bactérie peut alterner entre deux états adaptatifs A et B.
Des relevés statistiques ont montré que, d'un instant n au suivant :

- 5 % des bactéries passent de l'état A à l'état B ;
- 20 % des bactéries passent de l'état B à l'état A.

On note a_n et b_n les effectifs, exprimés en milliers, des deux populations de bactéries se trouvant respectivement dans l'état A et B à l'instant n.
On considère que la population reste constante au cours du temps.

Partie A : Conjectures sur l'évolution des populations

1) Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

2) Écrire un algorithme qui demande à l'utilisateur les valeurs de n et a_0, puis qui calcule et affiche les valeurs de a_n et b_n.

3) a) On fixe $a_0 = 375$. Tester l'algorithme pour $n = 10$, $n = 20$, puis $n = 30$.
Quelle conjecture peut-on faire sur l'évolution des effectifs a_n et b_n ?

b) On fixe $n = 30$. Tester l'algorithme pour $a_0 = 450$, puis $a_0 = 50$.
La répartition initiale des deux populations a-t-elle une influence sur leur évolution ?

Partie B : Modélisation à l'aide de suites de matrices

On définit la **suite de matrices colonnes** (U_n) telle que : $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

1) a) Montrer qu'il existe une matrice A telle que $U_{n+1} = AU_n$.
Par analogie avec les suites numériques, que peut-on dire de la suite de matrices (U_n) ?

b) En suivant l'analogie, exprimer le terme général U_n en fonction de U_0 et de A.

c) Déterminer A^n.

2) a) Montrer qu'il existe une matrice diagonale D et une matrice colonne E telles que :

$$U_{n+1} = DU_n + E.$$

b) Déterminer la matrice colonne telle que $C = DC + E$.

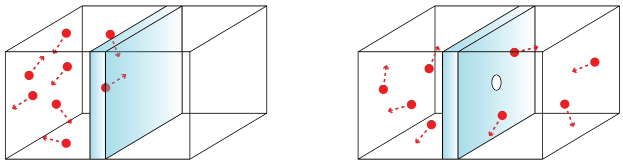
c) On considère la suite de matrices (X_n) définie par $X_n = U_n - C$.
Montrer que $X_{n+1} = DX_n$.

d) En déduire alors X_n, puis U_n en fonction de n, a_0 et b_0.

e) Montrer alors que la suite (U_n) converge vers C.

ACTIVITÉ 2 Modèle d'effusion d'Ehrenfest

Une enceinte hermétique est partagée en deux compartiments de même volume séparés par une paroi. On fait le vide dans l'un, on remplit l'autre d'un gaz, puis on perce un minuscule trou dans la paroi. Assez rapidement, les molécules de gaz migrent d'un compartiment vers l'autre, jusqu'à l'établissement d'une situation d'équilibre où, en moyenne, le nombre de molécules dans chaque compartiment est identique. Au niveau microscopique, rien n'empêche une molécule de revenir dans son compartiment d'origine : le phénomène est réversible. Mais, au niveau macroscopique, force est de constater que c'est irréversible. Il y a donc un paradoxe !



C'est dans l'idée d'expliquer ce paradoxe, qu'en 1907, les époux Ehrenfest imaginent un modèle avec deux urnes. Au départ, l'urne A contient n boules numérotées et l'urne B aucune. On tire alors au hasard un numéro entre 1 et n dans l'urne A ou B et on change d'urne la boule correspondante. Cette expérience aléatoire est répétée un certain nombre de fois.

Partie A : Quelques simulations pour étudier la réversibilité

```
1.  n, p, i, c EST_DU_TYPE NOMBRE
2.  X, Y EST_DU_TYPE LISTE
3.  TRAITEMENT
4.  LIRE n, p
5.  POUR i ALLANT_DE 1 A n
6.  Début POUR
7.   X[i] PREND_LA_VALEUR -random()
8.   Y[i] PREND_LA_VALEUR random()
9.   TRACER_POINT_Rouge (X[i],Y[i])
10. Fin POUR
11. POUR i ALLANT_DE 1 A p
12. Début POUR
13.  c PREND_LA_VALEUR ALGOBOX_ALEA_ENT(1,n)
14.  TRACER_POINT_Blanc (X[c],Y[c])
15.  X[c] PREND_LA_VALEUR -X[c]
16.  TRACER_POINT_Rouge (X[c],Y[c])
17. Fin POUR
```

Soit l'algorithme ci-contre.
La commande `random()` donne un nombre aléatoire dans $[0 ; 1]$ et `X[i]` désigne le `i`-ième élément de la liste `X`.

1) Programmer l'algorithme sous AlgoBox (utiliser un repère avec $Xmin = -1$, $Xmax = 1$, $Ymin = 0$ et $Ymax = 0$).

2) À quoi servent les lignes 6 à 9 ?

3) Expliquer comment le programme simule les échanges d'urnes dans les lignes 10 à 14 ?

4) Tester pour $\texttt{n} = 1\,000$ et $\texttt{p} = 10\,000$.
Le phénomène paraît-il réversible ?

5) Tester pour $\texttt{n} = 3$ et $\texttt{p} = 10$.
Le phénomène paraît-il réversible ?

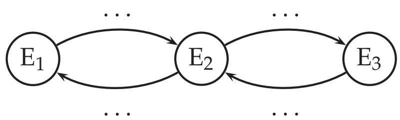
6) Afin de mieux étudier la réversibilité du phénomène, on souhaite que le programme s'arrête lors du premier retour à l'état initial et qu'il affiche le nombre d'échanges effectués.

- **a)** Supprimer la variable `p` et ajouter deux variables, `nA` et `compteur`, qui devront compter respectivement le nombre de boules dans l'urne A et le nombre d'échanges effectués.
- **b)** Remplacer la deuxième boucle `POUR...ALLANT_DE...A...` par une boucle du type `TANT_QUE...`
- **c)** En fonction de $\texttt{n} \in \{2, 3, \ldots, 10\}$, étudier la valeur de `compteur` affichée en sortie.

Partie B : Étude du cas où $n = 2$

1) Soit E_1 l'état initial et E_2 l'état après le premier échange.
Vérifier qu'il n'y a qu'un autre état différent possible. On l'appelle E_3.

2) Le schéma ci-dessous, appelé **graphe probabiliste**, indique les échanges entre les états par des arêtes orientées, pondérées par les probabilités de passer d'un état à l'autre.



Recopier ce graphe probabiliste et compléter ses probabilités.

3) Écrire la matrice T d'ordre 3 telle que t_{ij} est égal à la probabilité de passer de E_i à E_j.
On appelle cette matrice la **matrice de transition** associée au graphe probabiliste.

4) Soit (a_n), (b_n) et (c_n) trois suites de termes généraux a_n, b_n et c_n respectivement égaux aux probabilités d'être dans les états E_1, E_2 et E_3 à l'étape n.
On note U_n la matrice ligne $\begin{pmatrix} a_n & b_n & c_n \end{pmatrix}$ associée à l'étape n.

a) Déterminer U_0.

b) Justifier que, pour tout $n \in \mathbb{N}$, $U_{n+1} = U_n T$.

c) Démontrer que, pour tout $n \in \mathbb{N}$, $U_n = U_0 T^n$.

5) a) À l'aide de la calculatrice, calculer T^2 et T^3, puis conjecturer une expression de T^n.

b) Démontrer par récurrence la conjecture précédente.

6) Démontrer qu'au bout de n étapes, les deux boules sont dans la même urne si n est pair et ne sont pas dans la même urne si n est impair.

ACTIVITÉ 3 Des marches aléatoires

En 1905, pour expliquer les migrations d'une population de moustiques dans une forêt, le biostatisticien Karl Pearson décrit le premier une **marche aléatoire** [1] : « Un homme part d'un point O et parcourt ℓ yards en ligne droite ; il tourne d'un angle quelconque, et marche de nouveau ℓ yards en ligne droite. Il répète ce processus n fois. ». Assez vite, le physicien Lord Rayleigh calcule la probabilité que l'homme soit à une certaine distance de O quand n est grand et Pearson en tire la leçon que : « dans une zone ouverte, l'endroit le plus probable pour trouver un ivrogne encore capable de tenir sur ses pieds se trouve quelque part dans le voisinage de son point de départ. »

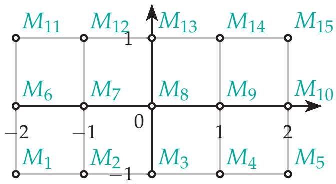
Partie A : Marche aléatoire sur un quadrillage

On modélise les déplacements d'un ivrogne dans un espace public en considérant, dans un repère orthonormé du plan, la marche aléatoire d'un point à coordonnées entières par des déplacements unitaires équiprobables vers l'un des quatre points cardinaux possibles.
On appelle « états » l'ensemble des points M_i atteignables qu'on numérote de bas en haut et de gauche à droite. On appelle « étape » de la marche aléatoire un changement d'état ou une conservation de l'état (par va-et-vient).

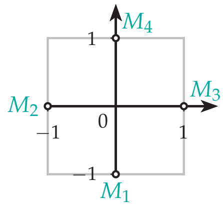
1. Cette expression est cependant introduite plus tard par le mathématicien hongrois György Pólya, vers 1919-1921.

Exemple

Si $-2 \leqslant x \leqslant 2$ et $-1 \leqslant y \leqslant 1$, la marche aléatoire a 15 états possibles. S'il est en M_8, alors, à l'étape d'après, il sera en M_9, M_{13}, M_7 ou M_3. S'il est en M_1, alors, à l'étape d'après, il sera en M_2 ou M_6.



1) Soit la marche aléatoire définie par le graphique ci-contre.



a) Représenter son graphe probabiliste (remarquer qu'on peut garder par exemple l'état M_1 par le va-et-vient $M_1 \to (-1\,;\,-1) \to M_1$).

b) Écrire sa matrice de transition T telle que t_{ij} est la probabilité de passage de M_i à M_j.

2) Soit la matrice ligne L_n de taille 4 dont les coefficients sont, dans l'ordre de gauche à droite, les probabilités d'être dans les états M_1, M_2, M_3 et M_4 après n étapes.
On dit que L_n est la **répartition de probabilité** de la marche aléatoire à l'étape n.

a) Dans toute la suite, on fixe $L_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$. Que représente cette matrice ?

b) Où l'ivrogne a-t-il le plus de chance de se trouver après :

- 1 étape ?
- 2 étapes ?
- 5 étapes ?
- 10 étapes ?

c) Intuitivement, pour n assez grand, où l'ivrogne a-t-il le plus de chance de se trouver ? Que peut-on alors supposer pour $\lim\limits_{n \to +\infty} (L_n)$?

d) Soit $L = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$. Vérifier que $LT = L$.
On dit que L est la **répartition stable** de la marche aléatoire.

e) La position initiale de l'ivrogne semble-t-elle avoir une influence sur sa marche aléatoire ?

Partie B : Marche aléatoire sur un triangle isocèle rectangle

Sur un triangle $S_1S_2S_3$ isocèle rectangle en S_1, un robot suit une marche aléatoire entre trois états qui sont les sommets du triangle et telle que la probabilité de passer d'un sommet à l'autre est proportionnelle à la longueur du côté emprunté (par exemple, si le robot est en S_1, la probabilité qu'il aille en S_2 ou en S_3 est $\frac{1}{2}$ puisque $S_1S_2 = S_1S_3$).

1) a) Soit $S_1S_2 = \ell$. Exprimer S_2S_3 en fonction de ℓ.

b) En déduire la probabilité que le robot aille en S_1 sachant qu'il est en S_2.

c) Représenter le graphe de cette marche aléatoire.

d) Vérifier que $T = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \sqrt{2}-1 & 0 & 2-\sqrt{2} \\ \sqrt{2}-1 & 2-\sqrt{2} & 0 \end{pmatrix}$ est sa matrice de transition.

2) Soit les matrices $P = \begin{pmatrix} 1 & 12\sqrt{2}-18 & 0 \\ 1 & 30\sqrt{2}-42 & 1 \\ 1 & 30\sqrt{2}-42 & -1 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-\sqrt{2} & 0 \\ 0 & 0 & \sqrt{2}-2 \end{pmatrix}$.

À l'aide d'un logiciel de calcul formel :

a) Vérifier que P est inversible et que $T = PDP^{-1}$.

b) Déterminer, pour tout entier naturel n, D^n.

c) Démontrer par récurrence que, pour tout entier naturel n, $T^n = PD^nP^{-1}$.

d) Déterminer T^n en fonction de n. En déduire $\lim\limits_{n \to +\infty} (T^n)$.

1. Puissances d'une matrice

La puissance n-ième d'une matrice intervient souvent dans les calculs mais en donner une expression en fonction de n est souvent difficile. Cependant, nous allons voir que, dans des cas particuliers, c'est possible.

A. Puissances d'une matrice diagonale

PROPRIÉTÉ : Puissance d'une matrice diagonale

Soit une matrice diagonale $D = \text{diag}(d_1, d_2, \ldots, d_p)$ d'ordre p et n un entier naturel.
La puissance n-ième de D est la matrice $D^n = \text{diag}(d_1^n, d_2^n, \ldots, d_p^n)$.

PREUVE

On démontre cette propriété par récurrence. Voici l'initialisation et l'hérédité :

- $D^0 = I = \text{diag}(1, 1, \ldots, 1) = \text{diag}(d_1^0, d_2^0, \ldots, d_p^0)$. Donc la propriété est vraie pour $n = 0$.
- Supposons que, pour un certain entier naturel n, $D^n = \text{diag}(d_1^n, d_2^n, \ldots, d_p^n)$.

$$D^{n+1} = D^n D = \begin{pmatrix} d_1^n & 0 & \ldots & 0 \\ 0 & d_2^n & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_p^n \end{pmatrix} \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_p \end{pmatrix} = \begin{pmatrix} d_1^{n+1} & 0 & \ldots & 0 \\ 0 & d_2^{n+1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_p^{n+1} \end{pmatrix}.$$

Donc la propriété est héréditaire.

Exemple Soit $D = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}$. Alors $D^n = \begin{pmatrix} (-2)^n & 0 \\ 0 & (-1)^n \end{pmatrix}$.

B. Puissances d'une matrice diagonalisable

DÉFINITION : Matrice diagonalisable

Une matrice carrée A est **diagonalisable** s'il existe une matrice inversible P et une matrice diagonale D telles que $A = PDP^{-1}$.

Exemple $A = \begin{pmatrix} -4 & 6 \\ -1 & 1 \end{pmatrix}$ est diagonalisable. En effet, soit $P = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}$.

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

PROPRIÉTÉ : Puissances d'une matrice diagonalisable

Si A est une matrice diagonalisable telle que $A = PDP^{-1}$ avec P une matrice inversible et D une matrice diagonale, alors, pour tout entier naturel non nul n, $A^n = PD^nP^{-1}$.

PREUVE On démontre cette propriété par récurrence. Voici l'initialisation et l'hérédité :

- $A^1 = A = PDP^{-1} = PD^1P^{-1}$. Donc la propriété est vraie pour $n = 1$.
- Supposons que, pour un entier n donné, $A^n = PD^nP^{-1}$. Montrons que $A^{n+1} = PD^{n+1}P^{-1}$
$A^{n+1} = A^nA = (PD^nP^{-1})(PDP^{-1}) = PD^n(P^{-1}P)DP^{-1} = PD^nIDP^{-1} = PD^{n+1}P^{-1}$.

Exemple Reprenons la matrice A de l'exemple précédent. Calculons A^4.

$$A^4 = PD^4P^{-1} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 16 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 48 & 2 \\ 16 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 46 & -90 \\ 15 & -29 \end{pmatrix}.$$

MÉTHODE 1 Déterminer M^n lorsque M est diagonalisable

► Ex. 11 p. 127

1) M est diagonalisable donc $M = PDP^{-1}$. En général, une au moins des matrices P et D est donnée (la **diagonalisation**, procédé pour les trouver, est hors programme en Terminale).
2) On démontre par récurrence que $M^n = PD^nP^{-1}$ (voir au bas de la page 120).

Exercice d'application On considère la matrice T diagonalisable telle que :

$$T = \begin{pmatrix} 0,6 & 0,3 & 0,1 \\ 0,3 & 0,6 & 0,1 \\ 0,5 & 0,5 & 0 \end{pmatrix} = PDP^{-1} \text{ avec } P \text{ inversible, } P = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & -10 \end{pmatrix}$$

et D une matrice diagonale.

Déterminer T^n avec une calculatrice, puis avec un logiciel de calcul formel.

Correction **Avec la calculatrice :**

- On sait que $T = PDP^{-1}$ donc $D = P^{-1}TP$. On obtient $D = \text{diag}\,(1\ ;\ 0,3\ ;\ -0,1)$.
- On calcule alors $T^n = PD^nP^{-1}$ avec $D^n = \text{diag}\,(1\ ;\ 0,3^n\ ;\ (-0,1)^n)$. On obtient :

$$T^n = \frac{1}{22}\begin{pmatrix} (-0,1)^n + 11 \times 0,3^n + 10 & (-0,1)^n - 11 \times 0,3^n + 10 & 2(1-(-0,1)^n) \\ (-0,1)^n - 11 \times 0,3^n + 10 & (-0,1)^n + 11 \times 0,3^n + 10 & 2(1-(-0,1)^n) \\ -10(-0,1)^n + 10 & -10(-0,1)^n + 10 & 2(1+10(-0,1)^n) \end{pmatrix}$$

Avec le logiciel de calcul formel Xcas :

- On crée la matrice T en mettant ses coefficients sous la forme de fraction :

```
T:=float2rational([[0.6,0.3,0.1],[0.3,0.6,0.1],[0.5,0.5,0]])
```

- On élève T à la puissance n : `matpow(T,n)`.

On obtient : $\left[\begin{array}{ccc} \frac{(-\frac{1}{10})^n+11*(\frac{3}{10})^n+10}{22} & \frac{(-\frac{1}{10})^n-11*(\frac{3}{10})^n+10}{22} & \frac{-((-\frac{1}{10})^n+1)}{11} \\ \frac{(-\frac{1}{10})^n-11*(\frac{3}{10})^n+10}{22} & \frac{(-\frac{1}{10})^n+11*(\frac{3}{10})^n+10}{22} & \frac{-((-\frac{1}{10})^n+1)}{11} \\ \frac{-10*((-\frac{1}{10})^n+10)}{22} & \frac{-10*((-\frac{1}{10})^n+10)}{22} & \frac{10*((-\frac{1}{10})^n+1)}{11} \end{array}\right]$.

2. Suites de matrices colonnes

A. Généralités

DÉFINITION : Suite de matrices colonnes

Une suite de matrices colonnes de taille $k \geqslant 2$ est une fonction qui, à tout entier naturel n, associe une matrice colonne de même taille.

REMARQUE : Cette définition prolonge celle de suite numérique. On peut ainsi rencontrer des suites de matrices définies explicitement ou par récurrence.

Exemple Soit (U_n) la suite de matrices colonnes $U_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $U_1 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$, $U_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$, ...

Cette suite peut être définie explicitement avec $U_n = \begin{pmatrix} 2n+1 \\ 2^n \end{pmatrix}$ mais aussi par la relation de récurrence $U_{n+1} = AU_n + B$ avec $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$ et $U_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

DÉFINITION : Convergence, limite d'une suite de matrices colonnes

Une suite de matrices colonnes $(U_n) = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ converge si les suites numériques (a_n) et (b_n) convergent. Sa limite est alors la matrice colonne formée par les limites de ces deux suites.

Exemple Soit (U_n) la suite de matrices colonnes de terme général $U_n = \begin{pmatrix} \frac{2n+1}{n+1} \\ \frac{1}{2^n} \end{pmatrix}$.

On a $\lim\limits_{n\to+\infty} \dfrac{2n+1}{n+1} = \lim\limits_{n\to+\infty} \dfrac{2+\frac{1}{n}}{1+\frac{1}{n}} = 2$ et $\lim\limits_{n\to+\infty} \dfrac{1}{2^n} = 0$. Donc $\lim\limits_{n\to+\infty} U_n = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$.

REMARQUE : On définit naturellement une suite de matrices colonnes de taille supérieure.

B. Suites définies par $U_{n+1} = AU_n$ ou $U_{n+1} = AU_n + B$

PROPRIÉTÉ

Soit (U_n) une suite de matrices colonnes de taille k définie par $U_{n+1} = AU_n$, pour tout $n \in \mathbb{N}$, avec A une matrice carrée d'ordre k. Alors, le terme général de (U_n) peut s'écrire $U_n = A^n U_0$.

PREUVE On démontre par récurrence sur n. Voici l'initialisation et l'hérédité :

- Initialisation : $U_0 = IU_0 = A^0 U_0$. Donc la propriété est vraie pour $n = 0$.
- Hérédité : Si, pour n entier donné, $U_n = A^n U_0$, alors $U_{n+1} = AU_n = A \times A^n U_0 = A^{n+1} U_0$.

MÉTHODE 2 Expliciter U_n pour (U_n) définie par $U_{n+1} = AU_n + B$

► Ex. 23 p. 128

Exercice d'application Soit la suite de matrices colonnes (U_n) définie par $U_{n+1} = AU_n + B$ avec :

$$U_0 = \begin{pmatrix} 6 \\ -1 \end{pmatrix},\ A = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \text{ et } B = \begin{pmatrix} 4 \\ -2 \end{pmatrix}.$$

1) Démontrer par récurrence que, pour tout $n \in \mathbb{N}$, $A^n = \begin{pmatrix} 2^n & 0 \\ n2^{n-1} & 2^n \end{pmatrix}$.
2) Déterminer la matrice C telle que : $C = AC + B$.
3) On pose, pour tout $n \in \mathbb{N}$, $V_n = U_n - C$. Montrer que, pour tout $n \in \mathbb{N}$, $V_n = A^n \times V_0$.
4) En déduire une expression U_n en fonction de n.

Correction

1)
- Pour $n = 0$, on a $A^0 = I$, donc la proposition est vraie.
- Supposons la proposition vraie pour n donné. Montrons qu'elle l'est encore au rang $n+1$.

$$A^{n+1} = A^n A = \begin{pmatrix} 2^n & 0 \\ n2^{n-1} & 2^n \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2^{n+1} & 0 \\ n2^n + 2^n & (-1)^{n+1} \end{pmatrix} = \begin{pmatrix} 2^{n+1} & 0 \\ (n+1)2^n & 2^{n+1} \end{pmatrix}.$$

- La proposition est initialisée au rang 0 et héréditaire, donc elle est vraie pour tout $n \in \mathbb{N}$.

2) $C = AC + B \Leftrightarrow (I - A)C = B$. Or, $\det(I - A) = 1$ donc $I - A$ est inversible.

On a $(I-A)^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$. D'où : $C = (I-A)^{-1}B = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 4 \\ -2 \end{pmatrix} = \begin{pmatrix} -4 \\ 6 \end{pmatrix}$.

3) Pour tout $n \in \mathbb{N}$, $V_{n+1} = U_{n+1} - C = AU_n + B - AC - B = A(U_n - C) = AV_n$.

Or, une suite $(V_n)_{n\geqslant 0}$ définie par $V_{n+1} = AV_n$ est telle que $V_n = A^n \times V_0$.

4) $U_n = V_n + C = A^n \times V_0 + C = \begin{pmatrix} 2^n & 0 \\ n2^{n-1} & 2^n \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} + \begin{pmatrix} -4 \\ 6 \end{pmatrix} = \begin{pmatrix} 2^{n+1} - 4 \\ n2^{n+1} + 6 \end{pmatrix}$.

3. Marche aléatoire

A. Marche aléatoire entre deux états

DÉFINITION : Marche aléatoire entre deux états

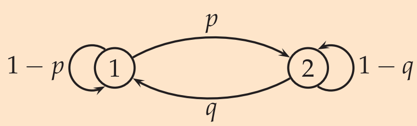
Lorsqu'un système n'ayant que deux états possibles évolue par étapes successives aléatoires et indépendantes, on dit qu'il suit une **marche aléatoire** entre ses deux états.

Exemple Akwa, un chien ayant une puce, rencontre Bali, un autre chien. Chaque seconde, la puce reste sur un chien ou va sur l'autre. On a un système à deux états : l'état 1 (la puce est sur Akwa) et l'état 2 (la puce est sur Bali) dont l'évolution est une marche aléatoire entre ces deux états.

DÉFINITIONS : Graphe probabiliste - Matrice de transition

Soit une marche aléatoire entre deux états 1 et 2 avec p la probabilité qu'il passe de 1 à 2 et q la probabilité qu'il passe de 2 à 1. On lui associe ci-dessous :

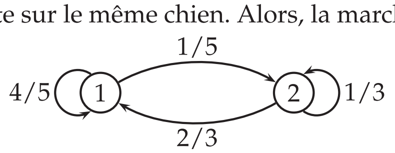
- le **graphe probabiliste** qui schématise les échanges entre 1 et 2 par des arêtes orientées, pondérées par les probabilités de passer d'un état à l'autre ou de rester au même état.
- la **matrice de transition** T est la matrice telle que le coefficient t_{ij} est égal à la probabilité :
  - de passer de l'état i à l'état j lorsque $i \neq j$;
  - de rester à l'état i lorsque $i = j$.



$$T = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}$$

Remarque : Une matrice de transition est dite **stochastique** : ses coefficients appartiennent à l'intervalle $[0\,;\,1]$ et la somme des coefficients de chacune de ses lignes est égale à 1.

Exemple Reprenons nos chiens et supposons que chaque seconde : soit la puce va d'Akwa (état 1) à Bali (état 2) une fois sur cinq, soit elle va de Bali à Akwa deux fois sur trois, soit elle reste sur le même chien. Alors, la marche aléatoire a pour graphe et matrice de transition :



$$T = \begin{pmatrix} 4/5 & 1/5 \\ 2/3 & 1/3 \end{pmatrix}$$

DÉFINITION

Pour $n \in \mathbb{N}$, on note :

- l'événement A_n : « le système est dans l'état A à l'étape n » ;
- l'événement B_n : « le système est dans l'état B à l'étape n » ;
- les probabilités $a_n = P(A_n)$ et $b_n = P(B_n)$ telles que $a_n + b_n = 1$.

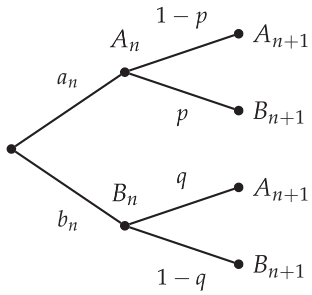
La matrice ligne $M_n = \begin{pmatrix} a_n & b_n \end{pmatrix}$ est appelée la **répartition de probabilité à l'étape n**.

PROPRIÉTÉ

Pour tout $n \in \mathbb{N}$, on a :

- $M_{n+1} = M_n T$
- $M_n = M_0 T^n$.

PREUVE Faisons un arbre de probabilité du passage de l'étape n à l'étape $n+1$.



$$\begin{aligned} P(A_{n+1}) &= P(A_n \cap A_{n+1}) + P(B_n \cap A_{n+1}) \\ &= (1-p)a_n + qb_n \\ P(B_{n+1}) &= P(A_n \cap B_{n+1}) + P(B_n \cap B_{n+1}) \\ &= pa_n + (1-q)b_n \end{aligned}$$

$$M_nT = \begin{pmatrix} a_n & b_n \end{pmatrix} \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix} = \begin{pmatrix} (1-p)a_n + qb_n & pa_n + (1-q)b_n \end{pmatrix} = M_{n+1}.$$

On démontre par récurrence que, pour tout $n \in \mathbb{N}$, on a $M_n = M_0T^n$.

B. Étude asymptotique d'une marche aléatoire entre deux états

DÉFINITION

Une **répartition stable de probabilité** est une répartition de probabilité M telle que $M = MT$.

PROPRIÉTÉ

Avec les notations précédentes, si $(p\,;\,q) \neq (0\,;\,0)$ et $(p\,;\,q) \neq (1\,;\,1)$, alors :

- il existe une unique répartition stable de probabilité donnée par $M = \begin{pmatrix} \dfrac{q}{p+q} & \dfrac{p}{p+q} \end{pmatrix}$;
- la suite (M_n) converge vers M, indépendamment de la répartition initiale M_0.

PREUVE

- $MT = M$ donc $\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix} = \begin{pmatrix} (1-p)x + qy & px + (1-q)y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix}$.

  D'où le système $\begin{cases} x - xp + yq = x \\ x + y = 1 \end{cases}$ qui a pour solution $\begin{cases} x = \dfrac{q}{p+q} \\ y = \dfrac{p}{p+q} \end{cases}$.

- $a_{n+1} = (1-p)a_n + qb_n$ et $b_n = 1 - a_n$ donc $a_{n+1} = (1-p-q)a_n + q$.

  Pour tout entier naturel n, posons $u_n = a_n - \dfrac{q}{p+q}$. Alors :

  $$\begin{aligned} u_{n+1} = a_{n+1} - \frac{q}{p+q} &= (1-p-q)a_n + q - \frac{q}{p+q} = (1-p-q)a_n - \frac{q(1-p-q)}{p+q} \\ &= (1-p-q)\left(a_n - \frac{q}{p+q}\right) = (1-p-q)u_n. \end{aligned}$$

  Donc (u_n) est une suite géométrique de raison $1-p-q$ et on a $u_n = (1-p-q)^n u_0$.

  Or, $0 \leqslant p+q \leqslant 2$, $p+q \neq 0$ et $p+q \neq 2$ donc $0 < p+q < 2$.

  D'où $-2 < -p-q < 0 \Leftrightarrow -1 < 1-p-q < 1$. Cela entraîne que $\lim\limits_{n \to +\infty} (1-p-q)^n = 0$.

  La suite (u_n) converge donc vers 0. Ainsi, $\lim\limits_{n \to +\infty} a_n = \dfrac{q}{p+q}$ et $\lim\limits_{n \to +\infty} b_n = \dfrac{p}{p+q}$.

  On a donc bien $\lim\limits_{n \to +\infty} M_n = M$ avec $M = \begin{pmatrix} \dfrac{q}{p+q} & \dfrac{p}{p+q} \end{pmatrix}$ quelle que soit M_0.

Remarque : En Terminale S, y compris à l'examen, il n'est pas demandé de connaître la définition de la répartition stable et la propriété précédente. Dans un exercice, tout ce qui concerne l'étude asymptotique d'une marche aléatoire est guidé.

MÉTHODE 3 Étudier le comportement asymptotique d'une marche aléatoire ► Ex. 27 p. 129

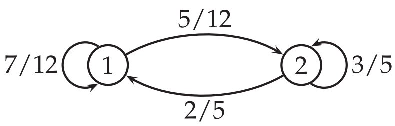
Exercice d'application

Akwa, un chien ayant une puce, rencontre Bali, un chien qui n'en a pas.
Chaque seconde, soit la puce va d'Akwa (état 1) à Bali (état 2) cinq fois sur douze, soit elle va de Bali à Akwa deux fois sur cinq, soit elle reste sur le même chien.
On note $M_n = \begin{pmatrix} a_n & b_n \end{pmatrix}$ la répartition de probabilité au bout de n secondes.

1) Déterminer le graphe et la matrice de transition T associés à cette marche aléatoire.
2) Quelle est la répartition de probabilité au bout de 2 secondes ?
3) Démontrer que, pour tout n entier naturel, $a_{n+1} = \dfrac{11}{60}a_n + \dfrac{2}{5}$.
4) On pose $u_n = a_n - \dfrac{24}{49}$. Démontrer que (u_n) est une suite géométrique de raison $\dfrac{11}{60}$.
5) En déduire que $\lim\limits_{n\to+\infty} M_n = M = \begin{pmatrix} \dfrac{24}{49} & \dfrac{25}{49} \end{pmatrix}$. Interpréter ce résultat.
6) Vérifier que M est une répartition stable de probabilité, c'est-à-dire que $M = MT$.

Correction

1) La marche aléatoire a pour graphe et matrice de transition :



$$T = \begin{pmatrix} 7/12 & 5/12 \\ 2/5 & 3/5 \end{pmatrix}$$

2) Initialement, la puce est sur Akwa donc $M_0 = \begin{pmatrix} 1 & 0 \end{pmatrix}$.
Avec la calculatrice, on calcule le produit $M_2 = M_0 \times T^2 = \begin{pmatrix} 73/144 & 71/144 \end{pmatrix}$.

3) $M_{n+1} = M_n T$ donc $\begin{pmatrix} a_{n+1} & b_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \end{pmatrix} \begin{pmatrix} 7/12 & 5/12 \\ 2/5 & 3/5 \end{pmatrix}$.

Cela donne le système $\begin{cases} a_{n+1} = \dfrac{7}{12}a_n + \dfrac{2}{5}b_n \\ b_{n+1} = \dfrac{5}{12}a_n + \dfrac{3}{5}b_n \end{cases}$. Or, $a_n + b_n = 1$ donc $b_n = 1 - a_n$.

Ainsi, $a_{n+1} = \dfrac{7}{12}a_n + \dfrac{2}{5}b_n = \dfrac{7}{12}a_n + \dfrac{2}{5} - \dfrac{2}{5}a_n = \dfrac{11}{60}a_n + \dfrac{2}{5}$.

4) $u_{n+1} = a_{n+1} - \dfrac{24}{49} = \dfrac{11}{60}a_n + \dfrac{2}{5} - \dfrac{24}{49} = \dfrac{11}{60}a_n - \dfrac{22}{245} = \dfrac{11}{60}\left(a_n - \dfrac{24}{49}\right) = \dfrac{11}{60}u_n$.

Donc (u_n) est une suite géométrique de raison $\dfrac{11}{60}$.

5) (u_n) est une suite géométrique de raison $\dfrac{11}{60} < 1$. Donc $\lim\limits_{n\to+\infty} u_n = 0$.

$u_n = a_n - \dfrac{24}{49}$ donc $\lim\limits_{n\to+\infty} a_n = \dfrac{24}{49}$. Et $b_n = 1 - a_n$ donc $\lim\limits_{n\to+\infty} b_n = 1 - \dfrac{24}{49} = \dfrac{25}{49}$.

Finalement, on a donc $\lim\limits_{n\to+\infty} M_n = \begin{pmatrix} \dfrac{24}{49} & \dfrac{25}{49} \end{pmatrix}$. Cela signifie qu'au bout d'un certain temps suffisamment long, il y a un peu plus de chance de trouver la puce sur Bali que sur Akwa puisque l'écart entre les deux probabilités est de $\dfrac{1}{49}$.

6) Avec la calculatrice ou un logiciel de calcul formel, on vérifie en effet que $MT = M$.

Remarque : Pour une marche aléatoire qui comporte trois états ou plus, l'étude asymptotique est similaire. La difficulté des calculs croît évidemment avec le nombre d'états et on aura alors recours à la calculatrice ou à un logiciel de calcul formel.

Activités mentales

1 Soit a et b deux réels et n un entier naturel.
Déterminer si chaque proposition est vraie ou fausse.

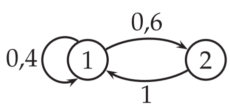
1) Soit $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. Pour tout n non nul, $A^n = \begin{pmatrix} 0 & 1 \\ 2^n & 0 \end{pmatrix}$.

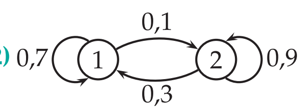
2) Soit $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Pour tout n, $A^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$.

3) Soit $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Pour tout n, $A^{4n} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

4) Soit $A = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}$. Pour tout $n \geqslant 2$, $A^n = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2 Le graphe donné peut-il être le graphe probabiliste d'une marche aléatoire ?

1) 

2) 

3 La matrice donnée peut-elle être la matrice de transition d'une marche aléatoire ?

1) $\begin{pmatrix} 0,43 & 0,67 \\ 0,57 & 0,33 \end{pmatrix}$

2) $\begin{pmatrix} 0,08 & 0,92 \\ 0,91 & 0,09 \end{pmatrix}$

3) $\begin{pmatrix} 1 & 0 \\ 0,5 & 0,5 \end{pmatrix}$

4) $\begin{pmatrix} 1,2 & -0,2 \\ -0,4 & 1,4 \end{pmatrix}$

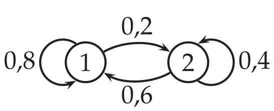
4 La matrice M est-elle la répartition stable de probabilité associée à la matrice de transition T, c'est-à-dire la matrice qui vérifie $M = MT$?

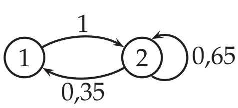
1) $M = \begin{pmatrix} \frac{1}{7} & \frac{6}{7} \end{pmatrix}$ et $T = \begin{pmatrix} 1/3 & 2/3 \\ 1/9 & 8/9 \end{pmatrix}$

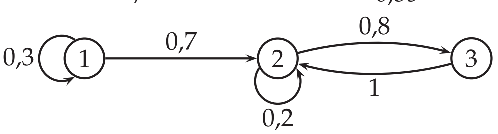
2) $M = \begin{pmatrix} \frac{5}{9} & \frac{4}{9} \end{pmatrix}$ et $T = \begin{pmatrix} 1/4 & 3/4 \\ 3/5 & 2/5 \end{pmatrix}$

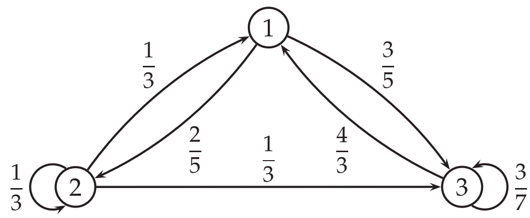
3) $M = \begin{pmatrix} \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix}$ et $T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$

5 Déterminer la matrice de transition associée à la marche aléatoire définie par le graphe donné.

1) 

2) 

3) 

4) 

6 On donne la matrice de transition d'une marche aléatoire. Déterminer, si elle existe, sa répartition stable, c'est-à-dire la matrice ligne M dont la somme des coefficients est égale à 1 et telle que $M = MT$.

1) $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

2) $T = \begin{pmatrix} 0,25 & 0,75 \\ 1 & 0 \end{pmatrix}$

Puissance n-ième d'une matrice

Pour les exercices **8** à **10**, on donne la **formule du binôme de Newton** pour $n \in \mathbb{N}$ et deux matrices commutatives A et B : $(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^{n-k}B^k$.

7 Soit la matrice $A = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$.

1) Calculer A^2.

2) En déduire que, pour tout $n \in \mathbb{N}$, $A^{2n} = 5^n I$.

8 Soit $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

1) Écrire M sous la forme $I + J$ et expliciter la matrice J.

2) Calculer J^2 et J^3.

3) Calculer $(I+J)^n$. En déduire M^n pour tout $n \in \mathbb{N}$.

9 Soit $A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

1) a) Calculer $A - B$, puis B^3.

b) Démontrer que $A^n = \dfrac{n(n-1)}{2}B^2 + nB + I$.

c) En déduire A^n en fonction de n.

2) a) Vérifier que l'expression de A^n trouvée précédemment est encore vraie pour $n = -1$.

b) En déduire qu'elle est vraie pour $n \in \mathbb{Z}$.

10 Soit la matrice $A = \begin{pmatrix} 5 & -4 \\ 4 & -3 \end{pmatrix}$.

1) Trouver le réel λ et la matrice B telle que $A = I + \lambda B$.

2) Vérifier que $B^2 = 0$.

3) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = I + \lambda n B$.

11 ► MÉTHODE 1 p. 121

Soit $A = \begin{pmatrix} 4 & 3 \\ -2 & -1 \end{pmatrix}$ et $P = \begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix}$.

1) Démontrer que P est inversible et calculer P^{-1}.

2) a) Vérifier que $A = P \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} P^{-1}$.

b) En déduire une expression de A^n.

12 Soit $A = \begin{pmatrix} 5 & 3 \\ -6 & -4 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$.

1) Vérifier que P est inversible et calculer P^{-1}.

2) a) Déterminer la matrice D telle que $A = PDP^{-1}$.

b) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = PD^nP^{-1}$.

c) En déduire une expression de A^n.

13 Soit les matrices $A = \begin{pmatrix} 2 & 2 & -1 \\ -1 & -1 & 1 \\ -2 & -4 & 3 \end{pmatrix}$,

$P = \begin{pmatrix} 1 & -3 & -2 \\ -1 & 1 & 1 \\ -2 & -1 & 0 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 2 & -1 \\ -2 & -4 & 1 \\ 3 & 7 & -2 \end{pmatrix}$.

1) Avec la calculatrice, vérifier que Q est l'inverse de P.

2) Soit la matrice diagonale $D = \text{diag}(2, 1, 1)$.

a) Établir l'égalité $A = PDQ$.

b) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = PD^nQ$.

c) En déduire une expression de A^n.

14 Soit les matrices $A = \begin{pmatrix} -2 & -1 & -3 \\ -7 & 4 & -9 \\ 1 & 1 & 2 \end{pmatrix}$,

$P = \begin{pmatrix} 1 & -2 & -1 \\ -1 & -1 & 2 \\ -1 & 1 & 1 \end{pmatrix}$ et $Q = \begin{pmatrix} -3 & 1 & -5 \\ -1 & 0 & -1 \\ -2 & 1 & -3 \end{pmatrix}$.

1) Avec la calculatrice, vérifier que Q est l'inverse de P.

2) Démontrer qu'il existe $D = \text{diag}(a, b, c)$ avec a, b, c réels telle que $A = PDQ$.

3) a) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = PD^nQ$.

b) En déduire une expression de A^n.

15 Soit $A = \begin{pmatrix} -1 & -6 \\ 1 & 4 \end{pmatrix}$ et $P = \begin{pmatrix} 3 & 2 \\ -1 & -1 \end{pmatrix}$.

1) Démontrer que P est inversible et calculer P^{-1}.

2) Démontrer que :

a) il existe α et β réels tels que $A = P \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} P^{-1}$;

b) pour tout $n \in \mathbb{N}$, $A^n = P \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} P^{-1}$.

3) En déduire une expression de A^n.

16 $A = \begin{pmatrix} 16 & 4 & -4 \\ -18 & -4 & 5 \\ 30 & 8 & -7 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 0 & -1 \\ -2 & 1 & 1 \\ 2 & 1 & -2 \end{pmatrix}$.

1) Avec la calculatrice :

a) déterminer les matrices $B = AP$ et P^{-1} ;

b) déterminer la matrice $D = P^{-1}B$.

2) a) Exprimer A en fonction de D.

b) Exprimer A^2 et A^3 en fonction de P, D^2, D^3 et P^{-1}.

3) On admet que, pour tout entier naturel non nul n :

$$A^n = PD^nP^{-1} \text{ et } D^n = \text{diag}(0, 1, 4^n).$$

Déterminer les coefficients de A^n en fonction de n.

17 Soit la matrice $M = \begin{pmatrix} -4 & 6 \\ -3 & 5 \end{pmatrix}$.

1) Vérifier que $M^2 = M + 2I$.

2) Exprimer M^3 et M^4 sous la forme $\alpha M + \beta I$ où α et β sont des réels.

3) Soit les suites (u_n) et (v_n) définies par $u_0 = 0$ et $v_0 = 1$ et, pour tout entier naturel n :

$$\begin{cases} u_{n+1} = u_n + v_n \\ v_{n+1} = 2u_n \end{cases}.$$

Démontrer que : $M^n = u_nM + v_nI$.

4) Soit la suite (w_n) définie par $w_n = u_n - v_n$.

a) Montrer que (w_n) est géométrique de raison -1.

b) En déduire une expression de w_n en fonction de n.

5) Soit la suite (x_n) définie par $x_n = u_n + \dfrac{(-1)^n}{3}$.

On admet que (x_n) est géométrique de raison 2.

En déduire une expression de x_n en fonction de n.

6) Déduire de ce qui précède u_n et v_n en fonction de n.

7) En déduire alors M^n en fonction de n.

Suites de matrices

18 Soit la suite de matrices lignes (U_n) définie par $U_0 = \begin{pmatrix} -1 & 1 \end{pmatrix}$ et, pour tout $n \in \mathbb{N}$, $U_{n+1} = \dfrac{1}{10}U_n$.

1) Calculer U_1, U_2 et U_3.

2) Déterminer l'expression de U_n en fonction de n.

3) La suite (U_n) converge-t-elle ?

19 Soit la suite de matrices colonnes (V_n) de taille 2 telle que, pour tout $n \in \mathbb{N}$, $V_{n+1} = V_n + R$ avec :

$$V_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ et } R = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

1) Calculer V_1, V_2 et V_3.

2) Déterminer l'expression de V_n en fonction de n.

3) La suite (V_n) converge-t-elle ?

20 Soit les suites réelles (u_n) et (v_n) définies par $\begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\begin{cases} u_{n+1} = \dfrac{u_n + v_n}{2} \\ v_{n+1} = \dfrac{u_n + 2v_n}{3} \end{cases}$.

Soit la suite de matrices (X_n) définie par $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$.

Soit enfin la matrice A définie par $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$.

1) a) Démontrer que, pour tout $n \in \mathbb{N}$, $X_{n+1} = AX_n$.

b) Démontrer que, pour tout $n \in \mathbb{N}$, $X_n = A^n X_0$.

2) Soit $P = \begin{pmatrix} \frac{4}{5} & \frac{6}{5} \\ -\frac{6}{5} & \frac{6}{5} \end{pmatrix}$ et $P' = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix}$.

a) Montrer que P et P' sont inversibles.

b) Déterminer la matrice diagonale B telle que $P'BP = A$.

c) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = P'B^nP$.

3) a) Exprimer B^n en fonction de n.

b) Démontrer que, pour tout $n \in \mathbb{N}$:

$$X_n = \begin{pmatrix} \frac{3}{5} - \frac{3}{5}\left(\frac{1}{6}\right)^n \\ \frac{3}{5} + \frac{2}{5}\left(\frac{1}{6}\right)^n \end{pmatrix}$$

4) En déduire les limites des suites (u_n) et (v_n).

21 Soit les matrices $T = \begin{pmatrix} \frac{7}{10} & -\frac{3}{10} \\ \frac{1}{5} & \frac{1}{5} \end{pmatrix}$ et $P = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$.

1) a) Montrer que P est inversible et calculer P^{-1}.

b) Montrer qu'il existe une matrice diagonale D telle que $T = PDP^{-1}$.

c) Démontrer par récurrence que, pour tout $n \in \mathbb{N}$, $T^n = PD^nP^{-1}$.

d) En déduire une expression de T^n.

2) Soit les suites réelles (a_n) et (b_n) définies par a_0 et b_0 et l'égalité matricielle $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = T \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

a) Démontrer par récurrence que, pour tout $n \in \mathbb{N}$:

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = T^n \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$$

b) Déterminer une expression des termes généraux des suites (a_n) et (b_n).

c) En déduire la limite de ces deux suites.

22 **Suite de Fibonacci**

La suite de Fibonacci est définie par $u_0 = 0$, $u_1 = 1$, et, pour tout entier naturel n, $u_{n+2} = u_{n+1} + u_n$.

1) Soit les matrices $F_n = \begin{pmatrix} u_n & u_{n+1} \end{pmatrix}$ et $T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Montrer que $F_{n+1} = F_nT$, puis que $F_n = F_0T^n$.

2) Soit la matrice $P = \begin{pmatrix} \frac{\sqrt{5}-1}{2} & \frac{-\sqrt{5}-1}{2} \end{pmatrix}$.

a) Déterminer la matrice D telle que $T = PDP^{-1}$.

b) En déduire T^n en fonction de n.

3) a) Démontrer que, pour tout $n \in \mathbb{N}$, on a :

$$u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

b) Démontrer que $\lim\limits_{n \to +\infty} \dfrac{u_{n+1}}{u_n} = \varphi$ où φ est le nombre d'or égal à $\dfrac{1+\sqrt{5}}{2}$.

4) Soit l'algorithme incomplet suivant.

```
1.  a PREND_LA_VALEUR 0
2.  b, c, d PRENNENT_LA_VALEUR 1
3.  TANT_QUE (d>0.0001) FAIRE
4.      a PREND_LA_VALEUR b
5.      b PREND_LA_VALEUR c
6.      c PREND_LA_VALEUR ...
7.      d PREND_LA_VALEUR abs((c/b-b/a))
```

a) Compléter la ligne 6 afin que l'algorithme calcule les termes successifs de la suite de Fibonacci.

b) Expliquer comment s'arrête la boucle `TANT_QUE`.

c) Programmer l'algorithme et obtenir une valeur approchée du nombre d'or à 10^{-6} près.

23 ► MÉTHODE 2 p. 122

Soit (U_n) une suite de matrices colonnes telle que, pour tout entier naturel n, $U_{n+1} = AU_n + B$ avec :

$$U_0 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, A = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} \text{ et } B = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

1) Déterminer une matrice C telle que $C = AC + B$.

2) On pose $V_n = U_n - C$.

Montrer que pour tout entier naturel n, $V_{n+1} = AV_n$.

3) Exprimer V_n en fonction de V_0.

4) En déduire que $U_n = A^n(U_0 - C) + C$.

5) a) Démontrer que, pour tout entier naturel n :

$$A^n = \begin{pmatrix} 3^n & 2n \times 3^{n-1} \\ 0 & 3^n \end{pmatrix}.$$

b) En déduire une expression de U_n pour tout $n \in \mathbb{N}$.

24 Soit (U_n) une suite de matrices lignes telle que, pour tout entier naturel n, $U_{n+1} = U_n A + B$ avec :

$$U_0 = \begin{pmatrix} 2 & 1 \end{pmatrix},\ A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

1) Déterminer la matrice C telle que $C = CA + B$.

2) On pose $V_n = U_n - C$.
Montrer que pour tout entier naturel n, $V_{n+1} = V_n A$.

3) Exprimer V_n en fonction de V_0.

4) En déduire que $U_n = (U_0 - C)A^n + C$.

5) **a)** Calculer A^2, puis A^3. En déduire A^6.
En déduire A^n en fonction du reste de la division euclidienne de n par 6.

b) Déterminer la matrice U_{57}.

25 Soit les suites réelles (x_n) et (y_n) telles que :

$$\begin{cases} x_{n+1} = x_n + y_n + 1 \\ y_{n+1} = -2x_n + 4y_n + 3 \end{cases}.$$

1) Soit $B = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ et, pour tout $n \in \mathbb{N}$, $X_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.
Déterminer la matrice A telle que $X_{n+1} = AX_n + B$.

2) **a)** Montrer que $I - A$ est inversible.
Calculer $(I - A)^{-1}$.

b) Déterminer la matrice X telle que $X = AX + B$.

c) Étudier la convergence de (x_n) et (y_n).

3) Soit (V_n) la suite de matrices définie par $V_n = X_n - X$.
Montrer que, pour tout entier naturel n, $V_n = A^n V_0$.

4) **a)** Justifier que $P = \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}$ est inversible.

b) On note D la matrice définie par : $D = P^{-1}AP$.
Donner une expression de D^n.

c) En déduire une expression de A^n.

5) Pour $x_0 = 1$ et $y_0 = 2$, que peut-on dire de la convergence des suites (x_n) et (y_n) ?

Marches aléatoires entre états

26 Une ville est composée de deux quartiers A et B comptant respectivement 251 et 386 citadins.
Soit a_n et b_n les probabilités qu'un citadin provienne des quartiers A et B lors de la n-ième année d'étude.

Soit la matrice colonne U_n définie par : $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

Chaque année, des citadins déménagent :

- 5 % des citadins du quartier A vont au quartier B ;
- 12 % des citadins du quartier B vont au quartier A.

1) Quelle est, à 10^{-3} près, la probabilité qu'un citadin choisi au hasard dans la ville vienne du quartier A ?

2) **a)** Établir le graphe qui décrit les flux de populations entre ces deux quartiers.

b) Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

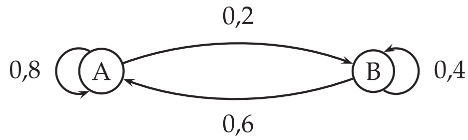
c) Déterminer la matrice T telle que $U_{n+1} = TU_n$.

3) Démontrer que, pour tout $n \in \mathbb{N}$, $U_n = T^n U_0$.

4) À l'aide de la calculatrice ou de l'ordinateur, calculer U_5, U_{10} et U_{20} (arrondir les coefficients à 10^{-5} près).

27 ▶ MÉTHODE 3 p. 125

Soit une marche aléatoire définie par le graphe :



On note $P_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ la répartition de probabilité à l'étape n de cette marche aléatoire.

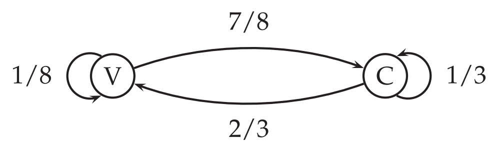
1) Déterminer la matrice de transition T telle que $P_{n+1} = TP_n$.

2) Démontrer que $a_{n+1} = 0,2a_n + 0,6$.

3) Démontrer que la suite (u_n) définie par la relation $u_n = a_n - 0,75$ est géométrique de raison 0,2.

4) En déduire que $\lim\limits_{n \to +\infty} M_n = \begin{pmatrix} 0,75 \\ 0,25 \end{pmatrix}$.
Que représente cette limite ?

28 Le graphe probabiliste suivant décrit la succession des voyelles (V) et des consonnes (C) dans le roman *Eugène Onéguine* de Pouchkine (voir **6** page 115) :



On note par une matrice ligne P_n la répartition de probabilité à la n-ième lettre du livre.

1) Déterminer la matrice de transition T telle que $P_{n+1} = P_n T$.

2) Déterminer un réel λ et une matrice Q tels que :

$$P_{n+1} = \lambda P_n + Q.$$

3) Démontrer par récurrence que, pour tout $n \in \mathbb{N}$:

$$P_n = \lambda^n \left(P_0 - \frac{24}{37}Q \right) + \frac{24}{37}Q.$$

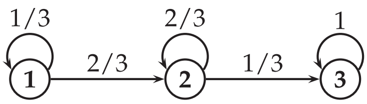
4) En déduire la répartition des consonnes et des voyelles dans le livre entier.

29 Jim était présent pour son premier jour de travail. Par la suite, s’il est là un jour, la probabilité qu’il soit là le lendemain est de 30 %. S’il s’absente un jour, la probabilité qu’il s’absente le lendemain est de 50 %.
Soit p_n et a_n les probabilités que Jim soit respectivement présent et absent le n-ième jour.
On pose $U_n = \begin{pmatrix} p_n \\ a_n \end{pmatrix}$ et $U_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

1) Exprimer p_{n+1} et a_{n+1} en fonction de p_n et a_n.
2) En déduire la matrice carrée A d’ordre 2 telle que $U_{n+1} = AU_n$.
3) Démontrer que $U_n = A^n U_0$.
4) Démontrer que :
$$A^n = \frac{1}{12}\begin{pmatrix} 5 & 5 \\ 7 & 7 \end{pmatrix} + \frac{1}{12}\left(\frac{-1}{5}\right)^n \begin{pmatrix} 7 & -5 \\ -7 & 5 \end{pmatrix}.$$
5) En déduire l’expression de U_n en fonction de n.
6) À long terme, quelle est la probabilité de voir Jim à son travail ?

30 Lors de l’Épiphanie, un boulanger insère dans chaque galette des Rois une fève naturelle : fève de cacao, de tonka ou de Gourgane. On suppose qu’il y a autant de chance d’avoir un type de fève ou un autre.

1) Déterminer la probabilité d’avoir deux types de fèves différents en achetant deux galettes.
2) Déterminer la probabilité d’avoir les trois types de fèves en achetant trois galettes.
3) On définit une marche aléatoire entre trois états qui correspondent au nombre de types de fèves obtenus par un client du boulanger. Le graphe pondéré ci-dessous indique les probabilités de passer d’un état à un autre après achat d’une galette.



a) Écrire la matrice M où m_{ij} égale la probabilité de passer de l’état i à j après achat d’une galette.
b) Justifier que le produit $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} M$ est égal à la matrice ligne d’éléments les probabilités d’être dans l’état 1, 2 et 3 après l’achat de deux galettes.
c) Calculer et interpréter le produit $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} M^2$.
d) Quel calcul matriciel donne la probabilité d’avoir les trois types de fèves en achetant cinq galettes ? Effectuer ce calcul à l’aide de la calculatrice.

31 On lance une pièce équilibrée jusqu’à faire deux « pile » consécutifs.

1) Traduire le processus par un graphe probabiliste.
2) Écrire la matrice de transition T associée.
3) Démontrer qu’en lançant quatre fois la pièce, la probabilité de succès est égale à 0,5.
4) Combien de fois doit-on lancer la pièce pour que cette probabilité soit égale à 0,9 ?
5) Déterminer la répartition stable de probabilité, c’est-à-dire la matrice ligne M telle que $M = MT$.
6) On admet que la suite des répartitions de probabilité converge vers M. Interpréter cette limite.

32 Dans une région impaludée, un individu est soit sain, immunisé (I) ou non immunisé (N), soit malade (M). D’un mois à l’autre, son état varie ainsi :

- I demeure avec une probabilité de 0,9 ou passe à N ;
- N demeure avec une probabilité de 0,6 ou passe à M ;
- M demeure avec une probabilité de 0,2 ou passe à N.

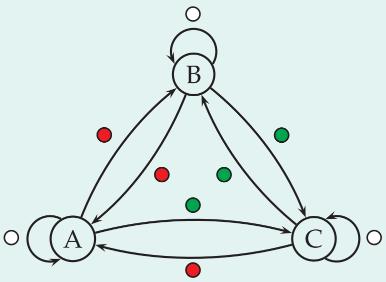
1) Réaliser un graphe de cette marche aléatoire.
2) Écrire la matrice de transition A.
3) On suppose qu’un individu sain est immunisé. En calculant A^2, déterminer la probabilité que :
   a) il soit encore immunisé au bout de deux mois ;
   b) il soit malade au bout de deux mois.
4) Selon l’état initial d’un individu, déterminer la probabilité qu’il soit malade au bout de :
   a) 5 mois b) 9 mois c) 1 an

33 On a analysé le cours du dollar : au lendemain d’un jour de hausse, la probabilité qu’il monte est 0,4 et qu’il ne varie pas 0,6 ; au lendemain d’un jour sans variation, la probabilité qu’il monte est 0,4 et qu’il baisse 0,3 ; au lendemain d’un jour de baisse, la probabilité qu’il ne varie pas est 0,4 et qu’il baisse est 0,6.

1) Traduire le processus par un graphe probabiliste.
2) Écrire la matrice de transition T associée.
3) Un jour donné, le dollar monte. Quelle est la probabilité qu’il ne varie pas sept jours après ?
4) Déterminer la répartition stable de probabilité, c’est-à-dire la matrice ligne M telle que $M = MT$.
5) On admet que la suite des répartitions de probabilité converge vers M. Interpréter cette limite.

34 D'après Bac (Métropole - 2015)

Sur les sommets d'un triangle ABC, un pion initialement en A suit une marche aléatoire. À chaque étape, on tire au hasard un jeton dans une boîte de 25 jetons (3 rouges, 4 verts et 18 blancs) puis on le remet.
Selon la couleur du jeton tiré et le sommet que le pion occupe, le graphe suivant indique où va le pion.



Exemple : si le pion est en A et qu'on tire un jeton rouge, le pion va en B.

Soit a_n, b_n et c_n les probabilités que le pion soit respectivement en A, B et C à l'étape n.
On considère les matrices :

$$X_n = \begin{pmatrix} a_n & b_n & c_n \end{pmatrix} \text{ et } T = \begin{pmatrix} 0,72 & 0,12 & 0,16 \\ 0,12 & 0,72 & 0,16 \\ 0,12 & 0,16 & 0,72 \end{pmatrix}$$

1) a) Donner X_0 et montrer que $X_{n+1} = X_n T$.

b) En déduire que $X_n = X_0 T^n$.

2) On admet que $T = PDP^{-1}$ avec :

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{5} & 0 \\ 0 & 0 & \frac{14}{25} \end{pmatrix} \text{ et } P^{-1} = \begin{pmatrix} \frac{3}{10} & \frac{37}{110} & \frac{4}{11} \\ \frac{1}{10} & -\frac{1}{10} & 0 \\ 0 & \frac{1}{11} & -\frac{1}{11} \end{pmatrix}$$

a) À l'aide de la calculatrice, montrer que la matrice P est à coefficients entiers.

b) Montrer que $T^n = PD^nP^{-1}$.

c) Écrire sans justification D^n.

On note $\alpha_n, \beta_n, \gamma_n$ les coefficients de la première ligne de la matrice T^n et on admet que :

$$\begin{cases} \alpha_n & = \dfrac{3}{10} + \dfrac{7}{10} \times 0,6^n \\ \beta_n & = \dfrac{37 - 77 \times 0,6^n + 40 \times 0,56^n}{110} \end{cases}.$$

3) a) Exprimer a_n et b_n, puis c_n en fonction de α_n et β_n.

b) Déterminer les limites des suites (a_n), (b_n) et (c_n).

c) Sur quel sommet a-t-on le plus de chance de trouver le pion après un grand nombre d'étapes ?

35 D'après Bac (Liban - 2015)

Un fumeur ayant décidé d'arrêter de fumer agit ainsi :

- s'il ne fume pas un jour donné, il ne fume pas le lendemain avec une probabilité de 0,9 ;
- s'il fume un jour donné, il fume le lendemain avec une probabilité de 0,6.

Soit p_n et q_n les probabilités qu'il ne fume pas (respectivement qu'il fume) n jours après sa décision d'arrêter de fumer. Le jour de cette décision, on suppose qu'il a fumé, c'est-à-dire que $p_0 = 0$ et $q_0 = 1$.

1) Calculer p_1 et q_1.

2) Dans un tableur, quelles formules peut-on écrire dans les cellules B3 et C3 de façon qu'en les recopiant vers le bas, on obtienne les termes successifs des suites (p_n) et (q_n) ?

	A	B	C
1	n	p_n	q_n
2	0	0	1
3	1		
4	2		

3) Soit les matrices $M = \begin{pmatrix} 0,9 & 0,4 \\ 0,1 & 0,6 \end{pmatrix}$, $X_n = \begin{pmatrix} p_n \\ q_n \end{pmatrix}$,

$A = \begin{pmatrix} 0,8 & 0,8 \\ 0,2 & 0,2 \end{pmatrix}$ et $B = \begin{pmatrix} 0,2 & -0,8 \\ -0,2 & 0,8 \end{pmatrix}$.

On admet que $X_{n+1} = MX_n$ et que $X_n = M^n X_0$.

a) Démontrer que $M = A + 0,5B$.

b) Vérifier que $A^2 = A$ et $AB = BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

On admet dans la suite que, pour tout entier naturel n non nul, $A^n = A$ et $B^n = B$.

c) Démontrer que $M^n = A + 0,5^n B$.

d) En déduire que $p_n = 0,8(1 - 0,5^n)$.

e) À long terme, peut-on affirmer avec certitude que le fumeur arrêtera de fumer ?

36 D'après Bac (Métropole - 2014)

Un pisciculteur élève des poissons dans deux bassins A et B. Tous les ans, à la même période :

- il vend tous les poissons du bassin B et y transfère tous les poissons du bassin A ;
- pour chaque poisson vendu, il achète deux petits poissons destinés au bassin A ;
- il achète et met 200 poissons dans le bassin A et 100 dans le bassin B.

Soit a_n et b_n les effectifs de poissons des bassins A et B au bout de n années, pour $n \geqslant 1$.
En début de première année, $a_0 = 200$ et $b_0 = 100$.
On note $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 200 \\ 100 \end{pmatrix}$ et $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

1) Justifier que $X_1 = \begin{pmatrix} 400 \\ 300 \end{pmatrix}$ puis calculer X_2.

2) a) Expliquer pourquoi $X_{n+1} = AX_n + B$.

b) Pour quels réels x et y a-t-on $\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} + B$?

c) Soit $Y_n = \begin{pmatrix} a_n + 400 \\ b_n + 300 \end{pmatrix}$. Prouver que $Y_{n+1} = AY_n$.

3) On pose $Z_n = Y_{2n}$.

a) Démontrer que $Z_{n+1} = A^2 Z_n$.

b) En déduire que $Z_{n+1} = 2Z_n$.

c) On admet que cela implique que $Y_{2n} = 2^n Y_0$.

En déduire que $Y_{2n+1} = 2^n Y_1$ puis prouver que :

$$a_{2n} = 600 \times 2^n - 400 \quad \text{et} \quad a_{2n+1} = 800 \times 2^n - 400.$$

4) Que fait l'algorithme ci-dessous ? Justifier.

```
Variables
a, p et n sont des entiers naturels
Traitement
Saisir p
Si p est pair
    n prend la valeur p/2
    a prend la valeur 600×2^n-400
Sinon
    n prend la valeur p-1/2
    a prend la valeur 800×2^n-400
Fin de Si
Afficher a
```

5) Le bassin A a une capacité de 10 000 poissons.

Écrire un algorithme qui affiche le nombre d'années pendant lesquelles le pisciculteur pourra exploiter le bassin A.

37 D'après Bac (Pondichéry - 2014)

Trois marques X, Y et Z se partagent le marché des petits pots pour bébé. On suppose qu'une famille consomme chaque mois une seule de ces marques et que :

- si le mois n elle est fidèle à la marque X, alors le mois suivant elle a 40 % de chance de changer pour Y et 10 % de chance de changer pour Z ;
- si le mois n elle est fidèle à la marque Y, alors le mois suivant elle a 50 % de chance de changer pour X et 20 % de chance de changer pour Z.
- si le mois n elle est fidèle à la marque Z, alors le mois suivant elle a 10 % de chance de changer pour X et 20 % de chance de changer pour Y.

Soit X_n (respectivement Y_n et Z_n) l'événement « la marque X (resp. Y et Z) est utilisée le mois n » et x_n sa probabilité (resp. y_n et z_n).

1) a) Exprimer x_{n+1} en fonction de x_n, y_n et z_n.

On admet que : $\begin{cases} y_{n+1} = 0,4x_n + 0,3y_n + 0,2z_n \\ z_{n+1} = 0,1x_n + 0,2y_n + 0,7z_n \end{cases}$.

b) Exprimer z_n en fonction de x_n et y_n, puis x_{n+1} et y_{n+1} en fonction de x_n et y_n.

2) Soit la matrice $U_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$. On admet que :

$$U_{n+1} = AU_n + B \text{ où } A = \begin{pmatrix} 0,4 & 0,4 \\ 0,2 & 0,1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0,1 \\ 0,2 \end{pmatrix}.$$

Au début de l'an 2016, on a $U_0 = \begin{pmatrix} 0,5 \\ 0,3 \end{pmatrix}$.

On fait alors tourner l'algorithme suivant :

```
Saisir un entier n
i prend la valeur 0
A prend la valeur (0,4 0,4 ; 0,2 0,1)
B prend la valeur (0,1 ; 0,2)
U prend la valeur (0,5 ; 0,3)
Tant que i < n
    U prend la valeur A×U+B
    i prend la valeur i+1
Fin de Tant que
Afficher U
```

a) Donner les résultats affichés par l'algorithme lorsque l'utilisateur saisit `n` $= 1$ puis `n` $= 3$.

b) Quelle est la probabilité qu'un client utilise la marque X au mois d'avril 2016 ?

Dans la suite de l'exercice, on cherche à déterminer une expression de U_n en fonction de n.

Soit les matrices I identité d'ordre 2 et $N = I - A$.

3) On désigne par C une matrice colonne à deux lignes.

a) Démontrer que $C = AC + B$ équivaut à $NC = B$.

b) On admet que N est inversible et qu'on a $N^{-1} = \begin{pmatrix} \frac{45}{23} & \frac{20}{23} \\ \frac{10}{23} & \frac{30}{23} \end{pmatrix}$. En déduire que $C = \begin{pmatrix} \frac{17}{46} \\ \frac{7}{23} \end{pmatrix}$.

4) On note V_n la matrice telle que $V_n = U_n - C$.

a) Montrer que $V_{n+1} = A \times V_n$.

b) On admet que $U_n = A^n \times (U_0 - C) + C$.

Quelles sont les probabilités qu'un client utilise les marques X, Y et Z au mois de mai 2016 ?

38 D'après Bac (Liban - 2013)

On considère la suite (u_n) définie par $u_0 = 3, u_1 = 8$ et, pour tout n supérieur ou égal à 0 :

$$u_{n+2} = 5u_{n+1} - 6u_n.$$

1) Calculer u_2 et u_3.

2) Pour tout entier naturel $n \geqslant 2$, on souhaite calculer u_n à l'aide de l'algorithme suivant :

```
1.  a, b et c réels
2.  i et n entiers supérieurs ou égaux à 2
3.  Traitement :
4.  a prend la valeur 3
5.  b prend la valeur 8
6.  Saisir n
7.  Pour i variant de 2 à n faire
8.      c prend la valeur a
9.      a prend la valeur b
10.     b prend la valeur ...
11. Fin Pour
12. Afficher b
```

a) Recopier et compléter l'algorithme.

b) Avec cet algorithme, on obtient pour $n \geqslant 7$ les termes suivants : 4 502, 13 378, 39 878, 119 122, 356 342, 1 066 978, 3 196 838, 9 582 322...
Quelle conjecture peut-on émettre concernant la monotonie de la suite (u_n) ?

3) Pour tout entier naturel n, soit $C_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$.

a) Déterminer la matrice carrée d'ordre 2 A telle que, pour tout $n \in \mathbb{N}$, $C_{n+1} = AC_n$.

b) Prouver que, pour tout $n \in \mathbb{N}$: $C_n = A^n C_0$.

4) Soit $P = \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ et $Q = \begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix}$.
Calculer QP.
On admet que $A = PDQ$. Démontrer par récurrence que, pour tout entier naturel non nul n, $A^n = PD^nQ$.

5) À l'aide des questions précédentes, on peut établir le résultat suivant, que l'on admet, pour tout entier naturel non nul n :

$$A^n = \begin{pmatrix} -2^{n+1} + 3^{n+1} & 3 \times 2^{n+1} - 2 \times 3^{n+1} \\ -2^n + 3^n & 3 \times 2^n - 2 \times 3^n \end{pmatrix}.$$

En déduire une expression de u_n en fonction de n.
La suite (u_n) a-t-elle une limite ?

39 D'après Bac (Pondichéry - 2013)

On étudie l'évolution dans le temps du nombre de jeunes et d'adultes dans une population d'animaux.
Pour tout $n \in \mathbb{N}$, on note j_n le nombre d'animaux jeunes après n années d'observation et a_n le nombre d'animaux adultes après n années d'observation.
En début d'étude, il y a 200 jeunes et 500 adultes. Ainsi $j_0 = 200$ et $a_0 = 500$.
On admet que, pour tout entier naturel n, on a :

$$\begin{cases} j_{n+1} = 0,125 j_n + 0,525 a_n \\ a_{n+1} = 0,625 j_n + 0,625 a_n \end{cases}$$

On introduit les matrices suivantes :

$$A = \begin{pmatrix} 0,125 & 0,625 \\ 0,525 & 0,625 \end{pmatrix} \text{ et } U_n = \begin{pmatrix} j_n & a_n \end{pmatrix}.$$

1) a) Montrer que pour tout $n \in \mathbb{N}$, $U_{n+1} = U_n \times A$.

b) Calculer le nombre d'animaux jeunes et d'animaux adultes après un an d'observation, puis après deux ans d'observation (résultats arrondis à l'unité près par défaut).

c) Pour tout entier naturel n non nul, exprimer U_n en fonction de A^n et de U_0.

2) On introduit les matrices suivantes :

$$Q = \begin{pmatrix} 5 & -5 \\ 7 & 3 \end{pmatrix} \text{ et } D = \begin{pmatrix} 1 & 0 \\ 0 & -0,25 \end{pmatrix}.$$

On admet que Q est inversible et que :

$$Q^{-1} = \begin{pmatrix} 0,06 & 0,1 \\ -0,14 & 0,1 \end{pmatrix}.$$

a) Montrer que $Q \times D \times Q^{-1} = A$.

b) Montrer par récurrence sur n que pour tout entier naturel n non nul : $A^n = Q \times D^n \times Q^{-1}$.

c) Pour tout entier naturel n non nul, déterminer D^n en fonction de n.

3) On admet que pour tout entier naturel n non nul,

$$A^n = \begin{pmatrix} 0,3 + 0,7(-0,25)^n & 0,5 - 0,5(-0,25)^n \\ 0,42 - 0,42(-0,25)^n & 0,7 + 0,3(-0,25)^n \end{pmatrix}$$

a) En déduire les expressions de j_n et a_n en fonction de n et déterminer les limites de ces deux suites.

b) Que peut-on en conclure pour la population d'animaux étudiée ?

40 **Avec les complexes**

Soit les matrices réelle $A = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$ et complexes

$P = \begin{pmatrix} 1 & 1 \\ 1+\mathrm{i} & 1-\mathrm{i} \end{pmatrix}$ et $Q = \begin{pmatrix} \frac{1}{2}+\frac{1}{2}\mathrm{i} & -\frac{1}{2}\mathrm{i} \\ \frac{1}{2}-\frac{1}{2}\mathrm{i} & \frac{1}{2}\mathrm{i} \end{pmatrix}$.

1) Montrer que P et Q sont inverses l'une de l'autre.

2) Montrer que $D = QAP$ est une matrice diagonale.

3) a) Démontrer que, pour tout $n \in \mathbb{N}$, $A^n = PD^nP^{-1}$.

b) Justifier que, pour tout entier n, $A^{n+4} = A^n$.

41 Pour faire des économies, Max veut privilégier le bus à la voiture lorsqu'il se rend au travail. La probabilité qu'il prenne le bus sachant qu'il l'a pris la veille est de 0,4. La probabilité qu'il prenne la voiture sachant qu'il l'a prise la veille est de 0,35.

On note b_n et v_n les probabilités que Max prenne respectivement le bus et la voiture le jour n.

On pose $P_n = \begin{pmatrix} b_n & v_n \end{pmatrix}$ et on fixe $P_0 = \begin{pmatrix} 1 & 0 \end{pmatrix}$.

Partie A

1) Représenter le graphe probabiliste du processus en numérotant les états 1 (bus) et 2 (voiture).

2) Donner la matrice de transition M.

3) Calculer P_1, P_2, P_3.

4) Quelle est la probabilité que Max prenne le bus le deuxième jour ? le troisième jour ?

Partie B

1) Soit $N = \begin{pmatrix} 0,52 & 0,48 \\ 0,52 & 0,48 \end{pmatrix}$ et $R = \begin{pmatrix} 0,48 & -0,48 \\ -0,52 & 0,52 \end{pmatrix}$.

Vérifier que $M = N - 0,25R$.

2) Calculer N^2 et N^3, puis R^2 et R^3.

En déduire N^n et R^n en fonction de n.

3) Calculer RN et NR.

4) Démontrer que, pour tout $n \in \mathbb{N}$:

$$M^n = N + (-0,25)^n R.$$

5) En déduire que :

$$M^n = \begin{pmatrix} 0,52 + 0,48(-0,25)^n & 0,48(1+(-0,25)^n) \\ 0,52(1+(-0,25)^n) & 0,48+0,52(-0,25)^n \end{pmatrix}.$$

Partie C

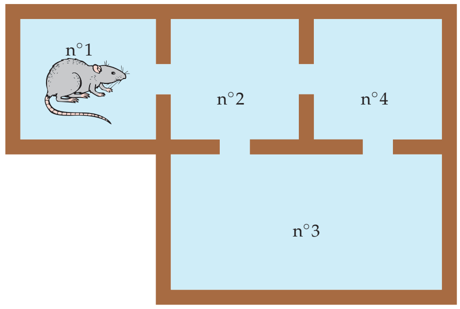
1) Exprimer P_n en fonction de n.

2) Vérifier que $b_n = 0,52 + (-0,25)^n \times 0,48$.

3) Déterminer la limite de b_n.

4) En fin de compte, l'objectif de Max sera-t-il atteint ?

42 On place un rat dans le sas n°1 d'une cage et on étudie ses déplacements selon différentes hypothèses.



Hypothèse 1 : Le rat change de sas avec une probabilité $\frac{1}{k}$ où k est le nombre de portes du sas quitté.

1) Établir le graphe probabiliste de la marche aléatoire.

2) Écrire la matrice de transition M.

3) On note X_n la variable aléatoire qui prend la valeur égale au numéro du sas où se trouve le rat après n changements.

Soit A_n la matrice ligne telle que $a_i = P(\{X_n = i\})$.

Vérifier que $A_{n+1} = A_n M$.

4) On s'intéresse à la position du rat après 6 changements de sas.

a) Dénombrer tous les chemins que le rat a pu suivre puis ceux qui l'ont ramené au sas n°1.

En déduire la probabilité que le rat retourne à la case départ.

b) Vérifier avec un calcul matriciel en déterminant la répartition de probabilité pour $n = 6$?

5) Vérifier que $A = \begin{pmatrix} \frac{1}{8} & \frac{3}{8} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$ est la répartition stable de probabilité.

On observe que le rat reste en moyenne plus longtemps dans le sas n°3 qui est deux fois plus grand. Ainsi, lorsque le rat y reste en moyenne deux fois plus longtemps qu'ailleurs, on assimile ce comportment à un « changement » dans le même sas.

Hypothèse 2 : Si le rat est dans le sas n° 3, il y reste, change pour le n° 2 ou le n° 4 avec la même probabilité ; sinon, on considère l'hypothèse 1.

1) Écrire la nouvelle matrice de transition M.

2) Déterminer la répartition de probabilité pour $n = 6$.

3) Déterminer la répartition stable de probabilité.

La comparer à celle de l'hypothèse 1.

43 Chaque consommateur d'une population étudiée utilise chaque mois une, et une seule, marque de dentrifice parmi Alenfresh, Blanchico et Carivor.

Pour un consommateur pris au hasard, on désigne par A_n (resp. B_n et C_n) l'événement : « Alenfresh (resp. Blanchico et Carivor) est utilisée au cours du n-ième mois » et par a_n (resp. b_n et c_n) sa probabilité.
Au cours du mois d'essai ($n = 0$), on a observé les valeurs initiales : $a_0 = 0,1$; $b_0 = 0,2$ et $c_0 = 0,7$.

Un sondage a déterminé le comportement suivant des consommateurs qu'on supposera ne pas changer.

- La probabilité qu'un client d'Alenfresh le mois n utilise Alenfresh (resp. Blanchico ou Carivor) le mois suivant est $0,4$ (resp. $0,3$ et $0,3$).
- La probabilité qu'un acheteur de Blanchico le mois n utilise Alenfresh (resp. Blanchico ou Carivor) le mois suivant est $0,3$ (resp. $0,4$ et $0,3$).
- La probabilité qu'un consommateur de Carivor le mois n utilise Alenfresh (resp. Blanchico ou Carivor) le mois suivant est $0,2$ (resp. $0,1$ et $0,7$).

Partie A

1) Modéliser la situation par un graphe (numéroter les sommets dans l'ordre alphabétique des marques).
2) Déterminer la matrice T de transition associée.
3) Soit L_n la matrice donnant la répartition au mois n. Que vaut L_0, L_1, L_2 ?
4) Comment semble évoluer la répartition pour de grandes valeurs de n ?

Partie B

1) Pour tout entier naturel n, exprimer a_{n+1}, b_{n+1} et c_{n+1} en fonction de a_n, b_n et c_n.
2) Soit $A = \begin{pmatrix} 0,2 & 0,1 \\ 0,2 & 0,3 \end{pmatrix}$, $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ et $B = \begin{pmatrix} 0,2 \\ 0,1 \end{pmatrix}$.
   Montrer que, pour tout $n \in \mathbb{N}$: $U_{n+1} = AU_n + B$.
3) On désigne par I la matrice identité de taille 2.
   a) Montrer que la matrice $I - A$ est inversible et déterminer son inverse.
   b) Déterminer la matrice C telle que $C = AC + B$.
4) Pour tout $n \in \mathbb{N}$, on pose $V_n = U_n - C$.
   Pour tout $n \in \mathbb{N}$, démontrer que : $V_n = A^n V_0$.
5) On note $P = \begin{pmatrix} 1/3 & -1/3 \\ 2/3 & 1/3 \end{pmatrix}$.
   a) Calculer $D = P^{-1}AP$, puis D^n.
   b) En déduire A^n en fonction de n.
   c) Que peut-on dire des coefficients de la matrice A^n lorsque n tend vers $+\infty$?
   d) Que conclure, à long terme, sur la position des trois marques de dentifrice sur le marché ?
   e) Est-ce cohérent avec les résultats de la partie **A** ?

44 Lors d'une épidémie de grippe A en France, les autorités sanitaires constatent qu'un individu est soit malade, soit immunisé car ayant déjà contracté un virus proche, soit ni malade ni immunisé.

De plus, d'une semaine à l'autre :

- une personne malade le reste avec une probabilité de 0,4 sinon elle guérit et est immunisée ;
- une personne immunisée a une probabilité de 0,1 de ne plus l'être sans pour autant tomber malade ;
- une personne ni malade ni immunisée tombe malade avec une probabilité de 0,3.

La première semaine du mois de septembre 2009, le centre de veille sanitaire estime que 1 % de la population est malade et 10 % de la population est immunisée.

1) Dresser un graphe modélisant la situation.
2) On note $X_n = \begin{pmatrix} m_n & i_n & r_n \end{pmatrix}$ la matrice donnant l'état du système n semaines après la première observation, où m_n, i_n, r_n représentent les proportions d'individus malades, immunisés ou ni l'un ni l'autre. Déterminer le vecteur ligne X_0 et la matrice de transition du système.
3) a) Faire un bilan sur la population les 6 premières semaines après la première observation.
   b) Déterminer, si elle existe, la répartition stable de probabilité.
   c) Que peut-on dire de la répartition de probabilité après un temps suffisamment long ?

45 **Approximation de $\sqrt{2}$**

Soit la fonction $f : x \mapsto \dfrac{x+2}{x+1}$ définie sur $\mathbb{R}_+$.
Soit trois suites (x_n), (y_n) et (z_n) définies par :

$$\begin{cases} x_{n+1} = x_n + 2y_n \\ y_{n+1} = x_n + y_n \end{cases} \text{ et } z_n = \frac{x_n}{y_n} \text{ avec } \begin{cases} x_0 = 1 \\ y_0 = 1 \end{cases}.$$

Partie A : Convergence d'une suite

1) Démontrer que $f(z_n) = z_{n+1}$.

2) Démontrer que :

$$\frac{z_{n+1}-\sqrt{2}}{z_{n+1}+\sqrt{2}} = \frac{\sqrt{2}-1}{\sqrt{2}+1} \cdot \frac{z_n-\sqrt{2}}{z_n+\sqrt{2}}.$$

3) Démontrer que :

$$\frac{z_n-\sqrt{2}}{z_n+\sqrt{2}} = \left(\frac{\sqrt{2}-1}{\sqrt{2}+1}\right)^{n+1}.$$

4) En déduire que $\lim\limits_{n\to+\infty} z_n = \sqrt{2}$.

Partie B : Algorithme de Théon de Smyrne

```
Variables
x, y sont des réels
i est un entier
Traitement
x prend la valeur 1
y prend la valeur 1
Pour i allant de 1 à 5
     x prend la valeur x+2y
     y prend la valeur x+y
     Afficher la valeur x/y
Fin Pour
```

1) a) Donner les valeurs affichées par l'algorithme.

b) Correspondent-elles aux termes de la suite (z_n) ?

c) Corriger l'algorithme pour qu'il en soit ainsi.

2) Modifier l'algorithme pour que s'affichent x et y tels que $\left|\texttt{x/y}-\sqrt{2}\right| < 10^{-7}$ ainsi que le rang du terme correspondant de la suite (z_n).
Donner x, y et le rang correspondant.

Partie C : Avec le calcul matriciel

Soit la matrice $A_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

1) Déterminer la matrice M telle que $A_{n+1} = MA_n$.

2) Sur Xcas, après avoir exécuté l'instruction `P,D:=jordan([[1,2],[1,1]])`, on obtient :

$$\left(\begin{bmatrix} \sqrt{2}, & -(\sqrt{2}) \\ 1, & 1 \end{bmatrix}, \begin{bmatrix} \sqrt{2}+1, & 0 \\ 0, & -(\sqrt{2})+1 \end{bmatrix}\right)$$

3) Vérifier que le couple (P, D) de matrices obtenu est tel que $PDP^{-1} = M$.

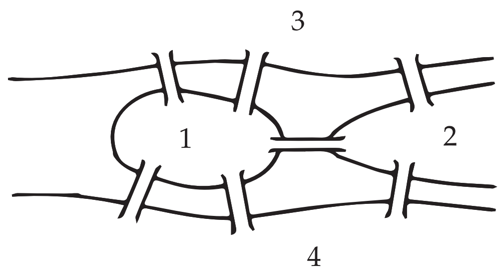
4) Que semble faire l'instruction `jordan` ?

5) Exprimer M^n en fonction de n sans logiciel de calcul formel.

6) En déduire une expression de z_n en fonction de n.

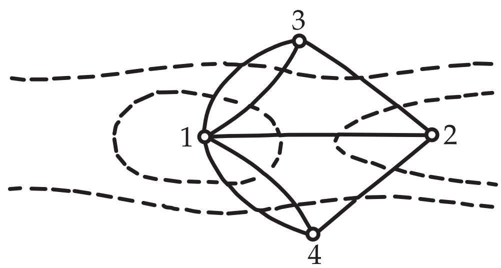
7) Vérifier avec un calcul matriciel le résultat obtenu à la question **2** de la partie **B** .

46 Balade à Königsberg INFO



Königsberg en 1736

Le problème des sept ponts de Königsberg est un problème mathématique que Leonhard Euler a résolu en 1736 et qui est connu pour être à l'origine de la théorie des graphes. On ne propose pas ici de résoudre ce problème mais de s'intéresser au graphe qui lui est associé.



Représentation graphique d'Euler

Partie A : Le promeneur

Un promeneur suit une marche aléatoire entre les quatre zones numérotées (1 et 2 correspondent aux deux îles sur la Pregolia, fleuve qui traverse la ville). On suppose qu'il change de zone toutes les 20 minutes, qu'il emprunte les ponts de façon équiprobable et qu'il est infatigable.

1) a) Faire le graphe probabiliste de la marche aléatoire.

b) Déterminer la matrice de transition associée.

c) Quelle est la probabilité que le promeneur soit sur une île deux heures après le début de sa marche ?

2) Un ami du promeneur, inquiet de n'avoir plus de ses nouvelles depuis très longtemps, souhaite le retrouver. Il veut donc chercher dans la zone où le promeneur a le plus de chance de se trouver.

a) Justifier que la marche aléatoire admet une répartition stable de probabilité.
Dépend-elle de la position initiale du promeneur ?

b) Un logiciel de calcul formel a donné deux matrices P et D telles que $T = PDP^{-1}$.

$$P = \begin{pmatrix} 0 & 1 & 1 & -2 \\ 0 & 1 & -3 & -2 \\ -1 & 1 & 1 & 3 \\ 1 & 1 & 1 & 3 \end{pmatrix} \text{ et } D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{1}{3} & 0 \\ 0 & 0 & 0 & -\frac{2}{3} \end{pmatrix}.$$

c) Déterminer P^{-1} avec une calculatrice.

d) Soit $P_n = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} M^n$.
Déterminer une expression de P_n en fonction de n.

e) En déduire la répartition stable de probabilité P de cette marche aléatoire.
Où l'ami du promeneur ira-t-il en priorité ?

PARTIE B : Le boîteux

Le promeneur s'est blessé à la cheville mais suit toujours inlassablement une marche aléatoire entre les quatre zones. Ainsi, toutes les vingt minutes :

- s'il est sur une île, 9 fois sur 10 il y reste, ou alors il change de zone en empruntant un pont au hasard ;
- s'il n'est pas sur une île, 3 fois sur 4 il reste où il est, ou alors il va sur une île en empruntant un pont au hasard.

1) Vérifier que la matrice de transition est :

$$D = \begin{pmatrix} 9/10 & 1/30 & 1/30 & 1/30 \\ 1/30 & 9/10 & 1/30 & 1/30 \\ 1/6 & 1/12 & 3/4 & 0 \\ 1/6 & 1/12 & 0 & 3/4 \end{pmatrix}.$$

2) Dans une session du logiciel Xcas :

a) Saisir les matrices T et $P = \begin{pmatrix} a & b & c & d \end{pmatrix}$.

b) Exécuter les deux instructions :

- `S:=P*T=P`
- `resoudre([a+b+c+d=1,S],P)`

Expliquer ce que chacune d'elles produit.

c) Au bout d'une très longue promenade, quelle est la probabilité de trouver le promeneur sur l'île 1 sachant qu'il est sur une île ?

47 De la couleur des gueules-de-loup

On s'intéresse dans cet exercice à l'évolution d'un caractère génétique, la couleur du muflier, plante herbacée appelée aussi gueule-de-loup ou gueule-de-lion. La couleur est déterminée par un gène biallélique (les deux allèles étant notées `A` et `a`).

Deux parents homozygotes (`AA` ou `aa`) ne peuvent avoir que des descendants homozygotes de même type alors que deux parents hétérozygotes (`Aa` ou `aA`) engendrent n'importe quel type de façon équiprobable.
Un muflier de génotype `AA` produit des fleurs rouges, `Aa` ou `aA` des fleurs mauves et `aa` des fleurs blanches.

PARTIE A : Effet de serre

1) Déterminer les probabilités d'obtenir des mufliers à fleurs rouges, blanches et mauves avec deux parents de génotype `AA`.

2) On décide de séparer chaque type de plantes (par exemple en utilisant trois serres différentes) pour déterminer leur évolution lorsque celles-ci ne sont fertilisées que par des plantes de génotype identique.
On note r_n, m_n et b_n les proportions des individus de chaque type, respectivement de génotype `AA`, `Aa` et `aa` à la n-ième génération, qui sont égales initialement.
Soit X_n la matrice ligne $\begin{pmatrix} r_n & m_n & b_n \end{pmatrix}$.

3) a) Déterminer la matrice carrée M telle que pour tout $n \in \mathbb{N}$, $X_{n+1} = AX_n$.

b) Exprimer X_n en fonction de X_0 et M.

4) Déterminer les proportions de mufliers de chaque couleur à la quatrième génération.

5) Soit $P = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -1 \\ -2 & 4 & 0 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0,5 \end{pmatrix}$.

a) Déterminer P^{-1} puis vérifier que $M = PDP^{-1}$.

b) Exprimer M^n en fonction de n.

c) En déduire X^n en fonction de n.

6) Déterminer la limite de X^n quand n tend vers ∞ ?
Peut-on en déduire que la séparation des cultures favorise la diversité biologique ?

Partie B : La nature reprend ses droits

On considère des mufliers de trois couleurs présents ensemble dans la nature. Les notations sont les mêmes que celles de la partie A .

1) Soit deux parents de types Aa et AA qui engendrent une fille. On écrit Aa $\times$ AA $= \{$AA, AA, Aa, Aa$\}$ pour dénombrer les types possibles chez la fille, sans distinguer de quel parent provient quel allèle.
   a) Écrire les ensembles Aa $\times$ Aa et Aa $\times$ aa.
   b) En déduire que le type Aa engendre des mufliers à fleurs rouges et blanches de façon équiprobable.
2) Montrer que la matrice de transition associée au processus d'évolution relatif à la couleur transmise est :
$$T = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 1/4 & 1/2 & 1/4 \\ 0 & 1/2 & 1/2 \end{pmatrix}.$$
3) Déterminer la répartition stable de probabilité du processus.
4) Pourquoi peut-on dire que la nature fait bien les choses ?

48 Aloha vs. Bigofone

Deux géants de la téléphonie mobile s'apprêtent à lancer simultanément chacun leur nouveau produit : Aloha et Bigofone. Pour mesurer l'efficacité de sa campagne publicitaire, le département responsable d'Aloha interroge chaque semaine un même échantillon de personnes sur le produit qu'ils ont l'intention d'acheter.

Pendant toute la campagne publicitaire, le comportement des personnes sondées est immuable : d'une semaine sur l'autre, 30 % des partisans d'Aloha et 20 % des partisans de Bigofone changent d'avis. Avant le lancement de cette campagne, Aloha n'avait la faveur que de 20 % des personnes interrogées.

Soit n un entier naturel. On note :

- a_n et b_n les probabilités qu'une personne sondée préfère respectivement Aloha et Bigofone la semaine n ;
- $P_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ la répartition de probabilité la semaine n.

1) Donner l'état initial P_0.
2) Représenter la situation par un graphe probabiliste de sommets A (Aloha) et B (Bigofone).
3) a) Écrire la matrice de transition M de ce graphe dans l'ordre alphabétique des sommets.
   b) Exprimer P_{n+1} en fonction de P_n et de M.
   c) Déterminer la répartition de probabilité P_3.
   En déduire qu'une personne interrogée préfère le téléphone Aloha la troisième semaine.
4) a) On cherche λ réel tel qu'il existe une matrice non nulle $V = \begin{pmatrix} x \\ y \end{pmatrix}$ vérifiant $MV = \lambda V$.
   Justifier que $M - \lambda I_2$ ne doit pas être inversible.
   b) En déduire les valeurs λ_1 et λ_2 possibles pour λ.
   c) Déterminer deux matrices colonnes V_1 et V_2 de taille 2 telles que :
   $$MV_1 = \lambda_1 V_1 \text{ et } MV_2 = \lambda_2 V_2.$$
   d) En déduire une matrice carrée P et une matrice diagonale D telle que $M = PDP^{-1}$.
5) a) Exprimer M^n en fonction de n.
   b) Déterminer la limite de la suite (M^n) quand n tend vers $+\infty$.
   c) Déterminer la matrice L, répartition limite de P_n lorsque n tend vers $+\infty$.
   Vérifier que $LM = L$.
   d) La campagne pour Aloha portera-t-elle ses fruits ?

49 Modèles matriciels de populations structurées

INFO

Partie A : Modèle de Leslie (1945)

Soit une population de souris femelles structurée en deux classes d'âge, les jeunes (âgées de moins d'un an) et les adultes (âgées entre un an et deux ans), telles que :

- chaque jeune donne naissance en moyenne à une femelle et chaque adulte à huit femelles ;
- la probabilité qu'un jeune devienne adulte est de 0,25 et un adulte ne survit jamais plus de deux ans.

On note j_t le nombre de jeunes, a_t le nombre d'adultes et n_t le nombre total de souris à l'instant t exprimé en années. Initialement, il y a 20 jeunes et aucun adulte.

1) Exprimer j_{t+1} et a_{t+1} en fonction de j_t et a_t.
2) On note V_t la matrice $\begin{pmatrix} j_t \\ a_t \end{pmatrix}$.
   a) Déterminer la matrice L telle que $V_{t+1} = LV_t$.
   La matrice L est appelée **matrice de Leslie**.
   b) Démontrer que, pour tout $t \in \mathbb{N}$, $V_{t+1} = L^t V_0$.

3) Soit la matrice $P = \begin{pmatrix} 8 & -4 \\ 1 & 1 \end{pmatrix}$.

a) Vérifier que $P^{-1}LP$ est une matrice diagonale D.

b) En déduire une expression de L^t en fonction de t.

c) Exprimer alors j_t, a_t et n_t en fonction de t.

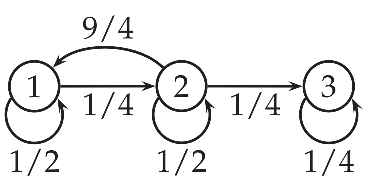
4) Déterminer les limites des quotients $\dfrac{j_t}{n_t}$, $\dfrac{a_t}{n_t}$ et $\dfrac{n_{t+1}}{n_t}$.

En donner une interprétation.

Partie B : Modèle de Lefkovitch (1965)

Le modèle de Lefkovitch divise la population en classes de stade et non plus d'âge comme celui de Leslie. La matrice associée, appelée **matrice de Lefkovitch**, intègre toujours les taux de fécondité et de survie mais aussi les probabilités qu'un individu change de stade.

Soit une population d'insectes structurée en trois classes de stade – larves, adultes reproductifs et adultes non reproductifs – qu'on numérote dans cet ordre et dont on note les effectifs après n semaines respectivement x_n, y_n et z_n. Son graphe de cycle de vie associé est :



1) Écrire la matrice de Lefkovitch L associée au graphe.

2) À l'aide du logiciel de calcul formel Xcas :

a) Créer la matrice L.

b) Exprimer sa puissance n-ième $M = L^n$ avec :

```
M:=matpow(L,n).
```

c) En déduire x_n, y_n et z_n en fonction de x_0, y_0 et z_0.

d) Montrer qu'au fil des semaines, la proportion de larves parmi tous les insectes tend vers $\dfrac{12}{17}$.

Partie C : Modèle d'Usher (1966)

En 1972, Usher modélise une population de rorquals bleus (une espèce de baleine) structurée en six classes d'âge d'amplitude égale à deux ans, plus une septième classe pour les individus de 12 ans ou plus.

On donne la **matrice d'Usher** associée à ce modèle :

$$U = \begin{pmatrix} 0 & 0 & 0,19 & 0,44 & 0,5 & 0,5 & 0,45 \\ 0,87 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0,87 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0,87 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0,87 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0,87 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0,87 & 0,8 \end{pmatrix}.$$

1) Faire le graphe de cycle de vie associé à cette matrice.

2) À partir de quel âge ces baleines peuvent mettre bas ?

3) On étudie l'évolution sur 50 ans d'une population constituée initialement de 10 baleineaux d'un an.

À l'aide du logiciel de calcul formel Xcas :

a) Créer la matrice U et la matrice colonne A des effectifs initiaux.

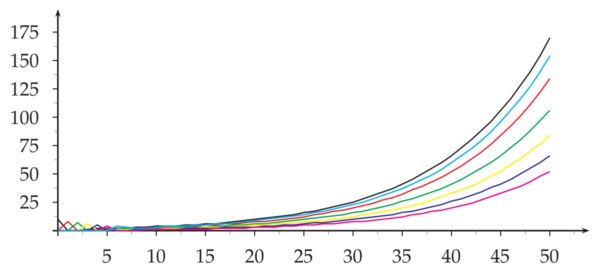
b) Déterminer ce que produit le programme suivant (touches Shift+Entrée pour aller à la ligne) :

```
M:=A;
for(n:=1;n<=50;n++){
M:=border(M,floor(U^n*A));}
```

c) Quelle est la répartition des baleines par classes après 50 ans ?

d) Interpréter le graphique donné par l'instruction :

```
seq(plotlist(row(M,n),color=n),n=0..6)
```



Je teste mes connaissances

À la fin de ce chapitre, je dois être capable de :

- Déterminer la puissance n-ième d'une matrice avec ou sans calculatrice ou logiciel de calcul formel, selon le cas
- Étudier une suite de matrices (U_n) définie par $U_{n+1} = AU_n$ ou par $U_{n+1} = AU_n + B$
- Définir une marche aléatoire par son graphe probabiliste et sa matrice de transition
- Étudier le comportement asymptotique d'une marche aléatoire entre états

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur **manuel.sesamath.net**

Pour chaque question, plusieurs réponses sont proposées. Déterminer celles qui sont correctes.

Soit $P = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, $A = \begin{pmatrix} 1 & -0,5 \\ 0,75 & -0,25 \end{pmatrix}$ et $D = P^{-1}AP$ trois matrices et n un entier naturel.

50 On a :

(a) $D = \begin{pmatrix} 0,5 & 0 \\ 0 & 0,25 \end{pmatrix}$ (b) $D = \begin{pmatrix} 0,25 & 0 \\ 0 & 0,5 \end{pmatrix}$ (c) $A^n = P^{-1}D^nP$ (d) $A^n = PD^nP^{-1}$

51 La matrice A^n est égale à :

(a) $\begin{pmatrix} -2\times 4^{-n} + 3\times 2^{-n} & -2\times 4^{-n} + 2^{-n+1} \\ -3\times 4^{-n} + 3\times 2^{-n} & -3\times 4^{-n} + 2^{-n+1} \end{pmatrix}$

(b) $\begin{pmatrix} -8^{-n} + 6^{-n} & -2^{-n+1} + 8^{-n} \\ -12^{-n} + 6^{-n} & -2^{-n+1} + 12^{-n} \end{pmatrix}$

(c) $\begin{pmatrix} -2\times 4^{-n} + 3\times 2^{-n} & -2^{-n+1} + 2\times 4^{-n} \\ -3\times 4^{-n} + 3\times 2^{-n} & -2^{-n+1} + 3\times 4^{-n} \end{pmatrix}$

(d) $\begin{pmatrix} \dfrac{3}{2^n} - \dfrac{2}{4^n} & \dfrac{2}{4^n} - \dfrac{4}{2^n} \\ \dfrac{3}{2^n} - \dfrac{3}{4^n} & \dfrac{3}{4^n} - \dfrac{4}{2^n} \end{pmatrix}$

52 Soit la matrice $B = P - 2AP$. Pour tout $n \neq 0$, la matrice B^n est égale à :

(a) $\begin{pmatrix} 0 & 1 \\ 0 & 1,5^n \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 1,5^n \\ 0 & 1,5^{n+1} \end{pmatrix}$ (c) $[(I-2A)P]^n$ (d) $[P(I-2D)]^n$

Soit $A = \begin{pmatrix} 1 & \dfrac{1}{3} \\ -1 & -\dfrac{1}{6} \end{pmatrix}$ et $B = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$. Pour n entier naturel, on donne $A^n = \begin{pmatrix} \dfrac{4}{2^n} - \dfrac{3}{3^n} & \dfrac{2}{2^n} - \dfrac{2}{3^n} \\ -\dfrac{6}{2^n} + \dfrac{6}{3^n} & -\dfrac{3}{2^n} + \dfrac{4}{3^n} \end{pmatrix}$.

53 Soit (U_n) la suite de matrices de terme général $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$ définie par $U_{n+1} = AU_n$ et $U_0 = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$.

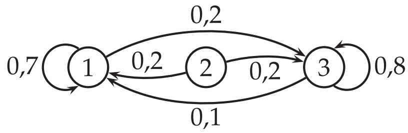
(a) $\lim\limits_{n\to+\infty} U_n = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (b) $U_n = \begin{pmatrix} \dfrac{6}{2^n} - \dfrac{5}{3^n} \\ \dfrac{10}{3^n} - \dfrac{9}{2^n} \end{pmatrix}$ (c) $U_n = \begin{pmatrix} \dfrac{1}{2^{n-1}} \\ -\dfrac{3}{2^n} \end{pmatrix}$ (d) $\lim\limits_{n\to+\infty} \dfrac{a_n}{b_n} = -\dfrac{2}{3}$

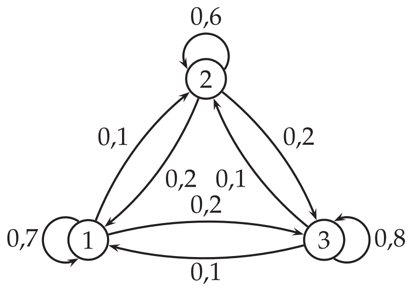
54 Soit (U_n) la suite de matrices définie par $U_{n+1} = AU_n + B$ et $U_0 = \begin{pmatrix} 5 \\ -8 \end{pmatrix}$. Alors U_n est égale à :

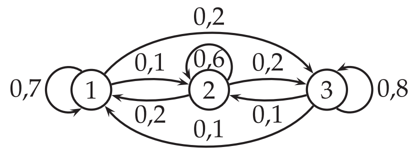
(a) $\begin{pmatrix} 4 + \dfrac{1}{2^{n-2}} + \dfrac{1}{3^n} \\ -6 - \dfrac{3}{2^{n-1}} - \dfrac{2}{3^n} \end{pmatrix}$ (b) $\begin{pmatrix} 4 + \dfrac{1}{3^n} \\ -6 - \dfrac{2}{3^n} \end{pmatrix}$ (c) $\begin{pmatrix} 2 + \dfrac{3}{2^{n-1}} - \dfrac{5}{3^n} \\ -3 - \dfrac{9}{2^n} + \dfrac{10}{3^n} \end{pmatrix}$ (d) $\begin{pmatrix} 2 + \dfrac{1}{3^n} \\ -3 - \dfrac{2}{3^n} \end{pmatrix}$

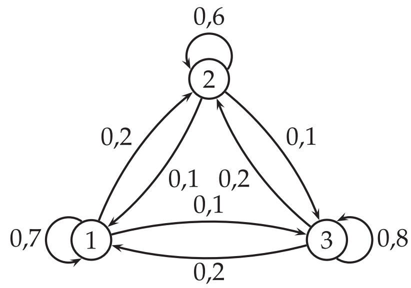
Le mental de l'équipe de football Saviola entraîne toujours le même processus qu'on assimile à une marche aléatoire entre trois états (1 : victoire, 2 : nul et 3 : défaite) : lorsqu'elle gagne un match, elle gagne le match suivant 7 fois sur 10 et le perd 1 fois sur 5 ; lorsqu'elle fait match nul, elle gagne le match suivant 1 fois sur 5 et le perd 1 fois sur 5 ; lorsqu'elle perd un match, elle gagne le match suivant 1 fois sur 10 et le perd 4 fois sur 5.

55 Son graphe probabiliste est :

(a) 

(b) 

(c) 

(d) 

56 Sa matrice de transition est :

(a) $\begin{pmatrix} 0,7 & 0 & 0,2 \\ 0,2 & 0 & 0,2 \\ 0,1 & 0 & 0,8 \end{pmatrix}$ (b) $\begin{pmatrix} 0,7 & 0,2 & 0,1 \\ 0,1 & 0,6 & 0,1 \\ 0,2 & 0,2 & 0,8 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 0,7 & 0,2 \\ 0,2 & 2 & 0,2 \\ 0,1 & 0,8 & 3 \end{pmatrix}$ (d) $\begin{pmatrix} 0,7 & 0,1 & 0,2 \\ 0,2 & 0,6 & 0,2 \\ 0,1 & 0,1 & 0,8 \end{pmatrix}$

57 Après quatre matchs, Saviola a plus de chance de perdre que de gagner le match suivant si :

(a) elle a gagné le premier match
(b) elle a fait match nul au premier match
(c) elle a perdu le premier match
(d) elle a fait n'importe quel résultat au premier match

58 On conjecture qu'il est probable qu'au bout d'un nombre de matchs suffisamment important, Saviola :

(a) perdra 1 fois sur 2 (b) gagnera 1 fois sur 2 (c) gagnera 3 fois sur 10 (d) ne gagnera plus

---

Soit une marche aléatoire, sa matrice de transition $T = \begin{pmatrix} 0,25 & 0,75 \\ 0,15 & 0,85 \end{pmatrix}$ et la suite (M_n) de répartitions de probabilité entre les deux états.

59 La répartition stable de cette marche aléatoire est la matrice M telle que $M = MT$. Alors :

(a) $M = \begin{pmatrix} 5/6 & 1/6 \end{pmatrix}$ (b) $M = \begin{pmatrix} 17/22 & 5/22 \end{pmatrix}$ (c) $M = \begin{pmatrix} 1/6 & 5/6 \end{pmatrix}$ (d) $M = \begin{pmatrix} 1/2 & 1/2 \end{pmatrix}$

60 Par la commande `matpow(T,n)` sur Xcas, on a obtenu $T^n = \frac{1}{6}\begin{pmatrix} \frac{5}{10^n}+1 & \frac{-5}{10^n}+5 \\ -\frac{1}{10^n}+1 & \frac{1}{10^n}+5 \end{pmatrix}$.

La suite de répartitions de probabilité de cette marche aléatoire :

(a) ne converge pas
(b) converge indépendamment de M_0
(c) converge vers une limite qui dépend de M_0
(d) converge vers $\begin{pmatrix} 5/6 & 1/6 \end{pmatrix}$

TP 1 Modèle proies/prédateurs de Lotka-Volterra

INFO

Soit deux suites (u_n) et (v_n) modélisant, en fonction du nombre d'années n, l'évolution des effectifs de deux populations, constituées respectivement de lièvres des neiges et de lynx.
Des statistiques ont montré que :

- lorsqu'il n'y a pas prédation, le nombre de proies u_n augmente à taux constant a et le nombre de prédateurs v_n diminue à taux constant c ;
- lorsqu'il y a prédation, le taux d'évolution des proies est diminué en proportion de v_n (coefficient de proportionnalité b) et le taux d'évolution des prédateurs est augmenté en proportion de u_n (coefficient de proportionnalité d).

Ainsi, on obtient le système $\begin{cases} \dfrac{u_{n+1}-u_n}{u_n} = a - bv_n \\ \dfrac{v_{n+1}-v_n}{v_n} = -c + du_n \end{cases}$.

A Étude de l'évolution du système à l'aide d'un tableur

1) Exprimer u_{n+1} et v_{n+1} en fonction de u_n et v_n.

2) Soit fixés les taux $a = 50$ ‰, $b = 1$ ‰, $c = 30$ ‰ et $d = 0,2$ ‰.

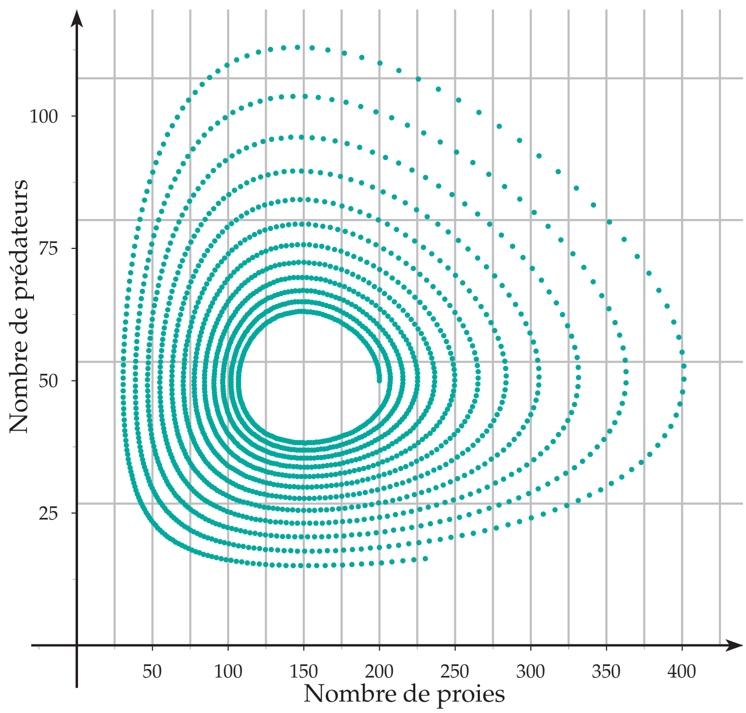
a) Dans un tableur, simuler l'évolution des deux populations pendant 2 000 ans sachant qu'initialement il y a 200 proies et 50 prédateurs.

b) Représenter sur un même graphique l'évolution des effectifs des deux espèces en fonction du nombre d'années.

c) Décrire et interpréter l'évolution des deux populations.

d) Représenter dans un nouveau graphique le nuage des points de coordonnées $(u_n\ ;\ v_n)$.

3) Faire varier les populations initiales. Ont-elles de l'influence sur leur évolution ?



B Équilibre des populations

1) Montrer qu'il existe un couple de suites constantes non nulles solution du système proies/prédateurs.
2) Dans le tableur, changer les populations initiales pour vérifier que ces suites sont constantes.
3) Que représente ce couple solution pour le graphique spiralé obtenu précédemment ?

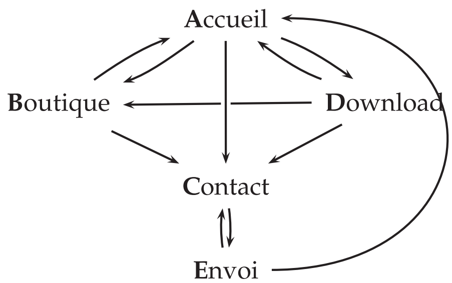
C Linéarisation autour du point d'équilibre

On pose $U_n = u_n - \frac{c}{d}$, $V_n = v_n - \frac{a}{b}$ et $X_n = \begin{pmatrix} U_n \\ V_n \end{pmatrix}$.

1) Écrire le système que vérifient U_n et V_n avec les paramètres fixés au **2** de la partie **A**.
2) a) Montrer qu'en ordre de grandeur, le produit $U_n V_n$ est négligeable par rapport à U_n et V_n.
b) En déduire une simplification du système.
c) Écrire ce système simplifié sous la forme matricielle $X_{n+1} = MX_n$ en explicitant M.
d) En déduire comment calculer les effectifs des populations de proies et de prédateurs au bout d'un nombre d'années donné.

TP 2 Pertinence d'une page web

Le site web d'un groupe de musique a cinq pages liées comme l'indique le graphe ci-contre. Le concepteur du site exige que les moteurs de recherche renvoient en premier lieu la page **A**. Il étudie alors la **pertinence** des pages selon quatre comptages.



A Premiers comptages

- **Comptage naïf** : la pertinence d'une page égale le nombre de liens qui renvoient vers elle.
- **Comptage pondéré** : on suppose qu'un surfeur suit une marche aléatoire sur le graphe.
  S'il est sur une page **P**, alors il se rend ensuite sur une page liée avec une probabilité égale à $\frac{1}{m}$ où m est le nombre de liens issus de la page **P**. La pertinence d'une page est alors la somme des probabilités affectées aux liens pointant vers cette page.

1) Calculer la pertinence des pages selon le comptage.
2) Montrer qu'aucun des deux comptages ne satisfait le concepteur du site.

B Comptage amélioré

Avec les comptages naïf et pondéré, on se rend compte qu'on peut augmenter artificiellement la pertinence d'une page en créant des liens superflus.
Pour éviter ce problème, on établit un nouveau comptage : le **comptage récursif**.

Le surfeur suit toujours une marche aléatoire sur le graphe et on cherche à établir la loi de probabilité de la position du surfeur sur le graphe après un temps infini.

Soit $U_n = \begin{pmatrix} a_n & b_n & c_n & d_n & e_n \end{pmatrix}$ la matrice des probabilités que le surfeur soit sur la page **A**, **B**, **C**, **D** et **E** après le parcours de n pages. La matrice initiale U_0 est nulle hormis un coefficient égal à 1 correspondant à la page par laquelle le surfeur entre sur le site.

a_n est la probabilité qu'après le parcours de n pages, le surfeur soit sur la page **A** qui donne accès aux pages **B**, **C** et **D**, donc, à la page suivante, a_n contribue équitablement pour $\frac{1}{3}a_n$ aux probabilités b_{n+1}, c_{n+1} et d_{n+1}. À l'inverse, les pages **B**, **C** et **E** renvoient à la page **A**, et ces pages émettent respectivement 2, 3 et 2 liens. Par conséquent, $a_{n+1} = \frac{1}{2}b_n + \frac{1}{3}c_n + \frac{1}{2}e_n$.

1) De manière analogue, donner les formules pour b_{n+1}, c_{n+1}, d_{n+1} et e_{n+1}.
2) Écrire la matrice carrée M telle que $U_{n+1} = U_n \times M$.
3) En déduire l'expression de U_n en fonction de n.
4) Avec un logiciel de calcul formel, déterminer la limite de la suite (M^n) des puissances de M. En déduire la limite de la suite (U_n).
5) Le concepteur du site est-il satisfait ?

C Comptage récursif avec échappement

La méthode de calcul de la pertinence d'une page web développée par un moteur de recherche tient compte qu'un surfeur puisse atteindre directement une page (par saisie de son adresse ou par marque-page) en intégrant un **coefficient d'échappement**.
Le coefficient d'échappement est une probabilité (que nous fixons à $0,15$) répartie équitablement entre toutes les pages du graphe tandis que son complément $(1 - 0,85)$ est appliqué à la marche aléatoire.
Avec les notations précédentes, on a donc :

$$U_{n+1} = \frac{0,15}{5}J + 0,85U_nM = U_n\left(0,3K + 0,85M\right)$$

où J est la matrice ligne de taille 5 et K est la matrice carrée d'ordre 5 remplies de 1.

1) Expliquer la formule :

$$U_{n+1} = \frac{0,15}{5}J + 0,85U_nM.$$

2) Justifier que :

$$U_{n+1} = U_n\left(0,3K + 0,85M\right).$$

3) Calculer la matrice $N = 0,3J + 0,85M$.
4) Avec un logiciel de calcul formel, déterminer la limite de la suite (N^n) à 10^{-4} près. En déduire la limite de la suite (U_n).
5) Le concepteur du site est-il enfin satisfait ?

D Une modification du graphe

1) Quel lien pourrait-on supprimer dans le graphe pour mieux contenter le concepteur du site ?
2) Étudier la pertinence des pages de ce nouveau graphe selon les trois autres comptages et la satisfaction du concepteur.

TP 3 Triangles rectangles pseudo-isocèles

Un **triangle rectangle pseudo-isocèle** (TRPI) est un triangle rectangle dont les longueurs de côtés sont des entiers a, $a+1$ et c, où c est la longueur de l'hypoténuse.

Le caractère pseudo-isocèle est d'autant plus marqué que a est grand. Par exemple, le triplet $(4\,059\ ;\ 4\,060\ ;\ 5\,741)$, forcément pythagoricien, définit un TRPI. Le théorème de Pythagore caractérise les TRPI par les couples $(a\ ;\ c)$ d'entiers vérifiant l'équation diophantienne :

$$a^2+(a+1)^2=c^2 \quad (*).$$

A Recherche exhaustive de TRPI

Une première approche consiste à faire varier a et à tester si $a^2+(a+1)^2$ est un carré parfait. Si c'est le cas, alors le triplet $(a\ ;\ a+1\ ;\ c)$ définit bien un TRPI.

1) Exprimer c en fonction de a.

2) Soit $n \in \mathbb{N}$. Comment tester si $\sqrt{n}$ est un entier ?

3) Compléter l'algorithme suivant et le programmer pour obtenir les solutions.

```
a, c sont des nombres
Pour a allant de 1 à 1000
    c prend la valeur ...
    Si ... alors
        Afficher a,a+1,c
    Fin Si
Fin Pour
```

B Obtenir des TRPI à l'aide des suites

Soit (a_n) et (c_n) les suites croissantes telles que $(a_n\ ;\ c_n)$ est solution de l'équation $(*)$.

Le couple $(0\ ;\ 1)$ étant solution, on considère les termes initiaux $a_0=0$ et $c_0=1$.

1) a) Montrer que, pour $n \in \{1,2,3\}$, il existe deux réels α et β tels que :

$$c_{n+1}+\alpha c_n+\beta c_{n-1}=0.$$

b) Soit la suite (v_n) définie par $v_0=1$, $v_1=5$ et, pour $n \geqslant 1$, $v_{n+1}-6v_n+v_{n-1}=0$.
Démontrer que, pour $n \geqslant 1$:

$$v_n=\frac{2+\sqrt{2}}{4}\left(3+2\sqrt{2}\right)^n+\frac{2-\sqrt{2}}{4}\left(3-2\sqrt{2}\right)^n.$$

2) a) Vérifier que, pour $n \in \{1,2,3\}$:

$$a_{n+1}-6a_n+a_{n-1}=2.$$

b) Soit la suite (u_n) définie par $u_0=0$, $u_1=5$ et, pour $n \geqslant 1$, $u_{n+1}-6u_n+u_{n-1}=2$.
Démontrer que, pour $n \geqslant 1$:

$$u_n=\frac{1+\sqrt{2}}{4}\left(3+2\sqrt{2}\right)^n+\frac{1-\sqrt{2}}{4}\left(3-2\sqrt{2}\right)^n-\frac{1}{2}.$$

3) Montrer que, pour tout $n \geqslant 1$, u_n et v_n sont les longueurs du petit côté et de l'hypoténuse d'un TRPI.

C Obtenir des TRPI à l'aide du calcul matriciel

1) a) Montrer que les suites (u_n) et (v_n) vérifient le système :

$$\begin{cases} u_{n+1} = 3u_n + 2v_n + 1 \\ v_{n+1} = 4u_n + 3v_n + 2 \end{cases}.$$

b) Écrire ce système sous la forme matricielle $X_{n+1} = AX_n + B$ avec $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$.

2) a) Montrer que $A - I$ est inversible et calculer son inverse.

b) Pour $n \in \mathbb{N}$, on pose $S_n = 1 + A + A^2 + \ldots + A^{n-1}$.
Calculer $(A - I)S_n$. En déduire S_n en fonction de $(A - I)$, I et A^n.

c) Exprimer X_n en fonction de A^n, S_n, B et X_0.

3) Montrer qu'on peut écrire $A = P \begin{pmatrix} 3+2\sqrt{2} & 0 \\ 0 & 3-2\sqrt{2} \end{pmatrix} P^{-1}$ avec $P = \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}$.
En déduire A^n. Calculer alors X_n en fonction de n.

4) Utiliser un logiciel de calcul formel pour obtenir d'autres TRPI.

Récréation, énigmes

La **fougère de Barnsley** est une fractale inventée par le mathématicien britannique Michael Barnsley qui ressemble à la Doradille noire, une fougère de la famille des *Aspleniaceae*. C'est un exemple simple d'objet autosimilaire, c'est-à-dire qui conserve sa forme, quelle que soit l'échelle à laquelle on l'observe. Les travaux de Barnsley ont été une source d'inspiration pour les artistes désireux de modéliser la nature.

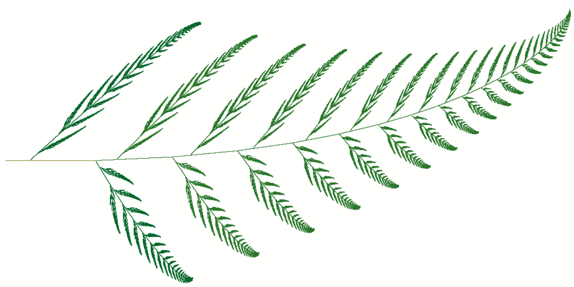
On construit une suite de points de coordonnées $(x_n; y_n)$, initialement $(x_0; y_0) = (0; 0)$, en itérant des transformations affines w caractérisées par une formule du même type (voir ci-dessous) selon une répartition de probabilité. La première construit la tige, la troisième et la quatrième construisent les folioles des deux plus grandes feuilles, respectivement celle de gauche et celle de droite, et la quatrième construit les folioles des autres feuilles. Dans son livre *Fractals Everywhere*, Barnsley fournit les coefficients des matrices et les probabilités p ci-dessous. En jouant sur ces coefficients, on peut imiter d'autres fougères.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix} + \underbrace{\begin{pmatrix} e \\ f \end{pmatrix}}_{B}$$

w	a	b	c	d	e	f	p
1	0	0	0	0,16	0	0	0,01
2	0,85	0,04	$-0,04$	0,85	0	1,60	0,85
3	0,20	$-0,26$	0,23	0,22	0	1,60	0,07
4	$-0,15$	0,28	0,26	0,24	0	0,44	0,07

1) Pour chaque transformation w :
- écrire les matrices A et B ;
- exprimer x_{n+1} et y_{n+1} en fonction de x_n et y_n.

2) Écrire un algorithme permettant de produire le dessin de la fougère et le programmer dans AlgoBox en utilisant un repère sachant que, pour tout $n \in \mathbb{N}$:
$-2,1820 < x_n < 2,6558$ et $0 \leqslant y_n < 9,9983$.



Fiche 1 Utiliser un tableur

Les fonctions suivantes s'appliquent dans les tableurs de type Excel ou Open Office.

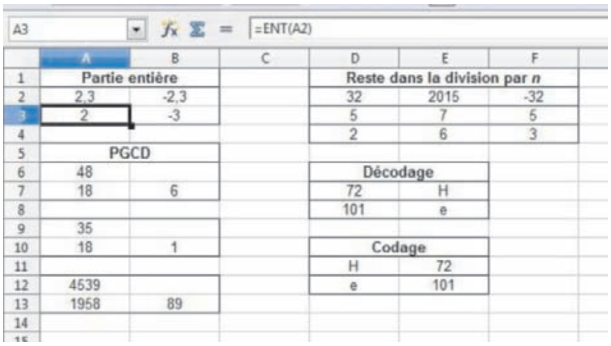
A Fonctions arithmétiques

ENT(n)	Renvoie la partie entière du nombre n
MOD(n ; d)	Renvoie le reste de la division euclidienne de n par d
PGCD(a ; b)	Renvoie le PGCD de a et de b
CAR(n)	Renvoie le caractère spécifié par le code ASCII du numéro n
CODE(Texte)	Renvoie le numéro de code ASCII du premier caractère du texte saisi

Exemples :

On a saisi la formule `=PGCD(A6;A7)` dans la cellule B7 qui renvoie 6.

On a saisi la formule `=CAR(72)` dans la cellule E7 qui renvoie la lettre H.



A3 =ENT(A2)

	A	B	C	D	E	F
1	Partie entière			Reste dans la division par *n*		
2	2,3	-2,3		32	2015	-32
3	2	-3		5	7	5
4				2	6	3
5	PGCD					
6	48			Décodage		
7	18	6		72	H	
8				101	e	
9	35					
10	18	1		Codage		
11				H	72	
12	4539			e	101	
13	1958	89				
14						

B Matrices

Lorsqu'on travaille avec des matrices dans une feuille de calcul, on valide en tapant : Ctrl + Maj + Entrée.

Création d'une matrice

Pour créer la matrice $A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \\ 6 & 7 \end{pmatrix}$, on rentre chaque coefficient de A dans une cellule en respectant la taille de la matrice (ici de A2 à B4 par exemple).

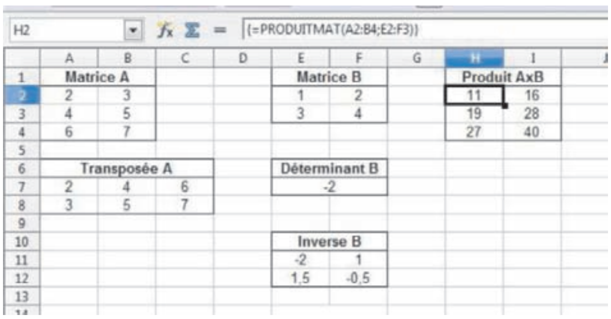
Opérations sur les matrices

TRANSPOSE(A2:B4)	Renvoie la transposée de la matrice A
PRODUITMAT(A2:B4;E2:F3)	Renvoie le produit de la matrice A avec la matrice B
DETERMAT(E2:F3)	Renvoie le déterminant de la matrice carrée B
INVERSEMAT(E2:F3)	Renvoie la matrice inverse de la matrice carrée B

Exemples :

Pour calculer A×B, on sélectionne la plage de cellules où apparaîtra la matrice du résultat, par exemple les cellules de H2 à I4, puis en rentre la formule `=PRODUITMAT(A2:B4;E2:F3)` et l'on valide par Ctrl+Maj+Entrée.

Pour calculer B^{-1}, on sélectionne la plage de cellules où apparaîtra la matrice du résultat, puis on rentre la formule `=INVERSEMAT(E2:F3)`.



H2 {=PRODUITMAT(A2:B4;E2:F3)}

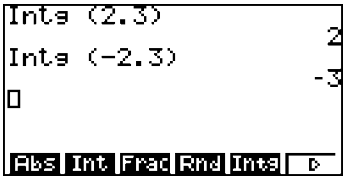
	A	B	C	D	E	F	G	H	I
1	Matrice A				Matrice B			Produit AxB	
2	2	3			1	2		11	16
3	4	5			3	4		19	28
4	6	7						27	40
5									
6	Transposée A				Déterminant B				
7	2	4	6		-2				
8	3	5	7						
9									
10					Inverse B				
11					-2	1			
12					1,5	-0,5			
13									

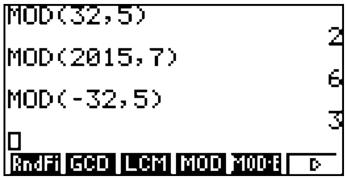
Fiche 2 Utiliser une calculatrice Casio

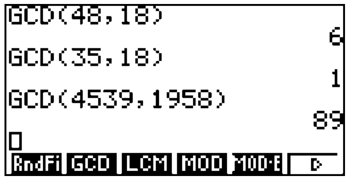
A Utiliser les fonctions arithmétiques

Pour accéder aux fonctions arithmétiques suivantes, depuis le menu RUN-MAT, taper OPTN, sélectionner le sous-menu F6 F4 (NUM) puis sélectionner :

- F5 (Intg) pour obtenir la partie entière d'un nombre ;
- F6 F2 (GCD) pour obtenir le PGCD de deux nombres ;
- F6 F4 (MOD) pour obtenir le reste de la division de a par n.







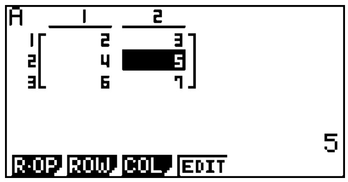
B Travailler avec les matrices

Créer une matrice

Depuis le menu RUN-MAT, sélectionner F3 (MAT) puis sélectionner l'une des matrices (A à Z).

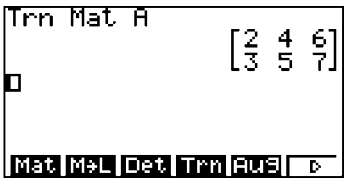
Rentrer les dimensions, puis saisir les coefficients.

Pour travailler avec la matrice A, taper SHIFT 2 (Mat) ALPHA X,θ,T (A).



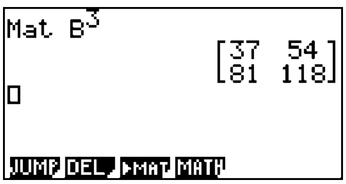
Calculer la transposée ou le déterminant d'une matrice

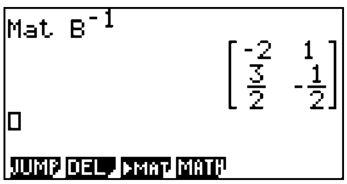
Taper OPTN, sélectionner le sous-menu F2 (MAT), puis F4 (Trn) pour la transposée, ou F3 (Det) pour le déterminant.

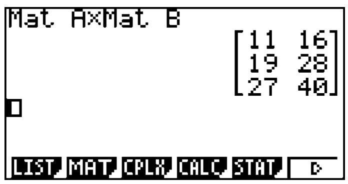


Déterminer la puissance n-ième d'une matrice, son inverse ou calculer le produit de deux matrices

Utiliser les touches ∧ pour calculer la puissance, x-1 pour obtenir l'inverse ou × pour la multiplication.





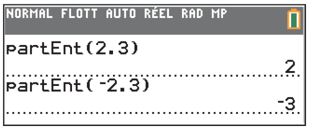


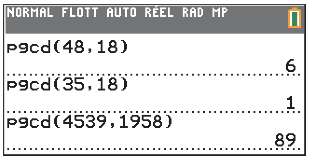
Fiche 3 Utiliser une calculatrice TI

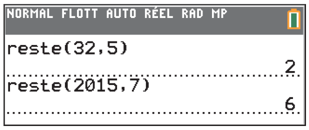
A Utiliser les fonctions arithmétiques

Pour accéder aux fonctions arithmétiques suivantes, taper MATH, sélectionner le sous-menu "Nbre" puis sélectionner :

- 5 (partEnt) pour obtenir la fonction entière d'un nombre ;
- 9 (PGCD) pour calculer le PGCD ;
- 0 (reste) pour obtenir le reste de la division de a par n.





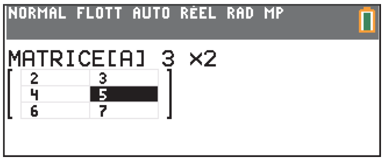


B Travailler avec les matrices

Créer une matrice

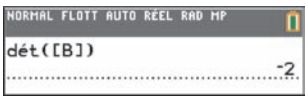
Sélectionner dans le menu MATRICE, le sous-menu EDIT puis le nom de la matrice, par exemple 1 (1:[A]).

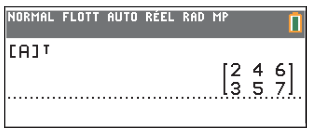
Rentrer les dimensions, puis rentrer les coefficients ligne par ligne.



Calculer la transposée ou le déterminant d'une matrice

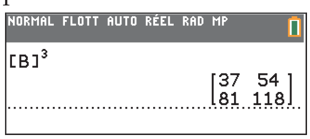
Dans le menu MATRICE puis MATH, sélectionner la commande 1 (1:det() pour calculer le déterminant ou 2 (2:^{T}) pour obtenir la transposée.

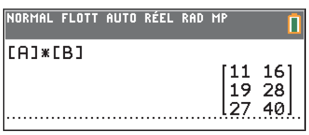


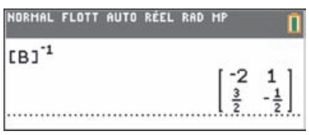


Déterminer la puissance *n*-ième d'une matrice, son inverse ou calculer le produit de deux matrices

Utiliser les touches ∧ pour calculer la puissance, x-1 pour obtenir l'inverse ou × pour la multiplication.







Fiche 4 Utiliser un logiciel de calcul formel

A Liste des commandes utiles en arithmétique

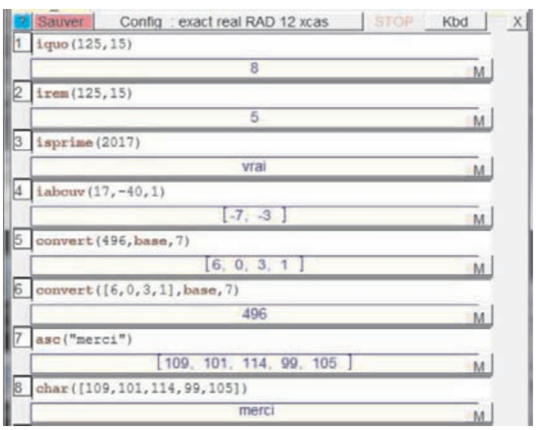
iquo(a,b), irem(a,b)	Renvoie le quotient, le reste de la division euclidienne de a par b
isprime(p)	Indique si un nombre est premier (vrai) ou non (faux)
gcd(a,b), lcm(a,b	Renvoie le PGCD, le PPCM de deux entiers
iabcuv(a,b,c)	Renvoie u et v tels que $au + bv = c$
powmod(a,n,m)	Renvoie a^n (mod m)
L :=convert(a,base,b)	Renvoie la liste des chiffres de a en base b
a :=convert(L,base,b)	Effectue la conversion inverse
asc("chaine")	Renvoie la liste des codes ASCII d'une chaîne
char(L)	Renvoie la chaîne de caractères à partir d'une liste

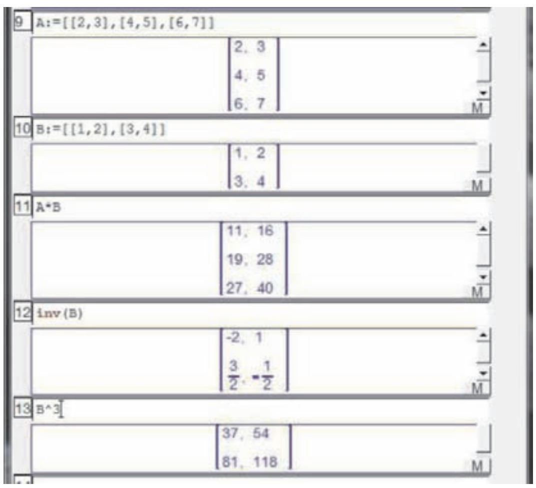
B Liste des commandes utiles avec des matrices

matrix(3,4,(j,k)->j+k)	Permet de saisir une matrice définie par une formule
M :=[[1,2,3],[4,5,6]]	Permet de saisir une matrice définie par des coefficients
v :=[0,1,0]	Permet de saisir un vecteur défini par ses coordonnées
$+,-,*$	Addition, soustraction, produit de matrices
inv(M)	Renvoie l'inverse d'une matrice carrée
Mˆn	Renvoie la puissance entière d'une matrice M

Exemples :

- Pour trouver un couple solution à l'équation : $17x - 40y = 1$, on écrit `iabcuv(17,-40,1)` qui renvoie $[-7\,;-3]$.
- Pour convertir le nombre 496 en base 7, on écrit `convert496,(base,7)` qui renvoie [6,0,3,1] pour $\overline{1306}^7$.
- Pour trouver le code ASCII du mot "merci", on écrit `asc("merci")` qui renvoie [109,101,114,99,105].
- Pour trouver l'inverse de la matrice B$=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$, on écrit `inv(B)` qui renvoie $\begin{pmatrix}-2 & 1\\ \frac{3}{2} & -\frac{1}{2}\end{pmatrix}$.





SOLUTIONS

Chapitre AR1
Multiples. Division euclidienne. Congruence

Auto-évaluation

1 1) Oui, car 36 divisible par 4
2) Non, car 14 non divisible par 4
3) Oui, car 52 divisible par 4
4) Non, car 94 non divisible par 4

2 1) Divisible par 3 mais pas par 9
2) Divisible par 3 et par 9
3) Divisible par 3 et par 9
4) Divisible par 3 et par 9

3 456 et 50 106

4 1) 1 ; 2 ; 3 ; 4 ; 6 ; 9 ; 12 ; 18 ; 36
2) 1 ; 2 ; 3 ; 4 ; 6 ; 8 ; 12 ; 16 ; 24 ; 48
3) 1 ; 2 ; 3 ; 4 ; 6 ; 8 ; 12 ; 16 ; 24 ; 32 ; 48 ; 96
4) 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 8 ; 10 ; 12 ; 15 ; 16 ; 20 ; 24 ; 30 ; 40 ; 48 ; 60 ; 80 ; 120 ; 240

5 1) 1 4) 7
2) 0 5) 2
3) 1 6) 3

6 Les restes obtenus sont 0, 1, 2, 3, 4, 5, 6.

7 1) Dividende : 117 ; quotient : 6 ; reste : 15
2) Reste : $15 - 12 = 3$

8 1) a et b ont même parité.
2) a et b ont des parités contraires.
3) La somme de deux entiers de même parité est paire ; la somme de deux entiers de parités contraires est impaire.

9 1) a ou b est pair.
2) a et b sont impairs.
3) Le produit de deux entiers dont l'un au moins est pair, et impair s'ils sont tous deux impairs.

10 1) a est pair.
2) a est impair.
3) Un entier et son carré ont même parité.

S'entraîner

1 $D_{150} = \{1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150\}$
$D_{230} = \{1, 2, 5, 10, 23, 46, 115, 230\}$
$D_{810} = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 27, 30, 45, 54, 81, 90, 135, 162, 270, 405, 810\}$

2 Un nombre est divisible par 6 s'il est divisible par 2 et par 3.
$n = a(a^2 - 1) = a(a-1)(a+1)$.
Comme $(a-1)$, a, $(a+1)$ sont 3 entiers consécutifs, alors l'un au moins est pair et un autre est divisible par 3. n est alors divisible par 2 et par 3.

3 1) Si d divise a et b, il divise toute combinaison linéaire de a et de b donc il divise $3a - 5b = 15k + 12 - 15k - 5 = 7$.
2) d est à chercher dans l'ensemble de diviseurs de 7, soit $\{1, 7\}$

4 1) $193 = 16 \times 12 + 1$ 3) $-20 = 7(-3) + 1$
2) $18 = 50 \times 0 + 18$ 4) $-354 = 17(-21) + 3$

5 On a : $63 = bq + 17 \Leftrightarrow bq = 46$
Comme $b > 17$, on a : $b = 46$ et $q = 1$ ou $b = 23$ et $q = 2$.

6 $x = 3 \times 7 + r$ avec $0 \leqslant r \leqslant 3$.
$x \in \{21, 22, 23\}$

7 $a = 18q + 13 = 6(3q + 2) + 1$. Le reste de la division de a par 6 est 1.

8 $$\begin{cases} a - b = 538 \\ a = 13b + 34 \end{cases} \Leftrightarrow \begin{cases} b = \dfrac{538 - 34}{12} = 42 \\ a = 538 + 42 = 580 \end{cases}$$

9 1) $a \equiv 2\ (9)$ 4) $a \equiv 4\ (9)$
2) $a \equiv -3\ (9)$ 5) $a \equiv -3\ (9)$
3) $a \equiv -1\ (9)$ 6) $a \equiv -4\ (9)$

10 $12^5 \equiv 1\ (11)$, $78^{15} \equiv 1\ (11)$, $10^7 \equiv 6\ (11)$

11 $2^5 = 33 - 1$ donc $2^5 \equiv -1\ (11)$
$13^{12} \equiv 2^{12} \equiv (2^5)^2 \times 2^2 \equiv 4\ (11)$
$(-2)^{19} = -(2^5)^3 \times 2^4 \equiv 16 \equiv 5\ (11)$

12 $6 \equiv 1\ (5)$ donc $6^n - 1 \equiv 0\ (5)$ donc $6^n - 1$ est divisible par 5.

13 1) $(x+y)(x-y=21$ donc

$$\begin{cases} x+y=21 \\ x-y=1 \end{cases} \text{ ou } \begin{cases} x+y=7 \\ x-y=3 \end{cases}$$

Les couples sont $(11;10)$ et $(5;2)$.

2) $x(x-7y)=17$ donc $\begin{cases} x=17 \\ x-7y=1 \end{cases}$

Système impossible, pas de solution entière.

20 $n=4r+r=5r$ avec $0 \leqslant r < 5$
$n \in \{0,5,10,15,20\}$

26 • $351=7\times 50+1$ et $85=7\times 12+1$
$351^{12}\times 85^{15} \equiv 1^{12}\times 1^{15} \equiv 1\ (7)$
Le reste de la division par 7 est 1.

• $16=7\times 2+2$ et $23=7\times 3+2$
$16^{12}-23^{12} \equiv 2^{12}-2^{12} \equiv 0\ (7)$
Le reste de la division par 7 est 0.

29 $25=26-1$ donc $25 \equiv -1\ (13)$.
$5^{4k}-1 \equiv (5^2)^{2k}-1 \equiv (-1)^{2k}-1 \equiv 1-1 \equiv 0\ (13)$
Donc $5^{4k}-1$ est divisible par 13.

31 $3^0 \equiv 1(11)$; $3^1 \equiv 3(11)$; $3^2 \equiv 9(11)$; $3^3 \equiv 5(11)$; $3^4 \equiv 4(11)$; $3^5 \equiv 1(11)$.
Le cycle est de 5. On peut remplir le tableau de congruence suivant :

$n \equiv\ (5)$	0	1	2	3	4
$3^n \equiv\ (11)$	1	3	9	5	4
$3^n-7 \equiv\ (11)$	8	10	5	1	0

1) Les restes possibles de la division de 3^n par 11 sont : 1,3,4,5 et 9.
2) 3^n-7 est divisible par 11 si $n \equiv 4\ (5)$.

Auto-évaluation QCM

56 b **57** c **58** a
59 b **60** c **61** d
62 d **63** a **64** d

Chapitre AR2
PGCD. Théorèmes de Bézout et de Gauss

Auto-évaluation

1 1) $\text{PGCD}(26,65)=13$ d'où $\dfrac{26}{65}=\dfrac{2}{5}$.

2) $\text{PGCD}(72,54)=18$ d'où $\dfrac{72}{54}=\dfrac{4}{3}$.

3) $\text{PGCD}(255,35)=5$ d'où $\dfrac{255}{35}=\dfrac{51}{7}$.

2 16, 32 et 40.

3 1) 9 et 16 sont premiers entre eux.
2) 35 et 91 ne sont pas premiers entre eux.
$35=5\times 7$ et $91=7\times 13$.
3) 31 et 67 sont premiers entre eux. En outre, ils sont tous les deux premiers.

4 1) Fausse. 36 est divisible par 6 et 9 mais pas par 54.
2) Vraie car 8 et 9 sont premiers entre eux.
3) Vraie car 36 est le plus petit multiple commun à 4 et 18.
4) Fausse car 30 est un multiple de 10 et 15 et $30 \not\equiv 0\ (150)$

5 1) Vraie car si x est multiple de 81, il est aussi multiple de 9.
2) Vraie car $(1\ ;\ 1)$ est un couple solution de l'équation.

6 1) $(3\ ;\ 2)$ 3) $(1\ ;\ 0)$
2) $(-1\ ;\ 1)$ 4) $(-3\ ;\ -2)$

7 Pierre peut donner 16 jetons de 3 points et Jean lui rend 2 jetons de 7 points.

S'entraîner

1 1) $\text{PGCD}(12\ ;\ 42)=6$ 3) $\text{PGCD}(92\ ;\ 69)=23$
2) $\text{PGCD}(45\ ;\ 105)=15$ 4) $\text{PGCD}(72\ ;\ 108)=36$

2 $\text{PGCD}(35,42)=7$ et $35=7\times 5$, $42=7\times 6$.
Lorsque le coureur A aura fait 6 tours, le coureur B aura fait 5 tours, soit un temps de $35\times 6=210$ s.

3 **1)** PGCD(24 ; 40) $= 8$. Le côté du carré doit diviser 24 et 40, donc le plus grand côté possible est de 8 cm.
2) $40 = 8 \times 5$ et $24 = 8 \times 3$
Pour former le plus petit carré, il faut mettre 3 fois la longueur et 5 fois la largeur du rectangle, soit 120 cm.

4 **1)** PGCD(78; 108) $= 6$ car
$$108 = 78 \times 1 + 30$$
$$78 = 30 \times 2 + 18$$
$$30 = 18 \times 1 + 12$$
$$18 = 12 \times 1 + 6$$
$$12 = 6 \times 2$$
2) PGCD(144; 840) $= 24$ car
$$840 = 144 \times 5 + 120$$
$$144 = 120 \times 1 + 24$$
$$120 = 24 \times 5$$
3) PGCD(202; 138) $= 2$ car
$$202 = 138 \times 1 + 64$$
$$138 = 64 \times 2 + 10$$
$$64 = 10 \times 6 + 4$$
$$10 = 4 \times 2 + 2$$
$$4 = 2 \times 2$$

5 $(-1)n + 1(n+1) = 1$. Donc d'après le théorème de Bézout, n et $(n+1)$ sont premiers entre eux.

6 **1)** 4 divise $5(x+3)$. Or PGCD$(4,5) = 1$, donc d'après le théorème de Gauss, 4 divise $(x+3)$.
On a donc $x + 3 = 4k$.
En remplaçant dans l'équation, on obtient $y = 5k$.
Les couples solutions sont : $\begin{cases} x = -3 + 4k \\ y = 5k \end{cases}, k \in \mathbb{Z}$
2) $41x = 9(-y)$ (1)
9 divise $41x$. Or PGCD$(9, 41) = 1$, donc d'après le théorème de Gauss, 9 divise x.
On a donc $x = 9k$.
En remplaçant dans l'équation, on obtient $y = -41k$.
Les couples solutions sont : $\begin{cases} x = 9k \\ y = -41k \end{cases}, \quad k \in \mathbb{Z}$

7 $(-2\,;\,3)$ est solution.

8 **1)** Oui car PGCD(37 ; 25) $= 1$, donc d'après le théorème de Bézout, il existe au moins un couple solution.
2) Non car PGCD(51 ; 39) $= 3$ et comme 1 n'est pas multiple de 3, d'après le corollaire de Bézout, il n'y a pas de solution.
3) Oui car PGCD(51 ; 39) $= 3$ et comme 2016 est divisible par 3, d'après le corollaire du Bézout, il existe des solutions entières.

13 **1)** PGCD(441 ; 777) $= 21$ car
$$777 = 441 \times 1 + 336$$
$$441 = 336 \times 1 + 105$$
$$336 = 105 \times 3 + 21$$
$$105 = 21 \times 5$$
2) PGCD(9185 ; 2004) $= 167$ car
$$9185 = 2004 \times 4 + 1169$$
$$2004 = 1169 \times 1 + 835$$
$$1169 = 835 \times 1 + 334$$
$$835 = 334 \times 2 + 167$$
$$334 = 167 \times 2$$

22 $(-2)(7k+3) + 7(2k+1) = -14k - 6 + 14k + 7 = 1$.
D'après le théorème de Bézout, $(7k+3)$ et $(2k+1)$ sont premiers entre eux pour tout entier relatif k.

28 On utilise l'algorithme d'Euclide :

$$40 = 17 \times 2 + 6 \qquad (1)$$
$$17 = 6 \times 2 + 5 \qquad (2)$$
$$6 = 5 \times 1 + 1 \qquad (3)$$

40 et 17 sont donc premiers entre eux.

On remonte l'algorithme d'Euclide :
de (3), on obtient $5 = 6 - 1$

On remplace dans (2) :
$17 = 6 \times 3 - 1$ donc $6 \times 3 = 17 + 1$

On multiplie (1) par 3

$$\begin{aligned} 40 \times 3 &= 17 \times 6 + 6 \times 3 \\ &= 17 \times 6 + 17 + 1 \\ &= 17 \times 7 + 1 \end{aligned}$$

On a alors $17 \times (-7) - 40 \times (-3) = 1$.

42 • $(2\,;\,2)$ est une solution particulière.
• Soit $(x\,;\,y)$ la solution générale, on écrit :

$$\begin{cases} 4x - 3y = 2 \\ 4(2) - 3(2) = 2 \end{cases}$$

En soustrayant termes à termes, on obtient :
$4(x-2) = 3(y-2)$ (1)
3 divise $4(x-2)$. Or $\text{PGCD}(4;3) = 1$, donc d'après le théorème de Gauss, 3 divise $(x-2)$. On a alors : $x - 2 = 3k$.
En remplaçant dans (1), on obtient : $y - 2 = 4k$.
L'ensemble des couples solutions est de la forme :

$$\begin{cases} x = 2 + 3k \\ y = 2 + 4k \end{cases} \quad k \in \mathbb{Z}$$

Auto-évaluation QCM

58 a **59** b **60** c
61 c **62** d **63** a
64 b **65** c **66** b
67 a **68** b **69** a, c et d
70 b et d

Chapitre AR3
Les nombres premiers

Auto-évaluation

1 Ils ne comptent aucun diviseur autre que 1 et eux-même.

2 **1)** divisible par 3 **5)** divisible par 11
2) divisible par 7 **6)** divisible par 7
3) divisible par 11 **7)** divisible par 11
4) divisible par 5 **8)** divisible par 3

3 **1)** 1, 2, 4, 8, 16
2) 1, 3, 5, 15
3) 1, 2, 3, 4, 6, 8, 12, 24
4) 1, 2, 3, 4, 6, 9, 12, 18, 36
5) 1, 3, 5, 9, 15, 45
6) 1, 3, 17, 51
7) 1, 3, 7, 9, 21, 63
8) 1, 7, 13, 91

4 **1)** $n \equiv 0\ (6)$ **3)** $n \equiv 0\ (12)$
2) $n \equiv 0\ (15)$ **4)** $n \equiv 0\ (72)$

5 **1)** n est divisible par 5.
2) Si n est divisible par 4 et 5, alors n est divisible par 20.
3) Si n est inférieur ou égal à 25 et si n n'est divisible ni par 2, ni par 3, ni par 5, alors n est premier.
4) Si p est premier et si p divise le produit ab, alors p divise a ou p divise b.

S'entraîner

1 47, 67, 83
2 31, 37, 41, 43, 47, 53, 59
3 Soit $a \in \{0, 5, 10, 15, 20\}$ et b quelconque, soit $b \in \{0, 5, 10, 15, 20\}$ et a quelconque.
4 Si p divise n^2, d'après le théorème de Gauss avec les nombres premier, p divise n et donc p^2 divise n^2.
5 Si 13 divise a^5, comme 13 est premier, d'après le théorème de Gauss, 13 divise a. Donc 13^4 divise a^4 et donc 13^4 divise $a^4 \times \dfrac{a}{13} = \dfrac{a^5}{13}$.

6

$30 = 2 \times 3 \times 5$	$120 = 2^3 \times 3 \times 5$
$40 = 2^3 \times 5$	$800 = 2^5 \times 5^2$
$64 = 2^6$	$2\,000 = 2^4 \times 5^3$
$70 = 2 \times 5 \times 7$	$60\,000 = 2^5 \times 3 \times 5^4$

7 $6! = 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 = 2^4 \times 3^2 \times 5$

8 $29^2 - 4 = (29-2)(29+2) = 27 \times 31 = 3^3 \times 31$

$85^2 - 16 = (85-4)(85+4) = 81 \times 89 = 3^4 \times 89$

9 $48 = 2^4 \times 3$ donc 48 a $5 \times 2 = 10$ diviseurs.

10 $60 = 2^2 \times 3 \times 5$ donc 60 a $3 \times 2 \times 2 = 12$ diviseurs.

11 Il faut utiliser les diviseurs premiers les plus petits possibles avec la puissance la plus grande possible :

- avec 1 diviseur premier : $2^5 = 32$, soit 6 diviseurs.
- avec 2 diviseurs premiers : $2^4 \times 3 = 48$, soit $5 \times 2 = 10$ diviseurs.
- avec 3 diviseurs premiers : $2 \times 3 \times 5 = 30$, soit $2 \times 2 \times 2 = 8$ diviseurs.

Le nombre qui possède le plus de diviseurs et qui est compris entre 2 et 50 est 48.

12 On utilise la même méthode que dans l'exercice **11**

- Avec 1 diviseur premier : $2^6 = 64$, soit 7 diviseurs.
- Avec 2 diviseurs premiers :

1) $2^5 \times 3 = 96$, soit $6 \times 2 = 12$ diviseurs.

2) $2^3 \times 3^2 = 72$, soit $4 \times 3 = 12$ diviseurs.

- Avec 3 diviseurs premiers :

1) $2^2 \times 3 \times 5 = 60$, soit $3 \times 2 \times 2 = 12$ diviseurs.

2) $2 \times 3^2 \times 5 = 90$, soit $2 \times 3 \times 2 = 12$ diviseurs.

Les nombres qui possèdent le plus de diviseurs sont donc 60, 72, 90 et 96.

13 • $9 < \sqrt{97} < 10$.

On teste tous les nombres premiers inférieurs à 10 soit : 2, 3, 5 et 7. Ils ne divisent pas 97.

97 est un nombre premier.

• $10 < \sqrt{109} < 11$

On teste tous les nombres premiers inférieurs à 11, soit 2, 3, 5, 7. Ils ne divisent pas 109.

109 est premier.

• 117 est divisible par 3 car : $1 + 1 + 7 = 9$.

117 n'est pas premier.

• $16 < \sqrt{271} < 17$.

On teste tous les nombres premiers inférieurs à 17, soit : 2, 3, 5, 7, 11, 13. Ils ne divisent pas 271.

271 est un nombre premier.

• $17 < \sqrt{323} < 18$.

On teste tous les nombres premiers inférieurs à 18, soit : 2, 3, 5, 7, 11, 13, 17.

17 divise 323 car $323 = 17 \times 19$.

323 n'est pas un nombre premier.

• $20 < \sqrt{401} < 21$.

On teste tous les nombres premiers inférieurs à 21, soit : 2, 3, 5, 7, 11, 13, 17, 19. Ils ne divisent pas 401.

401 est un nombre premier.

• $22 < \sqrt{527} < 23$.

On teste tous les nombres premiers inférieurs à 23, soit : 2, 3, 5, 7, 11, 13, 17, 19.

17 divise 527 car $527 = 17 \times 31$.

527 n'est pas un nombre premier.

• $26 < \sqrt{719} < 27$.

On teste les nombres premiers inférieurs à 27, soit : 2, 3, 5, 7, 11, 13, 17, 19, 23.

Ils ne divisent pas 719.

719 est un nombre premier.

25 $960 = 2^6 \times 3 \times 5$.

960 a $7 \times 2 \times 2 = 28$ diviseurs.

27 **1)** $2\,650 = 1\,272 \times 2 + 106$ et $1\,272 = 106 \times 12$ donc $\text{PGCD}(2\,650 ; 1\,272) = 106$.

2) $2650 = 2 \times 5^2 \times 53$ et $1272 = 2^3 \times 3 \times 53$ donc $\text{PGCD}(2\,650 ; 1\,272) = 2 \times 53 = 106$

3) Euclide est nettement plus efficace car il demande beaucoup moins d'opérations.

30 $792 = 2^3 \times 3^2 \times 11$.
792 a $4 \times 3 \times 2 = 24$ diviseurs.
Les diviseurs de 792 sont :
1, 2, 4, 8, 3, 6, 12, 24, 9, 18, 36, 72, 11, 22, 44, 88, 33, 66, 132, 264, 99, 198, 396, 792.

36 **1)** On a : $n^2 = 2^{2\alpha}3^{2\beta}$

$$(2\alpha+1)(2\beta+1) = 3(\alpha+1)(\beta+1)$$
$$4\alpha\beta + 2\alpha + 2\beta + 1 = 3\alpha\beta + 3\alpha + 3\beta + 3$$
$$\alpha\beta - \alpha - \beta + 1 = 3$$
$$\alpha(\beta-1) - (\beta-1) = 3$$
$$(\beta-1)(\alpha-1) = 3$$

2) $(\alpha-1)$ et $(\beta-1)$ sont des diviseurs de 3. Deux choix sont alors possibles :

$$\begin{cases} \alpha - 1 = 3 \\ \beta - 1 = 1 \end{cases} \quad \text{ou} \quad \begin{cases} \alpha - 1 = 1 \\ \beta - 1 = 3 \end{cases}$$

On obtient $\alpha = 4,\ \beta = 2$ ou $\alpha = 2,\ \beta = 4$.
Les valeurs de n possibles sont :
$n = 2^4 \times 3^2 = 144$ ou $n = 2^2 \times 3^4 = 324$.

Auto-évaluation QCM

53 c **54** a **55** c
56 b, c **57** c **58** a et b
59 b **60** d **61** d
62 d

Chapitre MS1
Matrices : opérations

Auto-évaluation

1 **1)** Avec $x = y = z = t = 1$, les quatre égalités sont vraies.

2) $a_{1,1} + a_{2,2} + a_{3,3} + a_{4,4}$
$16 + 10 + 7 + 1 = 34$.
$a_{4,1} + a_{3,2} + a_{2,3} + a_{1,4}$
$= 4 + 6 + 11 + 13 = 34$.

3) $$\begin{cases} 16x + 5y + 9z + 4t = 34 \\ 3x + 10y + 6z + 15t = 34 \\ 2x + 11y + 7z + 14t = 34 \\ 13x + 8y + 12z + t = 34 \end{cases}$$

2 **1)** **a)** Aucun couple solution.
b) Une solution : $(-24 ; 58)$.
c) Tout couple est solution.
1) $3 \times 6 = -2 \times (-9) = 18 ; 5 \times 3 = 15$ et $7 \times 2 = 14 ; 10 \times 12 = 8 \times 15 = 120$.
Le 1^er^ et le 3^e^ tableaux sont des tableaux de proportionnalité.

3 **1)** Les coordonnées du point de concours sont $(2 ; 1)$.
2) Les coordonnées du centre de gravité sont $\left(\dfrac{11}{3} ; \dfrac{5}{3}\right)$.

4 **1)** $P(x) = 2x^2 + 3x - 1$.
2) $P(x) = -\dfrac{1}{4}x^2 + \dfrac{1}{2}x + \dfrac{3}{4}$.

S'entraîner

1 1) F 2) F 3) V 4) F
2 1) F 2) V 3) F 4) V
3 1) V 2) F 3) F 4) V
4 1) V 2) V 3) V 4) F
5 1) F
2) a) F b) V c) V
d) F

6 1) F 2) F

7 **1)** 3×3 **2)** 3×1 **3)** n'existe pas **4)** 1×3

8 Les matrices suivantes existent : **1)** si $\det(C) \neq 0$.
3) pour toute condition.
4) pour toute condition.
5) pour toute condition.
7) si C a autant de colonnes que N a de lignes.
8) si N a autant de colonnes que C a de lignes.

9 **1)** $a_{13} = 18$ et $a_{31} = 12$.
2) **a)** 68 **b)** 3 **c)** 7

10 **1)** 5
2) Le nombre de T-shirts T_2 ; le nombre de T-shirts de taille L.

30 **1)** $\begin{pmatrix} 6 \\ -13 \end{pmatrix}$ **2)** $\begin{pmatrix} 4 & -3 \\ -8 & 3 \end{pmatrix}$ **3)** $\begin{pmatrix} 8 & -4 & 4 \\ 2 & -1 & 1 \\ 4 & -2 & 2 \end{pmatrix}$ **4)** $\begin{pmatrix} -4 \\ -2 \\ -7 \end{pmatrix}$

37 **1)** $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$; $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
2) $\begin{pmatrix} -2 & 6 \\ -2 & -2 \end{pmatrix}$; $\begin{pmatrix} -8 & 0 \\ 0 & -8 \end{pmatrix}$
3) $\begin{pmatrix} -1 & -4 \\ 8 & 7 \end{pmatrix}$; $\begin{pmatrix} -9 & -11 \\ 22 & 13 \end{pmatrix}$
4) $\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$; $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

68 **1)** $(13\ ;\ 18)$ **2)** $\varnothing$ **3)** $\varnothing$ **4)** $(1\,000\ ;\ 300)$

70 **1)** $(-1\ ;\ -5\ ;\ 6)$ **2)** $(-7\ ;\ 0\ ;\ 6)$ **3)** $(14\ ;\ -11\ ;\ 10)$ **4)** $(-3\ ;\ 2\ ;\ -1)$

Auto-évaluation QCM

109 c	**110** a	**111** d
112 b	**113** b c	**114** c
115 b	**116** c	**117** d
118 c	**119** b c	**120** c d
121 b d	**122** a b	**123** d
124 b d		

Chapitre MS2
Suites de matrices et marches aléatoires

Auto-évaluation

1 **1)** $u_n = \left(\frac{1}{3}\right)^n \times 27$.
2) $0 < \frac{1}{3} < 1$ donc u_n converge et $\lim\limits_{n \to +\infty} \left(\frac{1}{3}\right)^n = 0$ donc $\lim\limits_{n \to +\infty} u_n = 0$.

2 **1)** $k = 1$.
2) $b_{n+1} = -3b_n$ donc (b_n) est géométrique de raison -3.
3) $a_n = (-3)^n(a_0 - 1) + 1$.

3 **1)** $D^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$.
$D^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2\sqrt{2} & 0 \\ 0 & 0 & 8 \end{pmatrix}$.
2) $D^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (\sqrt{2})^n & 0 \\ 0 & 0 & 2^n \end{pmatrix}$.
3) Initialisation : $D^0 = I_3$.
Hérédité : $D^{n+1} = D^n D$
$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & (\sqrt{2})^n & 0 \\ 0 & 0 & 2^n \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & 2 \end{pmatrix}$
$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & (\sqrt{2})^{n+1} & 0 \\ 0 & 0 & 2^{n+1} \end{pmatrix}$.
4) $T^3 = 0$ et, par récurrence, $T^n = 0$ pour $n \geqslant 3$.

4 **1)** $\det(P) = a - b = \sqrt{5} \neq 0$.
P est donc inversible.
$P^{-1} = \begin{pmatrix} \frac{\sqrt{5}}{5} & \frac{-\sqrt{5}+5}{10} \\ -\frac{\sqrt{5}}{5} & \frac{\sqrt{5}+5}{10} \end{pmatrix}$.
2) $PDP^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

5 $P(B) = 0{,}7$ et $P_B(A) = \frac{3}{7}$ car
$P(A \cap B) = P_A(B) \times P(A)$ et $P_B(A) = \frac{P(A \cap B)}{P(B)}$.

6 **1)** 2 fois sur 3 une consonne suit une voyelle et 7 fois sur 8 une voyelle suit une consonne.

2) a) $P_{\{X_n=0\}}(\{X_{n+1}=1\})=\frac{2}{3}$.

$P_{\{X_n=1\}}(\{X_{n+1}=1\})=\frac{1}{3}$.

$P_{\{X_n=1\}}(\{X_{n+1}=0\})=\frac{7}{8}$.

$P_{\{X_n=0\}}(\{X_{n+1}=0\})=\frac{1}{8}$.

b) $P_{\{X_{n+1}=0\}}$ et $P_{\{X_{n+1}=1\}}$ valent respectivement : $\frac{1}{8}P_{\{X_n=0\}}+\frac{2}{3}P_{\{X_n=1\}}$ et $\frac{7}{8}P_{\{X_n=0\}}+\frac{1}{3}P_{\{X_n=1\}}$.

S'entraîner

1 **1)** Fausse **2)** Vraie **3)** Vraie **4)** Vraie

2 **1)** Oui **2)** Non

3 **1)** Non **2)** Oui **3)** Oui **4)** Non

4 **1)** Oui **2)** Non **3)** Oui

5 **1)** $\begin{pmatrix}0,8 & 0,2\\ 0,6 & 0,4\end{pmatrix}$ **2)** $\begin{pmatrix}0 & 1\\ 0,35 & 0,65\end{pmatrix}$ **3)** $\begin{pmatrix}0,3 & 0,7 & 0\\ 0 & 0,2 & 0,8\\ 0 & 1 & 0\end{pmatrix}$ **4)** $\begin{pmatrix}0 & 2/5 & 3/5\\ 1/3 & 1/3 & 1/3\\ 4/3 & 0 & 3/7\end{pmatrix}$

6 **1)** Non, il n'y en pas.

2) $M=\begin{pmatrix}4/7 & 3/7\end{pmatrix}$.

11 **1)** $\det(P)=-1\neq 0$. P est donc inversible.

$P^{-1}=\begin{pmatrix}1 & 1\\ -2 & -3\end{pmatrix}$.

2) a) $P\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}P^{-1}$

$=\begin{pmatrix}6 & 1\\ -4 & -1\end{pmatrix}P^{-1}=A$.

b) $A^n=P\begin{pmatrix}2^n & 0\\ 0 & 1\end{pmatrix}P^{-1}$

$=\begin{pmatrix}3\times 2^n-2 & 3(2^n-1)\\ -2^{n+1}+2 & -2^{n+1}+3\end{pmatrix}$.

23 **1)** $\begin{pmatrix}-0,5\\ -0,5\end{pmatrix}$.

2) $V_{n+1}=U_{n+1}-C=AU_n+B-C=AU_n+B-AC-B=AV_n$.

3) V_n est donc une suite géométrique, d'où : $V_n=A^nV_0$.

4) $U_n=V_n-C=A^n(U_0-C)+C$.

5) a) Preuve par récurrence.

Initialisation : triviale.

Hérédité : $A^{n+1}=A\times A^n$

$=\begin{pmatrix}3^{n+1} & 2(n+1)\times 3^n\\ 0 & 3^{n+1}\end{pmatrix}$.

b) $\begin{pmatrix}\dfrac{3^{n+1}}{2}+5n\times 3^{n-1}-0,5\\ \dfrac{5\times 3^n}{2}-0,5\end{pmatrix}$.

27 **1)** À l'étape n, on a : $a_{n+1}=0,8a_n+0,6b_n$ et $b_{n+1}=0,2a_n+0,4b_n$. D'où : $T=\begin{pmatrix}0,8 & 0,6\\ 0,2 & 0,4\end{pmatrix}$

2) $a_{n+1}=0,8a_n+0,6b_n$ avec $b_n=1-a_n$ d'où l'égalité cherchée.

3) $U_{n+1}=a_{n+1}-0,75=0,2a_n+0,6-0,75=0,2V_n$

4) $a_n=U_n+0,75$ avec $\lim_{n\to+\infty}U_n=0$ donc $\lim_{n\to+\infty}a_n=0,75$ et comme $b_n=1-a_n$, on a $\lim_{n\to+\infty}P_n=\begin{pmatrix}0,75\\ 0,25\end{pmatrix}$

Cette limite représente la répartition stable correspondant à la marche aléatoire définie par le graphe donné c'est-à-dire, qu'au bout d'un nombre d'étapes assez grand, la probabilité d'être sur le sommet A est trois fois plus importante que d'être sur le sommet B.

Auto-évaluation QCM

50 a d **51** c **52** b c d

53 c **54** a **55** b, c

56 d **57** a, c **58** a, c

59 c **60** b

LEXIQUE

Suivi éditorial : Catherine Rollet
Coordination éditoriale : Adrien Fuchs
Écriture de la maquette en LaTeX : Jean-Côme Charpentier et Sébastien Mengin
Mise en page du manuel en LaTeX : Sébastien Mengin (Édilibre)
Couverture : Maro Haas (MH Design)
Maquette Intérieure : Nicolas Balbao
Concepteurs/Techniciens des interfaces de Sésamath : Thomas Crespin et Daniel Caillibaud