Table des matières

Première partie

Livre de l'élève

Chapitre 1

Divisibilité

I Exercices

1.1 Divisibilité

Exercice 1.1

Déterminer tous les rectangles à côtés entiers d'aire 24 cm^2.

Exercice 1.2

Déterminer les points à coordonnées entières qui sont sur la droite d'équation $y = 13x$ dont l'ordonnée est comprise entre 200 et 230.

Exercice 1.3

1. Peut-on écrire la liste de tous les multiples de 12 ? Si la réponse est oui, écrire cette liste.
2. Peut-on écrire la liste de tous les diviseurs de 12 ? Si la réponse est oui, écrire cette liste.

Exercice 1.4

Pour chacune des affirmations ci-dessous, indiquer si elle est vraie ou fausse, en justifiant.

1. Tous les nombres entiers sont multiples de zéro.
2. Zéro est multiple de tous les nombres entiers.
3. Tous les nombres entiers sont multiples de 1.
4. 1 est multiple de tous les nombres entiers.

Exercice 1.5

Est-ce que pour tout nombre entier n, le nombre $n + 4$ est multiple de 2 ?

Si la réponse est oui, justifier pourquoi.

Si la réponse est non, pour quelles valeurs de n le nombre $n + 4$ est multiple de 2 ? Justifier.

Exercice 1.6

Pour un entier x, le nombre $9x^2 - 25$ est-il un multiple $3x - 5$?

Exercice 1.7

Lorsque n est un nombre entier, le nombre $3n + 12$ est-il multiple de 3 ? Justifier.

Exercice 1.8

1. Dans le repère de la figure 1.1 tracer la droite (d) d'équation cartésienne $6x - 2y = 5$.
2. La droite (d) a-t-elle des points à coordonnées entières ?

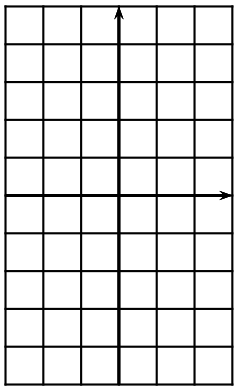


Fig. 1.1

Exercice 1.9

Déterminer les entiers n tels que $2n - 3$ divise 4.

Exercice 1.10

Déterminer les entiers naturels x et y tels que $x^2 - y^2 = 49$

Exercice 1.11

La somme de trois entiers consécutifs est-elle divisible par 3 ? Justifier.

Exercice 1.12

Démontrer que si n est multiple de 3, alors $n(n^2 + 18)$ est multiple de 27.

Exercice 1.13

Déterminer tous les triangles rectangles à côtés entiers tels qu'un côté de l'angle droit mesure 6 cm.

1.2 Propriétés de la divisibilité

Exercice 1.14

Un nombre entier a divise deux nombres entiers b et c, ce qui signifie que b et c sont multiples de a.

1. Le nombre a divise-t-il la somme $b + c$? Justifier.
2. Le nombre a divise-t-il la différence $b - c$? Justifier.
3. Pour deux autres entiers u et v, le nombre a divise-t-il la combinaison linéaire $bu+cv$? Justifier.

Exercice 1.15

Déterminer les entiers n tels que $n + 3$ divise $n + 5$. Indication : $n + 3$ divise $n + 3$.

Exercice 1.16

Déterminer les entiers n tels que $3n - 1$ divise $n - 2$.

1.3 Division euclidienne

Exercice 1.17 (Un code et sa clef de contrôle)

Un site Internet a prévu un système de numéro d'inscription à huit chiffres et une clef de contrôle à deux chiffres. On appelle a le nombre constitué par les huit chiffres. La clef de contrôle est le reste de la division euclidienne du nombre a par 97.

Prenons un exemple avec $a = 12\,345\,678$. La division euclidienne de a par 97 s'écrit :

$a = 12\,345\,678 = 97 \times 127\,275 + 3$.

Le reste de cette division est donc 3, ce qui donne 03 comme clef de contrôle. L'utilisateur saisit donc `12 345 678 | 03` et le site vérifie si `03` est bien la clef de contrôle de `12 345 678`.

1. Calculer la clef de contrôle du numéro `10 200 300`.
2. Un utilisateur saisit `10 200 345 | 17`
   a) Vérifier que ce numéro d'inscription est faux.
   b) L'utilisateur s'est trompé sur le dernier chiffre du numéro d'inscription c'est à dire le chiffre 5. Rectifier son erreur.

Exercice 1.18 (Code-barre et ISBN)

Les codes-barres figurent sur de nombreux articles vendus dans le commerce. Le code-barre d'un article est son numéro d'identification, c'est un numéro à 13 chiffres et son dernier chiffre est une clef de contrôle. Depuis 2007, le numéro ISBN, qui est réservé aux livres, utilise le même type de numérotation.
Le code-barre `9788073400972` est représenté sur la figure 1.2.

Fig. 1.2

On détermine sa clef de contrôle comme cela est indiqué ci-dessous.

- Dans les douze premiers chiffres,
  ▷ on calcule la somme des chiffres de rang impair : $S_1 = 9 + 8 + 0 + 3 + 0 + 9 = 29$;
  ▷ on calcule la somme des chiffres de rang pair : $S_2 = 7 + 8 + 7 + 4 + 0 + 7 = 33$.
- On calcule : $S = S_1 + 3S_2 = 29 + 3 \times 33 = 128$.
- On détermine le reste r de la division euclidienne de S par 10 : $r = 8$, puisque $128 = 10 \times 12 + 8$.
- La clef de contrôle est $10 - r = 10 - 8 = 2$.

Voici un code barre sans sa clef de contrôle c'est à dire avec ses douze premiers chiffres seulement : `978209172673`. Déterminer sa clef de contrôle.

Si l'on veut en savoir plus sur le code-barre et sur l'ISBN, voir le problème n° 8 pages 13, 14, 15 du manuel Hyperbole TS spécialité math.

Exercice 1.19

Effectuer la division euclidienne de a par b dans chacun des cas suivants. Écrire sa réponse sous la forme $a = bq + r$.

1. Sans calculatrice :
   a) $a = 26$ $b = 3$ **b)** $a = 534$ $b = 10$ **c)** $a = 837\,329$ $b = 100$
2. Avec calculatrice :
   a) $a = 453$ $b = 17$ **b)** $a = 2\,358$ $b = 43$ **c)** $a = 54\,200$ $b = 147$

Exercice 1.20

Comment obtient-on sans calcul le reste de la division d'un nombre entier par 10 ? par 100 ? par 1 000. Donner des exemples.

Exercice 1.21

1. **a)** Vérifier l'égalité $2\,882 = 23 \times 124 + 30$
   b) Ce calcul ne donne pas le quotient et le reste de la division euclidienne de 2 882 par 23. Pourquoi ?

2. Pour chacune des égalités suivantes, indiquer si l'égalité permet de donner le quotient et le reste de la division de a par b. Si la réponse est non, donner l'égalité correcte.

a) $a = 267$ $b = 18$ $267 = 18 \times 12 + 51$ **b)** $a = 3\,527$ $b = 73$ $3\,527 = 73 \times 48 + 23$

c) $a = 309$ $b = 7$ $309 = 7 \times 43 + 8$

Exercice 1.22

1. Donner toutes les divisions euclidiennes possibles de diviseur 4 et de quotient 12.

2. Donner toutes les divisions euclidiennes possibles de dividende 83 et de quotient 5.

Exercice 1.23

Une année non bissextile commence un lundi. Calculer le jour de la semaine correspondant au

1. 25 janvier **2.** 20 avril

Après avoir abordé la divisibilité, puis la division euclidienne, l'exercice ci-dessous permet de faire le lien entre divisibilité et la division euclidienne.

Exercice 1.24

1. **a)** Effectuer la division euclidienne de 9 953 par 37.

b) 9 953 est-il divisible par 37 ?

2. Mêmes questions **a)** et **b)** pour 10 511 par rapport à 53.

3. Pour un nombre entier a et un nombre entier b non nul, lorsque a est divisible par b, que peut-on dire de la divison euclidienne de a par b ?

1.4 Congruences

Dans tous les exercices sur les congruences modulo n, n désigne un entier naturel supérieur ou égal à 2.

Exercice 1.25

Lire dans le cours la définition 1.4 (congruence modulo n), puis répondre aux questions ci-dessous.

1. Indiquer chaque fois si c'est vrai ou faux. Justifier.

a) $53 \equiv 13\ [10]$ **b)** $35 \equiv 21\ [5]$ **c)** $88 \equiv 70\ [9]$ **d)** $17 \equiv -1\ [6]$ **e)** $14 \equiv -2\ [3]$

2. Compléter ci-dessous.

a) $11 \equiv 5\ [\ldots]$ **b)** $26 \equiv 12\ [\ldots]$ **c)** $87 \equiv 62\ [\ldots]$ **d)** $7 \equiv -3\ [\ldots]$

3. Compléter ci-dessous.

a) $17 \equiv \ldots\ [2]$ **b)** $43 \equiv \ldots\ [5]$ **c)** $\ldots \equiv 30\ [7]$ **d)** $\ldots \equiv -4\ [10]$

4. L'affirmation ci-dessous est-elle vraie ou fausse ? Justifier.
$a \equiv 0\ [n] \iff a$ est multiple de n

Exercice 1.26 (Conséquence de la définition pour la division euclidienne)

1. **a)** Écrire la division euclidienne de 38 par 5 et déterminer le reste.

b) 38 est-il congru à ce reste modulo 5 ?

2. Pour un entier a, si r est le reste de la division euclidienne de a par n le nombre a est-il congru à r modulo n ?

3. **a)** Justifier que $38 \equiv 8\ [5]$.

b) Le reste de la division euclidienne de 38 par 5 est-il égal à 8 ?

4. Si $a \equiv r\ [n]$, le nombre r est-il le reste de la division euclidienne de a par n ? Si la réponse est non, quelle condition faut-il ajouter pour que ce soit toujours vrai ?

Exercice 1.27

Dans chacun des cas suivants, a et n sont des entiers naturels. Calculer chaque fois le nombre entier naturel b tel que $a \equiv b\ [n]$ et $0 \leqslant b < n$.

1. Sans calculatrice :

a) $a = 44 \quad n = 6$ **b)** $a = 763 \quad n = 2$ **c)** $a = 829 \quad n = 10$ **d)** $a = 73\,956 \quad n = 100$

2. Avec calculatrice :

a) $a = 328 \quad n = 17$ **b)** $a = 4\,657 \quad n = 38$ **c)** $a = 1\,327 \quad n = 148$

Exercice 1.28 (Congruence et division euclidienne – Une propriété importante)

1. 23 et 17 ont-ils le même reste dans la division euclidienne par 3 ?

2. Vérifier si 23 est congru à 17 modulo 3.

La généralisation de cette propriété est la propriété 1.9 du cours.

Exercice 1.29 (Congruence et opérations)

1. Justifier que $61 \equiv 19\ [7]$ et $36 \equiv 22\ [7]$.

2. Vérifier que :

(1) $61 + 36 \equiv 19 + 22\ [7]$ **(2)** $61 - 36 \equiv 19 - 22\ [7]$

(3) $61 \times 36 \equiv 19 \times 22\ [7]$ **(4)** $61^3 \equiv 19^3\ [7]$

Les généralisations de ces propriétés sont regroupées dans la propriété 1.10 du cours. C'est ce qui va nous permettre de simplifier considérablement les calculs.

Étudier l'exemple du paragraphe 1.3.b du cours, puis traiter l'exercice ci-dessous.

Exercice 1.30 (Reste de la division d'un grand nombre)

Déterminer le reste de la division de 33 000 000 000 000 par 7.

Exercice 1.31 (Clef de contrôle d'un numéro de RIB)

Le numéro d'un compte bancaire est nommé relevé d'identité bancaire (RIB).

En voici un exemple sans la clef de contrôle :

Code banque	Code guichet	Numéro de compte	Clé RIB
12802	00750	20741300623	

On appelle a le nombre 12 802 007 502 074 130 062 300

La clef de contrôle sert à vérifier s'il n'y a pas eu d'erreur de saisie sur les 21 premiers chiffres et elle est définie de la manière suivante : si r est le reste de la division euclidienne de a par 97, la clef est $97 - r$.

Calculer cette clef de contrôle.

Indication : pour calculer le reste de la division euclidienne de a par 97, on pourra décomposer par exemple ce nombre ainsi : $a = 12\,802\,007\,502 \times 10^{12} + 74\,130\,062\,300$ et on a tout intérêt à effectuer les divisions euclidiennes par 97 à l'aide d'un programme.

Exercice 1.32 (Clef de contrôle d'un numéro d'INSEE)

En France, l'INSEE [1] attribue à tout individu en France un numéro d'INSEE [2] constitué de 13 chiffres et de 2 chiffres supplémentaires qui sont une clef de contrôle.

Le numéro d'INSEE d'une personne sans la clef de contrôle est 2 87 04 06 164 068.

La clef de contrôle est définie de la manière suivante : si r est le reste de la division euclidienne de $2\,870\,406\,164\,068$ par 97, la clef est $97 - r$.

Calculer cette clef de contrôle.

1.5 Numération

La numération est la façon d'écrire les nombres. Il y a eu des numérations comme les numérations maya, égyptienne, romaine, etc. Notre numération décimale vient des indiens et des arabes.

Lire l'exemple et les explications ci-dessous avant de commencer les exercices.

Exemple : le nombre 493 est égal à $4 \times 100 + 9 \times 10 + 3$.

Plus généralement un nombre entier naturel à trois chiffres qui s'écrit $\overline{abc}$ est égal à $a \times 100 + b \times 10 + c$ où a, b, c, sont des nombres entiers entre 0 et 9.

Exercice 1.33 (Critère de divisibilité par deux)

Le chiffre des unités d'un nombre entier naturel est 6, autrement dit ce nombre s'écrit $\overline{ab6}$.

Démontrer que ce nombre est multiple de 2.

C'est ainsi qu'on démontre le critère de divisibilité par deux.

Exercice 1.34 (Critère de divisibilité par cinq)

Démontrer le critère de divisibilité par cinq pour un nombre entier naturel à trois chiffres. Il y aura deux cas à étudier.

Exercice 1.35 (Critère de divisibilité par trois)

On considère un nombre entier naturel à trois chiffre $\overline{abc}$.

1. Démontrer que $\overline{abc} \equiv a + b + c$ [3].
2. Démontrer le critère de divisibilité par trois pour un nombre entier naturel à trois chiffres.

Exercice 1.36

Pour un nombre entier naturel n, quels sont les chiffres des unités possibles de $n^2 + n$? Justifier.

1.6 Exercices divers

Exercice 1.37

Déterminer le reste de la division euclidienne de 5^{2018} par 7.

Indication : étudier d'abord les congruences modulo 7 de 5, 5^2, 5^3, etc.

1. L'INSEE est l'Institut National de la Statistique et des Études Économiques.
2. Détails du numéro d'INSEE dans le manuel Hyperbole 1re S, problème 7 page 13.

Exercice 1.38

Quels sont les entiers n tels que $n^4 - 1$ est multiple de 5 ?

Indication : étudier d'abord les congruences modulo 5 de n, n^2, n^4.

Exercice 1.39

1. Donner l'expression numérique qui permet de calculer $1 + 7 + 7^2 + \cdots + 7^{2017}$.
2. Le nombre $7^{2018} - 1$ est-il divisible par 6 ? Justifier.

Exercice 1.40

1. Résoudre les équations :

   a) $2x \equiv 3\ [5]$ **b)** $5x \equiv 2\ [3]$ **c)** $7x \equiv 25\ [53]$

2. Résoudre les équations :

   a) $x^2 \equiv 4\ [6]$ **b)** $x^2 \equiv 3\ [6]$ **c)** $x^2 \equiv 2\ [6]$
   d) $x^2 \equiv 2\ [7]$ **e)** $x^2 \equiv 1\ [33]$ **f)** $x(x + 17) \equiv 33\ [55]$

1.7 Pour réviser

Chapitre du livre n° 1 – Divisibilité dans $\mathbb{Z}$

Les exercices résolus

- ex 1 p 9 : divisibilité entre expressions en fonctions de n.
- ex 7 p 11 : division euclidienne entre expressions en fonctions de n.
- ex 15 p 17 : congruences, démontrer que $n(n^2 + 5)$ est divisible par 3.
- ex 16 p 17 : reste de la division euclidienne par de 23^{41} par 7.

Rubrique *Pour s'exercer*, corrigés page 156

- ex 3 p 9 : divisibilité entre expressions en fonctions de n.
- ex 5 p 9 : équation en nombres entiers
- ex 12 p 11 : division euclidienne entre expressions en fonctions de n.
- ex 18 p 17 : congruence
- ex 22 p 17 : reste de la division euclidienne par de 12^{1527} par 5.

Rubrique *Objectif bac*, corrigés page 158

- ex 101 p 28 (QCM) : questions 1 à 5
- ex 103 p 28 : questions 1 et 2

II Cours

1.1 Divisibilité

1.1.a Les nombres entiers

Ce chapitre, ainsi que les chapitres sur les théorèmes de Bézout et Gauss, et sur les nombres premiers porteront sur l'arithmétique, c'est à dire sur des calculs avec des nombres entiers.

Ce premier paragraphe est donc une mise au point sur les nombres entiers.

Définition 1.1 (Nombres entiers)

- Un nombre entier est un nombre entier relatif c'est à dire un nombre entier négatif, nul ou positif.
- Un nombre entier naturel est un nombre entier positif ou nul.
- L'ensemble des nombres entiers (relatifs) est noté $\mathbb{Z}$.
- L'ensemble des nombres entiers naturels est noté $\mathbb{N}$.

Propriété 1.1 (Opérations entres nombres entiers)

Pour deux nombres entiers a et b,

- La somme $a+b$, la différence $a-b$, le produit ab sont des nombres entiers.
- le quotient $\dfrac{a}{b}$ $(b \neq 0)$ de deux nombres entiers n'est pas toujours un nombre entier.

Remarque

La conséquence fondamentale de la propriété 1.1 est qu'en arithmétique, on utilisera exclusivement l'addition, la soustraction et la multiplication.

1.1.b Définitions

Définition 1.2 (Divisibilité)

Dire qu'un nombre entier a est divisible par un nombre entier b non nul signifie qu'il existe un nombre entier k tel que $a = b \times k$.

Définition 1.3 (Divisible, multiple, diviseur, divise)

Pour deux nombres entiers a et b, les expressions suivantes sont équivalentes :

- a est divisible par b ;
- a est multiple de b ;
- b est un diviseur de a.
- b divise a.

Exemple

14 est divisible par 2, puisque : $14 = 2 \times 7$ et on dit aussi que 14 est multiple de 2 ou que 2 est un diviseur de 14 ou encore que 2 divise 14.

1.1.c Propriétés de la divisibilité

Propriété 1.2

Pour trois nombres entiers a, b, c, si a divise b et b divise c alors a divise c.

Démonstration

Pour trois nombres entiers a, b, c, si a divise b et b divise c, cela signifie qu'il existe k et k' tels que $b = ka$ et $c = k'b$. Par conséquent $c = k'ka$ autrement dit a divise c.

Remarque

La propriété précédente est très simple à démontrer, mais elle est importante et servira très souvent.

Ce type de propriété est important en mathématiques. on appelle cela la transitivité : si a est en relation avec b et b en relation avec c, alors a est en relation avec c.

On retrouve la transitivité pour les relations d'égalité, d'infériorité, de parallélisme, d'inclusion.

Propriété 1.3

Pour trois nombres entiers a, b, c, si a divise b et c, alors a divise $b + c$ et $b - c$.
Autrement dit, pour trois nombres entiers,
si un nombre divise deux autres nombres, alors il divise leur somme et leur différence.

Démonstration

Pour trois nombres entiers a, b, c, dire que a divise b et c signifie qu'il existe des entiers k et k' tels que $b = ak$ et $c = ak'$.

Par conséquent : $b + c = ak + ak' = a(k + k')$ et $b - c = ak - ak' = a(k - k')$.

Donc : a divise $b + c$ et $b - c$.

Propriété 1.4

Pour trois nombres entiers a, b, c, si a divise b et c, alors, pour tous entiers u et v, a divise $bu + cv$.
Autrement dit, pour trois nombres entiers,
si un nombre divise deux autres nombres, alors il divise toute combinaison linéaire à coefficients entiers de ces deux nombres.

Démonstration

a divise b et c donc il existe des entiers k et k' tels que $b = ak$ et $c = ak'$.

Par conséquent : $bu + cv = aku + ak'v = a(ku + k'v)$ donc a divise $bu + cv$.

1.2 La division euclidienne

1.2.a Propriété et exemples

Propriété 1.5 (Division euclidienne)

Pour un nombre entier a et un nombre entier naturel non nul b, il existe un seul couple de nombres entiers (q, r) tel que : $a = bq + r$ et $0 \leqslant r < b$.

Remarques

- On peut traduire la propriété 1.5 par :
  dividende = diviseur × quotient + reste et reste < diviseur
- La propriété 1.5 évoque la division euclidienne d'un entier a (relatif) par un entier naturel b (positif), autrement dit un dividende positif ou négatif par un diviseur strictement positif. On peut en fait avoir un diviseur b non nul positif ou négatif et on écrit alors :
  $a = bq + r$ et $0 \leqslant r < |b|$.

Un exemple avec des petits nombres

Une division euclidienne pour des petits nombres est effectuée à l'aide des tables de multiplication, par exemple la division euclidienne de 27 par 4 : $27 = 4 \times 6 + 3$; $3 < 4$

Un exemple avec des plus grands nombres

Effectuons par exemple la division euclidienne de 13 473 par 37.

Calculons d'abord le quotient décimal à la calculatrice : $\dfrac{13\,473}{37} \approx 364,1$

Le quotient euclidien de la division euclidienne de 13 473 par 37 est donc la partie entière du résultat précédent, soit 364.

Calculons maintenant le reste : $13\,473 - 37 \times 364 = 5$

On a finalement : $13\,473 = 37 \times 364 + 5$; $5 < 37$

1.2.b Utilisation des calculatrices

Reprenons l'exemple précédent : la division euclidienne de 13 473 par 37.

Division euclidienne avec les calculatrices TI

- **Quotient** Le quotient euclidien, est la partie entière de $\dfrac{13\,473}{37}$, donc :
  - on utilise les touches : [math] [→] [3]
  - on complète ainsi : `ent(13473/37)`
  - on appuie sur [entrer]
  - Affichage : [364]
- **Reste avec la TI-82 Advanced ou la TI-83 Premium**
  - on utilise les touches : [math] [→] [0]
  - on complète ainsi : `remainder(13473,37)` ou `reste(13473,37)`
  - on appuie sur [entrer]
  - Affichage : [5]
- **Calcul du reste sans la commande `reste` ou `remainder`**
  On calcule tout simplement : $13\,473 - 37 \times 364 = 5$.
  Si l'on veut calculer le reste en une seule suite de calculs :
  `13473-37*ent(13473/37)` Affichage : 5

Division euclidienne avec la CASIO

Appuyer sur la touche [MENU] et choisir le module `RUN MAT`.

Appuyer sur les touches : [OPTN] [F4] (CALC) [F6] (→) [F6] (→)

- **Quotient**
  - saisir : `13473` [F1] (`Int÷`) `37`
  - on voit : `13473 Int÷ 37`
  - appuyer sur [EXE]
  - Affichage : [364]
- **Reste**
  Même procédure que pour le quotient, en remplaçant [F1] (`Int÷`) par [F2] (`Rmdr÷`).

Division euclidienne avec la NUMWORKS

Dans l'application Calculs, on utilise la touche Toolbox : [paste"]

- **Quotient**
  - touche Toolbox
  - on choisit la rubrique `Arithmetique`
  - touche [→]
  - descendre jusqu'à : `quo(p,q)`
  - appuyer sur [EXE]
  - on voit : `quo(,)`
  - compléter ainsi : `quo(13473,37)`
  - appuyer sur [EXE]
  - Affichage : [364]
- **Reste**
  Même procédure que pour le quotient, en remplaçant `quo(p,q)` par `rem(p,q)` et `quo(13473,37)` par `rem(13473,37)`.

1.2.c Utilisation des logiciels et de python3

	GeoGebra	**LibreOffice**	**Xcas**	**wxMaxima**	**python3**
Quotient de la division euclidienne de a par b	Quotient[a,b]	=QUOTIENT(a ;b)	iquo(a,b)	floor(a/b)	a//b
Reste de la division euclidienne de a par b	Reste[a,b]	=MOD(a ;b)	irem(a,b)	mod(a,b)	a%b
Division euclidienne de a par b	Division[a,b]		iquorem(a,b)	divide(a,b)	

1.2.d Division euclidienne et divisibilité

Propriété 1.6

Pour un nombre entier a et un nombre entier b non nul, dire que a est divisible par b signifie que le reste de la division euclidienne de a par b est zéro.

Démonstration

Dire qu'un nombre entier a est divisible par un nombre entier b non nul signifie qu'il existe un nombre entier k tel que $a = b \times k$, autrement dit $a = b \times k + 0$, ce qui signifie que le reste de la division euclidienne de a par b est zéro.

Remarque : cette propriété vient compléter la définition 1.3.

1.3 Congruence

Un des objectifs de ce chapitre est de pouvoir étudier différents système de codes qui utilisent la division euclidienne, comme dans l'exercice 1.17, avec des nombres ayant jusqu'à 23 chiffres, or les calculatrices, et mêmes les logiciels n'utilisent pas des nombres aussi longs.

Nous allons donc étudier une méthode de calculs, appelé *les congruences*, qui va permettre de réduire le nombre de chiffres à utiliser dans les calculs.

1.3.a Définition et propriétés

Définition 1.4 (Congruence modulo n)

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$, dire que a est congru à b modulo n signifie que $a - b$ est multiple de n.
On écrit : $a \equiv b\ [n]$ ou $a \equiv b\ (n)$ ou $a \equiv b\ (\text{mod } n)$.

Exemple

$48 \equiv 13\ [5]$ parce que $48 - 13$ est multiple de 5, en effet : $48 - 13 = 35 = 5 \times 7$.

Propriété 1.7 (Conséquence de la définition pour la division euclidienne)

Pour un nombre entier a, un nombre entier naturel r et pour un nombre entier naturel $n \geqslant 2$,
- si r est le reste de la division euclidienne de a par n alors $a \equiv r\ [n]$;
- si $a \equiv r\ [n]$ et $0 \leqslant r < n$, alors r est le reste de la division euclidienne de a par n.

Exemple

$48 \equiv 3\ [5]$ parce que $48 - 3 = 45$ est multiple de 5, de plus $0 \leqslant 3 < 5$.

3 est bien le reste de la division euclidienne de 48 par 5 : $48 = 5 \times 9 + 3$

Démonstration

• Si r est le reste de la division euclidienne de a par n, alors $a = nq + r$, donc il existe un entier q tel que $a - r = nq$, de sorte que $a - r$ est multiple de n, par conséquent $a \equiv r\ [n]$.

• Si $a \equiv r\ [n]$ et $0 \leqslant r < n$, alors $a - r$ est multiple de n, donc il existe un entier k tel que $a - r = nk$ c'est à dire $a = nk + r$, et comme on sait que $0 \leqslant r < n$, on peut dire que r est le reste de la division euclidienne.

Propriété 1.8

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$,
- $a \equiv a\ [n]$;
- si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$;
- si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.

Démonstration

- Pour tout entier a, $a - a = 0$, et comme 0 est multiple de n, on a bien : $a \equiv a\ [n]$.
- Pour tous entiers a et b, $a - b$ est multiple de n équivaut à $b - a$ est multiple de n.
- Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a - b$ et $b - c$ sont multiples de n, donc $a - b + b - c$ est multiple de n, donc $a - c$ est multiple de n, c'est à dire $a \equiv c\ [n]$.

Propriété 1.9 (Congruence et division euclidienne)

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$,
$a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Exemple

$35 \equiv 11\ [4]$ parce que $35 - 11 = 24 = 4 \times 6$

35 et 11 ont le même reste dans la division euclidienne par 4, en effet $35 = 4 \times 8 + 3$ et $11 = 4 \times 2 + 3$.

Remarque

Dans d'autres cours la définition de congruence est la propriété 1.9, et la définition 1.4 est considérée comme une propriété. C'est le cas par exemple dans le manuel Hyperbole de TS spécialité. Il faut de toute façon bien connaître les deux.

Démonstration

• Pour deux nombres entiers a et b, si a et b ont le même reste dans la division euclidienne par n, alors on a les égalités $a = nq + r$ et $b = nq' + r$.

Donc : $a - b = (nq + r) - (nq' + r) = nq + \cancel{r} - nq' - \cancel{r} = n(q - q')$.

Donc $a - b$ est multiple de n, par conséquent $a \equiv b\ [n]$.

• Réciproquement, si $a \equiv b\ [n]$, écrivons les divisions euclidiennes de a et b par n :

$a = nq + r$ et $b = nq' + r'$, avec $0 \leqslant r < n$ et $0 \leqslant r' < n$, et démontrons que $r = r'$.

On a : $a - b = nq + r - (nq' + r') = nq + r - nq' - r' = n(q - q') + r - r'$

Or, sachant que $0 \leqslant r' < n$, on a donc $-n < -r' \leqslant 0$, et par conséquent $-n < r - r' < n$.

▷ Si $r - r' \geqslant 0$, on a alors $0 \leqslant r - r' < n$.

Donc $r - r'$ est le reste de la division euclidienne de $a - b$ par n.

Or $a \equiv b\ [n]$, si bien que $a - b$ est multiple de n, donc le reste de la division euclidienne de $a - b$ par n est égal à zéro.

Donc $r - r' = 0$, donc $r = r'$, ainsi a et b ont le même reste dans la division euclidienne par n.

▷ Si $r - r' \leqslant 0$, alors $r' - r \geqslant 0$ et on procède de la même façon que précédemment avec $b - a$ au lieu de $a - b$, et la conclusion est la même.

Propriété 1.10 (Congruence et opérations)

Pour deux nombres entiers a et b, pour un nombre entier naturel $n \geqslant 2$, et pour un nombre entier naturel p, si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors
(1) $a + c \equiv b + d\ [n]$ **(2)** $a - c \equiv b - d\ [n]$ **(3)** $a \times c \equiv b \times d\ [n]$ **(4)** $a^p \equiv b^p\ [n]$

Exemple

$17 \equiv 8\ [3]$ et $10 \equiv 4\ [3]$.

(1) $(17 + 10) - (8 + 4) = 15$ et 15 est multiple de 3 donc $17 + 10 \equiv 19 + 22\ [3]$

(2) $(17 - 10) - (8 - 4) = 3$ et 3 est multiple de 3 donc $17 - 10 \equiv 8 - 4\ [3]$

(3) $17 \times 10 - 8 \times 4 = 138$ et $138 = 3 \times 46$ est multiple de 3 donc $17 \times 10 \equiv 8 \times 4\ [3]$

(4) $17^3 - 8^3 = 4401$ et $4\,401 = 3 \times 1\,467$ donc $17^3 \equiv 8^3\ [3]$

Démonstration

Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a - b$ et $c - d$ sont multiples de n,
par conséquent, il existe des entiers k et k' tels que $a - b = kn$ et $c - d = k'n$,
donc : $a = b + kn$ et $c = d + k'n$.

On utilise alors ces deux égalités pour démontrer ci-dessous les propriétés (1), (2), (3).

(1) $a+c = b+kn+d+k'n = b+d+(k+k')n$ donc $(a+c)-(b+d) = (k+k')n$ donc $a+c \equiv b+d\ [n]$.

(2) $a - c = b + kn - (d + k'n) = b + kn - d - k'n = b - d + (k - k')n$

donc $(a - c) - (b - d) = (k - k')n$ donc $a - c \equiv b - d\ [n]$

(3) $a \times c = (b + kn) \times (d + k'n) = bd + kk'n + kdn + kk'n^2 = bd + n \times (kk' + kd + kk'n)$

donc $ac - bd = n \times (kk' + kd + kk'n)$, donc $ac - bd$ est multiple de n, donc $ac \equiv bd\ [n]$.

(4) On démontre cette égalité par récurrence sur p, en utilisant la propriété (3) pour l'hérédité.

1.3.b Exemple d'application

Utilisons tout ce que nous savons sur les congruences pour déterminer un reste dans une division euclidienne d'un grand nombre.

Énoncé : sans utiliser la calculatrice, déterminer le reste de la division euclidienne de $47\,000\,000\,000\,000\,000$ par 11.

Solution

$47\,000\,000\,000\,000\,000 = 47 \times 10^{15}$

Étudions les congruences de 47 et des puissances de dix modulo 11.

$47 = 11 \times 4 + 3$ donc $47 \equiv 3\ [11]$.

$10 \equiv -1\ [11]$ donc $10^2 \equiv (-1)^2 \equiv 1\ [11]$

$10^{14} = (10^2)^7 \equiv 1^7 \equiv 1\ [11]$

$10^{15} = 10^{14} \times 10 \equiv 1 \times 10 \equiv 10 \equiv -1\ [11]$

$47\,000\,000\,000\,000\,000 = 47 \times 10^{15} \equiv 3 \times (-1) \equiv -3 \equiv 8\ [11]$

Donc le reste de la division euclidienne de $47\,000\,000\,000\,000\,000$ par 11 est $\boxed{8}$.

1.4 Critères de divisibilité

Propriété 1.11

- Pour tout nombre divisible par 2, son chiffre des unités est 0 ou 2 ou 4 ou 6 ou 8.
- Pour tout nombre divisible par 3, sa somme des chiffres est un multiple de 3.
- Pour tout nombre divisible par 5, son chiffre des unités est 0 ou 5.

Chapitre 2

Introduction aux matrices

I Exercices

2.1 Un 1er exemple

Exercice 2.1 (Un problème à deux compartiments)

On conserve dans une enceinte une population de 500 000 bactéries qui ne peuvent se trouver que dans deux états :

- état A : reproduction par division cellulaire ;
- état B : quiescence (non reproduction).

On désigne par a_n et b_n les effectifs respectifs en milliers des bactéries dans l'état A ou dans l'état B, et on précise que $a_0 = 375$ et $b_0 = 125$.

Des observations menées sur une assez longue période permettent d'estimer que :

- 95 % des bactéries se trouvant à l'heure n dans l'état A n'ont pas changé d'état à l'heure $n+1$;
- 80 % des bactéries se trouvant à l'heure n dans l'état B n'ont pas changé d'état à l'heure $n+1$.

1. Calculer a_1 et b_1.

2. Justifier qu'on a le système :
$\begin{cases} a_{n+1} = 0,95\,a_n + 0,2\,b_n \\ b_{n+1} = 0,05\,a_n + 0,8\,b_n \end{cases}$

3. Dans un tableur, faire le calcul des effectifs a_n et b_n jusqu'à $n = 40$.

4. Quelles sont les formules à saisir dans les cellules B3 et C3, et à recopier vers le bas, pour obtenir les valeurs des termes des deux suites ?

5. D'après le tableau obtenu, quel semble être le comportement des suites (a_n) et (b_n) ?

	A	B	C
1	n	a_n	b_n
2	0	375	125
3	1		
4	2		

Exercice 2.2 (Utilisation de matrices)

Le système de l'exercice 2.1 s'écrit ainsi avec des matrices :

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} a_n \\ b_n \end{pmatrix}$$

1. On a donc : $\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$ c'est à dire $\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} 375 \\ 125 \end{pmatrix}$
Effectuer ce calcul de matrices à la calculatrice.

Il faut d'abord saisir la matrice $\begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix}$ dans A puis saisir la matrice $\begin{pmatrix} 375 \\ 125 \end{pmatrix}$ dans B.
Ensuite, on effectue le produit de matrices $A \times B$.
Pour l'utilisation de la calculatrice, voir le paragraphe 2.3 du cours.

2. Poursuivons les calculs au rang $n = 2$.
$\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} 0,95 & 0,2 \\ 0,05 & 0,8 \end{pmatrix} \times \begin{pmatrix} 375 \\ 125 \end{pmatrix}$
Effectuer ce calcul de matrices à la calculatrice, c'est à dire effectuer le produit de matrices $A \times A \times B$ ou encore $A^2 \times B$.

3. Retrouver par un calcul matriciel les effectifs à la dixième heure.

2.2 Entraînement sur les matrices

Exercice 2.3 (Produits de matrices pour s'entraîner)

On appelle A, B, C les matrices suivantes : $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ $B = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$ $C = \begin{pmatrix} 7 & 8 \end{pmatrix}$

1. En détaillant les calculs, calculer les matrices $A \times B$, $A \times A$, $C \times A$, pour cela lire les explications dans le cours, au paragraphe 2.2.c.

2. a) Parmi les calculs ci-dessous, certains ne peuvent pas être effectués. Pourquoi ?
$A \times C$, $B \times C$, B^2.

b) Vérifier aussi à la calculatrice.

Exercice 2.4 (Système et matrice)

1. Écrire le système suivant sous la forme d'une égalité avec des matrices : $\begin{cases} X = 5\,x + 3\,y \\ Y = 2\,x + 4\,y \end{cases}$

2. Écrire cette égalité sous la forme d'un sytème. $\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 2 & 1 & -3 \\ 5 & 0 & 4 \\ 6 & -2 & -1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

3. Comment choisir les coefficient a, b, c, d, de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ afin que pour tous réels x et y, on ait l'égalité : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix}$?

2.3 Exemples en gestion et en économie

Exercice 2.5 (Des tableaux de nombres pour la gestion)

Voici les productions (en milliers) de deux usines de cycles appartenant à une même enseigne pour le premier, puis le deuxième semestre de 2010.

	VTT adultes	Vélos enfants	VTC	BMX	Vélos de course
Usine 1	12,99	13,20	5,58	1,53	1,95
Usine 2	4,62	4,98	2,16	0,51	0,78

	VTT adultes	Vélos enfants	VTC	BMX	Vélos de course
Usine 1	11,79	15,84	4,38	1,29	1,59
Usine 2	3,78	4,14	2,40	0,51	0,66

1. Écrire ces deux tableaux sous forme de deux matrices respectives A et B.

2. Calculer la matrice : $C = \frac{1}{12}(A + B)$.

3. Que représente la matrice C ?

Exercice 2.6 (Indice de prix)

Une association de consommateurs compare les prix de cinq produits p_1, p_2, p_3, p_4, p_5 distincts dans trois magasins différents (prix à l'unité en euros). Le tableau ci-dessous indique ces prix dans trois magasins différents.

	Produit p_1	Produit p_2	Produit p_3	Produit p_4	Produit p_5
Magasin 1	1	5	2	3	4
Magasin 2	1,1	4,7	1,8	3,1	3,8
Magasin 3	0,9	5,1	1,9	3,2	4

Pour comparer la dépense d'une personne selon les magasins, on considère un « panier » indiquant les quantités respectives de produits p_1, p_2, p_3, p_4, p_5 : 2 ; 1 ; 3 ; 3 ; 2.

1. Écrire le tableau de prix sous la forme d'une matrice A.

2. Écrire les quantités du « panier » dans une matrice colonne Q.

3. Calculer le produit matriciel : $A \times Q = B$.

4. Que représente la matrice B ?

Exercice 2.7 (Gestion des entrées et sorties dans un hôpital)

Dans un service d'un hôpital, on estime que les patients admis peuvent être dans une des 4 situations suivantes : 1. Soins réguliers ; 2. Chirurgie ; 3. Soins intensifs ; 4. Sortie.

Le tableau ci-dessous indique les probabilités de passage d'une situation à l'autre dans un intervalle de 24 heures. Donnons deux exemples pour la compréhension du tableau :

- la probabilité qu'un patient en soins réguliers aille en chirurgie est 0,2 ;
- la probabilité qu'un patient en chirurgie aille en soins réguliers est 0,1.

↗	**Soins réguliers**	**Chirurgie**	**Soins intensifs**	**Sortie**
Soins réguliers	0,6	0,2	0	0,2
Chirurgie	0,1	0	0,8	0,1
Soins intensifs	0,5	0	0,33	0,17
Sortie	0	0	0	0

1. Un jour donné la répartition des patients est : Soins réguliers : 12 ; Chirurgie : 5 ; Soins intensifs : 6 ; Sortie : 3.

Calculer en détaillant le nombre de patients en soins réguliers le jour suivant.

2. Calculer le nombre de patients le jour suivant dans les trois autres situations : chirurgie, soins intensifs, sortie.

3. On appelle M la matrice correspondant à ce tableau.

Lequel des deux calculs matriciels suivants permettra de retrouver les résultats des calculs des questions **1.** et **2.** ?

- choisir $X = \begin{pmatrix} 12 \\ 5 \\ 6 \\ 3 \end{pmatrix}$ et calculer MX ;
- choisir $X = \begin{pmatrix} 12 & 5 & 6 & 3 \end{pmatrix}$ et calculer XM.

4. Supposons qu'au jour 0, dix patients soient admis en soins régulers, et qu'il n'y ait aucun patient dans les trois autres situations, et supposons également que 10 patients soient admis chaque jour, uniquement en soins réguliers. On appelle X_k la matrice des effectifs de patients le jour k.

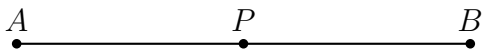
a) Écrire la matrice X_0.

b) Calculer les matrices X_1 et X_2.

2.4 Marches aléatoires sur un graphe

Exercice 2.8 (Marche aléatoire sur un segment)

Considérons un personnage fictif se déplaçant sur le segment $[AB]$ ci-dessous. Ce personnage ne peut se trouver qu'en A, P ou B. S'il est en A ou en B il ne peut aller qu'en P, s'il est en P, il peut aller en A ou en B avec la même probabilité. Il ne peut jamais rester en A, P ou B.



1. Compléter le tableau ci-dessous avec les probabilités de passage d'un point à un autre.

	vers A	vers P	vers B
De A			
De P			
De B			

2. On appelle M la matrice correspondant au tableau ci-dessus. Calculer la matrice M^2.

3. Calculer la probabilité d'aller de A en A en deux « pas ».

4. Justifier que cela revient à mutiplier terme à terme la première ligne de la matrice M avec sa première colonne.

5. On admet des résultats analogues pour la probabilité d'aller en deux « pas » d'un point à un autre. Que représentent alors les coefficients de la matrice M^2 ?

6. Calculer la matrice M^3. Que constate-t-on ?

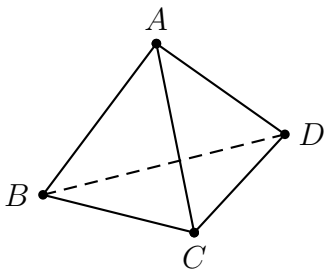
7. Que signifie ce résultat ?

8. Calculer les matrices M^4 et M^5.

9. Que signifient ces résultats ?

Exercice 2.9 (Marche aléatoire sur un tétraèdre)

Considérons un personnage fictif se déplaçant d'un sommet à un autre d'un tétraèdre $ABCD$. Dans un tétraèdre on peut aller de n'importe quel sommet vers n'importe lequel des trois autres sommets. On suppose que chacun de ces déplacements a la même probabilité. Il ne peut jamais rester sur un sommet.



1. Compléter le tableau ci-dessous avec les probabilités de passage d'un sommet à un autre.

	vers A	vers B	vers C	vers D
De A				
De B				
De C				
De D				

2. On appelle M la matrice correspondant au tableau ci-dessus. Calculer avec la calculatrice ou avec un logiciel les matrices M^2, M^4, M^{10}.

3. Conjecturer la limite de la matrice M^n lorsque n tend vers $+\infty$.

4. Que signifie cette limite ?

2.5 Transformations géométriques

Le programme de mathématiques de spécialité en terminale S fait utiliser les matrices pour étudier des suites de matrices lignes ou colonnes liées à des marches aléatoires sur des graphes.

Les matrices peuvent aussi être utilisées pour des transformations géométriques de figures, comme des symétries. Le but de l'exercice 2.10 est d'en étudier quelques exemples.

Exercice 2.10

Dans un repère orthonormé les coordonnées des points A, B, C, D, sont : $A(0\ ;\ 0)$ $B(0\ ;\ 2)$ $C(3\ ;\ 2)$ $D(3\ ;\ 0)$ et $ABCD$ est un rectangle.

La figure comportant le repère et le rectangle $ABCD$ est reproduite sur les figures 2.1, 2.2, 2.3, 2.4, 2.5, 2.6.

L'image d'un point M de coordonnées $(x\ ;\ y)$, par la transformation de matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est le point $M'(x'\ ;\ y')$ tel que : $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

1. Calculer les coordonnées des images A', B', C', D', des points A, B, C, D, par la transformation de matrice $T_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, puis tracer le quadrilatère $A'B'C'D'$ sur la figure 2.1.

2. Même consigne pour les transformations de matrices :
$T_2 = \begin{pmatrix} 2 & 0 \\ 0 & 0,5 \end{pmatrix}$ $T_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $T_4 = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$
en utilisant les autres figures.

3. Quelles sont les matrices respectives T_5 et T_6 de la symétrie par rapport à l'axe des abscisses et de la symétrie par rapport à l'origine du repère ? On pourra utiliser les figures 2.5 et 2.6 si nécessaire.

4. Compléter le tableau ci-dessous par oui ou non pour indiquer si chaque transformation conserve les distances, les angles, les aires. Certaines vérifications seront nécessaires.

	T_1	T_2	T_3	T_4	T_5	T_6
Conservation des distances ?						
Conservation des angles ?						
Conservation des aires ?						

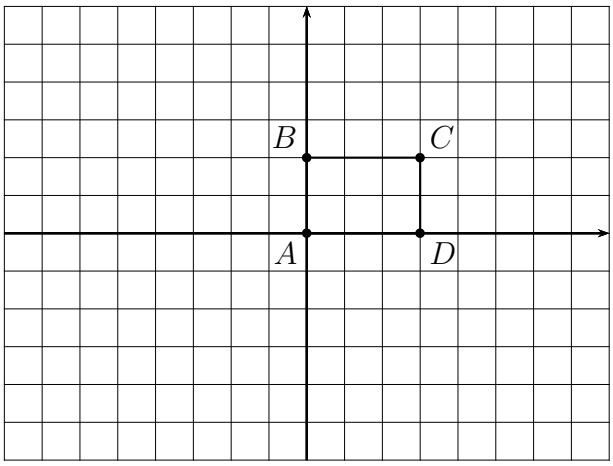


Fig. 2.1

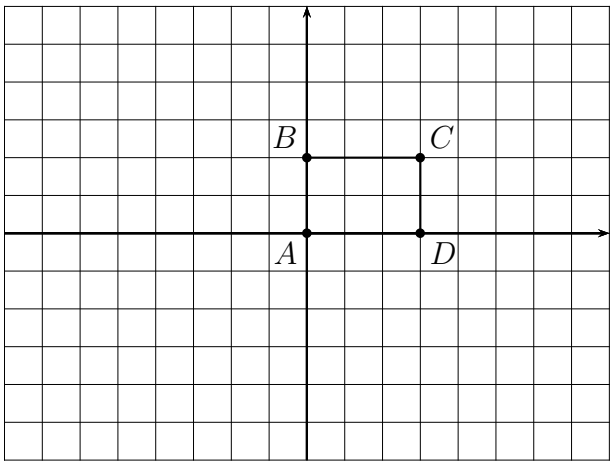


Fig. 2.2

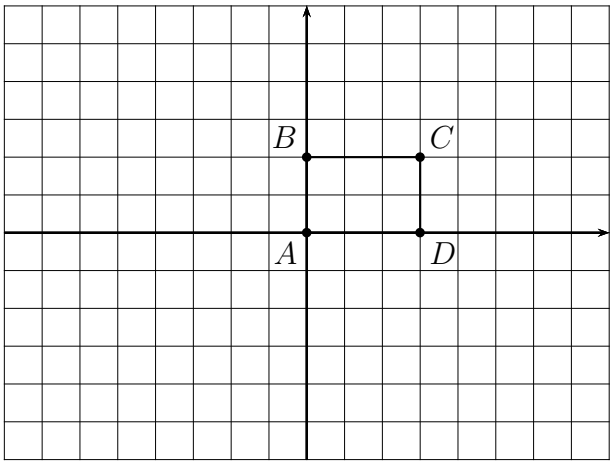


Fig. 2.3

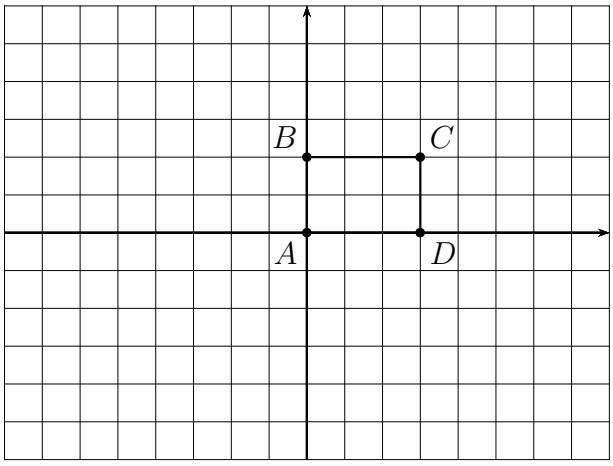


Fig. 2.4

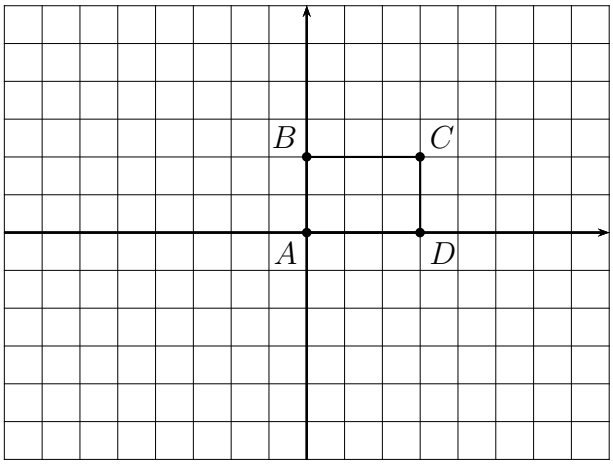


Fig. 2.5

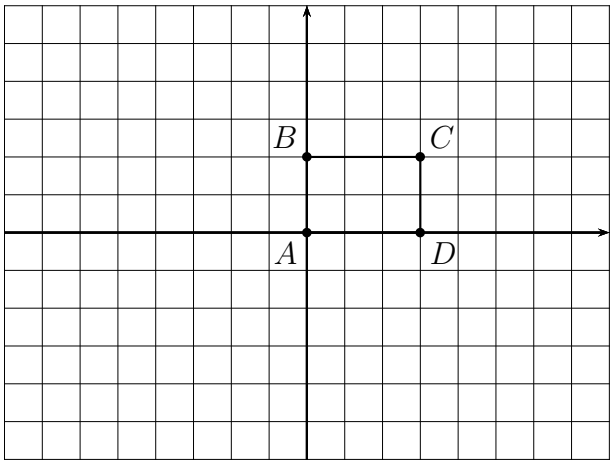


Fig. 2.6

II Cours

2.1 Définition de matrice

Définition 2.1 (Matrice de format $(m\ ;\ n)$)

Pour deux entiers naturels n et p, une matrice de format $(n\ ;\ p)$ est un tableau de nombres ayant n lignes et p colonnes.

Exemples et vocabulaire

$\begin{pmatrix}1 & -3\end{pmatrix}$: 1 ligne et 2 colonnes, on appelle cela une **matrice ligne**.

$\begin{pmatrix}-2\\4\end{pmatrix}$: 2 lignes et 1 colonne, on appelle cela une **matrice colonne**.

$\begin{pmatrix}1 & -5 & 0\\-7 & 4 & 6\end{pmatrix}$: 2 lignes et 3 colonnes.

$\begin{pmatrix}7 & -4\\5 & 0\end{pmatrix}$ $\begin{pmatrix}-1 & 0 & 3\\4 & 0 & 2\\0 & 1 & 5\end{pmatrix}$: même nombre de lignes et de colonnes, ce sont des **matrices carrées**.

Remarque

Le programme de terminale S prévoit d'étudier seulement les matrices lignes, les matrices colonnes et les matrices carrées.

2.2 Opérations sur les matrices

2.2.a Addition et soustraction

- On ne peut ajouter ou soustraire que deux matrices de même format $(n\ ;\ p)$.
- Pour ajouter deux matrices, on ajoute membre à membre les coefficients des deux matrices.
- Pour soustraire deux matrices, on soustrait membre à membre les coefficients des deux matrices.

Exemples pour l'addition

Matrices colonnes et ligne : $\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}x+x'\\y+y'\end{pmatrix}$ $\qquad \begin{pmatrix}s & t\end{pmatrix}+\begin{pmatrix}s' & t'\end{pmatrix}=\begin{pmatrix}s+s' & t+t'\end{pmatrix}$

Matrices carrées : $\begin{pmatrix}a & b\\c & d\end{pmatrix}+\begin{pmatrix}a' & b'\\c' & d'\end{pmatrix}=\begin{pmatrix}a+a' & b+b'\\c+c' & d+d'\end{pmatrix}$

2.2.b Multiplication par un réel

Matrices colonnes et ligne : $\lambda\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}\lambda x\\\lambda y\end{pmatrix}$ $\qquad \lambda\begin{pmatrix}s & t\end{pmatrix}=\begin{pmatrix}\lambda s & \lambda t\end{pmatrix}$

Matrices carrées : $\lambda\begin{pmatrix}a & b\\c & d\end{pmatrix}=\begin{pmatrix}\lambda a & \lambda b\\\lambda c & \lambda d\end{pmatrix}$

2.2.c Produit

Pour effectuer le produit de matrices $A\times B$, on les dispose ainsi : $\begin{array}{c|c} & B\\ \hline A & \end{array}$

Matrice carrée × matrice colonne :

	$\begin{pmatrix} x \\ y \end{pmatrix}$
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	$\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

Matrice ligne × matrice carrée :

	$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$
$\begin{pmatrix} s & t \end{pmatrix}$	$\begin{pmatrix} sa+ct & sb+td \end{pmatrix}$

Matrice carrée × matrice carrée :

	$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	$\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$

On obtient les trois formules ci-dessous qui ne sont pas à retenir.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

$$\begin{pmatrix} s & t \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} sa+ct & sb+td \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

2.2.d Puissances d'une matrice carrée

La définition est analogue à celle des puissances d'un nombre.

$A \times A = A^2$ $\quad$ $A \times A \times A = A^3$ $\quad$ etc.

Les calculs de puissances de matrices carrées seront souvent effectués à la calculatrice.

2.3 Utilisation des calculatrices

2.3.a Calculatrice TI 82

On accède aux matrices en appuyant sur matrice ou sur 2nde [matrice]

Saisir une matrice

Saisissons par exemple la matrice $D = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

- matrice ou 2nde [matrice]
- descendre sur `4: [D]`, ne pas appuyer sur entrer.
- aller sur `EDIT` : → →
- appuyer sur entrer
- compléter l'écran ainsi (appuyer sur entrer après chaque nombre) :

```
MATRICE [D] 2 × 3
[1     2     3    ]
[4     5     6    ]
```

Opération avec les matrices

Par exemple, pour calculer un produit $B \times C$:

- matrice ou 2nde [matrice]
- descendre sur [B], puis appuyer sur entrer
- on voit alors : [B]
- compléter avec un signe de multiplication : [B]*
- 2nde [matrice]
- descendre sur [C], puis appuyer sur entrer
- on voit : [B]*[C]
- appuyer sur entrer

Effacer une matrice

- 2nde [mém]
- aller sur 2:Gest Mem/Sup, puis entrer
- aller sur 5:Matrice..., puis
- aller sur la matrice choisie, puis entrer.

2.3.b Calculatrice CASIO

Saisir une matrice

Saisissons par exemple la matrice $D = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

- appuyer sur MENU, aller sur RUN-MAT, puis appuyer sur EXE
- appuyer sur F3 (▷MAT)
- descendre sur Mat D, appuyer sur EXE
- saisir les dimensions comme ci-dessous : appuyer sur 2, EXE, 3, EXE
  m :2
  n :3
- compléter l'écran ainsi (appuyer sur EXE après chaque nombre) :
  $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$

Opération avec les matrices

Par exemple, pour calculer un produit $B \times C$:

SHIFT [Mat] ALPHA [B] × SHIFT [Mat] ALPHA [C] EXE

2.3.c Calculatrice NUMWORKS

Saisir une matrice

Aller dans l'application Calculs

- appuyer sur shift e^x
- séparer les nombres avec les touches ←, →, ↑, ↓
- sortir de la matrice avec la touche →

2.4 Écriture matricielle d'un système linéaire

Propriété 2.1

Pour les nombres réels X, Y, x, y, a, b, c, d, on a l'équivalence :

$$\begin{cases} X = a\,x + b\,y \\ Y = c\,x + d\,y \end{cases} \iff \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix}$$

Chapitre 3

Nombres premiers entre eux

I Exercices

3.1 Chiffrement affine

Exercice 3.1

Le chiffrement affine est une méthode pour écrire un message codé.

- On associe un nombre x à chaque lettre de l'alphabet comme l'indique le tableau de la figure 3.1 ;
- on choisit deux entiers naturels a et b comme clef ;
- on détermine y tel que $ax + b \equiv y\ [26]$;
- enfin on associe une lettre à y d'après le tableau de la figure 3.1.

1. On choisit $a = 15$ et $b = 6$.

a) Coder le mot `MOT`.

b) Décoder le mot `KPO`.

2. On choisit $a = 21$ et $b = 4$. Améliorons le procédé de décodage.

a) Démontrer que $21x + 4 \equiv y\ [26] \iff x \equiv 5y + 6\ [26]$
Indication : déterminer d'abord le reste de la division euclidienne de 5×21 par 26.

b) Décoder le mot `UMPK`.

3. On choisit $a = 2$ et $b = 3$. Dans ce cas, on obtient un mauvais système de codage parce que deux lettres différentes peuvent être codées par la même lettre. Par exemple, déterminer les deux lettres dont le codage donne la lettre H.

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

Fig. 3.1

Remarques

L'exercice 3.1 est une première approche du chiffrement affine et nous y reviendrons ultérieurement.

La 3e question de cet exercice montre que pour certains choix de a et de b, on obtient un système de chiffrement non satisfaisant, mais alors, les deux choix précédents de a et de b donnent-ils des systèmes de chiffrement satisfaisants ? La réponse est oui, mais nous ne l'avons pas démontré, comme nous n'avons pas démontré pourquoi le système de chiffrement de la 3e question est incorrect.

Pour étudier la validité d'un système de chiffrement affine, nous devons d'abord revoir le PGCD et les nombres premiers entre eux, étudiés en troisième, puis étudier deux théorèmes importants en arithmétique : le théorème de Bézout et le théorème de Gauss.

3.2 PGCD

Exercice 3.2

1. Écrire la liste des diviseurs de 18, et la liste des diviseurs de 66.
2. Écrire la liste des diviseurs communs à 18 et à 66.
3. Quel est le PGCD de 18 et 66, c'est à dire leur plus grand diviseur commun ?
4. Écrire la liste des diviseurs du PGCD. Que constate-t-on ?
5. Retrouver le PGCD de 18 et 66 en effectuant l'algorithme d'Euclide. Pour se remémorer cet algorithme, on pourra lire l'exemple du paragraphe 3.1.a du cours.

Exercice 3.3

Déterminer chaque fois le PGCD des deux nombres indiqués en détaillant l'algorithme d'Euclide.

1. 204 et 84 **2.** 777 et 357 **3.** 69 696 et 9 339

3.3 PGCD et Identité de Bézout

Lire dans le cours la propriété 3.3 (Identité de Bézout), puis faire l'exercice ci-dessous.

Exercice 3.4

Le PGCD de 10 et 6 est 2. D'après l'identité de Bézout, il existe deux entiers u et v tels que $10 \times u + 6 \times v = 2$. Déterminer deux nombres u et v qui vérifient cette égalité.

Exercice 3.5

1. Vérifier l'égalité $10 \times 3 + 7 \times (-4) = 2$.
2. Le PGCD de 10 et 7 est-il égal à 2 ?
3. Que signifie cet exemple pour la propriété 3.3 du cours (Identité de Bézout) ?

Exercice 3.6

Le PGCD de 306 et 90 est 18, et l'algorithme d'Euclide est détaillé ci-dessous.

$$\begin{array}{rcrcrcl} 306 & = & 90 & \times & 3 & + & 36 \quad (1) \\ 90 & = & 36 & \times & 2 & + & 18 \quad (2) \\ 36 & = & 18 & \times & 2 & + & 0 \quad (3) \end{array}$$

On peut déterminer u et v tels que $306\,u + 90\,v = 18$ à l'aide de l'algorithme d'Euclide.

1. D'après la ligne (2), écrire 18 comme combinaison linéaire de 54 et de 36 :

   $18 =$ .....
2. D'après la ligne (1), écrire 36 comme combinaison linéaire de 198 et 54 :

   $36 =$ .....
3. Dans la combinaison linéaire du **1.** ci-dessus, remplacer 36 par la combinaison linéaire du **2.** ci-dessus.

   $18 =$ .....

   $18 =$ .....

   $18 =$ .....

Exercice 3.7

1. Déterminer d le PGCD de 240 et 56 avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $128\,u + 56\,v = d$.

Exercice 3.8

1. Déterminer d le PGCD de 532 et 434 avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $532\,u + 434\,v = d$.

Exercice 3.9

Dans chaque cas, déterminer une solution de l'équation.

1. $6x \equiv 2\ [8]$ **2.** $15x \equiv 5\ [35]$ **3.** $30x \equiv 10\ [50]$

3.4 Nombres premiers entre eux

3.4.a Théorème de Bézout

Lire dans le cours la définition 3.3. (Nombres premiers entre eux) et la propriété 3.8 (Théorème de Bézout) puis faire l'exercice ci-dessous.

Exercice 3.10

1. Justifier que les nombres 131 et 21 sont premiers entre eux avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $131\,u + 21\,v = 1$.

Exercice 3.11

1. Calculer $5 \times 45 - 16 \times 14$.
2. En déduire 4 paires de nombres premiers entre eux.

3.4.b Théorème de Gauss

Exercice 3.12

1. Déterminer un entier non nul x tel que 6 divise $15x$ et 6 ne divise pas x.
2. Déterminer un entier non nul x tel que 6 divise $11x$ et 6 ne divise pas x.
3. Un des deux problèmes ci-dessus n'a pas de solution. L'explication est donnée par la propriété 3.9 (théorème de Gauss).

3.4.c Équations diophantiennes

Les couples solutions $(x\ ;\ y)$ des équations qui suivent doivent être des couples de nombres entiers.

Exercice 3.13

1. Sans justifier, indiquer si les entiers 7 et 10 sont premiers entre eux.
2. Résoudre l'équation $7x = 10y$, c'est à dire déterminer tous les couples d'entiers $(x\ ;\ y)$ solutions de cette équation.

Exercice 3.14

Résoudre l'équation $7(x-1) = 10(y+2)$, c'est à dire déterminer tous les couples d'entiers $(x\ ;\ y)$ solutions de cette équation.

Exercice 3.15

1. Justifier pourquoi l'équation $7x + 10y = 1$ a des solutions.
2. Résoudre l'équation $7x + 10y = 1$.
   Indications :
   - Déterminer un couple solution $(x_0\ ;\ y_0)$ de cette équation.
   - Justifier qu'on peut alors écrire l'équation de départ sous la forme $7(x-x_0)+10(y-y_0) = 0$, puis sous la forme $7(x-x_0) = -10(y-y_0)$.
   - Achever la résolution de l'équation.

Exercice 3.16

Résoudre les équations diophantiennes ci-dessous.

1. $8x - 5y = 1$ **2.** $3x + 11y = 1$ **3.** $9x - 7y = 1$

Exercice 3.17

1. Donner sans justifier le PGCD de 6 et de 9.
2. L'équation $6x + 9y = 1$ a-t-elle des solutions ? Justifier.

Exercice 3.18

Le but de cet exercice est de résoudre l'équation diophantienne $11x - 8y = 7$.

1. Déterminer un couple $(u\ ;\ v)$ solution de l'équation $11u - 8v = 1$.
2. En déduire un couple $(x\ ;\ y)$ solution de $11x - 8y = 7$.
3. Résoudre l'équation $11x - 8y = 7$.

Exercice 3.19

Résoudre les équations diophantiennes ci-dessous.

1. $10x - 3y = 4$ **2.** $13x + 6y = 5$

3.4.d Conséquence du théorème de Gauss

Exercice 3.20

1. Déterminer un entier non nul x tel que 4 et 10 divisent x et 4×10 ne divise pas x.
2. Déterminer un entier non nul x tel que 4 et 7 divisent x et 4×7 ne divise pas x.
3. Un des deux problèmes ci-dessus n'a pas de solution. L'explication est donnée par la propriété 3.10 (conséquence du théorème de Gauss).

Exercice 3.21

1. Si 6 et 15 divisent un même nombre entier n, peut-on dire qu'alors 6×15 divise n. Justifier.
2. Si 8 et 15 divisent un même nombre entier n, peut-on dire qu'alors 8×15 divise n. Justifier.

Exercice 3.22

Démontrer que pour tout entier naturel n, le nombre $3n(n+1)$ est mutiple de 6.

3.5 Chiffrement affine (2)

Exercice 3.23

Le chiffrement affine a été décrit et étudié dans l'exercice 3.1. Un cas a été étudié où deux lettres différentes étaient codées par la même lettre, ce qui pose problème.

On rappelle qu'on associe un nombre x entre 0 et 25 à une lettre, puis on lui associe un autre nombre y entre 0 et 25 tel que $ax + b \equiv y\ [26]$ et on associe une lettre à y.

Comment choisir a et b pour que deux lettres associées à x_1 et x_2 soient codées par deux lettres différentes associées à y_1 et y_2 ?

Nous allons raisonner par la contraposée, en prouvant que si $y_1 \equiv y_2\ [26]$ et si a est un nombre premier avec 26, alors $x_1 \equiv x_2\ [26]$.

On a donc $\begin{cases} ax_1 + b \equiv y_1\ [26] \\ ax_2 + b \equiv y_2\ [26] \end{cases}$ et $y_1 \equiv y_2\ [26]$ et on suppose que a et 26 sont premiers entre eux.

1. Démontrer qu'il existe un entier k tel que $a(x_1 - x_2) = 26k$.
2. Que peut-on en déduire pour a et k ?
3. En déduire qu'il existe un entier k' tel que $x_2 - x_1 = 26k'$.
4. Que peut-on en déduire pour x_1 et x_2 ?

Exercice 3.24

En français les deux lettres les plus fréquentes sont le E (17,8 %) et le S (8,2 %).
Cela permet de décrypter un chiffrement affine, en effet, dans un chiffrement affine défini par une égalité $ax + b \equiv y\ [26]$, où a est premier avec 26, chaque lettre est codée par une lettre unique et on peut ainsi déterminer par quelles lettres sont codées le E et le S.

Un message est codé par un chiffrement affine tel que a est premier avec 26, et on remarque que les lettres D et X apparaissent avec des fréquences respectives proches de 17,8 % et 8,2 %, on suppose donc que E et S sont codés D et X.

Déterminer a et b d'après ces informations.

Indications :

- écrire un système d'équations d'inconnues a et b modulo 26 ;
- en déduire qu'il existe un entier k tel que $7a - 13k = 10$;
- résoudre cette équation et justifier qu'une seule valeur de a est possible entre 0 et 25 ;
- déterminer b.

3.6 Chiffrement de Vigenère

L'exercice 3.24 montre comment, s'il on connaît le codage de deux lettres, on peut décrypter une message codé par un chiffrage affine. Cela est dû au fait qu'avec un chiffrage affine, une lettre donnée, comme le E, est toujours codée par la même lettre qui est alors repérée dans le message codé par sa fréquence d'apparition.

Étudions maintenant le chiffrement, de Vigenère, qui évite qu'une lettre donnée soit toujours codée par la même lettre, sans que cela pose de problème de décodage.

Exercice 3.25

Le chiffrement de Vigenère utilise une clef de codage sous la forme d'un mot. Utilisons par exemple le mot `CLE` pour coder le mot `SUITE`, puis on répète la clef de codage autant de fois qu'il faut sous le message comme on le voit dans le tableau ci-dessous.

On associe un nombre entre 0 et 25 à chaque lettre (le tableau de correspondance est rappelé plus bas) : pour `S` $\rightarrow x = 18$ et pour `C` $\rightarrow y = 2$.

On calcule la somme modulo 26 : $x + y = 18 + 2 \equiv 20\ [26]$ et 20 correspond à `U`.

Lettre non codée	S	U	I	T	E	S
Lettre de la clef de codage	C	L	E	C	L	E
x	18					
y	2					
$x + y \equiv z[26]$	20					
Lettre codée	U					

1. Finir de coder le mot `SUITE`.
2. Décoder le mot codé : `DLG`

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

Remarque

- Le codage du mot `SUITES` dans l'exercice 3.25 montre bien que le premier et le deuxième `S` ne sont pas codés par la même lettre, ce qui empêche le décryptage par l'étude de la fréquence des lettres du message codé.
- Malgré cela, vers 1854, le mathématicien britannique Charles Babbage a trouvé une méthode de décryptage du chiffrement de Vigenère.

3.7 Chiffrement de Hill

Exercice 3.26

Le chiffrement de Hill s'effectue de la manière suivante.

- On groupe les lettres du message deux par deux
- On associe un nombre entre 0 et 26 à chaque lettre, et on obtient ainsi des couples de nombres $(x_1\ ;\ x_2)$
- On associe en suite ce couple $(x_1\ ;\ x_2)$ à un couple $(y_1\ ;\ y_2)$ de la manière suivante :
  $\begin{cases} ax_1 + bx_2 \equiv y_1\ [26] \\ cx_1 + dx_2 \equiv y_2\ [26] \end{cases}$

1. **Procédure de codage**

   Un chiffrement de Hill est effectué d'après le système ci-dessous.
   $\begin{cases} 3x_1 + 4x_2 \equiv y_1\ [26] \\ 2x_1 + 3x_2 \equiv y_2\ [26] \end{cases}$

   On veut coder le mot MATH.

   a) Associer un couple $(x_1\ ;\ x_2)$ aux lettres M-A

   b) Calculer un couple $(y_1\ ;\ y_2)$ d'après le système ci-dessus.

   c) Associer deux lettres au couple $(y_1\ ;\ y_2)$

   d) Procéder de la même façon pour T-H.

   e) Donner le codage du mot MATH.

2. **Procédure de décodage**

   Le codage consistait à calculer $(y_1\ ;\ y_2)$ d'après $(x_1\ ;\ x_2)$, le décodage consiste à calculer $(x_1\ ;\ x_2)$ d'après $(y_1\ ;\ y_2)$.

a) D'après le système donné au **1.**, écrire x_1 en fonction de y_1 et y_2, puis x_2 en fonction de y_1 et y_2. Pour cela, faire une combinaison linéaire qui élimine x_2, et une autre qui élimine x_1. On obtient ainsi un nouveau système

$$\begin{cases} x_1 \equiv py_1 + qy_2 \ [26] \\ x_2 \equiv ry_1 + sy_2 \ [26] \end{cases}$$

b) Utiliser ce système pour décoder Z-C

Exercice 3.27

x et y sont deux entiers qui vérifient l'égalité : $3x \equiv y \ [10]$. Écrire x en fonction de y.

Indication : déterminer un entier a tel que $3a \equiv 1 \ [10]$, puis multiplier les deux membres de l'égalité précédente par a.

Exercice 3.28

Pour chaque égalité ci-dessous, écrire x en fonction de y.

1. $8x \equiv y \ [15]$ **2.** $6x \equiv y \ [11]$ **3.** $9x \equiv y \ [26]$ **4.** $5x \equiv y \ [26]$

Exercice 3.29

Un chiffrement de Hill est effectué d'après le système ci-dessous.

$$\begin{cases} 2x_1 + 5x_2 \equiv y_1 \ [26] \\ x_1 + 4x_2 \equiv y_2 \ [26] \end{cases}$$

1. **Procédure de codage :** coder les lettres O-K.
2. **Procédure de décodage**

a) À partir du système précédent, justifier qu'on obtient le système ci-dessous.

$$\begin{cases} 3x_1 \equiv 4y_1 - 5y_2 \ [26] \\ 3x_2 \equiv -y_1 + 2y_2 \ [26] \end{cases}$$

b) Justifier ensuite qu'on obtient le système ci-dessous.

$$\begin{cases} x_1 \equiv 10y_1 + 7y_2 \ [26] \\ x_2 \equiv 17y_1 + 18y_2 \ [26] \end{cases}$$

c) Utiliser ce système pour décoder A-B.

3.8 Pour réviser

Chapitre du livre n° 2 – Théorème de Bézout, Théorème de Gauss, page 35

Les exercices résolus

- ex 1 p 41 : PGCD, algorithme d'Euclide, combinaison linéaire des deux nombres égale au PGCD
- ex 2 p 41 : démontrer que $2n + 1$ et $3n + 2$ sont premiers entre eux
- ex 9 p 47 : divisibilité d'une expression par 6
- ex 10 p 47 : équation diophantienne $(ax + by = c)$

Rubrique *Pour s'exercer*, corrigés page 156-157

- ex 3 p 41 : PGCD, algorithme d'Euclide, combinaison linéaire des deux nombres égale au PGCD.
- ex 7 p 41 : démontrer que deux expressions en fonction de n sont premiers entre eux
- ex 11 p 47 : divisibilité d'une expression par 6
- ex 15 p 47 : équation diophantienne $(ax + by = c)$

Rubrique *Objectif bac*, corrigés page 158

- ex 74 p 54 : QCM
- ex 75 p 54 : Vrai-Faux
- ex 76 p 54 : Vrai-Faux
- ex 77 p 55 : exercice de type bac, système de congruences

II Cours

3.1 PGCD

3.1.a Exemple

Étudions les diviseurs commun à 12 et à 20.

Liste des diviseurs de 12 :

$12 = 1 \times 12 = 2 \times 6 = 3 \times 4$

$\{-12\ ;\ -6\ ;\ -4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 12\}$

Liste des diviseurs de 20 :

$12 = 1 \times 20 = 2 \times 10 = 4 \times 5$

$\{-20\ ;\ -10\ ;\ -5\ ;\ -4\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 4\ ;\ 5\ ;\ 10\ ;\ 20\}$

Liste des diviseurs communs à 12 et à 20 :

$\{-4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\}$

Le PGCD de 12 et 20 est 4.

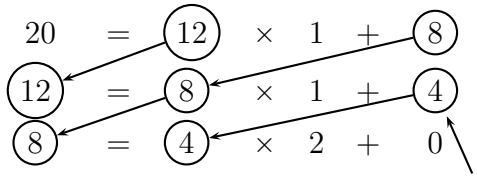
Écrivons maintenant la liste des diviseurs de 4 :

$4 = 1 \times 4 = 2 \times 2$

$\{-4\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 4\}$

Il s'avère donc que la liste des diviseurs communs à 12 et à 20 est la liste des diviseurs de leur PGCD.

On peut aussi obtenir le PGCD à l'aide de l'algorithme d'Euclide.



On effectue la division euclidienne de 20 par 12.

On recommence avec le dernier diviseur par le dernier reste.

Le PGCD est le dernier reste non nul dans l'algorithme d'Euclide, et on retrouve bien le nombre 4.

3.1.b Définition et propriété

Un nombre entier a un ensemble de diviseurs qui contient au moins 1 et lui même.

Deux nombres entiers non nuls a et b ont donc un ensemble de diviseurs communs qui contient au moins 1.

Définition 3.1

Pour deux nombres entiers non nuls a et b, on note PGCD le plus grand diviseur commun à ces deux nombres a et b.

Remarque

On dit « Plus Grand Diviseur Commun », on pourrait donc écrire PGDC au lieu de PGCD. Peut être s'agit-il d'un anglicisme, puisqu'en anglais le PGCD est appelé *Greatest Common Divisor* et se note GCD. Il se pourrait aussi que cela vienne de l'ancien français où l'on plaçait l'adjectif avant le nom, comme en anglais.

Propriété 3.1

Le PGCD de deux nombre est strictement positif.

Démonstration

L'ensemble des diviseurs communs contient des nombres strictement négatifs et des nombres strictement positif donc le plus grand d'entre eux est strictemnt positif.

Propriété 3.2 (PGCD d'un nombre et un de ses diviseurs)

Pour deux nombres entiers non nuls a et b tels que b divise a, le PGCD de a et b est b si b est positif et $-b$ si b est négatif.

Démonstration

Appelons d le PGCD de a et b.

Si b divise a, alors b et $-b$ font partie des diviseurs communs à a et à b, puisque b divise a et lui même, donc $b \leqslant d$ et $-b \leqslant d$, or le PGCD de a et b divise a et b donc d divise b et $-b$.

Si $b > 0$, alors d divise b implique que $d \leqslant b$, or $b \leqslant d$, donc $b = d$.

Si $b < 0$ alors d divise $-b$ implique que $d \leqslant -b$, or $-b \leqslant d$, donc $-b = d$, donc $d = -b$.

Propriété 3.3 (Identité de Bézout)

Si d est le PGCD de deux nombres entiers non nuls a et b, il existe des entiers u et v tels que $d = au + bv$.

Propriété 3.4

Si d est le PGCD de deux nombres entiers non nuls a et b, l'ensemble des diviseurs commun à a et à b est l'ensemble des diviseurs de d.

Remarque

La réciproque de l'identité de Bézout est fausse, par exemple $2 \times 7 + (-4) \times 3 = 2$ et pourtant le nombre 2 n'est pas le PGCD de 7 et 3, puisque 7 et 3 sont impairs.

Démonstration de ces deux propriétés.

On appelle E l'ensemble des combinaisons linéaires de a et b à coefficients entiers, c'est à dire l'ensemble des nombres de la forme $ua + vb$ où u et v sont des entiers.

- **Étudions d'abord cet ensemble E.**
  Remarquons d'abord que E est un ensemble d'entiers puisque si a, b, u, v sont des entiers $ua + vb$ est un entier.
  On peut remarquer aussi que cet ensemble contient a et b et zéro, puisque : $a = 1a + 0b$ et $b = 0a + 1b$ et $a = 1a + 0b$ et $0 = 0a + 0b$, et qu'il n'est donc pas vide.
  Cet ensemble E contient aussi des entiers naturels strictement positifs. C'est bien sûr le cas si a ou b est strictement positif, mais, même si a et b sont strictement négatifs, E contient $-a$ qui est strictement positif.
  L'ensemble des entiers naturels strictement positifs de E admet un plus petit élément qu'on appelle d'.

- **Démontrons que $d' = d$, c'est à dire que ce nombre d' est le PGCD de a et b.**
  Puisque d' appartient à E, il existe des entiers u' et v' tels que $u'a + v'b = d'$.
  Or, d'après la propriété 3.3 tout diviseur commun à a et à b divise toute combinaison linéaire de a et b.
  Donc, en particulier d, le PGCD, divise d', donc $d \leqslant d'$ puisque d et d' sont strictement positifs.

  Démontrons que d' est un diviseur commun à a et à b.
  Écrivons d'abord la division euclidienne de a par d' : $a = d'q + r$ et $0 \leqslant r < d'$.

On a donc : $r = a - d'q = a - (u'a + v'b) \times q = a - qu'a - qv'b = (1 - qu')a - qv'b$
c'est à dire que r est une combinaison linéaire de a et b.
Donc $r \in$ E, or $r \geqslant 0$, mais comme $r < d$ et d' est le plus petit élément de E, il est impossible d'avoir $0 < r < d'$, donc $r = 0$ et d' est un diviseur de a.
On démontre de même que d' est un diviseur de b.
Donc d' est un diviseur commun à a et à b, donc $d' \leqslant d$.

Donc $d = d' = u'a + v'b$, ce qui démontre la propriété 3.3.

- **Démontrons la propriété 3.4**
  Nous avons mentionné plus haut que tout diviseur commun à a et à b est un diviseur de d le PGCD de a et b, mais la réciproque est vraie, en effet, si un nombre entier est un diviseur de d qui est lui même un diviseur de a et b, ce nombre est un diviseur commun à a et à b.
  Nous venons donc aussi de prouver que l'ensemble des diviseurs commun à a et à b est l'ensemble des diviseurs de d, leur PGCD.

3.1.c L'algorithme d'Euclide

Propriété 3.5

Pour deux nombres entiers naturels non nuls a et b tels que $a > b$ et b ne divise pas a si r est le reste de la division euclidienne de a par b, alors PGCD$(a\ ;\ b)$ = PGCD$(b\ ;\ r)$

Remarque

Pour deux nombres entiers naturels non nuls a et b, la propriété 3.5 ci-dessus concerne le cas où $a > b$ et b ne divise pas a. Rappelons que d'après la propriété 3.2, si b divise a, alors leur PGCD est b.

Démonstration

$a = bq + r$ or le PGCD de b et r divise b et r donc d'après l'égalité précédente il divise a, ainsi le PGCD de b et r divise a et b, donc le PGCD de b et r divise le PGCD de a et b.

Réciproquement, $a = bq + r \iff r = a - bq$ or le PGCD de a et b divise a et b, donc d'après l'égalité précédente il divise r, ainsi le PGCD de a et b divise b et r, donc le PGCD de a et b divise le PGCD de b et r.

Par conséquent les deux PGCD sont égaux, puisqu'ils sont strictement positifs.

Définition 3.2 (Algorithme d'Euclide)

L'algorithme d'Euclide pour deux nombres entiers naturels non nuls a et b tels que $a > b$ et b ne divise pas a est décrit ci-dessous.

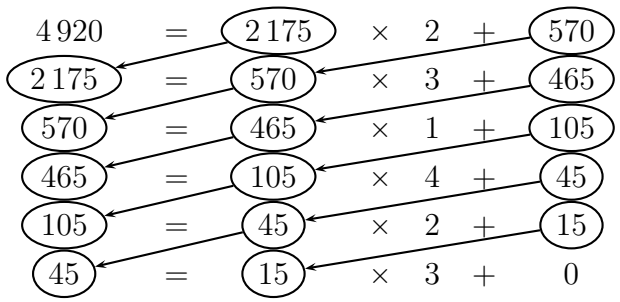
- **Entrées :** les nombres entiers a et b.
- **Initialisation :** on effectue la division euclidienne de a par b.
- À chaque étape suivante, on effectue la division euclidienne du dernier diviseur par le dernier reste, tant que le reste n'est pas nul.
- **Sortie :** le dernier reste non nul.

Propriété 3.6

Pour deux nombres entiers naturels non nuls, le dernier reste non nul de l'algorithme d'Euclide est le PGCD de ces deux nombres.

Exemple

Appliquons l'algorithme d'Euclide aux nombres 4 920 et 2 175.



On effectue la division euclidienne de 4 920 par 2 175
À chaque étape suivante, on effectue la division euclidienne du dernier diviseur par le dernier reste.

Le dernier reste non nul est le PGCD des 2 nombres.

Donc le PGCD de 4 920 et 2 175 est $\boxed{15}$.

Justifions cela d'après les calculs ci-dessus et à l'aide de la propriété 3.5.

$\text{PGCD}(4\,920\,;\,2\,175) = \text{PGCD}(2\,175\,;\,570) = \text{PGCD}(570\,;\,465) = \text{PGCD}(465\,;\,105) = \text{PGCD}(105\,;\,45) = \text{PGCD}(45\,;\,15)$

or 45 est multiple de 15, donc le PGCD de 45 et 15 est 15, donc 15 est bien le PGCD de 4 920 et 2 175.

3.1.d Obtenir le PGCD avec la calculatrice

Exemple : le PGCD de 6 et 8 est 2.

Avec la TI 82

math → (NUM), descendre jusqu'à `pgcd`, puis compléter ainsi : `pgcd(6,8)` et appuyer sur entrer.

Avec la CASIO

MENU choisir RUN-MAT OPTN F6 (→) F4 (NUM) F6 (→) F2 (GCD)
puis compléter ainsi : `GCD(6,8)` et appuyer sur EXE.

3.1.e Méthode : comment déterminer le PGCD de deux entiers ?

- On peut, comme dans l'exemple du paragraphe 3.1.a, écrire les listes des diviseurs des deux nombres, puis écrire la liste de leurs diviseurs communs, et le PGCD est alors le plus grand nombre de cette liste.
  Cette méthode ne peut être utilisée que pour des petits nombres.
- On peut aussi utiliser l'algorithme d'Euclide : voir paragraphe 3.1.c.
- Si l'énoncé ne demande ni justification ni calcul, on peut utiliser la calculatrice : voir paragraphe 3.1.d.
- On peut enfin utiliser la décomposition d'un entier en produit de puissances de nombres premiers, ce qui sera étudié au chapitre 5 *Nombres premiers*.

3.2 Nombres premiers entre eux

3.2.a Définition et propriété

Définition 3.3

Dire que deux nombres entiers non nuls a et b sont premiers entre eux signifie que leur PGCD est 1.

Exemple

35 et 6 sont premiers entre eux, puisque leur PGCD est 1, d'après l'algorithme d'Euclide ci-dessous.

$35 = 6 \times 5 + 5$
$6 = 5 \times 1 + 1$
$5 = 1 \times 5 + 0$

Propriété 3.7

Lorsque deux nombres entiers non nuls a et b sont premiers entre eux, les nombres a et $-b$, $-a$ et b, $-a$ et $-b$, sont aussi premiers entre eux.

3.2.b Théorème de Bézout

Propriété 3.8 (Théorème de Bézout)

Deux nombres entiers non nuls a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $au + bv = 1$

Démonstration

D'après la propriété 3.3, si d est le PGCD de deux nombres entiers non nuls a et b, il existe des entiers u et v tels que $d = au + bv$, et comme ici nous avons $d = 1$, nous pouvons affirmer qu'il existe des entiers u et v tels que $au + bv = 1$.

Réciproquement, s'il existe des entiers u et v tels que $au + bv = 1$, alors le PGCD de a et b divise aussi 1, donc le PGCD de a et b est égal à 1.

3.2.c Théorème de Gauss et conséquence

Propriété 3.9 (Théorème de Gauss)

Pour trois nombres entiers a, b, et c,
si a et b sont premiers entre eux et si a divise bc,
alors a divise c.

Démonstration

Considérons trois nombres entiers a, b, et c, tels que a et b sont premiers entre eux et tels que a divise bc.

Puisque a et b sont premiers entre eux, il existe des entiers u et v tels que $au + bv = 1$.

$au + bv = 1 \Rightarrow (au + bv)c = c \Rightarrow auc + bvc = c$

or a divise bc donc il existe un entier k tel que $bc = ka$.

Donc : $auc + vbc = c \Rightarrow auc + vka = c \Rightarrow a(uc + vk) = c$

Donc a divise c.

Propriété 3.10 (Conséquence du théorème de Gauss)

Pour trois nombres entiers a, b, et c,
si b et c sont premiers entre eux et si b et c divisent a,
alors bc divise a.

Démonstration

Puisque b divise a, il existe un entier k tel que $a = bk$.

Or, c divise aussi a, autrement dit c divise bk, or c est premier avec b, donc d'après le théorème de Gauss, c divise k.

Par conséquent il existe un entier k' tel que $k = ck'$.

On a donc : $a = bck'$, donc bc divise a.

Chapitre 4

Matrices carrées et systèmes

I Exercices

4.1 Propriétés du produit des matrices carrées

4.1.a Commutativité

L'addition et la multiplication des nombres sont commutatives c'est à dire que pour tous nombres réels a et b, $a+b=b+a$ et $a\times b=b\times a$.

Pour les matrices l'addition des matrices est commutative c'est à dire que pour toutes matrices A et B de même format, $A+B=B+A$.

Qu'en est-il pour la multiplication des matrices carrées ?

Exercice 4.1 (Le produit de matrices carrées est-il commutatif ?)

On considère les matrices $A=\begin{pmatrix}3&1\\0&4\end{pmatrix}$ et $B=\begin{pmatrix}2&5\\1&0\end{pmatrix}$

1. Vérifier si les produits $A\times B$ et $B\times A$ sont égaux ou pas. Détailler les calculs.
2. Le produit de matrices carrées est-il commutatif ?

4.1.b Autres propriétés du produit

Exercice 4.2 (Associativité)

Sans calculatrice, calculer $(A\times B)\times C$ et $A\times(B\times C)$ avec les matrices A, B, C ci-dessous.

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

Exercice 4.3 (Particularités de produits de matrices)

On considère les matrices : $A=\begin{pmatrix}1&2\\3&6\end{pmatrix}$ $\quad B=\begin{pmatrix}2&-4\\-1&2\end{pmatrix}$ $\quad C=\begin{pmatrix}2&1\\3&0\end{pmatrix}$ $\quad D=\begin{pmatrix}6&3\\1&-1\end{pmatrix}$

1. Calculer sans détailler les produits : $A\times B$, $A\times C$, $A\times D$. On peut utiliser la calculatrice.
2. **a)** Que constate-t-on pour $A\times B$.
   b) Peut-on avoir une telle situation pour deux nombres a et b ?
3. **a)** Que constate-t-on pour $A\times C$ et $A\times D$?
   b) Peut-on avoir une telle situation pour trois nombres a, c, d ?

Exercice 4.4 (Particularités de puissances de matrices)

On considère les matrices : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

1. **a)** Calculer A^2 à la calculatrice.
   b) Déterminer A^n pour $n \geqslant 3$.
2. **a)** Calculer B^5 à la calculatrice.
   b) Que peut-on en déduire pour B^6 ?

4.2 Matrice identité

Exercice 4.5

On considère les matrices : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $X = \begin{pmatrix} x \\ y \end{pmatrix}$

1. Effectuer les calculs suivants $I \times A$, $A \times I$, $I \times X$.
2. Que constate-t-on ?

4.3 Distributivité

Exercice 4.6

On considère les matrices : $A = \begin{pmatrix} 5 & 3 \\ 1 & 8 \end{pmatrix}$ $N = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$ $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et la matrice $B = I + N$.

1. Calculer à la calculatrice AN et N^2.
2. Sans calculatrice, calculer $A \times B$ en développant $A \times (I + N)$.
3. Sans calculatrice, calculer B^2 en développant $(I + N)^2$.

Exercice 4.7

On considère les matrices : $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ $E = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 4 & 0 & 0 \end{pmatrix}$ et la matrice $F = D + E$.

1. Calculer les matrices D^2, E^2, $D \times E$, $E \times D$.
2. Sans calculatrice, calculer la matrice F^2 en développant $(D + E)^2$.

Exercice 4.8

A est la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

1. **a)** Calculer en détaillant les matrices A^2 et A^3.
   b) Conjecturer l'expression de la matrice A^n, où n est un entier naturel.
   c) Démontrer cette conjecture par récurrence.
2. On décompose la matrice A sous la forme $A = I + B$ avec $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
   a) Écrire A^n en fonction de I et B.
   b) Redémontrer l'hérédité dans la démonstration par récurrence en utilisant cette expression.

4.4 Matrice inversible

Exercice 4.9

Résoudre le système d'équations ci-dessous. On donnera les valeurs exactes des solutions.

$$\begin{cases} 2\,x + 5\,y = 3 \\ x \quad + 4\,y = 1 \end{cases}$$

Exercice 4.10

A est la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et I est la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

La matrice A est inversible s'il existe une matrice $E = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ telle que $A \times E = I$.

1. L'égalité $A \times E = I$ s'écrit sous la forme de quatre équations d'inconnues x, y, z, t. Écrire ces quatre équations.
2. Dans ces quatre équations, il y a deux équations d'inconnues x et z.
   Résoudre le système formé par ces deux équations c'est à dire écrire x, puis z en fonction de a, b, c, d.
   Pour éliminer z, choisir une combinaison linéaire des deux équations, même chose pour éliminer x.
3. Résoudre le système formé par les deux équations d'inconnues y et t.
4. Écrire la matrice E en fonction de a, b, c, d.
5. À quelle condition sur a, b, c, d la matrice E existe-t-elle ?

Exercice 4.11

1. Pour chacune des matrices ci-dessous, vérifier si la matrice est inversible, et si c'est bien le cas, calculer son inverse. Utiliser des valeurs exactes.
   $A = \begin{pmatrix} 3 & 5 \\ 2 & 4 \end{pmatrix}$ $\quad B = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}$ $\quad C = \begin{pmatrix} 2 & 1 \\ 5 & 4 \end{pmatrix}$.
2. On admet que la matrice D ci-dessous est inversible. Déterminer son inverse D^{-1} à la calculatrice.
   $D = \begin{pmatrix} 3 & 2 & 1 \\ 5 & 4 & 7 \\ 1 & 2 & 3 \end{pmatrix}$.

Exercice 4.12 (Résoudre un système avec des matrices)

1. Écrire le système de l'exercice 4.9 sous la forme d'une égalité matricielle $AX = B$.
2. Justifier que : $X = A^{-1}B$.
3. Sans calculatrice, calculer la matrice A^{-1}.
4. Sans calculatrice, calculer la matrice $X = A^{-1}B$. On retrouve alors les solutions trouvées précédemment.

Exercice 4.13

Résoudre le système ci-dessous par un calcul matriciel.

Détailler les étapes **1. 3. 4.** données dans l'exercice 4.12, en utilisant la calculatrice.

$$\begin{cases} x \quad + 2\,y \quad\quad = 5 \\ 3x \quad\quad - z = 0 \\ x \quad + 4\,y \quad\quad = 7 \end{cases}$$

4.5 Cas particulier des matrices diagonales

Exercice 4.14 (Cas particulier des matrices diagonales)

Une matrice diagonale est une matrice de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, ou $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$, etc.

On considère les matrices diagonales $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 7 \end{pmatrix}$ et $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

1. Calculer les matrices $A \times B$, $B \times A$.
2. Calculer les matrices A^2 et A^3.
3. Écrire la matrice A^n en fonction de n.
4. Sachant que $A \times A^{-1} = I$, calculer la matrice A^{-1} (valeurs exactes).

4.6 Diagonalisation d'une matrice

Exercice 4.15

On considère les matrices : $A = \begin{pmatrix} -2 & 20 \\ -1 & 7 \end{pmatrix}$ $D = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ $P = \begin{pmatrix} 5 & 8 \\ 1 & 2 \end{pmatrix}$

1. Vérifier que la matrice P est inversible et calculer la matrice P^{-1}.
2. Vérifier que $PDP^{-1} = A$. On dit que la matrice A est diagonalisable.
3. Démontrer par récurrence que pour tout entier naturel n, $A^n = PD^nP^{-1}$.
4. Calculer l'expression de A^n en fonction de n.

Exercice 4.16

On considère la matrice : $A = \begin{pmatrix} -2 & 1 \\ -7,5 & 3,5 \end{pmatrix}$

1. La suite de matrices colonnes (U_n) est définie par $U_0 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ et pour tout entier naturel n, $U_{n+1} = AU_n$.
   a) Calculer U_1.
   b) Exprimer U_n en fonction de A^n.
2. On introduit les matrices suivantes : $D = \begin{pmatrix} 0,5 & 0 \\ 0 & 1 \end{pmatrix}$ $P = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$
   a) Vérifier que la matrice P est inversible et calculer la matrice P^{-1}.
   b) Vérifier que $PDP^{-1} = A$.
   c) On admet que pour tout entier naturel n, $A^n = PD^nP^{-1}$. Calculer l'expression de A^n en fonction de n.
3. Calculer U_n en fonction de n.
4. Déterminer la limite de U_n lorsque n tend vers $+\infty$.

4.7 Pour réviser

Chapitre du livre n° 4 – Matrices

Les exercices résolus

- ex 5 p 105 : inverse d'une matrice carrée $(2\,;\,2)$
- ex 6 p 105 : résolution d'un système d'équations
- ex 9 p 111 : puissance d'une matrice A, matrice A^n en fonction de n.

Rubrique *Pour s'exercer*, corrigés page 157

- ex 7 p 105 : matrices inverses
- ex 10 p 111 : puissance d'une matrice

Rubrique *Objectif bac*, corrigés page 159

- ex 48 p 116 : QCM
- ex 49 p 116 : Vrai/Faux

II Cours

4.1 Propriétés des opérations

Propriété 4.1

Pour deux matrices carrées A et B de format $(n\ ;\ n)$ et pour un réel λ,
les matrices $A+B$, λA, et $A\times B$ sont des matrices carrées de format $(n\ ;\ n)$.

Propriété 4.2 (Addition des matrices)

- L'addition de matrices de même format est commutative, c'est à dire que pour deux matrices A et B de même format $(n\ ;\ p)$, on a : $A+B=B+A$.
- L'addition de matrices de même format est associative, c'est à dire que pour trois matrices A, B, C de même format $(n\ ;\ p)$, on a : $(A+B)+C=A+(B+C)$.
- Pour trois matrices A, B, C de même format $(n\ ;\ p)$, si $A+B=A+C$, alors $B=C$.

Remarque : l'addition des matrices a donc les mêmes propriétés que l'addition des nombres.

Propriété 4.3 (Particularités de la multiplication)

- La multiplication de matrices carrées n'est pas commutative, c'est à dire qu'il existe des matrices A et B de format $(n\ ;\ n)$ telles que $A\times B\neq B\times A$.
- La multiplication des matrices carrées est associative, c'est à dire que pour toutes matrices carrées A, B, C de format $(n\ ;\ n)$ on a : $(A\times B)\times C=A\times(B\times C)$.
- La multiplication des matrices carrées est distributive par rapport à l'addition, c'est à dire que pour toutes matrices carrées A, B, C de format $(n\ ;\ n)$ on a : $A\times(B+C)=A\times B+A\times C$.
- Il existe des matrices A, B de format $(n\ ;\ n)$ telles que $A\neq 0$, $B\neq 0$ et $A\times B=0$.
- Il existe des matrices A, B, C de format $(n\ ;\ n)$ telles que $B\neq C$ et $A\times B=A\times C$.

Remarque

Rappelons que la multiplication des nombres a les propriétés suivantes :

- commutativité ;
- associativité ;
- distributivité de la multiplication par rapport à l'addition ;
- pour tous réels a et b, si $a\times b=0$, alors $a=0$ ou $b=0$;
- pour tout réel $a\neq 0$, si $a\times b=a\times c$, alors $b=c$.

Les seules propriétés que l'on retrouve pour la multiplication des matrices sont donc l'associativité et la distributivité de la multiplication par rapport à l'addition.

Définition 4.1 (La matrice identité)

- Au format $(2\ ;\ 2)$, la matrice identité est la matrice $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.
- Au format $(3\ ;\ 3)$, la matrice identité est la matrice $I_3=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$.

Propriété 4.4

- Pour toute matrice carrée A de format $(n\ ;\ n)$, on a l'égalité : $A\times I_n=I_n\times A$.
- Pour toute matrice colonne X de format $(n\ ;\ 1)$, on a l'égalité : $I_n\times X=X$.

Propriété 4.5

Pour toute matrice carrée A de format $(n\ ;\ n)$, on a l'égalité : $A^0=I_n$.

4.2 Matrice carrée inversible

4.2.a Définitions et propriétés

Définition 4.2

Dire qu'une matrice carrée A de format $(n\ ;\ n)$ est inversible signifie qu'il existe une matrice carrée A' de format $(n\ ;\ n)$ telle que $A' \times A = I_n$ et $A \times A' = I_n$.

Propriété 4.6

Si une matrice carrée A est inversible, alors la matrice A' telle que $A' \times A = A \times A' = I_n$ est unique.

Définition 4.3

Si une matrice carrée A est inversible, alors la matrice A' telle que $A' \times A = A \times A' = I_n$ est appelée la matrice inverse de la matrice A, et on la note A^{-1}.

Propriété 4.7

La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si $ad - bc \neq 0$.

Propriété 4.8

Pour une matrice inversible $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, sa matrice inverse est : $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Définition : pour la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ l'expression $ad-bc$ s'appelle le déterminant de la matrice A et on le note $\det(A)$.

Remarques

- On peut aussi calculer le déterminant d'une matrice de format $(3\ ;\ 3)$ ou d'un format supérieur, mais cela ne fait pas partie du programme de spécialité mathématiques, les formules de calculs sont plus complexes.
- Il en est de même pour le calcul de la matrice inverse d'une matrice inversible de format $(3\ ;\ 3)$ ou d'un format supérieur.
- Par conséquent le calcul de l'inverse d'une matrice inversible de format $(3\ ;\ 3)$ sera effectué à la calculatrice.

4.2.b Résolution d'un système avec une matrice inverse

Rappel : système d'équations sous forme matricielle

Un système de n équations du premier degré à n inconnues peut d'écrire sous la forme de l'égalité matricielle $AX = B$, où

- la matrice A est carrée au format $(n\ ;\ n)$;
- la matrice X est une matrice colonne au format $(n\ ;\ 1)$, et contient les inconnues ;
- la matrice B est une matrice colonne au format $(n\ ;\ 1)$.

Résolution du système

On calcule la matrice X de la manière suivante :

on a : $AX = B$ donc : $A^{-1} \times AX = A^{-1} \times B$ c'est à dire $I_n X = A^{-1}B$ autrement dit $X = A^{-1}B$.

Méthode

Pour résoudre un système de n équations du premier degré à n inconnues, on peut :
- écrire ce système sous la forme matricielle $AX = B$;
- calculer la matrice A^{-1} ;
- calculer les solutions avec l'égalité : $X = A^{-1}B$.

4.3 Cas particulier des matrices diagonales

Définition 4.4

Une matrice diagonale est une matrice carrée de la forme :

$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ ou $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$ ou $\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix}$ etc.

Propriété 4.9

Pour deux matrices diagonales A et B de format $(n\ ;\ n)$ et pour un réel λ,
les matrices $A + B$, λA, $A \times B$ sont des matrices diagonales de format $(n\ ;\ n)$.

Détail des opérations pour les matrices de format $(2\ ;\ 2)$

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix} \qquad \lambda \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} \lambda a & 0 \\ 0 & \lambda b \end{pmatrix}$$

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \times \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a \times c & 0 \\ 0 & b \times d \end{pmatrix} \qquad \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$$

Propriété 4.10

Le produit de deux matrices diagonales est commutatif.

Propriété 4.11

Une matrice diagonale est inversible si tous les coefficients de sa diagonale sont non nuls.

Propriété 4.12

Si $a \neq 0$ et $b \neq 0$, alors $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix}$

Si $a \neq 0$ et $b \neq 0$ et $c \neq 0$, alors $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & 0 & 0 \\ 0 & \frac{1}{b} & 0 \\ 0 & 0 & \frac{1}{c} \end{pmatrix}$

etc.

4.4 Diagonalisation d'une matrice

Propriété 4.13

Dire qu'une matrice A est diagonalisable signifie qu'il existe une matrice diagonale D et une matrice inversible P telles que $A = PDP^{-1}$.

Propriété 4.14

Si une matrice A est diagonalisable avec $A = PDP^{-1}$ alors pour tout entier naturel n, $A^n = PD^nP^{-1}$.

Chapitre 5

Nombres premiers

I Exercices

5.1 Les nombres premiers

5.1.a Vérifier si un nombre est premier

Exercice 5.1

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

1. zéro est-il premier ? Justifier.
2. 1 est-il premier ? Justifier.
3. Indiquer sans justifier les nombres premiers entre 2 et 20.

Exercice 5.2 (Crible d'Ératosthène)

Le crible d'Eratosthène consiste à déterminer tous les nombres premiers inférieurs ou égaux à un nombre donné. Déterminons par exemple tous les nombres premiers inférieurs ou égaux à 100 de la manière suivante, en utilisant le tableau ci-dessous.

1. Barrer 1 qui n'est pas premier.
2. Entourer 2 qui est premier.
3. Les autres multiples de 2 à partir de 4 ne sont pas premiers donc les barrer tous jusqu'à 100.
4. Entourer 3 qui est premier, puis barrer tous ses autres multiples à partir de 9.
5. Continuer ainsi jusqu'à obtenir tous les nombres premiers inférieurs ou égaux à 100.

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

Exercice 5.3

Pour chacun des nombres suivants, vérifier s'il est premier et s'il ne l'est pas indiquer son plus petit diviseur supérieur ou égal à 2 : 196, 219, 223, 259.

Exercice 5.4

Même consigne que pour l'exercice 5.3 pour les nombres suivants : 391, 409, 12 319.

Exercice 5.5

Voici un algorithme et le programme correspondant à la calculatrice.

1. Exécuter cet algorithme en complétant le tableau ci-dessous pour $n = 35$.

k											
r											

2. Que fait cet algorithme ?
3. Les nombres 223 et 259 ont été utilisés dans l'exercice 5.3. Combien y aura-t-il de passages dans la boucle Tant que

   a) pour $n = 223$ **b)** pour $n = 259$

4. Modifier cet algorithme et ce programme pour diminuer le nombre de passages dans la boucle.

Entrée(s) : un nombre entier $n \geqslant 2$
Sortie(s) : affichage « Premier » ou sinon affichage « Non premier » et plus petit diviseur.
Variables : des entiers n, k, r

Algorithme	**Programme sur la calculatrice**
Lire n	`Prompt N`
$k \leftarrow 1$	`1→K`
$r \leftarrow 1$	`1→R`
Tant que $r \neq 0$	`While R≠0`
$k \leftarrow k + 1$	`K+1→K`
$r \leftarrow n - k \times \text{Ent}(n/k)$	`N-K*ent(N/K)→R`
Fin du Tant que	`End`
Si $k = n$	`If K=N`
alors	`Then`
afficher « Premier »	`Disp "PREMIER"`
Sinon	`Else`
afficher « Non premier, plus petit diviseur», k	`Disp "NON PREM PLUS P DIV",K`
Fin du Si	`End`

5.1.b Infinitude et répartition des nombres premiers

Exercice 5.6 (Infinitude)

Nous allons démontrer que l'ensemble des nombres premiers est infini. Pour cela, nous allons supposer que l'ensemble des nombres premiers est fini, et nous allons prouver qu'il y alors une impossibilité.

On appelle cette façon de faire une *démonstration par l'absurde*.

Si l'ensemble des nombres premiers est fini alors cet ensemble s'écrit sous la forme : $E = \{p_1, p_2, \cdots, p_n\}$

Soit alors le nombre : $a = p_1 \times p_2 \times \cdots \times p_n + 1$.

Le nombre a admet un diviseur premier. Expliquer où est le problème.

Exercice 5.7 (Répartition)

Pour un entier naturel n, on appelle $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.

1. À l'aide du crible d'Ératosthène de l'exercice 5.2, déterminer $\pi(100)$.
2. Compléter le tableau ci-dessous.
3. D'après ce tableau, comment semble évoluer la fréquence de nombres premiers inférieurs ou égaux à x lorsque x tend vers $+\infty$?
4. Gauss en 1792 et Legendre en 1808 conjecturent que $\pi(x) \approx \dfrac{x}{\ln x}$.
   On appelle cette propriété le *théorème des nombres premiers*. Il a finalement été démontré par Hadamard et De La Vallée Poussin en 1896.

x	100	1 000	10 000	100 000	1 000 000
$\pi(x)$		168	1 229	9 592	78 498
$\frac{\pi(x)}{x}$					
$\frac{x}{\ln x}$					

Exercice 5.8 (Des trous aussi grands que l'on veut)

Dans cet exercice, nous allons montrer qu'on peut obtenir des suites d'entiers naturels successifs sans nombres premiers aussi longues que l'on veut.

Pour cela, nous allons utiliser la factorielle d'un nombre : la factorielle d'un entier naturel n non nul est le produit $n! = 1 \times 2 \times 3 \times \cdots \times n$, par exemple $5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$.

Factorielle sur la calculatrice TI 82 : math PRB 4:

1. Justifier que : $4! + 2$ est multiple de 2, $4! + 3$ est multiple de 3, $4! + 4$ est multiple de 4.
   Il n'est pas utile de calculer 4! pour répondre.
2. Donner sans calcul une suite de 10 nombres consécutifs non premiers.
3. Pour un nombre entier naturel n non nul, indiquer comment obtenir une suite de n nombres consécutifs non premiers.

5.1.c Les nombres de Mersenne et de Fermat

Exercice 5.9 (Nombres de Mersenne)

Marin Mersenne (1588-1648), est un moine français, mathématicien et philosophe qui s'est intéressé aux nombres premiers de la forme $2^n - 1$. On appelle ces nombres les *nombres de Mersenne*. Le plus grand nombre premier connu en 2016 est $2^{274\,207\,281} - 1$, il s'écrit avec plus de 22 millions de chiffres.

1. Compléter le tableau ci-dessous sans détailler ni justifier. Dans la 3e ligne, compléter par *Vrai* ou *Faux*.
2. Le but des questions suivantes est de démontrer la propriété :
   Si n n'est pas premier, alors $2^n - 1$ n'est pas premier.
   a) Vérifier cette propriété dans le tableau.
   b) Si n n'est pas premier, alors il existe des entiers naturels supérieurs ou égaux à 2 tels que $n = rs$. Justifier que $2^n - 1$ est divisible par $2^r - 1$, puis conclure.
   On pourra utiliser l'égalité $a^k - 1 = (a-1)(1 + a + a^2 + \cdots + a^{k-1})$.
3. Écrire la contraposée[1] de la propriété précédente.

1. La contraposée de *Si A alors B* est *Si non B alors non A* et elle est équivalente à *Si A alors B*.

4. Peut-on dire que *si n est premier, alors $2^n - 1$ est premier* ? Justifier.

n	2	3	4	5	6	7	8	9	10	11
$M_n = 2^n - 1$										
Premier ?										

Exercice 5.10 (Nombres de Fermat)

On appelle *nombre de Fermat* un nombre défini par $F_n = 2^{2^n} + 1$ où n est un entier naturel. Pierre de Fermat (1600-1665), magistrat, et mathématicien français conjectura que tous ces nombres sont premiers. Vérifier cette conjecture pour les 6 premiers nombres de Fermat en complétant le tableau ci-dessous.

n	0	1	2	3	4	5
$F_n = 2^{2^n} + 1$						
Premier ?						

5.1.d Système RSA

Le système RSA a été mis au point en secret par les mathématiciens britanniques James Ellis et Clifford Cocks en 1973, puis retrouvée et publiée en 1977 par les américains Ronald Rivest, Adi Shamir (deux informaticiens), et Leonard Adleman (un mathématicien).

Aujourd'hui ce système reste très utilisé pour la sécurité des cartes bancaires et pour la confidentialité des échanges sur Internet.

Propriété mathématique

Si p et q sont des nombres premiers distincts et si e est un entier premier avec $(p-1)(q-1)$, alors,

- il existe un entier d vérifiant $ed \equiv 1\ [(p-1)(q-1)]$,
- et pour tout entier naturel t on a : $(t^e)^d \equiv t\ [pq]$.

Exercice 5.11 (Exemple)

On choisit $p = 3$ et $q = 11$ et on calcule $(p-1)(q-1) = 2 \times 10 = 20$.

Comme nombre e premier avec 20 on choisit $e = 7$, et comme entier d vérifiant $ed \equiv 1\ [20]$ on choisit $d = 3$.

Le nombre t est le nombre associé au texte, par exemple $t = 8$ associé à la lettre H.

1. Codage : la lettre codée est la congruence de $t^e \equiv c\ [pq]$. Calculer le nombre c et laisser le résultat sous forme de nombre.

2. Décodage : le récepteur reçoit ce nombre c et le décode en calculant modulo pq le nombre c^d, c'est à dire $(t^e)^d$, or la propriété ci-dessus indique que $(t^e)^d \equiv t\ [pq]$ ce qui donne la lettre de départ. Vérifier qu'on a bien $c^d \equiv t\ [pq]$.

3. Reprendre le processus précédent (codage puis décodage) avec la lettre S.

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

Remarque

L'exemple ci-dessus fait intervenir de petits nombres premiers p et q. Dans la réalité ce sont de très grands nombres premiers qui sont utilisés.

Le nombre $n = pq$ et le nombre e sont rendus publics, on dit que le couple $(n\,;\,e)$ est la **clé publique**.

Les nombres p et q sont gardés secrets, or, pour des grands nombres, il est difficile en ayant le nombre n de le décomposer en produit de nombres premiers. On ne peut alors pas calculer le nombre $(p-1)(q-1)$ et on ne peut pas obtenir le nombre d qui permet le décodage.

Le nombre d n'est connu que du récepteur, on l'appelle la **clé privée**.

Enfin, il faut préciser aussi qu'un message n'est en réalité pas codé lettre par lettre mais par blocs de lettres, par exemple le mot MATHÉMATIQUE correspondrait à $t = 130120080513012009172105$.

5.2 Décomposition en facteurs premiers

Exercice 5.12 (Exemples)

Tout entier naturel supérieur ou égal à deux admet une unique décomposition sous forme de produit de puissances de nombres premiers, par exemple, $12 = 2^2 \times 3$ et $360 = 2^3 \times 5 \times 3^2$.

Décomposer de cette façon les nombres suivants : 42 ; 72 ; 150 ; 2 904 ; 34 425.

Exercice 5.13 (Diviseurs d'un entier naturel)

1. Écrire les décompositions en facteurs premiers de 252 ; 14 ; 18 ; 33 ; 60.
2. Indiquer parmi 14 ; 18 ; 33 ; 60 lesquels sont des diviseurs de 252.
3. Comment s'écrivent les décompositions en facteurs premiers des diviseurs de 252 ?
4. Déterminer alors tous les diviseurs de 252. On pourra s'aider d'un arbre.
5. 252 a 18 diviseurs : comment aurait-on pu calculer le nombre 18 à l'aide de la décomposition en facteurs premiers de 252 ?

Exercice 5.14

On donne les nombres suivants qu'on ne demande pas de calculer.

$a = 3^4 \times 7^2 \times 19^3$ $b = 3^2 \times 7 \times 19^2$ $c = 3^5 \times 7 \times 19$ $d = 3^2 \times 7^2 \times 11$ $e = 3^3 \times 19^3$

1. Parmi les nombres b, c, d, e, lesquels sont des diviseurs de a ?
2. Calculer le nombre de diviseurs de a.

Exercice 5.15

On donne les nombres suivants qu'on ne demande pas de calculer.

$a = 3^4 \times 5^3 \times 7^3$ $b = 2^5 \times 5^2 \times 7^6$

1. Déterminer d le PGCD de a et b.
2. Écrire les décompositions en facteurs premiers de a, b, d avec les nombres premiers 2 ; 3 ; 5 ; 7 quitte à mettre certains exposants égaux à zéro, puis comparer les trois expressions et leurs exposants.

Exercice 5.16

Déterminer le PGCD de a et b dans les cas suivants.

1. $a = 2^4 \times 5^3 \times 7^3$ $b = 2^5 \times 5 \times 11$
2. $a = 3^2 \times 5^4 \times 7^5$ $b = 3^5 \times 5^2 \times 7^3$
3. $a = 3^4 \times 7^3 \times 13$ $b = 2^5 \times 5^2 \times 11$

5.3 Pour réviser

Chapitre du livre n° 3 – Nombres premiers

Les exercices résolus

- ex 1 p 73 : reconnaître un nombre premier
- ex 2 p 73 : déterminer si un nombre est premier
- ex 10 p 81 : décomposition en facteurs premiers
- ex 11 p 81 : déterminer tous les diviseurs d'un entier naturel

Rubrique *Pour s'exercer*, corrigés page 157

- ex 3 p 73 : vérifier si des nombres sont premiers
- ex 6 p 73 : $n^2 + 2n + 1$ peut-il être premier ?
- ex 12 p 81 : décomposition en facteurs premiers, divisibilité
- ex 14 p 81 : décomposition en facteurs premiers, liste des diviseurs

Rubrique *Objectif bac*, corrigés page 158

- ex 68, 69 p 86 (QCM) : décomposition en facteurs premiers, nombre de Mersenne, division euclidienne, congruence, PGCD
- ex 70, 71 p 86 (Vrai-Faux)
- ex 72 p 87 : exercice de type bac

II Cours

5.1 Définition et propriétés

Définition 5.1

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

Exemples

Étudions les entiers de 0 à 20.

0 n'est pas premier, il a une infinité de diviseurs.

1 n'est pas premier parce qu'il a un seul diviseur : 1.

Les nombres 2, 3, 5, 7, 11, 13, 17, 19 sont premiers.

Le nombre 4 n'est pas premier puisque 4 a 3 diviseurs : 1, 2, 4.

De même les nombres 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 ne sont pas premiers.

Remarque : d'après ce qui précède un nombre premier est supérieur ou égal à 2.

Propriété 5.1

Deux nombres premiers distincts sont premiers entre eux.

Démonstration

Pour deux nombres premiers distincts p et q, les diviseurs de p sont 1 et p et les diviseurs de q sont 1 et q, donc le seul diviseur commun à p et q est 1, de sorte que p et q sont bien premiers entre eux.

Propriété 5.2

Pour un nombre entier naturel n et un nombre premier p,
p et n sont premiers entre eux si et seulement si p ne divise pas n.

Démonstration

Pour un nombre entier naturel n et un nombre premier p, si p et n sont premiers entre eux, alors il est évident que p ne divise pas n puisque p serait alors un diviseur commun supérieur ou égal à 2.

Réciproquement, si p ne divise pas n, soit d un diviseur commun à p et n.

Ce nombre d divise alors p qui est premier, par conséquent d est égal à 1 ou p. Or d ne peut être égal à p puisque d divise n et p ne divise pas n, donc $d = 1$.

On a prouvé qu'un diviseur commun à p et à n ne peut être qu'égal à 1, donc p et n sont premiers entre eux.

Remarque

La propriété 5.2 n'est plus vraie si p n'est pas premier.

Par exemple si $p = 6$ (non premier) et $n = 15$, alors 6 ne divise pas 15 et pourtant 6 et 15 ne sont pas premiers entre eux puisque leur PGCD est 3.

Propriété 5.3

Pour un nombre entier naturel $n \geqslant 2$,
- si n n'est pas premier, alors il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$;
- si n n'a aucun diviseur premier p tel que $p \leqslant \sqrt{n}$, alors n est premier.

Exemple

Vérifions si 97 est premier. $\sqrt{97} \approx 9,8$

Les nombres premiers inférieurs ou égaux à 9,8 sont : 2, 3, 5, 7.

97 n'est ni multiple de 2 ni de 5.

$9 + 7 = 16$ et 16 n'est pas multiple de 3, donc 97 n'est pas multiple de 3.

$97 = 7 \times 13 + 6$, donc 97 n'est pas multiple de 7.

Donc 97 n'a pas de diviseur premier inférieur ou égal à $\sqrt{97}$, par conséquent 97 est premier.

Démonstration de la première partie de la propriété.

Soit n un entier naturel supérieur ou égal à 2 et non premier. Cela signifie que n admet au moins un diviseur autre que 1 ou lui même.

Soit p le plus petit des diviseurs de n différents de 1.

➡ Démontrons que p est premier.

Soit d un diviseur de p. On peut avoir $d = 1$ ou $d \neq 1$.

Si $d \neq 1$, comme p divise n, le nombre d divise aussi n, or p est le plus petit des diviseurs de n différents de 1, donc $p \leqslant d$, mais comme d divise p, on a aussi $d \leqslant p$, donc finalement, $d = p$.

On a prouvé qu'un diviseur de p ne peut être qu'égal à 1 ou à p, donc p est premier.

➡ Démontrons maintenant que $p \leqslant \sqrt{n}$.

Puisque p est un diviseur de n, il existe un nombre entier naturel k tel que $pk = n$. Le nombre k est différent de 1 puisque sinon $p = n$ ce qui n'est pas le cas. Or p est le plus petit des diviseurs de n différents de 1, donc $p \leqslant k$, donc $p^2 \leqslant pk$, c'est à dire $p^2 \leqslant n$, soit $p \leqslant \sqrt{n}$.

Démonstration de la deuxième partie de la propriété.

La deuxième partie est la contraposée de la première partie. Justifions le.

Pour un nombre entier naturel $n \geqslant 2$, appelons A l'affirmation « n n'est pas premier » et B l'affirmation « n admet un diviseur premier p tel que $p \leqslant \sqrt{n}$ ».

Ainsi l'affirmation « n est premier » est l'affirmation contraire de A, qu'on appelle l'affirmation *non A*. De même l'affirmation « n n'a aucun diviseur premier p tel que $p \leqslant \sqrt{n}$ » est l'affirmation *non B*.

La première partie de la propriété s'écrit alors : *si A alors B*, et la deuxième partie de la propriété s'écrit : *si non B alors non A* et c'est la contraposée de *si A alors B*.

Or, la contraposée d'une propriété est équivalente à cette propriété.

Ainsi les deux parties de cette propriété sont équivalentes, donc la deuxième partie est vraie parce que la première partie est vraie.

Propriété 5.4

Tout nombre entier admet un diviseur premier.

Démonstration

Si un nombre entier naturel est premier, la propriété est vraie parce que ce nombre est divisible par lui même.

Si un nombre entier naturel n'est pas premier, on sait qu'il admet un diviseur premier d'après la propriété 5.3.

Si un nombre entier n est négatif, alors $-n$ est positif et admet un diviseur premier qui divise aussi n.

Propriété 5.5

L'ensemble des nombres premiers est infini.

Démonstration

Nous allons démontrer cette propriété par l'absurde, c'est à dire que nous allons supposer que l'ensemble des nombres premiers est fini et prouver qu'il y alors une impossibilité.

Si l'ensemble des nombres premiers est fini alors cet ensemble s'écrit sous la forme : $E = \{p_1, p_2, \cdots, p_n\}$

Soit alors le nombre : $a = p_1 \times p_2 \times \cdots \times p_n + 1$.

Comme tout nombre entier, le nombre a admet un diviseur premier donc l'un des nombres p_1, ou p_2, ou $\cdots$, ou p_n est un diviseur de a et donc aussi un diviseur de $a - p_1 \times p_2 \times \cdots \times p_n$ qui est égal à 1.

On aurait donc un nombre premier diviseur de 1 ce qui est impossible.

Donc a admet un diviseur premier qui ne fait pas partie de l'ensemble E, par conséquent, cet ensemble ne peut pas être un ensemble fini.

5.2 Décomposition en facteurs premiers

Propriété 5.6 (Décomposition en facteurs premiers)

Tout entier naturel supérieur ou égal à deux admet une unique décomposition sous forme de produit de puissances de nombres premiers.

Exemples

$12 = 2^2 \times 3$ $\qquad$ $360 = 2^3 \times 5 \times 3^2$

Propriété 5.7 (Diviseur d'un entier naturel)

Si la décomposition en facteurs premiers d'un entier naturel n est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$,
alors la décomposition en facteurs premiers de tout diviseur de n s'écrit :
$p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$ avec $\beta_1 \leqslant \alpha_1$, $\beta_2 \leqslant \alpha_2$, $\ldots$, $\beta_r \leqslant \alpha_r$.

Ensemble des diviseurs d'un entier naturel

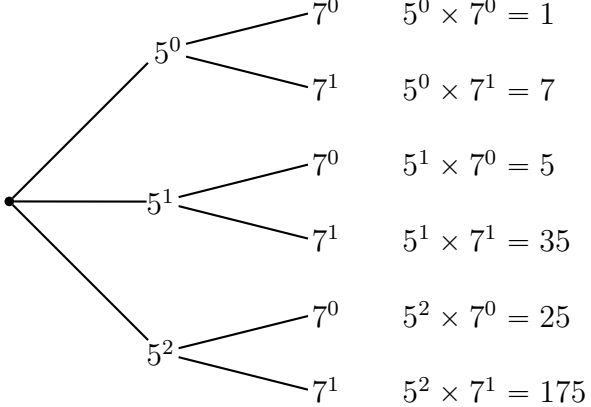
On peut utiliser la décomposition en facteurs premiers d'un entier naturel pour déterminer l'ensemble de ses diviseurs.

Déterminons par exemple l'ensemble des diviseurs de 175.

La décomposition en facteurs premiers de 175 est $175 = 5^2 \times 7$, donc d'après la propriété précédente, tout diviseur de 175 s'écrit : $5^{\beta_1} \times 7^{\beta_2}$ avec $\beta_1 \leqslant 2$, $\beta_2 \leqslant 1$.

Autrement dit β_1 peut être égal à 0, 1 ou 2 et β_2 peut être égal à 0 ou 1.

L'arbre ci-dessous permet de déterminer toutes les combinaisons possibles et donc tous les diviseurs de 175.



L'ensemble des diviseurs de 175 est donc $\boxed{1\,;\,5\,;\,7\,;\,25\,;\,35\,;\,175}$.

Nombre de diviseurs d'un entier naturel

Si la décomposition en facteurs premiers d'un entier naturel est $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, alors le nombre de diviseurs de cet entier naturel est égal à $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \cdots \times (\alpha_r + 1)$.

Par exemple la décomposition en facteurs premiers de 175 est $175 = 5^2 \times 7^1$ et le nombre de ses diviseurs, c'est à dire le nombre de chemins dans l'arbre tracé plus haut est égal à :
$(2 + 1) \times (1 + 1) = 3 \times 2 = \boxed{6}$.

Un autre exemple concernant l'ensemble des diviseurs d'un entier naturel et le nombre de ses diviseurs est détaillé dans l'exercice résolu n° 11 p 81.

Propriété 5.8 (PGCD de deux entiers naturels)

Si les décompositions en facteurs premiers de deux entiers naturels a et b sont :
$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$,
alors la décomposition en facteurs premiers du PGCD de a et b est :
$p_1^{\gamma_1} \times p_2^{\gamma_2} \times \cdots \times p_r^{\gamma_r}$ où γ_1 est le plus petit des deux exposants α_1 et β_1, γ_2 est le plus petit des deux exposants α_2 et β_2, etc.

Exemple

Déterminons le PGCD de 1 440 et 324.

$1\,440 = 2^5 \times 3^2 \times 5 = 2^5 \times 3^2 \times 5^1$ et $324 = 2^2 \times 3^4 = 2^2 \times 3^4 \times 5^0$

$\text{PGCD}(1\,440; 324) = 2^{\gamma_1} \times 3^{\gamma_2} \times 5^{\gamma_3}$

γ_1 est le plus petit des deux exposants 5 et 2, γ_2 est le plus petit des deux exposants 2 et 4, γ_3 est le plus petit des deux exposants 1 et 0.

$\text{PGCD}(1\,440; 324) = 2^2 \times 3^2 \times 5^0 = \boxed{36}$

Propriété 5.9 (Nombres premiers entre eux)

Deux entiers naturels sont premiers entre eux si et seulement si ils n'ont aucun diviseur premier en commun.

Exemples

$2 \times 7 = 14$ et $3 \times 11 = 33$ 14 et 33 sont premiers entre eux.

$2^3 \times 7 = 56$ et $3^4 \times 5^2 = 2\,025$ 56 et 2 025 sont premiers entre eux.

Chapitre 6

Compléments sur les matrices

I Exercices

6.1 Codage de Hill avec des matrices

Exercice 6.1

Le but de cet exercice est de montrer sur un exemple l'utilisation de matrices pour le chiffrement de Hill.

On rappelle ci-dessous comment s'effectue le chiffrement de Hill.

- On groupe les lettres du message deux par deux
- On associe un nombre entre 0 et 26 à chaque lettre (tableau de de la figure 6.1), et on obtient ainsi des couples de nombres $(x_1\ ;\ x_2)$.
- On associe en suite ce couple $(x_1\ ;\ x_2)$ à un couple $(y_1\ ;\ y_2)$ de la manière suivante :
  $\begin{cases} ax_1 + bx_2 \equiv y_1\ [26] \\ cx_1 + dx_2 \equiv y_2\ [26] \end{cases}$

Partie A – Procédure de codage

Un chiffrement de Hill est effectué d'après le système suivant : $\begin{cases} 2x_1 + 1x_2 \equiv y_1\ [26] \\ 3x_1 + 4x_2 \equiv y_2\ [26] \end{cases}$.

1. Écrire ce système sous forme matricielle $AX = Y$.
2. On veut coder le mot CODAGE.
   a) Pour CO, on a $x_1 = 2$ et $x_2 = 14$, et on écrit le couple $(x_1\ ;\ x_2)$ sous forme de matrice colonne : $\begin{pmatrix} 2 \\ 14 \end{pmatrix}$. Effectuer alors un calcul matriciel à la calculatrice pour coder CO.
   b) Procéder ainsi pour coder DA, puis GE (tableau de la figure 6.1).

Partie B – Procédure de décodage

On appelle I la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Le codage consiste à utiliser plusieurs fois l'égalité matricielle $AX = Y$.

Le décodage consiste donc à déterminer une matrice C telle que $CY = X$.

1. On pourrait penser que la matrice C est A^{-1} la matrice inverse de A.
   Déterminer la matrice A^{-1} et expliquer pourquoi cette matrice ne convient pas pour le décodage.

2. Il nous faut en fait une matrice C dont les coefficients soient des entiers entre 0 et 25, et qui soit l'inverse de A modulo 26, c'est à dire telle que $A \times C = C \times A \equiv I$ [26].

a) Calculer la matrice $B = 5A^{-1}$ et justifier que $A \times B = B \times A = 5I$.

b) Déterminer l'entier α entre 0 et 25 tel que $5\alpha \equiv 1$ [26] (autrement dit déterminer l'inverse de 5 modulo 26).

c) Justifier que $A \times (\alpha B) = (\alpha B) \times A \equiv I$ [26].

d) Déterminer la matrice C.

3. Utiliser la matrice C pour décoder OSVWBK.

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

Fig. 6.1

6.2 Une suite $u_{n+2} = au_{n+1} + bu_n$

Exercice 6.2

La suite (u_n) est définie par : $u_0 = 1$, $u_1 = 3$, et pour tout entier naturel n, $u_{n+2} = 3u_{n+1} - 2u_n$.

1. Calculer u_2 et u_3.

2. Pour tout entier naturel n, on note C_n la matrice $C_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$ et on note A la matrice carrée d'ordre 2 telle que $C_{n+1} = AC_n$.
Déterminer A et écrire C_n en fonction de A.

3. On note P et D les matrices : $P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

a) Vérifier que la matrice P est inversible et calculer sa matrice inverse P^{-1} en détaillant.

b) Calculer PDP^{-1} à la calculatrice.

c) On admet que pour tout entier naturel non nul n, $A^n = PD^nP^{-1}$.
Calculer l'expression de A^n en détaillant.

d) En déduire une expression de u_n en fonction de n.

6.3 Étude asymptotique d'une marche aléatoire

Exercice 6.3 (Marche aléatoire sur un graphe – Graphe probabiliste)

Concernant une maladie contagieuse dans la population d'une ville, on constate chaque mois que
- une personne saine peut tomber malade avec une probabilité égale à 0,03 ;
- une personne malade peut guérir avec une probabilité égale à 0,05.

Au départ personne n'est malade.

Au cours du $n^{\text{ième}}$ mois on choisit une personne au hasard et on considère les évènements suivants :
- S_n « La personne choisie au hasard est saine »
- A_n « La personne choisie au hasard est atteinte »

On appelle respectivement u_n et v_n les probabilités $p(S_n)$ et $p(A_n)$.

1. D'après l'énoncé, donner les valeurs de u_0 et v_0.

2. Compléter par des probabilités l'arbre de la figure 6.2, ainsi que le schéma de la figure 6.3, qu'on appelle un graphe probabiliste à 2 sommets.

3. Écrire u_{n+1} et v_{n+1} en fonction de u_n et v_n.

4. On appelle P_n la matrice $\begin{pmatrix} u_n & v_n \end{pmatrix}$ et $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice telle que $P_{n+1} = P_n M$.

Vocabulaire :
- on dit que la matrice P_n donne *l'état probabiliste* de la propagation de la maladie ;
- et M s'appelle la matrice de *matrice de transition* d'un mois au mois suivant.

a) Écrire la matrice M.

b) Préciser ce que signifient les nombres a, b, c, d et expliquer pourquoi on a $a + b = 1$ et $c + d = 1$.

5. Calculer P_1 et P_2. Arrondir au millième.

6. Donner l'expression de P_n en fonction de M, de n, et de P_0.

7. En arrondissant au millième, calculer à la calculatrice les probabilités qu'une personne choisie au hasard soit saine

a) le 3e mois ; **b)** le 12e mois (1 an) ; **c)** le 72e mois (6 ans).

8. On appelle D et Q les matrices : $D = \begin{pmatrix} 1 & 0 \\ 0 & 0,92 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 1 \\ 1 & -\frac{5}{3} \end{pmatrix}$.

On admet sans calcul que $M = QDQ^{-1}$, que $M^n = QD^nQ^{-1}$ et que :

$M^n = \begin{pmatrix} 0,625 + 0,375 \times 0,92^n & 0,375 - 0,375 \times 0,92^n \\ 0,625 - 0,625 \times 0,92^n & 0,375 + 0,625 \times 0,92^n \end{pmatrix}$.

Calculer la probabilité qu'une personne soit saine à long terme. Justifier.

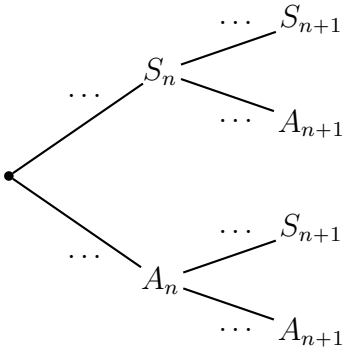


Fig. 6.2

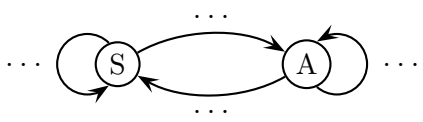


Fig. 6.3

Exercice 6.4 (État stable)

Une personne utilise un chemin A ou un chemin B pour aller à son travail. S'il y a des encombrements sur son trajet, elle change d'itinéraire le lendemain. La probabilité d'encombrement est 0,2 sur le trajet A et 0,5 sur le trajet B.

On appelle a_n la probabilité de choisir le trajet A le $n^{\text{ième}}$ jour et b_n la probabilité de choisir le trajet B le $n^{\text{ième}}$ jour.

1. Représenter le graphe probabiliste associé à cette situation.

2. On appelle P_n la matrice $\begin{pmatrix} a_n & b_n \end{pmatrix}$ (état probabiliste) et M la matrice carrée telle que $P_{n+1} = P_n M$ (matrice de transition).
Écrire la matrice M.

3. On admet que la matrice P_n converge vers une matrice $S = \begin{pmatrix} x & y \end{pmatrix}$ c'est à dire que les suites (a_n) et (b_n) sont toutes deux convergentes respectivement vers x et vers y.

a) Justifier qu'on a alors les égalités : $SM = S$ et $x + y = 1$.

b) Calculer la matrice S. On écrira ses coefficients sous forme de fractions.

c) Interpréter ce résultat.

Vocabulaire : on dit que la matrice S est l'*état stable* de ce processus aléatoire.

Exercice 6.5 (Avec des matrices colonnes)

Dans une ville de 250 000 habitants, 70 % d'entre eux utilisent leur voiture.

L'évolution de cette proportion les années suivantes est modélisée ainsi : chaque année, 5 % de ceux qui utilisent la voiture changent pour les transports en commun, et 1 % de ceux qui utilisent les transports en commun, changent pour la voiture.

On précise que les années suivantes la population de cette ville reste stable.

L'année n, pour un habitant choisi au hasard, on nomme les événements :

- V_n « cet habitant se déplace en voiture »
- T_n « cet habitant se déplace en transports en commun »

On appelle v_n la probabilité de V_n, et t_n la probabilité de T_n et pour tout entier naturel n, on pose $X_n = \begin{pmatrix} v_n \\ t_n \end{pmatrix}$.

1. Compléter l'arbre de la figure 6.4, ainsi que le graphe probabiliste de la figure 6.5.

2. Déterminer la matrice X_0.

3. Écrire v_{n+1} et t_{n+1} en fonction de v_n et t_n.

4. Déterminer la matrice M telle que $X_{n+1} = M\,X_n$.

5. Écrire sans justifier X_n en fonction de X_0 et M.

6. On admet que la suite de matrices (X_n) converge.
À l'aide de la calculatrice, conjecturer la limite de X_n, au centième près.

7. Déterminer cette limite en calculant l'état stable de cette évolution c'est à dire en résolvant l'équation $MX = X$ où $X = \begin{pmatrix} x \\ y \end{pmatrix}$, sans oublier que $x + y = 1$. Donner la réponse sous forme fractionnaire.

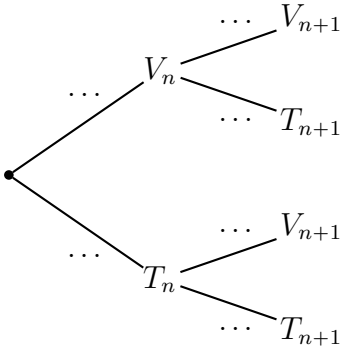


Fig. 6.4

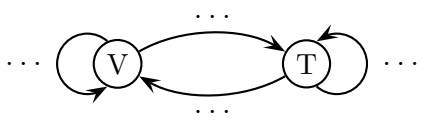


Fig. 6.5

Exercice 6.6 (Modèle de diffusion d'Ehrenfest)

Historique du problème

En 1907 le physicien Paul Ehrenfest et sa femme la mathématicienne Tatiana Ehrenfest ont proposé un modèle probabiliste à propos de l'expérience décrite ci-dessous.

Deux enceintes hermétiques A et B sont séparées par une cloison. Cette cloison a une ouverture qui est bouchée au départ. On remplit de gaz l'enceinte A et on débouche l'ouverture de la cloison. On constate que progressivement le gaz se répartit de manière équilibrée entre les deux enceintes.

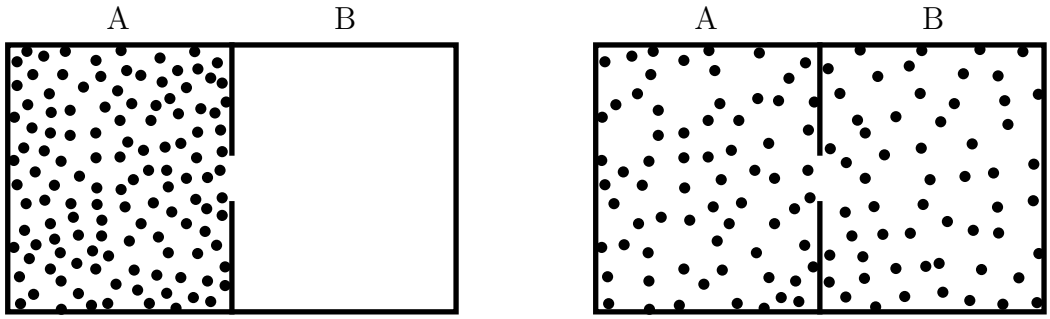


Fig. 6.6

Ce phénomène ne semble donc pas réversible, alors que les lois de la mécanique sont réversibles par rapport au temps.

Le modèle des urnes d'Ehrenfest va permettre de répondre à ce paradoxe.

Modèle mathématique des urnes d'Ehrenfest

On considère 2 urnes A et B, et N boules numérotées de 1 a N.

Initialement, toutes les boules se trouvent dans l'urne A. Ensuite, à chaque étape, on tire au hasard, de façon équiprobable, un nombre entre 1 et N, et on change d'urne la boule correspondante.

Étude du cas N = 2

Le nombre N de molécules de gaz dans l'enceinte A est de l'ordre du nombre d'Avogadro, soit $6,02 \times 10^{23}$, mais dans cet exercice, on étudiera le cas ou le nombre N est égal à 2. Ce nombre n'est bien sûr pas réaliste, mais il va nous aider à comprendre.

Les répartitions possibles R_1, R_2, R_3, des deux boules dans les deux urnes A et B sont schématisées ci-dessous.

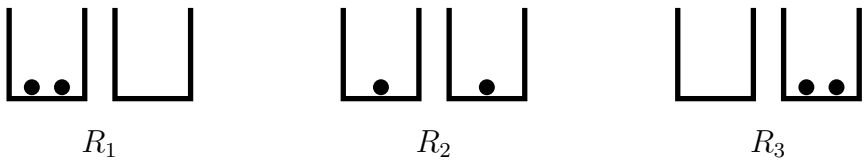


Fig. 6.7

À l'étape 0, c'est à dire au départ, la répartition est R_1.

On appelle X_k la variable aléatoire égale au nombre de boules dans l'urne B à l'étape k, et W_k est la matrice ligne $W_k = \big(p(X_k = 0) \quad p(X_k = 1) \quad p(X_k = 2)\big)$.

Partie A - Étude de la variable aléatoire X_k

1. Écrire la matrice W_0.
2. Représenter la situation par un graphe probabiliste.
3. Écrire P la matrice telle que pour tout entier naturel k, $W_{k+1} = W_k P$.
4. Avec la calculatrice, calculer P^2, P^3,P^4.

5. Pour tout entier naturel non nul k, conjecturer les expressions de P^{2k} et de P^{2k+1}, et le démontrer par récurrence.

6. En déduire les expressions possibles de W_k.

7. Calculer l'espérance $E(X_k)$ dans les différents cas et interpréter le résultat.

Partie B – Retour à l'état initial

Après un nombre pair d'étapes on peut revenir à l'état initial, c'est à dire deux boules dans l'urne A.

Nous allons déterminer le nombre moyen d'étapes pour revenir à l'état initial à l'aide de l'algorithme et du programme ci-dessous (figure 6.8).

La variable U correspond à la boule n° 1, et vaut -1 si la boule 1 est dans l'urne A et $+1$ sinon. Même chose pour la variable V qui correspond à la boule n° 2. La variable K est le numéro d'étape.

1. Compréhension de l'algorithme

a) Qu'indique l'initialisation de cet algorithme ?

b) Dans la boucle Tant que, à quoi correspondent les multiplications de U ou V par -1 ?

c) Pourquoi continue-t-on tant que $U = 1$ ou $V = 1$?

2. Utilisation du programme

a) Exécuter le programme 5 fois et calculer le nombre moyen d'étapes pour le retour à l'état initial.

b) Modifier l'algorithme et le programme pour qu'il calcule plusieurs fois le nombre K d'étapes de retour à l'état initial et qu'il en calcule la moyenne.

On pourra utiliser les variables suivantes :
- E le nombre de répétitions du calcul, à saisir par l'utilisateur ;
- S la somme des valeurs de K ;
- M la moyenne des valeurs de K.

c) Exécuter ce programme et compléter le tableau ci-dessous.

E nombre de répétitions du calcul	10	100	500	1 000
M nombre moyen d'étapes pour le retour à l'état initial				

Algorithme	`Programme sur TI 82`
Variables : U, V, K, R des entiers	
Initialisation	
$-1 \to U$	`:-1→U`
$1 \to V$	`:1→V`
$1 \to K$	`:1→K`
Traitement	`:`
Tant que $U = 1$ ou $V = 1$	`:While U=1 ou V=1`
$K + 1 \to K$	`:K+1→K`
Nombre aléatoire 1 ou 2 → R	`:entAléat(1,2)→R`
Si R=1	`:If R=1`
alors	`:Then`
$U \times (-1) \to U$	`:U*(-1)→U`
Sinon	`:Else`
$V \times (-1) \to V$	`:V*(-1)→V`
Fin du Si	`:End`
Fin du Tant que	`:End`
Sortie	`:`
Afficher "K =",K	`:Disp "K =",K`

Fig. 6.8

6.4 Modèle proie-prédateur

Un modèle proie-prédateur décrit l'évolution de deux populations de proies et de prédateurs, par exemple les lièvres et les lynxs dans la baie d'Hudson au Canada, ou les sardines et les requins dans l'Adriatique, ou les truites et les brochets dans une rivière etc.

En 1926, à partir d'un grand nombre de données d'observation, le mathématicien et physicien italien Volterra propose un modèle qui est étudié ci-dessous.

Exercice 6.7

x_n est l'effectif de lièvres et (y_n) est l'effectif de lynxs pour une année n donnée. Les suites (x_n) et (y_n) décrivent donc l'évolution de ces deux populations et sont définies par les égalités ci-dessous.

$$\begin{cases} x_{n+1} = 1,05\,x_n - 0,001\,x_n\,y_n \\ y_{n+1} = 0,97\,y_n + 0,0002\,x_n\,y_n \end{cases}$$

Ces deux suites sont basées sur les hypothèses suivantes :

- sans la présence des prédateurs, la population de proies augmente de 5 % par an ;
- sans la présence des proies, la population de prédateurs diminue de 3 % par an ;
- le nombre de proies tuées chaque année par des prédateurs est proportionnelle aux populations de proies et de prédateurs avec un coefficient de 0,1 % ;
- le nombre de naissances de prédateurs chaque année dépend presqu'exclusivement de leur nourriture, et elle est proportionnelle aux populations de proies et de prédateurs avec un coefficient de 0,02 %.

Partie A

1. Sans la présence de prédateurs, quelle serait la suite (x_n) ? plus précisément, quelle serait sa nature, son sens de variation et sa limite, si elle existe ?
2. Sans la présence de proies, quelle serait la suite (y_n) (nature, sens de variation, limite éventuelle) ?
3. Déterminer des populations initiales non nulles x_0 et y_0 telles que les deux populations resteraient constantes, c'est à dire telle que pour tout entier naturel n on ait : $x_{n+1} = x_n$ et $y_{n+1} = y_n$.

Partie B – Utilisation d'un tableur

On suppose que les populations initiales sont 200 lièvres et 30 lynxs.

Les explications ci-dessous sont valables pour le tableur *LibreOffice Calc*.

1. Ouvrir un tableur pour observer l'évolution de ces populations pendant 500 ans.
   On pourra procéder ainsi :
   - compléter les 2 premières lignes comme ci-dessous :

	A	B	C
1	n	x_n	y_n
2	0	200	30
3	1	204	31
4	2	208	31

   - dans les cellules B3 et C3, saisir des formules à recopier vers le bas qui permettront d'afficher les valeurs successives des populations x_n et y_n ;
   - sélectionner le bloc de cellules A3 : C3 et tirer la poignée de recopie vers le bas jusqu'à la ligne 502, c'est à dire jusqu'à $n = 500$.
2. Observer l'évolution des populations en parcourant le tableau.
3. On peut améliorer cette observation en traçant des graphiques, pour cela,

- sélectionner le bloc de cellules A1 : C502
- dans le menu Insertion, choisir Diagramme
- 1. Type de diagramme : choisir Lignes et Points et lignes.
- cliquer sur Suivant
- 2. Plage de données : cocher les trois mentions Série de données en colonnes, Première ligne comme étiquette, Première colonne comme étiquette
- cliquer sur Terminer

4. En observant les deux courbes d'évolution de populations,
a) comment évolue chaque population ?
b) comment évolue une population par rapport à l'autre ?

5. Modifier maintenant les populations initiales x_0 et y_0 et observer ce qui change (ou non). Voici quelques idées de valeurs à essayer :
a) $x_0 = 100$ et $y_0 = 100$; $x_0 = 100$ et $y_0 = 20$; $x_0 = 200$ et $y_0 = 100$;
b) $x_0 = 150$ et $y_0 = 50$ (point d'équilibre trouvé en A.3)
c) $x_0 = 151$ et $y_0 = 49$; $x_0 = 145$ et $y_0 = 52$ (valeurs proches du point d'équilibre)

Partie C – Linéarisation au voisinage du point d'équilibre

Revenons au système d'égalités de départ, rappelé ci-dessous.

$$\begin{cases} x_{n+1} = 1,05\,x_n - 0,001\,x_n\,y_n \\ y_{n+1} = 0,97\,y_n + 0,0002\,x_n\,y_n \end{cases}$$

1. Ce système ne peut pas être écrit sous forme matricielle. Pourquoi ?

2. Les questions qui suivent ont pour but d'arriver à modéliser les populations pour arriver à une forme matricielle, et cela ne sera possible que si les populations sont proches du point d'équilibre.
On définit : $X_n = x_n - 150$ et $Y_n = y_n - 50$.
a) D'après le système ci-dessus, calculer X_{n+1} et Y_{n+1} en fonction de X_n et Y_n.
b) Lorsque les populations sont proches du point d'équilibre, les valeurs de X_n et Y_n sont petites et on peut donc négliger la valeur du produit X_nY_n.
Écrire alors les égalités précédentes sans les termes avec X_nY_n.
On obtient alors un système linéaire, qui va permettre l'utilisation de matrices. Voilà pourquoi on dit qu'on a linéarisé.
c) On appelle U_n la matrice $\begin{pmatrix} X_n \\ Y_n \end{pmatrix}$
Les égalités simplifiées de la question précédente peuvent s'écrire sous la forme matricielle $U_{n+1} = AU_n$. Donner la matrice A.

3. Effectuons maintenant un calcul pour des populations initiales proches du point d'équilibre.
On prend : $x_0 = 151$ et $y_0 = 49$. Retrouver alors les populations de l'année 50 par un calcul matriciel.

6.5 Suites de matrices colonnes $U_{n+1} = AU_n + C$

Exercice 6.8

Dans un club de sport, chaque année, la moitié des benjamins part en minime, l'autre moitié reste en benjamins, la moitié des poussins part en benjamins l'autre moitié reste en poussins.

Chaque année 15 nouveaux adhérents arrivent en poussins et 10 en benjamins.

À sa création, l'année zéro, le club comptait 35 poussins et 60 benjamins.

On appelle respectivement b_n et p_n les effectifs de benjamins et de poussins.

1. Définition d'une suite de matrices colonnes.

On appelle U_n la matrice colonne $U_n = \begin{pmatrix} p_n \\ b_n \end{pmatrix}$.

a) Donner la matrice U_0.

b) D'après l'énoncé, écrire p_{n+1} et b_{n+1} en fonction de p_n et b_n.

c) En déduire une égalité matricielle de la forme $U_{n+1} = AU_n + B$, où A est une matrice carrée et B une matrice colonne.

2. État stable.

a) Déterminer une matrice $X = \begin{pmatrix} x \\ y \end{pmatrix}$ telle que $AX + B = X$.

b) Si la matrice U_0 était égale à X, quel serait le comportement de la suite (U_n) ?

c) Interpréter la réponse précédente pour les effectifs du club.

3. Calcul de U_n. On admet que $A^n = \dfrac{1}{2^n}\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$.

a) On définit la suite (V_n) par $V_n = U_n - X$.
Démontrer que pour tout entier naturel n, $V_{n+1} = AV_n$.

b) Écrire V_n en fonction de V_0 et en déduire que : $U_n = A^n(U_0 - X) + X$.

4. Évolution des effectifs.

a) D'après le 3. b), déterminer les expressions de p_n et b_n en fonction de n.

b) Comment évolue l'effectif des poussins à long terme ?

Exercice 6.9

On donne les matrices $A = \begin{pmatrix} 0,2 & 0,3 \\ 0 & 0,5 \end{pmatrix}$ et $B = \begin{pmatrix} -4 \\ 8 \end{pmatrix}$.

La suite (U_n) est définie par : $U_0 = \begin{pmatrix} 3 \\ 15 \end{pmatrix}$ et $U_{n+1} = AU_n + B$.

1. Calculer la matrice $X = \begin{pmatrix} x \\ y \end{pmatrix}$ telle que $AX + B = X$.

2. Soit $V_n = U_n - X$.

a) Démontrer que pour tout entier naturel n, $V_{n+1} = AV_n$.

b) Écrire V_n en fonction de V_0.

c) En déduire l'expression de U_n en fonction de A^n, U_0 et X.

3. On admet que $A^n = \begin{pmatrix} 0,2^n & 0,5^n - 0,2^n \\ 0 & 0,5^n \end{pmatrix}$.

a) Écrire U_n en fonction de n.

b) Déterminer les limites des coefficients de U_n.

6.6 Marche aléatoire avec saut – Pertinence d'une page web

Exercice 6.10

Une petite entreprise expérimente un miniréseau intranet pour son personnel, composé de 4 pages nommées A, B, C, D.

On attribue à chaque page un indice de pertinence égal à la probabilité d'aboutir à cette page après un grand nombre de clics.

C'est ainsi que sur un sujet donné, les moteurs de recherche ordonnent les pages web par ordre de pertinence.

Partie A

Le réseau intranet de l'entreprise est représenté par le graphe probabiliste de la figure. 6.9. Les flèches indiquent des liens hypertexte entre les pages.

Lorsqu'un utilisateur est sur une page contenant des liens, on considère qu'il clique sur les liens de manière équiprobable.

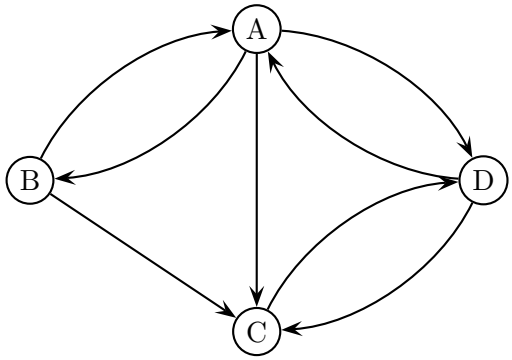


Fig. 6.9

1. Intuitivement, sans calcul, ranger les pages par ordre décroissant de fréquentation.

2. Compléter le graphe probabiliste de la figure 6.9 par des probabilités.

3. On appelle a_n, b_n, c_n, d_n les probabilités respectives d'être sur les pages A, B, C, D après n clics.

On appelle X_n la matrice $\begin{pmatrix} a_n \\ b_n \\ c_n \\ d_n \end{pmatrix}$.

Écrire la matrice T telle que $X_{n+1} = TX_n$, à partir du tableau suivant. Compléter avec des fractions.

↙	A	B	C	D
A				
B				
C				
D				

4. À l'aide de la matrice T et de la calculatrice, déterminer les probabilités :

a) de passer de B à C en trois clics ;

b) de passer de D à B en huit clics.

5. Écrire X_n en fonction de T, n, et X_0.

6. Déterminer les indices de pertinence des 4 pages de ce réseau intranet.

7. Comparer les résultats précédents à sa réponse du 1.

Partie B

Pour rendre le modèle précédent un peu plus réaliste, nous allons supposer que le comportement de l'utilisateur quand il est sur une page est le suivant :

- soit, avec une probabilité de $\frac{4}{5}$ il suit un lien de la page, comme dans la partie A ;
- soit, avec une probabilité de $\frac{1}{5}$ il accède à une page quelconque prise au hasard.

Ce type de marche aléatoire sur un graphe est nommée *marche aléatoire avec saut.*

Dans cette partie, on conserve les notations de la partie A pour les probabilités a_n, b_n, c_n, d_n, et pour la matrice X_n, mais l'égalité liant les matrices X_n et X_{n+1} sera modifiée.

1. Intuitivement, sans calcul, indiquer à quel point les indices de pertinence vont-être modifiés.

2. L'arbre de la figure 6.10 illustre le passage de l'étape n à l'étape $n+1$. Il est incomplet : il manque des branches et des probabilités.
Compléter le tracé de cet arbre. Une page entière sera nécessaire.

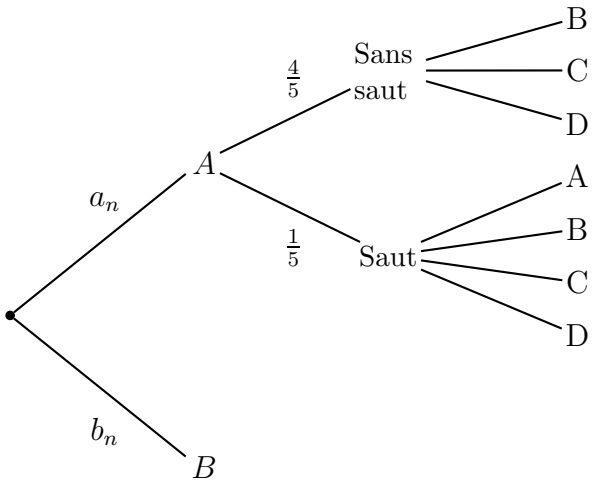


Fig. 6.10

3. Justifier que l'on obtient le système :

$$\begin{cases} a_{n+1} = \frac{4}{5}\times\left(b_n\times\frac{1}{2} + d_n\times\frac{1}{2}\right) + \frac{1}{5}\times\frac{1}{4}\times(a_n+b_n+c_n+d_n) \\ b_{n+1} = \frac{4}{5}\times\left(a_n\times\frac{1}{3}\right) + \frac{1}{5}\times\frac{1}{4}\times(a_n+b_n+c_n+d_n) \\ c_{n+1} = \frac{4}{5}\times\left(a_n\times\frac{1}{3} + b_n\times\frac{1}{2} + d_n\times\frac{1}{2}\right) + \frac{1}{5}\times\frac{1}{4}\times(a_n+b_n+c_n+d_n) \\ d_{n+1} = \frac{4}{5}\times\left(a_n\times\frac{1}{3} + c_n\right) + \frac{1}{5}\times\frac{1}{4}\times(a_n+b_n+c_n+d_n) \end{cases}$$

4. En déduire qu'on obtient alors $X_{n+1} = MX_n + P$ où M est une matrice carrée et P une matrice colonne.
Écrire les matrices M et P.

5. Calculer les nouveaux indices de pertinence des 4 pages de ce réseau intranet.

Partie C

1. Compléter le tableau ci-dessous avec les indices de pertinences obtenus dans les deux parties. Arrondir au millième près.

Page	A	B	C	D
Sans saut aléatoire (partie A)				
Avec saut aléatoire (partie B)				

2. Finalement, à quel point les indices de pertinence ont-ils été modifiés ?

6.7 Transformations géométriques

Exercice 6.11 (Bac S, Asie, juin 2013, exercice 4 de spécialité)

Un logiciel permet de transformer un élément rectangulaire d'une photographie.

Ainsi, le rectangle initial OEFG est transformé en un rectangle OE′F′G′, appelé image de OEFG.

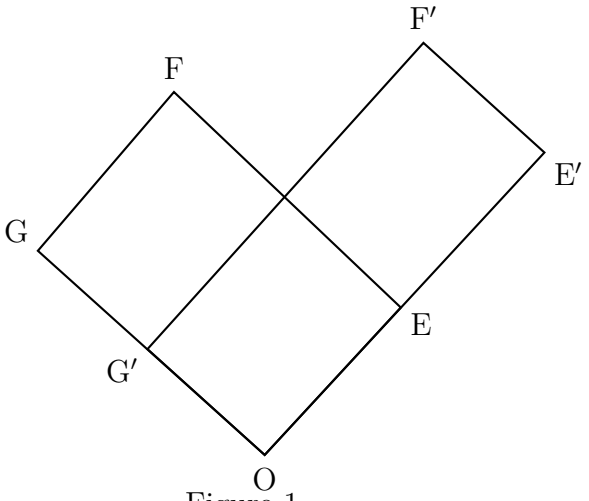


Figure 1

L'objet de cet exercice est d'étudier le rectangle obtenu après plusieurs transformations successives.

Partie A

Le plan est rapporté à un repère orthonormé $(O\ ;\ \vec{i}, \vec{j})$.

Les points E, F et G ont pour coordonnées respectives $(2\,;\,2)$, $(-1\ ;\ 5)$ et $(-3\ ;\ 3)$.

La transformation du logiciel associe à tout point $M(x\ ;\ y)$ du plan le point $M'(x'\ ;\ y')$, image du point M tel que :

$$\begin{cases} x' &= \dfrac{5}{4}x + \dfrac{3}{4}y \\ y' &= \dfrac{3}{4}x + \dfrac{5}{4}y \end{cases}$$

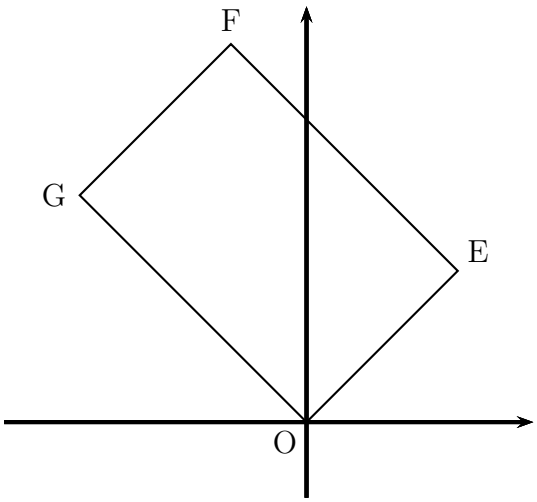


Figure 2

1. a) Calculer les coordonnées des points E′, F′ et G′, images des points E, F et G par cette transformation.

b) Comparer les longueurs OE et OE′ d'une part, OG et OG′ d'autre part.

Donner la matrice carrée d'ordre 2, notée A, telle que : $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$.

Partie B

Dans cette partie, on étudie les coordonnées des images successives du sommet F du rectangle OEFG lorsqu'on applique plusieurs fois la transformation du logiciel.

1. On considère l'algorithme suivant destiné à afficher les coordonnées de ces images successives. Une erreur a été commise.

Modifier cet algorithme pour qu'il permette d'afficher ces coordonnées.

Entrée	Saisir un entier naturel non nul N
Initialisation	Affecter à x la valeur -1 Affecter à y la valeur 5
Traitement	POUR i allant de 1 à N Affecter à a la valeur $\frac{5}{4}x + \frac{3}{4}y$ Affecter à b la valeur $\frac{3}{4}x + \frac{5}{4}y$ Affecter à x la valeur a Affecter à y la valeur b FIN POUR
Sortie	Afficher x, afficher y

2. On a obtenu le tableau suivant :

i	1	2	3	4	5	10	15
x	2,5	7,25	15,625	31,812 5	63,906 3	2 047,997 1	65 535,999 9
y	5,5	8,75	16,375	32,187 5	64,093 8	2 048,002 9	65 536,000 1

Conjecturer le comportement de la suite des images successives du point F.

Partie C

Dans cette partie, on étudie les coordonnées des images successives du sommet E du rectangle OEFG.
On définit la suite des points $E_n\,(x_n\ ;\ y_n)$ du plan par E_0 = E et la relation de récurrence :
$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix}$, où $(x_{n+1}\ ;\ y_{n+1})$ désignent les coordonnées du point E_{n+1}.
Ainsi $x_0 = 2$ et $y_0 = 2$.

1. On admet que, pour tout entier $n \geqslant 1$, la matrice A^n peut s'écrire sous la forme : $A^n = \begin{pmatrix} \alpha_n & \beta_n \\ \beta_n & \alpha_n \end{pmatrix}$.
Démontrer par récurrence que, pour tout entier naturel $n \geqslant 1$, on a :
$\alpha_n = 2^{n-1} + \dfrac{1}{2^{n+1}}$ et $\beta_n = 2^{n-1} - \dfrac{1}{2^{n+1}}$.

2. **a)** Démontrer que, pour tout entier naturel n, le point E_n est situé sur la droite d'équation $y = x$. On pourra utiliser le fait que, pour tout entier naturel n, les coordonnées $(x_n\ ;\ y_n)$ du point E_n vérifient : $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 2 \\ 2 \end{pmatrix}$.

b) Démontrer que la longueur OE_n tend vers $+\infty$ quand n tend vers $+\infty$.

6.8 Pour réviser

Chapitre du livre n° 4 – Matrices

Rubrique *Objectif bac*, corrigés page 159

- ex 50 p 116 (Vrai/Faux) : marche aléatoire sur un triangle, matrices
- ex 51 p 117 : graphe probabiliste, matrice de transition, suite de matrices

Chapitre du livre n° 5 – Suites de matrices

Les exercices résolus

- ex 1 p 131 : convergence d'une marche aléatoire
- ex 3 p 143 : suite de matrice, recherche d'un état stable

Rubrique *Pour s'exercer*, corrigés page 157

- ex 2 p 131 : graphe probabiliste à 2 sommets
- ex 4 p 143 : modèle proie-prédateur, suite de matrices colonnes $(1\,;\,2)$, $U_{n+1} = AU_n$, puis $U_{n+1} = AU_n + C$, recherche d'un état stable

Rubrique *Objectif bac*, corrigés page 159

- ex 35 p 148 : QCM
- ex 36 p 148 : Vrai/Faux, suite de matrices
- ex 37 p 148 : suite $U_{n+1} = AU_n + C$, état stable
- ex 38 p 149 : graphe probabiliste à 3 sommets, suite de matrices lignes, état stable

II Cours

6.1 Marche aléatoire sur un graphe

6.1.a Graphe probabiliste

On peut représenter différentes situations par un graphe comme celui de la figure 6.11 que l'on appelle **graphe probabiliste**.

Les lettres A et B représentent deux états, et chaque flèche représente le passage d'un état à un état.

Les nombres écrits le long des arêtes de ce graphe sont des probabilités, par exemple ici, la probabilité de passer de l'état A à l'état B est 0,2. Il s'agit d'une **probabilité conditionnelle** : la probabilité de B sachant A est 0,2, ce qui s'écrit $p_A(B) = 0,2$.
De même les autres nombres écrits le long des arêtes de ce graphe probabiliste sont des probabilités conditionnelles : $p_A(A) = 0,8 \quad p_B(A) = 0,3 \quad p_B(B) = 0,7$.

La situation de départ est l'état A ou B, et cela est représenté sur le graphe probabiliste par un objet qui se trouve en A ou en B.

À chaque étape suivante, les passages aléatoires d'un état à un autre, $A \to A$, $A \to B$, $B \to A$, $B \to A$, sont représentés par des déplacement successifs de cet objet sur ce graphe, on parle donc d'une **marche aléatoire sur un graphe**.

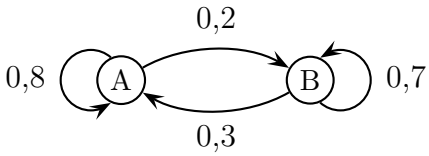


Fig. 6.11

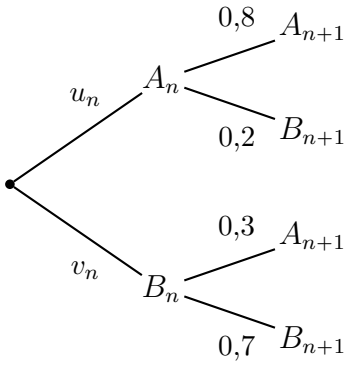


Fig. 6.12

6.1.b Arbre de probabilité, relation de récurrence

On appelle A_n l'événement « l'objet sur le graphe se trouve en A à l'étape n », et B_n l'événement « l'objet sur le graphe se trouve en B à l'étape n ».

On note : $u_n = p(A_n)$ et $v_n = p(B_n)$

Ces événements et leurs probabilités figurent sur l'arbre de la figure 6.12 qui est une autre façon de représenter la situation.

D'après cet arbre on peut calculer $p(A_{n+1})$ et $p(B_{n+1})$ en fonction de $p(A_n)$ et $p(B_n)$, c'est à dire u_{n+1} et v_{n+1} en fonction de u_n et v_n.

On obtient les égalités suivantes : $\begin{cases} u_{n+1} = 0,8u_n + 0,3v_n \\ v_{n+1} = 0,2u_n + 0,7v_n \end{cases}$

6.1.c Utilisation de matrices lignes

Le système $\begin{cases} u_{n+1} = 0,8u_n + 0,3v_n \\ v_{n+1} = 0,2u_n + 0,7v_n \end{cases}$ s'écrit sous forme matricielle ainsi :

$\begin{pmatrix} u_{n+1} & v_{n+1} \end{pmatrix} = \begin{pmatrix} u_n & v_n \end{pmatrix} \times \begin{pmatrix} 0,8 & 0,2 \\ 0,3 & 0,7 \end{pmatrix}$

On appelle alors P_n la matrice ligne $P_n = \begin{pmatrix} u_n & v_n \end{pmatrix}$ et M la matrice $\begin{pmatrix} 0,8 & 0,2 \\ 0,3 & 0,7 \end{pmatrix}$.

On a donc : $P_{n+1} = P_n M$.

La matrice ligne P_n s'appelle l'**état probabiliste** du processus, et la matrice carrée M s'appelle **la matrice de transition**.

On peut obtenir très simplement la matrice de transition à partir du graphe probabiliste en dressant le tableau ci-dessous. Le sens de la flèche en haut à gauche du tableau indique le sens de passage d'un état à un autre.

↱	A	B
A	0,8	0,2
B	0,3	0,7

6.1.d Utilisation de matrices colonnes

Cela se fait moins fréquemment mais on peut aussi utiliser des matrices colonnes, cela modifie alors l'écriture de la matrice de transition.

Le système $\begin{cases} u_{n+1} = 0,8u_n + 0,3v_n \\ v_{n+1} = 0,2u_n + 0,7v_n \end{cases}$ s'écrit sous forme matricielle ainsi :

$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} 0,8 & 0,3 \\ 0,2 & 0,7 \end{pmatrix} \times \begin{pmatrix} u_n \\ v_n \end{pmatrix}$

On appelle alors P_n la matrice colonnes $P_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$.

La matrice de transition s'écrit cette fois-ci $\begin{pmatrix} 0,8 & 0,3 \\ 0,2 & 0,7 \end{pmatrix}$.

On a donc : $P_{n+1} = MP_n$.

On obtient la matrice de transition à partir du graphe probabiliste en dressant le tableau ci-dessous. À noter le changement de sens de la flèche en haut à gauche du tableau.

↰	A	B
A	0,8	0,3
B	0,2	0,7

6.2 État stable

6.2.a Avec des matrices lignes

Reprenons l'exemple du paragraphe 6.1 en utilisant les matrices lignes du paragraphe 6.1.d.

L'état probabiliste à l'étape n est $P_n = \begin{pmatrix} u_n & v_n \end{pmatrix}$, $P_{n+1} = P_n M$, et la matrice de transition est $M = \begin{pmatrix} 0,8 & 0,2 \\ 0,3 & 0,7 \end{pmatrix}$.

Un état probabiliste stable est une matrice ligne $X = \begin{pmatrix} x & y \end{pmatrix}$ telle que $XM = X$.

On a : $XM = X \iff XM - X = 0 \iff X(M - I) = 0$

Cela se traduit par les équations

$\begin{cases} -0,2x + 0,2y = 0 \\ 0,3x - 0,3y = 0 \end{cases}$

Ces deux équations sont équivalentes à $x-y=0$, autrement dit $x=y$, et nous n'avons apparemment qu'une équation.
On sait d'autre part que, puisque la matrice $X=\begin{pmatrix}x & y\end{pmatrix}$ est un état probabiliste, on a $x+y=1$.
On résout donc le système $\begin{cases} x=y \\ x+y=1 \end{cases}$ et on obtient $x=y=0,5$.
Donc : $X=\begin{pmatrix}0,5 & 0,5\end{pmatrix}$

6.2.b Avec des matrices colonnes

Un état probabiliste stable est une matrice colonne $X=\begin{pmatrix}x\\y\end{pmatrix}$ telle que $MX=X$.
On a : $MX=X \iff MX-X=0 \iff (M-I)X=0$
On procède ensuite comme au paragraphe précédent.

6.3 État stable pour une suite de matrices colonnes

6.3.a Existence et calcul de l'état stable

Pour une suite de matrice colonnes (U_n) définie par $U_{n+1}=AU_n+B$, un état stable est une matrice colonne X telle que $X=AX+B$.
$X=AX+B \iff (I-A)X=B$
Par conséquent :

Propriété 6.1

Il existe un état stable si et seulement si la matrice carrée $I-A$ est inversible, et dans ce cas : $X=(I-A)^{-1}B$.

6.3.b Étude de la convergence.

À partir des égalités $U_{n+1}=AU_n+B$ et $X=AX+B$, on peut écrire :
$U_{n+1}-X=AU_n+B-(AX+B)=AU_n+B-AX-B=AU_n-AX=A(U_n-X)$
Donc, si l'on pose $V_n=U_n-X$, on a $V_{n+1}=AV_n$.
On démontre alors par récurrence que : $V_n=A^nV_0$, puis on prouve que : $U_n=A^n(U_0-X)+X$.
Cela permet d'obtenir les coefficients de la matrice U_n en fonction de n et de déterminer si ces coefficients tendent vers une limite ou non.

6.3.c État stable et convergence.

Propriété 6.2

Si la suite (U_n) converge, alors il existe un état stable X et la limite de la suite (U_n) est X.

Justification
Si la suite (U_n) converge vers une limite L, la suite U_{n+1} converge aussi vers L.
Or : $U_{n+1}=AU_n+B$, donc, par unicité de la limite $L=AL+B$.

Remarque importante
La réciproque est fausse, autrement dit l'existence d'un état stable ne prouve pas la convergence.

Index