

Mathématiques pour l'informatique

Pour le BTS SIO

Xavier Chanet

Professeur agrégé de mathématiques

Patrick Vert

Ancien professeur agrégé de mathématiques

3^e édition

DUNOD

Illustration de couverture : © agsandrew – Shutterstock.com

<p>Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.</p> <p>Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements</p>	<p>d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.</p> <p>Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).</p>
--	--



© Dunod, 2015, 2018, 2021

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-082870-8

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2^o et 3^o a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

TABLE DES MATIÈRES

Avant-propos	VI
PARTIE I	
<hr/> MATHÉMATIQUES	
Chapitre 1 ■ Arithmétique	3
1.1 Numération et conversion	3
1.2 Divisibilité des entiers	8
1.3 Nombres premiers	8
1.4 Congruences	11
TD – Le codage affine	13
Exercices corrigés	16
Chapitre 2 ■ Calcul matriciel	41
2.1 Généralités	41
2.2 Calcul matriciel élémentaire	42
2.3 Inverse d'une matrice carrée	48
2.4 Résolution de systèmes à l'aide de matrices	49
Exercices corrigés	50
Chapitre 3 ■ Logique	69
3.1 Calcul des propositions	69
3.2 Calcul des prédicats	74
3.3 Calcul booléen	77
TD – Expression booléenne	82
Exercices corrigés	85
Chapitre 4 ■ Ensembles	105
4.1 Langage ensembliste	105
4.2 Relations binaires	108
4.3 Applications d'un ensemble dans un ensemble	110

TD – Relation binaire dans un ensemble	113
Exercices corrigés	116
Chapitre 5 ■ Graphes et ordonnancement	133
5.1 Représentations d'un graphe	133
5.2 Chemins d'un graphe	136
5.3 Niveau des sommets d'un graphe sans circuit	141
5.4 Méthode MPM d'ordonnancement d'un graphe	144
TD – Déplacements dans un jeu vidéo	149
Exercices corrigés	152
Chapitre 6 ■ L'examen de mathématiques	169
Sujet n° 1	169
Sujet n° 2	172

PARTIE II

ALGORITHMIQUE APPLIQUÉE

Chapitre 7 ■ Premiers pas	177
7.1 Qu'est-ce qu'un algorithme ?	181
7.2 Le logiciel Python	182
Chapitre 8 ■ Concepts fondamentaux	179
8.1 Données : types et opérations	183
8.2 Stockage des données	188
8.3 Lecture et écriture des données	190
8.4 Instructions conditionnelles	192
8.5 Instructions itératives	193
8.6 Fonctions et procédures	196
8.7 Compléments : Récursivité	200
Exercices corrigés	202
Chapitre 9 ■ Travaux pratiques guidés	219
9.1 Numéro d'un(e) salarié(e) dans une entreprise	219
9.2 Codage hexadécimal d'un texte	221
9.3 Génération d'un mot de passe	224
Chapitre 10 ■ Travaux pratiques	223
10.1 Nombres parfaits	223
10.2 Évolution d'un salaire	226
10.3 Nombres premiers palindromes	229
10.4 Calcul formel	232

10.5 Calcul matriciel	234
10.6 Opérations sur les ensembles	238
10.7 Méthodes de tri	241
10.8 Cryptographie : chiffre de César	244
10.9 Cryptographie : chiffre des scouts sud-africains	247
Chapitre 11 ■ L'examen d'algorithmique	251
Examen 1 – Remplissage d'une tirelire	252
Examen 2 – La suite de Syracuse	256
Examen 3 – Calcul formel sur des entiers	260
PARTIE III	
<hr/>	
ANNEXE	
Exercices supplémentaires	267
Index	297

Ressources numériques

Le **code source** des exemples est disponible gratuitement en téléchargement à l'adresse suivante : <https://dunod.com/EAN/9782100828708>

AVANT-PROPOS

Ce livre s'adresse en premier lieu aux étudiants de première et de deuxième année préparant le BTS SIO (Services informatiques aux organisations). Il pourra également intéresser les étudiants en IUT d'informatique, ou ceux en classe préparatoire souhaitant acquérir les bases de l'algorithmique, ainsi que tous ceux qui souhaitent connaître et maîtriser les outils mathématiques nécessaires à une bonne pratique de la programmation informatique.

Les auteurs, tous deux ayant une solide expérience d'enseignement en BTS SIO, ont rédigé cet ouvrage dans le respect le plus strict des derniers programmes en vigueur. L'objectif pédagogique majeur est de fournir un outil d'accompagnement dans les apprentissages, pouvant être utilisé en classe par le professeur ou de manière plus personnelle par l'étudiant.

Dans la partie *Mathématiques*, on trouvera, dans chaque chapitre, le cours, présentant les notions essentielles du programme, des exercices, nombreux et variés, corrigés ou non, allant des applications directes du cours à des problèmes plus complexes pour se perfectionner, et des travaux dirigés corrigés. Deux sujets corrigés d'examen ponctuent cette partie.

Dans la partie *Algorithmique appliquée*, où les instructions et algorithmes sont exécutés en langage Python, on commence par présenter expérimentalement, avec les activités dites « de découverte », les fondamentaux de l'algorithmique. L'étudiant peut ensuite vérifier qu'il maîtrise les concepts clés en résolvant les nombreux exercices, corrigés ou non. Une série de travaux pratiques, tous corrigés, montrent comment résoudre des problèmes par l'utilisation judicieuse de solutions algorithmiques. On trouve enfin trois exemples de sujets officiels d'examen d'algorithmique appliquée, corrigés.

Partie 1

Mathématiques

PLAN

- 1.1 Numération et conversion
- 1.2 Divisibilité des entiers
- 1.3 Nombres premiers
- 1.4 Congruences

OBJECTIFS

- Présenter les grandes notions arithmétiques utiles à l'informatique.
- Maîtriser les principes de numération indispensables aux langages de bas niveau.
- Maîtriser les outils d'arithmétique modulaire utiles à l'algorithmique.

1.1 NUMÉRATION ET CONVERSION

1.1.1 Rappels sur la division euclidienne

Les **entiers naturels** sont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, etc.

Effectuer la **division euclidienne** d'un entier naturel A par un entier naturel B non nul c'est déterminer les uniques entiers Q (appelé **quotient**) et R (appelé **reste**) tels que : $A = BQ + R$ et $0 \leq R < B$.

Exemples

Le quotient et le reste de la division euclidienne de $A = 53$ par $B = 6$ sont respectivement $Q = 8$ et $R = 5$. En effet, $53 = 6 \times 8 + 5$ et $0 \leq 5 < 6$.

Dans la division euclidienne de 1 893 par 11, le quotient vaut 172 et le reste vaut 1.

On peut obtenir ces résultats en posant la division ou avec une calculatrice.

1.1.2 Numération des entiers

L'être humain compte naturellement **en base 10** (avec les dix chiffres) : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ... , 97, 98, 99, 100, 101, 102, etc.



On peut compter **en base 2** (on n'utilise que les chiffres 0 et 1) : 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, etc.

Pour compter **en base 16**, on utilise les dix chiffres et on en rajoute six autres (que l'on note *A, B, C, D, E* et *F*). Cela donne : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A, B, C, D, E, F*, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, *1A, 1B, 1C, 1D, 1E, 1F*, 20, 21, 22, etc.

Exemples

4 en base 10, c'est 100 en base 2.
A en base 16, c'est 10 en base 10.

9 en base 10, c'est 1001 en base 2.
1A en base 16, c'est 26 en base 10.



Le microprocesseur d'un ordinateur ne travaille qu'avec deux chiffres : 0 (pas de courant) et 1 (courant). Les calculs s'y font donc naturellement en base 2.

Le nombre 23, écrit en base 10, se note 10111 en base 2 et 17 en base 16, mais on ne peut pas écrire $23 = 10111 = 17$.

C'est pourquoi nous adoptons la **notation** $(n)_p$ pour indiquer que le nombre n est écrit en base p : $(23)_{10} = (10111)_2 = (17)_{16}$.

Les écritures en bases 2, 10 et 16 s'appellent aussi respectivement les écritures **binaire, décimale et hexadécimale**.

Lorsqu'un nombre est écrit en base 10, on peut simplifier la notation $(x)_{10}$. Par exemple $(201)_{10}$ peut s'écrire simplement 201.



L'écriture d'un nombre entier en base 2, 10 ou 16 est unique.

Pour convertir un entier d'une base à l'autre, il est important de comprendre la relation algébrique que l'on a entre une base p et l'écriture du nombre dans cette base p . C'est ce qu'énonce la propriété suivante.

Propriété 1.1

Quels que soient les nombres entiers $a_0, a_1, a_2, \dots, a_n$ compris entre 0 et $p - 1$, où p désigne 2, 10 ou 16, on a :

$$(a_n \dots a_2 a_1 a_0)_p = a_n \times p^n + \dots + a_2 \times p^2 + a_1 \times p + a_0$$

Dans le cas où $p = 16$, on remplace dans l'écriture du membre de gauche, tout a_i égal à 10, 11, 12, 13, 14 ou 15 par *A, B, C, D, E* ou *F* respectivement.

Exemple

Conversion vers la base 10 :

$$(11011)_2 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1 = 16 + 8 + 2 + 1 = 27$$

$$(5C8)_{16} = 5 \times 16^2 + 12 \times 16 + 8 = 1\,280 + 192 + 8 = 1\,480$$

Il existe plusieurs méthodes pour convertir un entier vers la base $p = 2$ ou 16. Nous allons déterminer l'écriture en base 2 du nombre 75 et l'écriture en base 16 du nombre 2 014 (méthodes 1 et 2), puis effectuer des conversions directes entre les bases 2 et 16 (méthode 3).

Méthode 1 : on effectue la division euclidienne du nombre par la plus grande puissance de p qui lui est inférieure ou égale, puis on recommence avec le reste et ainsi de suite jusqu'à ce qu'il soit nul.

$$75 = 1 \times 2^6 + 11, 11 = 1 \times 2^3 + 3 \text{ et } 3 = 1 \times 2 + 1$$

$$\text{Donc } 75 = 1 \times 2^6 + 1 \times 2^3 + 1 \times 2 + 1$$

$$= 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1$$

$$= (1001011)_2$$

$$\text{De même } 2\,014 = 7 \times 16^2 + 222 \text{ et } 222 = 13 \times 16 + 14$$

$$\text{d'où } 2\,014 = 7 \times 16^2 + 13 \times 16 + 14 = (7DE)_{16}$$

Méthode 2 : on effectue la division euclidienne du nombre par p puis on recommence avec le quotient et ainsi de suite jusqu'à obtenir 0. À la fin, on inverse l'ordre des restes obtenus.

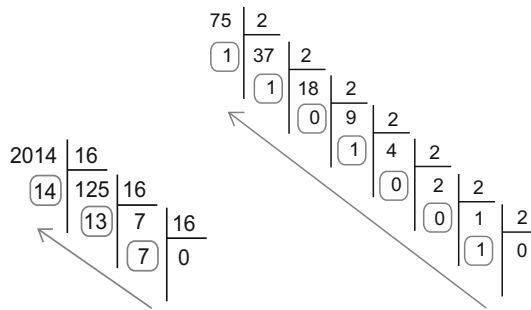


Figure 1.1

Ainsi, on retrouve $2\,014 = (7DE)_{16}$ et $75 = (1001011)_2$.

Méthode 3 : on peut passer directement de la base 2 à la base 16, et inversement, en utilisant le tableau de conversion suivant :

Base 16	0	1	2	3	4	5	6	7
Base 2	0000	0001	0010	0011	0100	0101	0110	0111
Base 16	8	9	A	B	C	D	E	F
Base 2	1000	1001	1010	1011	1100	1101	1110	1111

Conversion directe de $(2B)_{16}$ en base 2 :

$$(2B)_{16} = (00101011)_2 = (101011)_2$$

On ajoute, à partir du tableau, les écritures de 2 et de B en base 2, puis on supprime les zéros inutiles.

Conversion directe de $(110111)_2$ en base 16 :

$$(110111)_2 = (00110111)_2 = (37)_{16}$$

On ajoute à gauche des zéros inutiles pour « faire des paquets » de quatre chiffres que l'on remplace ensuite par leurs équivalents en base 16.



Puisque l'écriture en base 2 d'un nombre peut être très « longue » et du fait de la simplicité de conversion entre les bases 2 et 16, on utilise beaucoup le **système hexadécimal** en informatique.



Les calculatrices permettent de convertir un nombre d'une base à l'autre.

1.1.3 Numération des réels

Dans le dernier paragraphe, nous avons défini les écritures binaire, décimale et hexadécimale d'un nombre entier. Plus largement, tout nombre réel peut être écrit en base 2, 10 ou 16.

Pour comprendre, prenons l'exemple de deux réels et de la base 10 :

$$(53,627)_{10} = 5 \times 10 + 3 + 6/10 + 2/10^2 + 7/10^3$$

$$(456,905)_{10} = 4 \times 10^2 + 5 \times 10 + 6 + 9/10 + 0/10^2 + 5/10^3$$

Plus généralement on a la propriété suivante.

Propriété 1.2

Quels que soient les nombres entiers a_0, \dots, a_n et b_1, \dots, b_m compris entre 0 et $p - 1$ (où p désigne 2, 10 ou 16), on a :

$$(a_n \dots a_0, b_1 \dots b_m)_p = a_n \times p^n + \dots + a_2 \times p^2 + a_1 \times p + a_0 + \frac{b_1}{p} + \frac{b_2}{p^2} + \dots + \frac{b_m}{p^m}$$

Dans le cas où $p = 16$, on remplace dans l'écriture du membre de gauche, tout a_i ou b_i égal à 10, 11, 12, 13, 14 ou 15 par A, B, C, D, E ou F respectivement.

Exemple

$$7,25 \text{ en base 2 : } 7,25 = 7 + 0,25 = 1 \times 2^2 + 1 \times 2 + 1 + 1/2^2 = (111,01)_2$$

$$(101,11)_2 \text{ en base 10 : } (101,11)_2 = 1 \times 2^2 + 0 \times 2 + 1 + 1/2 + 1/2^2 = 5,75$$

$$(B,3C)_{16} \text{ en base 10 : } (B,3C)_{16} = 11 + 3/16 + 12/16^2 = 11,234375$$

1.1.4 Opérations élémentaires

En base 2 ou 16, on pose les opérations de la même manière qu'en base 10.

- L'**addition** : exemple $(101)_2 + (1110)_2 = (10011)_2$ (en base 10, cela donne $5 + 14 = 19$).

$$\begin{array}{r}
 1 \ 1 \quad \quad \quad | \quad (1)_2 + (0)_2 = (1)_2 \\
 + \ 1 \ 1 \ 1 \ 0 \ 1 | \quad (0)_2 + (1)_2 = (1)_2 \\
 \hline
 1 \ 0 \ 0 \ 1 \ 1 | \quad (1)_2 + (1)_2 = (10)_2 : \text{on pose 0, on retient 1.} \\
 \quad \quad \quad \quad | \quad (1)_2 + (1)_2 = (10)_2 : \text{on pose 0, on retient 1.}
 \end{array}$$

- La **soustraction** : exemple $(10110)_2 - (111)_2 = (1111)_2$ (en base 10 cela donne $22 - 7 = 15$).

$$\begin{array}{r}
 \quad \quad 1 \ 1 \ 1 \ 1 \quad | \quad \text{Puisque } 1 > 0, \text{ on pose une retenue de 1,} \\
 \ 1 \ 0 \ 1 \ 1 \ 0 \quad | \quad \text{puis } (10)_2 - (1)_2 = (1)_2. \\
 - \quad \quad 1 \ 1 \ 1 \quad | \quad \text{Nouvelle retenue de 1 puis } (11)_2 - ((1)_2 + (1)_2) = (1)_2, \text{ etc.} \\
 \hline
 1 \ 1 \ 1 \ 1 \quad | \\
 \hline
 0 \ 1 \ 1 \ 1 \ 1 \quad |
 \end{array}$$

- La **multiplication** : exemple $(F3)_{16} \times (2A)_{16} = (27DE)_{16}$ (en base 10 cela donne $42 \times 243 = 10\ 206$).

$$\begin{array}{r}
 \quad \quad \quad \mathbf{F \ 3} \\
 \times \quad \mathbf{2 \ A} \\
 \hline
 9 \ 7 \ E \\
 + 1 \ E \ 6 \ . \\
 \hline
 2 \ 7 \ D \ E
 \end{array}
 \left| \begin{array}{l}
 (A)_{16} \times (3)_{16} = 10 \times 3 = 30 = (1E)_{16}, \text{ on pose E, on retient 1.} \\
 (A)_{16} \times (F)_{16} = 10 \times 15 = 150 = (96)_{16}, \text{ avec la retenue, on obtient,} \\
 (96)_{16} + (1)_{16} = (97)_{16}, \text{ d'où } 97E. \\
 (2)_{16} \times (3)_{16} = (6)_{16}, \text{ on pose 6.} \\
 (2)_{16} \times (F)_{16} = 2 \times 15 = 30 = (1E)_{16}, \text{ on obtient } 1E6 \text{ avec le décalage} \\
 \ll \cdot \gg. \\
 \text{On effectue ensuite l'addition } (97E)_{16} + (1E60)_{16} : (E)_{16} + (0)_{16} = (E)_{16}, \\
 \text{on pose E ; } (7)_{16} + (6)_{16} = 7 + 6 = 13 = (D)_{16}, \text{ on pose D ; } (9)_{16} + (E)_{16} \\
 = 9 + 14 = 23 = (17)_{16}, \text{ on pose 7 et on retient 1 ; enfin, } (1)_{16} + (1)_{16} \\
 = (2)_{16}, \text{ on obtient alors le résultat } 27DE.
 \end{array}$$

- La **division** : exemple $(110)_2 \div (11)_2 = (10)_2$ (en base 10 cela donne $6 \div 3 = 2$).

$$\begin{array}{r}
 1 \ 1 \ 0 \quad | \quad 1 \ 1 \\
 - 1 \ 1 \quad | \quad \hline
 \quad \quad 0 \ 0 \quad | \quad 1 \ 0 \\
 \quad \quad - 0 \ 0 \quad | \\
 \quad \quad \quad \quad 0 \ 0 \quad |
 \end{array}
 \left| \begin{array}{l}
 \text{On sélectionne les deux premiers chiffres de } 110. \text{ Dans } (11)_2 \text{ on a une fois } (11)_2 \text{ et il reste } 0. \text{ On pose alors } 1 \text{ au} \\
 \text{quotient. On abaisse ensuite le } 0 \text{ de } 110. \text{ On obtient } 00. \\
 \text{Dans } (00)_2 \text{ on a zéro fois } (11)_2 \text{ et il reste } 0. \text{ On pose } 0 \text{ au} \\
 \text{quotient, ce qui termine la division.}
 \end{array}$$

1.1.5 Précision et arrondi

Considérons le nombre $N = 432,615$:

- L'arrondi à **10** près de N est 430 (car ce nombre est plus proche de N que 440).
- L'arrondi à **1** près de N est 433 (car ce nombre est plus proche de N que 432).
- L'arrondi à **0,1** près de N est 432,6 (car ce nombre est plus proche de N que 432,7).
- L'arrondi à **0,01** près de N est 432,62 (ce nombre est aussi plus proche de N que 432,61 et dans un tel cas on prend le plus grand).

Cette **notion d'arrondi** se généralise aux nombres réels écrits dans n'importe quelle base p : l'arrondi d'un nombre réel x à une certaine précision est le nombre le plus proche de x tel que tous les chiffres allant au-delà de cette précision soient nuls. Par convention, lorsqu'il existe deux nombres possibles, l'arrondi est alors le plus grand.

Considérons les nombres $N = (101,10011)_2$ et $M = (B82A,7AB)_{16}$:

- L'arrondi à $(10)_2$ près de N est $(110)_2$ car ce nombre est plus proche de N que $(100)_2$.
- L'arrondi à $(0,1)_2$ près de N est $(101,1)_2$ car ce nombre est plus proche de N que $(110,0)_2$.
- L'arrondi à $(100)_{16}$ près de M est $(B800)_{16}$ car ce nombre est plus proche de M que $(B900)_{16}$.
- L'arrondi à $(0,1)_{16}$ près de M est $(B82A,8)_{16}$ car ce nombre est plus proche de M que $(B82A,7)_{16}$.

1.2 DIVISIBILITÉ DES ENTIERS

Soient a et b des entiers naturels. a est **divisible** par b s'il existe un entier naturel k tel que : $a = bk$.

On dit alors que b divise a , que b est un **diviseur** de a et que a est un **multiple** de b .

Exemple

$65 = 13 \times 5$ donc on peut dire que 65 est divisible par 13 (et par 5 aussi), que 13 et 5 sont des diviseurs de 65 et que 65 est un multiple de 13 (et de 5 aussi).

Propriété 1.3

- Si a est divisible par b alors tout multiple de a est divisible par b .
- Si a est divisible par b et si b est divisible par c , alors a est divisible par c .
- Si a et b sont divisibles par c , alors $a+b$ et $a-b$ sont divisibles par c .

Les démonstrations de ces propriétés seront proposées dans l'exercice corrigé **1.20**.

1.3 NOMBRES PREMIERS

1.3.1 Reconnaissance des nombres premiers

Un **entier naturel** est premier s'il a exactement deux diviseurs : 1 et lui-même.

- 0 n'est pas premier car il possède une infinité de diviseurs.
- 1 n'est pas premier car il n'a qu'un seul diviseur : 1.
- 2 est **premier** car il a exactement deux diviseurs : 1 et 2.
- 3 est **premier** car il a exactement deux diviseurs : 1 et 3.

Théorème 1.1

Soit n un entier naturel supérieur ou égal à 2.

Si n n'est pas premier, alors n possède au moins un diviseur premier inférieur ou égal à \sqrt{n} .

Ce théorème permet d'avoir un critère de reconnaissance des nombres premiers : pour savoir si un nombre n est premier, on calcule \sqrt{n} . Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à \sqrt{n} , alors n est premier.



Mémorisez les nombres premiers inférieurs à 20, ils vous seront utiles par la suite : 2, 3, 5, 7, 11, 13, 17 et 19.

Exemple

Cherchons si 347 et 713 sont des nombres premiers :

$\sqrt{347} \approx 18,6$. Les nombres premiers inférieurs ou égaux à 18,6 sont 2, 3, 5, 7, 11, 13 et 17. 347 n'est divisible par aucun d'eux donc **347 est premier**.

$\sqrt{713} \approx 26,7$. Les nombres premiers inférieurs ou égaux à 26,7 sont 2, 3, 5, 7, 11, 13, 17, 19 et 23. 713 est divisible par 23 donc **713 n'est pas premier**.

1.3.2 Décomposition d'un nombre en produit de facteurs premiers

Un nombre qui n'est pas premier peut être divisible par un nombre premier, et même s'écrire uniquement avec des nombres premiers, sous forme de produit.

Théorème 1.2

Tout entier naturel supérieur ou égal à 2 se décompose de façon unique en un produit de facteurs premiers.

Exemple

84 n'est pas premier, il se décompose en un produit de facteurs premiers, cette décomposition est unique, à l'ordre des facteurs près :

$$84 = 2 \times 42 = 2 \times 6 \times 7 = 2 \times 2 \times 3 \times 7 = 2^2 \times 3 \times 7$$

975 n'est pas premier, il se décompose en un produit de facteurs premiers :

$$975 = 5 \times 195 = 5 \times 5 \times 39 = 5 \times 5 \times 3 \times 13 = 3 \times 5^2 \times 13$$

En pratique, on divise le nombre par son **plus petit diviseur premier**, et on recommence jusqu'à ce que le quotient soit 1.

84	2	975	3
42	2	325	5
21	3	65	5
7	7	13	13
1		1	

La décomposition d'un nombre en produit de facteurs premiers permet d'obtenir tous ses diviseurs. Par exemple, $84 = 2^2 \times 3 \times 7$, un diviseur de 84 s'écrit donc : $2^i \times 3^j \times 7^k$ avec $0 \leq i \leq 2, 0 \leq j \leq 1, 0 \leq k \leq 1$.

En utilisant l'algorithme suivant, on obtient les 12 diviseurs de 84 qui sont 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 et 84.

```

Variables : i, j, k (entiers)
Début
  Pour i de 0 à 2 Faire
    Pour j de 0 à 1 Faire
      Pour k de 0 à 1 Faire
        Afficher  $2^i \times 3^j \times 7^k$ 
      FinPour
    FinPour
  FinPour
Fin
    
```

1.3.3 PGCD de deux entiers naturels non nuls

Étant donné deux entiers naturels non nuls a et b , il existe un diviseur commun à a et à b qui est plus grand que tous les autres. Ce diviseur est appelé **Plus Grand Commun Diviseur** et se note $\text{PGCD}(a;b)$.



Deux entiers naturels non nuls sont **premiers entre eux** si et seulement si leur PGCD est égal à 1.

Exemples

Les diviseurs de 45 sont 1, 3, 5, 9, 15 et 45. Ceux de 105 sont 1, 3, 5, 7, 15, 21, 35 et 105. Les diviseurs communs à 45 et 105 sont 1, 3, 5, 15.

Le plus grand d'entre eux est 15 donc 15 est le PGCD de 45 et 105.

On écrit $\text{PGCD}(45;105) = 15$.

Les diviseurs de 15 sont 1, 3, 5 et 15. Ceux de 44 sont 1, 2, 4, 11, 22 et 44.

Le seul diviseur commun à 15 et à 44 est 1. Il est leur PGCD.

Donc $\text{PGCD}(15;44) = 1$.

15 et 44 sont premiers entre eux.

Propriété 1.4

Soient a et b deux entiers naturels supérieurs ou égaux à 2 dont on connaît les décompositions en produits de facteurs premiers :

- s'ils n'ont pas de facteur commun, alors leur PGCD est 1 ;
- sinon, leur PGCD est le produit des facteurs communs aux deux décompositions, chaque facteur étant affecté du plus petit exposant avec lequel il figure dans les deux décompositions.

Exemples

Soient $a = 4\,950 = 2 \times 3^2 \times 5^2 \times 11$ et $b = 4\,875 = 3 \times 5^3 \times 13$.

Les facteurs communs aux deux décompositions sont 3 et 5.

3 figure avec les exposants 2 et 1, on garde le plus petit, c'est-à-dire 1.

5 figure avec les exposants 2 et 3, on garde le plus petit, c'est-à-dire 2.

Donc $\text{PGCD}(4\,950; 4\,875) = 3 \times 5^2 = 75$.

Soient $a = 2^4 \times 3 \times 5^2 \times 7 \times 19$ et $b = 2^3 \times 3^2 \times 7^2 \times 17$. Les facteurs communs aux deux décompositions sont 2, 3 et 7. Les plus petits exposants sont 3 pour le facteur 2, 1 pour le facteur 3 et 1 pour le facteur 7.

Donc $\text{PGCD}(a; b) = 2^3 \times 3 \times 7$.

Propriété 1.5

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

Soit r le reste de la division euclidienne de a par b .

Alors $\text{PGCD}(a; b) = \text{PGCD}(b; r)$

Cette propriété (1.5) permet d'avoir une autre méthode pour chercher un PGCD. On applique plusieurs fois la propriété jusqu'à obtenir un reste nul. Le PGCD est alors le dernier diviseur essayé.

Son avantage est qu'elle est algorithmique, donc programmable. Elle est connue sous le nom **d'algorithme d'Euclide**.

Exemple

$\text{PGCD}(420; 182) = \text{PGCD}(182; 56)$ car 56 est le reste de la division euclidienne de 420 par 182.

$\text{PGCD}(182; 56) = \text{PGCD}(56; 14)$ car 14 est le reste de la division euclidienne de 182 par 56.

Le reste de la division euclidienne de 56 par 14 est 0, donc 14 est le PGCD de 420 et 182.

1.4 CONGRUENCES

Soit n un entier naturel non nul. On dit que deux entiers naturels a et b sont **congrus modulo n** si et seulement si a et b ont le même reste dans la division euclidienne par n . On écrit alors $a \equiv b[n]$ ou $b \equiv a[n]$.

Quel que soit a entier, $a \equiv a[n]$ et $a \equiv r[n]$, r étant le reste de la division euclidienne de a par n .

Exemples

$$101 = 7 \times 14 + 3 \text{ et } 66 = 7 \times 9 + 3$$

donc 101 et 66 sont congrus modulo 7 car ils ont le même reste dans les divisions euclidiennes par 7. On peut donc écrire $101 \equiv 66 [7]$.

$$67 = 12 \times 5 + 7 \text{ et } 139 = 12 \times 11 + 7$$

donc $67 \equiv 139 [12]$ car le reste est le même dans les divisions euclidiennes par 12. $29 = 8 \times 3 + 5$ donc $29 \equiv 5 [8]$.

90 et 80 ne sont pas congrus modulo 11, car les restes dans les divisions euclidiennes par 11 sont 2 et 3.

Propriété 1.6

Soient a et b deux entiers naturels tels que $a > b$ et soit n un entier naturel non nul. a est congru à b modulo n si et seulement si $a - b$ est multiple de n .

En effet, si $a \equiv b[n]$ alors a et b ont le même reste r dans la division euclidienne par n .

Donc on a $a = nq + r$ et $b = nq' + r$ puis $a - b = (nq + r) - (nq' + r) = nq - nq' = n(q - q')$ qui est un multiple de n puisque $q - q'$ est un entier.

Propriété 1.7

Soient a, b, c, d des entiers naturels et n un entier naturel non nul.

Si $a \equiv b[n]$ et $c \equiv d[n]$ alors :

- $a + c \equiv b + d[n]$ et $a - c \equiv b - d[n]$
- $pa \equiv pb[n]$ pour tout entier naturel p
- $ac \equiv bd[n]$
- $a^p \equiv b^p[n]$ pour tout entier naturel p

Des démonstrations de certaines de ces propriétés sont proposées dans l'exercice corrigé 1.45.

Exemples

À partir des congruences $2\ 014 \equiv 1[3]$ et $1\ 000 \equiv 1[3]$, les propriétés précédentes permettent d'obtenir facilement d'autres congruences :

$$2\ 014 + 1\ 000 \equiv 1 + 1[3] \text{ c'est-à-dire } 3\ 014 \equiv 2[3]$$

$$20 \times 2\ 014 \equiv 20 \times 1[3] \text{ c'est-à-dire } 40\ 280 \equiv 20[3] \text{ donc } 40\ 280 \equiv 2[3]$$

$$2\ 014 \times 1\ 000 \equiv 1 \times 1[3] \text{ c'est-à-dire } 2\ 014\ 000 \equiv 1[3]$$

$2\ 014^{70} \equiv 1^{70}[3]$ c'est-à-dire $2\ 014^{70} \equiv 1[3]$ (sur cet exemple, on vient de montrer très facilement que le reste de la division euclidienne de $2\ 014^{70}$ par 3 est 1, ce qui n'avait rien d'évident...).

TD - Le codage affine

Le chiffrement affine est une méthode simple de codage d'un message. À chaque lettre de l'alphabet, on commence par associer son rang dans l'alphabet, diminué de 1, comme l'indique le tableau 1.1. On obtient un entier x entre 0 et 25.

Tableau 1.1

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

Le codage affine nécessite deux clés a et b , qui sont des entiers naturels compris entre 0 et 25. On calcule alors le reste de $ax + b$ dans la division euclidienne par 26. On obtient un entier y tel que $y \equiv ax + b[26]$. On cherche à quelle lettre correspond cet entier y . Cette lettre code alors la lettre de départ.

Partie A

Dans cette partie, on choisit les clés $a = 3$ et $b = 11$. La fonction de codage est donc $y \equiv 3x + 11[26]$.

1. Montrer que G est codé par D. Comment est codé S ?
2. Remplir le tableau 1.2.

Tableau 1.2

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x							6						
y							3						
Codage							D						
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x													
y													
Codage													

3. Quel mot est codé par VBUTSB ?
4. On va maintenant chercher la fonction de décodage, c'est-à-dire l'expression de x en fonction de y . Chercher l'inverse de 3 modulo 26, c'est-à-dire le nombre entier k tel que $0 \leq k \leq 25$ et $3k \equiv 1[26]$. En déduire la fonction de décodage.

Partie B

Dans cette partie, on choisit $a = 7$ et $b = 12$.

1. Comment va-t-on coder le mot AFFINE ?
2. Déterminer la fonction de décodage.
3. Décoder le message CBMNJ QISO.

Partie C

Dans cette partie, on ne connaît pas les clés de codage a et b . On sait que E est codé par I et que V est codé par T.

1. Écrire les deux congruences vérifiées par a et b .
2. Montrer que $17a \equiv 11[26]$. Déterminer a puis b , puis la fonction de codage.
3. Déterminer la fonction de décodage.

Solution du TD

Partie A

1. Pour la lettre **G**, on a $x = 6$. $3x + 11 = 29$. Comme $29 \equiv 3[26]$, alors $y = 3$ ce qui correspond à la lettre **D**. **G** est donc codé par **D**.
Pour **S**, $x = 18$, $3x + 11 = 65 \equiv 13[26]$ donc $y = 13$. **S** est donc codé par **N**.
- 2.

Tableau 1.3

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

3. Pour décoder le mot **VBUTSB**, il suffit de repérer les correspondances du tableau. Le mot codé par VBUTSB est **MODULO**.

4. L'inverse de 3 est 9 modulo 26, car $3 \times 9 = 27 \equiv 1[26]$.
 $y \equiv 3x + 11[26] \Rightarrow 9y \equiv 27x + 99[26] \Rightarrow 9y \equiv x + 21[26]$
 $\Rightarrow 9y - 21 \equiv x[26] \Rightarrow x \equiv 9y + 5[26]$.

La fonction de décodage est donc $x \equiv 9y + 5[26]$. Par exemple, pour décoder la lettre D, on a $y = 3$, $9y + 5 = 32 \equiv 6[26]$, donc $x = 6$, ce qui correspond à la lettre G.

Partie B

1. La fonction de codage est $y \equiv 7x + 12[26]$. AFFINE se code MVVQZO.

Tableau 1.4

Lettre	A	F	I	N	E
x	0	5	8	13	4
y	12	21	16	25	14
Codage	M	V	Q	Z	O

2. L'inverse de 7 modulo 26 est 15 car $7 \times 15 = 105 \equiv 1[26]$
 $y \equiv 7x + 12[26] \Rightarrow 15y \equiv x + 180[26] \Rightarrow 15y \equiv x + 24[26] \Rightarrow 15y - 24 \equiv x[26]$
 $\Rightarrow x \equiv 15y + 2[26]$.
3. La fonction de décodage est $x \equiv 15y + 2[26]$.

Tableau 1.5

Codage	C	B	M	N	J	Q	I	S	O
y	2	1	12	13	9	16	8	18	14
x	6	17	0	15	7	8	18	12	4
Lettre	G	R	A	P	H	I	S	M	E

Partie C

1. E est codé par I, donc $y = 8$ lorsque $x = 4$ de sorte que $8 \equiv 4a + b[26]$.
 V est codé par T donc $y = 19$ quand $x = 21$ et par conséquent $19 \equiv 21a + b[26]$.
2. Par soustraction membre à membre des deux congruences, on obtient $19 - 8 \equiv 21a - 4a[26]$ donc $11 \equiv 17a[26]$ ce qui peut aussi s'écrire $17a \equiv 11[26]$.
 L'inverse de 17 modulo 26 est 23 car $17 \times 23 = 391 \equiv 1[26]$ donc $23 \times 17a \equiv 23 \times 11[26] \Rightarrow a \equiv 253[26] \Rightarrow a \equiv 19[26]$.
 On remplace maintenant a par 19 dans une des congruences :
 $8 \equiv 4 \times 19 + b[26] \Rightarrow 8 - 76 \equiv b[26] \Rightarrow b \equiv -68[26] \Rightarrow b \equiv 10[26]$.
3. La fonction de décodage était $y \equiv 19x + 10[26]$.

Exercices corrigés

1.1 Écrire en base 10 les nombres suivants, donnés en base 2 ou 16 : $(101010)_2$, $(1011101)_2$, $(11011010)_2$, $(135)_{16}$, $(F2)_{16}$ et $(4C)_{16}$.

1.2 Écrire en base 2 les nombres suivants : 14, 71, 238, $(B4)_{16}$, $(30A)_{16}$ et $(6D)_{16}$.

1.3 Écrire en base 16 les nombres suivants : 401, 8 247, 10 000, $(10001)_2$, $(110110)_2$ et $(10010111)_2$.

1.4 Écrire en base 10 les nombres suivants : $(1,11)_2$, $(10,01)_2$, $(0,101)_2$, $(C,4)_{16}$, $(20,5)_{16}$ et $(8,1)_{16}$.

1.5 Écrire en base 2 puis en base 16 les nombres suivants : 4,75; 25,25 et 16,5.

1.6 a) On donne $a = (10110)_2$ et $b = (1101)_2$. Calculer $a + b$, $a - b$ et ab .

b) Même exercice avec $a = (10101101)_2$ et $b = (1100)_2$.

1.7 a) On donne $a = (D1)_{16}$ et $b = (19)_{16}$. Calculer $a + b$, $a - b$ et ab .

b) Même exercice avec $a = (1B4)_{16}$ et $b = (37)_{16}$.

1.8 a) On donne $a = (1011111)_2$ et $b = (100110)_2$. Calculer $a + b$, $a - b$, ab et $a:b$.

b) Même exercice avec $a = (1001110)_2$ et $b = (11000)_2$.

1.9 a) On donne $a = (110,01)_2$ et $b = (100,1)_2$. Calculer $a + b$, $a - b$, ab .

b) Même exercice avec $a = (1000,1)_2$ et $b = (1,11)_2$.

1.10 a) Quel est l'arrondi de $(1101011)_2$ à $(100)_2$ près ?

b) Quel est l'arrondi de $(10,011)_2$ à $(0,1)_2$ près ?

c) Quel est l'arrondi de $(A,BB)_{16}$ à $(0,1)_{16}$ près ?

1.11 Dans chaque cas, donner le quotient q et le reste r de la division euclidienne de a par b , et écrire la division euclidienne en ligne :

a) $a = 65$ et $b = 23$ b) $a = 308$ et $b = 45$ c) $a = 1\,789$ et $b = 41$

1.12 Dans chaque cas, dire si les égalités proposées correspondent à des divisions euclidiennes. Préciser alors les valeurs du quotient et du reste.

a) $37 = 8 \times 4 + 5$ b) $100 = 14 \times 7 + 2$ c) $215 = 13 \times 14 + 33$

1.13 Dans chaque cas, dire si les égalités proposées correspondent à des divisions euclidiennes. Préciser alors les valeurs du quotient et du reste.

a) $900 = 16 \times 55 + 20$ b) $662 = 31 \times 20 + 42$ c) $981 = 26 \times 37 + 19$

1.14 On écrit les unes à la suite des autres, les 26 lettres de l'alphabet. Arrivé au Z, on recommence avec un deuxième alphabet, et ainsi de suite...

- Quelle est la 10 000^e lettre écrite ? Combien d'alphabets complets ont été écrits ?
- Mêmes questions avec la 50 000^e lettre.

1.15 Alice possède un nombre n de CD. Si elle les empile par 10, il lui reste 7 CD. Si elle les empile par 7, elle fait 13 piles de plus que si elle les empile par 10, et il lui reste 3 CD. Combien Alice possède-t-elle de CD ?

1.16 Un texte saisi avec un logiciel comporte 5 070 lignes. L'éditeur étudie quelques possibilités de mise en pages du texte :

- Si l'éditeur décide de mettre 64 lignes par page, combien de lignes comporte la dernière page sachant que toutes les autres sont complètes ?
- Si l'éditeur décide de mettre 81 pages complètes, combien de lignes comporte chaque page sachant que la dernière en comporte alors 48 ?

1.17 Faire la liste des diviseurs de 12, de 20 et de 30.

1.18 Chercher tous les couples $(a;b)$ tels que $a < b$ et a divise b , dans la liste de nombres suivante : 7, 13, 18, 28, 65, 84, 91. Présenter les résultats sous forme d'un graphique en reliant les nombres concernés par des flèches orientées comme ce modèle : $a < b$ et a divise b se code $a \rightarrow b$.

1.19 a) Montrer que la somme de trois entiers naturels consécutifs est un multiple de 3.

b) La somme de quatre entiers naturels consécutifs est-elle un multiple de 4 ?

c) La somme de cinq entiers naturels consécutifs est-elle un multiple de 5 ?

1.20 Démontrer les propriétés suivantes (voir propriété 1.3) :

- Si a est divisible par b alors tout multiple de a est divisible par b .
- Si a est divisible par b et si b est divisible par c , alors a est divisible par c .
- Si a et b sont divisibles par c , alors $a + b$ et $a - b$ sont divisibles par c .

1.21 Les nombres suivants sont-ils premiers ? Si oui, dire quel est le dernier diviseur testé, si non, donner un diviseur.

107 – 161 – 179 – 241 – 311 – 323 – 437 – 563 – 677 – 779 – 971

1.22 Un début de liste prometteur... Pour tout n entier naturel, on pose : $A_n = n^2 + n + 17$.

- Vérifier que, pour tout n de 0 à 15, A_n est un nombre premier.
- Montrer que A_{16} n'est pas premier.

1.23 On se propose de chercher s'il existe des nombres premiers de la forme $n^2 - 4$, pour n entier naturel supérieur ou égal à 3, et si possible, d'en faire la liste. On note A_n le nombre $n^2 - 4$.

- a) Tester si A_n est premier pour n valant 3, 4, 5, 6 puis 7.
- b) Montrer que, à part pour $n = 3$, A_n n'est jamais premier.

1.24 On se propose de chercher s'il existe des nombres premiers de la forme $n^3 + 8$, pour n entier naturel, et d'en faire la liste. On note A_n le nombre $n^3 + 8$.

- a) Montrer que si n est pair, alors A_n n'est pas premier car il est divisible par 8.
- b) Développer $(n + 2)(n^2 - 2n + 4)$. En déduire que A_n n'est jamais premier.

1.25 Sur un ordinateur 16 bits, un entier N est représenté de la manière suivante : le premier bit à gauche donne le signe (0 correspond à + et 1 à -), et lorsque l'entier est positif, les 15 suivants sont les chiffres de l'écriture binaire de N . Par exemple : **000000000011101** représente $+(11101)_2$, c'est-à-dire $+29$.

- 1) a) Que devrait logiquement représenter le nombre **100000000011101** ?
- b) À quoi devrait être égal **000000000011101 + 100000000011101** ? Est-ce le cas ?



À cause du problème précédent, on opère différemment pour coder les entiers négatifs : le premier bit représente bien - s'il est égal à 1. Cependant, la somme d'un nombre N et de son opposé $-N$ devra toujours être nulle. Pour cela on adopte la méthode dite des **compléments**.

Par exemple, pour -29 , on part de la représentation de 29, c'est-à-dire **000000000011101** et on détermine les 16 bits **XXXXXXXXXXXXXXXX** tels que : **000000000011101 + XXXXXXXXXXXXXXXXXXXX = 000000000000000**

Il s'agit alors de changer les 0 par des 1 et les 1 par des 0 dans la représentation de 29, puis d'ajouter 1 : cela donne **111111111100010+1** donc **111111111100011**. La représentation de $29+(-29)$ donne alors **1000000000000000**, donc **0000000000000000** (par dépassement des capacités de l'ordinateur).

- 2) Déterminer la représentation de l'entier -123 dans un ordinateur 16 bits, puis celle de l'entier -43 .

1.26 On crée un jeu simple sur un ordinateur : une bille est installée au « départ » de la grille suivante (figure 1.2 à gauche), on doit la faire parvenir à « l'arrivée » en utilisant uniquement des déplacements vers la droite et vers le bas.

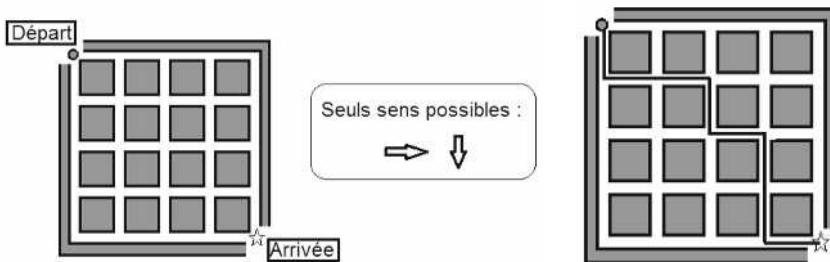


Figure 1.2