Delphine Massenet

# L'ARITHMÉTIQUE EN PRATIQUE

## De la division au chiffrement de messages secrets

ellipses

# L'ARITHMÉTIQUE EN PRATIQUE

# L'ARITHMÉTIQUE EN PRATIQUE

## De la division au chiffrement de messages secrets

Delphine Massenet

ellipses

**Conception graphique couverture :** Nathalie FOULLOY

ISBN 9782340-096547
©Ellipses Édition Marketing S.A., 2024
8/10 rue la Quintinie 75015 Paris




Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°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 une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

# Avant-propos

Un trop grand nombre de personnes sont réfractaires aux mathématiques, voire hostiles, parfois traumatisées par une pression sociale ou parentale qui ne permet pas l'acquisition de leurs concepts. Pourtant les mathématiques sont présentes partout dans notre monde, bien sûr pour compter, mais aussi dans la carte Vitale, le numéro de notre compte en banque, les jeux d'argent, à chaque fois que nous effectuons une recherche sur Internet ...
Ce livre s'adresse à tout lecteur curieux d'applications parlantes et est l'occasion d'introduire des outils d'arithmétique de manière simple.

Il s'adresse aussi à ces personnes qui gardent un mauvais souvenir des mathématiques, voire les ont en horreur ! mais qui souhaitent y revenir. Grâce à ce livre, elles pourront enfin répondre à la question qui les taraude depuis toujours « A quoi ça sert, les maths ? » ! Et, je l'espère, dépasser leur ancienne aversion jusqu'à ressentir la jubilation intellectuelle procurée par la compréhension de nouvelles notions, permettant celle d'applications concrètes, que nous utilisons quotidiennement sans le savoir. Parents, peut-être serez-vous soulagés, grâce à ce livre, de pouvoir répondre aux angoisses existentielles de vos enfants et de leur faire comprendre que les mathématiques sont utilisées par tout ce qu'ils aiment : tchatter, effectuer un achat sur internet ou dans un magasin, commander le centième épisode d'une série bien addictive.

Si, dans une journée, vous passez à la pharmacie avec votre carte Vitale, puis, arrivé au travail, vous vous connectez à votre intranet et répondez à des mails, déjeunez dans un café qui fournit sa carte par QR code, passez à la librairie en fin de journée pour acheter un livre avec votre carte bancaire, et enfin regardez un film sur une plateforme, vous aurez utilisé les mathématiques pour chacune de ces actions ! Alors autant mourir moins bête et en savoir plus sur les procédés qui sont mis en jeu dans toutes ces opérations utilisées tous les jours. Et peut-être deviendrez-vous alors un ardent défenseur des mathématiques, cette science tant redoutée.

Les mathématiques n'ont pas toujours été si impopulaires. Au XVI$^{e}$ siècle, en Italie, des duels publics opposaient parfois deux mathématiciens. Chacun posait trente questions à l'autre et le gagnant obtenait la notoriété, un poste dans une université renommée. L'enjeu était très grand et le public était nombreux à venir voir deux mathématiciens se confronter l'un à l'autre, les plus célèbres joutes étant les défis entre Tartaglia, mathématicien autodidacte, et Cardan, autour des équations du troisième degré, qui sont relatées dans *La formule secrète ou le duel mathématique qui enflamma l'Italie de la Renaissance*, de Fabio Toscano.

Dans ce livre, nous verrons comment la simple division de nombres entiers (appelée division euclidienne) a des applications aussi diverses que le contrôle d'un numéro Insee (celui de la carte Vitale) ou l'initialisation d'une communication en Wifi, moyennant quelques outils supplémentaires pour cette dernière. En effet, l'étude des nombres entiers peut être simple mais la théorie des nombres entiers peut aussi se compliquer un peu (mais pas trop !). Le code de chiffrement RSA, du nom de ses auteurs Rivert, Shamir et Adelman, en est un exemple.

Cette étude peut enfin devenir très complexe : la conjecture de Fermat (1601-1665), pourtant d'apparence simple − son énoncé tient en une ligne : si un nombre entier $n$ est supérieur à 2, il n'existe pas trois nombres entiers $a, b$ et $c$ tels que : $a^n + b^n = c^n$ − n'a été résolue qu'en 1994 par le mathématicien britannique Andrew Wiles (1953-). Celui-ci a contribué aux développements récents en recherche mathématique, notamment dans le domaine des courbes elliptiques. La conjecture est devenue le théorème de Fermat-Wiles et sa preuve comporte mille pages !

L'objectif est de pouvoir comprendre un certain nombre d'applications concrètes :

- la construction des années bissextiles,
- pourquoi février 2021 n'est pas un mois rare,
- les critères servant à vérifier les numéros des cartes Vitale, les cartes bancaires, les numéros ISBN des livres, les codes barres et les QR codes ;
- les fameux critères de divisibilité des nombres appris dans les petites classes ;
- enfin, le code de chiffrement secret RSA, qui permet, entre autres, l'exploitation du Wifi, que nous utilisons tous en permanence et celui de Diffie-Hellman.

Dans ce but, chaque notation est expliquée et le livre est donc lisible par toute personne non formée aux mathématiques.
Il est aussi l'occasion d'initier les lecteurs et lectrices :

- aux techniques de la démonstration : comment effectuer une démonstration par l'absurde, comment mener un raisonnement par récurrence, qui sont des techniques utilisées en permanence en mathématiques ;
- aux notions d'existence, d'unicité ;
- à ce que sont une condition nécessaire et une condition suffisante ;
- à ce que sont un théorème, une proposition, une proposition réciproque et une contraposée.

Bien sûr, ces rappels ne seront pas lus par les personnes qui les maîtrisent.

Des exemples et exercices, tous corrigés, sont proposés au lecteur pour qu'il soit le plus actif possible dans son apprentissage. Dès que la notion s'y prête, l'écriture de programmes informatiques est proposée. Ceux-ci sont corrigés en langage Python.
Cet ouvrage s'adresse également aux enseignants qui souhaitent exploiter des exemples concrets, du collège à la terminale.

En mathématiques, on passe son temps à apprendre de nouvelles notions, de nouvelles définitions et à prouver, démontrer des propositions, des théorèmes. Ici, les démonstrations seront toutes effectuées et rendues accessibles à toutes et à tous. Mais si elles vous paraissent trop compliquées, laissez-les de côté en première lecture.

# Table des matières

**Chapitre I. Les mots clefs de la logique mathématique ..... 9**
1 Hypothèse, proposition, proposition réciproque, contraposée, théorème ..... 9
2 Condition nécessaire, condition suffisante ..... 10
3 Conjecture, théorème, proposition ..... 11
4 Généralités sur les démonstrations ..... 13
5 Démonstration par récurrence ..... 13
6 Démonstration par l'absurde ..... 14

**Chapitre II. Rappels sur les techniques de calcul ..... 15**
1 Calcul littéral ..... 15
1.1 Simple développement ..... 15
1.2 Double développement ..... 17
1.3 Les identités remarquables ..... 19
1.4 Règles de suppression des parenthèses ..... 23
2 Notations somme et produit ..... 23
3 Les fractions ..... 24
3.1 Définitions ..... 24
3.2 Règles de calcul ..... 25
4 Les puissances d'un nombre ..... 28
4.1 Définition et propriétés ..... 28
4.2 Puissance de puissance d'un nombre ..... 30
4.3 Les puissances de dix ..... 30
5 Inégalité et opérations ..... 33
6 Fonction ..... 34
7 Partie entière d'un nombre ..... 36

**Chapitre III. Les nombres entiers - Divisibilité ..... 37**
1 Les nombres entiers ..... 37
2 Divisibilité ..... 39
3 Critères de divisibilité ..... 46
4 Application : les années bissextiles ..... 47
5 Février 2021, un bel exemple de « fake news » ..... 48

**Chapitre IV. Les codes détecteurs d'erreur de saisie ..... 51**
1 Deux outils pour comprendre ..... 51
1.1 La division euclidienne dans $\mathbb{N}$ ..... 51
1.2 Les nombres premiers ..... 54
2 La carte Vitale ..... 62
3 Les codes ISBN des livres ..... 64
4 Les codes-barres ..... 66
5 Les cartes bancaires - Algorithme de Luhn ..... 67

**Chapitre V. Les congruences ..... 69**
1 Les outils pour comprendre ..... 70
1.1 Tout le monde connaît les congruences ..... 70
1.2 Règles de calcul ..... 73
1.3 Éléments inversibles ..... 75
1.4 PGCD ..... 76
1.5 Calcul du PGCD par l'algorithme d'Euclide ..... 78
1.6 Théorème de Bézout ..... 80
1.7 Lemme de Gauss. ..... 82
1.8 Algorithme d'Euclide étendu ..... 85
2 Démonstration des critères de divisibilité ..... 87
3 Les numéros RIB et IBAN des comptes bancaires ..... 88

**Chapitre VI. Le théorème des restes chinois ..... 91**
1 Le théorème des restes chinois ..... 91
2 Comprendre par l'exemple ..... 92
3 Méthode de résolution d'un système de congruences ..... 93
4 Solstice d'été et pleine Lune ..... 94
5 Exemples historiques chinois ..... 96
5.1 Le problème des objets de Sun Zi ..... 96
5.2 Un problème de Qin Jiushao ..... 98
5.3 Le problème des voleurs, de Qin Jiushao ..... 101
6 Les pièces d'or, les pirates et le cuisinier ..... 101
7 Le problème des œufs ..... 101
7.1 Les outils pour comprendre - Le PPCM ..... 102
7.2 Le problème des œufs ..... 102

**Chapitre VII. Le chiffrement RSA ..... 105**
1 Quelques généralités sur la cryptographie et ses méthodes ..... 105
2 Comprendre le chiffrement RSA par l'exemple ..... 107

3 Les outils pour comprendre ..... 109
3.1 Les éléments inversibles modulo *n* ..... 109
3.2 Le petit théorème de Fermat ..... 110
3.3 L'indicatrice d'Euler ..... 113
3.4 Algorithme d'exponentiation rapide modulo *n* ..... 115
4 Procédure générale argumentée ..... 116
5 Un autre exemple ..... 117
6 Tests de primalité ..... 118
7 Un programme Python pour chiffrer et déchiffrer RSA ..... 120
8 Attaquer RSA par la factorisation des nombres entiers ? ..... 121
9 Utilisations de RSA ..... 124

**Chapitre VIII. Le chiffrement Diffie-Hellman ..... 125**
1 Les outils pour comprendre : les générateurs d'un ensemble ..... 125
2 Fonctionnement ..... 127
3 L'attaque de l'homme au milieu ..... 129

**Chapitre IX. Conjectures célèbres ..... 131**
1 Les nombres amis - Les nombres parfaits ..... 131
2 Les nombres de Fermat ..... 133
3 Les nombres de Mersenne ..... 135
4 Les nombres premiers de Sophie Germain ..... 136
5 La conjecture de Goldbach ..... 137
6 D'autres conjectures célèbres ..... 137

**Chapitre X. Corrigé des exercices ..... 139**

**Bibliographie ..... 193**
**Index ..... 195**
**Notations ..... 197**

# Chapitre I

# Les mots clefs de la logique mathématique

## 1 Hypothèse, proposition, proposition réciproque, contraposée, théorème

Une *hypothèse* est un énoncé supposé vrai.
Une *proposition* $P$ est un énoncé mathématique qui a une unique valeur : vraie ou fausse.
La *négation* d'une proposition $P$ est la proposition qui est vraie quand $P$ est fausse. Elle se note $\neg P$ et se lit *non* $P$.
$P \Rightarrow Q$ est une proposition qui dit que si $P$ est vraie, alors $Q$ est vraie.
$\Rightarrow$ est un symbole qui signifie *implique*.
La *contraposée* de la proposition $P \Rightarrow Q$ (ou proposition contraposée) est la proposition $\neg Q \Rightarrow \neg P$.
La proposition $P \Rightarrow Q$ et sa contraposée $\neg Q \Rightarrow \neg P$ sont *équivalentes*, ce qui signifie qu'elles sont soit vraies simultanément, soit fausses simultanément.
Cela se note : $(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$.
$\iff$ est un symbole qui signifie : *si et seulement si*, c'est-à-dire *équivalent à*. Il exprime le fait que l'on peut intervertir hypothèse et conclusion : les implications fonctionnent dans les deux sens. Quand on écrit $P \iff Q$, cela signifie que $P \Rightarrow Q$ est vraie et que la réciproque $Q \Rightarrow P$ l'est également. Par exemple, on a, pour tout $n$ entier : $n > 0 \iff n \geq 1$ car les implications sont vraies dans les deux sens. Si $n > 0$, alors $n \geq 1$ car $n$ est nombre entier. Et si $n \geq 1$, alors $n > 0$ car $1 > 0$.
Quand on écrit une proposition dans l'autre sens, en inversant hypothèse et conclusion, on appelle cela une *proposition réciproque* ou *réciproque*. Ce n'est pas parce qu'une proposition est vraie que sa réciproque est vraie. Voici un exemple de proposition dont la réciproque est fausse. Si $n > 5$, alors $n > 1$ est vraie mais la réciproque : si $n > 1$, alors $n > 5$ est fausse car, par exemple, c'est faux pour $2 : 2 > 1$ mais $2 < 5$. 2 est un *contre-exemple*.

Voici un autre exemple de proposition, en français, qui ne fonctionne pas non plus dans les deux sens : « S'il pleut, alors je prends mon parapluie. » ne fonctionne pas dans l'autre sens : « Si je prends mon parapluie, alors il pleut » n'est pas toujours vraie !

## 2 Condition nécessaire, condition suffisante

Il y a un lien entre *implication*, *condition suffisante* et *condition nécessaire*, comme le montre la définition qui suit.

**Définition 1**
$P \Rightarrow Q$ se lit : si $P$ est vraie, alors $Q$ est vraie. On dit alors que $Q$ est une *condition nécessaire* de $P$ et que $P$ est une *condition suffisante* de $Q$.

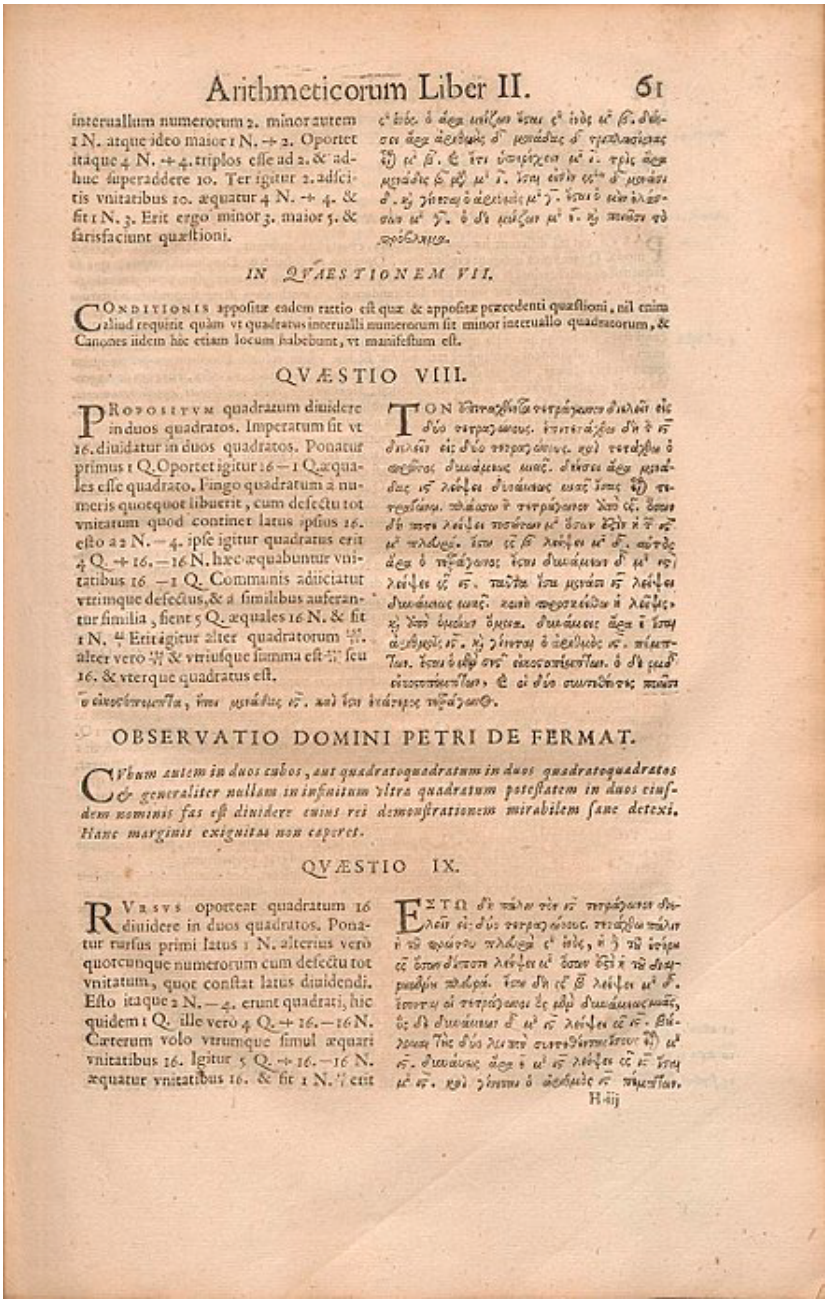
Voici un exemple non mathématique, pour illustrer cette notion : dans l'énoncé « si une personne va courir trois fois par semaine, alors elle est sportive », « elle est sportive » est une condition nécessaire. C'est une conséquence de « une personne va courir trois fois par semaine ». Ce n'est pas une condition suffisante car « elle est sportive » n'implique pas forcément la pratique de la course. Cela ne suffit pas à prouver que cette personne « va courir trois fois par semaine ». De même, dans l'énoncé « si je suis un être humain, alors je suis mortel », « je suis mortel » est une condition nécessaire de « je suis un être humain » mais ne suffit pas prouver que « je suis un être humain » car les chats, par exemple, sont aussi mortels.
Pour savoir si une condition nécessaire est suffisante, il faut inverser le sens de la proposition et regarder si l'énoncé obtenu est également vrai. Si c'est le cas, la condition est aussi une condition suffisante, sinon, ce ne l'est pas.
De même, il existe des conditions suffisantes qui ne sont pas nécessaires. Et pour savoir si une condition suffisante est nécessaire, on procède de la même manière, on inverse le sens de la proposition et on regarde si l'énoncé obtenu est vrai. Reprenons l'exemple plus haut : si $x > 5$, alors $x > 1$.
$x > 5$ est une condition suffisante de $x > 1$ mais n'en est pas une condition nécessaire car, en inversant le sens, la proposition devient : si $x > 1$, alors $x > 5$ et cet énoncé mathématique est faux car, comme nous l'avons déjà vu, 2 est supérieur à 1 mais pas à 5.
Remarquons que les définitions fonctionnent toujours dans les deux sens, puisqu'elles expriment des synonymes, mais on écrit plutôt « si » ou « quand » que « si et seulement si ». C'est une exception. Nous verrons d'autres exemples de conditions nécessaires ou suffisantes dans les exercices 7, 11, 17 du chapitre 5, et 5 du chapitre 7 .

# 3 Conjecture, théorème, proposition

Une *conjecture* est un énoncé dont on pense qu'il est vrai, mais sans en avoir encore la preuve. Dès qu'il est démontré, il porte le qualificatif de *théorème* ou de *proposition*, la différence entre les deux tenant à l'importance du résultat. Le mot proposition, ici, désigne un énoncé mathématique vrai. Son sens dépend donc du contexte, de pure logique, comme dans les paragraphes 1 et 2 ou de résultat.

**Une célèbre conjecture maintenant prouvée**

En mathématiques, un énoncé très court peut faire couler beaucoup d'encre. La démonstration de la conjecture de Pierre de Fermat (1607-1665), magistrat et mathématicien surnommé « le prince des amateurs », a été établie seulement en 1994 par Andrew Wiles (1953 -), mathématicien britannique, et comporte plus de mille pages de mathématiques.
Fermat possédait un exemplaire du livre II d'*Arithmetica*, œuvre de Diophante, mathématicien qui vivait à Alexandrie autour du III$^{e}$ siècle après J.-C. Dans la marge du problème 8, diviser un carré en deux carrés, Fermat a écrit : « Diviser un cube en deux cubes, une puissance 4 en deux puissance 4 ou une puissance quelconque en deux puissances de même dénomination, est impossible. J'ai trouvé une démonstration de cette proposition, mais je ne peux l'écrire dans cette marge car elle est trop longue. » Etant donné les domaines mathématiques mis en jeu dans la preuve de Wiles, il semble impossible que Fermat ait pu établir cette preuve et il est très probable qu'il se soit trompé. L'énoncé de sa conjecture, en latin, figure dans le livre de Diophante qu'il a annoté (voir la figure I.1), sous le titre "OBSERVATIO DOMINI PETRI DE FERMAT".



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto 2 a N. — 4. ipse igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{81}{25}$. & vtriusque summa est $\frac{337}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

*CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit



Figure I.1 : *Arithmetica* de Diophante, réédité en 1670 par le fils de Pierre de Fermat, augmenté des annotations de son père - Livre II, problème 8, page 61.

Cette conjecture, qui est maintenant prouvée, s'appelle aujourd'hui le grand théorème de Fermat et s'énonce comme suit.

**Théorème 1**
(Grand théorème de Fermat)
Il n'existe pas d'entier $n$ supérieur ou égal à 3 et d'entiers $a, b$ et $c$ tels que $a^n + b^n = c^n$.

# 4 Généralités sur les démonstrations

En mathématiques, un seul exemple, appelé contre-exemple, suffit à montrer qu'une proposition est fausse, tandis qu'il faut une démonstration générale pour montrer qu'une proposition est vraie.
Il y a des démonstrations tout au long de ce livre, qui montrent comment procéder en pratique. Elles peuvent être sautées en première lecture mais pour progresser davantage, il est nécessaire de les lire et de savoir les refaire soi-même.

# 5 Démonstration par récurrence

On effectue une démonstration par récurrence quand on doit montrer qu'une propriété est vérifiée pout tout nombre entier naturel $n$.
Il existe deux types de démonstration par récurrence.

- Dans une démonstration par récurrence dite *faible* :
  - on initialise en montrant que la propriété est vraie pour $n = 0$
  - et on montre que si elle est vraie pour l'entier $n$, alors elle est vraie pour $n + 1$.
- Dans une démonstration par récurrence dite *forte* :
  - on initialise en montrant que la propriété est vraie pour $n = 0$
  - et on montre que si elle est vraie pour tous les nombres inférieurs ou égaux à $n$, alors elle est vraie pour $n + 1$.

**Remarque :** si la propriété est à démontrer pour les entiers supérieurs ou égaux à un entier $n_0$, on effectue l'initialisation pour $n_0$ au lieu de 0.

Ce type de démonstration est basé sur le fait que pour obtenir tous les éléments de l'ensemble $\mathbb{N}$ (voir le rappel au chapitre 3), on ajoute 1 à 0, puis on ajoute 1 à l'entier obtenu 1, et ainsi de suite. Tous les entiers sont obtenus en ajoutant 1, de proche en proche, et il en est de même des propriétés dépendant de $n$.

# 6 Démonstration par l'absurde

Pour montrer qu'une proposition est vraie, on est parfois amené à effectuer un raisonnement par l'absurde : on suppose que la proposition est fausse et on montre qu'il y a une contradiction avec un des éléments dont on dispose, une absurdité. Ce procédé porte le nom de *démonstration par l'absurde*.

# Chapitre II

# Rappels sur les techniques de calcul

Tout au long de ce livre, vous allez avoir besoin de quelques techniques de calcul, que je rappelle ici.

## 1 Calcul littéral

Le *calcul littéral* est le calcul d'expressions mathématiques comportant des lettres. Une lettre représente un nombre.
La *factorisation* et le *développement* sont appris au collège.

**Définition 1**
*Factoriser*, c'est transformer une somme en un produit. Et *développer*, c'est transformer un produit en une somme.

### 1.1 Simple développement

**Proposition 1**
Soient $k, a$ et $b$ des nombres.

$$k\,a + k\,b = k\,(a + b)$$

Dans l'expression $k\,a + k\,b$, $k$ est appelé le *facteur commun*.
Quand on écrit l'expression $k\,(a + b)$, on dit qu'on a *factorisé* ou qu'*on a mis $k$ en facteur*.
En lisant cette égalité de droite à gauche, on *développe* :

$$k\,(a + b) = k\,a + k\,b$$

$k\,(a+b)$ signifie $k \times (a+b)$, $k\,a$ et $k\,b$ signifient $k \times a$ et $k \times b$. On omet le $\times$ pour alléger les notations.
Ici, c'est du *simple développement* car il n'y a que $k$ à gauche de $(a+b)$.

**Définition 2**
*Réduire une expression*, c'est calculer tout ce que l'on peut pour qu'elle soit la plus courte possible.

Par exemple, s'il y a plusieurs termes avec $x$, on met $x$ en facteur et on termine le calcul :
$2x + 3 - 5x - 1 + 12x = (2 - 5 + 12)x + 3 - 1 = 9x + 2$

**Interprétation géométrique**
Cette formule s'explique, pour des nombres positifs, grâce à la géométrie (voir la figure II.1).
L'aire d'un rectangle est *largeur* $\times$ *longueur*.
Considérons le grand rectangle ci-dessous. Sa largeur est $k$ et sa longueur est $a+b$. Son aire vaut : $k\,(a+b)$. Ce rectangle peut être divisé en deux rectangles d'aires $k \times a$ et $k \times b$. On a donc : $k\,(a+b) = k\,a + k\,b$.

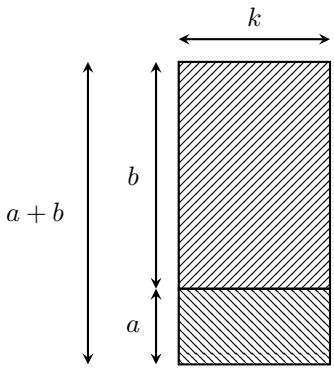



Figure II.1 : Simple développement et aires de rectangles

**Exemple :** Factorisons les expressions suivantes.
$A = 2x + 7x$ : quand on cherche à factoriser, on peut lire à voix haute. Ici, on entend deux fois $x$ : c'est donc $x$ que l'on va mettre en facteur.
$A = (2+7)x = 9x$
On met toujours en facteur le plus d'expressions communes possibles.
Par exemple, $B = 2x - 4x^2 = 2x \times 1 - 2x \times 2x = 2x(1 - 2x)$
$C = 7x - 3x + 5x + 4 - 2x$. On met $x$ en facteur. $C = (7-3+5-2)x + 4 = 7x + 4$
$D = 3a + 5 - 2b + 4a - 3b$. On met $a$ et $b$ en facteur.
$D = (3+4)a + 5 + (-2-3)b = 7a + 5 - 5b = 7a - 5b + 5$
$E = 3x^2 - 7x^2 + 8x^2$. On met $x^2$ en facteur.

$E = (3 - 7 + 8)x^2 = 4x^2$
Avec un peu d'habitude, on effectue ces factorisations de tête :
$F = 2x - 1 + 3x = 5x - 1$
$G = 3x + 6 = 3(x + 2)$

Développons les expressions suivantes.
$H = 6(1 + 2x) = 6 \times 1 + 6 \times 2x = 6 + 12x$
$I = -2(4 + x) = -2 \times 4 - 2 \times x = -8 - 2x$
Pour ne pas faire d'erreur de signe, il faut considérer que le signe est collé au nombre avec de la super glue. Dans l'expression $I$, le signe $-$ est collé à 2.

Avec un peu d'entraînement, on effectue aussi les développements de tête.
$J = 3(x + 5) = 3x + 15$
$K = -5(x - 2) = -5x + 10$
$J = 2x(3x - 5) = 6x^2 - 10x$

Le simple développement a des applications en technique de calcul mental. Par exemple, $4 \times 59 = 4 \times (60 - 1) = 4 \times 60 - 4 \times 1 = 240 - 4 = 236$.

**Exercice 1**

1. Factoriser les expressions suivantes.
   $A = -3x + 9$ $\qquad$ $B = 4y - 4$
   $C = 5x + 5y$ $\qquad$ $D = 6a - 18b$
   $E = 14x - 21y$ $\qquad$ $F = 3x^3 - 6x^2$
   $G = 7(x + 1) + 7(2x + 3)$
2. Développer les expressions suivantes.
   $H = 3(x - y)$ $\qquad$ $I = x(5x + 7)$
   $J = 2x(7x - 2)$ $\qquad$ $K = 3x^2(2 - 4x)$

## 1.2 Double développement

Une deuxième formule, appelée *double développement* est aussi très utilisée.

**Proposition 2**
Soient $a$, $b$, $c$ et $d$ des nombres.

$$(a + b)(c + d) = a\,c + a\,d + b\,c + b\,d$$

**Interprétation géométrique**
Cette formule s'explique aussi, pour des nombres positifs, grâce à la géométrie (voir la figure II.2).
Considérons le grand rectangle, de largeur $a + b$ et de longueur $c + d$. Son aire vaut : $(a + b)(c + d)$.