

# **NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS**

---

*Cours à l'Université de Rennes 1 (2005–2006)*

**Antoine Chambert-Loir**

*Antoine Chambert-Loir*

IRMAR, Campus de Beaulieu, 35042 Rennes Cedex.

*E-mail*: `antoine.chambert-loir@univ-rennes1.fr`

*Url*: `http://name.math.univ-rennes1.fr/antoine.chambert-loir`

*Version du 13 septembre 2006*

*La version la plus à jour est disponible sur le Web à l'adresse `http://name.math.univ-rennes.fr/antoine.chambert-loir/2005-06/a2/`*

# TABLE DES MATIÈRES

---

<b>1. Nombres entiers et principe de récurrence</b> .....	5
<i>Un peu d'histoire, 5 ; Récurrence et la définition des opérations élémentaires, 6 ; La relation d'ordre, 9 ; Quelques démonstrations par récurrence, 10 ; Suites définies par récurrence, 13.</i>	
<b>2. Combinatoire, probabilités</b> .....	15
<i>Rappels (sic) de théorie des ensembles, 15 ; Il est toujours bon d'avoir des principes, 18 ; Triangle de Pascal, 20 ; Probabilités, 23.</i>	
<b>3. Division euclidienne</b> .....	29
<i>Un peu de terminologie algébrique, 29 ; Le théorème de la division euclidienne, 32 ; Numération, 32 ; Divisibilité, 34 ; Plus grand diviseur commun, algorithme d'Euclide, 37.</i>	
<b>4. Nombres premiers</b> .....	43
<i>Crible d'Ératosthène, 43 ; Factorisation, 44 ; Combien y a-t-il de nombres premiers ?, 46 ; Le théorème de Tchebychev et le postulat de Bertrand, 47 ; Petit théorème de Fermat, 48.</i>	
<b>5. Congruences</b> .....	51
<i>Équations (du premier degré) aux congruences, 51 ; Théorème chinois, 53 ; Indicateur d'Euler, cryptographie RSA, 56 ; Équations polynomiales modulo <math>n</math>, 59 ; Équations polynomiales modulo un nombre premier, 60 ; Être ou ne pas être un carré modulo <math>p</math>..., 62 ; L'ordre multiplicatif modulo <math>p</math>, 63 ; Appendice : l'anneau <math>\mathbb{Z}/n\mathbb{Z}</math>, 65.</i>	
<b>6. Nombres décimaux, nombres rationnels</b> .....	67
<i>Nombres rationnels, 67 ; Le développement décimal d'un nombre rationnel, 68 ; Les nombres réels, 69 ; Quelques classes de nombres, 70 ; Quelques résultats d'irrationalité, 71 ; Un autre théorème de Fermat, 72.</i>	



# CHAPITRE 1

## NOMBRES ENTIERS ET PRINCIPE DE RÉCURRENCE

---

### §1. Un peu d'histoire

Leopold Kronecker, un mathématicien allemand du XIX<sup>e</sup> siècle a dit un jour : « Le Bon Dieu a inventé les nombres entiers, le reste est l'œuvre de l'homme ». <sup>(1)</sup> L'arithmétique, la science qui étudie les propriétés des nombres entiers, a fasciné les humains probablement depuis la nuit des temps. On trouve en tout cas des textes d'arithmétique parmi les tout premiers textes écrits qui nous restent (la plus ancienne tablette dont on dispose est une reconnaissance de dettes).

Parmi les propriétés des nombres entiers que nous allons étudier figurent des résultats très anciens : l'existence d'une infinité de nombres premiers est un théorème d'Euclide, un mathématicien grec qui vivait au IV<sup>e</sup> siècle avant Jésus-Christ. Certains problèmes remontent à Archimède (les bœufs du soleil par exemple).

Pourtant, la nécessité d'une *définition* des nombres entiers n'est apparue qu'au XIX<sup>e</sup> siècle qui fut un moment de bouleversement théorique en mathématique. C'est à ce moment que les mathématiciens commencèrent à ressentir fermement le besoin de définir plus précisément l'objet de leur science, faisant en particulier clairement la distinction entre axiomes, définitions, théorèmes, . . . Les mathématiciens durent aussi résoudre le problème de l'infini : qu'est-ce qu'un ensemble « infini » ? La possibilité d'appréhender mathématiquement l'infini fut d'ailleurs le sujet d'une controverse théologique — seul Dieu est infini. Pire, Georg Cantor découvrit qu'il existait des infinis plus grands que d'autres et, en un sens, l'ensemble des entiers est le plus petit ensemble infini.

C'est aussi qu'à la toute fin du XIX<sup>e</sup> siècle que Richard Dedekind, puis quelques années plus tard, Giuseppe Peano, énoncèrent des *axiomes* qui permettent de caractériser l'ensemble des nombres entiers. Du point de vue pratique, ces axiomes sont donc

---

<sup>(1)</sup> La citation originale, « Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk. » a été prononcée en 1886 lors d'une conférence à Berlin en 1886. Elle fut rapportée par Heinrich Weber dans la notice nécrologique consacrée à ce mathématicien (*Jahresberichte D.M.V* 2 (1893), p. 5–31). L'expression allemande « der liebe Gott » ne sous-entend pas une vision mystique des mathématiques, pas plus que l'expression française « le Bon Dieu ».

les « briques de base » que le mathématicien peut assembler pour démontrer une propriété liée aux nombres entiers. Voici les quatre premiers axiomes, sous la présentation de Peano (si ce n'est que Peano faisait débiter l'ensemble des entiers à 1).

- a) zéro (0) est un entier ;
- b) tout entier a un successeur ;
- c) zéro n'est le successeur d'aucun entier ;
- d) si deux entiers ont même successeur, ils sont égaux.

Du point de vue des entiers que vous connaissez, le successeur d'un entier  $n$  n'est rien d'autre que l'entier  $n+1$ . Si un entier  $n$  n'est pas égal à 0, il vérifie  $n \geq 1$  et l'entier  $(n-1)$  est le seul entier qui ait  $n$  pour successeur.

Le dernier axiome est le *principe de récurrence* :

e) Soit  $A$  un ensemble d'entiers. Supposons que  $A$  contienne 0 et que si un entier  $n$  appartient à  $A$ , son successeur appartienne à  $A$ . Alors  $A$  est l'ensemble de tous les entiers.

L'aspect remarquable de cet axiome est qu'il permet de démontrer une infinité de théorèmes en un temps fini. Supposons par exemple que l'on doive démontrer qu'une certaine propriété  $\mathcal{P}(n)$  qui dépend d'un entier  $n$  est vraie pour tout entier. En appliquant le principe de récurrence à l'ensemble des entiers  $n$  tels que  $\mathcal{P}(n)$  soit vérifié, on peut démontrer le résultat voulu de la façon suivante :

- on démontre la propriété  $\mathcal{P}$  pour  $n = 0$  (*initialisation*) ;
- on démontre que si la propriété  $\mathcal{P}(n)$  est vérifiée (*hypothèse de récurrence*), alors  $\mathcal{P}(n+1)$  est encore vraie.

Le principe de récurrence entraîne que la propriété  $\mathcal{P}$  est vérifiée pour tout entier. Sans lui, on devrait commencer par le cas  $n = 0$ , puis  $n = 1$ , puis  $n = 2$ , etc., et même à la 7<sup>e</sup> génération, vos « successeurs » n'en seront toujours pas venus à bout ! Pascal (XVII<sup>e</sup> siècle) avait déjà utilisé le principe de récurrence, mais il revient bien à Peano de l'avoir dégagé en tant qu'axiome qui caractérise les nombres entiers.

Il reste encore une tâche au mathématicien consciencieux : *démontrer* qu'il « existe » un ensemble avec ces propriétés : les entiers de  $\mathbb{M}$ . Tout le Monde les vérifie effectivement, mais ils ne forment pas un ensemble assez bien défini pour le mathématicien. On peut aussi démontrer qu'un tel ensemble est unique, en un sens à préciser.

Nous laisserons ce problème de côté dans la suite de ce cours et feront *comme si* les entiers naïfs étaient un objet mathématique obéissant aux axiomes de Peano.

L'ensemble de tous les entiers est noté  $\mathbb{N}$ .

## §2. Récurrence et la définition des opérations élémentaires

Le principe de récurrence permet aussi de *définir* des objets dépendant d'un entier. Ainsi, quelques années avant que Peano n'énonce ses axiomes, Grassmann avait défini les opérations arithmétiques à l'aide de l'opération  $x \mapsto x+1$  et d'un raisonnement par récurrence. Expliquons comment procéder et comment *démontrer* les propriétés élémentaires de l'addition et de la multiplication.

Tout d'abord, on note 1 le successeur de 0, 2 le successeur de 1, 3 celui de 2, etc. On notera aussi  $s(n)$  le successeur d'un entier  $n$ ; pour les entiers naïfs, cela correspond à ajouter 1.

Une première application du principe de récurrence, importante pour la suite, est que *tout entier non nul est le successeur d'un unique entier*. Notons enfin qu'un entier ne peut avoir deux prédécesseurs distincts, en vertu de l'axiome  $d$ ). Soit alors  $A$  la réunion du singleton  $\{0\}$  et de l'ensemble des entiers qui sont le successeur d'un entier. L'ensemble  $A$  contient 0, et s'il contient un entier  $n$ , il contient son successeur, puisqu'il contient tous les successeurs. Donc  $A$  est l'ensemble des entiers naturels et tout entier, sauf zéro, est le successeur d'un entier.

Si  $m$  et  $n$  sont deux entiers, on veut définir l'entier  $m + n$ , ce qu'on va faire par récurrence sur  $m$ . Si  $m = 0$ , on pose  $0 + n = n$ . Si  $m$  est un entier différent de 0,  $m$  est le successeur d'un entier  $m'$ ; l'entier  $m' + n$  a été défini par récurrence et on pose  $m + n = s(m' + n)$ . En termes naïfs,  $m' = 1 + m$  et la formule précédente signifie que  $m + n = (1 + m') + n = 1 + (m' + n)$ . Cela définit l'addition de deux entiers arbitraires. Par définition, on a  $1 + n = s(n)$  pour tout entier  $n$ .

Montrons maintenant que l'addition est commutative, c'est-à-dire que  $m + n = n + m$ . Notons  $\mathcal{P}(m)$  la propriété : pour tout entier  $n$ ,  $m + n = n + m$ .

La propriété  $\mathcal{P}(0)$  s'écrit : pour tout entier  $n$ , on a  $n + 0 = 0 + n$ , et  $0 + n = n$  par définition. Nous allons donc démontrer par récurrence sur  $n$  que  $n + 0 = n$  pour tout entier  $n$ . Pour  $n = 0$ , on doit démontrer  $0 = 0 + 0$ , ce qui est vrai. Supposons alors que  $n = n + 0$ ; on a alors  $s(n) + 0 = s(n + 0)$  par construction. Par l'hypothèse de récurrence,  $n + 0 = n$ , donc  $s(n) + 0 = s(n)$ , ce qui montre la propriété pour le successeur de  $n$ . Par récurrence, la propriété  $\mathcal{P}(0)$  est donc vraie.

Supposons que  $\mathcal{P}(m)$  soit vérifiée et montrons que la propriété est encore vraie pour le successeur de  $m$ . Si  $n$  est un entier, soit  $\mathcal{Q}(n)$  la propriété  $s(m) + n = n + s(m)$ ; nous allons encore la démontrer par récurrence! Si  $n = 0$ , on a  $s(m) + 0 = 0 + s(m) = s(m)$  car  $\mathcal{P}(0)$  est vraie. Si la propriété  $\mathcal{Q}(n)$  est vraie, alors

$$\begin{array}{ll}
 s(m) + s(n) = s(m + s(n)) & \text{par définition de } s(m) + s(n) \\
 = s(s(n) + m) & \text{car } \mathcal{P}(m) \text{ est vraie} \\
 = s(s(n + m)) & \text{par définition de } s(n) + m \\
 = s(s(m + n)) & \text{car } \mathcal{P}(m) \text{ est vraie} \\
 = s(s(m) + n) & \text{par définition de } s(m) + n \\
 = s(n + s(m)) & \text{car } \mathcal{Q}(n) \text{ est vraie} \\
 = s(n) + s(m) & \text{par définition de } s(n) + s(m).
 \end{array}$$

Ainsi, la propriété  $\mathcal{Q}(s(n))$  est vraie. Par récurrence, elle est donc vraie pour tout entier  $n$ , ce qui démontre la propriété  $\mathcal{P}(s(m))$ .

Par récurrence, la propriété  $\mathcal{P}(m)$  est vraie pour tout entier  $m$ . Autrement dit, l'addition est commutative.

Il faudrait maintenant démontrer l'associativité de l'addition, c'est-à-dire que si  $m, n, p$  sont des entiers, on a  $(m + n) + p = m + (n + p)$ . On peut le faire par récurrence, de manière analogue, mais un peu plus compliquée, que pour la commutativité.

Pour construire la multiplication, on utilise le fait que pour multiplier  $m$  par  $n$ , on doit effectuer l'addition  $n + n + \dots + n$ ,  $m$  fois. Posons ainsi, pour tout entier  $n$ ,  $1 \times n = n$ . Si  $m \times n$  est défini, on définit alors  $s(m) \times n$  par la formule

$$s(m) \times n = (m \times n) + n.$$

On démontre alors par récurrence que  $m \times n = n \times m$ , que  $(m \times n) \times p = m \times (n \times p)$ , etc.

On peut encore utiliser le principe de récurrence pour démontrer un certain nombre de formules classiques liant sommes et produits. Voici deux exemples.

a) Pour tout entier  $n$ ,  $1 + 2 + \dots + n = n(n + 1)/2$ .

Cette formule est vraie pour  $n = 0$ , car  $1 + \dots + 0 = 0 = 0(0 + 1)/2$ ; elle l'est aussi pour  $n = 1$  car  $1 = 1(1 + 1)/2$ . Supposons-la vraie pour  $n$  et montrons qu'elle est encore vraie pour  $n + 1$ . De fait, on a

$$1 + 2 + \dots + (n + 1) = (1 + 2 + \dots + n) + (n + 1) = n(n + 1)/2 + (n + 1) = (n + 1)(n + 2)/2,$$

ce qui est la formule au rang  $n + 1$ . Par récurrence, elle est donc vraie pour tout entier  $n$ .

b) Pour tout nombre réel  $a \neq 1$  et tout entier  $n$ ,  $1 + a + \dots + a^n = \frac{a^{n+1} - 1}{a - 1}$ .

Pour  $n = 0$ , cette formule s'écrit  $1 = \frac{a^1 - 1}{a - 1}$ , donc est vraie. Supposons qu'elle soit vraie pour  $n$ ; on a alors

$$1 + a + \dots + a^{n+1} = (1 + \dots + a^n) + a^{n+1} = \frac{a^{n+1} - 1}{a - 1} + a^{n+1} = \frac{(a^{n+1} - 1) + a^{n+1}(a - 1)}{a - 1} = \frac{a^{n+1} - 1}{a - 1},$$

ce qui montre qu'elle est vraie pour  $n + 1$ . Par récurrence, elle est vraie pour tout entier  $n$ .

*Exercices.* — 1) Démontrer l'associativité de l'addition, la commutativité et l'associativité de la multiplication.

2) a) Montrer que pour tout entier  $n \geq 4$ , on a  $2^n < n!$ .

b) Déterminer un entier  $A$  tel que pour tout  $n \geq A$ , on ait  $3^n < n!$ .

3) a) Montrer par récurrence sur  $n$  les formules

$$1 + 2 + \dots + n = \frac{n(n + 1)}{2} \quad \text{et} \quad 1^2 + 2^2 + \dots + n^2 = \frac{n(n + 1)(2n + 1)}{6}.$$

b) Que vaut, si  $n$  est impair, la somme  $1 + 3 + 5 + \dots + n$ ?

c) Montrer par récurrence que pour tout entier naturel  $n$ , on a

$$\sum_{k=0}^n (-1)^k k^2 = (-1)^n \frac{n(n + 1)}{2}.$$

4) a) Montrer que pour tout entier  $n$ ,  $4^n + 5$  est un multiple de 3.

b) Montrer que si  $10^n + 7$  est multiple de 9,  $10^{n+1} + 7$  l'est aussi. Que peut-on en déduire?

### §3. La relation d'ordre

Soit  $m$  et  $n$  des entiers ; on dit que  $m$  est inférieur ou égal à  $n$ , et on note  $m \leq n$  s'il existe un entier  $u$  tel que  $n = m + u$ . Si  $m$  est inférieur ou égal à  $n$ , on dit aussi que  $n$  est supérieur ou égal à  $m$ , ce qu'on note encore  $n \geq m$ . La notation  $m < n$  signifie que  $m \leq n$  mais que  $m \neq n$  ; de même, la notation  $m > n$  signifie que  $m \geq n$  mais  $m \neq n$ .

La relation  $\leq$  vérifie trois propriétés, qu'on résume en disant que c'est une relation d'ordre :

- a) pour tout entier  $m$ ,  $m \leq m$  ;
- b) si  $m \leq n$  et  $n \leq p$ , alors  $m \leq p$  ;
- c) si  $m \leq n$  et  $n \leq m$ , alors  $m = n$ .

La première est évidente puisque  $m = m + 0$ . Démontrons par exemple la deuxième. Supposons que  $m, n, p$  soient trois entiers tels que  $m \leq n$  et  $n \leq p$  ; par hypothèse, il existe un entier  $u$  tel que  $n = m + u$  et un entier  $v$  tel que  $p = n + v$ . Alors,  $p = m + (u + v)$ , ce qui entraîne  $m \leq p$ .

De même, on peut démontrer toutes les propriétés classiques sur cette relation  $\leq$  :

- c) deux entiers  $m$  et  $n$  étant donnés, l'un des deux est inférieur ou égal à l'autre (on dit que l'ordre est *total*) ;
- d) soit  $m, n, p$  des entiers ; si  $m \leq n$ , on a  $m + p \leq n + p$  ; inversement, si  $m + p \leq n + p$ , alors  $m \leq n$ .
- e) soit  $m, n, p$  des entiers ; si  $m \leq n$ , alors  $mp \leq np$  ; inversement, si  $mp \leq np$  et que  $p \neq 0$ , alors  $m \leq n$ .

Il y a deux variantes du principe de récurrence qu'il est utile de connaître.

a) Si l'on souhaite établir une propriété  $\mathcal{P}(n)$  à partir d'un certain rang, disons, pour fixer les idées, pour tout entier  $n \geq 10$ , il suffit de démontrer 1) qu'elle est vraie pour  $n = 10$  ; 2) que si elle est vraie pour un entier  $n \geq 10$ , elle l'est pour  $n + 1$ .

On peut se ramener au principe usuel en introduisant la propriété  $\mathcal{P}'(n)$  définie par «  $n < 10$  ou  $\mathcal{P}(n)$  est vraie ». Cette propriété est vraie pour  $n = 0$  (car  $0 < 10$ ). Supposons qu'elle soit vraie pour un entier  $n$  et montrons qu'elle l'est pour  $n + 1$ . Si  $n + 1 < 10$ ,  $\mathcal{P}'(n + 1)$  est vraie ; si  $n + 1 = 10$ , elle l'est encore car  $\mathcal{P}(10)$  est vraie. Enfin, si  $n + 1 > 10$ ,  $n \geq 10$  ; par hypothèse,  $\mathcal{P}(n)$  est donc vraie, donc  $\mathcal{P}(n + 1)$  aussi par l'hypothèse de récurrence, ce qui entraîne que  $\mathcal{P}'(n + 1)$  est vraie. Par récurrence, la propriété  $\mathcal{P}'(n)$  est vraie pour tout  $n$ . Lorsque  $n \geq 10$ , cela entraîne que  $\mathcal{P}(n)$  est vraie.

b) Si l'on souhaite établir une propriété  $\mathcal{P}(n)$  pour tout entier  $n \geq 0$ , il suffit de démontrer 1) qu'elle est vraie pour  $n = 0$  ; 2) que si elle est vraie pour *tout* entier  $\leq n$ , elle est vraie pour  $n + 1$ . C'est le principe parfois appelé *de récurrence forte*.

Il se déduit du principe usuel : notons  $\mathcal{P}^*(n)$  la propriété : «  $\mathcal{P}(k)$  est vraie pour tout entier  $k \leq n$  ». On a  $\mathcal{P}^*(0)$  ; et si  $\mathcal{P}^*(n)$  est vraie, alors  $\mathcal{P}(n + 1)$  aussi (par l'hypothèse de récurrence forte), donc  $\mathcal{P}^*(n + 1)$  est vraie, par définition de la propriété  $\mathcal{P}^*$ . Par suite,  $\mathcal{P}^*(n)$  est vraie pour tout entier  $n$ . En particulier,  $\mathcal{P}(n)$  est vraie pour tout  $n$ .

Une autre variante du principe de récurrence s'énonce en termes de la relation d'ordre : *toute partie non vide de l'ensemble des entiers possède un plus petit élément*. En termes mathématiques, pour toute partie non vide  $A$  de  $\mathbf{N}$ , il existe un entier  $a \in A$  tel que tout entier  $n \in A$  vérifie  $n \geq a$ . Pour l'établir, nous allons démontrer la propriété

$\mathcal{P}(n)$  suivante : si  $A$  est une partie de  $\mathbf{N}$  qui contient un élément inférieur ou égal à  $n$ , alors  $A$  possède un plus petit élément.

La propriété  $\mathcal{P}(0)$  signifie : si  $A$  est une partie de  $\mathbf{N}$  contenant un élément inférieur ou égal à 0, alors  $A$  possède un plus petit élément. Elle est vraie, ce plus petit élément est précisément 0.

Supposons que  $\mathcal{P}(n)$  soit vraie et démontrons  $\mathcal{P}(n+1)$ . Soit  $A$  une partie de  $\mathbf{N}$  contenant un élément inférieur ou égal à  $n+1$ . Si  $n+1$  est le plus petit élément de  $A$ , on a terminé. Sinon, il existe  $a \in A$  tel que  $a < n+1$ , donc  $a \leq n$ ; l'ensemble  $A$  contient un élément inférieur ou égal à  $n$ , donc, par l'hypothèse de récurrence, un plus petit élément. Par récurrence, la propriété  $\mathcal{P}(n)$  est vraie pour tout entier  $n$ .

Inversement, on peut déduire le principe de récurrence de cette variante (et des quatre premiers axiomes). Soit en effet  $A$  une partie de  $\mathbf{N}$  qui contient 0 et qui, si elle contient un élément, contient son successeur. Montrons que  $A = \mathbf{N}$ . Soit  $B$  le complémentaire de  $A$  dans  $\mathbf{N}$ , c'est-à-dire l'ensemble des entiers qui n'appartiennent pas à  $A$ . On veut montrer que  $B$  est vide. Raisonnons par l'absurde. Sinon,  $B$  possède un plus petit élément  $b$ . Comme  $0 \in A$ ,  $0 \notin B$ , d'où  $b \neq 0$ . Par suite,  $b$  est le successeur d'un élément  $a$  de  $\mathbf{N}$ . Si  $a \in A$ , alors  $b = s(a) \in A$ , ce qui est faux; mais si  $a \in B$ , on a l'inégalité  $a < b$  qui contredit l'hypothèse que  $b$  est le plus petit élément de  $B$ .

#### §4. Quelques démonstrations par récurrence

Si vous devez acheter une maison ou un bien assez cher, vous devrez probablement emprunter la somme correspondante à une banque. La banque avance alors l'argent et, chaque mois, vous devrez payer une somme fixée (la « mensualité »). Votre capital restant dû diminue d'autant, après avoir été majoré des intérêts sur la somme restant due. Intéressons-nous aux intérêts. La littérature bancaire fait en général mention d'un *taux annuel* — pour un prêt immobilier, il est en ce moment l'ordre de 4,5% par an. Mais comme vous remboursez chaque mois, vos intérêts sont aussi calculés chaque mois et le banquier doit utiliser un *taux mensuel*. On imaginerait a priori que ce taux mensuel est calculé de sorte que les intérêts d'un an (en l'absence de remboursement) correspondent au taux annuel.

Pour être plus clair, posons quelques équations. Appelons  $\tau_a$  le taux annuel et  $\tau_m$  le taux mensuel. En gros,  $\tau_a = 4,5/100 = 0,045$ . Si le capital dû au 1<sup>er</sup> janvier est  $C$ , les intérêts accumulés en un an seront de  $\tau_a \times C$ , d'où un capital dû au 31 décembre de  $(1 + \tau_a)C$ . Calculons mensuellement. Au 1<sup>er</sup> février, les intérêts accumulés s'élèvent à  $\tau_m C$ , d'où un capital dû de  $(1 + \tau_m)C$ . Un mois plus tard, le capital dû est multiplié par  $(1 + \tau_m)$ , donc il vaut  $(1 + \tau_m)^2 C$ , et finalement, au bout d'un an, le capital dû est de  $(1 + \tau_m)^{12} C$ . (Au passage, on a omis le raisonnement par récurrence qui calcule le terme général d'une suite géométrique...) Si le taux mensuel et le taux annuel se correspondent, on arrive à l'équation

$$1 + \tau_a = (1 + \tau_m)^{12}.$$

Pourtant, ce n'est pas ce qui se passe : les banquiers utilisent systématiquement la formule

$$\tau_a = 12\tau_m.$$

Précisément, si  $\tau_m$  est le taux mensuel effectivement, les prospectus affichent comme taux annuel la valeur  $12\tau_m$ . Se pose alors la question : est-ce pareil ? Bien sûr, ce n'est pas pareil et, si  $\tau_m > 0$  (ce qui est le cas !), on a l'inégalité

$$(1 + \tau_m)^{12} > 1 + 12\tau_m.$$

Autrement dit, le taux annuel que vous payez est plus élevé que celui que la banque vous annonce. Mais c'est comme ça, il semble que la réglementation officielle en matière de crédit le permette...

Dans l'inégalité précédente, le nombre 12 n'a rien à voir et nous allons montrer que pour tout entier  $n \geq 2$  et tout nombre réel  $x > 0$ , on a  $(1 + x)^n > 1 + nx$ . Si  $n = 2$ ,

$$(1 + x)^2 = 1 + 2x + x^2 > 1 + 2x.$$

car  $x^2 > 0$ . Supposons alors que l'inégalité est vraie pour  $n$  et calculons  $(1 + x)^{n+1}$ . On a d'abord

$$(1 + x)^{n+1} = (1 + x)^n(1 + x)$$

par définition des puissances. En multipliant l'inégalité pour  $n$  (l'hypothèse de récurrence) par le nombre réel  $(1 + x)$  qui est strictement positif, on obtient

$$(1 + x)^n(1 + x) > (1 + nx)(1 + x) = (1 + nx) + (1 + nx)x = 1 + (n + 1)x + nx^2,$$

d'où

$$(1 + x)^{n+1} > 1 + (n + 1)x + nx^2 > 1 + (n + 1)x$$

puisque  $nx^2 > 0$ . Cela démontre l'hypothèse pour  $n + 1$  et l'inégalité est vraie pour tout entier  $n$ .

*Exercices.* — 1) On dispose d'un stock illimité de pièces de 3 € et de 5 €. Quels sont les montants que l'on peut payer ?

2) Si  $n$  est un entier  $\geq 1$  et  $x$  un réel dans  $[0, 1]$ , montrer l'inégalité

$$1 - nx \leq (1 - x)^n \leq 1 - \frac{nx}{1 + (n - 1)x}.$$

3) Soit  $(x_n)$  une suite de réels dans  $]0, 1[$ . On pose  $S_n = x_1 + \dots + x_n$ . Montrer l'inégalité

$$1 - S_n \leq (1 - x_1)(1 - x_2) \dots (1 - x_n) \leq \frac{1}{1 + S_n}.$$

4) a) Déterminer deux nombres réels  $a$  et  $b$  tels que l'on ait, pour tout nombre réel  $x > 0$ ,

$$\frac{1}{x(x + 1)} = \frac{a}{x} + \frac{b}{x + 1}.$$

b) Montrer par récurrence que pour tout entier naturel  $n \geq 1$ , on a

$$\sum_{k=1}^n \frac{1}{k(k + 1)} = 1 - \frac{1}{n + 1}.$$

5) Montrer que pour tout entier  $n \geq 1$ , on a  $\prod_{k=1}^n (4k - 2) = \prod_{k=1}^n (n + k)$ .

- 6) a) Si  $x$  et  $y$  sont deux nombres réels positifs, montrer que  $\sqrt{xy} \leq (x + y)/2$ .  
 b) Montrer par récurrence sur  $n$  que si  $x_1, \dots, x_{2^n}$  sont des nombres réels positifs,

$$(x_1 \cdots x_{2^n})^{1/2^n} \leq (x_1 + \cdots + x_{2^n})/2^n.$$

- c) Soit  $N \geq 2$  et soit  $x_1, \dots, x_N$  des nombres réels positifs. Démontrer que

$$(x_1 \cdots x_N)^{1/N} \leq (x_1 + \cdots + x_N)/N$$

(*inégalité entre moyenne arithmétique et moyenne géométrique*). Pour cela, choisir un entier  $n$  tel que  $N \leq 2^n$ ; poser, pour  $N \leq k \leq 2^n$ ,  $x_k = (x_1 + \cdots + x_N)/N$ ; appliquer la question précédente.

7) a) Peut-on paver un échiquier privé de deux cases diagonalement opposées par des dominos (chacun recouvrant exactement deux cases).

b) Démontrer que l'on peut paver un échiquier  $8 \times 8$  par des triominos en forme de L (recouvrant trois cases) de sorte à laisser vide une case quelconque prescrite à l'avance. (Remplacer 8 par  $2^n$ , et faire une récurrence...)

c) Quels rectangles sont pavables par des triominos en forme de L? (La réponse générale n'est semble-t-il pas connue...)

8\*) On trace  $n$  droites dans le plan; on suppose que deux d'entre elles ne sont pas parallèles et que trois d'entre elles ne sont pas concourantes.

a) Quelle est le nombre de régions du plan qu'elles délimitent? Combien d'entre elles sont bornées? (Une  $(n + 1)$ -ième droite coupe chacune des  $n$  premières en  $n$  points distincts; elle traverse  $(n + 1)$  régions en les divisant en 2. Lesquelles sont bornées?)

b) Quel est le nombre maximal de parts d'un gâteau circulaire que l'on peut obtenir en  $n$  coups de couteau?

9) Nous allons démontrer par récurrence sur  $n$  que si, dans une salle de  $n$  personnes, il y a au moins une fille, alors il n'y a que des filles. Notons  $P(n)$  cette proposition.

Elle est vraie pour  $n = 1$ .

Supposons qu'elle soit vraie pour  $n$ , c'est-à-dire supposons que lorsqu'une salle contient  $n$  personnes dont au moins une fille, alors il n'y a que des filles; montrons qu'elle est vraie pour  $n + 1$ . Considérons donc une salle contenant  $n + 1$  personnes dont au moins une fille; appelons-la Chantal. Faisons sortir une personne autre que Chantal, disons, Vincent. La salle contient  $n$  personnes, dont une fille, Chantal. Par l'hypothèse de récurrence, il y a donc  $n$  filles dans la salle. On fait alors entrer Vincent, et on demande à Chantal de sortir. Dans la salle il y a  $n$  personnes dont  $n - 1$  filles. En appliquant à nouveau l'hypothèse de récurrence, on en déduit que la salle ne contient que des filles. On fait alors rentrer Chantal; la salle ne contient que des filles.

*Chercher l'erreur!*

10) Le jeu des tours de Hanoï est constitué de  $n$  disques de rayons distincts et de trois piquets pouvant les accueillir. On ne peut poser un disque que sur un disque plus grand. Au début, les disques sont empilés du plus grand au plus petit sur un des piquets; le but du jeu est de déplacer l'ensemble sur un des deux autres piquets. Montrer que c'est effectivement possible en  $2^n - 1$  étapes, mais pas en moins.

### §5. Suites définies par récurrence

Ce sont les suites (de nombres entiers, réels, de points, de fonctions,...) dont chaque terme est défini en fonction du précédent, voire des deux précédents,... Les suites arithmétiques, définies par une relation de la forme  $u_{n+1} = u_n + a$ , en sont un exemple. On démontre par récurrence que  $u_n = u_0 + na$  pour tout entier  $n$ .

De même, les suites géométriques sont définies par une relation  $u_{n+1} = au_n$ . Le nombre  $a$  est appelé *raison*, et l'on a  $u_n = a^n u_0$  pour tout entier  $n$ .

Revenons au problème des prêts bancaires. La question, connaissant le taux mensuel  $\tau_m$ , le capital emprunté  $C$  et le nombre de mensualités  $N$ , est de calculer le montant  $M$  de la mensualité. Ou à l'inverse, connaissant le taux mensuel, le capital dont vous avez besoin et la mensualité que vous pouvez payer, de calculer le nombre d'années pendant lesquelles vous devrez rembourser votre prêt.

On pose  $C_0 = C$  et, plus généralement, on note  $C_n$  le capital restant dû au bout de  $n$  mois. Au bout de chaque mois, la banque vous considère comme débiteur des intérêts mensuels sur le capital dû au début du mois mais vous crédite du montant de la mensualité, si bien que le capital restant dû au mois  $(n+1)$  vérifie la relation

$$C_{n+1} = C_n + \tau_m C_n - M = (1 + \tau_m)C_n - M.$$

La suite  $(C_n)$  est donc un mélange d'une suite arithmétique et d'une suite géométrique.

Il y a une astuce pour ramener cette suite à une suite géométrique. Cherchons un réel  $A$  tel que

$$C_{n+1} - A = (1 + \tau_m)(C_n - A)$$

En identifiant les deux relations, on obtient

$$A\tau_m = M.$$

La suite  $(C_n - A)$  est une suite géométrique de premier terme  $(C_0 - A)$  et de raison  $(1 + \tau_m)$ . On a ainsi, pour tout entier  $n$ ,

$$C_n - A = (1 + \tau_m)^n (C_0 - A),$$

d'où la formule

$$C_n = (1 + \tau_m)^n C_0 - \frac{(1 + \tau_m)^n - 1}{\tau_m} M.$$

Si tout le capital est remboursé en  $N$  mois, on a  $C_N = 0$  et cette formule permet de déterminer la mensualité  $M$ . Inversement, si  $M$  est fixée, on peut trouver  $n$  tel que  $C_n = 0$ ; à moins d'une coïncidence peu probable, on n'obtiendra pas un nombre entier mais un nombre réel de la forme  $N + x$  avec  $0 \leq x < 1$ . Cela signifie qu'on remboursera la mensualité fixée pendant  $N$  mois, et que la dernière mensualité sera plus faible.

*Exercices.* — 1) On considère une suite arithmétique  $(u_n)$  de premier terme  $u_0$  et de raison  $a$  et on pose  $U_n = u_0 + \dots + u_n = \sum_{k=0}^n u_k$ . Montrer que  $U_n = (n+1)(u_0 + \frac{1}{2}an)$ .

2) On considère une suite géométrique  $(u_n)$  de premier terme  $u_0$  et de raison  $a$  et on pose encore  $U_n = u_0 + \dots + u_n$ . On suppose que  $a \neq 1$ ; montrer alors que  $U_n = u_0 \frac{a^{n+1} - 1}{a - 1}$ . Que vaut  $U_n$  dans le cas où  $a = 1$ ?

3) Un récipient contient  $1 \text{ dm}^3$  de riz, chaque grain faisant  $1 \text{ mm}^3$ . On dispose un grain de riz sur la première case d'un échiquier, deux sur la deuxième, quatre sur la suivante, et ainsi de suite, en doublant à chaque fois le nombre de grains. Combien de cases de l'échiquier seront remplies lorsque le pot de riz ne contiendra plus assez de grains ? Combien en reste-t-il dans le pot ?

4) La suite  $(u_n)$  est définie par  $u_1 = 1/2$  et  $u_n = u_{n-1}/(2nu_{n-1} + 1)$ , si  $n \geq 2$ . Calculer  $u_1 + \dots + u_n$  pour tout entier  $n$ . (Commencez par calculer explicitement cette somme pour de petites valeurs de  $n$ , conjecturez alors une formule générale que vous démontrerez ensuite par récurrence.)

5) Soit  $(u_n)$  la suite définie par récurrence par la relation  $u_{n+1} = 3u_n + 2$  et  $u_0 = 1$ .

a) Déterminer un nombre réel  $a$  tel que la suite  $(v_n)$  définie par  $v_n = u_n + a$  soit une suite géométrique.

b) En déduire une formule simple pour  $v_n$  puis une formule simple pour  $u_n$ .

c) Déduire de l'exercice une *méthode générale* pour calculer le  $n$ -ième terme d'une suite  $(u_n)$  définie par une récurrence  $u_{n+1} = au_n + b$ , où  $a$  et  $b$  sont des nombres réels.

6) Soit  $(u_n)$  la suite définie par récurrence par  $u_0 = 1$  et  $u_{n+1} = u_n + 2n + 3$  pour  $n \geq 0$ .

a) Démontrer que pour tout entier  $n$ , on a  $u_n \geq n^2$ .

b) On définit une suite  $(v_n)$  en posant, pour tout entier  $n$ ,  $v_n = u_{n+1} - u_n$ . Calculer  $v_{n+1}$  en fonction de  $v_n$ , puis exprimer  $v_n$  en fonction de  $n$ .

c) Calculer  $u_n$  en fonction de  $n$ .

7) On définit une suite  $(u_n)$  en posant  $u_0 = 1$  et, si  $n \geq 0$ ,  $u_{n+1} = u_n/(1 + u_n)$ .

a) Montrer que l'on a  $u_n > 0$  pour tout entier  $n$ .

b) Montrer que la suite  $(1/u_n)$  est arithmétique.

c) Calculer  $u_n$  pour tout entier  $n$ .

8) Les taux d'intérêt (TEG annuel) des crédits à la consommation sont en 2005 de l'ordre de 8% pour des prêts d'une durée de 5 ans. Vous souhaitez acheter une Logan (7500 €) ; votre revenu mensuel est de 1200 € et l'organisme de prêt exige un endettement inférieur à 30%.

a) Quel est le nombre minimal de mensualités dont vous devrez vous acquitter ?

b) Quel est le coût total de votre crédit si vous souscrivez un tel crédit ? et si vous décider de rembourser pendant 5 ans ?

9) Un ingénieur au revenu mensuel de 3000 € décide d'acheter une maison ; le taux d'endettement que lui autorise son organisme de crédit est  $1/3$ , le taux d'intérêt du moment est 3,5%.

a) De quelle somme peut-il disposer s'il décide de souscrire un prêt d'une durée de 10 ans ? de 20 ans ?

b) Quel est le coût total du crédit (pour 100000 € empruntés) ?

c) En 1995, les taux d'intérêts étaient plutôt de l'ordre de 8,5%. Répondre aux questions ci-dessus.

10) a) Dans un prêt, calculer la somme totale  $S$  payée par le débiteur en fonction du nombre de mensualités, du taux mensuel et du capital emprunté. Avec MAPLE, tracer la fonction  $N \mapsto S$  (on fixera une valeur numérique de  $\tau_m$  et  $C = 1$ ).

b) Avec MAPLE (ou un tableur), produire un tableau de remboursements en donnant, mois par mois, la part d'intérêts dans la mensualité et le capital restant dû.

c) Une banque permet de rembourser une partie du prêt par anticipation, moyennant des frais de dossier. Le client de la banque a-t-il intérêt à rembourser partiellement son prêt ? (La réponse dépend du taux, du capital restant dû, des frais de dossier et du montant du remboursement exceptionnel. Écrire un programme qui fait l'ensemble des calculs.)

## CHAPITRE 2

# COMBINATOIRE, PROBABILITÉS

---

Il est dommage de consacrer un cours aux nombre entiers sans passer un peu de temps à leur vocation première : *compter*, c'est-à-dire dénombrer.

Dans de nombreuses formules, on aura besoin d'utiliser la fonction *factorielle* qui est définie comme suit. La factorielle d'un entier positif ou nul  $n$  est le produit de tous les entiers de 1 à  $n$ . on a  $1! = 1$ ,  $2! = 1 \times 2 = 2$ ,  $3! = 1 \times 2 \times 3 = 6$ , etc. Plus généralement,

$$n! = 1 \times 2 \times \cdots \times (n-1) \times n = n \times (n-1)!$$

On pose aussi, par une convention pratique,  $0! = 1$ . Je rappelle aussi que  $n!$  se prononce *factorielle n*.

### §1. Rappels (*sic*) de théorie des ensembles

Il est hors de question dans ce cours de fonder rigoureusement la théorie des ensembles et nous nous contenterons des quelques définitions qui suivent.

*1.1. Ensembles et éléments.* — On écrit  $x \in A$  et on prononce «  $x$  appartient à  $A$  » pour dire que  $x$  est un élément de l'ensemble  $A$ . Deux ensembles qui ont les mêmes éléments sont égaux ; en particulier, il n'y a dans un ensemble ni ordre ni répétition d'éléments. L'ensemble vide, noté  $\emptyset$  ou  $\{\}$ , n'a pas d'élément. On écrit  $A \subset B$  et on prononce «  $A$  est inclus dans  $B$  » pour dire que tout élément de  $A$  appartient à  $B$  ; on dit aussi que  $A$  est une partie de  $B$ . On a donc  $A \subset A$  (tout élément de  $A$  appartient à  $A$ ) et  $\emptyset \subset A$ . Si  $A \subset B$  et  $B \subset C$ , alors  $A \subset C$ . Si  $A \subset B$  et  $B \subset A$ , alors  $A = B$  : la première inclusion dit que tout élément de  $A$  est un élément de  $B$ , l'autre que tout élément de  $B$  est un élément de  $A$ , si bien que  $A$  et  $B$  ont les mêmes éléments.

La réunion de deux ensembles  $A$  et  $B$  est l'ensemble, noté  $A \cup B$  (on prononce «  $A$  union  $B$  »), dont les éléments sont ceux qui appartiennent à  $A$  ou à  $B$ . L'intersection de deux ensembles  $A$  et  $B$  est l'ensemble formé des éléments qui appartiennent à la fois à  $A$  et à  $B$  ; on le note  $A \cap B$  («  $A$  inter  $B$  »). Ces définitions se généralisent sans peine à plus de deux ensembles. On dit que  $A$  et  $B$  sont disjoints si l'on a  $A \cap B = \emptyset$ , c'est-à-dire si  $A$  et  $B$  n'ont aucun élément en commun.

Si, par exemple,  $A = \{1, 2, 3\}$ ,  $B = \{3, 4\}$  et  $C = \{1, 4\}$ , on a  $A \cap B = \{3\}$ ,  $A \cup B = A \cup C = \{1, 2, 3, 4\}$ ,  $A \cap C = \{1\}$  et  $A \cap B \cap C = \emptyset$ .

Un *couple* est la donnée de deux éléments, dans un ordre déterminé. Un couple  $(a, b)$  a donc une première coordonnée, à savoir  $a$ , et une seconde coordonnée,  $b$ . Deux couples  $(a, b)$  et  $(a', b')$  sont égaux si et seulement si  $a = a'$  et  $b = b'$ . Si  $A$  et  $B$  sont des ensembles, il existe un ensemble, qu'on note  $A \times B$ , et dont les éléments sont les *couples*  $(a, b)$ , où  $a$  est un élément de  $A$  et  $b$  un élément de  $B$ .

1.2. *Applications.* — Soit  $A$  et  $B$  des ensembles. Une application  $f$  de  $A$  dans  $B$  est la donnée, pour tout élément  $a$  de  $A$ , d'un élément de  $B$  qu'on note  $f(a)$ . On écrit  $f: A \rightarrow B$ ,  $a \mapsto f(a)$ . Si  $b = f(a)$ , on dit que  $b$  est l'*image* de  $a$  par  $f$ , et que  $a$  est un *antécédent* de  $b$  par  $f$ .

L'application identité de  $A$  dans  $A$  associe à tout  $a \in A$  lui-même ; on la note  $\text{Id}_A$ .

Soit  $f: A \rightarrow B$  et  $g: B \rightarrow C$  des applications. On définit l'application  $g \circ f: A \rightarrow C$  en posant  $(g \circ f)(a) = g(f(a))$  pour tout  $a \in A$ .

Le graphe de  $f$  est l'ensemble des couples  $(a, f(a))$ , pour  $a \in A$  ; c'est une partie de  $A \times B$ . Si  $S$  est une partie de  $A$ , l'ensemble des  $f(a)$ , pour  $a \in S$  est une partie de  $B$  qu'on appelle l'*image* de  $S$  par  $f$  et qu'on note  $f(S)$ . Si  $T$  est une partie de  $B$ , l'ensemble des  $a \in A$  tels que  $f(a) \in T$  (l'ensemble des antécédents des éléments de  $T$ ) est une partie de  $A$  qu'on appelle l'*image réciproque* de  $T$  par  $f$  et qu'on note  $f^{-1}(T)$ .

DÉFINITION 1.3. — Soit  $f: A \rightarrow B$  une application. On dit que  $f$  est *injective* si des éléments de  $A$  distincts ont des images distinctes par  $f$ .

Cela revient à dire que tout élément de  $B$  a au plus un antécédent par  $f$ . Supposons en effet que  $f$  soit injective. Soit  $b \in B$  et montrons que  $b$  a au plus un antécédent par  $f$ . Sinon, il existe  $a \in A$  et  $a' \in A$ , avec  $a \neq a'$ , tels que  $b = f(a)$  et  $b = f(a')$ . Alors,  $a$  et  $a'$  sont des éléments distincts de  $A$  tels que  $f(a) = f(a')$ , ce qui contredit l'hypothèse que  $f$  est injective. Inversement, supposons que tout élément de  $B$  ait au plus un antécédent et montrons que  $f$  est injective. Soit  $a$  et  $a'$  des éléments de  $A$ , avec  $a \neq a'$ , et montrons que  $f(a) \neq f(a')$ . Sinon,  $f(a)$  est un élément de  $B$  qui a deux antécédents,  $a$  et  $a'$ .

*Variante.* L'application  $f$  est injective si et seulement si, pour tous  $a, a' \in A$  tels que  $f(a) = f(a')$ , on a  $a = a'$ .

Une démonstration qu'une application  $f: A \rightarrow B$  est injective commencera ainsi par une phrase « Montrons que  $f$  est injective. Soit  $a, a' \in A$  tels que  $f(a) = f(a')$  ; montrons que  $a = a'$ . »

*Exemples.* L'application  $f: \mathbf{N} \rightarrow \mathbf{N}$ ,  $n \mapsto n^3 + n$  est injective. (Soit  $n, m \in \mathbf{N}$  tels que  $f(n) = f(m)$  ; montrons que  $n = m$ . On a

$$0 = f(n) - f(m) = (n^3 + n) - (m^3 + m) = (n^3 - m^3) + (n - m) = (n - m)(n^2 + nm + m^2 + 1).$$

Comme  $n^2 + nm + m^2 + 1 > 0$ , on a  $n = m$ .)

L'application  $g: \mathbf{R} \rightarrow \mathbf{R}$ ,  $x \mapsto x^2$  n'est pas injective car 1 et  $-1$  ont même image par  $g$  ; autrement dit,  $1 = 1^2 = (-1)^2$  a deux antécédents par  $g$ .

DÉFINITION 1.4. — On dit qu'une application  $f: A \rightarrow B$  est *surjective* si tout élément de  $B$  a (au moins) un antécédent. Cela revient à dire que  $f(A) = B$ .

L'application  $f: \mathbf{R} \rightarrow \mathbf{R}, x \mapsto x^3$ , est surjective. Mais pas l'application  $g: \mathbf{R} \rightarrow \mathbf{R}, x \mapsto x^2$ .

L'application  $f: \mathbf{R} \rightarrow \mathbf{R}_+, x \mapsto x^2$  est surjective (tout nombre réel positif a une racine carrée), mais pas injective.

DÉFINITION 1.5. — *On dit qu'une application  $f: A \rightarrow B$  est bijective si elle est à la fois injective et surjective.*

Cela revient à dire que tout élément de  $B$  a un antécédent et un seul par  $f$ . Si  $f$  est bijective, l'antécédent d'un élément  $b \in B$  est noté  $f^{-1}(b)$ . On a  $f \circ f^{-1} = \text{Id}_B$  : pour tout  $b \in B$ ,  $f^{-1}(b)$  est un antécédent de  $b$  par  $f$ , donc  $f(f^{-1}(b)) = b$ . On a  $f^{-1} \circ f = \text{Id}_A$  : pour tout  $a \in A$ ,  $f^{-1}(f(a))$  est l'unique antécédent de  $f(a)$  par  $f$  ; comme  $a$  est un antécédent, on a  $f^{-1}(f(a)) = a$ .

L'application  $f^{-1}$  est bijective ; on l'appelle la bijection réciproque de  $f$ . Si  $T$  est une partie de  $B$ , l'ensemble  $f^{-1}(T)$ , image réciproque de  $T$  par  $f$ , est aussi égal à l'image de  $T$  par  $f^{-1}$ .

*Exemples.* L'application  $f: \mathbf{R}_+ \rightarrow \mathbf{R}_+, x \mapsto x^2$  est bijective : tout nombre réel positif ou nul est le carré d'un unique nombre réel positif ou nul, sa racine carrée. La bijection réciproque de  $f$  est l'application  $g: \mathbf{R}_+ \rightarrow \mathbf{R}_+$  donnée par  $x \mapsto \sqrt{x}$ .

PROPOSITION. — *Soit  $f: A \rightarrow B$  et  $g: B \rightarrow C$  des applications.*

- a) *Si  $f$  et  $g$  sont injectives,  $g \circ f$  est injective.*
- b) *Si  $f$  et  $g$  sont surjectives,  $g \circ f$  est surjective.*
- c) *Si  $g \circ f$  est injective,  $f$  est injective.*
- d) *Si  $g \circ f$  est surjective,  $g$  est surjective.*

*Démonstration.* — Démontrons l'assertion c). Supposons que  $g \circ f$  soit injective et montrons que  $f$  l'est aussi. Soit  $a$  et  $a'$  des éléments de  $A$  tels que  $f(a) = f(a')$  et montrons que  $a = a'$ . On a  $g(f(a)) = g(f(a'))$ , c'est-à-dire  $(g \circ f)(a) = (g \circ f)(a')$ . Comme  $g \circ f$  est injective, on a alors  $a = a'$ .

Les autres propriétés sont laissées en exercice. □

1.6. *Ensembles finis, cardinal.* — Si  $n \geq 1$ , notons  $F_n$  l'ensemble  $\{1, \dots, n\}$  ; on pose  $F_0 = \emptyset$ .

LEMME. — *Soit  $n$  et  $m$  des entiers naturels et soit  $f: F_n \rightarrow F_m$  une bijection. Alors,  $n = m$ .*

*Démonstration.* — Montrons ce lemme par récurrence sur  $n$ .

Pour  $n = 0$ , si  $f: \emptyset \rightarrow F_m$  est une bijection, et si  $m \geq 1$ , on a  $1 \in F_m$ , mais 1 n'a pas d'antécédent dans  $\emptyset$  (un antécédent serait un élément de l'ensemble vide). Cela montre que  $m = 0$ .

Supposons le résultat vrai pour  $n$  et soit  $f: F_{n+1} \rightarrow F_m$  une bijection. Posons  $a = f(n+1)$  et définissons une application  $g$  de  $F_m$  sur lui-même en posant  $g(x) = x$  pour  $x < a$ ,  $g(a) = m$ , et  $g(x) = x - 1$  pour  $a + 1 \leq x \leq m$ . Cette application est bijective, l'unique antécédent de  $x$  étant lui-même si  $x < a$ ,  $x + 1$  si  $a \leq x \leq m - 1$ , et  $a$  si  $x = m$ . L'application  $h = g \circ f: F_{n+1} \rightarrow F_m$  est bijective et vérifie  $h(n+1) = g(a) = m$ . On en déduit que sa restriction à  $F_n$  définit une application injective de  $F_n$  dans  $F_{m-1}$ . Par récurrence,  $n = m - 1$ , donc  $n + 1 = m$ , ce qu'il fallait démontrer.

Le lemme est ainsi démontré par récurrence.  $\square$

On dit qu'un ensemble  $A$  est fini s'il existe un entier  $n \geq 0$  et une bijection de  $F_n$  sur  $A$ . Autrement dit, un ensemble est fini si et seulement si on peut numéroter ses éléments, en partant de 1 et en s'arrêtant à un certain entier  $n$ . Cet entier  $n$  ne dépend que de  $A$  : si  $f: F_n \rightarrow A$  et  $g: F_m \rightarrow A$  sont des bijections,  $g^{-1} \circ f$  est une bijection de  $F_n$  sur  $F_m$ , donc  $n = m$  d'après le lemme. Intuitivement, cela dit que si on numérote les éléments de  $A$  de deux façons différentes, on s'arrête en tout cas au même point.

Cet entier est appelé le *cardinal de  $A$* ; on le note  $\text{card } A$  ou  $|A|$ . Le cardinal de l'ensemble vide est 0, celui d'un singleton 1, etc. Deux ensembles finis qui sont en bijection ont même cardinal. Un ensemble qui n'est pas fini est dit infini.

## §2. Il est toujours bon d'avoir des principes

Deux principes généraux permettent d'évaluer le cardinal d'un ensemble : le principe des bergers et le principe d'inclusion-exclusion.

*2.1. Partitions.* — Soit  $A$  un ensemble et soit  $n$  un entier  $\geq 1$ . On dit que des parties  $A_1, \dots, A_n$  forment une partition de  $A$  si tout élément de  $A$  appartient à un et un seul des  $A_i$ . Cela signifie que les parties  $A_1, \dots, A_n$  sont deux à deux disjointes (elles n'ont aucun élément en commun) et que leur réunion est égale à  $A$ .

PRINCIPE DES BERGERS. — Soit  $X$  un ensemble fini et soit  $(A_i)_{1 \leq i \leq m}$  une partition de  $X$ , c'est-à-dire que chaque élément de  $X$  appartient à un des ensembles  $A_i$  et un seul. Alors,

$$\text{card } X = \sum_{i=1}^m \text{card } A_i.$$

Pour compter les éléments de  $X$ , il suffit de compter les éléments de chaque paquet  $A_i$  et de sommer les entiers obtenus.

Soit  $X$  un ensemble fini et  $A$  une partie de  $X$ . On a  $\text{card } A \leq \text{card } X$ ; l'égalité entraîne que  $A = X$ . Posons en effet  $B = X \setminus A$  (c'est le complémentaire de  $A$  dans  $X$ , c'est-à-dire l'ensemble des éléments de  $X$  qui n'appartiennent pas à  $A$ ). Par définition,  $A$  et  $B$  forment une partition de  $X$ . On a donc  $\text{card } X = \text{card } A + \text{card } B$ , donc  $\text{card } A \leq \text{card } X$ . Si  $\text{card } A = \text{card } X$ ,  $\text{card } B = 0$  donc  $B = \emptyset$ .

*Variante.* Soit  $f: X \rightarrow Y$  une application entre ensembles finis. Si  $f$  est injective,  $\text{card } X \leq \text{card } Y$ ; si  $f$  est surjective,  $\text{card } X \geq \text{card } Y$ . Dans les deux cas, l'égalité entraîne que  $f$  est bijective.

En particulier, si  $X$  est un ensemble fini et  $f: X \rightarrow X$  une application, les trois propriétés *a)  $f$  est injective; b)  $f$  est surjective; c)  $f$  est bijective;* sont équivalentes. Ceci est faux si  $X$  est infini. On remarquera par exemple que l'application  $f: \mathbf{N} \rightarrow \mathbf{N}$  définie par  $f(n) = 2n$  est injective mais pas surjective : son image est formée des nombres pairs.

*Cardinal du produit.* Si  $X$  et  $Y$  sont deux ensembles finis, le cardinal de l'ensemble produit  $X \times Y$  est égal à  $\text{card } X \times \text{card } Y$ . En effet, les parties  $X \times \{y\}$  de  $X \times Y$  forment

une partition de  $X \times Y$ . Chacune de ces parties est en bijection avec  $X$ , donc est de cardinal  $\text{card} X$ . Comme il y a  $\text{card} Y$  telles parties, on a  $\text{card}(X \times Y) = \text{card} X \times \text{card} Y$ .

*Cardinal de l'ensemble des fonctions de  $X$  dans  $Y$ .* Si  $X$  et  $Y$  sont deux ensembles finis, montrons que le cardinal de l'ensemble  $\mathcal{F}(X, Y)$  des applications de  $X$  dans  $Y$  est égal à  $(\text{card} Y)^{\text{card} X}$ . Le plus simple est de le démontrer par récurrence sur le cardinal de  $X$ . Si  $X$  est vide, il y a une seule application, de graphe vide (bof...). Si  $X$  est un singleton  $\{a\}$ , une application  $X \rightarrow Y$  est déterminée par l'image de  $a$ . On a donc  $\text{card} \mathcal{F}(X, Y) = \text{card} Y = (\text{card} Y)^{\text{card} X}$  dans ce cas. Supposons que cette formule soit vraie pour tout ensemble de cardinal  $< n$  et montrons la pour un ensemble  $X$  de cardinal  $n$ . On pose  $X' = X \setminus \{a\}$ , où  $a$  est un élément fixé de  $X$ . Pour se donner une application de  $X$  dans  $Y$ , il faut d'une part fixer l'image de  $a$  et d'autre part se donner une application de  $X'$  dans  $Y$ . Cela fait  $(\text{card} Y) \times (\text{card} Y)^{n-1} = (\text{card} Y)^n$  applications, d'où l'assertion voulue par récurrence sur  $n$ . Plus rigoureusement, définissons, si  $y \in Y$ , une partie  $\mathcal{F}_y$  de  $\mathcal{F}(X, Y)$  comme l'ensemble des  $f: X \rightarrow Y$  tels que  $f(a) = y$ . Ces parties  $\mathcal{F}_y$  forment une partition de  $\mathcal{F}(X, Y)$ ; chacune est en bijection avec  $\mathcal{F}(X', Y)$ , donc de cardinal  $(\text{card} Y)^{\text{card} X - 1}$ . Comme il y a  $(\text{card} Y)$  parties, le cardinal de  $\mathcal{F}(X, Y)$  vaut bien  $(\text{card} Y)^{\text{card} X}$ .

Comme conséquence du principe des bergers, on a le principe des tiroirs (utilisé pour la première fois par P. L. Dirichlet à la fin du XIX<sup>e</sup> siècle) : « si une commode de trois tiroirs contient quatre paires de chaussettes, l'un des tiroirs en contient au moins deux. »

PRINCIPE DES TIROIRS. — Soit  $X$  un ensemble fini et soit  $(A_i)_{1 \leq i \leq m}$  une partition de  $X$ . Si  $\text{card} X > m$ , une des parties est de cardinal  $\geq 2$ .

PRINCIPE D'INCLUSION-EXCLUSION. — Soit  $X$  un ensemble fini, soit  $A$  et  $B$  deux parties de  $X$ . Alors,

$$\text{card}(A \cup B) = \text{card} A + \text{card} B - \text{card}(A \cap B).$$

En effet, pour compter les éléments de  $A \cup B$ , il faut compter ceux de  $A$  et ceux de  $B$ . Ce faisant, ceux de  $A \cap B$  ont été comptés deux fois, d'où la formule.

*Exercices.* — 1) a) Au mois de janvier, Anatole a pris ses repas de midi au Restau U. Il y a mangé 17 fois de la pizza et 25 fois de la glace. Montrer qu'il a mangé de la pizza et de la glace au cours d'un des repas.

b) Dans une classe de 35 élèves, chaque étudiant doit apprendre au moins une des deux langues, anglais ou allemand. 25 étudient l'anglais et 20 apprennent les deux langues. Combien d'élèves étudient l'allemand ?

c) Hier soir, sur 100 français, 95 ont regardé le journal télévisé, 85 ont regardé le film qui suivait et 70 se sont couchés de bonne heure. Combien de français (au moins) se sont couchés tôt après avoir regardé le journal et le film ?

2) Le principe d'inclusion-exclusion donne lieu à des inégalités : si  $A_1, \dots, A_n$  sont des parties d'un ensemble  $X$ , montrer par exemple que

$$\sum_i |A_i| - \sum_{i \neq j} |A_i \cap A_j| \leq \left| \bigcup_i A_i \right| \leq \sum_i |A_i|.$$

Généraliser.

3) On considère  $n$  objets de différentes couleurs. Si  $a$  est un entier tel que  $a \leq \sqrt{n-1}$ , montrer que l'on peut trouver ou bien  $a+1$  objets de la même couleur, ou bien  $a+1$  objets de couleurs toutes différentes.

4) Dans un groupe de 6 personnes, deux personnes quelconques ou bien s'aiment, ou bien se détestent. Montrer que l'on peut en trouver 3 qui sont amis, ou 3 qui sont mutuellement ennemis. (*Fixer une personne Anatole ; parmi ses 5 relations, Anatole a (au moins) 3 amis, ou 3 ennemis. Si Anatole a trois amis et que deux d'entre eux sont amis, le résultat est obtenu. Sinon...*)

5\*) 1958 points sont reliés deux à deux par un segment d'une couleur parmi 6. Montrer qu'il existe un triangle dont les trois côtés sont de la même couleur.

### §3. Triangle de Pascal

Soit  $X$  un ensemble fini, de cardinal  $n$ .

Notons  $\mathcal{P}(X)$  l'ensemble des parties de  $X$ .

PROPOSITION. — Si  $\text{card} X = n$ , le cardinal de  $\mathcal{P}(X)$  est égal à  $2^n$ .

Intuitivement. Supposons que  $X = \{1, \dots, n\}$ . Pour construire une partie  $A$  de  $X$ , on peut décider si  $1 \in A$  ou pas, d'où deux choix. Puis deux nouveaux choix pour décider si  $2 \in A$  ou pas, et ainsi de suite.

Une version « fonctionnelle » de la démonstration intuitive. Il revient au même de se donner une partie  $A$  de  $X$  que de se donner sa *fonction indicatrice*  $\chi_A$  définie par  $\chi_A(x) = 1$  si  $x \in A$  et  $\chi_A(x) = 0$  sinon. L'ensemble des fonctions indicatrices est l'ensemble des fonctions de  $X$  dans  $\{0, 1\}$  ; il est donc de cardinal  $2^{\text{card} X}$ .

Par récurrence. Soit  $a$  un élément fixé de  $X$  et posons  $Y = X \setminus \{a\}$ , de sorte que  $\text{card} Y = n - 1$ . Par récurrence, l'ensemble  $Y$  possède  $2^{n-1}$  parties. Parmi les parties de  $X$ , certaines contiennent  $a$  et d'autres non. Une partie  $A$  de  $X$  qui contient  $a$  est de la forme  $\{a\} \cup B$ , où  $B = A \setminus \{a\}$  est une partie de  $Y$  ; il y a  $2^{n-1}$  parties  $B$  de  $Y$  ; d'où  $2^{n-1}$  parties de  $X$  qui contiennent  $a$ . Une partie  $A$  de  $X$  qui ne contient pas  $a$  est une partie de  $Y$  ; il y en a donc  $2^{n-1}$ . Finalement, l'ensemble  $X$  possède exactement  $2^{n-1} + 2^{n-1} = 2^n$  parties.

Notons maintenant  $\mathcal{P}_p(X)$  l'ensemble des parties de  $X$  dont le cardinal est exactement  $p$ . Si  $p < 0$  ou si  $p > \text{card} X$ , on a évidemment  $\mathcal{P}_p(X) = \emptyset$ . Une seule partie de  $X$  est de cardinal nul (la partie vide), une seule partie de  $X$  est de cardinal  $\text{card} X$ ,  $X$  lui-même.

Si  $n = \text{card} X$ , le cardinal de  $\mathcal{P}_p(X)$  est noté  $C_n^p$ , ou  $\binom{n}{p}$  avec les notations anglo-saxonnes. On l'appelle le nombre de *combinaisons* (sans répétition) de  $p$  éléments parmi  $n$ . On a ainsi  $C_n^p = 0$  si  $p < 0$  ou  $p > n$  et  $C_n^0 = C_n^n = 1$ .

Il est commode d'étudier en même temps le nombre  $A_n^p$  d'arrangements de  $p$  éléments parmi  $n$ , un arrangement étant la donnée de  $p$  éléments distincts numérotés de 1 à  $p$ . C'est aussi le nombre d'applications *injectives* de  $\{1, \dots, p\}$  dans  $\{1, \dots, n\}$ .

Tout arrangement définit une combinaison (on oublie la numérotation) et le nombre d'arrangements qui définissent une combinaison donnée est précisément égal au nombre de numérotations possibles d'un ensemble à  $p$  éléments. Autrement dit,

$$C_n^p = \frac{A_n^p}{A_p^p}.$$

Calculons  $A_n^p$ , c'est-à-dire comptons le nombre de suites d'entiers distincts  $(x_1, \dots, x_p)$  avec  $x_i \in \{1, \dots, n\}$ . On a  $n$  choix pour  $x_1$ , il reste alors  $n - 1$  choix pour  $x_2$ , puis  $n - 2$  choix pour  $x_3$ , etc. et finalement  $n - p + 1$  choix pour  $x_p$ . Ainsi,

$$A_n^p = n(n-1) \dots (n-p+1) = \frac{n!}{(n-p)!}.$$

En particulier,

$$A_p^p = p!$$

d'où l'on déduit

$$C_n^p = \frac{n!}{p!(n-p)!}, \quad 0 \leq p \leq n.$$

Soit  $X$  un ensemble de cardinal  $n$  et cherchons à évaluer le nombre de parties à  $p$  éléments de  $X$ . Supposons  $n \geq 1$  et soit  $a$  un élément de  $X$ . Une partie  $A \subset X$  de cardinal  $p$  peut contenir  $a$ ,  $A \setminus \{a\}$  est alors une partie de  $X \setminus \{a\}$  de cardinal  $p - 1$ . Elle peut aussi ne pas contenir  $a$  auquel cas c'est une partie de  $X \setminus \{a\}$  de cardinal  $p$ . Il en résulte que

$$C_n^p = C_{n-1}^{p-1} + C_{n-1}^p, \quad 0 \leq p \leq n-1.$$

On dispose classiquement les nombres de combinaisons  $C_n^p$ , comme un tableau triangulaire où  $n$  est l'indice de ligne et  $p$  l'indice de colonne, supposé tel que  $0 \leq p \leq n$ , tous les autres nombres étant nuls :

$$\begin{array}{cccccc} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ 1 & 5 & 10 & 10 & 5 & 1 & \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 \end{array}$$

chaque nombre est ainsi la somme de celui qui est au-dessus de lui et de celui qui est à sa gauche. Ce triangle est souvent appelé triangle de Pascal bien qu'il figure dans des textes chinois du VI<sup>e</sup> siècle, que Pascal le présenta à demi-renversé (*Triangulus arithmeticus* (1654), in *Œuvres complètes*, Bibliothèque de la Pléiade, 1998, p. 174).

FORMULE DU BINÔME DE NEWTON. — Si  $a$  et  $b$  sont deux nombres réels et  $n \geq 0$ , on a

$$(a + b)^n = \sum_{p=0}^n C_n^p a^p b^{n-p}.$$

Pour cette raison, les coefficients  $C_n^p$  sont appelés *coefficients binomiaux*.

On peut la démontrer de manière combinatoire : si l'on développe le produit  $(a + b)(a + b) \dots (a + b)$ , on doit compter le nombre de termes  $a^p b^{n-p}$ . Il y en a exactement  $C_n^p$  car on doit choisir les  $p$  facteurs dans lequel on multiplie  $a$ , et multiplier  $b$  dans les  $n - p$  autres.

On peut aussi le démontrer par récurrence : la formule est vraie pour  $n = 0$  car  $(a + b)^0 = 1 = C_0^0 a^0 b^0$ . Elle est vraie pour  $n = 1$  car elle s'écrit alors  $(a + b)^1 = a + b$ . Supposons la vraie pour  $n$ . Alors,

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \left( \sum_{p=0}^n C_n^p a^p b^{n-p} \right) \\ &= \left( \sum_{p=0}^n C_n^p a^{p+1} b^{n-p} \right) + \left( \sum_{p=0}^n C_n^p a^p b^{n+1-p} \right) \\ &= \left( \sum_{q=1}^{n+1} C_n^{q-1} a^q b^{n+1-q} \right) + \left( \sum_{q=0}^n C_n^q a^q b^{n+1-q} \right) \\ &= b^{n+1} + \sum_{q=1}^n C_n^{q-1} a^q b^{n+1-q} + a^{n+1} \\ &= a^{n+1} + b^{n+1} + \sum_{q=1}^n (C_n^{q-1} + C_n^q) a^q b^{n+1-q} \\ &= \sum_{q=0}^{n+1} C_{n+1}^q a^q b^{n+1-q}. \end{aligned}$$

La formule est ainsi vraie pour tout entier  $n$ .

*Exercices.* — 1) a) Soit  $X$  et  $Y$  deux ensembles finis. Combien y a-t-il d'applications injectives de  $X$  dans  $Y$ ? (La même question avec « surjectives » est naturelle, mais plus difficile.)

b) Estimer le nombre d'applications injectives de  $\{1, \dots, 30\}$  dans  $\{1, \dots, 365\}$ . Sur une classe de 30 élèves, quelle est la probabilité que deux élèves soient nés le même jour? (*Paradoxe des anniversaires*)

2) a) Démontrer la relation  $C_n^p = C_{n-1}^{p-1} + C_{n-1}^p$  pour  $n > p \geq 1$  en utilisant la formule qui calcule  $C_n^p$  à l'aide de factorielles.

b) Inversement, à l'aide de cette identité, démontrer par récurrence la formule qui calcule  $C_n^p$ .

3) a) Démontrer de deux façons la formule  $C_n^p = \frac{n}{p} C_{n-1}^{p-1}$  pour  $n \geq p \geq 1$ .

b) Démontrer de deux façons que  $C_n^p = C_n^{n-p}$ .

4) a) À l'aide de la formule du binôme, démontrer que

$$C_n^0 + C_n^1 + \dots + C_n^{n-1} + C_n^n = 2^n.$$

- b) Calculer de même  $\sum_{p=0}^n (-1)^p C_n^p$ .
- c) Calculer  $\sum_{p=1}^n p C_n^p$  et  $\sum_{p=2}^n p(p-1) C_n^p$ . En déduire la valeur de  $\sum_{p=1}^n p^2 C_n^p$ .
- d) Retrouver la question précédente en dérivant (une puis deux fois) la formule du binôme pour  $(1+x)^n$ .
- 5) a) En développant  $(1+x)^{2n} = (1+x)^n(1+x)^n$ , montrer que  $C_{2n}^n = \sum_{p=0}^n (C_n^p)^2$ . (Remarquer que  $C_n^p = C_n^{n-p}$ .)
- b) Donner une interprétation combinatoire de la formule précédente.
- 6) On pose  $F_n = \sum_{p \leq n/2} C_{n-p}^p = C_n^0 + C_{n-1}^1 + C_{n-2}^2 + \dots$  (Le dernier terme est  $C_p^p$  si  $n = 2p$  est pair, et  $C_{p+1}^p$  si  $n = 2p + 1$  est impair.)
- a) Calculer  $F_0, F_1, F_2, \dots, F_5$ .
- b) Montrer que  $F_{n+1} = F_n + F_{n-1}$  (suite de Fibonacci).
- 7) Une combinaison avec répétition de  $p$  éléments parmi  $n$  est une liste de  $p$  éléments de  $\{1, \dots, n\}$ , non nécessairement distincts, et où l'ordre n'intervient pas. On note  $R_n^p$  leur nombre.
- a) Montrer que l'on a  $R_n^p = R_{n-1}^p + R_n^{p-1}$  si  $n \geq 1$  et  $p \geq 1$ . Montrer aussi  $R_n^0 = 1, R_n^1 = n$  et  $R_1^p = 1$ , pour  $n \geq 1, p \geq 1$ .
- b) En déduire par récurrence que  $R_n^p = C_{n+p-1}^p$ .
- c) (autre méthode) On associe à une partie à  $n-1$  éléments de  $\{1, \dots, n+p-1\}$  une combinaison avec répétition de la façon suivante : si cette partie est formée de  $n-1$  entiers  $x_1 < \dots < x_{n-1}$ , on choisit  $(x_1 - 1)$  fois l'entier 1,  $(x_2 - x_1 - 1)$  fois l'entier 2, etc.,  $(x_{n-1} - x_{n-2} - 1)$  fois l'entier  $n-1$  et pour finir  $(n + p - x_{n-1} - 1)$  fois l'entier  $n$ . Montrer que cela définit une application bijective et en déduire la formule de la question précédente.
- 8) Un ordinateur (par exemple) ne sait calculer que le produit de deux facteurs et on s'intéresse au nombre de façons  $K_n$  d'introduire des parenthèses dans le produit  $x_1 x_2 \dots x_n$  de sorte à pouvoir le calculer. Si  $n = 2$ , c'est un produit de deux facteurs, donc  $K_2 = 1$ , mais on a  $K_3 = 2$  correspondant aux parenthésages  $x_1(x_2 x_3)$  et  $(x_1 x_2)x_3$ , de même que  $K_4 = 5$  avec les parenthésages
- $$(x_1 x_2)(x_3 x_4), ((x_1 x_2)x_3)x_4, (x_1(x_2 x_3))x_4, x_1((x_2 x_3)x_4), \text{ et } x_1(x_2(x_3 x_4)).$$
- a) Dans un parenthésage, le dernier produit que l'on calcule est le produit de deux facteurs : le sous-produit des  $p$  premiers, et celui des  $n-p$  derniers. En déduire que
- $$K_n = \sum_{p=1}^{n-1} K_p K_{n-p}.$$
- b\*) Montrer que  $K_n = \frac{1}{n} C_{2n-2}^{n-1}$ .

**§4. Probabilités**

(Paragraphe non enseigné en 2004–2005)

Une probabilité sur un ensemble fini  $\Omega$  est une application  $p: \mathcal{P}(\Omega) \rightarrow [0, 1]$  qui associe à toute partie  $A$  de  $\Omega$  sa probabilité  $p(A)$  de sorte que l'on ait  $p(\emptyset) = 0, p(\Omega) = 1$ ,

et  $p(A \cup B) = p(A) + p(B)$  si  $A$  et  $B$  sont deux parties *disjointes* de  $\Omega$ . Si  $A$  et  $B$  sont deux parties quelconques de  $\Omega$ , posons  $C = A \cap B$ ,  $A' = A \setminus C$  et  $B' = B \setminus C$ . On a alors et  $p(A \cup B) = p(A \cup B') = p(A) + p(B')$  car  $A$  et  $B'$  sont disjointes. De plus,  $p(B) = p(B') + p(C)$ . Il en résulte

$$p(A \cup B) + p(A \cap B) = p(A) + p(B).$$

Dans le langage des probabilités, l'ensemble  $\Omega$  est appelé *univers* et ses parties *événements*. Des événements définis par des parties disjointes sont dits *incompatibles*. Les singletons sont parfois appelés *événements élémentaires*. Notons  $\Omega = \{x_1, \dots, x_N\}$  et  $p_i = p(\{x_i\})$ . Si  $A = \{x_{i_1}, \dots, x_{i_m}\}$  est un événement, de cardinal  $m$ , on a alors

$$p(A) = \sum_{j=1}^m p(x_{i_j}) = \sum_{j=1}^m p_{i_j}.$$

En particulier,

$$1 = p(\Omega) = \sum_{i=1}^N p_i.$$

Autrement dit, la probabilité est déterminée par les probabilités des événements élémentaires, astreintes à être de somme 1.

La probabilité uniforme sur  $\Omega$  est définie par  $p(\{x\}) = 1/\text{card}\Omega$  pour tout  $x$  de  $\Omega$ . Alors,  $p(A) = \text{card } A / \text{card}\Omega$  pour toute partie  $A \subset \Omega$ .

Supposons qu'on *sache* qu'un événement  $A$  s'est produit. Alors, l'ensemble probabilisé  $\Omega$  ne modélise plus tout à fait la réalité, puisque il continue à contenir des événements — tels le complémentaire de  $A$  — qui n'ont plus aucune chance de se produire. On est ainsi amené à définir la probabilité conditionnelle suivant  $A$  : elle est définie à condition que  $p(A) \neq 0$  par la formule

$$p(B|A) = \frac{p(B \cap A)}{p(A)}.$$

On l'interprète comme la probabilité de l'événement  $B$  sachant que  $A$  se produit.

On dit que deux événements  $A$  et  $B$  sont indépendants si  $p(A \cap B) = p(A)p(B)$ . Cela signifie que savoir que  $A$  se produit ne change rien à la probabilité pour  $B$  de se produire.

Regardons un exemple, pour lequel on tire successivement deux dés. On représente cela par l'ensemble d'événements  $\Omega = \{1, 2, 3, 4, 5, 6\}^2$  dont les éléments sont les couples  $(a, b)$  correspondant à la valeur du premier dé et à celle du second. La probabilité d'un couple donné est  $\frac{1}{36}$ .

Les événements  $\{a = 1\}$  et  $\{b = 1\}$  sont indépendants : chacun a probabilité  $\frac{6}{36} = \frac{1}{6}$ , la probabilité de leur intersection est  $\frac{1}{36}$ .

Les événements  $A = \{a \leq 3\}$  et  $B = \{a + b \geq 7\}$  ne sont par contre pas indépendants. La probabilité du premier est  $\frac{3}{6} = \frac{1}{2}$ . L'événement  $\{a + b \geq 7\}$  se produit dans les cas  $(6, b)$  avec  $b$  quelconque,  $(5, b)$  avec  $b \geq 2$ , etc. jusque  $(1, b)$  avec  $b = 6$ , d'où  $6+5+4+3+2+1 = 21$  cas. Sa probabilité est ainsi de  $\frac{21}{36} = \frac{7}{12}$ . L'événement intersection correspond aux tirages  $(1, b)$  avec  $b = 6$ ,  $(2, b)$  avec  $b \geq 5$  et  $(3, b)$  avec  $b \geq 4$  et ces 6 tirages ont donc probabilité  $\frac{6}{36} = \frac{1}{6}$ . On constate que  $p(A)p(B) = \frac{1}{2} \frac{7}{12} = \frac{7}{24}$  alors que  $p(A \cap B) = \frac{1}{6} = \frac{4}{24}$ .

La probabilité pour  $B$  de survenir sachant que  $A$  est arrivé est ainsi  $p(B|A) = p(A \cap B)/p(A) = \frac{1}{3}$ . Intuitivement : comme la valeur de  $a$  est petite, on a moins de chance d'obtenir une valeur de  $a + b$  qui soit au moins 7.

Une des applications des probabilités conditionnelles est en statistique. Imaginons que vous écoutiez la météo chaque soir et que vous notiez la prévision (disons, ensoleillé, nuageux, ou changeant) ainsi que le temps qu'il a effectivement fait (beau ou mauvais). Les données que vous avez recueillies sont résumées dans le tableau :

	ensoleillé	nuageux	changeant
beau temps	0,8	0,1	0,1
mauvais temps	0,4	0,4	0,2

qui signifie que sur tous les jours où il a fait beau, la météo a prévu un temps ensoleillé 8 fois sur 10, un temps nuageux ou changeant une fois sur 10. Vous avez aussi remarqué qu'il fait beau 9 fois sur 10 (cela se passe dans un pays imaginaire!). La météo prévoit du beau temps pour demain. Comment estimer la probabilité qu'il fera effectivement beau? Appelons  $E, N, C$  les événements correspondant aux prévisions d'un temps ensoleillé, nuageux, changeant, et  $B, M$  l'événement correspondant à un beau ou à un mauvais temps. Le tableau ci-dessus signifie donc que  $p(E|B) = 0,8$ , etc. On veut calculer à l'inverse  $p(B|E)$ , la probabilité qu'il fasse beau sachant que la météo prévoit un temps ensoleillé.

On a  $p(B) = 0,9$  et  $p(M) = 0,1$ . Par ailleurs, les probabilités conditionnelles résumées par le tableau s'écrivent  $p(E \cap B) = 0,8p(B)$ ,  $p(N \cap B) = 0,1p(B)$ ,  $p(C \cap B) = 0,1p(B)$ , et aussi  $p(E \cap M) = 0,4p(M)$ ,  $p(N \cap M) = 0,4p(M)$  et  $p(C \cap M) = 0,2p(M)$ . Par suite, on connaît  $p(E \cap B) = 0,72$  et  $p(E \cap M) = 0,04$ . Comme  $E \cap B$  et  $E \cap M$  sont des événements incompatibles et que leur réunion est  $E$ , on a

$$p(E) = p(E \cap B) + p(E \cap M) = 0,72 + 0,04 = 0,76.$$

Finalement,

$$p(B|E) = \frac{p(B \cap E)}{p(E)} = \frac{0,72}{0,76} \sim 0,95.$$

On peut donc estimer à 95 chances sur 100 la probabilité qu'il fera effectivement beau.

Plus généralement :

FORMULE DE BAYES. — Soit  $A_1, \dots, A_n$  une partition de  $\Omega$  avec  $p(A_i) > 0$  pour tout  $i$ . Soit  $E$  un événement quelconque de probabilité  $p(E) > 0$ . Alors,

$$p(A_i|E) = \frac{p(A_i)p(E|A_i)}{\sum_{j=1}^n p(A_j)p(E|A_j)}.$$

C'est plus simple que ça n'en a l'air. Par définition,  $p(A_j)p(E|A_j) = p(E \cap A_j)$ . La somme au dénominateur du second membre est donc la somme des probabilités des événements incompatibles  $E \cap A_j$  dont la réunion est  $E$ . Le dénominateur vaut donc  $p(E)$ . Le numérateur vaut lui  $p(E \cap A_i)$ . Le second membre est donc égal à  $p(E \cap A_i)/p(E) = p(A_i|E)$ , ce qu'il fallait démontrer.

L'utilisation de cette formule est la suivante. Les événements  $A_i$  correspondent à des événements « réels » (le temps qu'il fait, le fait qu'on soit malade ou pas, qu'une pièce

soit correctement usinée, etc.) et l'événement  $E$  est le résultat d'un test qui n'est pas totalement fiable (prévision météo, test de vaccination, contrôle aléatoire dans une chaîne de production, etc.). Les probabilités  $p(E|A_i)$  représentent la fiabilité du test  $E$  : ce que dit  $E$  sachant que  $A_i$  se produit. Les probabilités  $p(A_i)$  sont inconnues en général, mais peuvent être estimées sur une grande échelle (observations du temps, épidémiologique, etc.). La formule permet de calculer une estimation de la probabilité qu'on soit dans le cas  $A_i$  sachant que le test  $E$  est positif.

Intéressons-nous maintenant à un jeu où l'on reproduirait un grand nombre de fois une expérience aléatoire, chacune étant effectuée de manière indépendante des précédentes.

On peut par exemple procéder à  $n$  tirages à pile ou face successifs, indépendants. On représente ceci par l'univers  $\Omega = \{P, F\}^n$  avec la probabilité uniforme (la pièce n'est pas pipée). La probabilité d'obtenir  $p$  fois face est alors égale à  $C_n^p/2^n$ . Le nombre de fois que l'on obtient face est compris entre 0 et  $n$ . On retrouve ainsi la formule

$$2^n = \sum_{p=0}^n C_n^p.$$

Supposant qu'on gagne 1€ à chaque tirage  $P$  (et qu'on ne perde rien sinon), combien pouvons-nous espérer gagner ? Comme la situation est symétrique, la réponse est alors claire :  $n/2$  euro. En effet, un joueur symétrique qui gagnerait 1 € à chaque tirage  $F$  peut espérer gagner la même somme. À nous deux, nous gagnons à chaque coup, donc  $n$  €, que nous devons nous partager...

Que se passerait-il si le jeu était truqué ? Imaginons donc une pièce pipée qui tombe sur  $P$  avec probabilité  $\pi$  et sur  $F$  avec probabilité  $1 - \pi$ . La probabilité d'obtenir  $p$  fois pile est égale à  $\pi_p = C_n^p \pi^p (1 - \pi)^{n-p}$  : les cas favorables sont les parties à  $p$  éléments de  $\{1, \dots, n\}$  ; chacun de ces cas apparaît avec probabilité  $\pi^p (1 - \pi)^{n-p}$ . Puisque le nombre de pile apparues est compris entre 0 et  $n$ , on obtient la formule :

$$1 = \sum_{p=0}^n C_n^p \pi^p (1 - \pi)^{n-p},$$

autrement dit, une interprétation probabiliste de la formule du binôme de Newton !

Quelle est l'espérance de gain : 0 avec probabilité  $\pi_0$ , 1 avec probabilité  $\pi_1$ , etc., d'où

$$G = \sum_{p=0}^n p \pi_p = \sum_{p=0}^n C_n^p p \pi^p (1 - \pi)^{n-p}.$$

Rappelons que  $p C_n^p = n C_{n-1}^{p-1}$ , si  $1 \leq p \leq n$ . Ainsi, comme le terme correspondant à  $p = 0$  est nul, on a

$$\begin{aligned} G &= \sum_{p=1}^n n C_{n-1}^{p-1} \pi^p (1 - \pi)^{n-p} \\ &= n \pi \sum_{p=1}^n C_{n-1}^{p-1} \pi^{p-1} (1 - \pi)^{n-p} \end{aligned}$$

$$\begin{aligned}
&= n\pi \sum_{k=0}^{n-1} C_{n-1}^k \pi^k (1-\pi)^{n-1-k} \\
&= n\pi(\pi + (1-\pi))^{n-1} = n\pi.
\end{aligned}$$

On peut ainsi espérer gagner  $n\pi$ .

Quelle est l'espérance de gain si l'on gagne 1 € lorsque  $P$  tombe, mais qu'on en perd un autre si c'est  $F$  qui apparaît. On interprète ce nouveau jeu comme : miser 1 € à chaque coup, et en gagner 2 si  $P$  tombe. L'espérance de gain est donc  $-n+2n\pi = n(2\pi-1)$ . Si  $\pi = 1/2$ , elle est nulle ; si  $\pi > 1/2$ , la pièce est truquée en notre faveur, donc on peut espérer s'enrichir ; si au contraire, ce qui est probable,  $\pi < 1/2$ , on ferait mieux d'arrêter rapidement de jouer.

*Exercices.* — 1) a) Quelle est la probabilité d'avoir deux dés identiques en lançant deux dés ? en lançant trois dés ?

b) Au Yam, votre deuxième lancer vous fournit 2, 3, 3, 4, 5. Que vaut-il mieux faire : lancer 2, 4, 5 pour un brelan de 3 ou le 3 pour une des deux suites ?

2) Quelle est la probabilité d'avoir trois bons numéros au Loto sur une grille de six numéros parmi 49 ? Quelle est l'espérance de gain (on néglige l'influence des autres joueurs) ? Sachant qu'une partie des mises du Loto est reversée directement à l'État, pourquoi les français pensent-ils que les impôts sont trop élevés ?

3) a) Deux joueurs reçoivent chacun 5 cartes. Le premier a un As ; quelle est la probabilité que le second ait une paire d'As ?

b) Quelle est la probabilité de n'avoir aucun honneur (Valet, Dame, Roi, As) parmi les 13 cartes d'une main de bridge ?

c\*) Au bridge, quelle est la probabilité que Sud n'ait pas de trèfle ? En ouvrant son jeu, Nord constate qu'il a 6 trèfles ; quelle est alors, selon lui, la probabilité que Sud n'ait pas de trèfle. Si Ouest ouvre d'un trèfle, admettant que cela signifie qu'il en a exactement trois, quelle est, toujours pour Nord, la probabilité que Sud n'ait pas de trèfle. Si l'enchère de Ouest signifie qu'il en a au moins trois, comment estimez-vous la probabilité pour Sud de n'avoir aucun trèfle ?

4) On dispose de  $n$  pièces indépendantes mais biaisées, de sorte que la probabilité que la  $k$ -ième pièce tombe sur *face* est  $1/(2k+1)$ . Quelle est la probabilité qu'en lançant les  $n$  pièces, le nombre de *faces* apparues soit impair ?

5) On suppose que  $p(A) = p(B) = \frac{1}{2}$  et  $p(A \cup B) = \frac{2}{3}$ . Les événements  $A$  et  $B$  sont-ils indépendants ?

6) Soit  $p$  une probabilité (finie) sur un ensemble  $\Omega$  et soit  $A$  une partie de  $\Omega$  de probabilité  $p(A) > 0$ . On pose, si  $X \subset \Omega$ ,  $p_A(X) = p(X|A)$ . Montrer que  $p_A$  est une probabilité sur  $\Omega$ .



## CHAPITRE 3

### DIVISION EUCLIDIENNE

---

#### §1. Un peu de terminologie algébrique

Le but de ce premier paragraphe est d'expliquer comment l'on peut *construire* les entiers relatifs à partir des entiers naturels donnés par les axiomes de Peano.

Il manque à l'ensemble des entiers naturels, avec son addition et sa multiplication, une soustraction (et d'ailleurs aussi une division, mais nous n'en parlerons qu'à la fin de ce cours). Si l'on peut écrire sans peine que  $3 - 1 = 2$ , pour dire que  $3 = 2 + 1$ , le symbole  $-3$  doit être défini, de même que l'on doit, dans une seconde étape, établir la validité d'une formule comme  $1 - 4 = -3$ .

Tout le problème est de définir des « entiers négatifs » et une soustraction.

Il y a deux moyens pour cela. Le plus élémentaire consiste à considérer un ensemble réunion de  $\{0\}$  et de deux copies des entiers non nul ; la première copie sera identifiée aux entiers strictement positifs, l'autre aux entiers strictement négatifs. Il faut alors fabriquer l'addition (par récurrence) et la multiplication (par la règle des signes). Cela marche dans ce cas, mais n'est ni très général, ni très élégant.

La meilleure méthode revient à introduire formellement « toutes » les soustractions  $a - b$  et à identifier celles qui doivent l'être. Cela nécessite un petit apparté.

*1.1. Relations d'équivalence.* — Soit  $S$  un ensemble et soit  $\mathcal{R}$  une relation entre les éléments de  $S$ . Comme exemple concret de relations, prenons pour  $S$  l'ensemble des êtres vivants et pour relation  $\mathcal{R}$  l'une des suivantes : « est né avant », « parle la même langue que », « n'est pas de la même nationalité que ».

On dit que la relation  $\mathcal{R}$  est *réflexive* : pour tout  $x \in S$ ,  $x\mathcal{R}x$ . Les relations « est né avant » et « parle la même langue que » sont réflexives, mais pas la relation « n'est pas de la même nationalité que ».

On dit que la relation  $\mathcal{R}$  est *symétrique* si pour tous  $x$  et  $y \in S$ , la condition  $x\mathcal{R}y$  entraîne que  $y\mathcal{R}x$ . Les relations « parle la même langue que » et « n'est pas de la même nationalité que » sont symétriques, mais pas la relation « est né avant ».

On dit que la relation  $\mathcal{R}$  est *transitive* si pour sous  $x$ ,  $y$  et  $z \in S$ , les conditions  $x\mathcal{R}y$  et  $y\mathcal{R}z$  entraînent  $x\mathcal{R}z$ . La relation « est né avant » est transitive, mais pas la relation « n'est pas de la même nationalité que ». La relation « parle la même langue que » est transitive si l'on suppose qu'un individu ne parle qu'une langue, mais pas sinon (si

Alice parle anglais et français, Bernard anglais et allemand, Charles allemand, Alice et Bernard sont en relation, de même que Bernard et Charles, mais pas Alice et Charles).

La relation d'ordre  $<$  dans les entiers naturels est transitive et antiréflexive (sa négation est réflexive).

Une relation qui est réflexive, symétrique est transitive est appelée *relation d'équivalence*. Dans l'ensemble des êtres humains vivants, la relation « est de la même nationalité que » est donc une relation d'équivalence (on exclut de cette discussion les problèmes liés à la double nationalité ou aux apatrides).

Si  $\mathcal{R}$  est une telle relation dans un ensemble  $S$ , on peut d'une certaine manière « identifier » tous les éléments qui sont en relation : au moins de ce point de vue, ils sont équivalents.

On appelle ainsi classe d'équivalence d'un élément  $x$  l'ensemble de tous les éléments de  $S$  qui sont équivalents à  $x$ . Notons  $C(x)$  la classe d'équivalence de  $x$  ; c'est une partie de  $S$ . Pour la relation « est de la même nationalité que », la classe d'équivalence d'un individu est l'ensemble de ceux qui ont la même nationalité que lui. Les classes d'équivalences sont donc les ensembles des Français, des Allemands, des Polonais, etc.

Observons un fait important : soit  $x$  et  $y$  des éléments de  $S$  dont les classes d'équivalence ont un élément commun, disons  $z$ . Par hypothèse,  $x\mathcal{R}z$  et  $y\mathcal{R}z$  ; comme la relation est symétrique, on a  $z\mathcal{R}y$  ; comme elle est transitive, on a  $x\mathcal{R}y$ . Soit alors  $a$  un élément quelconque de  $C(x)$  ; On a  $x\mathcal{R}a$ , d'où  $y\mathcal{R}a$  par symétrie et transitivité, si bien que  $a \in C(y)$ . Cela démontre que  $C(x) \subset C(y)$  et l'on démontre de même l'autre inclusion, si bien que  $C(x) = C(y)$ . Autrement dit : *deux classes d'équivalence sont ou bien disjointes ou bien égales*. Par conséquent, à condition de ne pas répéter deux fois une même classe, les classes d'équivalence des éléments de  $S$  définissent une partition de  $S$ .

Inversement, soit  $S$  un ensemble et soit  $(S_1, S_2, \dots)$  une partition de  $S$ . On peut définir une relation  $\mathcal{R}$  dans  $S$  en décrétant que  $x\mathcal{R}y$  si et seulement si il existe un indice  $i$  tel que  $x$  et  $y$  appartiennent tous deux à  $S_i$ . C'est une relation d'équivalence dont les classes d'équivalence sont exactement les parties  $S_i$ .

Par définition, l'ensemble quotient de  $S$  par la relation d'équivalence  $\mathcal{R}$  est l'ensemble de toutes les classes d'équivalence. C'est un ensemble de parties de  $S$ , donc un élément de  $\mathcal{P}(\mathcal{P}(S))$ . On le note souvent  $S/\mathcal{R}$  ; ses éléments sont les classes d'équivalence. Le passage à la classe d'équivalence définit une application  $C$  de  $S$  dans  $S/\mathcal{R}$  : cette application associe à un élément  $x \in S$  sa classe d'équivalence  $C(x)$  qui est, par définition, un élément de  $S/\mathcal{R}$ . Cette application  $C$  est surjective ; par construction, la relation  $x\mathcal{R}y$  et l'égalité  $C(x) = C(y)$  sont des assertions équivalentes.

*1.2. Construction de l'ensemble des entiers relatifs.* — Comme je l'ai déjà dit plus haut, il s'agit d'introduire toutes les soustractions possibles puis d'identifier celles qui sont censées donner le même résultat. Une soustraction  $a - b$  revient à la donnée des deux entiers  $a$  et  $b$ , dans un ordre déterminé. Introduisons ainsi l'ensemble  $S = \mathbf{N}^2$  des couples  $(a, b)$  d'éléments de  $\mathbf{N}$ . Deux soustractions  $a - b$  et  $c - d$  doivent donner le même résultat si  $a + d = b + c$ . Définissons ainsi une relation  $\mathcal{R}$ , « est équivalent à », dans  $S$  en décrétant que  $(a, b)\mathcal{R}(c, d)$  si  $a + d = b + c$ .

*La relation dans  $S$  ainsi définie est une relation d'équivalence.*

- Elle est réflexive : tout couple  $(a, b)$  est équivalent à lui-même. En effet,  $a + b = b + a$ .
- Elle est symétrique : si un couple  $(a, b)$  est équivalent à un couple  $(c, d)$ , alors  $(c, d)$  est équivalent à  $(a, b)$ . En effet, la première assertion signifie  $a + d = b + c$ , la seconde  $c + b = d + a$ .
- Elle est transitive : si  $(a, b)$  est équivalent à  $(c, d)$  et  $(c, d)$  est équivalent à  $(e, f)$ , alors  $(a, b)$  est équivalent à  $(e, f)$ . En effet, si les deux premières assertions sont vérifiées, on a  $a + d = b + c$  et  $c + f = d + e$ ; alors,  $a + c + f = a + d + e = b + c + e$ , d'où  $a + f = b + e$  en simplifiant par  $c$ , donc  $(a, b)$  est équivalent à  $(b, f)$ .

Notons  $\mathbf{Z}$  l'ensemble des classes d'équivalence et notons  $a - b$  la classe du couple  $(a, b)$ . Ainsi, écrire  $a - b = c - d$  signifie exactement que les couples  $(a, b)$  et  $(c, d)$  sont équivalents, c'est-à-dire que  $a + d = b + c$ . Les éléments de  $\mathbf{Z}$  sont appelés entiers relatifs.

Remarquons que l'application de  $\mathbf{N}$  dans  $\mathbf{Z}$  définie par  $a \mapsto a - 0$  est injective : si  $a - 0 = b - 0$ ,  $a + 0 = 0 + b$ , donc  $a = b$ . On prolonge alors l'addition des naturels  $\mathbf{N}$  aux entiers relatifs par la formule :  $(a - b) + (c - d) = (a + c) - (b + d)$ . Il faut vérifier qu'elle est bien définie, c'est-à-dire que si  $a', b', c', d'$  sont des entiers tels que  $a' - b' = a - b$  et  $c' - d' = c - d$ , alors  $(a' + c') - (b' + d') = (a + c) - (b + d)$ . Par hypothèse, on a en effet  $a + b' = a' + b$  et  $c + d' = c' + d$ , d'où

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

montrant que le couple  $(a + c, b + d)$  est équivalent au couple  $(a' + c', b' + d')$ , ce qu'on voulait démontrer.

L'addition dans  $\mathbf{Z}$  vérifie les propriétés suivantes :

- il y a un élément neutre  $0 - 0$ , de sorte que  $(a - b) + (0 - 0) = a - b$  pour tout couple  $(a, b)$ ;
- l'addition est commutative :  $(a - b) + (c - d) = (a + c) - (b + d) = (c - d) + (a - b)$ ;
- tout élément  $a - b$  a un opposé,  $b - a$ , tel que  $(a - b) + (b - a) = (a + b) - (a + b) = (0, 0)$ .

Ces trois propriétés sont caractéristiques de ce qu'on appelle un *groupe commutatif*.

De plus, tout élément de  $\mathbf{Z}$  est de la forme  $a - 0$  ou  $0 - a$  : si  $c \geq d$ , il existe  $n$  tel que  $c = d + n$  et  $c - d = n - 0$ ; sinon, il existe  $n$  tel que  $d = c + n$  et  $c - d = 0 - n$ . Pour alléger les notations, on note  $a$  l'élément  $a - 0$  de  $\mathbf{Z}$  et  $-a$  l'élément  $0 - a$ , qui est d'ailleurs l'opposé de  $a$ . À l'identification de notation près, tout entier relatif est ainsi ou bien un entier naturel, ou bien l'opposé d'un entier.

Sur  $\mathbf{Z}$ , on hérite aussi d'une multiplication, définie par  $a \times (c - d) = ac - ad$  et  $-a \times (c - d) = ad - ac$  si  $a, c$  et  $d$  sont des entiers naturels. (En général, cela donnerait  $(a - b)(c - d) = (ac + bd) - (ad + bc)$ , mais cette formule n'a aucun intérêt.) La multiplication est commutative, associative et est distributive par rapport à l'addition : si  $a, b, c \in \mathbf{Z}$ ,  $a(b + c) = ab + ac$ ; l'élément neutre est encore 1.

L'ensemble  $\mathbf{Z}$ , muni de cette addition et de cette multiplication, est ce qu'on appelle un *anneau commutatif unitaire*.

## §2. Le théorème de la division euclidienne

THÉORÈME (Division euclidienne). — Soit  $a$  et  $b$  deux entiers relatifs, avec  $b \neq 0$ . Il existe des entiers relatifs  $q$  et  $r$ , uniques, tels que  $a = bq + r$  et  $0 \leq r \leq |b| - 1$ .

L'entier  $q$  s'appelle le quotient de la division euclidienne de  $a$  par  $b$ ; l'entier  $r$ , le reste.

Soit  $R$  l'ensemble des entiers  $r \in \mathbf{N}$  tels qu'il existe  $q \in \mathbf{Z}$  avec  $a = bq + r$ . L'ensemble  $R$  n'est pas vide. En effet, si  $a \geq 0$ , la relation  $a = b \cdot 0 + a$  montre que  $a \in R$ . Si  $a \leq 0$ , soit  $\varepsilon \in \{-1, 1\}$  le signe de  $b$ ; on a la relation  $a = \varepsilon b \cdot a + (1 - \varepsilon b)a$  dans laquelle  $(1 - \varepsilon b)a \geq 0$  (car  $\varepsilon b \geq 1$  et  $a \leq 0$ ); par suite,  $a(1 - \varepsilon b)$  appartient à  $R$ .

Soit  $r$  le plus petit élément de  $R$  et soit  $q \in \mathbf{Z}$  tel que  $a = bq + r$ . Par hypothèse,  $r \geq 0$ . Supposons pour commencer  $b \geq 0$ . Supposons par l'absurde que  $r \geq |b|$ . Notons encore  $\varepsilon$  le signe de  $b$ . On a donc  $|b| = \varepsilon b$  d'où  $r \geq \varepsilon b$ . La relation  $a = bq + r = b(q + \varepsilon) + (r - \varepsilon b)$  implique ainsi que  $r - |b| \in R$ , ce qui contredit la minimalité de  $r$ .

*Exercices.* — 1) On range 461 pots de yaourts dans des caisses (toutes identiques), en remplissant entièrement une caisse avant de passer à la suivante. On utilise 14 caisses; combien chaque caisse contient-elle de pots? (D'après D. Perrin; plusieurs solutions sont possibles.)

2) Connaissant le reste de la division euclidienne d'un entier par 10, pouvez-vous en déduire celui de la division euclidienne de cet entier par 5? par 6?

3) Soit  $n$  un entier. Calculer le reste de la division euclidienne de  $n^2$  par 4, suivant que cet entier est pair ou impair. Existe-t-il des entiers  $a$  et  $b$  tels que  $a^2 + b^2 = 8123$ ?

4) Soit  $a$  et  $b$  des entiers relatifs,  $b \neq 0$ . Démontrer qu'il existe des entiers relatifs  $q$  et  $r$  uniques tels que  $a = bq + r$  et  $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$ .

5) Connaissant la division euclidienne de deux entiers  $n$  et  $n'$  par un entier  $b \geq 1$  (c'est-à-dire quotients et restes), donner un moyen simple de déterminer la division euclidienne de  $n + n'$  par  $b$ ?

6) Soit  $a$  et  $b$  des entiers naturels tels que  $a \geq 3$  et  $b \geq 2$ ; soit  $n$  un entier naturel. Supposant connu le quotient de la division euclidienne de  $a - 1$  par  $b$ , calculer le quotient de la division euclidienne de  $ab^n - 1$  par  $b^{n+1}$ .

## §3. Numération

Depuis bien longtemps, nous écrivons les entiers en base 10 : il y a 10 symboles (0, 1, 2, ..., 9) et chaque nombre s'écrit avec un chiffre des unités, un chiffre des dizaines, des centaines, etc. Nous allons étudier cette façon d'écrire les entiers et la généraliser à d'autres bases. La base 2 est utilisée au cœur des ordinateurs : il y a alors 2 symboles 0 et 1, correspondant à deux états électriques possibles : tension nulle / non nulle aux bornes d'un composant.

Soit  $b$  un entier supérieur ou égal à 2.

PROPOSITION. — Pour tout entier naturel  $n$ , il existe un entier  $k \geq 0$  et des entiers  $c_0, \dots, c_k \in \{0, \dots, b - 1\}$  tels que l'on ait

$$n = c_k b^k + c_{k-1} b^{k-1} + \dots + c_1 b + c_0.$$

On peut en outre imposer les conditions  $k = 0$  si  $n = 0$ , et  $c_k \neq 0$  si  $n \neq 0$ . Elles déterminent les entiers  $k$  et  $c_0, \dots, c_k$  de manière unique.

Par exemple, si  $b = 10$ ,  $1729 = 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 9$ . Si la base est autre que 10, on écrit  $n = \overline{c_k c_{k-1} \dots c_0}$ , voire  $n = \overline{c_k c_{k-1} \dots c_0}^{(b)}$  si l'on veut préciser la base. En pratique, on représente chaque entier entre 0 et  $b - 1$  par un symbole. Si  $b \leq 10$ , le choix  $0, \dots, b - 1$  s'impose. Pour les bases supérieures à 10, il est courant d'employer les lettres majuscules (c'est ce qu'utilisent les informaticiens pour l'hexadécimal — la base 16), ou les lettres grecques. On écrira par exemple  $\overline{A6B}^{(16)}$  pour  $10 \times 16^2 + 6 \times 16 + 11 = 2560 + 96 + 11 = 2667$ .

On démontre l'existence par récurrence sur  $n$ . Pour  $n = 0$ , on peut écrire  $n = 0$ , avec  $k = 0$  et  $c_0 = 0$ . Supposons qu'on puisse écrire de la sorte tout entier strictement inférieur à  $n$ . Soit alors  $q$  et  $r$  le quotient et le reste de la division euclidienne de  $n$  par  $b$ . On a bien  $0 \leq r \leq b - 1$ . Comme  $q \leq n/b < n$ , l'entier  $q$  s'écrit sous la forme  $d_m b^m + d_{m-1} b^{m-1} + \dots + d_0$ , où les  $d_i$  sont des entiers compris entre 0 et  $b - 1$ , avec  $m = 0$  si  $q = 0$ , et  $c_m \neq 0$  si  $q \neq 0$ . Posons alors  $c_0 = r$ ,  $k = m + 1$ , et  $c_i = d_{i-1}$  si  $1 \leq i \leq m + 1$ . On a

$$n = bq + r = b(d_m b^m + d_{m-1} b^{m-1} + \dots + d_0) + c_0 = c_{m+1} b^{m+1} + \dots + c_1 b + c_0,$$

ce qui montre l'existence d'une écriture de l'entier  $n$  en base  $b$ .

Démontrons maintenant l'unicité, toujours par récurrence sur  $n$ . Elle est vraie si  $n = 0$ , et même si  $n < b$ . Supposons qu'il y ait unicité pour tout entier strictement inférieur à  $n$  et supposons qu'un entier  $n$  supérieur ou égal à  $b$  s'écrive à la fois  $c_k b^k + \dots + c_0$  et  $d_m b^m + \dots + d_0$ . Comme on a supposé  $n \geq b$ , on a  $k \geq 1$  et  $m \geq 1$ . Alors, l'écriture

$$n = b(c_k b^{k-1} + \dots + c_1) + c_0 = b(d_m b^{m-1} + \dots + d_1) + d_0$$

montre que le reste de la division euclidienne de  $n$  par  $b$  est égal à  $c_0$  et à  $d_0$ . On a donc  $c_0 = d_0$ , et alors

$$\frac{n - c_0}{b} = c_k b^{k-1} + \dots + c_1 = d_m b^{m-1} + \dots + d_1.$$

Ce sont deux écritures en base  $b$  de l'entier  $(n - c_0)/b$ ; elles coïncident, ce qui entraîne  $k - 1 = m - 1$ , d'où  $k = m$ , et  $c_i = d_i$  pour  $1 \leq i \leq k$ .

Dans la démonstration, les chiffres du développement en base  $b$  sont déterminés de la droite vers la gauche, par des divisions euclidiennes par  $b$ . C'est ainsi qu'on procède en pratique. Écrivons par exemple 1729 en base 7. La division euclidienne de 1729 par 7 s'écrit  $1729 = 7 \times 247 + 0$ , puis on a  $247 = 7 \times 35 + 2$ , puis  $35 = 7 \times 5$ . Ainsi,

$$1729 = 7 \times 247 + 0 = 7 \times (7 \times 35 + 2) + 0 = 7^3 \times 5 + 7 \times 2 + 0,$$

donc s'écrit  $\overline{5020}^{(7)}$  en base 7.

Pour convertir, par exemple, l'entier  $\overline{6353}^{(8)}$ , de la base 8 à la base 10, on peut procéder de deux manières. La première est la plus lourde et consiste à écrire

$$\overline{6353}^{(8)} = 6 \times 8^3 + 3 \times 8^2 + 5 \times 8 + 3 = 6 \times 512 + 3 \times 64 + 5 \times 8 + 3 = 3072 + 192 + 40 + 3 = 3307$$

puisque  $8^2 = 64$  et  $8^3 = 8 \times 64 = 512$ . Il est plus facile et moins coûteux d'écrire

$$\overline{6353}^{(8)} = 3 + 8(5 + 8(3 + 8 \times 6)) = 3 + 8(5 + 8(51)) = 3 + 8(413) = 3 + 3304 = 3307.$$

Cela revient à écrire

$$c_k b^k + \dots + c_0 = c_0 + b(c_1 + b(c_2 + b(c_3 + \dots + b \times c_k))),$$

méthode parfois appelée de HÖRNER.

*Exercices.* — 1) Combien de chiffres faut-il utiliser pour écrire tous les entiers de 1 à 2004 ? Quel chiffre est utilisé le plus souvent ?

2) La pagination d'un livre qui commence à la page 1 utilise 3189 caractères. Combien de pages le livre a-t-il ?

3) Dans une certaine base, un entier s'écrit  $\overline{1254}$  et son double  $\overline{2541}$ . Quel est cet entier et quelle est la base ?

4) Calculer le produit 123456789 par 9 en moins de 5 secondes.

5) a) Écrire en base 7, puis en base 2, enfin dans la base hexadécimale le nombre mille sept-cent quatre-vingt-neuf.

b) Que vaut le nombre écrit  $\overline{101001001}$  en base 2 ?

c) Que vaut le nombre écrit  $\overline{BAC}$  en hexadécimal ?

6) a) Si un nombre s'écrit avec 27 chiffres en base 10, combien en faudra-t-il en base 2 ? en base 16 ?

b) Quel sont les entiers qui s'écrivent avec exactement  $m$  chiffres en base  $b$  ? Combien y en a-t-il ?

c) Si on ajoute deux nombres ayant au plus  $n$  chiffres en base  $b$ , combien de chiffres (au plus) aura leur somme ? leur produit ?

#### §4. Divisibilité

On dit qu'un entier relatif  $a$  divise un entier  $b$  s'il existe  $d \in \mathbf{Z}$  tel que  $b = ad$ . On dit aussi que  $b$  est multiple de  $a$  et on note  $a|b$ . L'entier 0 ne divise que lui-même, mais tout entier le divise.

Quelques propriétés simples de la divisibilité :

*Si  $a$  divise  $b$ , alors  $a$  divise  $bc$  pour tout entier  $c$ .*

*Si  $a$  divise  $b$  et  $b$  divise  $c$ , alors  $a$  divise  $c$ .* En effet, il existe  $d \in \mathbf{Z}$  tel que  $b = ad$  et  $e \in \mathbf{Z}$  tel que  $c = eb$ . Alors,  $c = e(ad) = a(ed)$  ; puisque  $ed \in \mathbf{Z}$ ,  $a$  divise  $c$ .

*Si  $a$  divise  $b$  et  $a$  divise  $c$ , alors  $a$  divise  $ub + vc$  pour tout couple  $(u, v)$  d'entiers relatifs.* Écrivons en effet  $b = ad$  et  $c = ae$ , où  $d \in \mathbf{Z}$  et  $e \in \mathbf{Z}$ . Alors,  $ub + vc = uad + vae = a(ud + ve)$  ; comme  $ud + ve \in \mathbf{Z}$ ,  $a$  divise  $ub + vc$ .

*Si  $a$  divise  $b$  et  $b \neq 0$ , alors  $|a| \leq |b|$ .* Si  $b = ad$ , on a  $d \neq 0$  car  $b \neq 0$ , d'où  $|d| \geq 1$  et finalement  $|b| = |a||d| \leq |a|$ .

*Si  $a$  divise  $b$  et  $b$  divise  $a$ , on a  $a = b$  ou  $a = -b$ .* Si l'un des deux est nul, ils le sont tous deux et la propriété est vraie. S'ils sont tous deux non nuls, on a simultanément  $|a| \leq |b|$  et  $|b| \leq |a|$  d'où l'égalité  $|a| = |b|$  et finalement  $a = \pm b$ .

*Si  $a$  divise  $b$  et  $n \in \mathbf{Z}$ , alors  $na$  divise  $nb$ .* Inversement, si  $n \neq 0$  et si  $na$  divise  $nb$ , alors  $a$  divise  $b$ . Si l'on a  $b = ad$ , avec  $d \in \mathbf{Z}$ , on a  $nb = nad$ , donc  $na$  divise  $nb$ . Dans

l'autre sens, soit  $b = aq + r$  la division euclidienne de  $b$  par  $a$ , avec  $0 \leq r \leq |a| - 1$ . On a  $nb = naq + nr$ , donc si  $na$  divise  $nb$ , il divise aussi  $nb - naq = nr$ . Cela entraîne  $|na| \leq |nr|$ , donc  $|a| \leq |r|$  car  $n \neq 0$ , ce qui contredit l'inégalité  $0 \leq r \leq |a| - 1$ .

Soit  $m$  un entier. On dit que deux entiers  $a$  et  $b$  sont congrus modulo  $m$ , et on note  $a \equiv b \pmod{m}$  si  $b - a$  est multiple de  $m$ .

C'est une relation d'équivalence :

- elle est réflexive : comme  $m|0$ , on a bien  $a \equiv a \pmod{m}$  ;
- elle est symétrique : si  $a \equiv b \pmod{m}$ ,  $m$  divise  $a - b$ , donc  $m$  divise  $b - a$  aussi et  $b \equiv a \pmod{m}$  ;
- elle est transitive : si  $a \equiv b \pmod{m}$  et  $b \equiv c \pmod{m}$ ,  $c - a = (c - b) + (b - a)$  est la somme de deux multiples de  $m$ , donc est multiple de  $m$ .

Remarquons que  $a \equiv b \pmod{0}$  signifie que  $a = b$ . On a  $a \equiv b \pmod{1}$  pour tout couple d'entiers  $a, b \in \mathbf{Z}$  car 1 divise tout entier. Dans ces deux cas, il n'est pas très intéressant d'introduire la relation de congruence.

Supposons maintenant que  $m \geq 2$ . Soit  $a = mq + \alpha$  la division euclidienne de  $a$  par  $m$  et  $b = mr + \beta$  la division euclidienne de  $b$  par  $m$ . On a  $b - a = m(r - q) + (\beta - \alpha)$ . Si  $b - a$  est multiple de  $m$ ,  $\beta - \alpha$  aussi et l'on a nécessairement  $\beta - \alpha = 0$ , car  $\beta - \alpha$  est un entier de valeur absolue inférieure ou égale à  $m - 1$ . Les divisions euclidiennes de  $a$  et  $b$  par  $m$  ont même reste. Dans l'autre sens, si  $\alpha = \beta$ ,  $b - a$  est multiple de  $m$ . Autrement dit :

PROPOSITION. — *Deux nombres entiers sont congrus modulo  $m$  si et seulement si leurs divisions euclidiennes par  $m$  ont même reste.*

Si  $a$  et  $b$  sont congrus modulo  $m$ , alors  $na \equiv nb \pmod{m}$  pour tout entier  $n \in \mathbf{Z}$ . En effet,  $nb - na = n(b - a)$  est multiple de  $b - a$ , donc de  $m$ .

Soit  $a, b, a', b'$  des entiers tels que  $a \equiv b \pmod{m}$  et  $a' \equiv b' \pmod{m}$ . Alors,  $a + a' \equiv b + b' \pmod{m}$ . En effet,  $(b + b') - (a + a') = (b - a) + (b' - a')$  est la somme de deux entiers multiples de  $m$ , donc est multiple de  $m$ . De même,

$$bb' - aa' = b(b' - a') + ba' - aa' = b(b' - a') + a'(b - a)$$

est la somme de deux multiples de  $m$ . On a donc  $aa' \equiv bb' \pmod{m}$ .

Ces propriétés permettent un véritable « calcul des congruences », susceptible de faciliter grandement certains calculs. Nous en verrons plus tard une version *hi-tech*, mais ce qui a déjà été dit fournit un outil rudimentaire mais efficace qui permet, par exemple, de comprendre la *preuve par 9*.

Soit  $n$  un entier. Calculons la somme de ses chiffres, la somme des chiffres du nombre obtenu, etc. Tous les entiers ainsi écrits sont congrus à  $n$  modulo 9. En effet, écrivons  $n = c_k c_{k-1} \dots c_0$  en base 10. Cela signifie que

$$n = c_k 10^k + c_{k-1} 10^{k-1} + \dots + c_1 \times 10 + c_0.$$

La somme des chiffres de  $n$  est l'entier  $c_k + c_{k-1} + \dots + c_0$ . Or, on a  $10 \equiv 1 \pmod{9}$ , car  $10 - 1 = 9$ . Par suite,  $10^2 \equiv 1 \pmod{9}$ , etc.,  $10^k \equiv 1 \pmod{9}$  pour tout entier  $k$ . On a

ainsi

$$n \equiv c_k + \cdots + c_0 \pmod{9} :$$

tout entier est congru modulo 9 à la somme de ses chiffres en écriture décimale. Si on continue le procédé, on obtient une suite d'entiers, tous congrus à  $n$  modulo 9. Si  $k \geq 1$ , c'est-à-dire, si  $n$  s'écrit avec au moins deux chiffres, la somme des chiffres de  $n$  est strictement inférieure à  $n$ . La suite des entiers obtenus est donc strictement décroissante, jusqu'au moment où l'on atteint un entier entre 0 et 9, congru à  $n$  modulo 9.

Si cet entier est égal à 9, c'est que  $n$  est multiple de 9. On pose  $s(n) = 0$ . Sinon, il est entre 0 et 8 ; c'est donc le reste de la division euclidienne de  $n$  par 9. On le note  $s(n)$ .

Soit  $A$  et  $B$  deux entiers dont on a calculé le produit  $C$  à la main. La « preuve par 9 » consiste à calculer  $s(A)$ ,  $s(B)$ ,  $s(C)$ , puis le produit  $D = s(A)s(B)$  et enfin l'entier  $s(D)$ . On a  $A \equiv s(A) \pmod{9}$ ,  $B \equiv s(B) \pmod{9}$ , donc  $AB \equiv D \pmod{9}$ , et enfin  $AB \equiv s(D) \pmod{9}$ . Si le calcul fait est juste,  $C = AB$ , donc on doit pouvoir vérifier que  $s(C) \equiv s(D) \pmod{9}$ , c'est-à-dire  $s(C) = s(D)$ . Si ce n'est pas le cas, c'est qu'on s'est trompé ! Remarquons cependant que la preuve par 9 ne garantit pas que le calcul fait est juste : elle détecte certaines erreurs (typiquement, l'oubli d'une retenue), mais pas toutes (par exemple, pas l'échange de deux chiffres en effectuant le calcul).

*Exercices.* — 1) Quel est le plus petit entier dont l'écriture décimale se termine par un 6 et tel que si l'on efface ce chiffre et qu'on l'écrit en tête des chiffres restants, on obtient quatre fois l'entier initial ?

2\*) Soit  $A$  l'entier 4444<sup>4444</sup> ; soit  $B$  la somme de ses chiffres,  $C$  la somme des chiffres de  $B$  et  $D$  la somme des chiffres de  $C$ . Que vaut  $D$  ?

3) Soit  $n$  un entier dont l'écriture décimale est  $\overline{abc}$ . Montrer que  $n \equiv 2a + 3b + c \pmod{7}$ .

4) Quels sont les trois derniers chiffres de  $7^{100} - 3^{100}$  ? (*Écrire  $7 = 10 - 3$  et utiliser la formule du binôme.*)

5) Imaginer une preuve par 9 pour les divisions euclidiennes. L'expérimenter sur un exemple.

6) Remarquer que  $10 \equiv -1 \pmod{11}$ . En déduire un procédé simple du calcul du reste de la division euclidienne par 11 d'un entier écrit sous forme décimale.

7) Soit  $N = \overline{mcd\bar{u}}$  un nombre de quatre chiffres écrit en base 10. On pose  $P = \overline{udc\bar{m}}$ . Montrer que  $N + P$  est divisible par 11 et donner le quotient de la division de  $N + P$  par 11.

8) Que pourrait être la « preuve par  $b - 1$  » en base  $b$  ?

9) Un problème de Bachet de Méziriac (1612) : « Étant donnée telle quantité qu'on voudra pesant un nombre de livres depuis 1 jusques à 40 inclusivement (sans toutefois admettre les fractions), on demande combien de poids pour le moins il faudrait employer à cet effet. ».

*Une variante en français contemporain* (et en système métrique) : On dispose d'une balance à deux plateaux (« de Roberval ») et d'une boîte de masses marquées de 1 g à 100 g. Montrer comment choisir cinq de ces masses marquées de telle sorte que l'on puisse déterminer la masse de tout objet dont la masse (supposée entière) est de 1 à 100 g.

10) Trois bouteilles contiennent chacune un nombre entier de litres d'eau. La seule opération permise consiste à doubler le contenu d'une des bouteilles en y versant une partie du contenu d'une autre. Montrer qu'il est possible de vider entièrement l'une des bouteilles. On suppose que chaque bouteille est assez grande pour contenir la totalité de l'eau. (Un problème classique repris par E. Busser et G. Cohen.)

### §5. Plus grand diviseur commun, algorithme d'Euclide

Soit  $a$  et  $b$  deux entiers relatifs, non tous deux nuls. Ils ont des diviseurs communs (1 par exemple), mais n'en ont qu'un nombre fini, car un diviseur de  $a$  et  $b$  est inférieur ou égal à  $\max(|a|, |b|)$  — en fait, à  $\min(|a|, |b|)$  si  $a$  et  $b$  sont tous deux distincts de 0. Ils ont par conséquent un *plus grand diviseur commun*. C'est un entier positif, noté  $\text{pgcd}(a, b)$ . On dit que  $a$  et  $b$  sont premiers entre eux si  $\text{pgcd}(a, b) = 1$ . On pose aussi  $\text{pgcd}(0, 0) = 0$ . Remarquons que  $\text{pgcd}(a, 0) = |a|$ .

On définit de manière analogue le  $\text{pgcd}$  d'une famille  $a_1, \dots, a_n$  d'entiers : s'ils sont tous nuls, c'est 0 ; sinon, c'est le plus grand diviseur commun à tous les  $a_i$ .

Il existe un algorithme pour calculer le  $\text{pgcd}$ , à la fois performant pour le calcul pratique (notamment au sein des ordinateurs) et fondamental pour la théorie.

ALGORITHME D'EUCLIDE. — Soit  $a$  et  $b$  deux entiers strictement positifs. On pose  $u_0 = a$ ,  $u_1 = b$  et, tant que  $u_{n+1} \neq 0$ , on définit par récurrence  $u_{n+2}$  comme le reste de la division euclidienne de  $u_n$  par  $u_{n+1}$ .

À un certain moment, on a  $u_{n+1} = 0$  et  $u_n = \text{pgcd}(a, b)$ .

Donnons un exemple et calculons le  $\text{pgcd}$  de 414 et 598. La suite est 414, 598, 414, 184, 46, 0. Le  $\text{pgcd}$  est donc égal à 46. On peut vérifier que  $414 = 46 \times 9$  et  $598 = 46 \times 13$ . Comme aucun entier ne divise à la fois 9 et 13, 46 est bien le plus grand diviseur commun de 414 et 598.

Pour démontrer cet algorithme, on remarque que l'on a  $\text{pgcd}(a, b) = \text{pgcd}(b, r)$  si  $a = bq + r$  est la division euclidienne de  $a$  par  $b$ . En effet si  $d$  divise  $a$  et  $b$ , il divise  $b$  et  $r = a - bq$ , et s'il divise  $b$  et  $r$ , il divise aussi  $a = bq + r$  et  $b$ . Par suite,  $(a, b)$  et  $(b, r)$  ont les mêmes diviseurs, donc le même  $\text{pgcd}$ . Cette formule entraîne que  $\text{pgcd}(u_{n+1}, u_{n+2}) = \text{pgcd}(u_n, u_{n+1})$  pour tout entier  $n$  (au moins tant que l'algorithme ne s'arrête pas), d'où par récurrence  $\text{pgcd}(u_n, u_{n+1}) = \text{pgcd}(u_0, u_1) = \text{pgcd}(a, b)$ .

Rappelons que  $u_{n+2}$  est le reste d'une division euclidienne par  $u_{n+1}$ . On a donc  $u_{n+2} < u_{n+1}$ . Comme il n'y a pas de suite infinie strictement décroissante d'entiers positifs ou nuls, l'algorithme s'arrête un jour ou l'autre. On a alors  $u_{n+1} = 0$  et  $\text{pgcd}(u_n, u_{n+1}) = u_n$ . On a donc bien  $u_n = \text{pgcd}(a, b)$ .

Une variante de l'algorithme d'Euclide fournit un complément important. Reprenons tout d'abord l'exemple précédent :

$$598 = 1 \times 598 + 0 \times 414$$

$$414 = 0 \times 598 + 1 \times 414$$

$$184 = 598 - 414 = 1 \times 598 - 1 \times 414 \qquad q = 1$$

$$46 = 414 - 2 \times 184 = -2 \times 598 + 3 \times 414 \qquad q = 2.$$

Chacune des lignes est obtenue à partir des deux précédentes en appliquant l'algorithme d'Euclide sur le membre de gauche et en complétant le calcul dans le membre de droite. À la fin, on reconnaît que 46 est le  $\text{pgcd}$  de 414 et 598, et l'on a obtenu une écriture de 46 comme somme d'un multiple de 598 et d'un multiple de 414.

Dans le cas général, l'algorithme est le suivant.

ALGORITHME D'EUCLIDE (ÉTENDU). — Soit  $a$  et  $b$  deux entiers strictement positifs. On définit des suites  $(d_n)$ ,  $(u_n)$  et  $(v_n)$  par récurrence en posant

$$\begin{array}{lll} d_0 = a & u_0 = 1 & v_0 = 0 \\ d_1 = b & u_1 = 0 & v_1 = 1 \end{array}$$

puis, si  $d_n \neq 0$ , soit  $q$  le quotient de la division euclidienne de  $d_{n-1}$  par  $d_n$ , et

$$d_{n+1} = d_{n-1} - qd_n \quad u_{n+1} = u_{n-1} - qu_n \quad v_{n+1} = v_{n-1} - qv_n.$$

Si  $d_{n+1} = 0$ , on a  $d_n = \text{pgcd}(a, b) = au_n + bv_n$ .

Démontrons cet algorithme. Remarquons pour commencer que la suite  $(d_n)$  reproduit l'algorithme d'Euclide précédent. Lorsque  $d_{n+1} = 0$ , l'entier  $d_n$  est donc le pgcd de  $a$  et  $b$ .

On va montrer par récurrence sur  $n$  que l'on a  $d_n = au_n + bv_n$ . C'est vrai pour  $n = 0$  car  $a = d_0 = a \times 1 + b \times 0 = au_0 + bv_0$ ; c'est aussi vrai pour  $n = 1$  puisque  $d_1 = b = a \times 0 + b \times 1$ . Supposons que ce soit vrai pour tout entier compris entre 0 et  $n$  et montrons que c'est vrai pour  $n + 1$ . On a en effet, si  $q$  est le quotient de la division euclidienne de  $d_{n-1}$  par  $d_n$ ,

$$\begin{aligned} d_{n+1} &= d_{n-1} - qd_n \\ &= (au_{n-1} + bv_{n-1}) - d(au_n + bv_n) \\ &= a(u_{n-1} - qu_n) + b(v_{n-1} - qv_n) \\ &= au_{n+1} + bv_{n+1}. \end{aligned}$$

Cette relation est donc vraie pour tout entier  $n$ , au moins tant que l'algorithme fonctionne.

Si  $d_{n+1} = 0$ , on a  $d_n = d = au_n + bv_n$ , comme il fallait démontrer.

Comme conséquence immédiate de cet algorithme explicite, on a le théorème suivant.

THÉORÈME DE BÉZOUT. — Soit  $a$  et  $b$  deux entiers relatifs, non tous deux nuls. Il existe des entiers relatifs  $u$  et  $v$  tels que  $\text{pgcd}(a, b) = au + bv$ .

Une première application montre que le pgcd de deux entiers est *le plus divisible* de leurs diviseurs communs.

COROLLAIRE. — Soit  $a$  et  $b$  deux entiers relatifs. Si  $n$  est un diviseur commun de  $a$  et  $b$ , alors  $n$  divise  $\text{pgcd}(a, b)$ .

Ou encore : *pour qu'un entier divise deux entiers, il faut et il suffit qu'il divise leur pgcd*. Par récurrence, cette dernière formulation s'étend au cas du pgcd d'une famille d'entiers : on a la formule  $\text{pgcd}(a_1, a_2, \dots, a_n) = \text{pgcd}(a_1, \text{pgcd}(a_2, \dots, a_n))$ . En effet, dans le cas où  $a_2, \dots, a_n$  ne sont pas tous nuls, cette formule reflète exactement le fait qu'un entier divise tous les  $a_i$ , pour  $1 \leq i \leq n$ , si et seulement s'il divise  $a_1$  et tous les  $a_i$ ,  $2 \leq i \leq n$ . Si  $a_2 = \dots = a_n = 0$ , les deux membres sont égaux à  $a_1$ .

Par récurrence, on peut alors déterminer des entiers  $u_1, \dots, u_n$  tels que  $\text{pgcd}(a_1, \dots, a_n) = a_1 u_1 + \dots + a_n u_n$ . Faisons-le sur un exemple, disons  $\text{pgcd}(6, 10, 15)$ . L'algorithme d'Euclide étendu appliqué au couple (10, 6) s'écrit comme suit :

$$\begin{array}{rcll} 10 & 1 & 0 & \\ 6 & 0 & 1 & q = 1 \\ 4 & 1 & -1 & q = 1 \\ 2 & -1 & 2 & q = 2 \\ 0 & & & \end{array}$$

si bien que l'on a  $\text{pgcd}(10, 6) = 2 = -10 + 2 \times 6$ . L'algorithme d'Euclide étendu appliqué au couple (15, 2) est alors

$$\begin{array}{rcll} 15 & 1 & 0 & \\ 2 & 0 & 1 & q = 7 \\ 1 & 1 & -7 & q = 2 \\ 0 & & & \end{array}$$

et  $\text{pgcd}(15, 2) = 1 = 15 - 7 \times 2$ . Reportant cette dernière relation dans la première, on trouve que 6, 10 et 15 sont premiers entre eux et que

$$1 = \text{pgcd}(6, 10, 15) = 15 - 7 \times (-10 + 2 \times 6) = 15 + 7 \times 10 - 14 \times 6.$$

Voici une autre application importante :

THÉORÈME DE GAUSS. — Soit  $a, b, c$  des entiers non nuls. On suppose que  $a$  et  $b$  sont premiers entre eux. Alors :

- a) si  $a$  divise  $bc$ , alors  $a$  divise  $c$  ;
- b) si  $a$  et  $b$  divisent  $c$ ,  $ab$  divise  $c$ .

Soit  $u$  et  $v$  des entiers tels que  $au + bv = 1$ . On a alors  $c = uac + vbc$ .

a) Supposons que  $a$  divise  $bc$ . L'entier  $a$  divise  $auc$  et  $bvc$ , donc leur somme qui est égale à  $c$ .

b) Soit  $x$  et  $y$  des entiers tels que  $c = ax$  et  $c = by$ . On a  $c = uac + vbc = uaby + vbax = ab(uy + vx)$ , ce qui démontre que  $c$  est multiple de  $ab$ .

Le *plus petit multiple commun* (ppcm) d'une famille d'entiers non nuls est le plus petit entier  $> 0$  qui soit multiple de chacun d'entre eux.

Soit  $a$  et  $b$  des entiers strictement positifs ; supposons que  $a$  et  $b$  soient premiers entre eux. Soit  $m$  un entier non nul qui est multiple de  $a$  et de  $b$ . D'après le corollaire du théorème de Gauss ci-dessus,  $m$  est multiple de  $ab$ , donc supérieur à  $ab$ . Inversement,  $ab$  est multiple de  $a$  et de  $b$ , d'où  $\text{ppcm}(a, b) = ab$  lorsque  $a$  et  $b$  sont premiers entre eux.

Calculons maintenant  $\text{ppcm}(a, b)$  dans le cas général. Si  $d = \text{pgcd}(a, b)$ , on peut écrire  $a = da'$  et  $b = db'$  ; alors,  $a'$  et  $b'$  sont premiers entre eux : si  $u > 1$  divise  $a'$  et  $b'$ , on écrit  $a' = ua''$ ,  $b' = ub''$  et l'on a  $a = (du)a''$ ,  $b = (du)b''$ , ce qui montre que  $du$  divise  $a$  et  $b$ , alors que  $du > d$ .

Si  $m$  est multiple de  $a$  et de  $b$ , il est multiple de  $d$  ; écrivons donc  $m = dm'$ . Par hypothèse  $dm'$  est multiple de  $da'$  ; on en déduit que  $m'$  est multiple de  $a'$ . De même,

$m'$  est multiple de  $b'$ . Par suite,  $m'$  est multiple de  $a'b'$ , car  $a'$  et  $b'$  sont premiers entre eux, donc  $m$  est multiple de  $da'b'$  et en particulier,  $m \geq da'b'$ . Inversement, l'entier  $da'b'$  vérifie  $da'b' = ab' = a'b$ , donc est multiple à la fois de  $a$  et de  $b$ . Nous avons donc démontré que  $\text{ppcm}(a, b) = da'b'$ . Remarquons que l'on a la formule  $\text{ppcm}(a, b) \text{pgcd}(a, b) = d^2 a' b' = ab$ .

Notons aussi que la démonstration précédente prouve en fait qu'un multiple commun de  $a$  et  $b$  est non seulement plus grand que  $\text{ppcm}(a, b)$ , mais aussi un multiple de  $\text{ppcm}(a, b)$ . Plus généralement, un entier est multiple commun des entiers non nuls  $a_1, \dots, a_n$  si et seulement si c'est un multiple de leur  $\text{ppcm}$   $\text{ppcm}(a_1, \dots, a_n)$ . Cela permet de déterminer le  $\text{ppcm}$  par récurrence ; par exemple,

$$\text{ppcm}(6, 10, 15) = \text{ppcm}(\text{ppcm}(6, 10), 15) = \text{ppcm}(30, 15) = 30,$$

où la relation  $\text{ppcm}(6, 10) = 30$  provient de la formule pour le  $\text{ppcm}$  de deux entiers et de ce que le  $\text{pgcd}$  de 6 et 10 est égal à 2.

*Exercices.* — 1) Si  $(a, b) = (462, 104)$ , calculer  $d = \text{pgcd}(a, b)$ ,  $\text{ppcm}(a, b)$  et déterminer un couple d'entiers  $(u, v)$  tels que  $au + bv = d$ . Mêmes questions avec  $(a, b) = (126, 69)$ .

2) a) Trouver des entiers relatifs  $u$  et  $v$  tels que  $29u + 24v = 1$ .

b) Déterminer l'ensemble des couples  $(u, v) \in \mathbb{Z}^2$  tels que  $29u + 24v = 3$ .

3) Calculer les plus grand diviseurs communs suivants :  $\text{pgcd}(46848, 2379)$ ,  $\text{pgcd}(13860, 4488)$ ,  $\text{pgcd}(30076, 12669, 21733)$ .

4) Quel est le plus petit entier (strictement positif) qui est multiple de 1, 2, 3, ..., 10 ?

5) Calculer  $\text{pgcd}(357, 629)$  puis  $d = \text{pgcd}(357, 629, 221)$ . Trouver des entiers  $x, y, z$  tels que  $357x + 629y + 221z = d$ .

6) a) Soit  $m$  et  $n$  des entiers relatifs tels que  $m$  divise à la fois  $8n + 7$  et  $6n + 5$ . Montrer que  $m = \pm 1$ .

b) Soit  $a$  un entier relatif. Déterminer le  $\text{pgcd}$   $d$  des entiers  $m = 14a + 3$  et  $n = 21a + 4$  et trouver des entiers  $u$  et  $v$  tels que  $um + vn = d$ .

7) Soit  $a$  et  $b$  des entiers premiers entre eux.

a) Montrer que le  $\text{pgcd}$  de  $a + b$  et  $a - b$  est égal à 1 ou 2. Préciser suivant les parités de  $a$  et  $b$  dans quel cas on se trouve.

b) Montrer que le  $\text{pgcd}$  de  $a + 2b$  et  $2a + b$  est égal à 1 ou 3.

8) Dans l'État Désuni, la monnaie est le Ralldo ( $\mathbb{R}$ ) et les pièces valent 7  $\mathbb{R}$  ou 11  $\mathbb{R}$ . Montrer que l'on peut y payer toute somme à partir de 60  $\mathbb{R}$ , mais qu'on ne peut pas y payer une somme de 59  $\mathbb{R}$ . Qu'en est-il si le commerçant peut rendre la monnaie ?

9) a) Soit  $a, b, c$  des entiers. On suppose que  $a$  divise  $bc$  et que  $\text{pgcd}(a, b) = 1$ . Montrer que  $a$  divise  $c$ . (*Multiplier par  $c$  une relation de Bézout  $1 = au + bv$ .*)

b) Soit  $a, b, c, d$  des entiers naturels non nuls. On suppose que  $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$  et que  $\frac{a}{b} + \frac{c}{d}$  est entier. Montrer que  $b = d$ .

10) Soit  $n$  un entier naturel.

a) Montrer que le plus petit multiple commun de  $9n + 8$  et  $6n + 5$  est égal à  $54n^2 + 93n + 40$ .

b) Calculer  $\text{pgcd}$  et  $\text{ppcm}$  des entiers  $12n^2 + 16n + 6$  et  $6n + 5$ .

11) a) Montrer que 15 et 28 sont premiers entre eux.

- b) Trouver une solution particulière dans  $\mathbf{Z} \times \mathbf{Z}$  de l'équation  $28x - 15y = 1$ . En déduire une solution particulière dans  $\mathbf{Z} \times \mathbf{Z}$  de l'équation  $28x - 15y = 11$ .
- c) Trouver l'ensemble des couples  $(x, y)$  d'entiers relatifs vérifiant  $28x - 15y = 11$ .
- d) Soit  $f$  l'application de  $\mathbf{Z} \times \mathbf{Z}$  dans  $\mathbf{Z}$  telle que  $f(x, y) = 28x - 15y$ . Montrer que  $f$  est surjective. L'application  $f$  est-elle injective?
- e) Calculer le pgcd de 15 et 21. L'équation  $15x - 21y = 5$  admet-elle des solutions dans  $\mathbf{Z} \times \mathbf{Z}$ ?
- 12) Soit  $m$  et  $n$  des entiers  $> 1$ .
- a) Montrer qu'un nombre complexe  $z$  vérifie  $z^n = z^m = 1$  si et seulement si  $z^{\text{pgcd}(m,n)} = 1$ .
- b) Si  $m > n$ , montrer que  $\text{pgcd}(a^m - 1, a^n - 1) = \text{pgcd}(a^m - 1, a^{m-n} - 1)$ . En déduire à l'aide de l'algorithme d'Euclide que  $\text{pgcd}(a^n - 1, a^m - 1) = a^{\text{pgcd}(m,n)} - 1$ .
- 13) On définit la suite de Fibonacci par  $F_0 = 0, F_1 = 1$  et  $F_{n+1} = F_n + F_{n-1}$ .
- a) Montrer (par récurrence) que  $F_{n+1}F_{n-1} - (F_n)^2 = (-1)^n$  pour tout  $n$ .
- b) Montrer que  $F_{n+m} = F_{n+1}F_m + F_nF_{m-1}$ . (Faire une récurrence sur  $m$ , puis sur  $n$ .)
- c) Montrer que l'on a, pour  $m < n$ ,  $\text{pgcd}(F_n, F_m) = \text{pgcd}(F_{n-m}, F_m)$  et  $\text{pgcd}(n, m) = \text{pgcd}(n - m, m)$ . En déduire par récurrence sur  $\max(m, n)$  que la relation  $\text{pgcd}(F_n, F_m) = F_{\text{pgcd}(n,m)}$ .
- d\*) Calculer  $F_n$  pour tout entier  $n$ . Quelle est la limite de  $F_{n+1}/F_n$  quand  $n$  tend vers l'infini? Montrer que  $F_n$  est l'entier le plus proche de  $((1 + \sqrt{5})/2)^n / \sqrt{5}$ .
- 14) Soit  $x, y, z$  des entiers  $> 0$ , premiers entre eux dans leur ensemble, tels que  $x^2 + y^2 = z^2$  (triplet pythagoricien).
- a) Soit  $d = \text{pgcd}(x, y)$ . Montrer que  $d$  divise  $z$ . En déduire que  $x, y, z$  sont premiers entre eux deux à deux.
- b) Montrer que de  $x$  et  $y$ , l'un des deux est pair et l'autre est impair. On supposera dans la suite que  $x$  est pair.
- c) Montrer que  $\text{pgcd}(z - y, z + y) = 2$ . En utilisant que  $x^2 = z^2 - y^2 = (z - y)(z + y)$ , montrer qu'il existe des entiers  $u$  et  $v$  tels que  $x = 2uv, z + y = 2u^2$  et  $z - y = 2v^2$ .
- d) Inversement, si  $u$  et  $v$  sont premiers entre eux, le triplet  $(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2)$  est un triplet pythagoricien.



## CHAPITRE 4

### NOMBRES PREMIERS

---

#### §1. Crible d'Ératosthène

Un *nombre premier* est un entier supérieur ou égal à 2 qui n'est divisible que par 1 et lui-même. Un entier qui n'est pas premier est dit composé. (On prendra garde à ne pas confondre cette notion avec la propriété que deux entiers sont premiers entre eux.)

Pour déterminer les entiers jusqu'à une certaine borne qui sont des nombres premiers, Ératosthène a inventé le procédé suivant, qu'on appelle *crible*.

On commence par écrire tous les entiers de 2 à, disons 30 :

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.

Le premier d'entre eux est premier, on le garde et on raye tous ses multiples. On trouve alors

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.

Le suivant non rayé, 3, n'est multiple d'aucun entier plus petit que lui, donc est premier. On le garde et on élimine les multiples de 3.

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.

Ensuite, il y a 5, d'où

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.

Le suivant est 7, et est supérieur à la racine carrée de 30.

LEMME. — Soit  $n$  un entier  $\geq 2$ . Si  $n$  n'est pas premier, il existe un nombre premier  $p \leq \sqrt{n}$  qui divise  $n$ .

Montrons ceci par récurrence sur  $n$ . C'est vrai pour  $n = 2$ ,  $n = 3$  qui sont premiers, et aussi pour  $n = 4$  qui n'est pas premier. Supposons que le résultat soit vrai pour tout entier  $< n$ . Si  $n$  est premier, le résultat est vrai. Sinon,  $n$  a un diviseur  $m$ , avec  $1 < m < n$ . On peut écrire  $n = km$ . Si  $m \leq k$ , on a  $m^2 \leq km = n$ , d'où  $m \leq \sqrt{n}$ . En particulier,  $m < n$ . Par récurrence, ou bien  $m$  est premier, ou bien  $m$  a un diviseur premier inférieur ou égal à sa racine carrée. En particulier,  $m$  a un diviseur premier  $p$  et  $p \leq m \leq \sqrt{n}$ . Dans l'autre cas,  $k \leq m$ , on raisonne de même en échangeant les rôles de  $k$  et  $m$ .

Par suite, tous les entiers qui restent sont des nombres premiers et la liste des nombres premiers inférieurs ou égaux à 30 est

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

## §2. Factorisation

On a déjà dit que tout entier admet un diviseur premier. Nous allons voir qu'il y a, à l'ordre près, une unique façon d'écrire tout nombre entier naturel comme produit de nombres premiers.

Pour démontrer l'unicité, nous aurons besoin d'un lemme, dont la démonstration remonte à Euclide, mais qu'il est plus court de démontrer à l'aide du théorème de Gauss.

LEMME D'EUCLIDE. — *Soit  $p$  un nombre premier et soit  $a, b$  deux entiers dont  $p$  divise le produit  $ab$ . Si  $p$  ne divise pas  $a$ ,  $p$  divise  $b$ .*

Soit  $d$  le pgcd de  $a$  et  $p$ . C'est un diviseur de  $p$ , donc il est égal à 1 ou à  $p$ . Comme  $p$  ne divise pas  $a$ , on a  $d = 1$ ; autrement dit,  $a$  et  $p$  sont premiers entre eux. D'après le théorème de Gauss,  $p$  divise  $b$ .

*Autre démonstration (Euclide) :* Soit  $x$  le plus petit entier  $\geq 1$  tel que  $p$  divise  $xb$ . Il en existe par hypothèse puisque  $p$  divise  $ab$ . La division euclidienne de  $a$  par  $p$  s'écrit  $a = pq + r$  avec  $r \neq 0$  car  $p$  ne divise pas  $a$ . Par suite, on a  $x < p$ . Considérons alors la division euclidienne de  $p$  par  $x$ ; elle s'écrit  $p = xq + r$ , avec  $0 \leq r \leq x - 1$ . Par suite,  $rb = pb - x bq$  est la différence de deux multiples de  $p$ , donc est multiple de  $p$ . Comme  $x$  était choisi minimal, cela entraîne  $r = 0$ , donc  $p = qx$ . Puisque  $p$  est un nombre premier et que  $x < p$ , on a nécessairement  $x = 1$  et  $p$  divise  $b$ .

THÉORÈME. — *Soit  $n$  un entier  $\geq 2$ . Il existe un entier  $r$  et des nombres premiers  $p_1 \leq \dots \leq p_r$  tels que  $n = p_1 \dots p_r$ . De plus, si  $n = q_1 \dots q_s$  avec  $q_1 \leq \dots \leq q_s$ , on a  $r = s$  et  $p_i = q_i$  pour  $1 \leq i \leq r$ .*

On démontre tout d'abord l'existence d'une factorisation par récurrence sur  $n$ . Soit  $p_1$  le plus petit nombre premier qui divise  $n$ ; il en existe d'après le lemme. Posons  $m = n/p_1$ ; on a  $m \leq n/2 < n$ . Si  $m = 1$ ,  $n = p_1$  et on pose  $r = 1$ . Sinon, il existe par récurrence un entier  $r$  et des nombres premiers  $p_2 \leq \dots \leq p_r$  tels que  $m = p_2 \dots p_r$ . On a donc  $n = p_1 m = p_1 p_2 \dots p_r$ . De plus,  $p_1 \leq p_2$  car  $p_2$  est un nombre premier qui divise  $m$  et  $p_1$  est le plus petit d'entre eux.

Soit  $p$  un nombre premier qui divise  $n$ . Montrons par récurrence sur  $r$  que  $p$  est l'un des  $p_i$ . Si  $r = 1$ ,  $n = p_1$  est un nombre premier donc ses seuls diviseurs sont 1 et lui-même, ce qui impose  $p = p_1$ . Supposons l'assertion vérifiée pour moins de  $r$  facteurs et supposons que  $p \neq p_1$ . D'après le lemme d'Euclide ci-dessus,  $p$  divise  $p_2 \dots p_r$ . Par récurrence, il existe donc  $i \in \{2, \dots, r\}$  tel que  $p = p_i$ .

Nous avons donc montré que tout diviseur premier de  $n$  est l'un des  $p_i$ . Le plus petit d'entre eux est donc  $p_1$ , d'où  $p_1 = q_1$  si  $n = q_1 \dots q_s$  avec  $q_1 \leq \dots \leq q_s$ . Alors  $p_2 \dots p_r = n/p_1 = q_2 \dots q_s$ . Par récurrence,  $r - 1 = s - 1$  et  $p_2 = q_2, \dots, p_r = q_r$ .

Lorsqu'on écrit la factorisation d'un nombre entier en produit de nombres premiers, il est coutume de regrouper les facteurs égaux à un même nombre premier, en écrivant  $n = p_1^{n_1} \dots p_s^{n_s}$ , où les  $p_i$  sont des nombres premiers distincts et, par exemple,  $p_1 < \dots < p_s$ . Les entiers négatifs, quant à eux, ont une décomposition en facteurs premiers de la forme

$$n = -p_1^{n_1} \dots p_s^{n_s}.$$

Soit  $n$  un entier relatif. L'exposant du nombre premier  $p$  dans la décomposition en facteurs premiers de  $n$  est appelé *valuation  $p$ -adique de  $n$*  et est noté  $v_p(n)$ . Cet exposant est nul si et seulement si  $p$  ne divise pas  $n$ . On peut alors récrire la formule précédente sous la forme

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

On pose aussi, par convention,  $v_p(0) = +\infty$ .

Soit  $m$  et  $n$  des entiers relatifs et soit  $p$  un nombre premier. On a  $v_p(mn) = v_p(m) + v_p(n)$ . De plus, on a  $v_p(m+n) \geq \min(v_p(m), v_p(n))$ , et l'égalité est obtenue dès que  $v_p(m) \neq v_p(n)$ .

Soit  $m, n$  deux entiers non nuls. Pour que  $m$  divise  $n$ , il faut et il suffit que pour tout nombre premier  $p$ , on ait  $v_p(m) \leq v_p(n)$ . Supposons en effet que  $m$  divise  $n$  et soit  $d$  le quotient de sorte que  $n = dm$ . Si  $p$  est un nombre premier, on a  $v_p(n) = v_p(dm) = v_p(m) + v_p(d)$ , d'où  $v_p(n) \geq v_p(m)$ . Inversement, supposons que ces inégalités soient satisfaites et soit  $d$  l'entier positif défini par

$$d = \prod_{p|n} p^{v_p(n) - v_p(m)}.$$

(Le produit est sur l'ensemble fini des nombres premiers qui divisent  $n$ .) On a  $md = n$  si  $m$  et  $n$  sont de même signe, et  $md = -n$  sinon. Par suite,  $m$  divise  $n$ .

Concernant le pgcd et le ppccm de deux entiers, on en déduit les formules :

$$v_p(\text{pgcd}(m, n)) = \min(v_p(m), v_p(n)) \quad \text{et} \quad v_p(\text{ppccm}(m, n)) = \max(v_p(m), v_p(n)).$$

*Exercices.* — 1) a) Soit  $p$  un nombre premier. Combien y a-t-il d'entiers  $m \in \{1, \dots, n\}$  multiples de  $p$ ? de  $p^k$  pour  $k \geq 1$ ? En déduire que

$$v_p(n!) = \sum_{k \geq 1} \lfloor n/p^k \rfloor.$$

(La somme est finie car les termes pour  $p^k > n$  sont nuls.)

- b) Combien y a-t-il de 0 à la fin du développement décimal de 1000!? Vérifier avec MAPLE.
- 2) a) Si tous les facteurs premiers  $p$  d'un entier  $n$  vérifient  $p \equiv 1 \pmod{4}$ , montrer que l'on a  $n \equiv 1 \pmod{4}$ .
- b) Si  $n \geq 4$ , en déduire qu'au moins un facteur premier de  $n! - 1$  est congru à  $-1$  modulo 4, puis qu'il existe une infinité de nombres premiers de la forme  $4n + 3$ .
- c) Montrer de même qu'il existe une infinité de nombres premiers de la forme  $6n + 5$ .
- 3) a) Montrer qu'aucun des entiers  $n! + 2, \dots, n! + n$  n'est un nombre premier.
- b) En s'inspirant de la question précédente, montrer qu'il existe des suites d'entiers consécutifs arbitrairement longues telles qu'aucun d'entre eux ne soit la puissance d'un nombre premier (*Olympiades internationales de mathématiques, 1989*).

4) On définit une suite  $(u_n)$  par  $u_0 = 0$  et  $u_{n+1} = (u_n)^2 - 3/2$ . Montrer que l'on a  $u_n \neq u_m$  pour  $n \neq m$ . (Montrer par récurrence que pour tout  $n \geq 1$ ,  $2^{2^{n-1}} u_n$  est un nombre entier impair.)

5) a) Montrer que pour tout entier  $n \geq 1$ , il existe un unique entier  $t$  tel que  $2^t \leq n < 2^{t+1}$ . On le note  $t_n$ .

b) Si  $n \geq 1$ , on pose

$$H_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}.$$

Montrer par récurrence sur  $n \geq 2$  qu'il existe des entiers impairs  $a_n$  et  $b_n$  tels que  $H_n = a_n/2^{t_n} b_n$ . En déduire que pour  $n \geq 2$ ,  $H_n$  n'est pas un nombre entier.

6) Résoudre l'équation  $x^2 - y^2 = 225$  (pour  $x, y$  entiers).

### §3. Combien y a-t-il de nombres premiers ?

Cette question, vague et fascinante, n'a toujours pas trouvé de réponse complète.

Une réponse qualitative, due à Euclide lui-même : *l'ensemble des nombres premiers est infini*. Voici la démonstration d'Euclide — il n'y en a pas de meilleure ! (Voir aussi les exercices du paragraphe précédent pour des raffinements.) Raisonnons par l'absurde et supposons qu'il n'y ait qu'un nombre fini de nombres premiers, soit  $p_1, \dots, p_r$ . Considérons l'entier  $n = p_1 \dots p_r + 1$  ; on a  $n > 1$ . Soit  $p$  un diviseur premier de  $n$ . Par hypothèse,  $p$  est l'un des  $p_i$ . Par suite,  $p$  divise  $n - p_1 \dots p_r = 1$ , ce qui est absurde.

On note alors, au moins depuis Riemann (1859),  $\pi(x)$  le nombre des nombres premiers inférieurs ou égaux à  $x$ . Le théorème d'Euclide affirme que  $\lim_{x \rightarrow \infty} \pi(x) = +\infty$ .

Gauss avait conjecturé à la fin du XVIII<sup>e</sup> siècle, et Hadamard et de la Vallée-Poussin ont démontré en 1896 le *théorème des nombres premiers*, à savoir que l'on a

$$\lim_{x \rightarrow \infty} \pi(x) \frac{\log x}{x} = 1.$$

Jusqu'aux années 1960 et la preuve d'Erdős et Selberg, les démonstrations de ce théorème utilisaient toutes des méthodes assez sophistiquées de la théorie des fonctions d'une variable complexe.

Un des aspects fascinants de cette conjecture est la façon dont Gauss l'a prévu : d'une part sur la base d'une table de nombres premiers assez importante, et d'autre part sur le calcul numérique de l'intégrale (appelée *logarithme intégral*)  $\text{li}(x) = \int_e^x \frac{dt}{\log t}$  dont la croissance est en  $x/\log x$  lorsque  $x \rightarrow \infty$ . Il est remarquable que deux siècles avant que les ordinateurs rendent ce genre de calcul numérique, Gauss ait été capable de prédire ce résultat, d'autant plus que le logarithme intégral fournit le meilleur équivalent possible.

Depuis un article génial de B. Riemann (1859), on sait que la répartition des nombres premiers est liée à une fonction d'une variable complexe, appelée *fonction zêta de Riemann*, et précisément aux zéros de cette fonction. Ainsi, *l'hypothèse de Riemann*, toujours non démontrée à ce jour, malgré la prime de 1 000 000 \$ qui lui est attachée par le milliardaire américain Clay, équivaut à ce que pour tout  $\alpha > 1/2$ , on ait

$$\lim_{x \rightarrow \infty} |\pi(x) - \text{li}(x)| x^{-\alpha} = 0.$$

Le résultat est vrai, mais trivial, pour  $\alpha \geq 1$ , et n'est connu pour aucune valeur de  $\alpha < 1$ . On sait aussi que cette limite ne pourrait être vraie pour aucune valeur de  $\alpha \leq 1/2$ .

Si le comportement de la fonction  $\text{li}(x)$  est très bien compris, celui de la fonction  $\pi(x)$  reste très mystérieux. Un exemple supplémentaire : la différence  $\pi(x) - \text{li}(x)$  semble être toujours négative, au moins pour les premières valeurs de  $x$ . On a cependant démontré d'une part que cette différence change de signe une infinité de fois, et d'autre part que le premier changement de signe intervient pour une valeur astronomique de  $x$  (supérieure à  $10^{10}$ , inférieure à  $2 \times 10^{1165}$  et probablement inférieure à  $7 \times 10^{370} \dots$ ) — il serait impossible de vérifier cela à la main !

*Exercices.* — 1) Démontrer l'équivalent  $\text{li}(x) \sim x/\log(x)$ .

#### §4. Le théorème de Tchebychev et le postulat de Bertrand

*Exercices.* — 1) L'exercice qui vient démontre une forme faible du théorème des nombres premiers, due à Tchebychev (1852).

a) Posons  $N = \binom{2n}{n}$ . Démontrer que l'on a

$$2^n \leq \frac{1}{2n} 4^n \leq N \leq 4^n.$$

- b) Soit  $p$  un nombre premier tel que  $n < p \leq 2n$ . Montrer que  $p$  divise  $N$ .  
 c) Montrer que  $(\pi(2n) - \pi(n)) \log n \leq 2n \log 2$ .  
 d) Soit  $p$  un nombre premier. Montrer que  $\nu_p(N) \leq \log(2n)/\log p$ .  
 e) Montrer que  $\pi(2n) \log(2n) \geq n \log 2$ .  
 f) Montrer que pour tout entier  $k$ ,

$$k\pi(2^k) \leq 3 \cdot 2^k.$$

g) Montrer que pour tout entier  $x \geq 1$ , on a l'inégalité

$$\frac{\log 2}{4} \frac{x}{\log x} \leq \pi(x) \leq 6 \log 2 \frac{x}{\log x}.$$

2) En 1845, J. Bertrand avait postulé l'existence, pour tout entier  $n \geq 2$ , d'un nombre premier entre  $n$  et  $2n$ . L'exercice suivant est consacré à une démonstration (due à P. Erdős, 1932) de ce fait.

- a) Soit  $n$  un entier ; on pose  $N = \binom{2n+1}{n}$ . Montrer que  $N \leq 4^n$ .  
 b) Montrer que le produit des nombres premiers  $p$  tels que  $n+1 < p \leq 2n+1$  divise  $N$ .  
 c) Montrer par récurrence sur  $n$  que pour tout entier  $n$ , on a

$$\prod_{p \leq n} p \leq 4^n.$$

- d) Soit  $p$  un facteur premier de  $N$  tel que  $p \leq n$ . Montrer que  $p < 2n/3$ .  
 e) Montrer qu'un nombre premier  $p$  tel que  $p^2 | N$  vérifie  $p \leq \sqrt{2n}$ . En déduire qu'il y a au plus  $\sqrt{2n}$  tels entiers.  
 f) Supposons par l'absurde qu'il n'existe pas de nombre premier  $p$  tel que  $n < p < 2n$ . Montrer que  $N \leq 2^{4n/3} (2n)^{\sqrt{2n}}$ .  
 g) (*suite*) En déduire que  $\log(x)/x \geq 1/6$ , où  $x = \sqrt{2n}$ , puis que  $x \leq 18$ . En déduire que  $n \leq 162$ .

h) Montrer (à la main) que pour tout entier  $n \leq 1000$ , il existe un nombre premier  $p$  vérifiant  $n < p < 2n$ .

### §5. Petit théorème de Fermat

Soit  $p$  un nombre premier. Si  $k$  est un entier tel que  $1 \leq k \leq p-1$ ,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

est un entier. Comme le dénominateur de cette fraction n'est pas multiple de  $p$ , cet entier est divisible par  $p$ .

PROPOSITION. — Pour tout entier  $n \in \mathbf{Z}$ , on a  $n^p \equiv n \pmod{p}$ . Si de plus  $n$  n'est pas multiple de  $p$ , on a  $n^{p-1} \equiv 1 \pmod{p}$ .

Montrons la première assertion par récurrence sur  $n$ . Elle est vraie pour  $n = 0$ . Si elle est vraie pour  $n$ , alors

$$(1+n)^p = 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p \equiv 1+n \pmod{p},$$

donc elle est vraie pour  $n+1$ . Par récurrence, elle est donc vraie pour tout entier  $\geq 0$ . Comme  $(-n)^p \equiv -n^p \pmod{p}$  (c'est même vrai sans congruence si  $p$  est impair), le résultat s'en déduit pour tout entier négatif.

Autrement dit,  $p$  divise  $n^p - n = n(n^{p-1} - 1)$ , pour tout entier  $n \in \mathbf{Z}$ . Supposons de plus que  $n$  ne soit pas multiple de  $p$ . Alors, le lemme d'Euclide entraîne que  $p$  divise  $n^{p-1} - 1$ , c'est-à-dire  $n^{p-1} \equiv 1 \pmod{p}$ .

Soit  $p$  un nombre premier et soit  $n$  un entier qui n'est pas multiple de  $p$ . Il existe des entiers  $k$  tels que  $n^k \equiv 1 \pmod{p}$ , par exemple  $k = p-1$  convient. Appelons *ordre multiplicatif* de  $n$  modulo  $p$ , et notons  $\text{ord}_p(n)$ , le plus petit entier  $d \geq 1$  tel que  $n^d \equiv 1 \pmod{p}$ . Si  $m$  et  $n$  sont congrus modulo  $p$ ,  $n^d \equiv m^d \pmod{p}$  pour tout entier  $d$ , si bien que  $n$  et  $m$  ont même ordre multiplicatif modulo  $p$ .

Posons  $d = \text{ord}_p(n)$ ; soit alors  $k$  un entier tel que  $n^k \equiv 1 \pmod{p}$  et écrivons la division euclidienne de  $k$  par  $d$ , soit  $k = dq + r$ , où  $0 \leq r < d$ . On a les congruences modulo  $p$ :

$$1 \equiv n^k \equiv n^{dq+r} \equiv (n^d)^q n^r \equiv n^r \pmod{p}.$$

Comme  $d$  est le plus petit entier strictement positif tel que  $n^d \equiv 1 \pmod{p}$  et que  $0 \leq r < d$ , on a nécessairement  $r = 0$ . Autrement dit, les entiers  $k$  tels que  $n^k \equiv 1 \pmod{p}$  sont les multiples de  $d$ . Appliquons ce raisonnement à l'entier  $p-1$  (rappelons que  $n^{p-1} \equiv 1 \pmod{p}$  d'après le petit théorème de Fermat). On a ainsi démontré que l'ordre multiplicatif de  $n$  modulo  $p$  est un diviseur de  $p-1$ .

*Exercices.* — 1) a) Soit  $p$  un nombre premier tel que  $p > 5$ . Montrer que  $p^4 - 1$  est multiple de 240.

b) Un magicien demande à un participant de choisir un grand nombre premier, de calculer son carré puis de diviser par 24. Le magicien devine le reste. Explication ?

2) Pour  $p = 2, 3, 5, 7, 11$  et  $13$  calculer l'ordre multiplicatif de tout entier  $n$  compris entre 1 et  $p$ . Que remarquez-vous ?

3) Soit  $p$  un nombre premier et soit  $a$  un entier compris entre 1 et  $p - 1$  ; soit  $d$  l'ordre multiplicatif de  $a$  modulo  $p$ .

a) Montrer que les restes des divisions euclidiennes par  $p$  des entiers  $1, a, a^2, \dots, a^{d-1}$  sont deux à deux distincts.

b) Si  $d = p - 1$ , montrer que pour tout entier  $n$  compris entre 1 et  $p - 1$ , il existe un entier  $k$  tel que  $a^k \equiv n \pmod{p}$ .

On peut reformuler la propriété précédente en disant que  $n^{p-1} \equiv 1 \pmod{p}$  pour tout entier  $n$  tel que  $1 \leq n < p$ . Autrement dit, si un couple  $(n, p)$  d'entiers, avec  $1 \leq n < p$  est tel que  $n^{p-1} \not\equiv 1 \pmod{p}$ , alors on peut affirmer que  $p$  n'est pas un nombre premier. Cela donne un moyen de démontrer qu'un entier n'est pas un nombre premier sans pour autant être capable de le factoriser.

Donnons un exemple idiot pour commencer. Si  $n = 2$  et  $p = 9$ , on a, modulo 9,

$$n^{p-1} = 2^8 = 4^4 = 16^2 \equiv 49 \equiv 4 \pmod{9},$$

donc 9 n'est pas premier. Mais il n'est pas certain que ce soit la meilleure solution pour le démontrer. Un peu plus compliqué, prenons  $n = 2$  et  $p = 221$ . Modulo 221, on a

$$2^{220} = 4^{110} = 8^{55} = 8 \times 16^{27} = 8 \times 16 \times 256^{13} = 108 \times 35^{13} = 108 \times 35 \times (35^2)^6 = (3780) \times (1225)^6$$

puis  $3780 = 221 \times 10 + 1570 = 221 \times 17 + 3 \equiv 3 \pmod{221}$  et  $1225 = 221 \times 5 + 120 \equiv 120 \pmod{5}$ . Alors,

$$2^{220} \equiv 3 \times (120)^6 \equiv 3 \times (14400)^3,$$

or  $14400 = 221 \times 65 + 35$  et  $35^3 \equiv 35 \times 120 \equiv 4200 = 19 \times 221 + 1 \equiv 1$ . Par suite,  $2^{220} \equiv 3 \pmod{221}$ , ce qui montre que 221 n'est pas premier. En fait, on a  $221 = 13 \times 17$ .

Inversement, est-il possible de démontrer de la sorte qu'un entier est un nombre premier ? Avant d'expliquer pourquoi la réponse est — hélas — négative, donnons une définition. On dira qu'un nombre entier  $p$  est *pseudo-premier* en base  $n$  si l'on a  $n^{p-1} \equiv 1 \pmod{p}$ , c'est-à-dire si le test du petit théorème de Fermat fonctionne. Remarquons que si  $a$  est un facteur commun à  $n$  et  $p$ , alors  $n^{p-1}$  est multiple de  $a$ , donc ne peut pas être congru à 1 modulo  $p$ .

Si l'on fixe la base, on ne peut pas espérer trop ; par exemple,  $2^{340} \equiv 1 \pmod{341}$  (*le vérifier...*), alors que  $341 = 11 \times 31$  n'est pas premier. On dira qu'un nombre entier  $p$  est pseudo-premier s'il est premier en toute base  $n$  qui est première à  $p$ . Les nombres premiers sont pseudo-premiers : c'est précisément ce qu'affirme le petit théorème de Fermat. Les nombres entiers qui sont pseudo-premiers sans être premiers sont appelés *nombres de Carmichael*. Il en existe ; le plus petit d'entre eux est  $561 = 3 \times 11 \times 17$ . Alford, Granville et Pomerance ont démontré en 1999 qu'il y a une infinité de nombres de Carmichael.

Il y a toutefois des algorithmes efficaces pour déterminer si un entier donné est un nombre premier. Le sujet est d'ailleurs en pleine effervescence.

## CHAPITRE 5

### CONGRUENCES

---

#### §1. Équations (du premier degré) aux congruences

Dans ce paragraphe, il s'agit d'expliquer la résolution de l'équation  $ax = b \pmod{n}$ , où  $a$ ,  $b$  et  $n$  sont des entiers fixés. Si  $a = 0$ , l'équation est  $b = 0 \pmod{n}$ . Il n'y a pas de solution si  $b$  n'est pas multiple de  $n$ , et tout entier est solution sinon. Nous supposons dans la suite que  $a \neq 0$ .

Par définition des congruences, on cherche donc à déterminer les entiers  $x$  tel que  $ax - b$  soit multiple de  $n$ , c'est-à-dire s'écrive  $yn$ , avec  $y \in \mathbf{Z}$ .

Cette relation peut s'écrire  $b = ax - ny$ . Posons  $d = \text{pgcd}(a, n)$ . Comme  $d$  divise  $a$  et  $n$ , la somme d'un multiple de  $a$  et d'un multiple de  $n$  est un multiple de  $d$ . Une condition nécessaire pour qu'il existe des solutions est donc que  $b$  soit multiple de  $d$  : il n'y a pas de solution si  $b$  n'est pas un multiple de  $d$ .

Supposons donc que  $b$  soit multiple de  $d$ . Posons  $A = a/d$ ,  $B = b/d$ ,  $N = n/d$  (comme  $a \neq 0$ ,  $d \neq 0$ ) ; ce sont des entiers. La congruence  $ax \equiv b \pmod{n}$  équivaut alors, par simplification par  $d$  à la congruence  $Ax \equiv B \pmod{N}$  dans laquelle  $A$  et  $N$  sont des entiers *premiers entre eux*.

PROPOSITION. — *Soit  $n$  un entier  $\geq 2$ . Soit  $a$  un entier. Pour qu'il existe un entier  $b$  tel que  $ab \equiv 1 \pmod{n}$ , il faut et il suffit que  $a$  et  $n$  soient premiers entre eux. On dit que  $a$  est inversible modulo  $n$  et que  $b$  est un inverse de  $a$  modulo  $n$ .*

*Supposons que  $a$  soit inversible modulo  $n$ . Si  $x$  et  $y$  sont des entiers tels que  $ax \equiv ay \pmod{n}$ , on a  $x \equiv y \pmod{n}$  :  $a$  est « simplifiable » modulo  $n$ .*

Supposons que  $a$  et  $n$  soient premiers entre eux. Soit  $1 = au + nv$  une relation de Bézout ; on a  $au \equiv 1 \pmod{n}$ . Inversement, si  $b$  est un entier tel que  $ab \equiv 1 \pmod{n}$ , il existe  $c \in \mathbf{Z}$  tel que  $ab + nc = 1$  ; cela entraîne qu'un diviseur commun à  $a$  et  $n$  divise 1, donc  $\text{pgcd}(a, n) = 1$ .

Supposons que  $a$  soit inversible modulo  $n$  et que  $ax \equiv ay \pmod{n}$ . Multiplions cette relation par un entier  $b$  tel que  $ab \equiv 1 \pmod{n}$ . Il vient  $abx \equiv aby \pmod{n}$ , d'où  $x \equiv y \pmod{n}$ . On peut aussi démontrer ce résultat à l'aide du théorème de Gauss : si  $ax \equiv ay \pmod{n}$ ,  $a(x - y)$  est multiple de  $n$ , donc  $x - y$  est multiple de  $n$  puisque  $a$  et  $n$  sont premiers entre eux ; par suite,  $x \equiv y \pmod{n}$ .

Notons que si  $b$  et  $b'$  sont des inverses de  $a$  modulo  $n$ , alors  $ab \equiv ab' \equiv 1 \pmod{n}$ , d'où  $b \equiv b' \pmod{n}$ . Modulo  $n$ , il n'y a qu'un seul inverse de  $a$  modulo  $n$ .

Revenons à la résolution de l'équation  $Ax \equiv B \pmod{N}$ , où  $A$  et  $N$  sont premiers entre eux. D'après la proposition, il existe un entier  $U$  tel que  $AU \equiv 1 \pmod{N}$ . Multiplions par  $U$  l'équation; on obtient  $AUx \equiv BU \pmod{N}$ , d'où  $x \equiv BU \pmod{N}$ . Inversement, si  $x \equiv BU \pmod{N}$ , on obtient, en multipliant par  $A$  les deux membres, la relation  $Ax \equiv ABU \equiv B \pmod{N}$ .

Pour déterminer  $U$ , remarquons qu'il suffit d'écrire une relation de Bézout pour  $a$  et  $n$ : si  $d = au + nv$ , alors  $1 = Au + Nv$  et  $Au \equiv 1 \pmod{N}$ , donc  $U = u$  convient!

En résumé, la résolution de l'équation  $ax = b \pmod{n}$  se fait comme suit :

Soit  $d$  le pgcd de  $a$  et  $n$ ; soit  $d = au + nv$  une relation de Bézout, calculée à l'aide de l'algorithme d'Euclide étendu.

Si  $b$  n'est pas multiple de  $d$ , il n'y a pas de solution.

Si  $b$  est multiple de  $d$ , l'équation équivaut à  $x \equiv bu/d \pmod{n/d}$ , les solutions étant donc les entiers  $x$  de la forme  $bu/d + k(n/d)$  avec  $k \in \mathbf{Z}$ .

*Exercices.* — 1) Résoudre les congruences suivantes :

- a)  $3x \equiv 5 \pmod{7}$ ;
- b)  $12x \equiv 8 \pmod{6}$ ;
- c)  $9x \equiv 6 \pmod{12}$ .

2) Résoudre les systèmes d'équations suivants :

- a)  $x + 2y \equiv 3 \pmod{7}$  et  $y \equiv 5 \pmod{7}$ ;
- b)  $x + 2y \equiv 3 \pmod{9}$  et  $x + y \equiv 5 \pmod{9}$ ;
- c)  $2x + 3y \equiv 3 \pmod{9}$  et  $3x + 4y \equiv 5 \pmod{9}$ ;
- d)  $2x + 3y \equiv 1 \pmod{15}$  et  $x + 4y \equiv 2 \pmod{15}$ ;
- e)  $2x + 3y \equiv 1 \pmod{15}$  et  $x + 4y \equiv 3 \pmod{15}$ .

3) Le code ISBN a été inventé dans les années 60 pour faciliter le travail de catalogage des livres dans les bibliothèques. Il se compose de 10 chiffres décimaux séparés par des espaces ou des tirets, dont le dernier peut aussi être le symbole X représentant la valeur 10. Le premier représente la langue (0 pour l'anglais, 2 pour le français, 3 pour l'allemand...), le bloc suivant l'éditeur (Springer-Verlag en Allemagne : 540, aux États-Unis : 387, Cassini : 84225, Dargaux : 205, etc.), le suivant le numéro du livre chez l'éditeur — il reste d'autant peu de place que l'éditeur a un gros numéro — et le dernier est un code permettant de s'assurer (au moins partiellement) de l'intégrité du code. Si les 10 chiffres sont  $a_1, \dots, a_{10}$ , la condition qu'ils doivent vérifier s'écrit

$$\sum_{i=1}^{10} i a_i \equiv 0 \pmod{11}.$$

a) Vérifier que 2-205-00694-0 (*Astérix en Corse*) et 0-387-54894-7 (*Introduction to Coding Theory* de J. H. van Lint) sont des codes ISBN valides.

b) Vérifier que 2-84225-007-1 n'est pas un ISBN valide. Peut-on le corriger ?

c) Montrer que l'on peut détecter un chiffre inexact, ou l'interversion de deux chiffres dans un ISBN (en supposant qu'il n'y ait qu'une seule erreur de ce type).

4) Le code de sécurité sociale est formé de 13 chiffres décimaux suivi d'une clef de deux chiffres. Si  $N$  est l'entier de 13 chiffres et  $c$  la clef, la contrainte de vérification est la relation

$$N + c \equiv 0 \pmod{97}.$$

- a) Quelle est la clef d'un individu dont le numéro de sécurité sociale serait 1-71-04-78-646-378 ?
- b) Un numéro de sécurité sociale est 2-xx-07-35-231-584, clé 19, mais les caractères xx sont illisibles. Pouvez-vous retrouver l'année de naissance de la personne en question ? (Solution : 1943)
- c) Montrer que la clef de contrôle détecte une erreur sur un chiffre, ainsi que l'interversion de deux chiffres consécutifs.
- d) Montrer que 97 est un nombre premier et que  $n = 96$  est le plus petit entier  $> 0$  tel que  $10^n \equiv 1 \pmod{97}$ .
- e) Montrer plus généralement que la clef de contrôle détecte l'interversion de deux chiffres quelconques.
- 5) Soit  $\varphi$  l'application de  $\{0, \dots, 9\}$  dans lui-même définie par  $\varphi(x) = 2x$  si  $x \leq 4$  et  $\varphi(x) = 1 + 2(x - 5)$  si  $x \geq 5$ . Un numéro de carte bancaire est un nombre décimal de la forme  $a_n a_{n-1} \dots a_1 a_0$ , où les chiffres décimaux satisfont à la règle (dite de Luhn) :

$$a_0 + \varphi(a_1) + a_2 + \varphi(a_3) + \dots \equiv 0 \pmod{10}.$$

- a) Montrer que cela permet de détecter la présence d'un chiffre décimal erroné.
- b) Montrer que cela permet de détecter une permutation de deux chiffres consécutifs, à l'exception de la permutation  $09 \rightarrow 90$ .

Avant l'introduction de l'Euro, les billets de banque allemands utilisaient paraît-il un code obtenu par l'adjonction d'un chiffre décimal à un nombre décimal de 9 chiffres qui détectait une erreur ou l'interversion de deux chiffres consécutifs.

## §2. Théorème chinois

On trouve dans un traité chinois (III-V<sup>e</sup> siècle ap. J.-C.) l'énoncé suivant :

Nous avons des choses dont nous ne connaissons pas le nombre ;

- si nous les comptons par paquets de trois, le reste est 2 ;
- si nous les comptons par paquets de cinq, le reste est 3 ;
- si nous les comptons par paquets de sept, le reste est 2.

Combien y a-t-il de choses ? Réponse : 23.

Si  $x$  est le nombre de paquets, les conditions signifient respectivement que  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$  et  $x \equiv 2 \pmod{7}$  : il s'agit de résoudre simultanément plusieurs congruences. Mathématiquement, la solution de ce problème repose sur le théorème (appelé *théorème chinois*) qui permet, dans certains cas, de regrouper deux équations en congruences en une seule.

THÉORÈME. — Soit  $m$  et  $n$  deux entiers premiers entre eux. Soit  $a$  et  $b$  deux entiers. Il existe un unique entier  $c$  tel que  $0 \leq c < mn$  et qui vérifie  $c \equiv a \pmod{m}$  et  $c \equiv b \pmod{n}$ .

Soit  $x$  un entier relatif tel que  $x \equiv a \pmod{m}$  et  $x \equiv b \pmod{n}$ ; alors  $x \equiv c \pmod{mn}$ .

Pour démontrer ce théorème, considérons l'application  $r$  de  $\{0, \dots, mn - 1\}$  dans  $\{0, \dots, l - 1\} \times \{0, \dots, n - 1\}$  qui, à un entier  $x \in \{0, \dots, mn - 1\}$ , associe le couple formé des restes des divisions euclidiennes de  $x$  par  $m$  et  $n$ . Elle est injective. En effet, si  $x \equiv y \pmod{m}$  et  $x \equiv y \pmod{n}$ ,  $x - y$  est divisible à la fois par  $m$  et par  $n$ , donc par leur produit  $mn$ , puisqu'ils sont premiers entre eux. Comme ensembles de départ et d'arrivée ont même cardinal, cela entraîne le théorème.

Appliquons ce théorème à un système d'équations en congruences. Avec les notations du théorème chinois, déterminons l'ensemble des solutions du système des deux équations en nombres entiers  $x \equiv a \pmod{m}$  et  $x \equiv b \pmod{n}$ . Soit  $r$  le reste de la division euclidienne de  $x$  par  $mn$ . Comme  $m$  et  $n$  divisent  $mn$ , on a  $x \equiv r \pmod{m}$  et  $x \equiv r \pmod{n}$ . Par suite, le système à résoudre équivaut aux deux congruences  $r \equiv a \pmod{m}$  et  $r \equiv b \pmod{n}$ . D'après le théorème chinois, il existe un unique entier  $c \in \{0, \dots, mn - 1\}$  qui vérifie ces congruences. Par conséquent,  $x$  est solution du système initial si et seulement si  $r = c$  et l'ensemble des solutions cherché est l'ensemble des entiers  $x$  tels que  $x \equiv c \pmod{mn}$ .

Toutefois, la démonstration du théorème chinois que nous avons donnée ne précise pas *comment* trouver effectivement un tel entier.

Pour cela, nous allons utiliser la décomposition d'un entier en base mixte.

THÉORÈME. — Soit  $b_1, \dots, b_k$  des entiers  $\geq 2$ . Tout entier  $n$  s'écrit de manière unique sous la forme

$$n = a_1 + a_2 b_1 + a_3 b_1 b_2 + \dots + a_k b_1 \dots b_{k-1} + n' b_1 \dots b_k$$

où  $a_1, \dots, a_k$  sont des entiers tels que  $0 \leq a_i < b_i$  pour tout  $i \in \{1, \dots, k\}$  et  $n' \in \mathbf{Z}$ .

La démonstration par récurrence de cette écriture est très simple : nécessairement, l'entier  $a_1$  est le reste de la division euclidienne de  $n$  par  $b_1$ . Soit  $n_1$  le quotient ; par récurrence, il existe des entiers  $a_2, \dots, a_k$ , uniquement déterminés par la condition  $0 \leq a_i < b_i$ , et un entier  $n' \in \mathbf{Z}$  tels que  $n_1 = a_2 + a_3 b_2 + \dots + a_k b_2 \dots b_{k-1} + n' b_2 \dots b_k$ . Alors,  $n = a_1 + b_1 n_1$  s'écrit sous la forme annoncée.

Remarquons que l'on a  $n' = 0$  si et seulement si  $0 \leq n < b_1 \dots b_k$ .

Pour résoudre les congruences  $x \equiv x_k \pmod{b_k}$  (pour  $1 \leq k \leq n$ ) on cherche  $x$  dans sa décomposition en base mixte  $a_1 + a_2 b_1 + \dots + a_n b_1 \dots b_{n-1} + q b_1 \dots b_n$ . La première condition  $x \equiv x_1 \pmod{b_1}$  entraîne  $a_1 = x_1 \pmod{b_1}$ , car tous les autres termes sont multiples de  $b_1$ , d'où  $x_1$ . Si  $a_1, \dots, a_{k-1}$  sont déterminés, la condition  $x \equiv x_k \pmod{b_k}$  s'écrit

$$a_k (b_1 \dots b_{k-1}) \equiv x_k - a_1 - a_2 b_1 - \dots - a_{k-1} b_1 \dots b_{k-2} \pmod{b_k},$$

car tous les autres termes sont multiples de  $b_k$ . Il reste à résoudre cette équation à l'aide des méthodes du paragraphe précédent.

Notons le cas particulier important où *les  $b_k$  sont premiers entre eux deux à deux*. Alors,  $b_1 \dots b_{k-1}$  est premier à  $b_k$  pour tout entier  $k$  tel que  $1 \leq k \leq n$ . (Un nombre premier qui divise  $b_k$  ne divise aucun autre  $b_i$ , donc ne divise pas  $b_1 \dots b_{k-1}$ .) D'après le paragraphe précédent, l'équation  $a_k(b_1 \dots b_{k-1}) \equiv y_k \pmod{b_k}$  possède une unique solution modulo  $b_k$ , d'où l'existence d'un unique entier  $a_k$  qui vérifie cette congruence et tel que  $0 \leq a_k < b_k$ . À la fin de la résolution, on a déterminé l'*unique* entier  $x_0$  tel que  $0 \leq x_0 < b_1 \dots b_n$  et  $x_0 \equiv x_k \pmod{b_k}$  pour tout  $k$  compris entre 1 et  $n$ . Les solutions du système de congruences sont les entiers de la forme  $x_0 + c b_1 \dots b_n$ , avec  $c \in \mathbf{Z}$ .

Cela démontre la généralisation suivante du théorème chinois :

PROPOSITION. — *Soit  $b_1, \dots, b_n$  des entiers premiers entre eux deux à deux et soit  $a_1, \dots, a_n$  des entiers relatifs. Il existe un unique entier  $a$  tel que  $0 \leq x < b_1 \dots b_n$  qui vérifie les congruences  $a \equiv a_i \pmod{b_i}$  pour tout entier  $i$  compris entre 1 et  $n$ .*

*De plus, si  $x$  est un entier relatif tel que  $x \equiv a_i \pmod{b_i}$ , alors  $x \equiv a \pmod{b_1 \dots b_n}$ .*

Donnons maintenant un exemple concret en résolvant le problème chinois du début de ce paragraphe. On cherche un entier  $x$  tel que  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$  et  $x \equiv 2 \pmod{7}$ . Remarquons que 3, 5 et 7 sont premiers entre eux deux à deux; on va donc obtenir un unique entier  $x$  modulo 105 vérifiant ces congruences.

Pour déterminer  $x$ , on l'écrit en base mixte, sous la forme  $a + 3b + 15c + 105d$ , avec  $0 \leq a < 3$ ,  $0 \leq b < 5$  et  $0 \leq c < 7$ . La relation  $x \equiv 2 \pmod{3}$  entraîne  $a = 2$ . La relation  $x \equiv 3 \pmod{5}$  se réécrit  $2 + 3b \equiv 3 \pmod{5}$ , d'où  $3b \equiv 1 \pmod{5}$ ;  $b = 2$  convient; comme 3 et 5 sont premiers entre eux, c'est la seule solution modulo 5, d'où  $b = 2$ . La dernière relation  $x \equiv 2 \pmod{7}$  devient  $15c \equiv 2 - 2 - 6 \equiv 1 \pmod{7}$ . On constate que  $c = 1$  convient ( $15 - 2 \times 7 = 1$ ) et c'est la seule solution modulo 7 car 15 et 7 sont premiers entre eux, d'où  $c = 1$ . Finalement  $x = 2 + 6 + 15 + 105d = 23 + 105d$ , où 105 est un entier arbitraire. Les solutions sont donc les entiers congrus à 23 modulo 105.

- Exercices.* — 1) Trouver le plus petit entier  $> 10000$  qui divisé par 5, 12 et 14 ait pour reste 3.  
 2) Quel est le plus petit entier plus grand que 10000 qui divisé par 5, 12 et 17 ait pour reste 3?  
 3) Trouver tous les entiers compris entre 100 et 1000 qui divisés par 21 aient pour reste 8 et par 17 pour reste 5.  
 4) Sachant que le 1<sup>er</sup> janvier 1901 était un mardi, combien de vendredi 13 y a-t-il eu au XX<sup>e</sup> siècle? Dans le calendrier grégorien, calculer les fréquences des lundi 13, mardi 13, etc.  
 5) Une vieille fermière s'en allant marché voit ses œufs écrasés par un cheval. Le cavalier voulant la rembourser lui demande combien d'œufs elle avait. Tout ce dont elle se souvient est qu'en les rangeant par 2, il en restait un, et de même en les rangeant par 3, 4, 5 ou 6; toutefois, en les rangeant par 7, il n'en restait pas. Combien d'œufs, au moins, avait-elle? (D'après Lauritzen, repris de Ore)  
 6) Sur une île déserte, cinq hommes et un singe ramassent des noix de coco. La nuit tombée, il s'endorment. Le premier homme se réveille et prend sa part du butin : il divise le tas de noix en cinq parts égales et donne au singe la noix de coco restante, prend sa part et va se recoucher. Le second se réveille, prend un cinquième du tas restant et donne au singe une noix qui restait à part. Et ainsi de suite des cinq hommes. Combien de noix de coco, au moins, avaient été ramassées? (D'après Lauritzen)

7) « Une dame ayant rencontré des pauvres, a eu la pensée charitable de leur donner ce qu'elle avait. Pour donner à chacun 9 sous, il lui en manquait 32 ; alors elle leur a donné 7 sous, et il lui en est resté 24. Combien avait-elle et quel est le nombre des pauvres ? » (J. Vinot, *Récréations mathématiques*, années 30).

8) L'armée de César comptait plus de 1000 hommes, mais moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 11, il n'en resta pas ; par groupes de 9, il en resta 5 ; par groupes de 13, il en resta 8. Combient y avait-il de soldats dans cette armée ? (D'après J. Vinot)

9) Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques. Leur loi exige un partage à égalité : chacun doit recevoir le même nombre de pièces d'or et, s'il y a un reste, celui-ci est attribué au cuisinier de bord. Dans le cas présent, la part du cuisinier serait de trois pièces, mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une terrible tempête, le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur, le butin est sauvé. La part du cuisinier est maintenant de cinq pièces. Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage, sachant que c'est la plus petite des solutions possibles ?

### §3. Indicateur d'Euler, cryptographie RSA

Soit  $n$  un entier  $\geq 2$ . On note  $\varphi(n)$  le nombre des entiers  $m$  avec  $1 \leq m \leq n$  qui sont premiers à  $n$ . Si  $n$  est un nombre premier, on a par exemple  $\varphi(n) = n - 1$ .

PROPOSITION. — *Pour tout entier  $a$  qui est premier à  $n$ , on a la congruence  $a^{\varphi(n)} \equiv 1 \pmod{n}$ . En outre, le plus petit entier  $m \geq 1$  tel que  $a^m \equiv 1 \pmod{n}$  est un diviseur de  $\varphi(n)$ .*

Par suite, on peut définir l'ordre multiplicatif modulo  $n$  d'un entier  $a$  qui est premier à  $n$  comme le plus petit entier  $k$  tel que  $a^k \equiv 1 \pmod{n}$  ; c'est un diviseur de  $\varphi(n)$ . Cela généralise un résultat déjà démontré au chapitre précédent lorsque  $n$  est un nombre premier.

Notons  $\Phi$  l'ensemble des entiers  $m$  tels que  $1 \leq m \leq n - 1$  qui sont premiers à  $n$ . Soit  $a$  un entier premier à  $n$  et considérons l'application  $f$  de  $\{0, \dots, n - 1\}$  dans lui-même qui, à un entier  $x$ , associe le reste de la division euclidienne de  $ax$  par  $n$ .

Cette application est bijective. Soit  $b \in \mathbf{Z}$  tel que  $ab \equiv 1 \pmod{n}$ . Si  $y \in \{0, \dots, n - 1\}$ , la relation  $ax \equiv y \pmod{n}$  entraîne  $x \equiv abx \equiv by \pmod{n}$ , et inversement. Cela montre que  $y$  a un unique antécédent modulo  $n$ .

Montrons que  $f(\Phi) \subset \Phi$ . Soit  $d$  le plus grand diviseur commun de  $n$  et  $f(x)$ . Soit  $q \in \mathbf{Z}$  tel que  $ax = qn + f(x)$ . Alors,  $d$  divise  $ax$ . Comme  $d$  divise  $n$  et que  $a$  est premier à  $n$ ,  $d$  est premier à  $a$ , d'où  $d$  divise  $x$ . Si  $x \in \Phi$ , cela entraîne  $d = 1$ , donc  $n$  et  $f(x)$  sont premiers entre eux, c'est-à-dire  $f(x) \in \Phi$ . Comme  $\Phi$  est fini,  $f$  définit une bijection de  $\Phi$  dans lui-même. Il en résulte que

$$\prod_{x \in \Phi} f(x) = \prod_{x \in \Phi} x.$$

Notons  $N$  cet entier. C'est un produit d'entiers premiers à  $n$ , donc est premier à  $n$ .

Comme  $\varphi(n)$  est le cardinal de  $\Phi$ , on a aussi

$$\prod_{x \in \Phi} f(x) \equiv \prod_{x \in \Phi} (ax) \equiv a^{\varphi(n)} \prod_{x \in \Phi} x \pmod{n}.$$

Autrement dit,  $N(a^{\varphi(n)} - 1)$  est multiple de  $n$ . Puisque  $N$  est premier à  $n$ ,  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , ainsi qu'il fallait démontrer.

Soit  $m$  le plus petit entier  $\geq 1$  tel que  $a^m \equiv 1 \pmod{n}$  et montrons que  $m$  divise  $\varphi(n)$ . La division euclidienne de  $\varphi(n)$  par  $m$  s'écrit  $\varphi(n) = qm + r$ , avec  $0 \leq r \leq m - 1$ . On a alors

$$1 \equiv a^{\varphi(n)} \equiv (a^m)^q a^r \equiv a^r \pmod{n}.$$

Par minimalité de  $m$ ,  $r = 0$ , ce qui montre que  $m$  divise  $\varphi(n)$ .

À la fin des années 1970, Rivest, Shamir et Adleman ont utilisé ces résultats pour élaborer un *système de cryptographie à clef publique* : système depuis appelé RSA, du nom de ses auteurs.

Il repose sur le fait qu'il existe des applications bijectives  $f: A \rightarrow B$  d'un ensemble fini  $A$  dans un ensemble  $B$  pour lesquelles il est facile de calculer  $f(a)$ , si  $a \in A$ , alors que personne ne sait calculer efficacement  $f^{-1}(b)$ , si  $b \in B$ . Il y a bien une solution évidente, consistant à calculer toutes les valeurs possibles pour  $f(a)$  et à attendre le moment où l'on obtient  $b$ , mais si  $A$  et  $B$  ont un cardinal énorme, de l'ordre de  $10^{1000}$ , le temps que cela risque de prendre dépasse la durée de vie du soleil!

Imaginons qu'un élément de  $A$  soit un message (ou un morceau de message); le message crypté sera  $f(a)$ . À moins de connaître  $f^{-1}$  explicitement, personne ne peut le décoder. Notons aussi qu'on peut même rendre la fonction  $f$  publique, de sorte que n'importe qui puisse coder des messages, sans rompre la sécurité du système. Mais comment produire de telles fonctions  $f$ ? C'est là que réside l'astuce des auteurs de RSA : les congruences fournissent précisément ce genre d'applications.

Précisément, soit  $p$  et  $q$  deux nombres premiers et soit  $N = pq$ . On choisit  $A$  et  $B$  égaux à l'ensemble des entiers  $n \in \{1, \dots, N\}$  qui sont premiers à  $N$ . Si  $n \in A$ , on sait (Euler) que  $n^{\varphi(N)} \equiv 1 \pmod{N}$ .

Or,  $\varphi(N) = (p-1)(q-1)$ . Soit ainsi  $e$  un entier petit, premier à  $\varphi(N)$  (en pratique,  $e = 3$ , ou  $11$ ; c'est-à-dire que  $p$  et  $q$  sont choisis en fonction de  $d \dots$ ). La fonction  $f$  est la fonction  $x \mapsto x^e \pmod{N}$ ; la fonction  $g$  est la fonction  $x \mapsto x^d \pmod{N}$ , où  $d$  est un entier tel que  $de \equiv 1 \pmod{\varphi(N)}$ . Si  $de = 1 + \varphi(N)k$ , on a bien

$$g \circ f(x) \equiv (x^d)^e \equiv x^{de} \equiv x^{1+\varphi(N)k} \equiv x \pmod{N},$$

donc  $g$  est l'inverse de  $f$  et celui qui connaît l'entier  $d$  peut décoder les messages.<sup>(1)</sup> C'est donc cet entier  $d$  qui constitue la *clé secrète*; les entiers  $e$  et  $N$  constituent la clé publique. Les nombres premiers  $p$  et  $q$  sont aussi gardés secrets; dans la pratique, l'ordinateur qui les fabrique les détruit après avoir calculé  $N$ ,  $d$  et  $e$ .

Pourquoi est-ce que cela marche?

<sup>(1)</sup> Les lettres  $e$  et  $d$  sont les premières lettres des mots anglais *encoding* et *decoding*.

1) Il est très facile de calculer  $x^k \pmod{N}$ . On pourrait croire qu'il faut  $k - 1$  multiplications, mais en fait, il en faut beaucoup moins. En effet, écrivons  $k$  en base 2 :  $k = c_r 2^r + \dots + c_0$ , avec  $c_i \in \{0, 1\}$ . On écrit alors

$$x^k = x^{c_0} (x^2)^{c_1} (x^4)^{c_2} \dots (x^{2^r})^{c_r}.$$

On a donc  $r$  élévations au carré et  $r$  multiplications à effectuer, donc en gros  $2 \log_2 k$  opérations : c'est bien moins que  $k$ .

2) Pour l'instant, personne ne peut espérer retrouver  $d$  dans un temps raisonnablement court s'il ne connaît que  $e$  et  $N$ . Bien entendu, il suffit de calculer  $\varphi(N)$ , car on peut alors calculer  $d$  à l'aide de la relation de Bézout. Mais comment calculer  $\varphi(N)$  ? On ne connaît rien de mieux que de factoriser  $N$ , c'est-à-dire, de retrouver  $p$  et  $q$ . Et ceci est très long, au moins dans la pratique, et si les entiers  $p$  et  $q$  sont convenablement choisis. La méthode naïve demanderait de tester la divisibilité par tous les entiers successifs. Cependant, même si l'on sait qu'on n'a pas besoin d'aller plus loin que  $\sqrt{N}$ , cela fait tout de même plus de  $10^{30}$  années pour un entier  $N$  de 100 chiffres, en effectuant  $10^{10}$  divisions par seconde.

En 1999, 300 ordinateurs en réseau ont pu casser un *challenge* RSA en environ six mois : c'était un entier d'environ 150 chiffres. Le coût de l'opération est estimé à environ 1 million de dollars. Les recommandations actuelles demandent d'utiliser des entiers de plus de 250, voire plus de 500 chiffres dans des situations critiques... Un article récent (2003) propose la construction d'une machine, l'ensemble revenant à au moins 30 millions de dollars.

3) On a aussi besoin de fabriquer de grands nombres premiers Il y a des méthodes pour cela, à base de formules du genre de celles définissant les nombres de Fermat, Mersenne, etc. Parmi les entiers produits, il faut savoir lesquels sont des nombres premiers. Comment faire ? Là encore, il y a des astuces : on a vu que le petit théorème de Fermat permet de montrer qu'un entier n'est pas premier ; on a vu qu'il y a aussi des nombres de Carmichael pour lesquels ce test laisse croire que l'on a affaire à un nombre premier. Il existe cependant un raffinement assez simple de ce test de Fermat pour lequel il n'y a plus ce phénomène de nombres de Carmichael. On parle de *nombre fortement pseudo-premier en base a*. Un joli théorème de Rabin montre que si un entier n'est pas premier, au moins 3/4 des bases le mettent en évidence. La méthode consiste alors à tirer des bases au hasard et à regarder ce qui se passe ; au bout de 10 essais réussis, la *probabilité* que l'entier choisi ne soit pas premier est égale à  $2^{-20}$ . C'est paraît-il bien moins que la probabilité qu'au même moment, un rayon cosmique détruise l'ordinateur qui fait le calcul...

*Exercices.* — 1) Pour chaque valeur de l'entier  $n$ ,  $2 \leq n \leq 20$ , calculer  $\varphi(n)$  en dénombrant les entiers de  $\{1, \dots, n\}$  qui sont premiers avec  $n$ .

2) a) Calculer  $\varphi(n)$  si  $n$  est une puissance d'un nombre premier  $p$ .

b) En utilisant le théorème chinois, démontrer que  $\varphi(mn) = \varphi(m)\varphi(n)$  si  $m$  et  $n$  sont des entiers premiers entre eux.

c) En déduire  $\varphi(n)$  en fonction de la décomposition en facteurs premiers de  $n$ .

- 3) Soit  $n$  un entier qui est le produit de deux nombres premiers distincts. Montrer que pour tout  $x \in \mathbf{Z}$ , on a  $x^{\varphi(n)+1} \equiv x \pmod{n}$ .
- 4) Soit  $n$  un entier  $\geq 2$ ; si  $0 \leq k \leq n-1$ , on note  $c_k = \exp(2ik\pi/n)$ .
- Montrer que  $\{c_0, \dots, c_n\}$  est l'ensemble des racines complexes du polynôme  $X^n - 1$ .
  - Soit  $c \in \mathbf{C}^*$ ; on suppose que  $c^n = 1$ . Soit  $d$  le plus petit entier  $> 0$  tel que  $c^d = 1$ . (On dit que  $c$  est d'ordre  $d$ .) Montrer que  $n$  est multiple de  $d$ .
  - On suppose que  $n$  est le plus petit entier  $> 0$  tel que  $c^n = 1$ . Montrer qu'il existe un unique entier  $k \in \{0, \dots, n\}$  tel que  $\text{pgcd}(k, n) = 1$  et tel que  $c = c_k$ . Combien y a-t-il de tels nombres complexes  $c$ ?
  - Plus généralement, si  $d$  divise  $n$ , combien y a-t-il d'éléments  $c \in \mathbf{C}^*$  qui sont d'ordre  $d$ ?
  - Montrer que  $\sum_{d|n} \varphi(d) = n$ , où la somme est prise sur l'ensemble des diviseurs  $> 0$  de  $n$ .

#### §4. Équations polynomiales modulo $n$

On a appris à résoudre des équations de la forme  $ax \equiv b \pmod{n}$ , où  $a$ ,  $b$  et  $n$  sont des nombres entiers. Dans ce paragraphe, il s'agit d'expliquer comment trouver les solutions modulo  $n$  d'une équation polynomiale.

Un polynôme à coefficients entiers en une variable  $X$  est une expression de la forme  $P(X) = a_0 + a_1X + \dots + a_dX^d$ , où  $a_0, \dots, a_d$  sont des nombres entiers. Si  $a_d \neq 0$ , on dit que le polynôme  $P$  est de degré  $d$ ; quitte à ne pas écrire les termes dont le coefficient est nul, on peut facilement se ramener à ce cas.

Soit  $n$  un entier et  $P$  un polynôme à coefficients entiers en une variable  $X$ . On dit qu'un entier  $x$  est *racine de  $P$  modulo  $n$*  si  $P(x) \equiv 0 \pmod{n}$ .

Si  $x \equiv y \pmod{n}$ , alors  $P(x) \equiv P(y) \pmod{n}$ ; en particulier, tout entier congru modulo  $n$  à une racine de  $P$  modulo  $n$  est une racine de  $P$  modulo  $n$ . Par suite, il suffit, pour connaître les racines de  $P$  modulo  $n$ , de connaître la liste de celles qui sont comprises entre 0 et  $n-1$ .

Il y a trois principes permettant de déterminer, dans la pratique, les racines d'une équation polynomiale donnée  $P$  modulo un entier donné  $n$ . Notons  $n = \prod p_i^{m_i}$  la décomposition en facteurs premiers de  $n$ .

- Si l'on connaît les racines de  $P$  modulo  $p_i^{m_i}$ , pour tout  $i$ , le théorème chinois permet de déterminer les racines de  $P$  modulo  $n$ .
- Supposons que  $n = p^m$  soit une puissance d'un nombre premier  $p$ . On commence par déterminer les racines de  $P$  modulo  $p$ .
- Pour chacune de ces racines  $a$ , on cherche une racine de  $P$  modulo  $p^m$  de la forme  $x = a + py$ ; on transforme l'équation en développant pour obtenir une équation  $P(a + py) = Q(y) \equiv 0 \pmod{p^m}$ ; on constate que les coefficients de  $Q$  sont tous multiples de  $p$ , d'où en simplifiant une équation de la forme  $Q_1(y) \equiv 0 \pmod{p^{m-1}}$ , qu'on résout en itérant le processus.

*Exemple.* — Soit à résoudre l'équation  $x^2 + 5x + 6 \equiv 0 \pmod{18}$ . On a  $18 = 2 \times 3^2$ . On commence par résoudre les deux équations  $x^2 + 5x + 6 \equiv 0 \pmod{2}$  et  $x^2 + 5x + 6 \equiv 0 \pmod{9}$ .

- modulo 2.* La première se réécrit  $x^2 + x \equiv 0 \pmod{2}$ , dont tout entier est solution.

2) *modulo 3*. Pour résoudre la seconde, on commence par regarder l'équation  $x^2 + 5x + 6 \equiv 0 \pmod{3}$ ; comme  $5 \equiv -1 \pmod{3}$  et 3 divise 6, elle se réécrit  $x^2 - x \equiv 0 \pmod{3}$ . Là, 0 et 1 sont solutions, mais pas 2.

2a) *solutions modulo 9 congrues à 0 modulo 3*. Cherchons les solutions de l'équation modulo 9 qui sont congrues à 0 modulo 3; on écrit  $x = 3y$ , d'où  $9y^2 + 15y + 6 \equiv 0 \pmod{9}$ ; simplifiant tout par 3, on obtient  $3y^2 + 5y + 2 \equiv 0 \pmod{3}$  puis  $2(y + 1) \equiv 0 \pmod{3}$  dont la seule solution est  $2 \pmod{3}$ . On obtient  $x \equiv 6 \pmod{9}$  pour ce premier sous-cas.

2b) *solutions modulo 9 congrues à 1 modulo 3*. On écrit  $x = 1 + 3y$ , d'où  $1 + 6y + 9y^2 + 5 + 15y + 6 \equiv 0 \pmod{9}$  puis  $3(4 + 7y + 3y^2) \equiv 0 \pmod{9}$ , soit encore  $4 + 7y + 3y^2 \equiv 0 \pmod{3}$  et enfin  $1 + y \equiv 0 \pmod{3}$ . On trouve  $y \equiv 2 \pmod{3}$ , d'où  $x \equiv 7 \pmod{9}$ .

3) *solutions communes aux congruences modulo 2 et modulo 9*. Pour chaque combinaison des solutions de chaque congruence, il y a un système du type « théorème chinois » à résoudre.

3a)  $x \equiv 0 \pmod{2}$  et  $x \equiv 6 \pmod{9}$ ; on obtient  $x \equiv 6 \pmod{18}$ .

3b)  $x \equiv 0 \pmod{2}$  et  $x \equiv 7 \pmod{9}$ ; on obtient  $x \equiv 16 \pmod{18}$ .

3c)  $x \equiv 1 \pmod{2}$  et  $x \equiv 6 \pmod{9}$ ; on obtient  $x \equiv 15 \pmod{18}$ .

3d)  $x \equiv 1 \pmod{2}$  et  $x \equiv 7 \pmod{9}$ ; on obtient  $x \equiv 7 \pmod{18}$ .

## §5. Équations polynomiales modulo un nombre premier

Commençons par le cas d'une *équation du second degré*, c'est-à-dire d'une équation de la forme  $ax^2 + bx + c \equiv 0 \pmod{p}$ .

On suppose que  $a \not\equiv 0 \pmod{p}$ ; dans le cas contraire, l'équation est du premier degré.

Si  $p = 2$ , il suffit de regarder si 0 et 1 sont racines modulo 2.

Supposons maintenant  $p \neq 2$ . Alors, il existe  $b' \in \mathbf{Z}$  tel que  $b \equiv 2ab' \pmod{p}$ ; l'équation devient alors  $ax^2 + 2ab'x + c \equiv 0 \pmod{p}$ . On remarque un début d'identité remarquable

$$ax^2 + 2ab'x + c = a(x^2 + 2b'x) + c = a(x + b')^2 + c - a(b')^2,$$

d'où finalement l'équation

$$a(x + b')^2 \equiv a(b')^2 - c \pmod{p}.$$

Multiplions cette équation par un inverse  $a'$  de  $a$  modulo  $p$ ; on trouve

$$(x + b')^2 \equiv (b')^2 - ca' \pmod{p}.$$

Posons  $\Delta' = (b')^2 - ca'$  (*discriminant réduit*). Il y a alors deux cas : ou bien il existe  $u \in \mathbf{Z}$  tel que  $u^2 \equiv \Delta' \pmod{p}$  (l'entier  $\Delta'$  est un carré modulo  $p$ ); l'équation devient alors

$$(x + b')^2 \equiv u^2 \pmod{p},$$

donc  $(x + b' - u)(x + b' + u) \equiv 0 \pmod{p}$  dont les solutions sont  $x \equiv -b' + u \pmod{p}$  et  $x \equiv -b' - u \pmod{p}$ . (Si  $u \equiv 0 \pmod{p}$ , c'est-à-dire si  $\Delta' \equiv 0 \pmod{p}$ , ces deux solutions ne font qu'une.) Dans l'autre cas,  $\Delta'$  n'est pas un carré modulo  $p$ , il n'existe pas d'entier  $u$  tel que  $u^2 \equiv \Delta' \pmod{p}$ ; l'équation n'a alors pas de solution.

Il convient aussi de remarquer que

$$(2a)^2 \Delta' = (2a)^2 ((b')^2 - ca') \equiv (2ab')^2 - 4a(aa')c \equiv b^2 - 4ac \pmod{p}.$$

Par suite, pour que  $\Delta'$  soit un carré modulo  $p$ , il faut et il suffit que l'entier  $\Delta = b^2 - 4ac$  (*discriminant*) soit un carré modulo  $p$ .

On remarque qu'il y a 0, 1 racine (« double ») ou 2 racines modulo  $p$  suivant que le discriminant n'est pas un carré modulo  $p$ , est nul modulo  $p$  ou est un carré non nul modulo  $p$ . La résolution de l'équation du second degré modulo  $p$  est ainsi formellement identique à la résolution d'une équation du second degré en nombres réels.

Concernant l'équation générale de degré  $d$  arbitraire, le seul résultat que nous démontrerons est qu'il y a *au plus*  $d$  racines modulo  $p$ .

LEMME 5.1. — *Soit  $P$  un polynôme à coefficient entiers de degré  $d$ , soit  $p$  un nombre premier et soit  $c$  une racine de  $P$  modulo  $p$ . Il existe un unique polynôme  $Q$  de degré  $d-1$  tel que  $P(x) - P(c) = (x-c)Q(x)$ . Pour qu'un entier  $x$  soit racine de  $P$  modulo  $p$  il faut et il suffit qu'on ait  $x \equiv c \pmod{p}$  ou que  $x$  soit racine de  $Q$  modulo  $p$ .*

Notons  $a_0, \dots, a_d$  les coefficients de  $P(x)$ , de sorte que  $P(x) = a_d x^d + \dots + a_0$  et développons l'expression  $P(x) - P(c)$ . On a  $P(x) - P(c) = \sum_{k=0}^d a_k (x^k - c^k)$ . En appliquant l'identité remarquable

$$x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \dots + xy^{k-2} + y^{k-1})$$

avec  $y = c$ , on trouve

$$P(x) - P(c) = \sum_{k=0}^d a_k (x-c) \sum_{j=0}^{k-1} x^j c^{k-1-j} = (x-c)Q(x),$$

où  $Q$  est le polynôme de degré au plus  $d-1$

$$Q(x) = \sum_{k=1}^d \sum_{j=0}^{k-1} a_k x^j c^{k-1-j} = \sum_{j=0}^{d-1} \left( \sum_{k=j+1}^d a_k c^{k-1-j} \right) x^j.$$

Comme le coefficient dominant de  $Q$  est  $a_d x^{d-1}$ , le polynôme  $Q$  est effectivement de degré  $d-1$ .

Soit maintenant  $x$  un entier. Si  $x \equiv c \pmod{p}$ , alors  $P(x) \equiv P(c) \equiv 0 \pmod{p}$ , donc  $x$  est racine de  $P$  modulo  $p$ . Si  $Q(x) \equiv 0 \pmod{p}$ ,  $P(x) \equiv P(c) + (x-c)Q(x) \equiv 0 \pmod{p}$ , donc  $x$  est aussi racine de  $P$  modulo  $p$ . Inversement, si  $x$  est racine de  $P$  modulo  $p$ ,  $(x-c)Q(x) \equiv P(x) - P(c) \equiv 0 \pmod{p}$ . Si de plus  $x$  n'est pas congru à  $c$  modulo  $p$ , le lemme d'Euclide entraîne que  $Q(x) \equiv 0 \pmod{p}$ , autrement dit  $x$  est racine de  $Q$  modulo  $p$ .

THÉORÈME. — *Soit  $p$  un nombre premier et soit  $A = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0$  un polynôme à coefficients entiers. Alors, le nombre d'entiers  $k \in \{0, \dots, p-1\}$  tels que  $A(k) \equiv 0 \pmod{p}$  est au plus égal à  $d$ .*

Montrons ce résultat par récurrence sur le degré  $d$  de  $A$ . Si  $n = 0$ ,  $A = a_0$  est constant,  $a_0$  n'est pas multiple de  $p$ , et il n'y a aucun entier  $k$  tel que  $A(k) \equiv 0 \pmod{p}$ .

Supposons maintenant le résultat vrai pour tout polynôme de degré  $< d$ . Notons  $c_1, \dots, c_m$  les éléments  $k$  de  $\{0, \dots, p-1\}$  tel que  $A(k) \equiv 0 \pmod{p}$ . Appliquons le lemme à l'entier  $c_m$ ; il existe un polynôme  $B$  à coefficients entiers, de degré  $d-1$  et de coefficient dominant 1 tel que  $A(x) = A(c) + (x-c)B(x)$ . Les entiers  $c_1, \dots, c_{m-1}$  sont racines de  $B$  modulo  $p$  et appartiennent à  $\{0, \dots, p-1\}$ ; par récurrence,  $m-1 \leq d-1$ . On a donc  $m \leq d$ .

### §6. Être ou ne pas être un carré modulo $p$ ...

Soit  $p$  un nombre premier, supposons  $p \geq 3$  de sorte que  $p-1$  est pair.

Soit  $s$  l'application de  $\{1, \dots, p-1\}$  dans lui-même telle que  $s(x)$  est le reste de la division euclidienne de  $x^2$  par  $p$ . On a ainsi  $s(x) \equiv x^2 \pmod{p}$ . Notons  $C$  l'image de  $s$ ; ce sont les entiers de  $\{1, \dots, p-1\}$  qui sont congrus modulo  $p$  au carré d'un nombre entier. Soit  $a \in C$ . L'équation  $s(x) = a$  a au moins une solution  $x$ . Elle a aussi la solution  $p-x$  car  $p-x \equiv -x \pmod{p}$ , donc  $(p-x)^2 \equiv x^2 \equiv a \pmod{p}$ . De plus,  $x \neq p-x$  car  $p$  est impair. Il en résulte que les deux solutions de l'équation polynomiale  $x^2 \equiv a \pmod{p}$  sont  $x$  et  $p-x$  modulo  $p$ . Autrement dit,  $a$  possède exactement deux antécédents par l'application  $s$ . D'après le principe des bergers, le cardinal de  $C$  est la moitié de celui de  $\{1, \dots, p-1\}$ , c'est-à-dire  $(p-1)/2$ . Il y a ainsi  $(p-1)/2$  éléments de  $\{1, \dots, p-1\}$  qui sont des carrés modulo  $p$ , et  $(p-1)/2$  qui ne le sont pas.

Soit  $x$  un entier qui n'est pas multiple de  $p$ . D'après le petit théorème de Fermat,  $x^{p-1} \equiv 1 \pmod{p}$ , si bien que  $a = x^{(p-1)/2}$  vérifie  $a^2 \equiv 1 \pmod{p}$ . Cette équation a deux solutions modulo  $p$ , 1 et  $-1$ ; elle n'en a pas d'autres d'après le théorème précédent (facile dans ce cas : si  $a^2 \equiv 1 \pmod{p}$ ,  $a^2 - 1 = (a-1)(a+1)$  est multiple de  $p$ , donc  $a-1$  ou  $a+1$  est multiple de  $p$ , ce qui entraîne  $a \equiv 1 \pmod{p}$  ou  $a \equiv -1 \pmod{p}$ ). Donc  $a \equiv \pm 1 \pmod{p}$ .

Supposons qu'il existe un nombre entier  $y$  tel que  $x \equiv y^2 \pmod{p}$ . Alors,  $x^{(p-1)/2} \equiv y^{p-1} \equiv 1 \pmod{p}$ . Ainsi, si  $x$  est un carré modulo  $p$ ,  $x^{(p-1)/2}$  est congru à 1 modulo  $p$ . Les éléments de  $C$  sont donc les solutions modulo  $p$  de l'équation polynomiale  $x^{(p-1)/2} \equiv 1 \pmod{p}$ . Ce sont les seules. On a ainsi démontré le résultat suivant :

**PROPOSITION.** — Soit  $p$  un nombre premier,  $p \neq 2$ , et soit  $a$  un entier qui n'est pas multiple de  $p$ . Si  $a$  est congru modulo  $p$  au carré d'un nombre entier, alors  $a^{(p-1)/2} \equiv 1 \pmod{p}$ . Dans le cas contraire,  $a^{(p-1)/2} \equiv -1 \pmod{p}$ .

Exemple : Pour que  $-1$  soit un carré modulo  $p$ , il faut et il suffit que  $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ . Or,  $(p-1)/2$  est pair si  $p \equiv 1 \pmod{4}$ , et est impair sinon. Par suite,  $(-1)^{(p-1)/2}$  vaut 1 lorsque  $p \equiv 1 \pmod{4}$ , et vaut  $-1$  sinon. Il en résulte que  $-1$  est un carré modulo  $p$  si et seulement si  $p$  est congru à 1 modulo 4.

*Exercices.* — 1) Soit  $a$  et  $b$  des entiers relatifs et soit  $p$  un nombre premier. On s'intéresse à l'équation  $x^2 + 2ax + b \equiv 0 \pmod{p}$ . On pose  $\delta = a^2 - b$ .

a) Remarquer que  $x^2 + 2ax + b = (x+a)^2 - \delta$ .

b) Montrer que l'équation  $x^2 + 2ax + b \equiv 0 \pmod{p}$  a 0, 1 ou 2 solutions modulo  $p$ , suivant que  $\delta$  n'est pas un carré modulo  $p$ ,  $\delta$  est multiple de  $p$ , ou  $\delta$  est un carré non nul modulo  $p$ .

Si  $u^2 \equiv \delta \pmod{p}$ , montrer que les racines de l'équation sont  $-a + u$  et  $-a - u$  modulo  $p$ .

2) Soit  $p$  un nombre premier distinct de 2 et 3. Soit  $S$  l'ensemble  $\{1, \dots, p-1\}$  et soit  $f: S \rightarrow S$  l'application telle que  $f(x)$  est le reste de la division euclidienne de  $x^3$  par  $p$ .

a) Combien l'équation  $x^3 \equiv 1 \pmod{p}$  a-t-elle de solutions modulo  $p$ ? (Discuter suivant que  $-3$  est un carré modulo  $p$  ou pas.)

b) Supposons que  $p-1$  ne soit pas multiple de 3. Montrer qu'il existe un entier  $n$  tel que  $3n \equiv 1 \pmod{p-1}$ . Montrer que pour tout  $x \in \mathbf{Z}$ ,  $y^3 \equiv x \pmod{p}$ , où  $y = x^n$ . Conclure que l'application  $f$  est bijective.

c) Supposons dans la suite de l'exercice que  $p-1$  est multiple de 3. Montrer qu'un élément  $y \in S$  appartient à l'image de  $f$  si et seulement si  $y^{(p-1)/3} \equiv 1 \pmod{p}$ .

d) En remarquant que pour  $y \in S$ ,  $f^{-1}(y)$  a au plus 3 éléments, montrer que le cardinal de  $S$  est égal à  $(p-1)/3$ .

e) Dédurre de l'exercice que  $-3$  est un carré modulo  $p$  si et seulement si  $p \equiv 1 \pmod{3}$ .

### §7. L'ordre multiplicatif modulo $p$

Soit  $n$  un entier au moins 2. Tout nombre entier  $x$  qui est premier à  $n$  possède un ordre multiplicatif modulo  $n$  : c'est le plus petit entier  $k \geq 1$  tel que  $x^k \equiv 1 \pmod{n}$ . Ce paragraphe a pour objet de préciser quelles valeurs de  $k$  sont possibles. On a déjà démontré que cet entier divise  $\varphi(n)$ .

LEMME. — a) Soit  $x$  un nombre entier premier à  $n$  et soit  $a$  son ordre multiplicatif modulo  $n$ . Tout diviseur de  $a$  est l'ordre multiplicatif d'un nombre entier premier à  $n$  ; précisément, si  $a = de$ , alors  $d$  est l'ordre multiplicatif modulo  $n$  de  $x^e$ .

b) Soit  $x$  et  $y$  des entiers premiers à  $n$  respectivement d'ordres multiplicatifs  $a$  et  $b$  modulo  $n$ . Si  $a$  et  $b$  sont premiers entre eux, alors  $xy$  est premier à  $n$  et son ordre multiplicatif modulo  $n$  est égal à  $ab$ .

c) Il existe un nombre entier relatif  $x$  premier à  $n$  tel que pour tout entier relatif  $y$  premier à  $n$ , l'ordre multiplicatif modulo  $n$  de  $y$  divise celui de  $x$ .

Démontrons d'abord a). On a  $(x^e)^d \equiv x^{de} \equiv 1 \pmod{n}$  ; en outre, pour tout entier  $k$  tel que  $1 \leq k < d$ ,  $(x^e)^k = x^{ke}$ , donc  $(x^e)^k \not\equiv 1 \pmod{n}$  puisque  $1 \leq ke < a$ . L'ordre multiplicatif de  $x^e$  est donc égal à  $d$ .

Démontrons b). Soit  $d$  un entier tel que  $(xy)^d \equiv 1 \pmod{n}$ . On a donc  $(xy)^{ad} \equiv 1 \pmod{n}$ , d'où  $y^{ad} \equiv 1 \pmod{n}$  puisque  $x^{ad} \equiv (x^a)^d \equiv 1 \pmod{n}$ . Par suite,  $b$  divise  $ad$ . D'après le théorème de Gauss,  $b$  divise  $d$ , car  $a$  et  $b$  sont premiers entre eux. De même,  $a$  divise  $d$ . Comme  $a$  et  $b$  sont premiers entre eux, le théorème de Gauss entraîne à nouveau que  $ab$  divise  $d$ . Inversement,  $(xy)^{ab} \equiv (x^a)^b (y^b)^a \equiv 1 \pmod{n}$ . Par suite, l'ordre multiplicatif de  $xy$  modulo  $n$  est égal à  $ab$ .

Avant de démontrer c) prouvons que si  $a$  et  $b$  sont les ordres multiplicatifs modulo  $n$  de deux nombres entiers  $x$  et  $y$ , il existe un nombre entier relatif  $z$ , premier à  $n$ , dont l'ordre multiplicatif est égal à  $\text{ppcm}(a, b)$ . Pour cela, écrivons la décomposition en facteurs premiers de  $a$  et  $b$  sous la forme  $a = \prod p_i^{\alpha_i}$  et  $b = \prod p_i^{\beta_i}$ . On a donc

$\text{ppcm}(a, b) = \prod p_i^{\max(\alpha_i, \beta_i)}$ . Posons  $\alpha'_i = \alpha_i$  si  $\alpha_i \geq \beta_i$ , et  $\alpha'_i = 0$  sinon. Posons aussi  $\beta'_i = 0$  si  $\alpha_i \geq \beta_i$  et  $\beta'_i = \beta_i$  sinon. Posons  $a' = \prod p_i^{\alpha'_i}$  et  $b' = \prod p_i^{\beta'_i}$ ; par construction,  $\text{ppcm}(a, b) = a'b'$  puisque  $\alpha'_i + \beta'_i = \max(\alpha_i, \beta_i)$  pour tout  $i$ . De plus,  $a'$  et  $b'$  n'ont aucun facteur commun.

D'après *a*),  $a'$  et  $b'$  sont les ordres multiplicatifs modulo  $n$  d'entiers  $x'$  et  $y'$ . Comme ils sont premiers entre eux,  $a'b' = \text{ppcm}(a, b)$  est l'ordre multiplicatif d'un entier relatif premier à  $n$ .

Démontrons enfin *c*). Si  $x \equiv y \pmod{n}$ , alors  $x$  et  $y$  ont même ordre multiplicatif modulo  $n$ . Il suffit donc de s'intéresser aux ordres multiplicatifs des entiers compris entre 1 et  $n$ . Notons ainsi  $x_1, \dots, x_{\varphi(n)}$  les entiers compris entre 1 et  $n$  qui sont premiers à  $n$ . Par récurrence, il existe un entier  $x$  dont l'ordre multiplicatif modulo  $n$  est le ppcm des ordres multiplicatifs modulo  $n$  des  $x_i$ . L'ordre multiplicatif modulo  $n$  de tout élément divise celui de  $x$ .

**THÉORÈME (Gauss).** — *Soit  $p$  un nombre premier. Il existe un élément  $\omega \in \{1, \dots, p-1\}$  dont l'ordre multiplicatif modulo  $p$  est égal à  $p-1$ . De plus, tout élément de  $\{1, \dots, p-1\}$  est congru à un unique élément de l'ensemble  $\{1, \omega, \omega^2, \dots, \omega^{p-2}\}$ .*

Soit  $\omega$  un entier qui n'est pas multiple de  $p$  et dont l'ordre multiplicatif modulo  $p$ , disons  $a$ , est maximal. D'après la partie *c*) du lemme, l'ordre multiplicatif de tout élément divise  $a$ . En particulier  $x^a \equiv 1 \pmod{p}$  pour tout entier  $x$  qui n'est pas multiple de  $p$ .

L'équation polynomiale en congruences  $x^a - 1 \equiv 0 \pmod{p}$  a au plus  $a$  solutions modulo  $p$ . Cela entraîne que  $a \geq p-1$ , d'où finalement l'égalité  $a = p-1$ . Il existe donc un élément  $\omega$  de  $\{1, \dots, p-1\}$  dont l'ordre multiplicatif est  $p-1$ .

Les éléments  $1, \omega, \dots, \omega^{p-2}$  sont alors non nuls, et distincts modulo  $p$ . En effet, si  $\omega^i \equiv \omega^j \pmod{p}$ , avec  $i < j$ , on en déduit  $\omega^i(\omega^{j-i} - 1) \equiv 0$ , d'où  $\omega^{j-i} \equiv 1 \pmod{p}$  (car  $\omega$  est premier à  $p$ ), ce qui contredit l'hypothèse que l'ordre multiplicatif de  $\omega$  est égal à  $p-1$ . Autrement dit, les restes de la division euclidienne des  $p-1$  éléments  $1, \omega, \dots, \omega^{p-2}$  par  $p$  épuisent l'ensemble  $\{1, \dots, p-1\}$ . Tout élément de  $\mathbf{Z}$  qui n'est pas multiple de  $p$  est donc congru modulo  $p$  à un unique élément de la forme  $\omega^i$ , avec  $0 \leq i \leq p-2$ .

Un tel élément  $\omega$  est appelé *générateur multiplicatif modulo  $p$* .

*Exercices.* — 1) a) Déterminer les générateurs multiplicatifs modulo  $p$ , lorsque  $p \leq 19$ .

b) Pour quelles valeurs de  $n$  telles que  $2 \leq n \leq 20$  existe-t-il un entier premier à  $n$  dont l'ordre multiplicatif est égal à  $\varphi(n)$  ?

2) Soit  $p$  un nombre premier. Soit  $a$  un entier qui est un générateur multiplicatif modulo  $p$ .

a) Montrer que l'ordre multiplicatif de  $a$  modulo  $p^2$  est égal à  $(p-1)$ , ou à  $p(p-1)$ .

b) Si  $a^{p-1} \not\equiv 1 \pmod{p^2}$ , montrer que  $a$  est un générateur multiplicatif modulo  $p^2$ , c'est-à-dire que son ordre multiplicatif de  $a$  modulo  $p^2$  est égal à  $p(p-1)$ .

c) Posons  $b = a + p$ . Montrer que  $b^{p-1} \equiv a^{p-1} - pa^{p-2} \pmod{p^2}$ . (Utiliser la formule du binôme de Newton.)

d) Si  $a^{p-1} \equiv 1 \pmod{p^2}$ , montrer que  $b$  est un générateur multiplicatif modulo  $p^2$ .

e) Application numérique : trouver un générateur multiplicatif modulo  $p^2$  pour  $p = 2, 3, 5$  ou  $7$ .

### §8. Appendice : l'anneau $\mathbf{Z}/n\mathbf{Z}$

Il s'agit de rendre les calculs de congruences modulo un entier  $m$  le plus automatique possible. Dans la discussion précédente, j'ai choisi de ne parler que d'entiers relatifs et d'ajouter systématiquement l'expression « modulo  $n$  » après le symbole d'égalité.

Lorsqu'on raisonne avec des congruences modulo un entier  $n$  fixé, on peut à tout instant remplacer un entier  $x$  par son reste  $r$  dans la division euclidienne par  $n$ . Ainsi, tant qu'il ne s'agit que de congruences modulo  $n$ , les entiers  $x$  et  $r$  sont indiscernables et l'on peut utiliser indifféremment l'un ou l'autre, voire tout autre entier qui leur serait congru modulo  $n$ .

On voit qu'on gagnerait en concision à définir un objet dont les éléments représenteront les différentes classes de congruences modulo  $n$  et qui sera muni d'une addition et d'une multiplication. Cet objet existe, c'est *l'ensemble des classes d'équivalences pour la relation de congruence modulo  $n$* !

La classe d'équivalence d'un entier  $a$ , notée  $\text{cl}(a)$  ou  $\bar{a}$ , est l'ensemble des entiers  $x$  qui sont congrus à  $a$  modulo  $n$ , c'est donc l'ensemble des entiers de la forme  $a + kn$ , avec  $k \in \mathbf{Z}$ . Cet ensemble, que l'on note en général  $\mathbf{Z}/n\mathbf{Z}$ , a donc  $n$  éléments : la classe de 0, de 1, etc. jusqu'à la classe de  $n - 1$ .

On a déjà remarqué que l'addition est compatible à la relation d'équivalence modulo  $n$  : si  $a \equiv a' \pmod{n}$  et  $b \equiv b' \pmod{n}$ , alors  $a + b \equiv a' + b' \pmod{n}$ . Cela permet de définir une addition sur l'ensemble  $\mathbf{Z}/n\mathbf{Z}$  de la façon suivante : si  $x$  et  $y$  sont des éléments de  $\mathbf{Z}/n\mathbf{Z}$ , choisissons des représentants  $a$  et  $b$  de ces classes, de sorte que  $a$  et  $b$  sont des nombres entiers vérifiant  $x = \text{cl}(a)$  et  $y = \text{cl}(b)$ . La compatibilité de l'addition à la congruence entraîne que la classe de  $a + b$  ne dépend pas du choix que l'on a fait pour  $a$  et  $b$  et l'on pose  $x + y = \text{cl}(a + b)$ . Autrement dit, l'addition dans  $\mathbf{Z}/n\mathbf{Z}$  est donnée par la formule  $\text{cl}(a) + \text{cl}(b) = \text{cl}(a + b)$ .

Il y a un élément neutre, noté 0, en fait la classe de 0, tel que  $x + 0 = 0 + x = x$  pour toute classe  $x$  : si  $x = \text{cl}(a)$ ,  $x + 0 = \text{cl}(a) + \text{cl}(0) = \text{cl}(a + 0) = \text{cl}(a)$ . En outre, toute classe a un opposé : si  $a \in \mathbf{Z}$ , l'opposée de  $\text{cl}(a)$  est la classe de  $-a$ .

On définit de la même façon une multiplication sur les classes, de sorte que  $\text{cl}(x)\text{cl}(y) = \text{cl}(xy)$ . On note encore 1 la classe de 1 ; elle vérifie  $1x = x1 = x$  pour toute classe  $x$ , traduction de ce que  $\text{cl}(1)\text{cl}(a) = \text{cl}(1a) = \text{cl}(a)$  pour tout entier  $a$ .

L'ensemble  $\mathbf{Z}/n\mathbf{Z}$  ainsi défini, avec son addition et sa multiplication, est donc un anneau commutatif unitaire.

L'intérêt d'introduire  $\mathbf{Z}/n\mathbf{Z}$ , c'est que le calcul des classes permet de s'affranchir définitivement du choix des représentants : on utilise souvent les représentants compris entre 0 et  $n - 1$  mais on pourrait choisir les entiers compris entre  $-n/2$  (exclu si  $n$  est pair) et  $n/2$  (inclus si  $n$  est pair). Pire, à une ligne du calcul, le choix  $n - 1$  du représentant de la classe de  $-1$  pourrait être préférable, sans qu'il cesse d'être souhaitable, de

vouloir revenir au représentant  $-1$  à la ligne suivante. Avec le calcul des classes, cette question devient sans objet : dans  $\mathbf{Z}/n\mathbf{Z}$ ,  $n$  (entendre «  $\bar{n}$  », c'est-à-dire sa classe) est égal à  $0$ , donc  $n-1$  et  $-1$  sont tout simplement égaux !

Les propriétés algébriques de  $\mathbf{Z}/n\mathbf{Z}$  dépendent profondément de l'entier  $n$ .

Supposons que  $n$  ne soit pas un nombre premier et soit  $a$  et  $b$  des entiers tels que  $ab = n$ , avec  $1 < a, b < n$ . Alors,  $\text{cl}(a)$  et  $\text{cl}(b)$  sont distincts de la classe de  $0$  (car  $a$  et  $b$  ne sont pas multiples de  $n$ ). Toutefois, leur produit, étant égal à  $\text{cl}(ab) = \text{cl}(n)$ , est égal à la classe de  $0$ . Cela démontre que le produit de deux classes non nulles peut être nulle si  $n$  n'est pas un nombre premier.

On peut aller plus loin. Dire que  $\text{cl}(a)\text{cl}(b) = \text{cl}(0)$  signifie que  $ab$  est multiple de  $n$ . Si  $a$  est premier avec  $n$ , on a démontré qu'alors  $b$  est multiple de  $n$ , c'est-à-dire  $\text{cl}(b) = 0$ . Si, de plus,  $u$  est un inverse de  $a$  modulo  $n$ , de sorte que  $au \equiv 1 \pmod{n}$ , on a  $\text{cl}(a)\text{cl}(u) = \text{cl}(1)$  : la classe de  $u$  se comporte exactement comme un *inverse* de celle de  $a$  ; en multipliant par  $\text{cl}(u)$ , on divise en fait par  $\text{cl}(a)$  !

Lorsque  $n$  est un nombre premier  $p$ , dire que  $a$  est premier à  $p$  équivaut à dire que  $a$  n'est pas multiple de  $p$ , c'est-à-dire  $\text{cl}(a) \neq \text{cl}(0)$ . On dispose donc dans l'anneau  $\mathbf{Z}/p\mathbf{Z}$  d'une division par toute classe non nulle ! On dit que c'est un *corps* commutatif.

## CHAPITRE 6

# NOMBRES DÉCIMAUX, NOMBRES RATIONNELS

---

Il s'agit maintenant d'expliquer le calcul des « nombres à virgule », puis celui des fractions. Le but de ce paragraphe est de montrer comment ces objets familiers sont justiciables d'une *construction* mathématique précise, une fois admise la construction des entiers naturels.

### §1. Nombres rationnels

On avait déjà expliqué comment *définir* les entiers relatifs à partir des entiers naturels. La méthode consistait à introduire un symbole  $[a, b]$  pour la soustraction  $a - b$ , et en identifiant les soustractions dont les résultats doivent être égaux. Le calcul des fractions permettant de définir les nombres rationnels se construit de la même façon. Dans  $\mathbf{Z}$ , toutes les divisions ne sont pas exactes et l'on souhaite définir un objet mathématique, le *corps des nombres rationnels*, contenant  $\mathbf{Z}$ , muni d'une addition, d'une soustraction, d'une multiplication et d'une division par tout élément non nul.

Soit ainsi  $F$  l'ensemble des couples  $(a, b)$  d'éléments de  $\mathbf{Z}$ , avec  $b \neq 0$ . Le couple  $(a, b)$  est censé représenter la fraction  $a/b$ ; on dit ainsi que deux couples  $(a, b)$  et  $(a', b')$  sont équivalents si l'on a la relation (produit en croix)  $ab' = a'b$  dans  $\mathbf{Z}$ . C'est une relation d'équivalence. On note  $[a, b]$  la classe d'équivalence de  $(a, b)$ . Soit  $\mathbf{Q}$  l'ensemble des classes d'équivalence.

On définit l'addition et la multiplication dans  $\mathbf{Q}$  par les formules

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b] \times [c, d] = [ac, bd],$$

reflets des relations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Il est alors aisé quoique fastidieux de montrer que l'addition et la multiplication sont bien définies (les formules données ne dépendent pas des couples  $(a, b)$ ,  $(c, d)$  choisis dans les classes  $[a, b]$ ,  $[c, d]$ ), commutatives, associatives, que  $(0, 1)$  est un élément neutre pour  $+$ ,  $(1, 1)$  est un élément neutre pour  $\times$ , et que la multiplication est distributive par rapport à l'addition. Tout élément  $[a, b]$  de  $\mathbf{Q}$  a un opposé (pour  $+$ ), à savoir  $[-a, b]$ , et, s'il est non nul, un inverse (pour  $\times$ ),  $[b, a]$ . En outre l'application de  $\mathbf{Z}$  dans  $\mathbf{Q}$  donnée par  $n \mapsto [n, 1]$  est injective et est compatible aux lois  $+$  et  $\times$ ; on notera donc  $n$

la classe  $[n, 1]$ . Si  $a$  et  $b$  sont des entiers, avec  $b \neq 0$ , on a ainsi  $[a, b] = a/b$ . Mission réussie!

Un nombre rationnel non nul possède une décomposition en facteurs premiers dont les exposants sont des entiers relatifs. Soit  $x$  un nombre rationnel non nul. Si  $x = a/b = c/d$ , on a  $v_p(a) - v_p(b) = v_p(c) - v_p(d)$  pour tout nombre premier  $p$ . On peut ainsi poser

$$v_p(x) = v_p(a) - v_p(b)$$

et appeler cet entier relatif la valuation  $p$ -adique de  $x$ .

Les entiers sont les nombres rationnels dont toutes les valuations  $p$ -adiques sont positives ou nulles. Pour  $x, y \neq 0$ , on a  $v_p(x + y) \geq \max(v_p(x), v_p(y))$  (si  $x + y \neq 0$ ), avec égalité lorsque  $v_p(x) \neq v_p(y)$ ,  $v_p(xy) = v_p(x) + v_p(y)$ , et  $v_p(1/x) = -v_p(x)$ .

Soit  $x$  un nombre rationnel. Parmi les fractions  $a/b$  égales à  $x$ , il en est une privilégiée, à savoir celle telle que  $a$  et  $b$  soient premiers entre eux et  $b > 0$ . On dira qu'une telle fraction est irréductible.

## §2. Le développement décimal d'un nombre rationnel

Soit  $b \geq 2$  un entier, base de nos développements « décimaux ». L'idée du développement en base  $b$  des rationnels est de noter  $\underline{0,1}_b$  le nombre rationnel  $1/b$ . Plus généralement, on note

$$\underline{a_n a_{n-1} \dots a_0, a_{-1} \dots a_{-k}}_b = b^{-k} \underline{a_n \dots a_0 a_{-1} \dots a_{-k}}_b.$$

Dans l'autre sens, considérons une fraction irréductible  $m/n$  et supposons qu'il existe un entier  $d \geq 1$  tel que  $nd$  soit une puissance de  $b$ . Si  $b = 10$ , on dit que  $m/n$  est un nombre décimal, et, faute de mieux<sup>(1)</sup>, on garde cette terminologie dans le cas général. Par exemple,  $1/5$  et  $22/100$  sont des nombres décimaux (en base 10), mais pas  $22/7$ . Le calcul de fractions dont disposaient les égyptiens revient en gros à celui des nombres décimaux en base 60.

Dire que le nombre rationnel  $x$  a un développement décimal (en base  $b$ ) avec  $k$  chiffres après la virgule revient donc à dire que  $b^k x$  est entier.

Pour introduire le développement illimité d'un nombre rationnel, revenons sur la méthode concrète qui conduit à la détermination du développement décimal d'un tel nombre, quand il existe. Soit donc  $x = A/B$  un nombre rationnel. On procède en effectuant d'abord la division euclidienne de  $A$  par  $B$ ; on obtient un quotient  $q$  et un reste  $r$  qui vérifient  $A = Bq + r$ , avec  $0 \leq r < B$ . Par conséquent,  $x = \frac{A}{B} = q + \frac{r}{B}$ , d'où  $q \leq x < q + 1$ ; autrement dit,  $q$  est le plus grand entier inférieur ou égal à  $x$ . On dit que c'est la *partie entière* de  $x$ . On écrit alors une virgule après le quotient  $q$ , on abaisse un zéro après le reste  $r$ , et on recommence. On effectue donc la division euclidienne de  $br$  par  $B$ ; comme  $r < B$ ,  $br < bB$  et le quotient obtenu  $q_1$  vérifie  $0 \leq q_1 < b$ . Si  $r_1$  est le reste, on a  $br = Bq_1 + r_1$ , d'où  $\frac{r}{B} = q_1 b^{-1} + \frac{r_1}{B} b^{-1}$  et  $x = q + q_1 b^{-1} + \frac{r_1}{B} b^{-1}$ . Le procédé peut se

<sup>(1)</sup> nombre  $b$ -cimal, bécimal,  $b$ -mal, etc.

poursuivre, on obtient des nombres entiers  $q_1, \dots, q_n$  tels que  $0 \leq q_i < b$ , ainsi qu'un reste  $r_n$  tels que

$$x = q + q_1 b^{-1} + q_2 b^{-2} + \dots + q_n b^{-n} + \frac{r_n}{B} b^{-n}.$$

Dans cette écriture,  $q + q_1 b^{-1} + \dots + q_n b^{-n}$  est un nombre décimal (en base  $b$ ) et  $\varepsilon_n = r_n / B b^{-n}$  est un nombre rationnel tel que  $0 \leq \varepsilon_n < b^{-n}$ .

Nous avons ainsi démontré la première partie de la proposition suivante :

**PROPOSITION.** — *Pour tout nombre rationnel  $x$  et tout entier  $n \geq 0$ , il existe un unique couple  $(\tilde{x}, \varepsilon)$  formé d'un nombre décimal en base  $b$ ,  $\tilde{x}$ , qui possède  $n$  chiffres après la virgule, et un nombre rationnel  $\varepsilon$  tel que  $0 \leq \varepsilon < b^{-n}$ .*

On peut démontrer directement l'existence d'un tel couple  $(\tilde{x}, \varepsilon)$  en considérant la partie entière  $y$  de  $b^n x$ . C'est un entier tel que  $y \leq b^n x < y + 1$ . Posons alors  $\tilde{x} = y / b^n$ ; c'est un nombre décimal avec  $b$  chiffres après la virgule tel que  $\tilde{x} \leq x < \tilde{x} + b^{-n}$ . Par suite,  $\varepsilon = x - \tilde{x}$  vérifie l'inégalité  $0 \leq \varepsilon < b^{-n}$ . Pour l'unicité, on remarque que si  $(\tilde{x}, \varepsilon)$  vérifie les conditions de l'énoncé, alors  $b^n \tilde{x}$  est un entier tel que  $b^n \tilde{x} \leq b^n x < b^n \tilde{x} + 1$ . Autrement dit,  $b^n \tilde{x}$  est le plus grand entier inférieur ou égal à  $b^n x$ , puis  $\varepsilon = x - \tilde{x}$ .

On dira que  $\tilde{x}$  est une approximation par défaut à  $b^{-n}$  près de  $x$ .

L'assertion d'unicité montre que cette approximation par défaut est fournie par le procédé par récurrence expliqué avant l'énoncé de la proposition. En particulier, le processus s'arrête si  $x$  est un nombre décimal en base  $b$ , fait nullement évident *a priori*.

### §3. Les nombres réels

La notion de nombre réel est extrêmement ancienne, même si la formalisation mathématique que je vais présenter maintenant est plus récente. De manière un peu imagée — et c'était, incidemment, le point de vue des mathématiciens de l'école de Pythagore — les nombres rationnels ne permettent que d'exprimer les longueurs multiples d'une unité fixée, ou que l'on peut au besoin diviser en parties égales. Mais la longueur de la diagonale d'un carré de côté unité ne rentre pas dans ce cadre ! En effet, si l'on croit le théorème de Pythagore, cette longueur  $d$  vérifie  $d^2 = 1^2 + 1^2$ , soit  $d^2 = 2$ . Écrivons, si possible,  $d$  sous forme d'une fraction irréductible  $d = a/b$ , où  $a$  et  $b$  sont des entiers non nuls et premiers entre eux. On a alors  $a^2 = 2b^2$ . Par suite, 2 divise  $a^2$ , donc  $a$  est pair; écrivons  $a = 2a'$ . On a alors  $4(a')^2 = 2b^2$ , d'où  $2(a')^2 = b^2$ . Nécessairement,  $b$  est pair. Alors,  $a$  et  $b$  sont tous deux multiples de 2, ce qui contredit l'hypothèse qu'ils étaient premiers entre eux. Donc la diagonale d'un carré de côté l'unité n'existe pas !

**PROPOSITION 3.1.** — *Il n'existe pas de nombre rationnel dont le carré soit égal à 2.*

On sait pourtant qu'un tel nombre existe, au sens où l'on sait construire des approximations décimales de plus en plus précises d'un nombre « réel », disons  $x_n$ , à  $10^{-n}$  près, telles que  $x_n^2 \leq 2 < (x_n + 10^{-n})^2$ . Il semble donc qu'il suffise de donner un sens à un développement décimal illimité, même s'il ne provient pas d'un nombre rationnel. Que

ce soit bien le cas nécessite un raisonnement mathématique élaboré et trop long pour qu'il vaille la peine de le développer ici.

Qu'il faille être prudent est certain; que pourrait par exemple être le nombre réel  $\overline{0,9999\dots}$ ? Par construction, il est inférieur à 1, mais si on lui ajoute (par les règles de calcul de l'addition extrapolées) un nombre aussi petit soit-il, disons  $10^{-n}$ , on obtient le développement décimal  $\overline{1,0\dots0999\dots}$ , avec  $n$  chiffres 0 avant le premier 9, donc un nombre supérieur à 1. Si l'on désire que 0 soit le seul nombre réel qui soit plus petit que toute borne fixée à l'avance, on a donc  $\overline{0,999\dots} = 1$ .

Contentons-nous de dire qu'un nombre réel est donné par un développement décimal illimité « propre », ce qui signifie qu'on exclut les développements décimaux formés uniquement de 9 à partir d'un certain rang. L'addition et la multiplication sont définies comme d'habitude, en prenant garde aux retenues et en remplaçant d'éventuels développements impropres  $\overline{a_0, a_1 \dots a_n 9999\dots}$ , où  $a_n \neq 9$ , par le développement décimal  $\overline{0, a_1 \dots a_{n-1} (a_n + 1)}$ .

On obtient alors l'ensemble des nombres réels dont le lycée a permis de se forger une intuition. C'est un ensemble que l'on note  $\mathbf{R}$ , qui possède une addition, une soustraction, une multiplication et une division par tout élément non nul. (On dit que c'est un *corps*.)

On peut de plus démontrer que *toute suite croissante majorée converge*, résultat sur lequel le reste du cours d'analyse de Licence peut être fondé.

#### §4. Quelques classes de nombres

PROPOSITION. — *Un nombre réel est rationnel si et seulement si son développement décimal est périodique à partir d'un certain rang.*

Supposons d'abord que  $x$  soit un nombre réel dont le développement décimal à partir d'un certain rang est formé de la répétition d'un nombre à  $k$  chiffres  $a$ . On peut écrire  $x = d + 10^{-b}(a10^{-k} + (a10^{-k}) + (a10^{-2k} + \dots))$ , où  $d$  est un nombre décimal et  $b$  la position à partir de laquelle le développement décimal de  $x$  est périodique. On a alors

$$x = d + \frac{a}{10^k - 1} 10^{-b-k}.$$

C'est en particulier un nombre rationnel. Si on l'écrit sous forme d'une fraction irréductible, notons que le dénominateur va diviser  $(10^k - 1)10^{b+k}$ . Si  $q$  est le dénominateur auquel on ôte ses facteurs premiers 2 et 5,  $q$  divise  $10^k - 1$  et  $10^k \equiv 1 \pmod{q}$ . Par suite, l'entier  $k$  — la période — est multiple de l'ordre multiplicatif de 10 modulo  $q$ .

Inversement, écrivons  $x$  sous la forme d'une fraction  $2^u 5^v p/q$ , où  $p$  et  $q$  sont des nombres entiers entre eux et premiers avec 10 et où  $u$  et  $v$  sont des entiers relatifs. Soit  $k$  l'ordre multiplicatif de 10 modulo  $q$ . Cela entraîne que  $10^k \equiv 1 \pmod{q}$ , donc qu'il existe un entier  $a$  tel que  $10^k - 1 = aq$ ; comme  $k \geq 1$ ,  $a$  n'est pas nul. On peut alors écrire

$$x = 2^u 5^v \frac{ap}{aq} = 2^u 5^v \frac{ap}{10^k - 1}.$$

Soit  $n$  un entier tel que  $n + u \geq 0$  et  $n + v \geq 0$ ; alors,

$$10^n x = (2^{n+u} 5^{n+v} ap) \frac{1}{10^k - 1} = A \frac{1}{10^k - 1},$$

où  $A$  est un entier. Soit  $B$  le quotient de la division euclidienne de  $A$  par  $10^k - 1$  et  $C$  le reste. On a  $0 \leq C < 10^k - 1$  et

$$10^n x = B + \frac{C}{10^k - 1} = B + C10^{-k} + C10^{-2k} + \dots$$

possède un développement périodique à partir d'un certain rang. Il en est de même de  $x$ .

On a démontré au passage que la période du développement est égale à l'ordre multiplicatif de 10 modulo le dénominateur de  $x$  (dont on a ôté les facteurs 2 et 5).

Les nombres rationnels forment un ensemble dénombrable, de même que les nombres algébriques.

L'ensemble des nombres réels n'est pas dénombrable. Procédé diagonal de Cantor.

Donc l'ensemble des nombres transcendants n'est pas dénombrable (Cantor, 1874).

Théorème (Hermite, 1873 et Lindemann, 1882) :  $e \sim 2,71828\dots$  et  $\pi \sim 3,14159\dots$  sont transcendants.

## §5. Quelques résultats d'irrationalité

On a déjà démontré que  $\sqrt{2}$  est irrationnel.

PROPOSITION. — *Le nombre réel  $e$ , base des logarithmes népériens, est irrationnel.*

Rappelons que  $e$  est défini comme la limite des sommes

$$S_n = \sum_{k=0}^n \frac{1}{k!},$$

lorsque  $n$  tend vers l'infini. Raisonnons par l'absurde et supposons que  $e$  soit un nombre rationnel. Soit  $a$  et  $b$  des nombres entiers, supérieurs ou égaux à 1, tels que  $e = a/b$ . Posons  $N = b!(e - S_b)$ . On a

$$N = b! \left( e - \sum_{k=0}^b \frac{1}{k!} \right) = b! \frac{a}{b} - \sum_{k=0}^b \frac{b!}{k!} = (b-1)! a - \sum_{k=0}^b (k+1)(k+2)\dots b,$$

ce qui démontre que  $N$  est un entier. D'autre part,

$$N = \left( e - \sum_{k=0}^b \frac{1}{k!} \right) = \sum_{k=b+1}^{\infty} \frac{b!}{k!}$$

si bien que  $N > 0$  et que

$$N < \sum_{n=1}^{\infty} \frac{1}{(b+1)^n} = \frac{1}{b} < 1.$$

C'est absurde car aucun entier n'est compris strictement entre 0 et 1.

PROPOSITION (Lambert, 1761). — *Le nombre  $\pi$  est irrationnel.*

Supposons  $\pi = a/b$ , posons  $P_n(x) = x^n(a - bx)^n/n!$  et introduisons l'intégrale

$$I_n = \int_0^\pi P_n(x) \sin(\pi x) dx.$$

$P_n^{(k)}(0)$  et  $P_n^{(k)}(a/b)$  sont entiers pour tout  $k \geq 0$ .

Intégration par parties,

$$I_n = \sum_{k \geq 0} \left[ (-1)^k P_n^{(k)}(x) \sin\left(\pi x - (k+1)\frac{\pi}{2}\right) \right]_0^\pi$$

est entier.

Signe :  $I_n > 0$  et est majoré par  $C^n/n!$ . Donc  $I_n$  tend vers zéro. Absurde.

*Exercices.* — 1) Si  $p$  est un nombre premier, montrer que  $\sqrt{p}$  n'est pas un nombre rationnel.

2) Soit  $x$  un nombre réel, solution d'une équation polynomiale  $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ , où  $a_0, \dots, a_{n-1}$  sont des nombres entiers. Si  $x$  n'est pas un entier, alors  $x$  est irrationnel.

## §6. Un autre théorème de Fermat

THÉORÈME. — *Pour tout nombre premier  $p$  tel que  $p \equiv 1 \pmod{4}$ , il existe des entiers  $u$  et  $v$  tels que  $p = u^2 + v^2$ .*

Partons de la congruence du théorème de Wilson,  $(p-1)! \equiv -1 \pmod{p}$ . Elle se démontre en regroupant les termes 2 par 2, chacun avec son inverse modulo  $p$ , autrement dit, l'entier  $a$  avec l'unique entier  $b$  compris entre 1 et  $p-1$  tel que  $ab \equiv 1 \pmod{p}$ . Dire que  $a = b$  signifie  $a^2 \equiv 1 \pmod{p}$ , donc  $(a-1)(a+1) \equiv 1 \pmod{p}$ , d'où  $a = \pm 1$ . Ainsi, 1 et  $-1$  restent seuls. Alors,

$$(p-1)! \equiv (a_1 b_1)(a_2 b_2) \dots (a_{(p-3)/2} b_{(p-3)/2})(1)(-1) \equiv -1 \pmod{p}.$$

Dans cette congruence, regroupons de nouveau les termes 2 par 2, mais différemment : 1 avec  $p-1$ , 2 avec  $p-2$  et  $q$  avec  $p-q$ , où  $q = (p-1)/2$  est l'entier tel que  $p = 2q+1$ . Le premier facteur est congru à  $-1$  modulo  $p$ , le second à  $-2^2$ , etc. jusqu'au  $q$ -ième facteur  $q(p-q)$  qui est congru à  $-q^2$  modulo  $p$ . Par suite,

$$-1 \equiv (p-1)! \equiv (-1^2) \dots (-q^2) \equiv (-1)^q (q!)^2 \pmod{p}.$$

Comme  $p \equiv 1 \pmod{4}$ ,  $q$  est pair et  $(-1)^q = 1$ . L'entier  $a = q!$  vérifie alors  $a^2 \equiv -1 \pmod{p}$ . Autrement dit,  $p$  divise  $a^2 + 1$ .

Lorsque  $x$  et  $y$  varient parmi les entiers compris entre 0 et  $\sqrt{p}$ , il y a  $n = \lfloor \sqrt{p} \rfloor + 1$  choix pour  $x$  et  $y$ , donc  $n^2$  expressions de la forme  $ax + y$ . Or,  $n > \sqrt{p}$  par définition de la partie entière, donc  $n^2 > p$ . Cela entraîne qu'il existe deux couples  $(x, y)$  et  $(x', y')$  distincts tels que  $ax + y \equiv ax' + y' \pmod{p}$ . Posons  $u = x - x'$  et  $v = y - y'$ . Ce sont des entiers tels que  $|u| \leq \sqrt{p}$ ,  $|v| \leq \sqrt{p}$  et  $au + v$  est multiple de  $p$ . Si  $u$  était nul,  $v$  serait multiple de  $p$ ; comme  $\sqrt{p} < p$ ,  $v$  serait nul, ce qui contredit l'hypothèse que les couples  $(x, y)$  et  $(x', y')$  sont distincts. Donc  $u \neq 0$  et, de même,  $v \neq 0$ .

Alors la congruence  $u^2 + v^2 \equiv u^2 + a^2 u^2 \equiv u^2(1 + a^2) \pmod{p}$  entraîne que  $u^2 + v^2$  est multiple de  $p$ . L'inégalité  $0 < u^2 + v^2 < 2p$  implique que l'on a  $u^2 + v^2 = p$ . Cela conclut la démonstration du théorème de Fermat.

Par des techniques analogues (mais avec des matrices  $2 \times 2$ ), Lagrange a pu démontrer le résultat suivant : *Tout entier est somme de quatre carrés.*