NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS

Cours à l'Université de Rennes 1 (2004–2005)

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 15 décembre 2004

TABLE DES MATIÈRES

§1. Nombres entiers et principe de récurrence

A. Un peu d'histoire

Leopold Kronecker, un mathématicien allemand du XIX^{e} siècle a dit un jour : « Dieu a inventé les nombres entiers, le reste est l'œuvre de l'homme ». 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^{e} 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^{e} 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^{e} 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 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 débuter l'ensemble des entiers à 1).

a) zéro (0) est un entier ;
b) tout entier a un successeur ;
c) tout entier autre que zéro est le successeur d'un 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 $n \geqslant 1$ 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 $\mathscr{P}(n)$ 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 $\mathscr{P}(n)$ soit vérifié, on peut démontrer le résultat voulu de la façon suivante :

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

Le principe de récurrence entraîne que la propriété $\mathscr{P}$ 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$^{\text{e}}$ génération, vos « successeurs » n'en seront toujours pas venu à bout ! Pascal (XVII$^{\text{e}}$ 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 y a une variante importante du principe de récurrence qui s'énonce comme suit : *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 $n \geqslant a$. Pour l'établir, nous allons démontrer la propriété $\mathscr{P}(n)$ suivante : si A est une partie de $\mathbf{N}$ tel que $n \in A$, alors A possède un plus petit élément.

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

Supposons que $\mathscr{P}(n)$ soit vraie et démontrons $\mathscr{P}(n+1)$. Soit A une partie de $\mathbf{N}$ tel que $n+1 \in A$. 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 $a \leqslant n$. Posons $B = A \cup \{n\}$. On a $n \in B$; par récurrence, B admet un plus petit élément b. Cet élément est nécessairement inférieur ou égal à a car $a \in A$ et $A \subset B$, et inférieur ou égal à n, car $n \in B$. Si $b = n$, alors $n \leqslant a \leqslant n$, d'où $n = a$, ce qui montre que $b \in A$; sinon, $b < n$ et $b \in A$ aussi. Alors, pour tout élément m de A, on a $b \leqslant m$, car $m \in B$. Cela montre que A possède un plus petit élément et achève la démonstration par récurrence.

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.

Il reste encore une tâche au mathématicien consciencieux : *démontrer* qu'il « existe » un ensemble avec ces propriétés : les entiers de M. Tout le Monde les vérifient effectivement, mais ils ne forment pas un ensemble assez bien défini pour le mathématicien. 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.

B. 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 τ_{a} le taux annuel et τ_{m} le taux mensuel. En gros, $\tau_{\mathrm{a}} = 4{,}5/100 = 0{,}045$. Si le capital dû au 1^{er} janvier est C, les intérêts accumulés en un an seront de $\tau_{\mathrm{a}} \times C$, d'où un capital dû au 31 décembre de $(1+\tau_{\mathrm{a}})C$. Calculons mensuellement. Au 1^{er} février, les intérêts accumulés s'élèvent à $\tau_{\mathrm{m}}C$, d'où un capital dû de $(1+\tau_{\mathrm{m}})C$. Un mois plus tard, le capital dû est multiplié par $(1+\tau_{\mathrm{m}})$, donc il vaut $(1+\tau_{\mathrm{m}})^2C$, et finalement, au bout d'un an, le capital dû est de $(1+\tau_{\mathrm{m}})^{12}C$. (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

$$1+\tau_{\mathrm{a}} = (1+\tau_{\mathrm{m}})^{12}.$$

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

$$\tau_{\mathrm{a}} = 12\tau_{\mathrm{m}}.$$

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

$$(1+\tau_{\mathrm{m}})^{12} > 1 + 12\tau_{\mathrm{m}}.$$

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 $n \geqslant 2$ 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 $\geqslant 1$ et x un réel dans $[0,1]$, montrer l'inégalité

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

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

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

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

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

5) 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 ?

6) a) Montrer par récurrence sur n les formules

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

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

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

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

7) 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 $n \geqslant 1$, on a

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

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

9) a) Si x et y sont deux réels positifs, montrer que $\sqrt{xy} \leqslant (x+y)/2$.

b) Montrer par récurrence sur n que si $x_1,\dots,x_{2^n}$ sont des réels positifs,

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

c) Soit $N \geqslant 2$ et soit $x_1,\dots,x_N$ des réels. Démontrer que

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

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

10) 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 8×8 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…)

11*) 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 ?

12) 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 !

13) 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.

C. 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.

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

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

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

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

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

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

Par récurrence, la propriété $\mathscr{P}$ est vraie pour tout entier.

Il faudrait maintenant démontrer l'associativité de l'addition, c'est-à-dire que si m, n, p sont des entiers, on a $(m+n)+p=m+(n+p)$.

Pour construire la multiplication, on utilise le fait que pour multiplier m par n, on doit effectuer l'addition $n+n+\cdots+n$, 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.

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

D. 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 $u_n=a^nu_0$ pour tout entier n.

Revenons au problème des prêts bancaires. La question, connaissant le taux mensuel τ_{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

$$C_{n+1} = C_n + \tau_{\mathrm{m}} C_n - M = (1+\tau_{\mathrm{m}})C_n - M.$$

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

$$C_{n+1} - A = (1+\tau_{\mathrm{m}})(C_n - A)$$

En identifiant les deux relations, on obtient

$$A\tau_{\mathrm{m}} = M.$$

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

$$C_n - A = (1+\tau_{\mathrm{m}})^n (C_0 - A),$$

d'où la formule

$$\boxed{C_n = (1+\tau_{\mathrm{m}})^n C_0 - \frac{(1+\tau_{\mathrm{m}})^n - 1}{\tau_{\mathrm{m}}} M.}$$

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 $0 \leqslant x < 1$. 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 $U_n = u_0 + \cdots + u_n = \sum_{k=0}^{n} u_k$. Montrer que $U_n = (n+1)(u_0 + \frac{1}{2}an)$.

2) On considère une suite géométrique (v_n) de premier terme u_0 et de raison a et on pose encore $U_n = u_0 + \cdots + u_n$. 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 dm^3 de riz, chaque grain faisant 1 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 $n \geqslant 2$. Calculer $u_1 + \cdots + u_n$ 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 $n \geqslant 0$.

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

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 $n \geqslant 0$, $u_{n+1} = u_n/(1 + u_n)$.

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) 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 τ_{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.)

§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 $0! = 0$, $1! = 1$, $2! = 1 \times 2 = 2$, $3! = 1 \times 2 \times 3 = 6$, etc. Plus généralement,

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

Je rappelle aussi que $n!$ se prononce *factorielle n*.

A. 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.

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. L'ensemble vide, noté $\varnothing$ ou $\{\}$, n'a pas d'élément. On écrit $B \subset A$ et on prononce « A est inclus dans B » pour dire que tout élément de B appartient à A ; on dit aussi que B est une partie de A. On a donc $A \subset A$ (tout élément de A appartient à A) et $\varnothing \subset A$. 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.

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.

2.1. 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 $f : A \to B$, $a \mapsto f(a)$. 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 Id_A.

Soit $f : A \to B$ et $g : B \to C$ des applications. On définit l'application $g \circ f : A \to C$ 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 A' 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 2.2. — *Soit $f : A \to B$ 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 $f : A \to B$ 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 $f : \mathbf{N} \to \mathbf{N}$, $n \mapsto n^3 + n$ 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 $g : \mathbf{R} \to \mathbf{R}$, $x \mapsto x^2$ 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 2.3. — *On dit qu'une application $f : A \to B$ est surjective si tout élément de B a (au moins) un antécédent. Cela revient à dire que $f(A) = B$.*

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

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

DÉFINITION 2.4. — *On dit qu'une application $f : A \to B$ 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 $f \circ f^{-1} = \mathrm{Id}_B$: pour tout $b \in B$, $f^{-1}(b)$ est un antécédent de b par f, donc $f(f^{-1}(b)) = b$. On a $f^{-1} \circ f = \mathrm{Id}_A$: 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 $f : \mathbf{R}_+ \to \mathbf{R}_+$, $x \mapsto x^2$ 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 $g : \mathbf{R}_+ \to \mathbf{R}_+$ donnée par $x \mapsto \sqrt{x}$.

PROPOSITION. — *Soit $f : A \to B$ et $g : B \to C$ 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. □

2.5. Partitions. — Soit A un ensemble et soit n un entier $\geqslant 1$. On dit que des parties $A_1, \ldots, A_n$ forment une partition de A si tout élément de A appartient à un et un seul des A_i.

2.6. Ensembles finis, cardinal. — Si $n \geqslant 1$, notons F_n l'ensemble $\{1, \ldots, n\}$; on pose $F_0 = \varnothing$.

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

Démonstration. — Montrons ce lemme par récurrence sur n.

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

Supposons le résultat vrai pour n et soit $f : F_{n+1} \to F_m$ 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 $a + 1 \leqslant x \leqslant m$. Cette application est bijective, l'unique antécédent de x étant lui-même si $x < a$, $x + 1$ si $a \leqslant x \leqslant m - 1$, et a si $x = m$. L'application $h = g \circ f : F_{n+1} \to F_m$ 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. □

On dit qu'un ensemble A est fini s'il existe un entier $n \geqslant 0$ 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 $f : F_n \to A$ et $g : F_m \to A$ 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 $\operatorname{card} A$ 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.

B. 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.

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

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

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 $\operatorname{card} A \leqslant \operatorname{card} X$ *; 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 $\operatorname{card} X = \operatorname{card} A + \operatorname{card} B$, donc $\operatorname{card} A \leqslant \operatorname{card} B$. Si $\operatorname{card} A = \operatorname{card} X$, $\operatorname{card} B = 0$ donc $B = \varnothing$.

Variante. Soit $f : X \to Y$ une application entre ensembles fini. Si f est injective, $\operatorname{card} X \leqslant \operatorname{card} Y$; si f est surjective, $\operatorname{card} X \geqslant \operatorname{card} Y$. Dans les deux cas, l'égalité entraîne que f est bijective.

Cardinal du produit. Si X et Y sont deux ensembles finis, le cardinal de l'ensemble produit $X \times Y$ est égal à $\operatorname{card} X \times \operatorname{card} Y$. 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 $\operatorname{card} X$. Comme il y a $\operatorname{card} Y$ telles parties, on a $\operatorname{card}(X \times Y) = \operatorname{card} X \times \operatorname{card} Y$.

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 $\mathscr{F}(X, Y)$ des applications de X dans Y est égal à $(\operatorname{card} Y)^{\operatorname{card} X}$. 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 $X \to Y$ est déterminée par l'image de a. On a donc $\operatorname{card} \mathscr{F}(X, Y) = \operatorname{card} Y = (\operatorname{card} Y)^{\operatorname{card} X}$ 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 $(\operatorname{card} Y) \times (\operatorname{card} Y)^{n-1} = (\operatorname{card} Y)^n$ applications, d'où l'assertion voulue par récurrence sur n. Plus rigoureusement, définissons, si $y \in Y$, une partie $\mathscr{F}_y$ de $\mathscr{F}(X, Y)$ comme l'ensemble des $f : X \to Y$ tels que $f(a) = y$. Ces parties $\mathscr{F}_y$ forment une partition de $\mathscr{F}(X, Y)$; chacune est en bijection avec $\mathscr{F}(X', Y)$, donc de cardinal $(\operatorname{card} Y)^{\operatorname{card} X - 1}$. Comme il y a $\operatorname{card} Y$-parties, le cardinal de $\mathscr{F}(X, Y)$ vaut bien $(\operatorname{card} Y)^{\operatorname{card} X}$.

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$^{\text{e}}$ 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 $(A_i)_{1 \leqslant i \leqslant m}$ une partition de X. Si* $\operatorname{card} X > m$*, une des parties est de cardinal $\geqslant 2$.*

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

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

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 couché 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

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

Généraliser.

3) On considère n objets (non nécessairement distincts). Si a est un entier tel que $a \leqslant \sqrt{n-1}$, montrer que l'on peut trouver ou bien $a+1$ objets identiques, ou bien $a+1$ objets distincts.

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 touristes parlent 6 langues différentes mais leur guide constate que d'eux quelconques d'entre eux ne peuvent se parler que dans une seule de ces langues. Montrer qu'il existe un groupe de trois touristes qui peuvent communiquer entre eux dans une même langue.

C. Triangle de Pascal

Soit X un ensemble fini, de cardinal n.
Notons $\mathscr{P}(X)$ l'ensemble des parties de X.

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

Intuitivement. Supposons que $X = \{1, \dots, n\}$. Pour construire une partie de A, 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* χ_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 $2^{\operatorname{card} X}$.

Par récurrence. Soit a un élément fixé de X et posons $Y = X \setminus \{a\}$, de sorte que $\operatorname{card} Y = n-1$. 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 $\mathscr{P}_p(X)$ l'ensemble des parties de X dont le cardinal est exactement p. Si $p<0$ ou si $p>\operatorname{card} X$, on a évidemment $\mathscr{P}_p(X)=\varnothing$. Une seule partie de X est de cardinal nul (la partie vide), une seule partie de X est de cardinal $\operatorname{card} X$, X lui-même.

Si $n=\operatorname{card} X$, le cardinal de $\mathscr{P}_p(X)$ 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.

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,

$$\mathrm{C}_n^p=\frac{\mathrm{A}_n^p}{\mathrm{A}_p^p}.$$

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,

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

En particulier,

$$\mathrm{A}_p^p=p!$$

d'où l'on déduit

$$\boxed{\mathrm{C}_n^p=\frac{n!}{p!(n-p)!}.}$$

Soit X un ensemble de cardinal n et cherchons à évaluer le nombre de parties à p éléments de X. 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

$$\mathrm{C}_n^p=\mathrm{C}_{n-1}^{p-1}+\mathrm{C}_{n-1}^p.$$

Si on les dispose comme ceci (n est l'indice de ligne, p l'indice de colonne),

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

chaque coefficient est ainsi la somme du coefficient qui est au-dessus de lui et du coefficient qui est à sa gauche. Ce triangle est souvent appelé triangle de Pascal bien qu'il figure dans des textes chinois du VI^e siècle.

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

$$\boxed{(a+b)^n = \sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p}.}$$

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 $(a+b)^0 = 1 = \mathrm{C}_0^0 a^0 b^0$. Elle est vraie pour $n=1$ car elle s'écrit alors $(a+b)^1 = a+b$. Supposons la vraie pour n. Alors,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\Big(\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p}\Big) \\
&= \Big(\sum_{p=0}^{n} \mathrm{C}_n^p a^{p+1} b^{n-p}\Big) + \Big(\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n+1-p}\Big) \\
&= \Big(\sum_{q=1}^{n+1} \mathrm{C}_n^{q-1} a^q b^{n+1-q}\Big) + \Big(\sum_{q=0}^{n} \mathrm{C}_n^q a^q b^{n+1-q}\Big) \\
&= b^{n+1} + \sum_{q=1}^{n} \mathrm{C}_n^{q-1} a^q b^{n+1-q} + a^{n+1} \\
&= a^{n+1} + b^{n+1} + \sum_{q=1}^{n} \big(\mathrm{C}_n^{q-1} + \mathrm{C}_n^q\big) a^q b^{n+1-q} \\
&= \sum_{q=0}^{n+1} \mathrm{C}_{n+1}^q a^q b^{n+1-q}.
\end{aligned}$$

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 $\mathrm{C}_n^p = \mathrm{C}_{n-1}^{p-1} + \mathrm{C}_{n-1}^p$ pour $n > p \geqslant 1$ 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 $\mathrm{C}_n^p = \dfrac{n}{p}\mathrm{C}_{n-1}^{p-1}$ pour $n \geqslant p \geqslant 1$.

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

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

b) Calculer de même $\sum_{p=0}^{n} (-1)^n C_n^p$.

c) Calculer $\sum_{p=1}^{n} pC_n^p$ 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 $C_{2n}^n = \sum_{p=0}^{n} \left(C_n^p\right)^2$. (Remarquer que $C_n^p = C_n^{n-p}$.)

b) Donner une interprétation combinatoire de la formule précédente.

6) On pose $F_n = \sum_{p \leqslant n/2} C_{n-p}^p = C_n^0 + C_{n-1}^1 + C_{n-2}^2 + \ldots$. (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,..., 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 $\{1,\ldots,n\}$, 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 $n \geqslant 1$ et $p \geqslant 1$. Montrer aussi $R_n^0 = 1$, $R_n^1 = n$ et $R_1^p = 1$, pour $n \geqslant 1$, $p \geqslant 1$.

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 $\{1,\ldots,n+p-1\}$ une combinaison avec répétition de la façon suivante : si cette partie est formée de $n-1$ entiers $x_1 < \cdots < x_{n-1}$, 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 $x_1x_2\ldots x_n$ 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 $x_1(x_2x_3)$ et $(x_1x_2)x_3$, de même que $K_4 = 5$ avec les parenthésages

$$(x_1x_2)(x_3x_4), \quad ((x_1x_2)x_3)x_4), \quad (x_1(x_2x_3))x_4, \quad x_1((x_2x_3)x_4), \quad \text{et} \quad x_1(x_2(x_3x_4)).$$

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 $K_n = \dfrac{1}{n} C_{2n-2}^{n-1}$.

D. Probabilités

(*Paragraphe non enseigné en 2004–2005*)

Une probabilité sur un ensemble fini Ω est une application $p\colon \mathscr{P}(\Omega) \to [0,1]$ qui associe à toute partie A de Ω sa *probabilité* $p(A)$ de sorte que l'on ait $p(\varnothing) = 0$, $p(\Omega) = 1$, et $p(A \cup B) = p(A) + p(B)$ si A et B sont deux parties *disjointes* de Ω. Si A et B sont deux parties quelconques de Ω, 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 Ω 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 Ω est définie par $p(\{x\}) = 1/\operatorname{card}\Omega$ pour tout x de Ω. Alors, $p(A) = \operatorname{card} A/\operatorname{card}\Omega$ pour toute partie $A \subset \Omega$.

Supposons qu'on *sache* qu'un événement A s'est produit. Alors, l'ensemble probabilisé Ω 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 $A = \{a \leqslant 3\}$ et $B = \{a + b \geqslant 7\}$ ne sont par contre pas indépendants. La probabilité du premier est $\frac{3}{6} = \frac{1}{2}$. L'événement $\{a + b \geqslant 7\}$ se produit dans les cas $(6,b)$

avec b quelconque, $(5,b)$ avec $b \geqslant 2$, 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 $b \geqslant 5$ et $(3,b)$ avec $b \geqslant 4$ 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. Imaginions 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 $A_1, \ldots, A_n$ une partition de Ω 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 $\mathrm{C}_n^p/2^n$. Le nombre de fois que l'on obtient face est compris entre 0 et n. On retrouve ainsi la formule

$$2^n = \sum_{p=0}^{n} \mathrm{C}_n^p.$$

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 π et sur F avec probabilité $1-\pi$. La probabilité d'obtenir p fois pile est égale à $\pi_p = \mathrm{C}_n^p \pi^p (1-\pi)^{n-p}$: 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 :

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

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

Quelle est l'espérance de gain : 0 avec probabilité π_0, 1 avec probabilité π_1, etc., d'où

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

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

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

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 Ω et soit A une partie de Ω 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 Ω.

§3. Division euclidienne

A. Un peu de terminologie algébrique

Les mathématiques du XX^{e} siècle ont mis en évidence l'intérêt des *structures*. Concrètement, il s'agit de dégager un certain nombre de propriétés importantes d'un objet mathématique donné (ici, l'ensemble des nombres entiers) et de développer la théorie générale d'un objet vérifiant ces propriétés. Au passage, on lui donne un nom.

Dans le cas que je vais évoquer maintenant, il s'agit de la notion d'*anneau*, l'ensemble des nombres entiers relatifs en est l'exemple le plus fondamental.

DÉFINITION. — *Soit A un ensemble muni de deux lois internes $A \times A \to A$, l'addition et la multiplication, notées respectivement $+$ et $\times$, et muni de deux éléments, notés 0 et 1. On dit que A est un anneau si les propriétés suivantes sont satisfaites :*

– 0 *est un élément neutre pour $+$: pour tout $a \in A$, $a+0=0+a=a$;*

– *l'addition est commutative (pour tout a et tout b dans A, $a+b=b+a$) et associative (pour tous a, b, c dans A, $(a+b)+c=a+(b+c)$) ;*

– *tout élément a un symétrique pour $+$, appelé opposé : pour tout $a \in A$, il existe $b \in A$ tel que $a+b=b+a=0$;*

– 1 *est un élément neutre pour $\times$: pour tout $a \in A$, $a \times 1 = 1 \times a = a$;*

– *la multiplication est commutative (pour tout a et tout b dans A, $a \times b = b \times a$) et associative (pour tous a, b, c dans A, $(a \times b) \times c = a \times (b \times c)$) ;*

– *la multiplication est distributive par rapport à l'addition : pour tous a, b, $c \in A$, $a \times (b+c) = a \times b + a \times c$.*

Nous ne nous en servirons pas tout de suite mais on résume les trois premières propriétés en disant que A muni de $+$ et de 0 est un *groupe commutatif*.

L'ensemble des entiers naturels, avec son addition et sa multiplication, n'est pas un anneau : en effet, seul 0 a un opposé pour $+$. En revanche, l'ensemble $\mathbf{Z}$ des entiers relatifs — que vous connaissez sans l'avoir jamais construit en détail — est un anneau. Voyons comment on peut le définir. 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 ni général, ni très élégant.

La meilleure méthode revient à introduire formellement « toutes » les soustractions $a-b$ et à identifier celles qui doivent l'être. Soit S l'ensemble des couples (a,b) d'éléments de $\mathbf{N}$. On va dire que deux couples (a,b) et (c,d) sont équivalents si $a+d=b+c$ (à la fin, cela signifiera $a-b=c-d$).

La relation dans S ainsi définie est une relation d'équivalence. Démontrons-le en rappelant au passage ce que cela signifie.

– 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).

La *classe d'équivalence* d'un couple est l'ensemble des couples qui lui sont équivalents. 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.

Sur $\mathbf{Z}$, on hérite de l'addition de $\mathbf{N}$, 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 $(a'+c',b'+d')$, c'est-à-dire $[a+c,b+d]=[a'+c',b'+d']$.

Cette addition munit $\mathbf{Z}$ d'une structure de groupe commutatif, dont l'élément neutre est $[0,0]$; l'opposé de $[a,b]$ est $[b,a]$. 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 $a=b$) et est compatible à l'addition. On notera $-a$ l'élément $[0,a]$; c'est l'opposé de $[a,0]$, identifié à l'élément a de $\mathbf{N}$. De plus, tout élément de $\mathbf{Z}$ est de la forme $[a,0]$ ou $[0,a]$.

Sur $\mathbf{Z}$, on hérite aussi d'une multiplication, définie par $a\times[c,d]=[ac,ad]$ et $-a\times[c,d]=-[ac,ad]$ si $a\in\mathbf{N}$. (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.

On résume ces propriétés en disant que $(\mathbf{Z},+,\cdot,0,1)$ est un *anneau commutatif unitaire*.

B. Le théorème de la division euclidienne

Si x est un nombre réel, il existe un unique entier relatif n tel que $n\leqslant x<n+1$: c'est le plus grand entier relatif inférieur ou égal à x. On le note $\lfloor x\rfloor$ et on l'appelle la *partie entière de x*.

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

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

Donnons deux démonstrations. La plus rapide consiste à remarquer que nécessairement, q est la partie entière du nombre réel a/b, comme le montre la formule $\frac{a}{b} = q + \frac{r}{b}$ et l'inégalité $0 \leqslant \frac{r}{b} < 1$. Posons donc $q = \lfloor a/b \rfloor$. Il vient nécessairement $r = a - bq$. Comme $q \leqslant a/b < q+1$, $bq \leqslant a < bq + b$ et l'on a $0 \leqslant r < b$. Puisque r est un entier, $r \leqslant b-1$. Cela montre l'existence et l'unicité de la division euclidienne.

Il est peut-être préférable d'avoir une démonstration qui n'utilise rien sur les nombres réels. Supposons d'abord que a soit positif ou nul et soit R l'ensemble des entiers $r \in \mathbf{N}$ tels qu'il existe $q \in \mathbf{N}$ avec $a = bq + r$. L'ensemble R est non vide, car on peut écrire $a = b\cdot 0 + a$, donc $a \in R$. Soit r son plus petit élément et soit $q \in \mathbf{N}$ tel que $a = bq + r$. Par hypothèse, $r \geqslant 0$. Si l'on avait $r \geqslant b$, la relation $a = bq + r = b(q+1) + (r-b)$ montrerait que $r - b \in R$, ce qui contredit la minimalité de r. Par suite, $r \leqslant b-1$.

Si $a \leqslant 0$, alors $b - 1 - a \geqslant 0$; soit q et r le quotient et le reste de la division euclidienne de $b-1-a$ par b. La relation $b-1-a = bq + r$ s'écrit $a = b(-q) + (b-1-r)$, ce qui montre l'existence de la division euclidienne de a par b. De plus, si $a = bq' + r'$, avec $0 \leqslant r' \leqslant b-1$, on a $b-1-a = -bq' + (b-1-r')$. Vu l'unicité de la division euclidiene de $b-1-a$ par b. cela entraîne $q' = -q$ et $b-1-r' = r$.

Si a et b sont deux entiers relatifs, avec $b < 0$, il existe des entiers q et $r \in \mathbf{Z}$, uniques, tels que $a = bq + r$ et $0 \leqslant r \leqslant |b| - 1$. En effet, cela revient à dire que $a = |b|(-q) + r$ est la division euclidienne de a par $|b|$.

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)

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 $-\frac{1}{2}|b| < r \leqslant \frac{1}{2}|b|$.

5) Connaissant la division euclidienne de deux entiers n et n' par un entier $b \geqslant 1$, que pouvez-vous dire de la division euclidienne de $n + n'$ par b ?

6) Soit a et b des entiers naturels tels que $a \geqslant 3$ et $b \geqslant 2$; 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}.

C. 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 $k \geqslant 0$ et des entiers $c_0, \dots, c_k \in \{0, \dots, b-1\}$ tels que l'on ait*

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

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 $b \leqslant 10$, 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 $0 \leqslant r \leqslant b-1$. Comme $q \leqslant n/b < n$, l'entier q s'écrit sous la forme $d_m b^m + d_{m-1} b^{m-1} + \cdots + d_0$, 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 $1 \leqslant i \leqslant m+1$. On a

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

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 $c_k b^k + \cdots + c_0$ et $d_m b^m + \cdots + d_0$. Comme on a supposé $n \geqslant b$, on a $k \geqslant 1$ et $m \geqslant 1$. Alors, l'écriture

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

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

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

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 $1 \leqslant i \leqslant k$.

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

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

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 ?

D. 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 $|a| \leqslant |b|$. Si $b = ad$, on a $d \neq 0$ car $b \neq 0$, d'où $|d| \geqslant 1$ et finalement $|b| = |a||d| \leqslant |a|$.

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 $|a| \leqslant |b|$ et $|b| \leqslant |a|$ 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 $0 \leqslant r \leqslant |a| - 1$. On a $nb = naq + nr$, donc si na divise nb, il divise aussi $nb - naq = nr$. Cela entraîne $|na| \leqslant |nr|$, donc $|a| \leqslant |r|$ car $n \neq 0$, ce qui contredit l'inégalité $0 \leqslant r \leqslant |a| - 1$.

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 $m \geqslant 2$. 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 : *deux 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

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

La somme des chiffres de n est l'entier $c_k + c_{k-1} + \cdots + c_0$. 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 $k \geqslant 1$, c'est-à-dire, si n s'écrit avec au moins deux chiffres, la somme des chiffres de n est strictement inférieure à n. Le 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^{4444} ; 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 $N = \overline{mcdu}$ un nombre de quatre chiffres écrit en base 10. On pose $P = \overline{udcm}$. 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 boite de masses marquées de 1 g à 100 g. Comment déterminer la masse d'un objet pesant de 1 à 100 g en n'utilisant que cinq masses marquées ?

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.)

E. Plus grand diviseur commun, algorithme d'Euclide

Soit a et b deux entiers, 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 $\mathrm{pgcd}(a,b)$. On dit que a et b sont premiers entre eux si $\mathrm{pgcd}(a,b)=1$.

THÉORÈME DE BÉZOUT. — *Soit a et b deux entiers relatifs, non tous deux nuls. Il existe des entiers relatifs u et v tels que $d=au+bv$.*

Voici une première démonstration. Notons I l'ensemble des entiers relatifs $n\in\mathbf{Z}$ qui sont de la forme $au+bv$ avec $(u,v)\in\mathbf{Z}^2$. Remarquons que la somme de deux éléments de I appartient à I. En effet, si $n=au+bv$ et $n'=au'+bv'$, alors $n+n'=a(u+u')+b(v+v')\in I$. De même, si $n\in I$ et $m\in\mathbf{Z}$, alors $mn\in I$.

Comme a et b ne sont pas tous deux nuls, I est différent de $\{0\}$ (il contient a et b). Il contient donc des entiers strictement positifs Si I contient un entier $n<0$, il contient aussi $-n$, donc I contient des entiers strictement positifs. Soit δ le plus petit entier strictement positif qui appartienne à I et montrons que $d=\delta$.

Soit $a=\delta q+r$ la division euclidienne de a par δ. Si $\delta=au+bv$, on a alors $r=a-\delta q=a(1-u)-bv$, ce qui montre que $r\in I$. De plus, $0\leqslant r<\delta$. Comme δ est le plus petit élément strictement positif de I, cela impose $r=0$, donc a est multiple de δ. Par le même argument, on montre que δ divise b. Ainsi, δ est un diviseur commun de a et b. En particulier, $\delta\leqslant d$.

Comme a et b sont multiples de d, tout élément de I, étant de la forme $au+bv$, est multiple de d. Par suite, δ est multiple de d et $d\leqslant\delta$.

On a donc $d=\delta$.

Voici une application importante :

THÉORÈME DE GAUSS. — *Soit a, b, c des entiers non nuls. On suppose que a et b sont premiers entre eux et que a divise bc ; alors, a divise c.*

Soit u et v des entiers tels que $au+bv=1$. On a alors $auc+bvc=c$. L'entier a divise auc, et il divise $bvc=bcv$ puisqu'il divise bc. Il divise donc leur somme $auc+bcv$ qui vaut c.

On définit de manière analogue le pgcd d'une famille $a_1,\dots,a_n$ d'entiers non tous nuls. On a $\mathrm{pgcd}(a_1,a_2,\dots,a_n)=\mathrm{pgcd}(a_1,\mathrm{pgcd}(a_2,\dots,a_n))$. En effet, cette formule reflète exactement le fait qu'un entier divise tous les a_i, pour $1\leqslant i\leqslant n$, si et seulement s'il divise a_1 et tous les a_i, $2\leqslant i\leqslant n$.

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. On écrit ainsi $m=bu$.

Par hypothèse, a divise bu et est premier avec b. D'après le lemme de Gauss, a divise u. On écrit ainsi $u = av$ et l'on a $m = abv$. Autrement dit, m est multiple de ab, donc supérieur à ab. Inversement, ab est multiple de a et de b, d'où $\operatorname{ppcm}(a,b) = ab$ dans le cas où a et b sont premiers entre eux.

Calculons maintenant $\operatorname{ppcm}(a,b)$ dans le cas général. Si $d = \operatorname{pgcd}(a,b)$, 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 $da'b' = ab/d$. Inversement, si $da'b' = ab' = a'b$ est multiple de a et de b. Nous avons donc démontré que $\operatorname{ppcm}(a,b) = ab/\operatorname{pgcd}(a,b)$.

La démonstration du théorème de Bézout que nous avons donnée n'est pas constructive : elle ne permet pas de déterminer effectivement, en pratique, des entiers u et v tels que $\operatorname{pgcd}(a,b) = au + bv$. Elle ne permet pas non plus de calculer le pgcd. Il existe un algorithme pour ce faire, 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 $u_n = \operatorname{pgcd}(a,b)$.

Donnons un exemple et calculons le pgcd de 414 et 598. La suite est 414, 598, 414, 184, 46, 0. Le 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 $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$ 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 pgcd. Cette formule entraîne que $\operatorname{pgcd}(u_{n+1}, u_{n+2}) = \operatorname{pgcd}(u_n, u_{n+1})$ pour tout entier n (au moins tant que l'algorithme ne s'arrête pas), d'où par récurrence $\operatorname{pgcd}(u_n, u_{n+1}) = \operatorname{pgcd}(u_0, u_1) = \operatorname{pgcd}(a,b)$.

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 $\operatorname{pgcd}(u_n, u_{n+1}) = u_n$. On a donc bien $u_n = \operatorname{pgcd}(a,b)$.

Pour déterminer les coefficients u et v du théorème de Bézout, il y a une variante de l'algorithme d'Euclide dans laquelle on travaille avec des triplets d'entiers. Si $L = (x,y,z)$ est un tel triplet, $L_1 = x$ est son premier élément ; on soustrait des lignes et on multiplie une ligne par un entier en effectuant les opérations correspondantes élément par élément.

ALGORITHME D'EUCLIDE (ÉTENDU). — *Soit a et b deux entiers strictement positifs. On pose $L_0 = (a, 1, 0)$ et $L_1 = (b, 0, 1)$.*

Si le premier coefficient $L_{n+1,1}$ de la ligne L_{n+1} n'est pas nul, soit q le quotient de la division euclidienne de $L_{n,1}$ par $L_{n+1,1}$ et on pose $L_{n+2} = L_{n+1} - qL_n$.

Si $L_{n+1,1} = 0$, posons $L_n = (d, u, v) =$. On a alors $d = \mathrm{pgcd}(a, b) = au + bv$.

Dans l'exemple précédent, les lignes que l'on obtient sont successivement

$$\begin{aligned}
&(414, 1, 0)\\
&(598, 0, 1)\\
&(414, 1, 0) = (414, 1, 0) - 0 \cdot (598, 0, 1) && q = 0\\
&(184, -1, 1) = (598, 0, 1) - 1 \cdot (414, 1, 0) && q = 1\\
&(46, 3, -2) = (414, 1, 0) - 2 \cdot (184, -1, 1) && q = 2\\
&(0, -13, 9) = (184, -1, 1) - 4 \cdot (46, 3, -2) && q = 4.
\end{aligned}$$

À la fin, on reconnaît que 46 est le pgcd de 414 et 598, et l'on a bien

$$3 \times 414 - 2 \times 598 = 46.$$

Démontrons cet algorithme. Remarquons pour commencer que la première colonne reproduit l'algorithme d'Euclide précédent. À la fin, l'entier d est donc le pgcd de a et b.

Notons $L_n = (d_n, u_n, v_n)$. On va montrer par récurrence sur n que l'on a $d_n = au_n + bv_n$. C'est vrai pour $n = 0$ car $L_0 = (a, 1, 0)$ et $a = a \times 1 + b \times 0$; c'est aussi vrai pour $n = 1$ puisque $L_1 = (b, 0, 1)$ et $b = a \times 0 + b \times 1$.

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.

Exercices. — 1) a) Soit a, b, c des entiers. On suppose que a divise bc et que $\mathrm{pgcd}(a, b) = 1$. 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 $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(c, d) = 1$ et que $\dfrac{a}{b} + \dfrac{c}{d}$ est entier. Montrer que $b = d$.

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

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

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

4) Calculer les plus grand diviseurs communs suivants : pgcd(46848,2379), pgcd(13860,4488), pgcd(30076,12669,21733).

5) Calculer pgcd(357,629) puis d = 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 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 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 pgcd de $a+2b$ et $2a+b$ est égal à 1 ou 3.

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

9) 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 pgcd et ppcm des entiers $12n^2+16n+6$ et $6n+5$.

10) 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 $\mathbf{Z}\times\mathbf{Z}$?

11) Soit m et n des entiers >1.

a) Montrer qu'un nombre complexe $z\in\mathbf{C}$ vérifie $z^n=z^m=1$ si et seulement si $z^{\mathrm{pgcd}(m,n)}=1$.

b) Si $m>n$, montrer que pgcd(a^m-1,a^n-1) = pgcd$(a^m-1,a^{m-n}-1)$. En déduire à l'aide de l'algorithme d'Euclide que pgcd$(a^n-1,a^m-1)=a^{\mathrm{pgcd}(m,n)}-1$.

12) 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 $m<n$, pgcd(F_n,F_m) = pgcd(F_{n-m},F_m) et pgcd(n,m) = pgcd$(n-m,m)$. En déduire par récurrence sur max(m,n) que la relation pgcd$(F_n,F_m)=F_{\mathrm{pgcd}(n,m)}$.

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 $((1+\sqrt{5})/2)^n/\sqrt{5}$.

13) 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 = 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 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.

§4. Nombres premiers

A. 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.

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

$$\mathbf{2},3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30.$$

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.

$$\mathbf{2},\mathbf{3},4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30.$$

Ensuite, il y a 5, d'où

$$\mathbf{2},\mathbf{3},4,\mathbf{5},6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30.$$

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

LEMME. — *Soit n un entier $\geqslant 2$. Si n n'est pas premier, il existe un nombre premier $p \leqslant \sqrt{n}$ 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 $m \leqslant k$, on a $m^2 \leqslant km = n$, d'où $m \leqslant \sqrt{n}$. 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 $p \leqslant m \leqslant \sqrt{n}$. Dans l'autre cas, $k \leqslant m$, 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

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

Exercices. — 1) Ce nombre s'écrit avec 8 chiffres en base 2 et 6 chiffres en base 3. Quel est-il ? Ah, j'oubliais, c'est un nombre premier.

2) a) Soit a et b des entiers > 1 et soit $n = ab$. Si $n \geqslant 5$, démontrer que ab divise $(n-1)!$. (C'est facile si $a \neq b$; si $a = b$, montrer que $2a^2$ divise $(n-1)!$.)

b) Inversement, si n est un nombre premier, alors n ne divise pas $(n-1)!$.

3) Soit n un nombre entier et posons $M_n = 2^n - 1$ (*nombre de Mersenne*).

a) Si M_n est un nombre premier, montrer que n est premier.

b) Trouver le plus petit nombre premier n tel que M_n ne soit pas premier.

4) Pour $n > 0$, on pose $F_n = 2^{2^n+1}$ (*nombre de Fermat*).

a) Montrer que $F_1, \dots, F_4$ sont des nombres premiers.

b) Si k n'est pas une puissance de 2, 2^k+1 n'est pas un nombre premier. (Si $k = ab$, avec a impair, montrer que 2^b+1 divise 2^k+1.)

c) Montrer que F_5 n'est pas un nombre premier (Euler), contrairement à une affirmation de Fermat que tous les F_n sont des nombres premiers. Précisément, montrer que 641 divise F_5. (Écrire $2^{32}+1 = 16(2^7)^4+1$ et remarquer que $16 = 641-625$.)

d) Démontrer que $\prod_{k=0}^{n-1} F_k = F_n - 2$. Si $m \neq n$, en déduire que F_n et F_m sont premiers entre eux.

5) a) Si p est un nombre premier impair, $2^{p-1}-1$ est multiple de p.

b) Montrer que pour tout entier $n \geqslant 0$, $2^{F_n-1}-1$ est multiple de F_n, où $F_n = 2^{2^n}+1$ désigne le n-ième nombre de Fermat.

c) Cela entraîne-t-il que F_n est un nombre premier ?

6) Soit a et b deux entiers tels que a^2+b^2 soit multiple de 7. Montrer que a et b sont multiples de 7.

7) Trois entiers a, b, c vérifient $a^2 = b^2+c^2$.

a) Montrer que l'un au moins de b et c est multiple de 3.

b) Montrer que l'un au moins de a, b, c est multiple de 5.

c) Montrer que l'un au moins de b et c est multiple de 4.

8) Soit a et b des entiers ; on pose $A = 11a+2b$ et $B = 18a+5b$.

a) Montrer que si 19 divise l'un des deux entiers A ou B, il divise l'autre.

b) On suppose que a et b sont premiers entre eux. Montrer que A et B ne peuvent avoir d'autre diviseur commun que 1 et 19.

9) Soit p un nombre premier et soit a un entier premier à p.

a) Montrer qu'il existe $b \in \{1, \dots, p-1\}$ tel que $ab \equiv 1 \pmod{p}$.

b) Soit k le plus petit entier > 0 tel que $a^k \equiv 1 \pmod{p}$. On va montrer que k divise $p-1$.

Soit $d = \operatorname{pgcd}(k, p-1)$ et soit u, v des entiers relatifs tels que $d = uk + v(p-1)$. Si $u \geqslant 0$ et $v \leqslant 0$, calculer $a^{uk}b^{-v(p-1)} \pmod{p}$. En déduire que $a^d \equiv 1 \pmod{p}$, puis que $d = k$.

c) Traiter les autres cas de manière analogue.

10) On rappelle que $F_n = 2^{2^n}+1$ désigne le n-ième nombre de Fermat.

a) Soit p un facteur premier de F_n. Montrer que $2^{2^n} \equiv -1 \pmod{p}$, puis que 2^{n+1} est le plus petit entier $d > 0$ tel que $2^d \equiv 1 \pmod{p}$. À l'aide de l'exercice 9, montrer que $p \equiv 1 \pmod{2^{n+1}}$.

b) On suppose que $3^{2^{2^n-1}} \equiv -1 \pmod{F_n}$. Soit p un facteur premier de F_n. Montrer que le plus petit entier d tel que $3^d \equiv 1 \pmod{p}$ est égal à 2^{2^n}.

c) Déduire de l'exercice 9 que 2^{2^n} divise $p-1$, puis que $p \equiv 1 \pmod{2^{2^n}}$. Montrer enfin que $p = F_n$, autrement dit que F_n est premier (*critère de Pépin*).

11) a) Soit p un nombre premier ; pour tout entier $k \geqslant 0$, on pose $S_k = 1^k + 2^k + \cdots + (p-1)^k$. Calculer S_0, S_1, S_{p-1}, S_p modulo p. Montrer que $S_k \equiv S_m \pmod{p}$ si $k \equiv m \pmod{p-1}$.

b) Si $k \in \mathbf{N}$, on pose $b_k(x) = x(x-1)\dots(x-k+1)$; c'est un polynôme de degré k, à coefficients entiers et de coefficient dominant 1. (On a $b_0 = 1$, $b_1 = x$, $b_2 = x(x-1)$, etc.)

Pour tout couple (k, n) d'entiers, calculer $\sum_{i=1}^{n} b_k(x)$.

c) Si p est un nombre premier et k un entier, en déduire la valeur de

$$b_0(1) + \cdots + b_0(p-1) \pmod{p}.$$

d) Montrer par récurrence sur n que pour tout polynôme P à coefficients entier, de degré n, il existe des entiers $a_0, \dots, a_n$ tels que

$$P(x) = a_0 b_0(x) + a_1 b_1(x) + \cdots + a_n b_n(x).$$

e) Calculer $S_k \pmod p$ en fonction de k.

12) Soit p un nombre premier et soit $P(x)$ le polynôme $P(x) = x^p - x$. D'après l'exercice 11, il existe des entiers $a_0, \dots, a_p$ tels que $P(x) = a_0 b_0(x) + a_1 b_1(x) + \cdots + a_p b_p(x)$.

a) Montrer que par récurrence sur n que a_n est multiple de p si $0 \leqslant n < p$. (Calculer $P(0) \pmod p$, puis $P(1) \pmod p$,...)

b) Montrer que

$$x(x-1)\dots(x-p+1) \equiv x^p - x \pmod p.$$

B. 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 comme produit de nombres premiers.

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

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 $m \leqslant n/2 < n$. Si $m = 1$, $n = p_1$ et on pose $r = 1$. Sinon, il existe par récurrence un entier r et des nombres premiers $p_2 \leqslant \cdots \leqslant p_r$ tels que $m = p_2 \dots p_r$. On a donc $n = p_1 m = p_1 p_2 \dots p_r$. De plus, $p_1 \leqslant p_2$ 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-dessous, 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 $q_1 \leqslant \cdots \leqslant q_s$. Alors $p_2 \dots p_r = n/p_1 = q_2 \dots q_s$. Par récurrence, $r - 1 = s - 1$ et $p_2 = q_2$, …, $p_r = q_r$.

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 x le plus petit entier $\geqslant 1$ 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 $0 \leqslant r \leqslant x - 1$. Par suite, $rb = pb - xbq$ 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.

Autre démonstration : 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 $d = 1$. D'après le théorème de Bézout, il existe des entiers u et v tels que $1 = au + pv$. Alors, $b = b(au + pv) = abu + p(bv)$ est multiple de p.

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, $p_1 < \dots < p_s$.

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

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

Soit m et n des entiers $\geqslant 1$. On a $v_p(mn) = v_p(m) + v_p(n)$. De plus, on a $v_p(m+n) \geqslant \min(v_p(m), v_p(n))$, et l'égalité est obtenue dès que $v_p(m) \neq v_p(n)$.

Exercices. — 1) Soit n un entier strictement positif ; on note $n = \prod_{i=1}^r p_i^{n_i}$ sa décomposition en facteurs premiers, les p_i sont des nombres premiers deux à deux distincts, les n_i des entiers $\geqslant 1$.

a) Montrer qu'un entier $d > 0$ divise n si et seulement si il existe des entiers m_i, $0 \leqslant m_i \leqslant n_i$ tel que $d = \prod_{i=1}^r p_i^{m_i}$.

b) Montrer que le nombre de diviseurs strictement positifs de n est égal à $\prod_{i=1}^r (1 + n_i)$.

c) Calculer en fonction des p_i et des n_i la somme des diviseurs positifs de n.

2) a) Décomposer en facteurs premiers les entiers $a = 46\,848$, $b = 2379$, $c = 8\,633$, $d = 4\,183$.

b) En déduire pgcd(a,b) et pgcd(c,d). Calculer ppcm(a,b) et ppcm(c,d).

c) Comparer avec l'algorithme d'Euclide.

3) a) Décomposer 51 et 216 en facteurs premiers ; calculer pgcd(51,216). Déterminer toutes les expressions de 216 comme le produit de deux entiers naturels premiers entre eux.

b) Soit a et b des entiers > 0 tels que $a + b = 51$, $a < b$ et ppcm$(a,b) = 216$. Montrer que $d = \text{pgcd}(a,b)$ divise pgcd(51,216).

c) Montrer que $a' = a/d$ et $b' = b/d$ sont premiers entre eux. Que vaut ppcm(a',b') ? En déduire la liste des couples (a,b) possibles.

4) 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 $k \geqslant 1$? En déduire que

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

(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.

5) 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 qu'il existe pour tout $n \geqslant 1$ des entiers impairs a_n et b_n tels que l'on ait $u_n = a_n/2^{2n-1} b_n$.)

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

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

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

Montrer par récurrence sur $n \geqslant 2$ 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 H_n n'est un pas en entier si $n \geqslant 2$.

C. 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 $p_1, \ldots, p_r$. Considérons l'entier $n = p_1 \ldots p_r + 1$; on a $n > 1$. Soit p un diviseur premier de n. Par hypothèse, p est l'un des p_i. Par suite, p divise $n - p_1 \ldots p_r = 1$, 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 $\lim_{x\to\infty} \pi(x) = +\infty$.

Gauss avait conjecturé à la fin du XVIII$^{\text{e}}$ siècle, et Hadamard et de la Vallée-Poussin ont démontré en 1896 le *théorème des nombres premiers*, à savoir que l'on a

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

Jusqu'aux années 1960 et la preuve d'Erdös 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*) $\mathrm{li}(x) = \int_e^x \frac{dt}{\log t}$ dont la croissance est en $x/\log x$ lorsque $x \to \infty$. 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

$$\lim_{x\to\infty} |\pi(x) - \mathrm{li}(x)|\, x^{-\alpha} = 0.$$

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

Si le comportement de la fonction $\mathrm{li}(x)$ est très bien compris, celui de la fonction $\pi(x)$ reste très mystérieux. Un exemple supplémentaire : la différence $\pi(x) - \mathrm{li}(x)$ 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 2×10^{1165} et probablement inférieure à $7\times 10^{370}\ldots$) — il serait impossible de vérifier cela à la main !

Exercices. — 1) a) Montrer qu'aucun des entiers $n!+2,\ldots,n!+n$ 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*).

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) 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) Démontrer l'équivalent $\mathrm{li}(x)\sim x/\log(x)$.

D. 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

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

b) Soit p un nombre premier tel que $n<p\leqslant 2n$. Montrer que p divise N.

c) Montrer que $(\pi(2n)-\pi(n))\log n\leqslant 2n\log 2$.

d) Soit p un nombre premier. Montrer que $v_p(N)\leqslant\log(2n)/\log p$.

e) Montrer que $\pi(2n)\log(2n)\geqslant n\log 2$.

f) Montrer que pour tout entier k,

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

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

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

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

a) Soit n un entier ; on pose $N=\binom{2n+1}{n}$. Montrer que $N\leqslant 4^n$.

b) Montrer que le produit des nombres premiers p tels que $n+1<p\leqslant 2n+1$ divise N.

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

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

d) Soit p un facteur premier de N tel que $p\leqslant n$. Montrer que $p<2n/3$.

e) Montrer qu'un nombre premier p tel que $p^2|N$ vérifie $p\leqslant\sqrt{2n}$. 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 $N\leqslant 2^{4n/3}(2n)^{\sqrt{2n}}$.

g) (*suite*) En déduire que $\log(x)/x\geqslant 1/6$, où $x=\sqrt{2n}$, puis que $x\leqslant 18$. En déduire que $n\leqslant 162$.

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

E. Petit théorème de Fermat

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

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

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 $\geqslant 0$. 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 $n^{p-1} \equiv 1 \pmod{p}$.

On peut reformuler la propriété précédente en disant que $n^{p-1} \equiv 1 \pmod{p}$ pour tout entier n tel que $1 \leqslant n < p$. Autrement dit, si un couple (n, p) d'entiers, avec $1 \leqslant n < p$ 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 $341 = 31 \times 11$ 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 Carmichaël*. 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 Carmichaël.

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.

Exercices. — 1) a) Soit p un nombre premier et soit x un entier tel que $x^2 \equiv 1 \pmod{p}$. Montrer que l'on a $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$.

b) Calculer $2^{140} \pmod{561}$. En déduire que 561 n'est pas un nombre premier.

2) a) Montrer que pour tout entier n, $n(n^4-1)$ est divisible par 15.

b) Montrer que pour tout entier n, $n^2(n^4-1)$ est divisible par 60. Peut-on faire mieux ?

c) Montrer que pour tout entier n, $n(n^6-1)$ est divisible par 42. Peut-on faire mieux ?

3) Pour quelles valeurs de l'entier n,

a) le nombre $4^n + 2^n + 1$ est-il divisible par 7 ?

b) le nombre $9^n + 3^n + 1$ est-il divisible par 13 ?

c) le nombre $25^n + 5^n + 1$ est-il divisible par 31 ?

4) a) Calculer les restes modulo 13 des entiers 5^{206}, 5^{381}, 5^{883}, puis 5^n pour tout entier $n \in \mathbf{N}$.

b) Calcler les restes modulo 13 des entiers 1617^{206}, 1617^{381}, 1617^{883}, 1617^n, pour $n \in \mathbf{N}$.

5) Soit p un nombre premier > 2.

a) Soit a un entier tel que $a^2 \equiv -1 \pmod{p}$. Déduire du petit théorème de Fermat que $(p-1)/2$ est pair, donc que $p \equiv 1 \pmod{4}$.

b) Soit $x \in \{1, \ldots, p-1\}$; montrer qu'il existe un unique entier $y \in \{1, \ldots, p-1\}$ tel que $xy \equiv 1 \pmod{p}$. Montrer que $y \neq x$, sauf si $x = 1$ ou $x = p-1$.

c) En regroupant les entiers compris entre 1 et $p-1$ deux par deux, comme dans la question précédente, montrer que $(p-1)! \equiv -1 \pmod{p}$. (*théorème de Wilson*).

d) On suppose que $p \equiv 1 \pmod{4}$ et on pose $a = \left(\frac{p-1}{2}\right)!$. Montrer $a^2 \equiv -1 \pmod{p}$. (Dans $(p-1)!$, regrouper i et $p-i$.)

§5. Congruences

A. Théorème chinois

On trouve dans un traité chinois (III-V^{e} 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.

Mathématiquement, la solution de ce problème repose sur le théorème (appelé *théorème chinois*) :

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

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.

L'une des applications de ce théorème est la résolution de systèmes 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 $x \equiv c \pmod{n}$.

Toutefois, la démonstration du théorème chinois que nous avons donnée ne précise pas *comment* trouver effectivement un tel entier. Pour cela, nous allons utiliser le théorème de Bézout. Si $x \equiv a \pmod{m}$, on peut écrire $x = a + tm$, avec $t \in \mathbf{Z}$, et inversement, tout entier de cette forme est congru à a modulo m. La relation $x \equiv b \pmod{n}$ devient alors $a + tm = b \pmod{n}$, d'où $tm = b - a \pmod{n}$. D'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $um + vn = 1$, donc $um \equiv 1 \pmod{n}$. On en déduit que $t \equiv utm \equiv u(b-a) \pmod{n}$, d'où finalement une solution

$$x = a + um(b-a) = a(1-um) + umb = avn + umb.$$

Cela donne une solution particulière des deux équations en congruence, les autres sont obtenues par ajout d'un multiple de mn, et celle du théorème est le reste de sa division euclidienne par mn.

Résolvons maintenant 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 $x \equiv 2 \pmod 7$. La conjonction de la première et la troisième condition équivaut à la relation $x \equiv 2 \pmod{21}$, car 3 et 7 sont premiers entre eux. Une relation de Bézout pour 21 et 5 est $1 \times 21 - 4 \times 5 = 1$. La formule ci-dessus s'écrit alors

$$x = 2 \times (-20) + 3 \times 21 = 23 \pmod{105}.$$

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 1er janvier 1901 était un mardi, combien de vendredi 13 y a-t-il eu au XXe 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 ile 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 ?

B. Indicateur d'Euler, cryptographie RSA

Soit n un entier $\geqslant 2$.

PROPOSITION. — *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 alors que a est inversible 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 $\operatorname{pgcd}(a, n) = 1$.

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, $x \equiv y \pmod{n}$.

On note $\varphi(n)$ le nombre des entiers m avec $1 \leqslant m \leqslant n$ 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 $m \geqslant 1$ tel que $a^m \equiv 1 \pmod{n}$ est un diviseur de $\varphi(n)$.*

Notons Φ l'ensemble des entiers m tels que $1 \leqslant m \leqslant n-1$ qui sont premiers à n. Soit a un entier premier à n et considérons l'application f de $\{0, \ldots, n-1\}$ 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 $y \in \{0, \ldots, n-1\}$, 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 Φ est fini, f définit une bijection de Φ 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 Φ, 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 $\geqslant 1$ 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 $0 \leqslant r \leqslant m-1$.

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 $f : A \to B$ 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 d un entier petit, premier à $\varphi(N)$ (en pratique, $d = 3$, ou 11 ; c'est-à-dire que p et q sont choisis en fonction de d...). La fonction f est la fonction $x \mapsto x^d \pmod{N}$; la fonction g est la fonction $x \mapsto x^e \pmod{N}$, où e 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 e peut décoder les messages. C'est donc cet entier e qui constitue la *clé secrète*; les entiers d 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 ?

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 : $k = c_r 2^r + \cdots + c_0$, 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 e dans un temps raisonnablement court s'il ne connaît que d et N. Bien entendu, il suffit de calculer $\varphi(N)$, car on peut alors calculer e 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. Les recommandations actuelles demandent d'utiliser des entiers de plus de 250 chiffres. Cela multiplie le temps nécessaire par quelque chose comme 10^{50}...

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 Carmichaël 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 Carmichaël. 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 soit 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) Le code ISBN a été inventé dans les années 60 pour faciliter le travail de catalogage des livres dans les librairies. 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).

2) 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.

3) Soit φ l'application de $\{0,\dots,9\}$ dans lui-même définie par $\varphi(x) = 2x$ si $x \leqslant 4$ et $\varphi(x) = 1+2(x-5)$ si $x \geqslant 5$. 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) :

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

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 $09 \to 90$.

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.

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

5) 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.

6) Soit n un entier qui est le produit de deux nombres premiers distincts. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^{\varphi(n)+1} \equiv x \pmod{n}$.

7) Soit n un entier $\geqslant 2$; si $0 \leqslant k \leqslant n-1$, on note $c_k = \exp(2ik\pi/n)$.

a) Montrer que $\{c_0,\dots,c_n\}$ est l'ensemble des racines complexes du polynôme $X^n - 1$.

b) 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.

c) 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 $\operatorname{pgcd}(k,n) = 1$ et tel que que $c = c_k$. Combien y a-t-il de tels nombres complexes c ?

d) Plus généralement, si d divise n, combien y a-t-il d'éléments $c \in \mathbf{C}^*$ qui sont d'ordre d ?

e) Montrer que $\sum_{d|n} \varphi(d) = n$, où la somme est prise sur l'ensemble des diviseurs > 0 de n.

C. 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 — en supposant d'ailleurs que vous saviez ce dont il s'agit. Lorsqu'on raisonne avec des congruences modulo un entier n fixé, on peut à tout instant remplacer un entier x ar 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.

D'abord la définition la plus élémentaire. Posons $R_n = \{0, 1, \ldots, n-1\}$ et introduisons une addition $\oplus$ et une multiplication $\otimes$ sur R_n : on définit $a \oplus b$ et $a \otimes b$ comme les restes des divisions euclidiennes de $a+b$ et ab par n. Montrons qu'elles munissent R_n d'une structure d'anneau (commutatif unitaire) :

– $a \oplus b$ et $b \oplus a$ sont tous deux égaux au reste de la division euclidienne de $a+b = b+a$ par n. L'addition est donc commutative ;

– on a $b + c \equiv (b \oplus c) \pmod{n}$, donc

$$a + (b + c) \equiv a + (b \oplus c) \pmod{n} \equiv a \oplus (b \oplus c) \pmod{n},$$

ce qui montre que $a \oplus (b \oplus c)$ est le reste de la division euclidienne de $a + (b + c)$ par n, car c'est un élément de R_n. De même, $(a \oplus b) \oplus c$ est le reste de la division euclidienne de $(a+b)+c$ par n. Comme $a+(b+c) = (a+b)+c$, on en déduit que $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ et l'addition est associative ;

– $a \oplus 0$ est le reste de la division euclidienne de $a + 0 = a$ par n ; pour $a \in R_n$, on a donc $a \oplus 0 = a$.

– l'opposé d'un élément $a \in R_n$ est le reste de la division euclidienne de $-a$ par n ; c'est $n - a$ si $a \neq 0$ et 0 si $a = 0$.

Ainsi, $(R_n, 0, \oplus)$ est un groupe abélien. Les propriétés de la multiplication se démontrent de manière analogue :

– $a \otimes b$ et $b \otimes a$ sont tous deux le reste de la division euclidienne de ab par n, donc sont égaux : la multiplication est commutative ;

– $a \otimes (b \otimes c)$ et $(a \otimes b) \otimes c$ sont égaux au reste de la division euclidienne de abc par n : la multiplication est associative ;

– $a \otimes 1 = a$, pour $a \in R_n$;

– $a \otimes (b \oplus c)$ est égal au reste de la division euclidienne de $a(b+c)$ par n, ainsi que $(a \otimes b) \oplus (a \otimes c)$, d'où la distributivité de la multiplication sur l'addition.

Remarquons que l'ensemble $\mathbf{Z}$ des entiers relatifs vérifie aussi ces propriétés. En outre, l'application $r \colon \mathbf{Z} \to R_n$ qui, à un entier x, associe le reste de la division euclidienne de x par n est compatible aux deux additions et aux deux multiplications : elle applique 0 sur 0, 1 sur 1, somme $(+)$ sur somme $(\oplus)$ et produit $(\cdot)$ sur produit $(\oplus)$. On dit que c'est un *homomorphisme d'anneaux*.

Outre le fait qu'elle ne se généralise pas facilement, cette définition a un défaut : dans certains cas, il pourrait être préférable de ne pas utiliser le reste de la division euclidienne par n, qui est le représentant dans $\{0, \ldots, n-1\}$ de la classe de congruence modulo n, mais plutôt un représentant dans l'intervalle $\{-n/2, \ldots, n/2\}$. Ce choix nécessite d'introduire un nouvel ensemble, de refaire la démonstration, alors que toutes les propriétés de R_n proviennent de deux choses :

– addition et multiplication sont compatibles à la relation de congruence ;

– tout élément de $\mathbf{Z}$ est congru modulo n à un unique élément de R_n.

On voit que tout choix d'une famille de représentants permettra de définir un anneau.

Si l'on ne veut pas privilégier un représentant, il est nécessaire d'adopter une définition plus générale et plus abstraite, et par là-même plus efficace : définir R_n comme *l'ensemble des classes d'équivalence pour la relation de congruence modulo n*. La classe d'équivalence d'un entier 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 $k \in \mathbf{Z}$. Notons $\mathrm{cl}(a)$ la classe d'un entier a. Il y a un calcul sur les classes, donné par les formules

$$\mathrm{cl}(a)+\mathrm{cl}(b)=\mathrm{cl}(a+b), \quad \mathrm{cl}(a)\,\mathrm{cl}(b)=\mathrm{cl}(ab), \quad \text{etc.}$$

L'anneau R_n sera noté $\mathbf{Z}_n$, la notation la plus courante en arithmétique est plutôt $\mathbf{Z}/n\mathbf{Z}$.[(1)]

[(1)] Lorsque p est un nombre premier, $\mathbf{Z}_p$ désigne souvent quelque chose de bien différent — et bien plus compliqué...

§6. Permutations

A. Le groupe des permutations d'un ensemble à n éléments

Soit A un ensemble. Une *permutation* de A est une bijection de A dans lui-même. La composée de deux permutations est une permutation ; la bijection réciproque d'une permutation est encore une permutation. L'identité de A est une permutation. Notons S_A l'ensemble des permutations de A. Muni de la loi de composition $\circ$, il forme ce qu'on appelle un *groupe*.

Cette bête algébrique est en effet définie de la façon suivante.

DÉFINITION. — *Un groupe est un ensemble G muni d'une application, $G \times G \to G$, $(g,h) \mapsto g * h$, appelée « loi de composition interne », et vérifiant les propriétés suivantes :*

- *la loi est* associative *: pour tous $g,h,k \in G$, $(g*h)*k = g*(h*k)$;*
- *il existe un élément $e \in G$ tel que $e*g = g*e = g$ pour tout $g \in G$ (existence d'un* élément neutre*) ;*
- *pour tout $g \in G$, il existe un élément $h \in G$, appelé* inverse de *h tel que $g*h = e$.*

Dans le cas qui nous intéresse, la loi est la composition des applications, l'élément neutre de S_A est l'application identique de A et l'inverse d'une permutation f est sa bijection réciproque.

Si n est un entier, on note S_n l'ensemble des permutations de l'ensemble fini $F_n = \{1,\dots,n\}$. Une permutation de F_n est exactement un arrangement de n éléments de $\{1,\dots,n\}$. Un tel arrangement est une application injective de $\{1,\dots,n\}$ dans lui-même, mais elle sera alors surjective car l'image de $\{1,\dots,n\}$ a n éléments et est contenue dans $\{1,\dots,n\}$, donc est égale à $\{1,\dots,n\}$. On a donc $\operatorname{card} S_n = n!$.

Il y a plusieurs façons de représenter une permution ; une solution un peu lourde mais parfois pratique consiste à écrire un tableau de 2 lignes et n colonnes, où chaque colonne est formée d'un élément de $\{1,\dots,n\}$ et de son image. Par exemple, $\left(\begin{smallmatrix}1&2&3&4\\3&2&1&4\end{smallmatrix}\right)$ désigne la permutation qui échange 1 et 3.

Une habitude courante en théorie des groupes veut qu'on omette le symbole pour la loi de composition interne ; on note par exemple fg pour la composée $f \circ g$ de deux permutations f et g. Si f est une permutation, on note $f^2 = f \circ f$, $f^3 = f^2 \circ f = f$, etc. On note aussi f^{-1} l'inverse de f. Cela définit f^k pour tout entier $k \in \mathbf{Z}$.

Dans le groupe des permutations, on peut simplifier des relations (en fait, ceci est valable dans n'importe quel groupe). Soit en effet f, g, h des permutations telles que $fg = fh$. Multiplions à gauche cette relation par f^{-1}. On obtient

$$g = \mathrm{id} \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h) = (f^{-1} \circ f) \circ h = \mathrm{id} \circ h = h.$$

De même, si $gf = hf$, on en déduit $g = h$.

Si f et g sont des permutations, l'inverse de $f \circ g$ est égale à $g^{-1} \circ f^{-1}$. En effet,

$$(fg)(g^{-1}f^{-1}) = f \circ (gg^{-1}) \circ f^{-1} = ff^{-1} = \mathrm{id},$$

et, par un raisonnement analogue, $(g^{-1}f^{-1})(fg) = \mathrm{id}$.

On prendra garde qu'on ne peut pas, en général, échanger l'ordre des facteurs d'un produit. Soit par exemple $f = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ la permutation de l'ensemble $\{1,2,3\}$ qui

échange 1 et 2 et $g = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$ celle qui échange 2 et 3. On a $f \circ g(1) = f(1) = 2$ mais $g \circ f(1) = g(2) = 3$. Par conséquent, $f \circ g \neq g \circ f$.

Exercices. — 1) Soit $D_{n,k}$ le nombre de permutations de $\{1,\dots,n\}$ qui ont exactement k points fixes (*dérangements*).

a) Montrer que $D_{n,0} + \cdots + D_{n,n} = n!$.

b) Montrer que $D_{n,k} = \mathrm{C}_n^k D_{n-k,0}$

c) En déduire que

$$\frac{1}{n!} D_{n,0} = 1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n \frac{1}{n!}.$$

B. Transpositions ; un algorithme de tri

Un des aspects intéressants des groupes de permutations est qu'on peut visualiser une permutation en étudiant sur *action* sur les éléments de F_n.

On appelle par exemple *transposition* une permutation qui laisse fixe tous les éléments de F_n, sauf deux qu'elle échange. On note $(a\,,\,b)$ la transposition qui échange a et b. Notons τ cette transposition. On a $\tau(a) = b$, $\tau(b) = a$; par suite, $\tau^2(a) = \tau(b) = a$ et $\tau^2(b) = \tau(a) = b$. En outre, si $i \notin \{a, b\}$, $\tau(i) = i$, donc $\tau^2(i) = \tau(i) = i$.

THÉORÈME. — *Toute permutation est composée de transpositions. Plus précisément, on peut écrire toute permutation comme composée de transpositions de la forme* $(i\,,\,i+1)$.

Avant de démontrer ce théorème, donnons-en une interprétation informatique : il s'agit de l'algorithme de *tri à bulle*. Cet algorithme fonctionne comme ceci :

– si le premier élément est plus grand que le second, on les échange ;
– dans la liste modifiée, si le second est plus grand que le troisième, on les échange ;
– et ainsi de suite jusqu'à arriver au bout de la ligne.
– À ce moment, on recommence du début, le tout n fois. À la fin, la liste est triée.

Comment ça marche ? Tout bonnement, à la fin du premier passage, le plus grand élément se retrouve à la fin de la liste. En effet, une fois qu'on est tombé dessus, on le transporte de proche en proche jusqu'à la fin. Au second passage, le deuxième plus grand subit le même sort, mais s'arrête en avant-dernière position. Etc, et au dernier passage, la liste est triée.

Quel est le lien avec les permutations ? Voyons une liste non triée comme la permutation des rangs : $\sigma(1)$ est le rang du premier élément de la liste, etc. Échanger les deux premiers éléments de la liste revient à considérer une nouvelle permutation, disons τ, qui applique 1 sur $\sigma(2)$, 2 sur $\sigma(1)$, et un entier $i > 2$ sur $\sigma(i)$. On a ainsi $\tau = \sigma \circ (1\,,\,2)$. De même, échanger les éléments de la liste en position i et j revient à remplacer une permutation σ par la permutation $\sigma \circ (i\,,\,j)$.

L'algorithme du tri à bulle part d'une permutation σ et la remplace par une permutation σ' de la forme $\sigma \circ \tau_1 \circ \cdots \circ \tau_r$, où r est le nombre d'échanges effectués et les τ_i sont des transpositions de la forme $(i\,,\,i+1)$. Puisque la liste est triée, $\sigma' = \mathrm{id}$, d'où

$$\sigma = \tau_r \circ \tau_{r-1} \circ \cdots \circ \tau_1,$$

comme on le voit en faisant les échanges à l'envers.

C. Signature ; le jeu de taquin

Soit σ une permutation de $\{1,\dots,n\}$. On appelle inversion de σ un couple (i,j) d'entiers appartenant à $\{1,\dots,n\}$ tels que $i<j$ et $\sigma(j)>\sigma(i)$. Notons $i(\sigma)$ le nombre d'inversions de la permuation σ. On appelle signature de σ le nombre $\varepsilon(\sigma)=(-1)^{i(\sigma)}$: c'est un entier, égal à -1 si $i(\sigma)$ est impair et à 1 sinon. On dira que σ est paire ou impaire suivant que $i(\sigma)$ est pair ou impair.

THÉORÈME. — a) *L'identité est la seule permutation qui n'ait pas d'inversion ;*

b) *si σ est une transposition de la forme $(i\,,\,i+1)$, on a $n(\sigma)=1$;*

c) *si σ est une permutation de $\{1,\dots,n\}$ et τ une transposition de la forme $(k\,,\,k+1)$, on a $\varepsilon(\sigma\circ\tau)=-\varepsilon(\sigma)$;*

d) *si σ et τ sont deux permutations de $\{1,\dots,n\}$, on a $\varepsilon(\sigma\circ\tau)=\varepsilon(\sigma)\varepsilon(\tau)$.*

C'est un théorème un peu délicat.

a) Il est clair que l'identité n'a pas d'inversion. Inversement, supposons que l'on ait $\sigma(i)<\sigma(j)$ pour tout couple (i,j) tel que $i<j$. Alors, $\sigma(1)$ est strictement inférieur aux $n-1$ entiers $\sigma(2),\dots,\sigma(n)$; nécessairement $\sigma(1)=1$. Ensuite, $\sigma(2)$ est strictement inférieur à $n-2$ entiers distincts appartenant à $\{2,\dots,n\}$; là encore, la seule possibilité est $\sigma(2)=2$. On continue ainsi de suite (il faudrait faire une récurrence), d'où $\sigma=\mathrm{id}$.

b) Supposons $\sigma=(k\,,\,k+1)$. Il n'y a pas d'inversion (i,j) si ni i ni j n'appartient à $\{k,k+1\}$. Un couple (i,k) ou $(i,k+1)$ avec $i<k$ n'est pas une inversion, pas plus qu'un couple (k,j) ou $(k+1,j)$ avec $j>k+1$. Par contre le couple $(k,k+1)$ est une inversion. On a donc $n(\sigma)=1$.

c) Nous allons ainsi déterminer le nombre d'inversions de la permutation $\sigma'=\sigma\circ(k\,,\,k+1)$ en fonction du nombre d'inversions de σ.

On a déjà expliqué à propos du tri à bulle que σ' applique un entiers i distinct de k et $k+1$ sur $\sigma(i)$. On a en outre $\sigma'(k)=\sigma(k+1)$ et $\sigma'(k+1)=\sigma(k)$.

Si $i<k$ et $j>k+1$, (i,j) est une inversion de σ si et seulement si c'en est une de σ'.

Si $i<k$, (i,k) est une inversion de σ si et seulement si $(i,k+1)$ en est une de σ' ; $(i,k+1)$ est une inversion de σ si et seulement si (i,k) est une inversion de σ'.

Si $j>k+1$, (k,j) est une inversion de σ si et seulement si $(k+1,j)$ est une inversion de σ' ; $(k+1,j)$ est une inversion de σ si et seulement si (k,j) est une inversion de σ.

Étudions ce qui se passe pour la dernière inversion possible, $(k,k+1)$: si $\sigma(k)<\sigma(k+1)$, $(k,k+1)$ n'est pas une inversion de σ mais en est une de σ', tandis que si $\sigma(k)>\sigma(k+1)$, $(k,k+1)$ est une inversion de σ mais pas de σ'.

En définitive, cela démontre que $i(\sigma')=i(\sigma)+1$ si $\sigma(k)<\sigma(k+1)$, et $i(\sigma')=i(\sigma)-1$ si $\sigma(k)>\sigma(k+1)$. En particulier, $\varepsilon(\sigma')=-\varepsilon(\sigma)$, d'où le théorème.

d) On sait qu'on peut écrire $\tau=\tau_1\dots\tau_r$, où les τ_i sont des transpositions de la forme $(k\,,\,k+1)$. Grâce au résultat précédent, on a, par récurrence sur r, les relations $\varepsilon(\tau)=(-1)^r$ et $\varepsilon(\sigma\tau)=(-1)^r\varepsilon(\sigma)$. Par suite, $\varepsilon(\sigma\tau)=\varepsilon(\sigma)\varepsilon(\tau)$, comme il fallait démontrer.

Voici quelques conséquences importantes :

a) *Une permutation et son inverse ont même signature.* En effet, si σ est une permutation,

$$\varepsilon(\sigma^{-1})\varepsilon(\sigma)=\varepsilon(\sigma^{-1}\sigma)=\varepsilon(\mathrm{id})=1,$$

ce qui impose $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

b) *La signature d'une transposition est égale à* -1. Soit en effet $i < j$ deux entiers et soit τ la transposition $(i\,,\,j)$. Soit σ une permutation telle que $\sigma(1) = i$ et $\sigma(2) = j$, les autres valeurs n'ayant pas d'importance. Les permutations $\tau_1 = \sigma \circ (1\,,2)$ et $\tau_2 = (i\,,\,j) \circ \sigma$ appliquent 1 sur j, 2 sur i, et k sur $\sigma(k)$, si $k \geqslant 3$. Elles sont donc égales. En particulier, $\varepsilon(\tau_1) = \varepsilon(\tau_2)$, d'où

$$\varepsilon(\sigma)\varepsilon((1\,,2)) = \varepsilon((i\,,\,j))\varepsilon(\sigma)$$

et l'égalité $\varepsilon((i\,,\,j)) = -1$ en simplifiant par $\varepsilon(\sigma)$.

c) *Si* $\tau_1, \ldots, \tau_r$ *sont des transpositions et* $\sigma = \tau_1 \ldots \tau_r$*, on a* $\varepsilon(\sigma) = (-1)^r$. Cela montre en particulier que *la parité du nombre de transpositions qu'il faut utiliser pour écrire une permutation donnée ne dépend pas de l'écriture choisie.*

Voici enfin une application au jeu de taquin qu'avait inventé Sam Lloyd. On associe à une position une permutation de $\{1, \ldots, 16\}$, où les nombres 1 à 15 représentent les pièces tandis que 16 représente la case noire. Les mouvements autorisés sont les transpositions de la forme $(i\,,16)$. Supposons avoir résolu le jeu en r coups. La signature de la permutation obtenue est alors $(-1)^r$. Mais dans le jeu de Sam Lloyd, la case vide est en bas à gauche au début et à la fin. Superposons un damier au jeu de taquin ; alors, lors d'un mouvement élémentaire, la case vide passe d'une case blanche à une case noire, et réciproquement. Comme il faut être revenu à une case de même couleur, le nombre de coups nécessaires est pair et les seules permutations qu'on peut obtenir en jouant au taquin sont des permutations paires.

Sam Lloyd avait promis 1000 dollars pour qui parviendrait à échanger les cases 14 et 15. Comme la transposition $(14\,,15)$ est de signature -1, c'est impossible !

Exercices. — 1) Calculer la signature de la permutation qui applique 1 sur 2, 2 sur 3, etc., $n-1$ sur n et n sur 1.

2) a) Dans le jeu de taquin, est-il possible, à partir de la position de départ usuelle (case vide en bas à droite), de ranger les cases dans l'ordre croissant, la case vide étant en haut à gauche.

b) Montrer que toute permutation de $\{1, \ldots, n\}$ est composée de permutations de la forme $(i\,,\,n)$.

c) Au taquin, montrer qu'il est possible d'atteindre n'importe quelle position dont la permutation associée est paire.

3) Soit σ une permutation de $\{1, \ldots, n\}$, écrite comme composée de r transpositions de la forme $(i\,,\,i+1)$.

a) Montrer que le nombre d'inversions de σ est inférieur ou égal à r.

b) Au cours d'un tri à bulle, quelle liste requiert le plus d'opérations pour être rangée ?

D. Orbites, ordre d'une permutation

Il n'y a qu'un nombre fini d'éléments dans le groupe S_n. Par conséquent, dans la suite infinie $f, f^2, \ldots$, au moins deux termes se répètent et il existe deux entiers i et j, avec $i < j$, tels que $f^i = f^j$. Alors, $f^i = f^i \circ f^{j-i}$, d'où $f^{j-i} = \mathrm{id}$ en simplifiant par f^i. Cela montre qu'il existe des entiers $p > 0$ tels que $f^p = \mathrm{id}$; soit d le plus petit d'entre eux. Cette entier est appelé l'*ordre* de la permutation.

Comme $f^d = \mathrm{id}$, on a $f^{kd} = f^d \circ \cdots \circ f^d = \mathrm{id}$ pour tout entier $k > 0$, mais aussi pour tout entier < 0. Soit p un entier tel que $f^p = \mathrm{id}$. Notons $p = dq + r$ la division euclidienne de p par d. On a $f^r = f^{p-dq} = f^p \circ (f^d)^{-q} = \mathrm{id}$. Commme d est le plus petit entier > 0 tel que $f^d = \mathrm{id}$ et que l'on a $0 \leqslant r < d$, il vient nécessairement $r = 0$. Autrement dit, p est multiple de d.

Nous avons ainsi montré que les entiers p tels que $f^p = \mathrm{id}$ sont exactement les multiples de l'ordre de la permutation f.

Soit σ une permutation de F_n. Si $a \in F_n$, les éléments $a, \sigma(a), \sigma^2(a), \ldots$ forment une partie O_a de $\{1, \ldots, n\}$ qu'on appelle l'orbite de a.

Supposons que b soit dans l'orbite de a ; il existe alors $i \geqslant 0$ tel que $b = \sigma^i(a)$. On a alors $a = \sigma^{-i}(b)$; si r est le reste de la division euclidienne de $-i$ par d (l'ordre de σ), on a $\sigma^{-i} = \sigma^r$, d'où $a = \sigma^r(b)$ et a appartient à l'orbite de b. Enfin, si b appartient à l'orbite de a et si c appartient à l'orbite de a, il existe des entiers i et j tels que $b = \sigma^i(a)$ et $c = \sigma^j(b)$. Alors, $c = \sigma^{i+j}(a)$ ce qui montre que c appartient à l'orbite de a. Ces raisonnements montrent que la relation « b appartient à l'orbite de a » est une relation d'équivalence. Les classes d'équivalence pour cette relation définissent une partition de l'ensemble $\{1, \ldots, n\}$ qu'on appelle *décomposition en orbites* de la permutation σ.

Soit encore σ une permutation et soit $a \in F_n$. Comme il y a une infinité d'entiers positifs mais seulement n éléments dans F_n, les éléments de la liste $\{a, \sigma(a), \sigma^2(a), \ldots\}$ doivent se répéter et il existe deux entiers $i < j$ tels que $\sigma^i(a) = \sigma^j(a)$. Écrivons $j = i + p$; on a $\sigma^i(a) = \sigma^i(\sigma^p(a))$, donc $a = \sigma^p(a)$ car σ^i, étant bijective, est injective. Soit alors p le plus petit entier > 0 tel que $\sigma^p(a) = a$. Sur l'orbite de a, σ se comporte très simplement : elle applique a sur $\sigma(a)$, $\sigma(a)$ sur $\sigma^2(a)$, etc., puis $\sigma^{p-1}(a)$ sur $a = \sigma^p(a)$. Autrement dit, σ permute circulairement les éléments de O_a. La longueur de l'orbite O_a est le plus petit entier $p > 0$ tel que $\sigma^p(a) = a$.

Voyons maintenant comment ces notions permettent de redémontrer la formule d'Euler selon laquelle $a^{\varphi(n)} \equiv 1 \pmod{n}$ si a et n sont des entiers premiers entre eux.

Soit n un entier $\geqslant 2$ et soit Φ l'ensemble des entiers de $\{1, \ldots, n\}$ qui sont premiers à n. On a $\operatorname{card} \Phi = \varphi(n)$. Soit $a \in \Phi$ et soit f l'application de $\{1, \ldots, n\}$ dans lui-même qui à x associe le reste de la division euclidienne de ax par n. On a déjà démontré que c'est une permutation. Si $x \in \Phi$, c'est-à-dire que x et n sont premiers entre eux, montrons que $f(x)$ appartient à Φ. Écrivons donc la division euclidienne de ax par n : si q est le quotient, on a $ax = qn + f(x)$. Par suite, un diviseur commun d à n et $f(x)$ divise ax. Comme d divise n, d est premier avec a. D'après le théorème de Gauss, d divise donc x : c'est un diviseur commun à x et n, d'où $d = 1$.

La restriction de f à l'ensemble Φ est alors une application de Φ dans lui-même ; elle est injective car f est injective. Comme Φ est un ensemble fini, c'est une permutation g de Φ.

Quelles sont les orbites de g ? Soit $x \in \Phi$; son orbite est l'ensemble $\{x, g(x), \ldots, g^{r-1}(x)\}$, où r est le plus petit entier > 0 tel que $g^r(x) = x$. Or, $g(x) \equiv ax \pmod{n}$, et par récurrence, $g^r(x) \equiv a^r x \pmod{n}$. La relation $g^r(x) = x$ équivaut alors à $a^r x \equiv x \pmod{n}$. Comme x est premier à n, on peut simplifier par x (théorème de Gauss), donc cette relation équivaut à $a^r \equiv 1 \pmod{n}$. Inversement, si $a^r \equiv 1 \pmod{n}$, on a $g^r(x) = x$

pour tout $x \in \Phi$. Autrement dit, le cardinal de l'orbite de x est le plus petit entier $r > 0$ tel que $a^r \equiv 1 \pmod{n}$. Cela montre que toutes les orbites ont même cardinal r ; si t est le nombre d'orbites, on a alors $tr = \operatorname{card}\Phi = \varphi(n)$. Puisque $a^r \equiv 1 \pmod{n}$, on a, $a^{tr} \equiv (a^r)^t \equiv 1 \pmod{n}$, et donc $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Exercices. — 1) On appelle *type* d'une permutation la liste des cardinaux de ses orbites, rangée en ordre croissant.

a) Pour chaque valeur de n telle que $2 \leqslant n \leqslant 7$, faire la liste des types possibles d'une permutation de $\{1,\dots,n\}$. Combien y a-t-il de permutations d'un type donné ?

b) Soit σ une permutation de l'ensemble $\{1,\dots,n\}$. Montrer que l'ordre de σ est le ppcm des cardinaux des orbites de σ. L'ordre d'une permutation ne dépend donc que de son type.

c) Si $2 \leqslant n \leqslant 7$, combien y a-t-il de permutations de chaque ordre ?

2) Soit r un entier compris entre 2 et r et soit $a_1,\dots,a_r$ des éléments distincts de $\{1,\dots,n\}$. Soit σ la permutation qui applique a_1 sur a_2, a_2 sur a_3, etc., a_{r-1} sur a_r, a_r sur a_1 et qui fixe tous les autres éléments de $\{1,\dots,n\}$.

On note parfois $\sigma = (a_1\,, a_2\,, \dots\,, a_r)$ et on dit que c'est un cycle de longueur r.

a) Quelles sont les orbites de σ ?

b) Calculer la signature du cycle $(1,\dots,r)$.

c) Montrer qu'il existe une permutation $a \in S_n$ telle que $a(i) = a_i$ pour $1 \leqslant i \leqslant r$. Montrer que $a \circ (1,\dots,r) = \sigma \circ a$. En déduire que la signature de σ est égale à $(-1)^{r+1}$.

d) Soit σ une permutation de $\{1,\dots,n\}$; soit t le nombre d'orbites de σ. Montrer qu'il existe t cycles $\sigma_1,\dots,\sigma_t$ tels que $\sigma = \sigma_1 \dots \sigma_t$.

En déduire que $\varepsilon(\sigma) = (-1)^{n-t}$, où t est le nombre d'orbites de σ.

3) Soit σ la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 8 & 5 & 2 & 9 & 10 & 6 & 3 & 1 & 7 \end{pmatrix}.$$

a) Déterminer ses orbites.

b) Quel est l'ordre de σ ; calculer σ^{1000}.

c) Quelle est la signature de σ ?