ARITHMÉTIQUE ET ALGÈBRE

Cours à l'Université de Rennes 1 (2003–2004)

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

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 en particulier 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.

a) un (1) est un entier ;
b) tout entier a un successeur ;
c) tout entier autre que un 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 1, il vérifie $n \geqslant 2$ 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 1 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 $n = 1$ (*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 pourrait commencer par $n = 0$, 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 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 *admettrons* que les entiers naïfs sont un objet mathématique et satisfont les 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 banquaire 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, $\tau_{\text{a}} = 4{,}5/100 = 0{,}045$. Si le capital dû au 1$^{\text{er}}$ janvier est C, les intérêts accumulés en un an seront de $\tau_{\text{a}} \times C$, d'où un capital dû au 31 décembre de $(1+\tau_{\text{a}})C$. Calculons mensuellement. Au 1$^{\text{er}}$ février, les intérêts accumulés s'élèvent à $\tau_{\text{m}}C$, d'où un capital dû de $(1+\tau_{\text{m}})C$. Un mois plus tard, le capital dû est multiplié par $(1+\tau_{\text{m}})$, donc il vaut $(1+\tau_{\text{m}})^2C$, et finalement, au bout d'un an, le capital dû est de $(1+\tau_{\text{m}})^{12}C$. (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

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

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

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

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

4) (*suite*) Montrer par récurrence sur n que si $x_1, \ldots, x_{2^n}$ sont des réels positifs,

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

5) (*suite*) Soit $N \geqslant 2$ et soit $x_1, \ldots, x_N$ 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.

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

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

7*) 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. 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 ?)

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 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 $n=1$, on pose $m+1=s(m)$. Si n est un entier différent de 1, 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 $\mathscr{P}(1)$ s'écrit : pour tout entier m, on a $m+1=1+m$. Nous allons la démontrer par récurrence sur m. Pour $m=1$, on doit démontrer $1+1=1+1$, ce qui est vrai. Supposons alors que $m=1+m$; on a alors $1+s(m)=s(1+m)$ par construction. Par l'hypothèse de récurrence, $1+m=m+1=s(m)$, donc $s(1+m)=s(s(m))=s(m)+1$ et finalement $1+s(m)=s(m)+1$, ce qui montre la propriété pour le successeur de m. Par récurrence, la propriété $\mathscr{P}(1)$ est 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 $m=1$, on a $1+s(n)=s(n)+1$ car $\mathscr{P}(1)$ 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.

Exercice. — 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 $u_n = a^n u_0$ pour tout entier n.

Revenons au problème des prêts banquaires. 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) Montrer par récurrence sur n les formules

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

Que vaut, si n est impair, la somme $1 + 3 + 5 + \cdots + n$?
5) 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 $C = 1$).
6) 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.
7) 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.)
8) 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.)

§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. Il est toujours bon d'avoir des principes

Le cardinal d'un ensemble fini est un entier. Deux ensembles finis qui sont en bijection ont même cardinal. On note $\operatorname{card} X$ ou $|X|$ le cardinal de l'ensemble X. Le cardinal de l'ensemble vide est 0, celui d'un singleton 1, etc.

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.

Si X et Y sont deux ensembles finis, le cardinal de l'ensemble $X\times Y$ 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 $\operatorname{card}(X\times Y) = \operatorname{card} X\times\operatorname{card} Y$.

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 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 $f\colon X\to Y$ 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) 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.
2) 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 ?
3) 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 ?
4) 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.
5) 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.
6) 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...*)
7*) 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.

B. 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

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

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),

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

chaque 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*

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

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) 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.)

2) 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 ?
3) Démontrer la relation $C_n^p = C_{n-1}^{p-1} + C_{n-1}^p$ pour $n > p \geqslant 1$ en utilisant la formule qui calcule C_n^p à l'aide de factorielles.
4) Inversement, à l'aide de cette identité, démontrer par récurrence la formule qui calcule C_n^p.
5) Démontrer de deux façons la formule $C_n^p = \dfrac{n}{p} C_{n-1}^{p-1}$ pour $n \geqslant p \geqslant 1$.
6) Démontrer de deux façons que $C_n^p = C_n^{n-p}$.
7) À l'aide de la formule du binôme, démontrer que

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

8) On pose

$$F_n = \sum_{p \leqslant n/2} C_{n-p}^p = C_n^0 + C_{n-1}^1 + C_{n-2}^2 + \dots$$

(Le dernier terme est C_p^p si $n = 2p$ est pair, et C_{p+1}^p si $n = 2p+1$ est impair.) Calculer F_0, F_1, F_2,..., F_5. Montrer que $F_{n+1} = F_n + F_{n-1}$ (*suite de Fibonacci*).
9) Une combinaison avec répétition de p éléments parmi n est une liste de p éléments de $\{1,\dots,n\}$, non nécessairement distincts, et où l'ordre n'intervient pas. On note R_n^p leur nombre. 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 $n \geqslant 1$, $p \geqslant 1$. En déduire par récurrence que $R_n^p = C_{n+p-1}^p$.
10) (*autre méthode*) On associe à une partie à $n-1$ éléments de $\{1,\dots,n+p-1\}$ une combinaison avec répétition de la façon suivante : si cette partie est formée de $n-1$ entiers $x_1 < \cdots < x_{n-1}$, 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.
11) Un ordinateur (par exemple) ne sait calculer que le produit de deux facteurs et on s'intéresse au nombre de façons K_n d'introduire des parenthèses dans le produit $x_1 x_2 \dots x_n$ de sorte à pouvoir le calculer. Si $n = 2$, c'est un produit de deux facteurs, donc $K_2 = 1$, mais on a $K_3 = 2$ correspondant aux parenthésages $x_1(x_2 x_3)$ et $(x_1 x_2)x_3$, de même que $K_4 = 5$ avec les parenthésages

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

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

$$K_n = \sum_{p=1}^{n-1} K_p K_{n-p}.$$

12*) (*suite*) Montrer que

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

En développant $(1+x)^{2n} = (1+x)^n (1+x)^n$, montrer que

$$C_{2n}^n = \sum_{p=0}^{n} \left(C_n^p\right)^2.$$

13) Soit $D_{n,k}$ le nombre de permutations de $\{1,\dots,n\}$ qui ont exactement k points fixes (*dérangements*). Montrer que $D_{n,0} + \cdots + D_{n,n} = n!$. Montrer que $D_{n,k} = C_n^k D_{n-k,0}$ En déduire que

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

C. Probabilités

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 événéments définies 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) Quelle est la probabilité d'avoir deux dés identiques en lançant deux dés ? en lançant trois dés ?

2) 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 ?

3) 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 ?

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

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

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

7) Soit p une probabilité 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. Le théorème de la division euclidienne

Soit $\mathbf{Z}$ l'ensemble des entiers relatifs. Sur cet ensemble, on a une addition et une multiplication. L'addition est associative : $(a+b)+c = a+(b+c)$, pour a, b, $c \in \mathbf{Z}$. Comme $0+a = a+0 = a$ pour tout $a \in \mathbf{Z}$, on dit que 0 est un élément neutre pour l'addition. De plus, tout élément $a \in \mathbf{Z}$ a un opposé $-a$ tel que $a+(-a) = (-a)+a = 0$. On dit alors que $(\mathbf{Z}, +, 0)$ est un groupe. Comme $a+b = b+a$ pour a et b dans $\mathbf{Z}$, c'est même un groupe commutatif.

La multiplication est associative et est distributive par rapport à l'addition : si a, b, $c \in \mathbf{Z}$, $a(b+c) = ab+ac$. Elle est aussi commutative : $ab = ba$ si a et $b \in \mathbf{Z}$. Enfin, 1 est un élément neutre puisque $1a = a1 = a$ pour tout entier a.

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

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) 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 $-\frac{1}{2}|b| < r \leqslant \frac{1}{2}|b|$.
3) 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 ?
4) 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 $a^2 + b^2 = 8123$?
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 ?

B. 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 $c_0, \ldots, c_k \in \{0, \ldots, b-1\}$ 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 $c_0, \ldots, c_k$ 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 $n = \overline{c_k c_{k-1} \ldots c_0}$, voire $n = \overline{c_k c_{k-1} \ldots c_0}^{(b)}$ 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 $0, \ldots, b-1$ 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) Quel sont les entiers qui s'écrivent avec exactement m chiffres en base b ? Combien y en a-t-il ?
4) Dans une certaine base, un entier s'écrit $\overline{1254}$ et son double $\overline{2541}$. Quel est cet entier et quelle est la base ?
5) Calculer le produit 123456789 par 9 en moins de 5 secondes.
6) 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 ?

C. 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) 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 ?
2) Soit n un entier dont l'écriture décimale est $\overline{abc}$. Montrer que $n \equiv 2a+3b+c \pmod{7}$.
3) Quels sont les trois derniers chiffres de $7^{100}-3^{100}$?
4) 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.
5) Imaginer une preuve par 9 pour les divisions euclidiennes. L'expérimenter sur un exemple.
6) Que pourrait être la « preuve par $b-1$ » en base b ?

D. 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 $\mathrm{pgcd}(a,b)$.

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 $d = \delta$.

Cette démonstration n'est pas constructive : elle ne permet pas de déterminer effectivement, en pratique, des entiers u et v tels que $\mathrm{pgcd}(a,b) = au + bv$. 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 $u_n = \mathrm{pgcd}(a,b)$.

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 $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$ 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 $\text{pgcd}(u_{n+1}, u_{n+2}) = \text{pgcd}(u_n, u_{n+1})$ pour tout entier n (au moins tant que l'algorithme ne s'arrête pas), d'où par récurrence $\text{pgcd}(u_n, u_{n+1}) = \text{pgcd}(u_0, u_1) = \text{pgcd}(a, b)$.

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

Pour déterminer les coefficients u et v du théorème de Bézout, il y a une variante de l'algorithme d'Euclide.

ALGORITHME D'EUCLIDE (ÉTENDU). — *Soit a et b deux entiers strictement positifs. On part de la matrice $\left(\begin{smallmatrix} a & 1 & 0 \\ b & 0 & 1 \end{smallmatrix}\right)$ à deux lignes et 3 colonnes.*

À chaque étape, on effectue les opérations suivantes : $L_1 \to L_1 - qL_2$, puis $L_2 \leftrightarrow L_1$, où q est le quotient de la division euclidiene du premier coefficient de la première ligne par le premier coefficient de la seconde ligne.

L'algorithme s'arrête lorsque le premier coefficient de la seconde ligne est nul. Si la première ligne est alors (d, u, v), on a $d = \text{pgcd}(a, b) = au + bv$.

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

$$\begin{pmatrix} 414 & 1 & 0 \\ 598 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 598 & 0 & 1 \\ 414 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 414 & 1 & 0 \\ 184 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 184 & -1 & 1 \\ 46 & 3 & -2 \end{pmatrix}, \quad \begin{pmatrix} 46 & 3 & -2 \\ 0 & -13 & 9 \end{pmatrix}.$$

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.

Dans cet algorithme, on manipule une suite de matrices 2×3 et pour chacune de ces matrices, on peut calculer 3 déterminants 2×2, obtenus en ôtant une des trois colonnes. Notons D_i le déterminant de la matrice dont on a enlevé la colonne i.

Au début, la matrice vaut $\left(\begin{smallmatrix} a & 1 & 0 \\ b & 0 & 1 \end{smallmatrix}\right)$, d'où $D_1 = 1$, $D_2 = a$ et $D_3 = -b$.

À chaque étape, on effectue une combinaison linéaire ($L_1 \to L_1 - qL_2$) qui ne change pas les déterminants et l'échange des deux lignes L_1 et L_2 qui change les déterminants en leur opposé. Au bout de n étapes, les déterminants sont donc multipliés par un même signe ε. (En fait, $\varepsilon = (-1)^n$.)

À la fin de l'algorithme, la matrice est de la forme $\left(\begin{smallmatrix} d & u & v \\ 0 & x & y \end{smallmatrix}\right)$. Par suite, $D_1 = uy - vx$, $D_2 = dy$ et $D_3 = dx$. On a donc $uy + vx = \varepsilon$, $dy = \varepsilon a$ et $dx = -\varepsilon b$. Finalement, $a = \varepsilon^2 a = \varepsilon dy$, $b = (-\varepsilon)^2 b = -\varepsilon dx$ et

$$au + bv = \varepsilon dyu - \varepsilon dxv = \varepsilon d(uy - xv) = \varepsilon^2 d = d.$$

Exercices. — 1) 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 ?

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

3) On définit la suite de Fibonacci par $F_0 = 0$, $F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$. Montrer que l'on a

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

4) Montrer que $F_{n+1}F_{n-1} - (F_n)^2 = (-1)^n$ pour tout n.
5) Montrer que $F_{n+m} = F_{n+1}F_m + F_nF_{m-1}$.
6) Montrer que l'on a, pour $m < n$, $\mathrm{pgcd}(F_n, F_m) = \mathrm{pgcd}(F_{n-m}, F_m)$ et $\mathrm{pgcd}(n, m) = \mathrm{pgcd}(n - m, m)$. En déduire par récurrence sur $\max(m, n)$ que la relation $\mathrm{pgcd}(F_n, F_m) = F_{\mathrm{pgcd}(n,m)}$.
7) 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 $((1+\sqrt{5})/2)^n/\sqrt{5}$.

§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

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

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, $p_1 < \cdots < p_s$.

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 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.)
2) Combien y a-t-il de 0 à la fin du développement décimal de 1000! ? Vérifier avec MAPLE.
3) Si tous les facteurs premiers p d'un entier n vérifient $p \equiv 1 \pmod 4$, montrer que l'on a $n \equiv 1 \pmod 4$. 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 $4n+3$.
4) Montrer de même qu'il existe une infinité de nombres premiers de la forme $6n+5$.
5) Montrer qu'aucun des entiers $n!+2,\dots,n!+n$ n'est un nombre premier.
6) 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*).
7) 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 $u_n = a_n/2^{2n-1}b_n$.
8) 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. 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 $p_1,\dots,p_r$. Considérons l'entier $n = p_1 \dots p_r + 1$; on a $n > 1$. Soit p un diviseur premier de n. Par hypothèse, p est l'un des p_i. Par suite, p divise $n - p_1 \dots p_r = 1$, ce qui est absurde.

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

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

D. Le théorème de Tchebychev et le postulat de Bertrand

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

Problème. — 1) Posons $N = \binom{2n}{n}$. Démontrer que l'on a

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

2) Soit p un nombre premier tel que $n < p \leqslant 2n$. Montrer que p divise N.
3) Montrer que $\pi(2n)\log(2n) \geqslant n\log 2$.
4) Soit p un nombre premier. Montrer que $v_p(N) \leqslant \log(2n)/\log p$.
5) Montrer que $(\pi(2n) - \pi(n))\log n \leqslant 2n\log 2$.
6) Montrer que pour tout entier k,
$$k\pi(2^k) \leqslant 3 \cdot 2^k.$$
7) Montrer que pour tout entier $x \geqslant 1$, on a l'inégalité
$$\frac{\log 2}{4}\,\frac{x}{\log x} \leqslant \pi(x) \leqslant 6\log 2\,\frac{x}{\log x}.$$

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.

Problème. — 1) On pose $N = \binom{2n+1}{n}$. Montrer que $N \leqslant 4^n$.
2) Montrer que pour tout entier m, le produit des nombres premiers p tels que $n+1 < p \leqslant 2m+1$ divise N.
3) Montrer par récurrence sur n que l'on a

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

4) Soit p un facteur premier de N tel que $p \leqslant n$. Montrer que $p < 2n/3$.
5) 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.
6) Supposons par l'absurde qu'il n'existe pas de nombre premier p tel que $n < p < 2n$. Montrer que $N \leqslant 2^{4n/3}(2n)^{\sqrt{2n}}$.
7) (*suite*) En déduire que $\log(x)/x \geqslant 1/6$, où $x = \sqrt{2n}$, puis que $x \leqslant 18$. En déduire que $n \leqslant 162$.
8) Montrer (à la main) que pour tout entier $n \leqslant 1000$, il existe un nombre premier p vérifiant $n < p < 2n$.

§5. Congruences

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

Raconter les nombres de Carmichaël... Exemple : $561 = 3 \times 11 \times 17$.

B. Théorème chinois

On trouve dans un traité chinois (III-V$^{\text{e}}$ 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 $x \equiv b \pmod{n}$.*

Par suite, l'ensemble des solutions du système des deux équations en nombres entiers $x \equiv a \pmod{m}$ et $x \equiv b \pmod{n}$ est l'ensemble des entiers x tels que $x \equiv c \pmod{n}$.

Pour démontrer ce théorème, considérons l'application r de $\{0, \ldots, mn-1\}$ dans $\{0, \ldots, l-1\} \times \{0, \ldots, n-1\}$ qui, à un entier $x \in \{0, \ldots, mn-1\}$, 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*. Cela entraîne Comme ensembles de départ et d'arrivée ont même cardinal, cela entraîne le théorème.

Toutefois, cette démonstration ne permet pas de trouver effectivement un tel entier. Si $x \equiv a \pmod{m}$, on peut écrire $x = a + tm$, avec $t \in \mathbf{Z}$. 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) Trouver tous les entiers compris entre 100 et 1000 qui divisés par 21 aient pour reste 8 et par 17 pour reste 5.
3) 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.

C. Indicateur d'Euler, cryptographie RSA

Soit n un entier $\geqslant 2$. 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 injective. En effet, si $f(x) = f(y)$, on a $ax \equiv ay \pmod{n}$, donc n divise $a(x-y)$. Comme a est premier avec n, n divise $x-y$, d'où $x = y$ car ces deux entiers sont compris entre 0 et $n-1$.

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 alors

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

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 $\varphi(n)$.

Raconter RSA...

Exercices. — 1) Calculer $\varphi(n)$ si n est une puissance d'un nombre premier p.
2) En utilisant le théorème chinois, démontrer que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont des entiers premiers entre eux.
3) Soit n un entier qui est le produit de deux nombres premiers $p \neq q$. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^{\varphi(n)+1} \equiv x \pmod{n}$.

D. Appendice : construction de l'anneau $\mathbf{Z}/m\mathbf{Z}$

Il s'agit de rendre les calculs de congruences modulo un entier m le plus automatique possible. Cela se fait en *définissant* un nouvel anneau, que l'on notera $\mathbf{Z}/m\mathbf{Z}$.

D'abord la définition la plus élémentaire. Posons $R_m = \{0, 1, \ldots, m-1\}$ et introduisons une addition $\oplus$ et une multiplication $\otimes$ sur R_m : $a \oplus b$ et $a \otimes b$ sont les restes de la division euclidienne de $a+b$ et ab par m. Montrons qu'elles munissent R_m d'une structure d'anneau (commmutatif unitaire) :

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

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

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

ce qui montre que $a \oplus (b \oplus c)$ est le reste de la division euclidienne de $a + (b + c)$ par m, car c'est un élément de R_m. De même, $(a \oplus b) \oplus c$ est le reste de la division euclidienne de $(a+b)+c$ par m. 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 m ; pour $a \in R_m$, on a donc $a \oplus 0 = a$.

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

Ainsi, $(R_m, 0, \oplus)$ 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 m, 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 m : la multiplication est associative ;

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

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

En outre, l'application $r : \mathbf{Z} \to R_m$ qui, à un entier n, associe le reste de la division euclidienne de n par m est un *homomorphisme d'anneaux* : elle applique 0 sur 0, 1 sur 1, somme $(+)$ sur somme $(\oplus)$ et produit $(\cdot)$ sur produit $(\oplus)$.

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 m, qui est le représentant dans $\{0, \dots, m-1\}$ de la classe de congruence modulo m, mais plutôt le représentant dans l'intervalle $\{-m/2, \dots, m/2\}$. Ce choix nécessite d'introduire un nouvel ensemble, de refaire la démonstration, alors que toutes les propriétés de R_m proviennent de deux choses :

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

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

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 utile d'adopter une définition plus efficace, plus générale, et plus abstraite : définir R_m comme *l'ensemble des classes d'équivalence pour la relation de congruence modulo m*. La classe d'équivalence d'un entier a est l'ensemble des entiers n qui sont congrus à a modulo m, c'est donc l'ensemble des entiers de la forme $a + km$, 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_m sera noté $\mathbf{Z}_m$, la notation la plus courante en arithmétique est plutôt $\mathbf{Z}/m\mathbf{Z}$.[1]

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