Université Blaise Pascal
U.F.R. Sciences et Technologies
Département de Mathématiques et Informatique

Notes de cours pour

"L'Univers des Nombres"

U.E. libre de deuxième et troisième années des licences scientifiques.
2011-2012

François Dumas

Ces quelques pages ne constituent pas un cours (complet, structuré, rédigé...) mais de simples notes destinées à soutenir le travail collectif et personnel des étudiants (issus de cursus diversifiés) en "fixant le cadre" sur la partie théorique d'un enseignement conçu avant tout pour ses prolongements applicatifs et pratiques, en particulier lors des séances de travaux dirigés et calculs sur machine. Ces notes sont, à la date d'aujourdhui, sous une forme très provisoire et je remercie par avance pour toutes les observations et corrections qui pourraient m'être transmises.

Version du 18 avril 2012

Chapitre 1: les nombres entiers naturels

1 Propriétés de base de l'ensemble $\mathbb{N}$ des entiers naturels

1.1 La définition des entiers naturels

L'ensemble $\mathbb{N}$ des ENTIERS NATURELS est donné par les axiomes de Peano[1]

1) $0 \in \mathbb{N}$,
2) tout $n \in \mathbb{N}$ admet un successeur $s(n)$,
3) si $s(n) = s(m)$, alors $n = m$,
4) il n'existe pas de $n \in \mathbb{N}$ tel que $0 = s(n)$,
5) si $P \subseteq \mathbb{N}$ vérifie $0 \in P$ et $[n \in P \Rightarrow s(n) \in P]$, alors $P = \mathbb{N}$ (axiome d'induction).

L'axiome d'induction est à la base du principe de démonstration par récurrence:

si une propriété dépendant d'un entier naturel n est vraie pour $n = 0$,
et si, chaque fois qu'elle est vraie pour un entier naturel, elle est vraie pour le suivant,
alors elle est vraie pour tous les entiers naturels.

Ces axiomes suffisent à reconstruire tout ce que l'on sait sur $\mathbb{N}$; en particulier les notions fondamentales que sont les opérations d'addition et de multiplication, l'ordre et la division euclidienne.

1.2 Les opérations sur les entiers naturels

les lois $+$ et $\times$ dans $\mathbb{N}$ sont définies par

addition: $[\forall\, n \in \mathbb{N},\ n + 0 = n]$ et $[\forall\, n, m \in \mathbb{N},\ n + s(m) = s(n + m)]$;
multiplication: $[\forall\, n \in \mathbb{N},\ n \times 0 = 0]$ et $[\forall\, n, m \in \mathbb{N},\ n \times s(m) = n \times m + n]$.

Les propriétés algébriques de ces lois s'en déduisent: pour tous $a, b, c \in \mathbb{N}$, on a :

$a + (b + c) = (a + b) + c$, $\quad a + b = b + a$,
$a \times (b \times c) = (a \times b) \times c$, $\quad a \times b = b \times a$,
$a \times (b + c) = a \times b + a \times c$.

1.3 La relation d'ordre sur les entiers naturels

La relation $\leqslant$ est définie de la façon suivante:
si a et b sont deux entiers naturels, on dit que a est inférieur (au sens large) à b, ce que l'on note $a \leqslant b$, lorsqu'il existe $n \in \mathbb{N}$ tel que $a + n = b$.

C'est une relation d'ordre, ce qui signifie qu'elle est:

réflexive [pour tout $a \in \mathbb{N}, a \leqslant a$],
antisymétrique [pour tous $a, b \in \mathbb{N}$, si $a \leqslant b$ et si $b \leqslant a$, alors $a = b$],
transitive [pour tous $a, b, c \in \mathbb{N}$, si $a \leqslant b$ et si $b \leqslant c$, alors $a \leqslant c$].

Elle est est compatible avec $+$ et $\times$, ce qui signifie que:

soient $a, b \in \mathbb{N}$; si $a \leqslant b$, alors pour tout $c \in \mathbb{N}$ on a $a + c \leqslant b + c$ et $a \times c \leqslant b \times c$.

[1] Giuseppe Peano, 1858-1932, mathématicien italien ayant travaillé (entre autres) sur l'axiomatisation de l'arithmétique.

Elle vérifie aussi les propriétés importantes suivantes:

- c'est un ordre **total** [deux entiers naturels a, b quelconques vérifient toujours $a \leqslant b$ ou $b \leqslant a$];
- c'est un **bon ordre** [toute partie non-vide de $\mathbb{N}$ admet un plus petit élément];
- on a la **propriété d'Archimède** [si $a, b \in \mathbb{N}$ avec $b \neq 0$, il existe $n \in \mathbb{N}$ tel que $nb \geqslant a$];
- **toute partie non-vide et majorée de $\mathbb{N}$ admet un plus grand élément.**

1.4 La division euclidenne des entiers naturels

On introduit d'abord les deux notations suivantes:

1) si $a \leqslant b$ avec $a \neq b$, on note $a < b$ (et on dit que a est strictement inférieur à b)

2) si $a \leqslant b$, on note $b - a$ l'entier c tel que $b = a + c$.

Proposition. *Quels que soient a et b dans $\mathbb{N}$, avec $b \neq 0$, il existe q et r uniques dans $\mathbb{N}$ tels que*

$$a = bq + r \quad \textit{et} \quad r < b.$$

Preuve. Pour montrer l'unicité, supposons l'existence de deux couples (q, r) et (q', r') d'entiers naturels satisfaisant aux conditions $a = bq + r$ avec $r < b$, et $a = bq' + r'$ avec $r' < b$. L'ordre étant total, on peut, quitte à échanger les rôles de q et q', supposer que $q \leqslant q'$. Donc $q' = q + (q' - q)$. On tire alors de légalité $bq' + r' = bq + r$ que $b(q' - q) + r' = r$. Ce qui implique que $r' \leqslant r$ et $r - r' = b(q' - q)$. Mais $r - r' < b$ puisque $r < b$ et $r' < b$. Ainsi $b(q' - q) < b$, ce qui ne peut se produire dans $\mathbb{N}$ que si $q' - q = 0$. Par conséquent $q' = q$, et finalement $r = r'$.

Pour montrer l'existence, posons $B = \{k \in \mathbb{N};\ kb \leqslant a\}$. C'est une partie de $\mathbb{N}$ qui est non-vide (car $0 \in B$) et qui est majorée (par a). Donc elle admet un plus grand élément. Notons-le q. Par définition de q, on a: $qb \leqslant a < (q + 1)b$, donc l'entier naturel $r = a - qb$ vérifie $r < b$. □

On reviendra plus loin sur la division euclidienne, en l'étendant aux nombres entiers relatifs.

2 Bases de numération

2.1 Systèmes d'écriture des entiers naturels

Le point qui nous intéresse ici est celui des divers systèmes permettant d'écrire l'infinité des entiers naturels à l'aide d'un nombre fini de signes (les chiffres).

A priori, la succession des entiers naturels est: $0, s(0), s(s(0)), s(s(s(0))), \ldots$

Il devient bien sûr indispensable d'avoir des signes plus brefs pour les noter; l'usage commun est celui des chiffres arabes:

$$0, \quad s(0) = 1, \quad s(s(0)) = s(1) = 2, \quad s(s(s(0))) = s(2) = 3, \ \ldots$$

mais historiquement il y en a d'autres, comme les chiffres romains:

$$\text{pas de zéro, I}, \ s(\text{I}) = \text{II}, \quad s(\text{II}) = \text{III}, \quad s(\text{III}) = \text{IV}, \ \ldots$$

Il est clair qu'on ne peut pas désigner tous les entiers en inventant un nouveau signe pour tout entier non encore symbolisé. Il faut inventer un code permettant, à l'aide d'un nombre pas trop grand de signes, de représenter et de nommer tous les entiers, à la fois de façon NON-AMBIGÜE, CONCISE, et ADAPTÉE aux types de calculs ou de manipulations que l'on vise dans les applications. Historiquement, il y a eu de très nombreux systèmes différents (on pourra sur ce point consulter de façon instructive les ouvrages ou sites web consacrés à l'histoire des mathématiques).

Avant même d'aller plus loin, donnons quelques exemples évidents du principe des BASES DE NUMÉRATION, (dont les justifications seront précisées dans la suite).

a) Le système décimal (de nos dix doigts);
les chiffres sont $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, et l'on note:

$$s(9) = 10,\ s(10) = 11, \ldots,\ s(18) = s(19),\ s(19) = 20,\ s(20) = 21, \ldots$$

Alors tout entier naturel s'écrit de façon unique (on le montrera au théorème suivant) comme la juxtaposition d'une suite finie de chiffres désignant de droite à gauche le chiffre des unités, des dizaines, des centaines,...
Par exemple: $7 \times 10^3 + 4 \times 10^2 + 1 \times 10 + 6 \times 10^0 = 7416$.

b) Le système binaire (des machines lisant le passage ou non d'un courant électrique);
les chiffres sont $0, 1$, et l'on note:

$$s(\overline{0}) = \overline{1},\ s(\overline{1}) = \overline{10},\ s(\overline{10}) = \overline{11},\ s(\overline{11}) = \overline{100},\ s(\overline{100}) = \overline{101},$$
$$s(\overline{101}) = \overline{110},\ s(\overline{110}) = \overline{111},\ s(\overline{111}) = \overline{1000},\ s(\overline{1000}) = \overline{1001}, \ldots$$

De droite à gauche, les chiffres désignent donc le chiffre des unités, des 2-aines, des 2^2-aines, des 2^3-aines,...

On peut bien sûr passer d'un système à l'autre, (la barre servant ici à distinguer les deux écritures); par exemple: $\overline{10010110} = 2^7 + 2^4 + 2^2 + 2^1 = 150 = 10^2 + 5 \times 10$.

c) Un système de base plus grande que dix nécessite l'introduction de chiffres supplémentaires; par exemple en base douze: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \diamondsuit, \heartsuit$. En utilisant encore une barre pour les écritures en base douze et pas de barre pour l'écriture décimale, on a:

$$\overline{0} = 0,\ \overline{1} = 1,\ \overline{2} = 2, \ldots, \overline{9} = 9,\ \overline{\diamondsuit} = 10,\ \overline{\heartsuit} = 11,\ \overline{10} = 12,\ \overline{11} = 13, \ldots$$
$$\overline{258} = 2 \times 144 + 5 \times 12 + 8 = 356, \qquad \overline{1000} = 12^3 = 1728,$$
$$\overline{3\diamondsuit} = 3 \times 12 + 10 = 46, \qquad \overline{1\heartsuit 5} = 1 \times 144 + 11 \times 12 + 5 = 281.$$

2.2 Existence et unicité de la représentation en une base donnée

a) Point de départ. C'est celui que l'on a résumé au début de 1.1. En particulier, on connaît 0; on sait qu'il a un successeur que l'on convient de noter $s(0) = 1$. Par définition de l'addition, on a $s(n) = n + 1$ pour tout $n \in \mathbb{N}$. Par définition de l'ordre, on a $1 > 0$. A ce stade, l'usage de tout autre chiffre serait prématuré et infondé, et les entiers naturels ne peuvent être désignés que par:

$$0,\ 1 = s(0),\ 1 + 1 = s(s(0)),\ 1 + 1 + 1 = s(s(s(0))),\ 1 + 1 + 1 + 1 = s(s(s(s(0)))), \ldots$$

► On convient d'utiliser la notation classique $\mathbb{N}^*$ pour désigner le sous-ensemble de $\mathbb{N}$ formé de tous les entiers naturels qui sont distincts de 0.
► On utilisera aussi la notation $[\![n, m]\!]$ pour désigner, quels que soient $n \leqslant m$ fixés dans $\mathbb{N}$, l'ensemble des entiers naturels a vérifiant $n \leqslant a \leqslant m$.

b) Lemme. *Fixons $b \in \mathbb{N}$ quelconque tel que $b > 1$. Alors:*

$$\textit{pour tout } m \in \mathbb{N}^*, \textit{ il existe } n \in \mathbb{N} \textit{ unique tel que } \ b^n \leqslant m < b^{n+1}.$$

Preuve. Montrons d'abord l'unicité. Supposons donc $b^n \leqslant m < b^{n+1}$ et $b^{n'} \leqslant m < b^{n'+1}$. Alors $b^n \leqslant m < b^{n'+1}$ donc $n < n' + 1$ donc $n \leqslant n'$. De même $n' \leqslant n$, d'où $n = n'$.

Pour montrer maintenant l'existence, considérons l'application $f : \mathbb{N} \to \mathbb{N}^*$ définie par $x \mapsto b^x$. Notons $E = f(\mathbb{N})$ le sous-ensemble de $\mathbb{N}^*$ formé donc de tous les entiers naturels de la forme b^x pour un certain $x \in \mathbb{N}$. Comme $b \neq 0$ et $b \neq 1$, il est clair que si $x \neq y$ dans $\mathbb{N}$, alors

$b^x \neq b^y$ (on dit alors que f est injective). Comme $\mathbb{N}$ est infini, ceci implique que que E est infini. Donc E n'est pas borné. Il en résulte que, pour $m \in \mathbb{N}^*$ quelconque fixé, l'ensemble $A_m = \{x \in \mathbb{N};\ b^x > m\}$ est non-vide. Il possède donc un plus petit élément; soit z. Comme $b^z > m \geqslant 1$, on doit avoir $z \geqslant 1$, et l'on peut poser $z = n+1$ avec $n \in \mathbb{N}$. Donc $b^{n+1} > m$. Par minimalité de z dans A_m, on a $n = z-1 \notin A_m$ c'est-à-dire $b^n \leqslant m$. On conclut que $b^n \leqslant m < b^{n+1}$. □

c) Théorème et définitions. *Fixons* $b \in \mathbb{N}$ *quelconque tel que* $b > 1$. *Alors:*
pour tout $m \in \mathbb{N}^*$, *il existe* $n \in \mathbb{N}$ *unique et une unique suite finie* $(a_0, a_1, \ldots, a_n)$ *d'éléments de* $\mathbb{N}$ *tels que:*

(i) $0 \leqslant a_i < b$ pour tout $0 \leqslant i \leqslant n$; (ii) $a_n \neq 0$; (iii) $m = \sum_{i=0}^{n} a_i b^i$.

► On note alors $m = \overline{a_n \ldots a_0}^b$, et on dit que m est représenté en numération dans la base b.
► L'entier $b > 1$ est donc la BASE de cette numération.
► L'entier $n+1$ est par définition appelé la LONGUEUR de la représentation de m en base b.

En particulier, on a toujours: $b = \overline{10}^b$.

Remarquons que, si l'on veut expliciter les indices dans la suite $(a_0, a_1, \ldots, a_n)$, il faudrait à ce stade les énumérer sous la forme $(a_0, a_1, a_{1+1}, a_{1+1+1}, \ldots, a_n)$.

Preuve. Montrons d'abord l'unicité. Supposons $m = \overline{a_k a_{k-1} \ldots a_0}^b = \overline{c_h c_{h-1} \ldots c_0}^b$.

On montre l'égalité des longueurs h et k. Chaque a_i est $\leqslant b-1$, donc:

$$m = \sum_{i=0}^{k} a_i b^i \leqslant \sum_{i=0}^{k} (b-1) b^i = (b-1) \sum_{i=0}^{k} b^i = b^{k+1} - 1,$$

de sorte que $m < b^{k+1}$. Par ailleurs, on sait que $a_k \neq 0$ c'est-à-dire $a_k \geqslant 1$, donc:

$$m = \sum_{i=0}^{k} a_i b^i \geqslant a_k b^k \geqslant b^k.$$

En résumé, $b^k \leqslant m < b^{k+1}$. De même bien sûr, $b^h \leqslant m < b^{h+1}$. D'où $k = h$ en utilisant l'unicité dans le lemme précédent.

L'égalité de départ $m = \overline{a_k a_{k-1} \ldots a_0}^b = \overline{c_h c_{h-1} \ldots c_0}^b$ se réécrit alors:

$$m = \sum_{i=0}^{k} a_i b^i = \sum_{i=0}^{k} c_i b^i \qquad (\star).$$

Supposons qu'il existe $p_0 \in [\![1, k]\!]$ tel que $a_{p_0} \neq c_{p_0}$. L'ensemble $E = \{p \in [\![1, k]\!];\ a_p \neq c_p\}$ est alors non-vide, donc admet un plus petit élément: soit q.

Premier cas: $0 < q < k$. On réécrit $(\star)$ sous la forme:

$$a_q b^q + \sum_{i=q+1}^{k} a_i b^i = c_q b^q + \sum_{i=q+1}^{k} c_i b^i.$$

En simplifiant par b^q et en posant $A = \sum_{i=q+1}^{k} a_i b^{i-q-1}$ et $C = \sum_{i=q+1}^{k} c_i b^{i-q-1}$, on tire que $a_q + bA = c_q + bC$. Comme $a_q < b$ et $c_q < b$, l'unicité de la division euclidienne dans $\mathbb{N}$ implique $a_q = c_q$. Contredit le fait que $q \in E$.

Deuxième cas: $q = k$. Alors $(\star)$ donne directement $a_q b^q = c_q b^q$ d'où $a_q = c_q$ et la contradiction.

Troisième cas: $q = 0$. On réécrit $(\star)$ sous la forme:

$$a_0 + \sum_{i=1}^{k} a_i b^i = c_0 + \sum_{i=1}^{k} c_i b^i;$$

on obtient encore soit $a_0 = c_0$ lorsque $k = 0$, soit si $k > 0$ une égalité du type $a_0 + bA = c_0 + bC$, et on conclut comme dans le premier cas.

Tous les cas conduisent à une contradiction. C'est donc que l'hypothèse $E \neq \emptyset$ est fausse. On conclut que $a_p = c_p$ pour tout $p \in [\![1, k]\!]$.

• On montre maintenant l'existence de la représentation. On raisonne par récurrence. Si $1 \leqslant m < b$, alors pour $k = 0$ et $a_0 = m$, on a bien $m = \overline{a_0}^b$. Faisons l'hypothèse de récurrence:

(H.R.) jusqu'à un certain rang $p \in \mathbb{N}$, tout $m \in \mathbb{N}$ tel que $b^q \leqslant m < b^{q+1}$ avec $q \leqslant p$ admet une représentation en base b.

Considérons $m \in \mathbb{N}^*$ tel que $b^{p+1} \leqslant m < b^{p+2}$. Par division euclidienne de m par b, il existe $a, a_0 \in \mathbb{N}$ tel que $m = ba + a_0$ et $0 \leqslant a_0 < b$. D'une part alors:

$$ba = m - a_0 \geqslant b^{p+1} - a_0 > b^{p+1} - b = b(b^p - 1),$$

d'où en simplifiant par b on obtient $a > b^p - 1$ et donc $a \geqslant b^p$. D'autre part:

$$ba = m - a_0 \leqslant m < b^{p+2}$$

d'où de même $a < b^{p+1}$. En résumé, $b^p \leqslant a < b^{p+1}$ ce qui permet d'appliquer l'H.R. Il existe donc une suite finie $(\alpha_0, \dots, \alpha_k)$ d'entiers naturels telle que $0 \leqslant \alpha_i < b$ pour tout $i \in [\![1, k]\!]$, telle que $\alpha_k \neq 0$, et telle que $a = \sum_{i=0}^{k} \alpha_i b^i$. Il en résulte que $m = ba + a_0 = a_0 + \sum_{i=0}^{k} \alpha_i b^{i+1}$. En notant $a_{i+1} = \alpha_i$ pour tout $i \in [\![1, k]\!]$, on aboutit à $m = \sum_{j=0}^{k+1} a_j b^j$. On a bien $0 \leqslant a_0 < b$, $0 \leqslant \alpha_i = a_{i+1} < b$ pour tout $i \in [\![1, k]\!]$, et $a_{k+1} = \alpha_k \neq 0$. On a ainsi montré que $m = \overline{a_{k+1} a_k \dots a_0}^b$, ce qui achève la preuve. □

d) Chiffres. Reprenons les données et notations du théorème; pour exprimer effectivement tout $m \in \mathbb{N}^*$ en base b, il faut choisir b symboles, que l'on appelle CHIFFRES, qui représentent les entiers compris entre 0 et $b-1$. Les chiffres 0 et 1 sont communs à toutes les bases. On a toujours $b = \overline{10}^b$.

Comme $b > 1$, la plus petite base possible est $b = 1 + 1$. On appelle deux cet entier, et la numération de base deux est dite BINAIRE. Elle n'utilise que les chiffres 0 et 1.

Si $b = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$, que l'on appelle dix, on introduit les b chiffres dans l'écriture usuelle $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. La numération est dite DÉCIMALE.

On est donc ramené aux exemples et aux considérations de 2.1, qui sont maintenant justifiées.

On convient que: *dans toute la suite, le système décimal sera toujours pris comme référence; en particulier, une écriture "sans barre" sera toujours relative au système décimal.*

2.3 Exemples

1) Exprimer 99 en base 2 et en base 12.

SOLUTION.
$99 = 9 \times 10 + 9 = (2^3+1)(2^3+2) + (2^3+1) = 2^6 + 2^4 + 2^3 + 2 + 2^3 + 1 = 2^6 + 2^5 + 2 + 1 = \overline{1100011}^2$.
$99 = 96 + 3 = 8 \times 12 + 3 = \overline{83}^{12}$.

2) Construire la table d'addition en base 5, et la table de multiplication en base 4.

SOLUTION.

+	1	2	3	4
1	2	3	4	10
2	3	4	10	11
3	4	10	11	12
4	10	11	12	13

×	1	2	3
1	1	2	3
2	2	10	12
3	3	12	21

3) Quels sont les entiers à 3 chiffres qui s'écrivent $\overline{xyz}^7$ en base 7 et $\overline{zyx}^{11}$ en base 11.

SOLUTION. On doit avoir $49x + 7y + z = 121z + 11y + x$ c'est-à-dire $y = 12x - 30z = 6(2x - 5z)$, avec $1 \leqslant x \leqslant 6$, $0 \leqslant y \leqslant 6$ et $1 \leqslant z \leqslant 6$. Les seules solutions sont $y = 0$ (avec alors $x = 5$ et $z = 2$) ou $y = 6$ (et alors $x = 3$ et $z = 1$). En résumé, on obtient $\overline{502}^7 = \overline{205}^{11}$ et $\overline{361}^7 = \overline{163}^{11}$.

4) Déterminer la base b telle que $\overline{46}^b + \overline{53}^b = \overline{132}^b$. Calculer alors $\overline{46}^b \times \overline{53}^b$.

SOLUTION. $\overline{46}^b + \overline{53}^b = \overline{132}^b$ équivaut à $4b+6+5b+3 = b^2+3b+2$, ou encore $(b-7)(b+1) = 0$. Donc $b = 7$.

$(4b+6)(5b+3) = 20b^2+42b+18 = (2b+6)b^2+6bb+2b+4 = 2b^3+12b^2+2b+4 = 2b^3+(b+5)b^2+2b+4 = 3b^3+5b^2+2b+4$. Donc $\overline{46}^b \times \overline{53}^b = \overline{3524}^b$.

5) L'entier 341 en base 10 s'écrit $\overline{2331}^a$ en base a. Déterminer a.

SOLUTION. On a $341 = 2a^3+3a^2+3a+1$, donc $a(2a^2+3a+3) = 340 = 17 \times 2^2 \times 5$. Donc a divise $17 \times 2^2 \times 5$. Or $a \geqslant 4$ puisque les chiffres 1,2,3 apparaissent. Comme $(2a^2+3a+3)$ divise 340, on forcément $a < 17$. Les seules solutions a priori possibles sont $1, 4, 5, 10$. Parmi elles, seule $a = 5$ vérifie $a(2a^2+3a+3) = 340$.

6) Montrer que, dans toute base $b \geqslant 3$, l'entier $\overline{11211}^b$ n'est pas premier.

SOLUTION. $\overline{11211}^b = b^4+b^3+2b^2+b+1 = (b^2+1)(b^2+b+1)$. Les deux facteurs sont $\neq 1$.

Pour d'autres exemples, voir aussi les feuilles d'exercices de travaux dirigés.

2.4 Comparaison de deux entiers naturels par leur représentation dans une base

a) Observation préliminaire. Soient deux entiers distincts $m, n \in \mathbb{N}^*$. Supposons-les écrits dans le système décimal. La question est de reconnaître lequel des deux est le plus grand. Si l'une des deux représentations a plus de chiffres, l'entier correspondant est le plus grand. Supposons maintenant que les deux représentations ont le même nombre de chiffres. Par exemple quatre pour fixer les idées. On compare le chiffre des milliers: s'ils diffèrent, le plus grand donne le plus grand des deux entiers. S'ils sont égaux, on regarde le chiffre des centaines. S'ils diffèrent, le plus grand donne le plus grand des deux entiers. Sinon, on réitère, et le processus s'arrête forcément puisque la non-égalité des deux entiers au départ implique qu'un chiffre au moins des deux représentations décimales diffère (d'après l'argument d'unicité dans le théorème 2.2.c).
C'est cette observation triviale (que l'on utilise naturellement depuis l'école primaire) que la proposition suivante formalise et démontre en base quelconque.

b) Proposition. *Soient* $m, n \in \mathbb{N}^*$. *On suppose* $m \neq n$. *On fixe une base de numération* b *quelconque; on note* $\mathrm{Long}_b\, m = p+1$ *et* $\mathrm{Long}_b\, n = q+1$, *et les décompositions:*

$$m = \overline{a_p \dots a_0}^b \quad \textit{et} \quad m' = \overline{c_q \dots c_0}^b, \qquad \textit{avec } a_p \neq 0 \neq c_q.$$

- *Si* $p < q$, *alors* $m < n$;
- *Si* $q < p$, *alors* $n < m$;
- *Si* $p = q$, *en notant* r *le plus grand élément de* $\{k \in [\![0, p]\!]\,;\, a_k \neq c_k\}$, *on a:*
  ou bien: $a_r < c_r$, *et alors* $m < n$;
  ou bien: $c_r < a_r$, *et alors* $n < m$.

Preuve Comme on l'a vu dans la preuve de 2.2.c, $m = \overline{a_p \dots a_0}^b$ implique $b^p \leqslant m < b^{p+1}$.

De même, $b^q \leqslant n < b^{q+1}$. Si $p < q$, alors $m < b^{p+1} \leqslant b^q \leqslant n$, donc $m < n$. De même $q < p$ implique $n < m$.

Supposons maintenant $p = q$; comme $m \neq n$, l'ensemble $A = \{k \in [\![0, p]\!]\,;\, a_k \neq c_k\}$ est non-vide (d'après l'unicité dans le théorème 2.2.c). Comme A est une partie de $\mathbb{N}$ majorée par p, elle possède un plus grand élément r.

• Supposons que $r = 0$. Cela signifie que $a_0 \neq c_0$ et $a_k = c_k$ pour tout $k \in [\![1, p]\!]$. D'où:

$$m - n = a_0 + \sum_{i=1}^{p} a_i b^i - c_0 - \sum_{i=1}^{p} c_i b^i = a_0 - c_0.$$

Donc on a bien dans ce cas $m < n$ si et seulement si $a_0 < c_0$.

• Supposons que $1 \leqslant r$. On a $a_r \neq c_r$ et $a_k = c_k$ pour tout $k \in [\![r+1, p]\!]$. Pour fixer les idées, supposons que $a_r < c_r$ (si c'est le contraire $c_r < a_r$, il suffit d'échanger m et n). Décomposons:

$$m = \sum_{i=0}^{r-1} a_i b^i + a_r b^r + S, \quad \text{avec } S = \sum_{i=r+1}^{p} a_i b^i \ \ (S \text{ est nul si } r = p), \tag{1}$$

$$n = \sum_{i=0}^{r-1} c_i b^i + c_r b^r + S, \quad \text{avec le même } S = \sum_{i=r+1}^{p} a_i b^i = \sum_{i=r+1}^{p} c_i b^i. \tag{2}$$

Rappelons que l'on a toujours $a_i \leqslant b - 1$, de sorte que l'on peut majorer:

$$\sum_{i=0}^{r-1} a_i b^i \leqslant \sum_{i=0}^{r-1} (b-1) b^i = b^r - 1.$$

Donc, d'après (1), il vient $m \leqslant b^r - 1 + a_r b^r + S = (a_r + 1) b^r - 1 + S$. Or puisqu'on a supposé au départ que $a_r < c_r$, on a: $(a_r + 1) b^r - 1 < (a_r + 1) b^r \leqslant c_r b^r$. Par suite: $m < c_r b^r + S$. Or il résulte de (2) que $c_r b^r + S \leqslant n$. On conclut que $m < n$. □

2.5 Estimation de la longueur de la représentation en une base donnée

a) Observation préliminaire. Pour tout entier $b > 1$ et tout $m \in \mathbb{N}^*$, on veut pouvoir calculer la longueur $\mathrm{Long}_b(m)$ de la représentation de m en base b. La méthode proposée ici suppose de connaître l'ensemble $\mathbb{R}$ des nombre réels et les fonctions logarithmes sur $\mathbb{R}$.

Pour tout $x \in \mathbb{R}$, on note $E(x)$ la partie entière de x. On note ln le logarithme néperien. Pour tout réel $a > 1$, on note $\log_a$ la fonction logarithme de base a, qui est définie par $\log_a(x) = \frac{\ln x}{\ln a}$, et qui est strictement croissante sur $]0, +\infty[$.

b) Proposition. *Soit* $a \in \mathbb{R}$ *tel que* $a > 1$. *Soit* $b \in \mathbb{N}$ *tel que* $b > 1$.

Pour tout $m \in \mathbb{N}^*$, *on a:* $\mathrm{Long}_b(m) = E\big(\frac{\log_a m}{\log_a b}\big) + 1$.

Preuve. Soit $m = \overline{a_k \dots a_0}^b$ avec $a_k \neq 0$ donc $\mathrm{Long}_b(m) = k + 1$. On a vu au début de la preuve du théorème 2.2.c qu'alors $b^k \leqslant m < b^{k+1}$. En appliquant la fonction $\log_a$, il vient $k \log_a b \leqslant \log_a m < (k+1) \log_a b$, ou encore $k \leqslant \frac{\log_a m}{\log_a b} < k+1$. Cela signifie que $k = E\big(\frac{\log_a m}{\log_a b}\big)$, ce qui prouve le résultat voulu. □

Remarque: Si on choisit $a = b$, on obtient en particulier $\mathrm{Long}_b(m) = E(\log_b m) + 1$. Pour $m = b$, il vient $\mathrm{Long}_b(b) = E(1) + 1 = 2$, ce que l'on savait déja puisque $b = \overline{10}^b$.

c) Exemples.

(i) *Calculer le nombre de chiffres de* 100 *en base* 2.

SOLUTION. On applique la proposition avec $b = 2$ et $m = 100$; on choisit $a = 10$ donc:

$$\mathrm{Long}_2(100) = E\big(\tfrac{\log_{10} 100}{\log_{10} 2}\big) + 1 = E\big(\tfrac{2}{0{,}30103\cdots}\big) + 1 = 6 + 1 = 7.$$

On peut vérifier en explicitant $100 = 64 + 32 + 4 = 2^6 + 2^5 + 2^2 = \overline{1100100}^2$.

(ii) *Calculer la longueur de la représentation décimale de* 2^{11213} *puis de* $2^{11213} - 1$.

SOLUTION. On applique encore la formule, avec $a = b = 10$. D'abord pour $m = 2^{11213}$, il vient:

$$\mathrm{Long}_{10} m = E\left(\frac{\log_{10} m}{\log_{10} 10}\right) + 1 = E(\log_{10} m) + 1.$$

Or en notant $x = 11213$, on a: $m = 2^x = 10^{x \log_{10} 2}$ c'est-à-dire $\log_{10} m = x \log_{10} 2$. Donc $E(\log_{10} m) = E(11213 \times 0,30103\cdots) = 3375$. Ainsi $\mathrm{Long}_{10} m = 3376$.

Posons maintenant $m' = m - 1$. L'écriture décimale de m ne se termine pas par 0 (car sinon m serait un multiple de 5, ce qui n'est pas). Donc l'écriture décimale de m' est la même que celle de m, hormis le chiffre des unités, qui est diminué de 1. En particulier $\mathrm{Long}_{10} m' = \mathrm{Long}_{10} m = 3376$.

On verra plus tard, après l'étude des congruences, d'autres applications de l'écriture décimale des entiers naturels (preuve par neuf, critère de divisibilité de Pascal...)

Chapitre 2: écritures décimales et nombres réels

1 Nombres décimaux et nombres réels

1.1 Rappel sur $\mathbb{R}$ et divers sous-ensembles de nombres

On suppose ici connu l'ensemble $\mathbb{R}$ des nombres réels, muni de ses opérations (permettant de faire du calcul algébrique dans $\mathbb{R}$) et de sa relation d'ordre $\leqslant$ (permettant de faire de l'analyse dans $\mathbb{R}$). Parmi les sous-ensembles de nombres classiques de $\mathbb{R}$, on distingue:

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.}$$

• $\mathbb{N}$ est l'ensemble des nombres entiers naturels $0, 1, 2, 3, \ldots, 9, 10, 11, 12, \ldots 453, 454, \ldots$ étudiés au chapitre précédent.

> *Remarque:* des équations du type $x + 3 = 0$ ou $x \times 7 = 1$ n'ont pas de solution dans $\mathbb{N}$ (cela correspond au fait que $\mathbb{N}$ n'est pas un groupe pour l'addition ni pour la multiplication).

La somme et le produit de deux entiers naturels est un entier naturel.

• $\mathbb{Z}$ est l'ensemble des nombres entiers relatifs $\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 \ldots$ formés des entiers naturels et de leurs opposés.

> *Remarque:* toutes les équations du type $x + a = 0$ avec $a \in \mathbb{Z}$ ont maintenant des solutions dans $\mathbb{Z}$ (à savoir $x = -a$), mais les équations du type $x \times 7 = 1$ n'en ont toujours pas (cela correspond au fait que $\mathbb{Z}$ est un groupe pour l'addition mais pas pour la multiplication).

La somme, la différence et le produit de deux entiers relatifs est un entier relatif; on dit que $\mathbb{Z}$ **est un anneau**.

• $\mathbb{Q}$ est l'ensemble des nombres rationnels, c'est-à-dire de la forme $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

> *Remarque:* toutes les équations du type $x + \frac{a}{b} = 0$ avec $a \in \mathbb{Z}, b \in \mathbb{N}^*$ ont maintenant des solutions dans $\mathbb{Q}$ (à savoir $x = -\frac{a}{b}$), et toutes les équations du type $x \times \frac{a}{b} = 1$ avec $a \in \mathbb{Z}^*$, $b \in \mathbb{N}^*$ ont maintenant des solutions dans $\mathbb{Q}$ (à savoir $x = \frac{b}{a}$).
>
> En revanche, une équation du type $x^2 = 2$ n'a toujours pas de solution dans $\mathbb{Q}$ (voir plus loin en 3.1.b). De plus, sur le plan de la relation d'ordre $\leqslant$, il existe dans $\mathbb{Q}$ des parties non-vides et majorées qui n'admettent pas de borne supérieure dans $\mathbb{Q}$ (voir plus loin en 3.2.b). Il en résulte des insuffisances pour "faire de l'analyse": par exemple une suite strictement croissante et majorée de rationnels ne converge pas nécessairement dans $\mathbb{Q}$ (voir plus loin en 3.1.d).

La somme, la différence et le produit de deux rationnels est un rationnel, et le quotient de tout rationnel par tout rationnel non-nul est un rationnel; on dit que $\mathbb{Q}$ **est un corps**.

• $\mathbb{R}$ est l'ensemble des nombres réels. Il contient tous les nombres rationnels, mais aussi d'autres qui ne le sont pas (ils sont dits irrationnels) comme π, $\sqrt{2}$, $\ln 2$, e,...

> *Remarque:* algébriquement, $\mathbb{R}$ **un corps**; et sur le plan de la relation d'ordre, toute partie non-vide et majorée de $\mathbb{R}$ admet une borne supérieure dans $\mathbb{R}$ (les conséquences pour l'analyse dans $\mathbb{R}$ sont fondamentales).

Il existe plusieurs méthodes théoriques de construction de $\mathbb{R}$ (soit par les coupures de Dedekind[2], soit par les suites de Cauchy[3])... aucune n'est triviale et nous ne les reprenons pas ici.

On développe dans ce qui suit un point de vue concret (et adapté au calcul) sur les nombres réels via l'écriture décimale. On commence pour cela par étudier un type particulier de nombres rationnels, les nombres décimaux.

1.2 Nombres décimaux

a) Définition. On appelle NOMBRE DÉCIMAL tout nombre rationnel de la forme particulière :

$$\frac{a}{10^n} = 10^{-n}a, \quad \text{où } a \in \mathbb{Z} \text{ et } n \in \mathbb{N}.$$

On note $\mathbb{D}$ l'ensemble des nombres décimaux.

► Tout nombre entier est un nombre décimal. En d'autres termes, on a:

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}}$$

► La somme et la différence de deux nombres décimaux est un nombre décimal. Le produit de deux nombres décimaux est un nombre décimal. En revanche, l'inverse d'un nombre décimal non-nul n'est pas forcément un nombre décimal.

> *En effet:* pour $a, b \in \mathbb{Z}$ et $n, m \in \mathbb{N}$, on a $\frac{a}{10^n} + \frac{b}{10^m} = \frac{a10^m + b10^n}{10^{m+n}}$ et $\frac{a}{10^n} \times \frac{b}{10^m} = \frac{a \times b}{10^{m+n}}$, ce qui montre le premier point. Pour le second, considérons le nombre 3, qui est un entier donc un rationnel. Si son inverse était un nombre décimal, on aurait $\frac{a}{10^n} = \frac{1}{3}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$, donc $10^n = 3a$, ce qui est impossible puisque 10 n'est pas divisible par 3. □

► On résume ces propriétés en disant que l'ensemble $\mathbb{D}$ des nombres décimaux est un sous-anneau de $\mathbb{Q}$, contenant $\mathbb{Z}$.

b) Remarque. (Les écritures de l'école primaire)

Soit $x \in \mathbb{D}$. Il est donc de la forme: $x = \frac{a}{10^n} = 10^{-n}a$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$.
Mais, comme dans le chapitre 1, a s'écrit de façon unique:

$a = 10^n a_0 + 10^{n-1}a_1 + \cdots + 10a_{n-1} + a_n$, avec $a_0 \in \mathbb{Z}$ et $0 \leqslant a_k \leqslant 9$ pour tout $1 \leqslant k \leqslant n$.

(Ceci résulte de la division euclidienne, mais attention: ce n'est pas forcément l'écriture décimale de a. Par exemple: $-235 = -3.10^2 + 6.10 + 5$)

On en déduit que le décimal $x = 10^{-n}a$ s'écrit de façon unique

$$a10^{-n} = a_0 + a_1 10^{-1} + a_2 10^{-2} \cdots + a_{n-1}10^{n-1} + a_n 10^{-n},$$
$$\text{avec } a_0 \in \mathbb{Z} \text{ et } 0 \leqslant a_k \leqslant 9 \text{ pour tout } 1 \leqslant k \leqslant n.$$

Lorsque a est positif, on note $a = a_0, a_1 a_2 \ldots a_n$

Exemples:

- $x = 28.10^{-2} = (0.10^2 + 2.10 + 8).10^{-2} = 0 + 2.10^{-1} + 8.10^{-2}$; on note $x = 0,28$.
- $x = 3514.10^{-2} = (35.10^2 + 1.10 + 4).10^{-2} = 35 + 1.10^{-1} + 4.10^{-2}$; on note $x = 35,14$.
- $x = -321.10^{-2} = (-4.10^2 + 7.10 + 9).10^{-2} = -4 + 7.10^{-1} + 9.10^{-2}$
  alors que $y = 321.10^{-2} = (3.10^2 + 2.10 + 1).10^{-2} = 3 + 2.10^{-1} + 1.10^{-2}$;
  on note $y = 3,21$ et $y = -x = -3,21$.

[2] Richard Dedekind, 1831- 1916, mathématicien allemand reconnu en particulier pour ses travaux sur les fondements des mathématiques et en algèbre

[3] Augustin Louis Cauchy, 1789-1857, l'un des mathématicien français les plus important du XIXème siècle, dont l'influence a été fondamentale dans tous les domaines, mais tout particulièrement en analyse réelle et complexe

Le but de ce qui suit est de définir une écriture décimale pour tout nombre réel, ce qui ne peut se faire qu'en passant d'une suite finie de chiffres (suffisante pour écrire tout nombre décimal) à une suite éventuellement infinie (nécessaire pour étendre à tout réel).

c) Suites décimales. On appelle SUITE DÉCIMALE toute suite d'entiers $(a_n)_{n\geqslant 0}$ telle que $a_0 \in \mathbb{Z}$ et $0 \leqslant a_n \leqslant 9$ pour tout $n \geqslant 1$. On note $\mathcal{S}$ l'ensemble des suites décimales.
Soit $s = (a_n)_{n\geqslant 0} \in \mathcal{S}$;

- s est dite FINIE lorsqu'il existe $N \in \mathbb{N}$ telle que $a_n = 0$ pour tout $n \geqslant N$.
- s est dite IMPROPRE lorsqu'il existe $N \in \mathbb{N}$ telle que $a_n = 9$ pour tout $n \geqslant N$.
- s est dite PROPRE lorsqu'elle n'est pas impropre, (i.e. $\forall\, N \in \mathbb{N},\ \exists\, n \geqslant N,\ a_n \neq 9$.)

On note $\mathcal{S}_p$ l'ensemble des suites décimales PROPRES.

1.3 Valeurs décimales approchées d'un réel

Rappelons d'abord que, quel que soit $x \in \mathbb{R}$, on appelle partie entière de x, notée $E(x)$, l'unique entier relatif tel que $E(x) \leqslant x < E(x) + 1$.

a) Définition. Soient $x \in \mathbb{R}$ et $n \in \mathbb{N}$. On appelle VALEUR DÉCIMALE APPROCHÉE de x à 10^{-n} près par défaut, ou par excès, les nombres décimaux définis respectivement par:

$$x_n = 10^{-n}E(10^n x) \qquad \text{et} \qquad y_n = 10^{-n}(E(10^n x) + 1) = x_n + 10^{-n}.$$

Par définition de la partie entière: $10^n x_n = E(10^n x) \leqslant 10^n x < E(10^n x) + 1 = 10^n y$. Donc:

$$\text{pour tout } n \in \mathbb{N}, \text{ on a:} \quad x_n \leqslant x < y_n \quad \text{et} \quad y_n - x_n = 10^{-n}.$$

b) Remarques.

- Pour tout $x \in \mathbb{R}$, on a $x_0 = E(x) \leqslant x < y_0 = E(x) + 1$.
- Pour tout $x \in \mathbb{Z}$ et tout $n \in \mathbb{N}$, on a $E(10^n x) = 10^n x$, donc $x_n = x < y_n = x + 10^{-n}$.
- Pour tout $x \in \mathbb{D}$, la suite (x_n) est stationnaire.

  En effet: soit $x = 10^{-n}a$ avec $n \in \mathbb{N}$ et $a \in \mathbb{Z}$; soit $m \geqslant n$, de sorte que $10^m x = 10^{m-n}a$ qui est entier ; donc $x_m = 10^{-m}E(10^m x) = 10^m 10^{m-n}a = 10^{-n}a$; ainsi $x_m = x$ dès lors que $m \geqslant n$.

Par exemple: soit $x = 1976.10^{-2} = 19,76$. On a: $x_0 = 19$ et $y_0 = 20$, $x_1 = 19,7$ et $y_1 = 19,8$, $x_2 = 19,76 = x$ et $y_2 = 19,77$, puis $x_m = x$ et $y_m = x + 10^{-m}$ pour $m \geqslant 2$.

c) Exercice.
Calculer les cinq premiers termes des suites (x_n) et (y_n) pour le réel (rationnel) $x = \frac{9}{7}$.
Calculer tous les termes des suites (x_n) et (y_n) pour le réel (décimal) $x = -6532.10^{-2}$.

d) Théorème. *Pour tout réel x, les suites (x_n) et (y_n) définies ci-dessus sont adjacentes, et convergent vers x.*

Preuve On part de: $10^n x_n = E(10^n x) \leqslant 10^n x < E(10^n x) + 1 = 10^n y$.

En multipliant par 10, il vient: $10E(10^n x) \leqslant 10^{n+1}x < 10E(10^n x) + 10$.

Par définition de la partie entière:

d'une part $10E(10^n x) \leqslant 10^{n+1}x$ implique $10E(10^n x) \leqslant E(10^{n+1}x)$, ce qui conduit en multipliant par 10^{-n-1} à $x_n \leqslant x_{n+1}$;

d'autre part $10^{n+1}x < 10E(10^n x) + 10$ implique $E(10^{n+1}x) + 1 \leqslant 10E(10^n x) + 10$, ce qui conduit en multipliant par 10^{-n-1} à $y_{n+1} \leqslant y_n$.

Ainsi (x_n) est croissante et (y_n) est décroissante; comme de plus $(y_n - x_n) = 10^{-n}$ converge vers 0, on conclut que les deux suites sont adjacentes.

On sait qu'alors elles convergent vers une même limite ℓ; puisque $x_n \leqslant x < y_n$ pour tout $n \in \mathbb{N}$, on a nécessairement $\ell = x$. □

e) Remarque. On pourrait dans tout ce paragraphe remplacer 10 par n'importe quel nombre entier $p \geqslant 2$ (de façon à avoir (p^{-n}) qui converge vers 0), et ce que l'on va dire maintenant du développement décimal des réels s'adapterait aussi (on parlerait du développement p-adique).

2 Développement décimal d'un réel

2.1 Existence et unicité du développement décimal propre

a) Lemme et notation. *Soit $x \in \mathbb{R}$. On définit une suite (a_n) d'entiers en posant:*

$$a_0 = E(x) \quad \textit{et} \quad a_{n+1} = E(10^{n+1}x) - 10\,E(10^n x) \ \textit{ pour tout } n \in \mathbb{N}.$$

Alors:

(i) *la suite $(a_n)_{n\geqslant 0}$ est une suite décimale propre (au sens de 1.2.c);*

(ii) *pour tout $n \geqslant 1$, la valeur décimale approchée x_n de x à 10^{-n} près par défaut est donnée par:* $x_n = a_0 + \sum_{k=1}^{n} a_k 10^{-k}$

Comme $x = \lim_{n\to+\infty} x_n$, *on note:* $x = a_0 + \lim_{n\to+\infty} \sum_{k=1}^{n} a_k 10^{-k} = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}$.

Preuve. On a: $E(10^n x) \leqslant 10^n x < E(10^n x) + 1$.

En multipliant par 10, il vient: $10\,E(10^n x) \leqslant 10^{n+1}x < 10\,E(10^n x) + 10$.

D'une part $10^{n+1}x < 10\,E(10^n x)+10$ implique: $E(10^{n+1}x) < 10\,E(10^n x)+10$ (simplement parce que $E(10^{n+1}x) \leqslant 10^{n+1}x$), donc $a_{n+1} < 10$.

D'autre part $10\,E(10^n x) \leqslant 10^{n+1}x$ implique $10E(10^n x) \leqslant E(10^{n+1}x)$ (par définition de la partie entière), et donc $0 \leqslant a_{n+1}$.

En résumé, on a bien: $0 \leqslant a_{n+1} \leqslant 9$ pour tout $n \in \mathbb{N}$.

Par ailleurs, par définition de a_{n+1}, on a:

$10^{-(n+1)}a_{n+1} = 10^{-(n+1)}E(10^{n+1}x) - 10^{-n}E(10^n x) = x_{n+1} - x_n$.

Par une récurrence évidente, on en tire $x_{n+1} = x_0 + \sum_{k=1}^{n+1} a_k 10^{-k}$. Il suffit de rappeler que $x_0 = E(x) = a_0$ pour obtenir le point (ii) du lemme.

• Le seul point qui reste à montrer pour (i) est que la suite $s_x = (a_n)_{n\geqslant 0}$ est propre. Par l'absurde, supposons qu'il existe $N \in \mathbb{N}$ tel que $a_n = 9$ pour tout $n \geqslant N$. Pour un tel $n \geqslant N$, on aurait donc:

$x_n = a_0 + \sum_{k=1}^{N} a_k 10^{-k} + \sum_{k=N+1}^{n} 9.10^{-k} = x_N + \sum_{k=N+1}^{n} 9.10^{-k}$.

Mais $\sum_{k=N+1}^{n} 9.10^{-k} = \sum_{k=N+1}^{n} (10-1).10^{-k} = \sum_{k=N+1}^{n} 10^{-k+1} - 10^{-k} = 10^{-N} - 10^{-n}$;

donc on aurait $x_n - x_N = 10^{-N} - 10^{-n}$, c'est-à-dire: $x_n + 10^{-n} = x_N + 10^{-N}$,

ou encore $y_n = y_N$ (avec les notations de 1.2.a). On aboutirait ainsi à $y_N = y_n$ pour tout $n \geqslant N$. Comme on sait d'après 1.2.d que (y_n) converge vers x, on conclurait $x = y_N$, ce qui contredirait le fait que $x < y_n$ pour tout $n \in \mathbb{N}$ (par définition de la valeur décimale approchée par excès). □

On a, par ce lemme, associé à tout $x \in \mathbb{R}$ une certaine suite $(a_n)_{n\geqslant 0}$ qui est dans $\mathcal{S}_p$. Le lemme suivant prend un point de vue réciproque.

b) Lemme. *Soit $(a_n)_{n\geqslant 0} \in \mathcal{S}_p$ une suite décimale propre. On définit deux suites $(u_n)_{n\geqslant 0}$ et $(v_n)_{n\geqslant 0}$ de nombres décimaux en posant, pour tout $n \in \mathbb{N}$:*

$$u_n = a_0 + \sum_{k=1}^{n} a_k 10^{-k} \quad \text{et} \quad v_n = u_n + 10^{-n}.$$

Alors, les suites (u_n) et (v_n) sont adjacentes et, si l'on note x leur limite commune, u_n et v_n sont exactement les valeurs décimales approchées à 10^{-n} près de x, par défaut et par excès respectivement.

Preuve. Par définition des suites (u_n) et (v_n), on a pour tout $n \geqslant 0$:

$u_{n+1} - u_n = a_{n+1}10^{-(n+1)}$ et

$v_n - v_{n+1} = u_n - u_{n+1} + 10^{-n} - 10^{-(n+1)} = (-a_{n+1} + 10 - 1)10^{-(n+1)}$.

Comme $0 \leqslant a_k \leqslant 9$ pour tout $k \geqslant 1$, il en résulte que (u_n) est croissante et (v_n) décroissante. En outre $\lim\limits_{n\to+\infty}(u_n - v_n) = \lim\limits_{n\to+\infty} 10^{-n} = 0$; les deux suites sont donc adjacentes. On note x leur limite commune.

On sait (propriété générale des suites adjacentes) que cette limite x vérifie:

$$u_n \leqslant x \leqslant v_n, \qquad (1)$$

mais, et c'est là un point crucial (voir plus loin remarque f), on a ici plus précisément:

$$u_n \leqslant x < v_n, \qquad (2)$$

> En effet, par l'absurde, supposons qu'il existe $N \in \mathbb{N}$ tel que $x = v_N$. Comme (v_n) est décroissante et minorée par x, on aurait $x = v_n = v_N$ pour tout $n \geqslant N$. Donc $v_{n+1} = v_n$ pour tout $n \geqslant N$. Rappelons que l'on a vu au début de la preuve que $v_n - v_{n+1} = (-a_{n+1} + 9)10^{-(n+1)}$. On aurait ainsi $a_{n+1} = 9$ pour tout $n \geqslant N$, ce qui contredirait que la fait que la suite décimale (a_n) est choisie propre.

Comme $10^n u_n$ et $10^n v_n = 10^n u_n + 1$ sont entiers, (2) montre exactement que u_n et v_n sont les valeurs décimales approchées à 10^{-n} près de x, par défaut et par excès respectivement. □

On peut maintenant synthétiser les deux lemmes en un seul énoncé:

c) Théorème. *L'application $\sigma : \mathbb{R} \to \mathcal{S}_p$ qui, à tout réel x, associe la suite décimale propre $(a_n)_{n\geqslant 0}$ définie au lemme a) est une bijection de $\mathbb{R}$ sur $\mathcal{S}_p$.*

Preuve. Lorsque $x \in \mathbb{R}$, on lui associe par le lemme a) une suite $(a_n) \in \mathcal{S}_p$.

Notons $\sigma(x)$ cette suite, ce qui définit une application $\sigma : \mathbb{R} \to \mathcal{S}_p$.

Réciproquement, le lemme b) permet d'associer à toute suite $s \in \mathcal{S}_p$ un réel que l'on notera $\tau(s)$, ce qui définit une application $\tau : \mathcal{S}_p \to \mathbb{R}$.

• Ceci étant, partons d'un réel x quelconque fixé. Notons (x_n) et (y_n) les suites de valeurs approchées décimales de x (par défaut et par excès) définies par 1.3. Par le lemme a), on construit la suite $\sigma(x) = (a_n)$. D'après le point (ii) du lemme a), elle vérifie que $a_0 + \sum\limits_{k=1}^{n} a_k 10^{-k} = x_n$.

Pour la suite $s = (a_n)$ ainsi obtenue, appliquons maintenant le lemme b. Les suites (u_n) et (v_n) que l'on construit dans le lemme b sont alors (par construction même) exactement les suites (x_n) et (y_n) ci-dessus, ce qui implique que leur limite commune [c'est-à-dire $\tau(s)$] n'est autre que la limite commune de (x_n) et (y_n) [c'est-à-dire x].

On a ainsi vérifié que $\tau(\sigma(x)) = x$, ce qui prouve que $\tau \circ \sigma = \mathrm{id}_{\mathbb{R}}$.

• On vérifie de la même façon que $\sigma \circ \tau = \mathrm{id}_{\mathcal{S}_p}$, ce qui achève la preuve. □

On retiendra la formulation pratique suivante de ce théorème:

d) Corollaire. *Pour tout* $x \in \mathbb{R}$*, il existe une unique suite décimale propre* $(a_n)_{n\geqslant 0}$ *tq:*

$$x = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}. \qquad (\star)$$

Dans ce cas, les valeurs décimales approchées à 10^{-n} *près de* x *sont données par:*

$$x_n = a_0 + \sum_{k=1}^{n} a_k 10^{-k} \leqslant x < y_n = x_n + 1.$$

e) Terminologie et notation: $(\star)$ s'appelle **le** DÉVELOPPEMENT DÉCIMAL (propre) de x.

Lorsque x est positif, on note $x = a_0, a_1 a_2 a_3 \ldots$, les points de suspension exprimant le fait qu'il ne s'agit pas forcément d'une suite finie.

Par exemple: $\frac{12}{25} = 0,48 = 0,4800000\ldots$, $\quad \frac{12}{11} = 1,09090909\ldots$, $\quad \pi = 3,141592653589793\ldots$,
le nombre de Mahler[4] $= 0,123456789101112131415\ldots$

f) Remarque sur l'unicité. Si l'on reprend la construction du lemme b) en partant d'une suite $s = (a_n) \in \mathcal{S}$ (non nécessairement propre), on peut définir de la même façon les suites (u_n) et (v_n), montrer qu'elles sont adjacentes, mais en notant $x = \tau(s)$ leur limite commune, on ne peut pas conclure que (u_n) et (v_n) sont les suites de valeurs décimales approchées de x. En effet, il nous a fallu pour cela pouvoir remplacer (1) par (2), ce qui a utilisé le fait que s est propre.

Plus précisément, on a toujours $\tau(\sigma(x)) = x$ pour tout $x \in \mathbb{R}$ (et donc $\tau \circ \sigma = \mathrm{id}_{\mathbb{R}}$), mais on peut montrer qu'une suite $s \in \mathcal{S}$ vérifie $\sigma(\tau(s)) = s$ si et seulement si $s \in \mathcal{S}_p$.

> *Par exemple,* prenons $x = 1$. On construit $(a_n) = \sigma(x)$ par le lemme a); il vient: $a_0 = 1$, $a_1 = a_2 = \cdots = a_n = \cdots = 0$ pour tout $n \geqslant 1$. Si l'on note $s = \sigma(x)$, on a donc $s \in \mathcal{S}_p$ et $\tau(s) = x = 1$. Prenons maintenant une autre suite $s' \in \mathcal{S}$, impropre, définie par: $a'_0 = 0$, $a'_1 = a'_2 = \cdots = a'_n = \cdots = 9$ pour tout $n \geqslant 1$. Appliquons la construction du lemme b. Les suites (u'_n) et (v'_n) correspondantes sont données par: $u'_0 = 0$, $u'_1 = 0,9$, $u'_2 = 0,99$, $u'_3 = 0,999$,... $v'_0 = 1$, $v'_1 = 1$, $v'_2 = 1$, $v'_3 = 1$,... et leur limite commune est encore $\tau(s') = 1$. On a donc: $\tau(s) = \tau(s') = 1$ avec $s \neq s'$, $s \in \mathcal{S}_p$, $s' \notin \mathcal{S}_p$. On écrit: $1 = 1,000000\ldots = 0,999999\ldots$, la deuxième écriture étant impropre !

Plus généralement, tout nombre décimal est image par τ de deux suites décimales, une propre et une impropre, (par exemple $7,25 = 7,25000000\ldots = 7,24999999\ldots$) et l'on peut montrer que, parmi les réels, cela caractérise les nombres décimaux.

*Dans la pratique, afin de conserver l'*UNICITÉ *du développement décimal, on ne considère* QUE DES SUITES DÉCIMALES PROPRES.

g) Exercice. En utilisant les résultats de ce paragraphe, démontrer que l'ensemble $\mathbb{R}$ n'est pas dénombrable (voir plus loin en 3.3).

2.2 Comparaison de deux réels par leur développement décimal

a) Proposition. *Soient* x *et* y *deux réels donnés par leur développement décimal (propre):*

$$x = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k} \quad \textit{et} \quad y = b_0 + \sum_{k=1}^{+\infty} b_k 10^{-k}.$$

Alors : $(x < y)$ *si et seulement si* $(\exists\, N \in \mathbb{N},\ a_N < b_N$ *et* $a_k = b_k$ *pour tout* $0 \leqslant k < N)$.

[4] Kurt Mahler, 1903-1988, mathématicien anglais d'origine allemande, spécialiste des questions de transcendance en théorie des nombres

Preuve. Supposons $x \neq y$. Par unicité du développement décimal, on peut considérer le plus petit entier $N \geqslant 0$ tel que $a_N \neq b_N$. Supposons $a_N < b_N$. En reprenant les notations du lemme 2.1.b, on a:

$u_N = a_0 + \sum_{k=1}^{N} a_k 10^{-k} \leqslant x < v_N = u_N + 10^{-N}$ et $u'_N = b_0 + \sum_{k=1}^{N} b_k 10^{-k} \leqslant y < v'_N = u'_N + 10^{-N}$.

On en déduit: $x < a_0 + a_1 10^{-1} + a_2 10^{-2} \cdots + a_{N-1} 10^{N-1} + (a_N + 1)10^{-N}$

et $\qquad b_0 + b_1 10^{-1} + b_2 10^{-2} \cdots + b_{N-1} 10^{N-1} + b_N 10^{-N} \leqslant y$

d'où $x < y$ puisque $a_k = b_k$ si $0 \leqslant k \leqslant N-1$ et $a_N + 1 \leqslant b_N$.

De même bien sûr $y < x$ si l'on suppose au contraire que $b_N < a_N$. □

b) Exercice. En utilisant la proposition ci-dessus, donner une preuve du théorème classique: *toute partie non-vide et majorée de* $\mathbb{R}$ *admet une borne supérieure* (voir plus loin en 3.2.a).

2.3 Caractérisation des rationnels par leur développement décimal

a) Définition. Soit $s = (a_n)_{n \geqslant 0}$ une suite décimale. On dit que s est PÉRIODIQUE lorsqu'il existe deux entiers $N, p \in \mathbb{N}$ tels que, pour tout $n \geqslant N$, on ait $a_n = a_{n+p}$.

En clair cela signifie que, à partir d'un certain rang, on a un même "paquet" de chiffres qui se répètent. Par exemple:

- $\frac{377}{300} = 1.25666666\ldots$, $\frac{1}{11} = 0,909090909\ldots$, $\frac{5}{7} = 0,714285714285714285\ldots$ sont périodiques ;
- toute suite finie (représentant donc un nombre décimal) est périodique : $\frac{37}{100} = 0,3700000\ldots$;
- les suites $0,1234567891011121314\ldots$ ou $0,01001000100001\ldots$ ne sont pas périodiques.

b) Exemples préliminaires.

- On vient de voir que les rationnels $\frac{377}{300}$, $\frac{1}{11}$ ou $\frac{5}{7}$ ont tous des développements décimaux qui sont périodiques. Le théorème suivant va montrer que c'est le cas de tous les rationnels.

- Considérons le nombre réel $x = 15,7659428428428428\ldots$, dont le développement est périodique.

On calcule: $10^4 x = 157659,428428428\ldots$ et $10^7 x = 157659428,428428428\ldots$
Donc: $10^7 x - 10^4 x = 157659428 - 157659$ est un entier, et donc: $x = \frac{157659428-157659}{10^7-10^4}$ est un rationnel (que l'on peut simplifier en $x = \frac{157501769}{999000}$). Le théorème suivant va montrer que c'est le cas de tous les réels dont le développement décimal propre est périodique.

c) Théorème. *Soit* x *un réel et* $x = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}$ *son développement décimal (propre). Alors* $x \in \mathbb{Q}$ *si et seulement si la suite décimale* $(a_n)_{n \geqslant 0}$ *est périodique.*

Preuve. Supposons $x \in \mathbb{Q}$; notons $x = \frac{p}{q}$ avec $p \in \mathbb{Z}, q \in \mathbb{N}^*$ premiers entre eux. On définit par récurrence deux suites (a_n) et (r_n) par division euclidienne:

$p = a_0 q + r_0$, $10r_0 = a_1 q + r_1$, $10r_1 = a_2 q + r_2$, ... avec $0 \leqslant r_0, r_1, r_2, \ldots < q$;

et plus généralement: $10r_{n-1} = a_n q + r_n$ avec $0 \leqslant r_n < q$,

ce qui détermine a_n et r_n de façon unique à partir des précédents.

1) La suite $s = (a_n)_{n \geqslant 0}$ ainsi formée est une suite décimale. En effet, pour tout $n \geqslant 1$, on a $0 \leqslant a_n q = 10r_{n-1} - r_n \leqslant 10r_{n-1} < 10q$ d'où $0 \leqslant a_n < 10$.

2) Cette suite (a_n) est exactement la suite décimale $\sigma(x)$ du développement décimal propre de x. En effet:

$p = a_0 q + r_0$ donc $\frac{p}{q} = a_0 + \frac{r_0}{q}$;

$10r_0 = a_1 q + r_1$ donc $\frac{r_0}{q} = \frac{a_1}{10} + \frac{r_1}{10q}$, d'où $\frac{p}{q} = a_0 + \frac{a_1}{10} + \frac{r_1}{10q}$;

$10r_1 = a_2 q + r_2$ donc $\frac{r_1}{10q} = \frac{a_2}{10^2} + \frac{r_2}{10^2 q}$, d'où $\frac{p}{q} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{r_2}{10^2 q}$

et par récurrence évidente: $x = \frac{p}{q} = a_0 + \sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{r_n}{10^n q}$

Mais $0 \leqslant r_n < q$ implique $0 \leqslant \frac{r_n}{10^n q} < \frac{1}{10^n}$,

de sorte que l'écriture de x précédente conduit immédiatement à l'encadrement:

$$a_0 + \sum_{k=1}^{n} \frac{a_k}{10^k} \leqslant x < a_0 + \sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{1}{10^n},$$

ce qui d'après le lemme 2.1.a prouve que la suite (a_n) ainsi définie n'est autre que $\sigma(x)$.

3) Cette suite (a_n) est périodique. En effet, comme tout reste r_n vérifie $0 \leqslant r_n < q$, on retrouve forcément dans la suite des divisions euclidiennes effectuées le même reste après au plus q opérations. Plus précisément, il existe des entiers k, l tels que $0 \leqslant k < l \leqslant q$ et $r_k = r_l$. On a donc: $a_{k+1} q + r_{k+1} = 10 r_k = 10 r_l = a_{l+1} q + r_{l+1}$ d'où $a_{l+1} = a_{k+1}$ et $r_{l+1} = r_{k+1}$ (par unicité du quotient et du reste dans la division euclidienne). En itérant, on obtient $r_{l+m} = r_{k+m}$ et $a_{l+m} = a_{k+m}$ pour tout $m \geqslant 1$. Ceci implique que, en notant $p = l - k$, on a $a_{n+p} = a_n$ pour tout $n \geqslant k+1$.

• Réciproquement, soit $x = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}$ un réel donné par son développement décimal, que l'on suppose périodique: il existe donc $p \geqslant 1$ tel que $a_{n+p} = a_n$ pour $n \geqslant$ à un certain rang N, que l'on suppose choisi minimum. Posons alors comme en 2.1.b : $u_n = a_0 + \sum_{k=1}^{n} a_k 10^{-k}$ pour tout $n \geqslant 0$, et définissons une nouvelle suite (b_k) par $b_k = u_{N+kp}$. C'est une suite extraite de (u_n), donc elle converge vers la même limite que (u_n), c'est-à-dire x.

On vérifie alors que : $b_{k+1} - b_k = 10^{-kp}(u_{N+p} - u_N)$,

si bien que: $b_{k+1} = b_0 + (u_{N+p} - u_N)(1 + 10^{-p} + 10^{-2p} + \cdots + 10^{-kp})$.

Il en résulte que (limite de la somme des termes d'une suite géométrique):

$x = \lim_{k \to +\infty} b_k = b_0 + (u_{N+p} - u_N)(1 - 10^{-p})^{-1}$,

qui est bien un rationnel puisque la suite (u_n) est à termes rationnels. □

3 Résultats annexes.

3.1 Quelques remarques sur les réels irrationnels

Rappelons qu'un réel est irrationnel lorsqu'il n'est pas rationnel, c'est-à-dire qu'il n'appartient pas au sous-ensemble $\mathbb{Q}$ de $\mathbb{R}$.

a) Exemple. D'après ce qui précède, le nombre de Mahler $0,12345678910111213141516\ldots$ est irrationnel (puisque, par définition, son développement décimal n'est pas périodique).

b) Exemple. Le nombre $\sqrt{2}$ est irrationnel.

Preuve (historiquement classique). Le nombre réel $x = \sqrt{2}$ est défini par le fait que $x^2 = 2$.

Raisonnons en supposons, "par l'absurde", que x est un rationnel. Cela signifie que $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Quitte à simplifier, on peut supposer que $x = \frac{a}{b}$ est "irréductible", ou encore non-simplifiable, ce qui signifie que les entiers a et b n'ont aucun diviseur commun (on dit qu'ils sont premiers entre eux).

On a: $\frac{a^2}{b^2} = x^2 = 2$, donc $a^2 = 2b^2$.

Ainsi a^2 est pair. Cela implique que a est pair (car le carré d'un entier impair est impair). Donc $a = 2c$ pour un certain entier c. Mais alors $a^2 = 4c^2$, donc $4c^2 = 2b^2$, donc $b^2 = 2c^2$.

Ainsi b^2 est pair. De la même façon que précédemment, cela implique que b est pair, et s'écrit donc $b = 2d$ avec $d \in \mathbb{N}^*$. On obtient une contradiction puisque $a = 2c$ et $b = 2d$ alors que l'hypothèse de départ supposait x irréductible. □

On peut montrer par une preuve analogue (par un raisonnement arithmétique simple utilisant le lemma de Gauss) que, pour tout $n \in \mathbb{N}$ qui n'est pas un carré dans $\mathbb{N}$, le réel $\sqrt{n}$ est irrationnel.

On peut en déduire l'exercice suivant: montrer que $\alpha = \sqrt{6} - \sqrt{2} - \sqrt{3}$ est irrationnel.

Solution. On calcule α^2, d'où $\beta := \frac{1}{2}(2\alpha - \alpha^2 + 11) = \sqrt{3} + 2\sqrt{2}$; on a $\beta^2 = 11 + 4\sqrt{6}$. Comme $\sqrt{6} \notin \mathbb{Q}$, ceci implique que $\beta^2 \notin \mathbb{Q}$. Il en résulte que $\beta \notin \mathbb{Q}$ (car le carré d'un rationnel est rationnel). On en déduit immédiatement que $\alpha \notin \mathbb{Q}$. □

c) Exercice. Montrer que $\log_{10}(2)$ est irrationnel.

Solution: Sinon il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $10^{p/q} = 2$ donc $10^p = 2^q$. Impossible □

d) Exercice. Montrer que le réel e (base du logarithme néperien) est irrationnel.

Solution. On procède par un raisonnement sur des suites adjacentes qui, s'il n'utilise pas directement le développement décimal, est tout à fait de même nature que les considérations précédentes. Cela consiste à établir le lemme suivant:

LEMME. *Soit $(u_n)_{n\geqslant 0}$ la suite de rationnels définie par:*

$$u_n = 1 + 1 + \tfrac{1}{2} + \tfrac{1}{6} + \tfrac{1}{24} + \cdots + \tfrac{1}{n!} = \sum_{k=0}^{n} \tfrac{1}{k!}$$

Alors la suite (u_n) converge dans $\mathbb{R}$ et sa limite e est irrationnelle.

Preuve. Posons $v_n = u_n + \frac{1}{n\times n!}$. Il est clair que $(v_n - u_n)$ converge vers 0, et que (u_n) est strictement croissante.
De plus, $v_{n+1} - v_n = u_{n+1} - u_n + \frac{1}{(n+1)\times(n+1)!} - \frac{1}{n\times n!} = \frac{1}{(n+1)!} + \frac{1}{(n+1)\times(n+1)!} - \frac{1}{n\times n!}$
$= \frac{-1}{n(n+1)(n+1)!} < 0.$
Donc la suite (v_n) est strictement décroissante; on conclut que les deux suites (u_n) et (v_n) sont adjacentes; elles admettent donc une limite commune que l'on note e.
Il est clair que $e > 0$, et en calculant les premiers termes de la suite (u_n), on vérifie immédiatement que: $e = 2,1718\ldots$. On va montrer que e est irrationnel
Par l'absurde, supposons que $e = \frac{p}{q}$ avec $p, q \in \mathbb{N}^*$. En réduisant tous les termes de $u_q = \sum_{k=0}^{q} \frac{1}{k!}$ au même dénominateur $q!$, on peut écrire $u_q = \frac{a}{q!}$ avec $a \in \mathbb{N}^*$.
Rappelons que les deux suites (u_n) et (v_n) sont *strictement* croissante et décroissante.
On a donc l'encadrement $u_q < e < v_q$ qui conduit à: $\frac{a}{q!} < \frac{p}{q} < \frac{a}{q!} + \frac{1}{q\times q!}$
Donc: $a < p \times (q-1)! < a + \frac{1}{q}$. On en tire en particulier: $a < p \times (q-1)! < a + 1$, ce qui est impossible puisque $p \times (q-1)!$ est entier. □

3.2 Quelques remarques sur l'axiome de la borne supérieure

Rappelons d'abord que, si E est une partie non-vide de $\mathbb{R}$, on appelle MAJORANT de E tout réel M tel que $x \leqslant M$ pour tout élément de E. Si E admet des majorants, et s'il existe parmi eux un plus petit majorant S, on dit que S est la BORNE SUPÉRIEURE de E. Une propriété tout à fait fondamentale de $\mathbb{R}$ est qu'une telle borne supérieure existe toujours dans $\mathbb{R}$ dès lors que E est admet des majorants. On en donne ci-dessous une démonstration utilisant les développements décimaux, et l'on montre que cette propriété n'est plus vraie si l'on se restreint à $\mathbb{Q}$.

a) La propriété de la bonne supérieure pour $\mathbb{R}$.

Proposition. *Toute partie non-vide et majorée de $\mathbb{R}$ admet une borne supérieure dans $\mathbb{R}$.*

Preuve. Soit un ensemble non-vide de nombres réels majoré par un réel M.

Pour $x \in E$ quelconque, notons $x = a_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}$ le développement décimal propre de x. Comme E est majorée, parmi toutes les valeurs prises par a_0 lorsque x parcourt E, il en est une qui majore toutes les autres. Notons-la b_0 en remarquant que $b_0 \leqslant E(M)$.

Considérons alors l'ensemble E_0 formé de tous les éléments de E dont le développement décimal propre est de la forme $x_0 = b_0 + \sum_{k=1}^{+\infty} a_k 10^{-k}$. Par définition, E_0 est non vide et majoré par M.

Parmi toutes les valeurs prises par a_1 lorsque x_0 parcourt E_0, il en est une qui majore toutes les autres puisque $0 \leqslant a_1 \leqslant 9$. Notons-la b_1.

Considérons alors l'ensemble E_1 formé de tous les éléments de E_0 dont le développement décimal propre est de la forme $x_1 = b_0 + b_1 10^{-1} + \sum_{k=2}^{+\infty} a_k 10^{-k}$.

On construit ainsi par récurrence une suite de sous-ensembles $E \supset E_0 \supset E_1 \supset \cdots \supset E_n \supset \cdots$ tous non-vide, et une suite décimale $s = (b_n)_{n \geqslant 0}$ (dont rien ne dit qu'elle est propre) vérifiant par construction la propriété suivante pour tout $n \in \mathbb{N}$:

$$\text{si } b_0 + b_1 10^{-1} + \cdots + b_n 10^{-n} + \sum_{k=n+1}^{+\infty} a_k 10^{-k} \text{ est dans } E_n, \text{ alors } a_{n+1} \leqslant b_{n+1}.$$

Posons $y = b_0 + \sum_{k=1}^{+\infty} b_k 10^{-k}$. Il résulte de la proposition 2.2.a que $x \leqslant y$ quel que soit $x \in E$. Donc y est un majorant de E.

Soit maintenant z un réel tel que $z < y$. Il existe un entier $n \geqslant 1$ tel que $z < y - 10^{-n}$. Or tout élément t dans $E_{n+1} \subset E$ vérifie que $y - 10^{-n} \leqslant t \leqslant y$, donc en particulier $z < t$, de sorte que z n'est pas un majorant de E. Ceci prouve que y est la borne supérieure de E. □

b) La propriété de la bonne supérieure n'est pas vraie pour $\mathbb{Q}$.

Rappelons d'abord que $\mathbb{Q}$ est archimédien: $\forall\, x \in \mathbb{Q}_+,\ \forall y \in \mathbb{Q}_+^*,\ \exists\, n \in \mathbb{N},\ ny \geqslant x.$ $\quad(\star)$

Considérons dans $\mathbb{Q}$ les deux parties suivantes: $A = \{x \in \mathbb{Q}_+\,;\, x^2 < 2\}$ et $B = \{x \in \mathbb{Q}_+\,;\, x^2 > 2\}$.

(i) $\forall\, x \in A,\ \exists\, y \in A,\ y > x$

En effet: soit $x \in A$. Donc $x^2 < 2$, de sorte que $2 - x^2 \in \mathbb{Q}_+$. Comme de plus $2x + 1 \in \mathbb{Q}_+$, il résulte de $(\star)$ qu'il existe $n \in \mathbb{N}^*$ tel que $n(2 - x^2) > 2x + 1$, donc $\frac{2x+1}{n} < 2 - x^2$.

Posons $y = x + \frac{1}{n}$ d'où $y > x$ et $y^2 = x^2 + \frac{1}{n^2} + \frac{2x}{n}$.

Or $\frac{1}{n^2} \leqslant \frac{1}{n}$, donc $y^2 \leqslant x^2 + \frac{1}{n} + \frac{2x}{n} = x^2 + \frac{2x+1}{n} < x^2 + (2 - x^2) = 2$. On a bien $y \in A$.

(ii) $\forall\, x \in B,\ \exists\, y \in B,\ y < x$

En effet : soit $x \in B$. Donc $x^2 > 2$, de sorte que $x^2 - 2 \in \mathbb{Q}_+$. Comme de plus $2x + 1 \in \mathbb{Q}_+$, il résulte de $(\star)$ qu'il existe $m \in \mathbb{N}^*$ tel que $m(x^2 - 2) > 2x + 1$, donc $\frac{2x+1}{m} < x^2 - 2$.

Posons $y = x - \frac{1}{m}$ d'où $y < x$ et $y^2 = x^2 + \frac{1}{m^2} - \frac{2x}{m}$.

Or $\frac{1}{m^2} \geqslant -\frac{1}{m}$, donc $y^2 \geqslant x^2 - \frac{1}{m} - \frac{2x}{m} = x^2 - \frac{2x+1}{m} > x^2 + (2 - x^2) = 2$.

Enfin, $y \in \mathbb{Q}_+$ car $y = x - \frac{1}{m} > x - \frac{x^2-2}{2x+1} = \frac{x^2+x+1}{2x+1} > 0$. On a bien $y \in B$.

(iii) $\mathbb{Q}_+ = A \cup B$.

En effet : il n'existe pas de rationnel x tel que $x^2 = 2$ (voir plus haut en 3.1.b).

(iv) B est l'ensemble des majorants de A dans $\mathbb{Q}$.

En effet : il est clair que tout élément de B majore A. Réciproquement, soit M un majorant de A dans $\mathbb{Q}$. D'une part $M \in \mathbb{Q}_+$ puisque $A \subset \mathbb{Q}_+$, d'autre part il résulte de (i) que $M \notin A$. Donc d'après (iii), $M \in B$.

Bilan: comme d'après (ii) B n'a pas de plus petit élément, il résulte de (iv) que la partie A (qui n'est pas vide puisque $1 \in A$) n'a pas de plus petit majorant dans $\mathbb{Q}$, c'est-à-dire n'a pas de borne supérieure dans $\mathbb{Q}$ (bien sûr, A admet dans $\mathbb{R}$ une borne supérieure, à savoir $\sqrt{2}$).

CONCLUSION: *il existe des parties de $\mathbb{Q}$ non-vides et majorées qui n'admettent pas de borne supérieure dans $\mathbb{Q}$.*

3.3 Une preuve de la non-dénombrabilité de $\mathbb{R}$

Rappelons tout d'abord qu'un ensemble E est dit DÉNOMBRABLE lorsqu'on peut construire une bijection f de E sur l'ensemble $\mathbb{N}$ des entiers naturels.

Rappelons que cela signifie que $f : E \to \mathbb{N}$ permet d'associer à chaque élément x de E un unique entier $n = f(x) \in \mathbb{N}$, et que réciproquement chaque entier $n \in \mathbb{N}$ est de la forme $n = f(x)$ pour un unique élément $x \in E$.

Il est bien connu (et pas très difficile à montrer) que $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables. On donne ci-dessous une preuve du fait que $\mathbb{R}$ n'est quant à lui pas dénombrable basée sur le développement décimal des réels.

Proposition. *L'ensemble $\mathbb{R}$ n'est pas dénombrable.*

Preuve. Raisonnons par l'absurde en supposant qu'il existe une bijection f de $\mathbb{N}$ sur $\mathbb{R}$. Considérons pour tout $n \in \mathbb{N}$ le développement décimal propre de $f(n)$, noté:

$$f(n) = a_{n,0} + \sum_{k=1}^{+\infty} \frac{a_{n,k}}{10^k}.$$

Soit y le réel dont le développement décimal propre $y = b_0 + \sum_{k=1}^{+\infty} \frac{b_k}{10^k}$ est défini de la façon suivante:

$b_0 =$ n'importe quel entier sauf $a_{0,0}$, de sorte que $y \neq f(0)$ puisque leurs parties entières diffèrent,

$b_1 =$ n'importe quel entier de $\{0, 1, 2, \ldots, 9\}$ sauf $a_{1,1}$, de sorte que $y \neq f(1)$ puisque leurs chiffres des dixièmes diffèrent,

et plus généralement, pour tout $k \geqslant 1$,

$b_k =$ n'importe quel entier de $\{0, 1, 2, \ldots, 9\}$ sauf $a_{k,k}$, de sorte que $y \neq f(k)$ puisque leurs k-ièmes décimales diffèrent.

Par construction, $y \neq f(n)$ pour tout $n \in \mathbb{N}$, ce qui contredit la bijectivité (en fait la surjectivité) de f. □

Chapitre 3: congruences

1 Rudiments sur la divisibilité

On travaille dans cette section dans l'anneau $\mathbb{Z}$ des entiers, mais la plupart des applications concerneront plus spécifiquement les entiers naturels.

1.1 Division euclidienne

On a introduit au chapitre 1 la division euclidienne des entiers naturels. Une adaptation immédiate de la même preuve (laissée au lecteur) permet de l'étendre à $\mathbb{Z}$ sous la forme suivante:

Proposition. *Quels que soient des entiers* a *et* b *avec* $b \neq 0$, *il existe des entiers* q *et* r, *avec* $r \geqslant 0$, *uniques tels que :*

$$a = bq + r \quad \textit{avec} \;\; 0 \leqslant r < |b|.$$

1.2 Multiples et diviseurs

a) Définition. Soient a et b deux entiers. On dit que a DIVISE b, ou que a est un DIVISEUR de b, ou encore que b est MULTIPLE de a, lorsqu'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$.

> *Remarque.* Dire que a divise b équivaut alors à dire que le reste de la division euclidienne de b par a est nul.

▶ Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z}$ l'ensemble des multiples de a; donc: $a\mathbb{Z} = \{ka \;;\; k \in \mathbb{Z}\}$.

▶ Pour tout $b \in \mathbb{Z}$, on note D_b l'ensemble des diviseurs de b; donc: $D_b = \{a \in \mathbb{Z} \,;\, \exists\, k \in \mathbb{Z},\; b = ka\}$.

En d'autres termes :

$$\forall\, a \in \mathbb{Z},\; \forall\, b \in \mathbb{Z},\;\; \text{on a:}\;\; (b \in a\mathbb{Z}) \;\; \text{si et seulement si} \;\; (a \in D_b).$$

Exemples:

- $2\mathbb{Z}$ est l'ensemble des nombres pairs; $7\mathbb{Z} = \{\ldots, -35, -28, -21, -14, -7, 0, 7, 14, 21, 28, 35, \ldots\}$; $0\mathbb{Z} = \{0\}$; $1\mathbb{Z} = \mathbb{Z}$. $\rightarrow$ Il est clair que si $a \neq 0$, alors $a\mathbb{Z}$ est infini.
- $D_{12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$; $D_7 = \{-7, -1, 1, 7\}\}$; $D_0 = \mathbb{Z}$; $D_1 = \{-1, 1\}$. $\rightarrow$ Il est clair que si $b \neq 0$, alors D_b est fini, majoré par $|b|$.

b) Proposition. *Soient* a *et* b *deux entiers. On a:*

(i) (a divise b) $\Leftrightarrow$ ($b \in a\mathbb{Z}$) $\Leftrightarrow$ ($b\mathbb{Z} \subset a\mathbb{Z}$) $\Leftrightarrow$ ($D_a \subset D_b$)

(ii) (a divise b et b divise a) $\Leftrightarrow$ ($b\mathbb{Z} = a\mathbb{Z}$) $\Leftrightarrow$ ($D_a = D_b$) $\Leftrightarrow$ ($a = b$ ou $a = -b$)

> *Preuve.* Les équivalences du point (i) se déduisent directement des définitions précédentes. Pour le (ii), supposons d'abord que a divise b et b divise a. Il existe alors k et k' dans $\mathbb{Z}$ tels que $a = kb$ et $b = k'a$, donc $(1 - kk')a = 0$, donc l'un des deux facteurs est nul. Si $a = 0$, alors $b = k' \times 0 = 0$. Si $a \neq 0$, alors $kk' = 1$, donc $k = k' = \pm 1$, d'où finalement $a = \pm b$. Le reste de la preuve est clair. □

c) Plus grand diviseur commun. Commençons par l'exemple suivant. Considérons les entiers $a = 12$ et $b = 30$. Leurs ensembles de diviseurs sont: $D_{12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ et $D_{30} = \{-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$. Leurs diviseurs communs sont donc les éléments de $D_{12} \cap D_{30} = \{-6, -3, -2, -1, 1, 2, 3, 6\}$, c'est-à dire que $D_{12} \cap D_{30} = D_6$.

Théorème et définition. *Quels que soient deux entiers* a *et* b*, il existe un unique entier naturel* d *vérifiant la propriété suivante :*

> *l'ensemble des diviseurs communs à* a *et* b *est égal à l'ensemble des diviseurs de* d *;*
> *en d'autres termes:* $D_a \cap D_b = D_d$.

L'entier naturel d *est appelé le* PLUS GRAND COMMUN DIVISEUR *de* a *et* b*. On note* $d = \text{pgcd}(a, b)$ *ou* $d = a \wedge b$.

Preuve. Commençons par montrer l'unicité. S'il existe deux entiers naturels d et d' vérifiant $D_a \cap D_b = D_d$ et $D_a \cap D_b = D_{d'}$, on a $D_d = D_{d'}$, donc $d' = \pm d$ d'après la propriété précédente, et finalement $d' = d$ puisque les deux sont supposés positifs.

Montrons maintenant l'existence de d. Il est clair que l'on peut prendre $d = b$ lorsque $a = 0$ et $d = a$ lorsque $b = 0$. On peut donc supposer désormais que a et b sont non-nuls. Comme $D_a = D_{-a}$ et $D_b = D_{-b}$, on peut de plus sans restriction supposer que a et b sont tous les deux dans $\mathbb{N}^*$. Considérons E l'ensemble de tous les entiers qui peuvent s'écrire sous la forme $au + bv$ pour certains $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

$$E = \{au + bv\,;\ u, v \in \mathbb{Z}\}.$$

Cet ensemble E contient en particulier tous les multiples de a (prendre $v = 0$) et tous les multiples de b (prendre $u = 0$). Comme il est clair que l'opposé d'un élément de E est encore dans E, l'ensemble E contient forcément des entiers positifs. On peut alors considérer (propriété de l'ordre dans $\mathbb{N}$, voir précédemment):

soit d le plus petit élément strictement positif de E.

En particulier, comme $d \in E$, il existe u_0 et v_0 dans $\mathbb{Z}$ tels que $d = au_0 + bv_0$. Par division euclidienne (avec ici d positif), il existe des entiers naturels uniques q et r vérifiant $a = dq + r$ avec $r < d$. On a donc: $r = a - dq = a - (au_0 + bv_0)q = a(1 - u_0 q) + bv_0 q$. Ceci prouve que $r \in E$. Comme $r < d$, la minimalité de d implique que $r = 0$. On conclut que d divise a.

On montrerait de même que d divise b, et donc d est bien un diviseur commun de a et b. En d'autres termes $a = dq$ et $b = dp$, avec q et p dans $\mathbb{N}$. Il en résulte que tout élément $au + bv$ de E peut s'écrire $dqu + dpv = d(qu + pv)$ et apparaît ainsi comme un multiple de d. Réciproquement un multiple de d est un élément de la forme ds avec $s \in \mathbb{Z}$, qui vérifie $ds = (au_0 + bv_0)s = a(u_0 s) + b(v_0 s)$ et appartient donc à E. On conclut que:

$$E = d\mathbb{Z}.$$

Pour finir, considérons un entier c qui est un diviseur commun de a et de b. Il existe donc des entiers m, n tels que $a = cm$ et $b = cn$. Tout élément $au + bv$ de E peut alors s'écrire $cmu + cnv = c(mu + nv)$. Ainsi tout élément de E est un multiple de c. C'est en particulier le cas de d, c'est-à-dire que c divise d. □

► *Remarque 1.* Il résulte immédiatement de la définition du pgcd que, pour tout $(a, b) \in \mathbb{Z}^2$: $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$. Et donc, *on peut toujours se ramener à considérer le pgcd de deux entiers naturels.* Il est clair par ailleurs que:

$\text{pgcd}(a, b) = \text{pgcd}(b, a)$; $(\text{pgcd}(a, b) = |a|) \Leftrightarrow (a \text{ divise } b)$; $\text{pgcd}(a, 0) = |a|$ et $\text{pgcd}(a, 1) = 1$.

► *Remarque 2.* Si a ou b est non-nul, l'ensemble $D_a \cap D_b$ est fini, et il résulte du théorème que le pgcd de a et b est simplement le plus grand élément de $D_a \cap D_b$ (pour l'ordre usuel des entiers).

► *Remarque 3.* Pour a et b deux entiers non-nuls, l'ensemble E considéré ci-dessus est noté de façon naturelle $a\mathbb{Z} + b\mathbb{Z}$. La preuve que l'on a donnée du théorème établit donc en fait la caractérisation suivante du pgcd de a et b :

$$\Big[\ d \text{ est le pgcd de } a \text{ et } b\ \Big] \ \Leftrightarrow\ \Big[\ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}, \quad \text{où } a\mathbb{Z} + b\mathbb{Z} = \{au + bv\,;\, u, v \in \mathbb{Z}\}\ \Big].$$

Exercice. Montrer que, pour tous $(a, b, c) \in \mathbb{Z}^3$, on a:

$$\mathrm{pgcd}(\mathrm{pgcd}(a, b)\,,\, c) = \mathrm{pgcd}(a\,,\, \mathrm{pgcd}(b, c)) \quad \textit{et} \quad \mathrm{pgcd}(ca, cb) = |c|\,\mathrm{pgcd}(a, b).$$

1.3 Entiers premiers entre eux

a) Définition. Deux entiers a et b sont dits PREMIERS ENTRE EUX lorsque leur pgcd est égal à 1.

En d'autres termes, a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1.

Lemme (très utile). *Soient a et b deux entiers non tous les deux nuls, et d leur pgcd. Alors $d \neq 0$, et les entiers uniques a' et b' définis par $a = da'$ et $b = db'$ sont premiers entres eux.*

Preuve. Si on avait $d = 0$, on aurait $a = 0$ ou $b = 0$. Donc $d \neq 0$. Il existe donc a' et b' dans $\mathbb{Z}$ uniques tel que $a = da'$ et $b = db'$. Il en résulte que, pour tout diviseur commun c de a' et b', l'entier cd est un diviseur commun de a et b, donc un diviseur de d (par définition du pgcd), d'où $c = \pm 1$. On conclut que $\mathrm{pgcd}(a', b') = 1$. □

b) Théorème de Bézout[5]. *Deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.*

Preuve. Posons $d = \mathrm{pgcd}(a, b)$. D'après la remarque 3 ci-dessus, on a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Si $d = 1$, il en résulte que $1 \in a\mathbb{Z} + b\mathbb{Z}$, et donc il existe u, v dans $\mathbb{Z}$ tels que $au + bv = 1$. Si réciproquement il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$; alors 1 appartient à $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc d divise 1, d'où $d = 1$. □

► Attention, pour $d \neq 1$, l'existence de u, v tels que $au + bv = d$ n'implique pas que d est le pgcd de a et b. Par exemple $3 \times 10 + (-2) \times 14 = 2$, mais 2 n'est pas le pgcd de 3 et -2.

► Attention, dans le théorème de Bézout, il n'y a pas unicité du couple (u, v); on verra plus loin lors de l'étude de l'algorithme d'Euclide comment calculer tous les couples (u, v) solutions.

c) Théorème de Gauss[6]. *Soient a, b, c trois entiers. Si a divise bc, et si a et b sont premiers entre eux, alors a divise c.*

Preuve. Comme $\mathrm{pgcd}(a, b) = 1$, il existe d'après le théorème de Bézout un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Donc $c = cau + cbv$. Comme a divise bc, on a $bc \in a\mathbb{Z}$, donc $bcv \in a\mathbb{Z}$. Par ailleurs, $acu \in a\mathbb{Z}$. Comme il est clair que la somme de deux multiples de a est un multiple de a, on conclut que $c = acu + bcv \in a\mathbb{Z}$. Ce qui achève la preuve. □

Exercice. Démontrer comme autre application du théorème de Bézout la proposition suivante: *Soient a, b, c trois entiers;*

(i) *a et bc sont premiers entre eux si et seulement si a et b sont premiers entre eux, et a et c sont premiers entre eux;*

(ii) *si a divise c et b divise c, et si a et b sont premiers entre eux, alors ab divise c.*

[5] Etienne Bézout, 1730-1783, mathématicien français connu en particulier pour ses travaux précurseurs en géométrie algébrique. A noter qu'une première preuve de ce résultat sur les entiers connu maintenant sous le nom de théorème de Bézout apparaît dès 1624 chez Bachet de Méziriac

[6] Johann Carl Friedrich Gauß, 1777-1855, mathématicien allemand, dont le surnom usuel de "prince des mathématiciens" traduit bien l'importance considérable de son œuvre et de son influence dans tous les domaines des mathématiques classiques.

2 Notion de congruence.

2.1 Relation de congruence

a) Définition. Soit n un entier naturel. Soient a et b deux entiers. On dit que a est CONGRU à b modulo n lorsque $a-b$ est divisible par n. On note alors $a \equiv b \bmod n$, ou encore $a \equiv b\,[n]$.

$$a \equiv b \bmod n \quad \Leftrightarrow \quad a-b \in n\mathbb{Z} \quad \Leftrightarrow \quad \exists\, k \in \mathbb{Z},\ a-b = nk.$$

► Il est clair que $a \equiv b \bmod n$ est équivalent à $b \equiv a \bmod n$; on dira donc alors simplement que a et b sont congrus modulo n.

► Chaque entier est congru à lui-même modulo n (en effet $a \equiv a \bmod n$ puisque $a-a=0$ est un multiple de n).

► Si $a \equiv b \bmod n$ et si $b \equiv c \bmod n$, alors $a \equiv c \bmod n$ (en effet, $a-c=(a-b)+(b-c)$ est un multiple de n comme somme de deux multiples de n). On pourra donc parler d'une famille d'entiers qui sont tous congrus entre eux modulo n pour dire qu'ils sont deux à deux congrus modulo n, ou encore que chacun d'eux est congru modulo n à l'un quelconque fixé d'entre eux.

Exemple. Considérons dans $\mathbb{Z}$ l'ensemble $E = \{-77, -17, -1, 7, 11, 19, 43, 139\}$. Tous les éléments de E sont congrus modulo 4 (la différence de deux quelconque d'entre eux est un multiple de 4) ; chacun d'eux est congru à 3 modulo 4.

Cette dernière observation n'est pas un cas particulier puisque le lemme suivant montre que, quel que soit $n \in \mathbb{N}^*$, on peut trouver pour tout entier a un entier naturel r qui est congru à a modulo n et qui strictement inférieur à n.

b) Lemme. *Soit n un entier naturel non-nul.*

(i) *Tout entier a est congru modulo n au reste de la division euclidienne de a par n.*

(ii) *Deux entiers a et b sont congrus modulo n si et seulement s'ils ont le même reste dans la division euclidienne par n.*

> *Preuve.* Soit $a = pn + r$ avec p, r dans $\mathbb{Z}$ tels que $0 \leqslant r < n$. On a $a - r = pn \in n\mathbb{Z}$, donc $x \equiv r \bmod n$, ce qui montre (i). Considérons de plus $b = p'n + r'$ avec p', r' dans $\mathbb{Z}$ tels que $0 \leqslant r' < n$. On a $a - b = (p-p')n + (r-r')$. Si $r = r'$, alors $a - b = (p-p')n \in n\mathbb{Z}$, donc $a \equiv b \bmod n$. Si $a \equiv b \bmod n$, alors $a-b \in n\mathbb{Z}$, donc $r-r' = a-b-(p-p')n$ est un multiple de n comme somme de deux multiples de n. Mais il résulte de $0 \leqslant r < n$ et $0 \leqslant r' < n$ que $-n < r - r' < n$, et donc le fait que $r-r'$ est divisible par n implique que $r - r' = 0$, ce qui achève la preuve. □

2.2 Classes de congruence

Le lemme précédent permet, pour un entier $n \in \mathbb{N}^*$ fixé, d'écrire l'ensemble $\mathbb{Z}$ comme la réunion d'exactement n sous-ensembles, dont chacun est formé d'entiers tous congrus entre eux modulo n.

Commençons par un exemple en prenant $n = 4$. D'après le lemme, chaque entier $a \in \mathbb{Z}$ est congru soit à 0, soit à 1, soit à 2, soit à 3 modulo 4. On note:

$\overline{0} = \{b \in \mathbb{Z};\ b \equiv 0 \bmod 4\} = \{4k;\ k \in \mathbb{Z}\} = 4\mathbb{Z}$ est l'ensemble des multiples de 4 ;
$\overline{1} = \{b \in \mathbb{Z};\ b \equiv 1 \bmod 4\} = \{4k+1;\ k \in \mathbb{Z}\} = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, \ldots\}$;
$\overline{2} = \{b \in \mathbb{Z};\ b \equiv 2 \bmod 4\} = \{4k+2;\ k \in \mathbb{Z}\} = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, \ldots\}$;
$\overline{3} = \{b \in \mathbb{Z};\ b \equiv 3 \bmod 4\} = \{4k+3;\ k \in \mathbb{Z}\} = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, \ldots\}$;

Il est clair que $\mathbb{Z}$ est la réunion de ces quatre sous-ensembles, et qu'ils sont deux à deux disjoints. Plus généralement, on peut définir:

a) Définition. *Soit n un entier naturel. Pour tout entier a, on appelle* CLASSE DE CONGRUENCE *de a modulo n l'ensemble de tous les entiers qui sont congrus à a modulo n. On note:*

$$\overline{a} \;=\; \{b \in \mathbb{Z}\,;\; b \equiv a \bmod n\} \;=\; \{a + kn\,;\; k \in \mathbb{Z}\}.$$

► Tout élément d'une classe $\overline{a}$ s'appelle un REPRÉSENTANT de cette classe $\overline{a}$. Dire qu'un entier b est un représentant de la classe $\overline{a}$ signifie donc que $a \equiv b \bmod n$, c'est-à-dire encore que $\overline{a} = \overline{b}$.

► Deux classes distinctes sont disjointes ; en d'autres termes, ou bien $\overline{a} = \overline{b}$, ou bien $\overline{a}$ et $\overline{b}$ n'ont aucun élément commun.

En effet, s'il existe $c \in \overline{a} \cap \overline{b}$, alors $c \equiv a \bmod n$ et $c \equiv b \bmod n$, ce qui implique $a \equiv b \bmod n$, donc $\overline{a} = \overline{b}$. □

► La réunion des classes de congruence est égal à l'ensemble $\mathbb{Z}$.

► On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de toutes les classes de congruences modulo n de tous les entiers.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}\,;\; a \in \mathbb{Z}\}.$$

Remarques

(i) Si $n = 0$, la relation de congruence modulo 0 est l'égalité dans $\mathbb{Z}$. Dans ce cas, on a $\overline{a} = \{a\}$ pour tout $a \in \mathbb{Z}$, et $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

(ii) Si $n = 1$, la relation de congruence modulo 1 est la relation triviale dans $\mathbb{Z}$, c'est-à-dire $a \equiv a \bmod 1$ quels que soient les entiers a et b. Donc $\overline{a} = \mathbb{Z}$ pour tout $a \in \mathbb{Z}$, et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

On ne considérera plus dans la suite que le cas où $n \geqslant 2$.

b) Théorème. *Soit n un entier naturel supérieur ou égal à 2.*

(i) *Pour tout $a \in \mathbb{Z}$, il existe un unique représentant de $\overline{a}$ qui appartient à $\{0, 1, 2, \ldots, n-1\}$.*

(ii) *il y a exactement n classes de congruences, à savoir : $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.*

(iii) $\mathbb{Z}$ est égal à la réunion de ces n classes et elles sont deux à deux disjointes.

Preuve. D'après le lemme vu au début de ce paragraphe, le reste de la division euclidienne de x par n est l'unique représentant de $\overline{a}$ qui appartient à $\{0, 1, 2, \ldots, n-1\}$, d'où (i). Le point (ii) découle directement de (i), et (iii) résulte des propriétés vues plus haut des classes de congruences. □

Avec la notation vue plus haut, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc un ensemble fini à n éléments:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

2.3 Opérations sur les classes de congruence

a) Proposition. *Pour tout entier naturel n, la relation de congruence modulo n est compatible avec l'addition et avec la multiplication, ce qui signifie que, quels que soient des entiers a, b, c, d:*

si $a \equiv b \bmod n$ *et si* $c \equiv d \bmod n$, *alors* $a + c \equiv b + d \bmod n$

et

si $a \equiv b \bmod n$ *et si* $c \equiv d \bmod n$, *alors* $a \times c \equiv b \times d \bmod n$.

Preuve. On a $a - b \in n\mathbb{Z}$ et $c - d \in n\mathbb{Z}$. La somme $(a + c) - (b + d) = (a - b) + (c - d)$ est bien un multiple de n comme somme de deux multiples de n, ce qui prouve que $a + c \equiv b + d \bmod n$. Par ailleurs, $ac - bd = a(c - d) + (a - c)d$. Le fait que $c - d \in n\mathbb{Z}$ implique que $a(c - d) \in n\mathbb{Z}$. De même $(a - c) \in n\mathbb{Z}$ implique que $(a - c)d \in n\mathbb{Z}$, et donc la somme $a(c - d) + (a - c)d$ appartient à $n\mathbb{Z}$, ce qui prouve que $ac \equiv bd \bmod n$. □

Une application fondamentale de cette proposition est la possibilité de munir l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence d'opérations $+$ et $\times$ définies à partir des opérations correspondantes dans $\mathbb{Z}$.

> Principe: soient $\overline{a}$ et $\overline{c}$ deux classes de congruence dans $\mathbb{Z}/n\mathbb{Z}$. On veut définir le somme des deux classes $\overline{a}+\overline{c}$. L'idée naturelle est de poser $\overline{a}+\overline{c}=\overline{a+c}$. Le problème est que cette définition semble dépendre des représentants a et c de ces deux classes...
>
> En d'autres termes, si on prend un autre représentant b dans $\overline{a}$, et un autre représentant d dans $\overline{c}$, on a $\overline{b}=\overline{a}$ et $\overline{c}=\overline{d}$: a-t-on bien $\overline{a}+\overline{c}=\overline{b}+\overline{d}$? C'est-à-dire, a-t-on bien $\overline{a+c}=\overline{b+d}$? La proposition précédente affirme que la réponse est positive, puisque $a+c\equiv b+d \bmod n$!
>
> Le raisonnement étant identique pour la multiplication, on peut conclure:

On définit, indépendamment des représentants choisis dans les classes de congruence, une addition et une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par:

pour toutes classes $\overline{a}$ et $\overline{b}$ dans $n\mathbb{Z}$, on pose: $\quad \overline{a}+\overline{b}=\overline{a+b} \quad$ *et* $\quad \overline{a}\times\overline{b}=\overline{ab}.$

Les opérations ainsi définies sur $\mathbb{Z}/n\mathbb{Z}$ héritent des propriétés des opérations sur $\mathbb{Z}$.

> *Remarque d'ordre "culturel" :* en algèbre, on traduit plus précisément ces propriétés en disant que $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif, et plus précisément encore que c'est l'anneau quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Concrètement: calculer modulo n, c'est-à-dire calculer sur les classes de congruences modulo n, consiste à identifier chaque entier a avec le reste de la division euclidienne de a par n.

> *Exemple.* Dans $\mathbb{Z}/7\mathbb{Z}$, on calcule par exemple : $\overline{4}+\overline{2}=\overline{6}$; $\overline{4}+\overline{5}=\overline{2}$ (car $9\equiv 2 \bmod 7$) ; $\overline{3}\times\overline{2}=\overline{6}$; $\overline{4}\times\overline{2}=\overline{1}$ (car $8\equiv 1 \bmod 7$) ; $\overline{3}^3=\overline{6}$ (car $27\equiv 6 \bmod 7$).

Comme illustration, donnons les tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour les premières valeurs de n ($2\leqslant n\leqslant 6$) :

$\mathbb{Z}/2\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\mathbb{Z}/3\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/4\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/5\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/6\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

3 Exemples d'application des congruences

3.1 Preuve par 9

Il s'agit d'un petit test classique dans la tradition scolaire pour détecter certaines erreurs dans le résultat d'une multiplication (attention: c'est une condition nécessaire, mais pas suffisante; en d'autres termes, si le test est négatif, c'est que le résultat de la multiplication est faux, mais le test peut tre positif avec un résultat faux...

Exemple: considérons la multiplication $745 \times 521 = 388145$.

Modulo 9, la somme des chiffres de 745 est $s_1 = 7$, et la somme des chiffres de 521 est $s_2 = 8$.

Le produit $s_1 \times s_2$ vaut 56, c'est-à-dire 2 modulo 9.

La somme des chiffres du résultat est 29, c'est-à-dire encore 2 modulo 9 $\rightarrow$ le test est positif.

Proposition.

(i) *Tout entier naturel est congru modulo 9 à la somme des chiffres de son écriture décimale.*

(ii) *Soient* $x, y, z \in \mathbb{N}$ *; notons* $x = \overline{a_n \dots a_0}$, $y = \overline{b_m \dots b_0}$, $z = \overline{c_p \dots c_0}$ *leurs écritures décimales.*

$$\textit{Si } \ xy = z, \ \textit{ alors: } \ \Big(\sum_{i=0}^{n} a_i\Big)\Big(\sum_{i=0}^{m} b_i\Big) \equiv \Big(\sum_{i=0}^{p} c_i\Big) \bmod 9.$$

Preuve. Soit $x = \overline{a_n \dots a_0}$; donc $x = \sum_{i=0}^{n} a_i 10^i$. Or pour tout $i \in \mathbb{N}$, on a $10^i = (9+1)^i \equiv 1 \bmod 9$, donc $a_i 10^i \equiv a_i \bmod 9$. On déduit $x \equiv \sum_{i=0}^{n} a_i \bmod 9$. Ce qui prouve (i).

Le (ii) est alors une conséquence immédiate de la compatibilité de la congruence modulo 9 avec la multiplication, puisque:

$$\Big[\ x \equiv \sum_{i=0}^{n} a_i \bmod 9\ \Big] \ \text{ et } \ \Big[\ y \equiv \sum_{i=0}^{m} b_i \bmod 9\ \Big] \ \text{ impliquent } \ \Big[\ xy \equiv \Big(\sum_{i=0}^{n} a_i\Big)\Big(\sum_{i=0}^{m} b_i\Big) \bmod 9\ \Big]. \ \square$$

Remarques. Comme on le mentionnait ci-dessus, la proposition donne une condition nécessaire pour l'égalité $xy = z$ (qui permet par contraposée de repérer une erreur éventuelle dans le calcul du produit xy), mais elle n'est pas suffisante. En effet, si l'on écrit $z = \overline{c_p \dots c_1 c_2 c_0}$ au lieu de $z = \overline{c_p \dots c_2 c_1 c_0}$, la congruence reste réalisée.

De plus, il est clair que la proposition reste vraie si l'on remplace 10 par une base de numération quelconque b, et 9 par $b-1$ ("preuve par $b-1$").

3.2 Critères de divisibité et théorème de Pascal[7]

Savoir si un entier est divisible par un autre sans effectuer la division euclidienne est souvent très utile en arithmétique. D'où l'intérêt pratique de critères tels que ceux que résume l'énoncé suivant.

Théorème.

Soit $m \in \mathbb{N}^*$. *On définit une suite* (r_i) *d'entiers dans* $\{0, 1, 2, \dots, m-1\}$ *par:*

$$r_0 = 1 \quad \textit{et} \quad r_{i+1} = \textit{le reste de la division euclidienne de } 10r_i \textit{ par } m.$$

Alors, pour tout entier naturel $x = \overline{a_n \dots a_0}$ *en numération décimale, on a:*

$$x \equiv \sum_{i=0}^{n} a_i r_i \bmod m.$$

[7] Blaise Pascal, 1623-1662, mathématicien, physicien et philosophe français, dont les contributions en géométrie, en calcul infinitésimal, en arithmétique et sur l'origine de la théorie des probabilités sont de grande importance dans l'histoire des mathématiques.

Preuve. Il suffit de montrer que: pour tout $i \in \mathbb{N}$, on a $r_i \equiv 10^i \bmod m$, car cela implique $a_i r_i \equiv a_i 10^i \bmod m$, d'où $x = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i r_i \bmod m$.

Pour montrer donc la congruence voulue, on fait une preuve par récurrence. Pour $i = 0$, on a $r_0 = 1$ donc $r_0 \equiv 10^0 \bmod m$. Supposons (H.R.) que $r_i \equiv 10^i \bmod m$. Alors $10r_i \equiv 10^{i+1} \bmod m$. Mais par définition de la suite des r_i, on a: $10r_i = q_i m + r_{i+1}$ pour un certain quotient $q_i \in \mathbb{N}$. Donc $r_{i+1} \equiv 10r_i \bmod m$. Finalement, $r_{i+1} \equiv 10^{i+1} \bmod m$, ce qui est la propriété voulue à l'ordre $i+1$. □

Exemples.

• Pour $m = 3$, on a $r_0 = 1$, $r_1 = 1$ car $10 = 3 \times 3 + 1$, et donc $r_i = 1$ pour tout $i \in \mathbb{N}$. Avec les notations du théorème: $x \equiv \sum_{i=0}^{n} a_i \bmod 3$. Il en résulte que:

$$[x = \overline{a_n \dots a_0} \text{ divisible par } 3] \Leftrightarrow [\sum_{i=0}^{n} a_i \text{ divisible par } 3]$$

• Pour $m = 9$, on a aussi $r_i = 1$ pour tout $i \in \mathbb{N}$, car $10 = 1 \times 10 + 1$. Donc comme ci-dessus:

$$[x = \overline{a_n \dots a_0} \text{ divisible par } 9] \Leftrightarrow [\sum_{i=0}^{n} a_i \text{ divisible par } 9]$$

• Pour $m = 5$, on a $r_0 = 1$, $r_1 = 0$ car $10 = 2 \times 5 + 0$, et donc $r_i = 0$ pour tout $i \in \mathbb{N}^*$. Avec les notations du théorème: $x \equiv a_0 \bmod 5$. Il en résulte que:

$$[x = \overline{a_n \dots a_0} \text{ divisible par } 5] \Leftrightarrow [a_0 \text{ divisible par } 5] \Leftrightarrow [a_0 = 0 \text{ ou } a_0 = 5]$$

• Pour $m = 6$, on a $r_0 = 1$, $r_1 = 4$ car $10 = 1 \times 6 + 4$, puis $r_2 = 4$ car $10 \times 4 = 6 \times 6 + 4$, et ensuite $r_i = 4$ pour tout $i \in \mathbb{N}^*$. Avec les notations du théorème: $x \equiv a_0 + \sum_{i=1}^{n} 4a_i \bmod 6$. Il en résulte:

$$[x = \overline{a_n \dots a_0} \text{ divisible par } 6] \Leftrightarrow [a_0 + \sum_{i=1}^{n} 4a_i \text{ divisible par } 6]$$

• Pour $m = 11$, on a $r_0 = 1$, $r_1 = 10$ car $10 = 0 \times 11 + 10$, puis $r_2 = 1$ car $10 \times 10 = 9 \times 11 + 1$, et ensuite $r_i = 1$ pour tout i pair et $r_i = 10$ pour tout i impair. Comme de plus $10 \equiv -1 \bmod 11$, On a avec les notations du théorème: $x \equiv \sum_{i=0}^{n} (-1)^i a_i \bmod 11$. Il en résulte que:

$$[x = \overline{a_n \dots a_0} \text{ divisible par } 11] \Leftrightarrow [a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n \text{ divisible par } 11]$$

3.3 Clefs de contrôle de codes numériques

a) Exemple des UPC. Le code barre d'un produit (Universal Product Code) est, dans le système usuel EAN 13 (European Article Numbering) une suite de treize chiffres compris entre 0 et 9. Les douze premiers $a_1 a_2 a_3 \dots a_{12}$ sont les chiffres significatifs qui identifient le produit. Le treizième a_{13} est une clef de contrôle pour détecter d'éventuelles erreurs de saisie, qui est définie par:

$$3 \sum_{i=1}^{6} a_{2i} + \sum_{i=0}^{6} a_{2i+1} \equiv 0 \bmod 10.$$

Cette formule définit bien effectivement l'entier a_{13}

En effet: Posons $s = 3 \sum_{i=1}^{6} a_{2i} + \sum_{i=0}^{5} a_{2i+1}$.

Il existe un et en seul entier a_{13} qui soit compris entre 0 et 9 et qui vérifie $s + a_{13} \equiv 0 \bmod 10$. C'est l'unique représentant compris entre 0 et 9 dans la classe de congruence $\overline{-s}$ modulo 10, c'est-à-dire encore le reste de la division euclidienne de $-s$ par 10, ou encore le complément à 10 du reste de la division euclidienne de s par 10.

Considérons par exemple le code barre dont les douze chiffres d'identification sont: 5 271485 33113. On calcule $s = 3(2+1+8+3+1+3) + (5+7+4+5+3+1) = 3 \times 18 + 25 = 79$. Donc $a_{13} = 1$. Le code barre complet est donc: 5 271485 331131.

1. Supposons qu'une erreur de saisie sur un chiffre ait conduit à 5 271484 331131. Le calcul sur les douze chiffres significatifs donne: $s' = 3(2+1+8+3+1+3)+(5+7+4+4+3+1) = 3\times 18+24 = 78$. La clef de contrôle devrait alors être 2, et donc l'erreur est détectée.

2. Supposons qu'une permutation de chiffres à la saisie ait conduit à 5 217485 33113. Le calcul sur les douze chiffres significatifs donne: $s'' = 3(2+7+8+3+1+3)+(5+1+4+4+3+1) = 3\times 24+18 = 90$. La clef de contrôle devrait alors être 0, et donc l'erreur est détectée.

3. Supposons qu'une permutation de chiffres à la saisie ait conduit à 5 721485 331131. Le calcul sur les douze chiffres significatifs donne: $s''' = 3(7+1+8+3+1+3)+(5+2+4+5+3+1) = 3\times 23+20 = 89$. La clef de contrôle est alors encore 1, et donc l'erreur n'est pas détectée !

On peut en fait préciser quels types d'erreurs sont ou non détectés :

Proposition.

(i) *Si un et un seul des douze chiffres significatifs est erroné, alors l'erreur est détectée par la clef de contrôle.*

(ii) *Si deux chiffres consécutifs parmi les douze chiffres significatifs sont intervertis, alors l'erreur est détectée par la clef de contrôle si et seulement si la différence de ces deux chiffres n'est pas un multiple de 5.*

Preuve. Supposons qu'un et un seul des chiffres a_j ait été remplacé par un chiffre $b_j \neq a_j$. En notant $s = 3\sum_{i=1}^{6} a_{2i} + \sum_{i=0}^{5} a_{2i+1}$ la somme à calculer pour le code exact, la nouvelle somme à calculer pour le code avec un chiffre changé devient $s' = s + b_j - a_j$ si j est impair, et $s' = s+3(b_j-a_j)$ si j est pair. Comme $s+a_{13} \equiv 0 \bmod 10$ par hypothèse, dire que l'erreur n'est pas détectée équivaut à dire que la même clef a_{13} vérifie aussi $s' + a_{13} \equiv 0 \bmod 10$, c'est-à-dire que $b_j-a_j \equiv 0 \bmod 10$ dans le premier cas, et $3(b_j-a_j) \equiv 0 \bmod 10$ dans le second cas. Comme $-9 \leqslant b_j - a_j \leqslant 9$, on ne peut avoir que $b_j - a_j = 0$, ou $3(b_j - a_j) = 0$, ou $3(b_j - a_j) = 10$, ou $3(b_j - a_j) = 20$. Par le lemme de Gauss (et parce que 3 est premier avec 10 et 20) toutes ces idendités conduisent à $b_j - a_j = 0$. Or on avait supposé que $b_j \neq a_j$. On conclut que la clef a_{13} ne peut pas convenir pour le second code, et donc l'erreur est détectée.

Supposons que deux chiffres consécutifs a_{2k-1} et a_{2k} (avec $1 \leqslant k \leqslant 6$) aient été intervertis. L'erreur n'est pas détectée si et seulement si $3a_{2k} + a_{2k-1} \equiv 3a_{2k-1} + a_{2k} \bmod 10$, ce qui équivaut à : $2a_{2k-1} - 2a_{2k} \equiv 0 \bmod 10$, et finalement à : $a_{2k-1} - a_{2k} \equiv 0 \bmod 5$. On conclut de même lorsque les deux chiffres consécutifs inversés sont de la forme a_{2k} et a_{2k+1}. □

b) Autres exemples.

• Le numéro INSEE est formé de 13 chiffres significatifs, suivi d'une clef de contrôle à deux chiffres. Cette clef $c = a_{14}a_{15}$ est définie comme le complément à 97 du reste r de la division euclidienne par 97 de l'entier naturel dont l'écriture décimale est la suite des 13 chiffres significatifs ($c = 97 - r$).

• Les numéros d'identité bancaire des RIB comportent 21 chiffres significatifs (code banque en 5 chiffres, code agence en 5 chiffres, code compte client en 11 chiffres), suivis d'une clef de contrôle à deux chiffres. En appelant n l'entier dont les 21 chiffres significatifs constituent l'écriture en base 10, la clef $c = a_{22}a_{23}$ est le complément à 97 du reste r de la division euclidienne par 97 de $n \times 100$.

• Le code ISBN sert à identifier les livres publiés pour leur catalogage. Il est constitué de dix chiffres (séparés par des espaces ou des tirets), donc les neuf premiers $a_1a_2\ldots a_9$ sont compris entre 0 et 9, et dont le dixième a_{10} est soit compris entre 0 et 9, soit la lettre X représentant l'entier 10. Les neufs premiers sont significatifs (pays, éditeurs,...) et la dixième est un clef donnée par $\sum_{i=1}^{10} ia_i \equiv 0 \bmod 11$. Elle permet de détecter un chiffre inexact ou l'intervention de deux chiffres.

• Dans le numéro à 16 chifres d'une carte bancaire, les 15 premiers sont significatifs (type de carte, établissement bancaire, numéro de carte) et le 16ème est un clef calculée par la formule de Lühn: si $a_1, a_2, \ldots, a_{15}$ sont les quinze chiffres significatifs, on calcule $s = \sum_{i=1}^{7} a_{2i} + \sum_{j=0}^{7} b_{2j+1}$, où b_{2j+1} est l'entier à un chiffre égal à la somme des chiffres dans l'écriture décimale de $2 \times a_{2j+1}$. La clef c est alors le complément à 10 du reste de la division euclidienne de s par 10.

• Chaque billet de banque en euros comporte un numéro constitué d'une lettre suivie de 11 chiffres. On calcule d'abord la somme s de ces 11 entiers avec l'entier (compris entre 1 et 26) correspondant au rang alphabétique de la lettre (1 pour A, 2 pour B,..., 26 pour Z). Le reste de la division euclidienne de s par 9 doit toujours être à 8. Remarquons que, d'après le point 1 de la proposition vue pour la preuve par 9, ce reste est aussi celui de la division euclidienne par 9 de la somme des chiffres dans l'écriture décimale de s.

3.4 Systèmes de congruences et théorème des restes chinois

a) Introduction. D'innombrables petits problèmes concrets (les recueils d'énigmes mathématiques en regorgent) apparaissent comme liés à la question abordée ici. Le nom de "théorème des restes chinois" qui y est traditionnellement attaché semble faire allusion à différents traités de la Chine ancienne (Sun Zi au IIIème siècle, Qin Jiushao au XIIIème siècle) mentionnant des questions de nature mathématique comme:

- Sachant qu'il reste aujourd'hui 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?
- Combien l'arme de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

Le premier problème revient à trouver un entier x vérifiant les deux conditions: $\begin{cases} x \equiv 6 \bmod 365 \\ x \equiv 3 \bmod 28 \end{cases}$,

le second à trouver un entier y vérifiant les trois conditions: $\begin{cases} y \equiv 2 \bmod 3 \\ y \equiv 3 \bmod 5 \\ y \equiv 2 \bmod 7 \end{cases}$

b) Remarque préliminaire. Si a et b sont deux entiers premiers entre eux, alors l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et b est égal à l'ensemble $ab\mathbb{Z}$ des multiples de leur produit.

> *Preuve.* Il est clair que tout multiple de ab est un multiple de a et un multiple de b. Réciproquement, soit m un multiple commun de a et b. Il existe des entiers p et q tels que $m = ap = bq$. En particulier, a divise bq. Comme a et b sont premiers entre eux, cela implique avec le lemme de Gauss que a divise q. Il existe donc un entier r tel que $q = ar$. Ainsi $m = bq = bar$, ce qui prouve que m est un multiple de ab. □

c) Proposition. *Soient a et b deux entiers naturels non-nuls que l'on suppose premiers entre eux. Alors, quels que soient des entiers α et β arbitrairement fixés, le système de congruences :*

$$(\Sigma) \quad \begin{cases} x \equiv \alpha \bmod a \\ x \equiv \beta \bmod b \end{cases}$$

admet des solutions dans $\mathbb{Z}$. Plus précisément, l'ensemble des solutions de (Σ) dans $\mathbb{Z}$ est :

$$S = \{au\beta + bv\alpha + \lambda ab\,;\, \lambda \in \mathbb{Z}\},$$

où (u, v) désigne un couple d'entiers tels que $au + bv = 1$.

Preuve. Fixons α et β quelconques et considérons le système (Σ) associé. Comme a et b sont premiers entre eux, il existe d'après le théorème de Bézout des entiers u, v tels que $au + bv = 1$. Posons alors $x_0 = au\beta + bv\alpha$. Il est clair que $x_0 \equiv au\beta \bmod b$. Or $au\beta \equiv \beta \bmod b$ car $au \equiv 1 \bmod b$. Ainsi, $x_0 \equiv \beta \bmod b$. On démontre de même que $x_0 \equiv \alpha \bmod a$. On conclut que l'ensemble des solutions de (Σ) n'est pas vide puisqu'il contient au moins x_0.

Dès lors, un entier x appartient à S si et seulement si $x - x_0 \equiv 0 \bmod a$ et $x - x_0 \equiv 0 \bmod b$, c'est-à-dire si et seulement si $x - x_0$ est un multiple commun de a et b. On conclut grâce à la remarque préliminaire que S est l'ensemble des entiers x qui s'écrivent $x = x_0 + \lambda ab$ pour un certain $\lambda \in \mathbb{Z}$. □

d) Cas des systèmes de plus de deux congruences. Soient $a_1, a_2, \ldots, a_n$ des entiers naturels non-nuls deux à deux premiers entre eux. On fixe des entiers $\alpha_1, \alpha_2, \ldots, \alpha_n$ quelconques et l'on considère le système (Σ) de n congruences à une inconnue:

$$(\Sigma): \quad x \equiv \alpha_1 \bmod a_1, \quad x \equiv \alpha_2 \bmod a_2, \quad \ldots, \quad x \equiv \alpha_n \bmod a_n.$$

On pose $b = a_1 a_2 \ldots a_n$. Pour tout $1 \leqslant i \leqslant n$, on considère le produit $b_i = a_1 a_2 \ldots a_{i-1} a_{i+1} \ldots a_n$ et le système de congruences :

$$(\Sigma_i) \begin{cases} x \equiv 1 \bmod a_i \\ x \equiv 0 \bmod b_i \end{cases}$$

- On montre alors (le faire en exercice) que:
  - ► (Σ) *a des solutions dans* $\mathbb{Z}$ *et, pour tout* $1 \leqslant i \leqslant n$, (Σ_i) *a des solutions dans* $\mathbb{Z}$,
  - ► *l'ensemble des solutions de* (Σ) *dans* $\mathbb{Z}$ *est:*

$$S = \{\, \alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_n y_n + b\lambda \,;\, \lambda \in \mathbb{Z} \,\}$$

  où y_i *désigne pour tout* $1 \leqslant i \leqslant n$ *une solution de* (Σ_i).

- Développons à titre d'illustration de la méthode, l'exemple du système $(\Sigma) \begin{cases} x \equiv 7 \bmod 4 \\ x \equiv 2 \bmod 3 \\ x \equiv 4 \bmod 5 \end{cases}$

On a ici: $a_1 = 4$, $a_2 = 3$, $a_3 = 5$, $\alpha_1 = 7$, $\alpha_2 = 2$, $\alpha_3 = 4$, $b = 60$, $b_1 = 15$, $b_2 = 20$, $b_3 = 12$,

et on introduit les systèmes: $(\Sigma_1) \begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 0 \bmod 15 \end{cases}$ $(\Sigma_2) \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 0 \bmod 20 \end{cases}$ $(\Sigma_3) \begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 0 \bmod 12 \end{cases}$

Comme 4 et 15 sont premiers entre eux, (Σ_1) a des solutions; une solution évidente est: $y_1 = 45$.
Comme 3 et 20 sont premiers entre eux, (Σ_2) a des solutions; une solution évidente est: $y_2 = 40$.
Comme 5 et 12 sont premiers entre eux, (Σ_3) a des solutions; une solution évidente est: $y_3 = 36$.

$$\left.\begin{array}{lcl} y_1 \equiv 1 \bmod 4 & \Rightarrow & \alpha_1 y_1 = 7y_1 \equiv 7 \bmod 4 \\ y_2 \equiv 0 \bmod 20 & \Rightarrow & \alpha_2 y_2 = 2y_2 \equiv 0 \bmod 4 \\ y_3 \equiv 0 \bmod 12 & \Rightarrow & \alpha_3 y_3 = 4y_3 \equiv 0 \bmod 4 \end{array}\right\} \Rightarrow\ x_0 := \alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3 \equiv 7 \bmod 4$$

$$\left.\begin{array}{lcl} y_1 \equiv 0 \bmod 15 & \Rightarrow & \alpha_1 y_1 = 7y_1 \equiv 0 \bmod 3 \\ y_2 \equiv 1 \bmod 3 & \Rightarrow & \alpha_2 y_2 = 2y_2 \equiv 2 \bmod 3 \\ y_3 \equiv 0 \bmod 12 & \Rightarrow & \alpha_3 y_3 = 4y_3 \equiv 0 \bmod 3 \end{array}\right\} \Rightarrow\ x_0 = \alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3 \equiv 2 \bmod 3$$

$$\left.\begin{array}{lcl} y_1 \equiv 0 \bmod 15 & \Rightarrow & \alpha_1 y_1 = 7y_1 \equiv 0 \bmod 5 \\ y_2 \equiv 0 \bmod 20 & \Rightarrow & \alpha_2 y_2 = 2y_2 \equiv 0 \bmod 5 \\ y_3 \equiv 1 \bmod 5 & \Rightarrow & \alpha_3 y_3 = 4y_3 \equiv 3 \bmod 5 \end{array}\right\} \Rightarrow\ x_0 = \alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3 \equiv 3 \bmod 5$$

L'entier $s = 7 \times 45 + 2 \times 40 + 4 \times 36 = 539$ est donc une solution particulière de (Σ).
Il est clair qu'un entier x appartient à l'ensemble S de toutes les solutions de (Σ) si et seulement $x - x_0$ vérifie à la fois $x - x_0 \equiv 0 \bmod 4$, $x - x_0 \equiv 0 \bmod 3$, et $x - x_0 \equiv 0 \bmod 5$. Ceci équivaut à dire que $x - x_0$ est multiple de 60. On conclut que $S = \{539 + 60\lambda\,;\, \lambda \in \mathbb{Z}\}$.

e) Une interprétation algébrique (plus théorique) du théorème des restes chinois. Soient a et b deux entiers non-nuls premiers entre eux. On note $\mathbb{Z}/a\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{a-1}\}$ l'ensemble des classes de congruence modulo a. En utilisant une notation permettant de différencier les classes modulo a des classes modulo b, on note $\mathbb{Z}/b\mathbb{Z} = \{\widetilde{0}, \widetilde{1}, \widetilde{2}, \ldots, \widetilde{b-1}\}$. Enfin on peut considérer les classes modulo ab, et donc $\mathbb{Z}/ab\mathbb{Z} = \{\widehat{0}, \widehat{1}, \widehat{2}, \ldots, \widehat{ab-1}\}$.

En rappelant que la notation $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ désigne l'ensemble des couples dont le premier terme est un élément de $\mathbb{Z}/a\mathbb{Z}$ et le second terme est un élélement de $\mathbb{Z}/b\mathbb{Z}$, on définit l'application:

$$\begin{array}{rccc} f: & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & \widehat{x} & \longmapsto & (\overline{x}, \widetilde{x}) \end{array}$$

• Cette application f est effectivement bien définie au sens où, si x et y sont deux entiers représentants de la même classe modulo ab, c'est-à-dire tels que $\widehat{x} = \widehat{y}$, alors $\overline{x} = \overline{y}$ et $\widetilde{x} = \widetilde{y}$. Cela résulte du fait que $x - y \equiv 0 \bmod ab$ implique à la fois $x - y \equiv 0 \bmod a$ et $x - y \equiv 0 \bmod b$.

• Cette application f est un morphisme pour l'addition, ce qui signifie que,
pour tous $x, y \in \mathbb{Z}$, on a $f(\widehat{x} + \widehat{y}) = f(\widehat{x}) + f(\widehat{y})$.

Cela résulte du fait que $f(\widehat{x} + \widehat{y}) = f(\widehat{x+y}) = (\overline{x+y}, \widetilde{x+y}) = (\overline{x}, \widetilde{x}) + (\overline{y}, \widetilde{y}) = f(\widehat{x}) + f(\widehat{y})$.

• De même, f est un morphisme pour la multiplication, ce qui signifie que,
pour tous $x, y \in \mathbb{Z}$, on a $f(\widehat{x} \times \widehat{y}) = f(\widehat{x}) \times f(\widehat{y})$.

• Le point crucial est que f est surjective, ce qui signifie que, quelles que soient deux classes $\overline{\alpha} \in \mathbb{Z}/a\mathbb{Z}$ et $\widetilde{\beta} \in \mathbb{Z}/b\mathbb{Z}$, il existe un entier x tel que $(\overline{\alpha}, \widetilde{\beta}) = f(\widehat{x})$. Et ceci est une traduction immédiate de la proposition c) ci-dessus !

• Comme les ensembles finis $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ont le même nombre d'éléments (à savoir ab éléments), la surjectivité suffit pour conclure que f est bijective.

• On synthétise ces propriétés en disant que: *si a et b sont premiers entre eux, alors f est un isomorphisme d'anneaux de $\mathbb{Z}/ab\mathbb{Z}$ sur $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$*, ce qui est un autre énoncé courant du théorème des restes chinois.

• A noter que l'on peut aussi démontrer la réciproque, c'est-à-dire que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ab\mathbb{Z}$ si et seulement si a et b sont premiers entre eux.

f) Exercice. Résoudre les systèmes de congruence correspondant aux deux exemples préliminaires de l'introduction a) ci-dessus.

4 Congruences et cryptographie[8]

4.1 Codages monographiques

a) Principe. On note: $\mathcal{A} = \{A, B, C, D, \ldots, Y, Z\}$ l'alphabet, et $\mathcal{E} = \{0, 1, 2, 3, \ldots, 24, 25\}$ l'ensemble des 26 premiers entiers naturels. On considère la bijection naturelle g de $\mathcal{A}$ sur $\mathcal{E}$ consistant à numéroter les lettres:

$$g(A) = 0,\ g(B) = 1,\ g(C) = 2,\ g(D) = 3,\ \ldots\ldots,\ g(Y) = 24,\ g(Z) = 25.$$

Coder un message littéral consiste alors à introduire une bijection f de $\mathcal{E}$ sur $\mathcal{E}$, et à transformer dans un message :

- chaque lettre α par le nombre $n := g(\alpha)$ qui la numérote,
- puis le nombre n par le nouveau nombre $m := f(n)$,
- puis le nombre m par la lettre $\beta := g^{-1}(m)$ qu'il numérote.

[8] Cette section utilise largement le chapitre 5 de l'ouvrage collectif "Arithmétique" publié par l'IREM de Clermont-Ferrand et le CRDP d'Auvergne en 1998.

En résumé, le codage consiste à appliquer: $\begin{array}{ccccccc} \mathcal{A} & \xrightarrow{g} & \mathcal{E} & \xrightarrow{f} & \mathcal{E} & \xrightarrow{g^{-1}} & \mathcal{A} \\ \alpha & \longmapsto & g(\alpha) & \longmapsto & f(g(\alpha)) & \longmapsto & g^{-1}(f(g(\alpha))) \end{array}$

et le décodage consiste à appliquer: $\begin{array}{ccccccc} \mathcal{A} & \xrightarrow{g} & \mathcal{E} & \xrightarrow{f^{-1}} & \mathcal{E} & \xrightarrow{g^{-1}} & \mathcal{A} \\ \beta & \longmapsto & g(\beta) & \longmapsto & f^{-1}(g(\beta)) & \longmapsto & g^{-1}(f^{-1}(g(\beta))) \end{array}$

Comme dans toute action cryptographique, le processus doit permettre :

- un codage facile dans un temps raisonnable (appliquer f quand on le connaît) par l'émetteur du message,
- un décodage facile dans un temps raisonnable (appliquer f^{-1} quand on connaît f) par le destinataire du message,
- un décryptage difficile (trouver f quand on ne le connaît pas) pour un éventuel intercepteur du message, auquel l'information n'est pas destinée, et qui veut casser le code pour y accéder.

b) Choix de la permutation de codage. Il est bien connu (et facile à démontrer, faites-le !) que, si l'on se donne un ensemble fini $\mathcal{E}$ de N objets, il y a exactement $N!$ façons de permuter ces objets, c'est-à-dire $N!$ bijections de $\mathcal{E}$ sur $\mathcal{E}$ (de telles bijections sont appeler des PERMUTATIONS sur N objets, et l'ensemble de ces $N!$ permutations est appelé le groupe symétrique).

Ici $\mathcal{E} = \{0, 1, 2, 3, \ldots, 24, 25\}$, avec $N = 26$, donc il existe $26!$ façon de choisir la permutation f.

L'entier $26!$ est évidemment "très grand" ($26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 > 4.10^{26}$), mais la pratique du codage et du décodage incite à privilégier des choix de f qui ne sont pas arbitraires (obligeant le codeur et le décodeur à disposer de la table complète des 26 correspondances), mais qui obéissent à une règle simple, basée sur un principe de déduction arithmétique, facile à mettre en œuvre et à modifier si nécessaire.

> *Remarque.* On exige parfois dans le choix de la permutation de codage qu'elle ne conserve aucune lettre inchangée. Cela revient à dire que f est un DÉRANGEMENT de $\mathcal{E}$, c'est-à-dire une permutation de $\mathcal{E}$ qui ne fixe aucun élément de $\mathcal{E}$ (on a $f(n) \neq n$ quel que soit $n \in \mathcal{E}$). Une formule est connue, qui donne le nombre de dérangements sur un ensemble à N éléments :
>
> $$N! \sum_{i=0}^{N} \frac{(-1)^i}{i!}.$$
>
> Avec ici $N = 26$, le nombre de dérangements est ici égal à 148 362 637 348 470 135 821 287 825 qui demeure "très grand" (supérieur à 10^{26}). A noter de plus que l'information qu'aucune lettre est inchangée peut devenir un indice supplémentaire pour le cryptoanalyste qui cherche à casser le code (voir plus loin).

c) Exemple élémentaire: codages par translations. On prête à Jules César l'emploi d'un codage consistant à décaler chaque lettre de 3 rangs, c'est-à-dire à utiliser la permutation :

$$A \to D, \quad B \to E, \quad C \to F, \quad D \to G, \ldots\ldots, V \to Y, \quad W \to Z, \quad X \to A, \quad Y \to B, \quad Z \to C,$$

c'est-à-dire la permutation:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 0 & 1 & 2 \end{pmatrix}.$$

La permutation de codage f est donc donnée par:

pour tout $n \in \mathcal{E}$, $f(n)$ est l'unique élément de $\mathcal{E}$ tel que $f(n) \equiv n + 3 \bmod 26$,

c'est-à-dire encore que $f(n)$ est le reste de la division euclidienne de $n + 3$ par 26.

Réciproquement, le décodage est alors donné par:

pour tout $m \in \mathcal{E}$, $f^{-1}(m)$ est l'unique élément de $\mathcal{E}$ tel que $f^{-1}(m) \equiv m - 3 \bmod 26$.

► *Exemple:* coder par le code de César le message: CE MESSAGE EST CONFIDENTIEL.

► *Exemple:* décoder suivant le code de César le message: OH FUBSWDJH HVW ODUW GH FRGHU XQ PHVVDJH.

On peut, dans le codage de César, remplacer 3 par n'importe quelle valeur b dans $\mathcal{E}$ (sachant que le cas $b = 0$ correspond à l'écriture en clair). C'est l'objet du résultat suivant :

Proposition. *Soit $b \in \mathcal{E}$ fixé ; l'application f qui, à tout entier $n \in \mathcal{E}$, associe l'unique entier $f(n)$ dans $\mathcal{E}$ vérifiant:*

$$f(n) \equiv n + b \bmod 26$$

est une bijection de $\mathcal{E}$ sur $\mathcal{E}$.

Preuve. Le fait que $f(n)$ soit bien défini et unique quel que soit $n \in \mathcal{E}$ résulte de l'existence et unicité du reste de la division euclidienne de $n + b$ par 26. Le fait que l'application $f : \mathcal{E} \to \mathcal{E}$ ainsi définie soit bijective résulte du fait que l'application qui, à tout $m \in \mathcal{E}$, associe le reste de la division euclidienne de $m - b$ par 26, est clairement la réciproque de f. □

Ce type de codage (dit par translation arithmétique) est évidemment sommaire, et peut être perfectionné en remplaçant la translation par une fonction affine, comme on va le voir maintenant.

4.2 Codages monographiques par transformations affines

a) Principe. On note toujours $\mathcal{A} = \{A, B, C, D, \ldots, Y, Z\}$, $\mathcal{E} = \{0, 1, 2, 3, \ldots, 24, 25\}$, et g la bijection de numérotation des lettres de $\mathcal{A}$ sur $\mathcal{E}$:

$$g(A) = 0,\ g(B) = 1,\ g(C) = 2,\ g(D) = 3,\ \ldots\ldots,\ g(Y) = 24,\ g(Z) = 25.$$

Proposition. *Soient a et b deux entiers fixés dans $\mathcal{E}$. On suppose que a est premier avec 26. Alors l'application f qui, à tout entier $n \in \mathcal{E}$, associe l'unique entier $f(n)$ dans $\mathcal{E}$ vérifiant:*

$$f(n) \equiv an + b \bmod 26$$

est une bijection de $\mathcal{E}$ sur $\mathcal{E}$.

Preuve. Le fait que $f(n)$ soit bien défini et unique quel que soit $n \in \mathcal{E}$ résulte de l'existence et unicité du reste de la division euclidienne de $an + b$ par 26.

Montrons que l'application $f : \mathcal{E} \to \mathcal{E}$ ainsi définie est injective. Pour cela, supposons que deux entiers n et n' de $\mathcal{E}$ aient la même image $f(n) = f(n')$. On a alors $an + b \equiv an' + b \bmod 26$, donc 26 divise $a(n - n')$. Comme par hypothèse 26 et a sont premiers entre eux, il résulte du lemme de Gauss que 26 divise $n - n'$. Ainsi $n \equiv n' \bmod 26$, ce qui, comme $0 \leqslant n, n' \leqslant 25$, implique que $n = n'$. Ceci prouve que f est injective.

Il reste à montrer que f est surjective, c'est-à-dire par définition que, quel que soit $m \in \mathcal{E}$, il existe $n \in \mathcal{E}$ tel que $m = f(n)$.

On peut pour cela faire une preuve directe en utilisant le théorème de Bézout: comme a et 26 sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $au + 26v = 1$; donc $au \equiv 1 \bmod 26$. Soit $m \in \mathcal{E}$ quelconque. Notons n le reste de la division euclidienne de $u(m - b)$ par 26, qui vérifie donc $n \in \mathcal{E}$ et $n \equiv u(m - b) \bmod 26$. On a alors $an \equiv au(m - b) \bmod 26$, c'est-à-dire $an \equiv m - b \bmod 26$. Ainsi $m \equiv an + b \bmod 26$ avec $n \in \mathcal{E}$: on conclut que $m = f(n)$.

On peut aussi rappeler que f étant une application de l'ensemble *fini* $\mathcal{E}$ dans lui-même, il suffit de montrer que f est injective ou de montrer que f est surjective pour conclure qu'elle est bijective. □

► *Exemple:* coder par le code affine $n \mapsto 3n + 5$ le message: CE MESSAGE EST CONFIDENTIEL.

► *Exemple:* décoder par le même code le mot: IEFQV.

b) Choix de la permutation de codage affine. Les entiers de $\mathcal{E}$ premiers avec 26 sont: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 ; il y a donc 12 choix possibles pour a. Comme b est choisi arbitrairement dans $\mathcal{E}$, il y a 26 choix pour b. On obtient ainsi $12 \times 26 = 312$ possibilités de codages affines (et donc $11 \times 26 = 286$ si l'on exclut les codages par translations, qui correspondent à $a = 1$).

c) Remarque sur la cryptoanalyse des codages affines. Le but du cryptoanalyste est, à partir de la version codée d'un message (qui ne lui est a priori pas destiné), de deviner le principe du codage qui a été utilisé pour le cryptage. S'il sait que la méthode de codage utilisée est par permutation affine, il a théoriquement 312 possibilités. Mais le fait que les différentes lettres de l'alphabet n'apparaissent pas avec la même fréquence dans une langue (et donc dans un texte codé pour peu que ce texte soit assez long pour être représentatif) donne un indice permettant de restreindre les recherches.

> *Exemple.* Partons d'un message codé YM QMGGKAM MGN NEL GMYZMN. On sait que c'est du Français et que le codage est affine. En Français, la lettre la plus courante est le E, suivi du S puis du A. On fait la conjecture que le M (qui apparaît six fois) correspond au E, et que le G (qui apparaît quatre fois) correspond au S. Comme $g(E) = 4$ et $g(M) = 12$, on a $f(4) = 12$; comme $g(S) = 18$ et $g(G) = 6$, on a $f(18) = 6$. On cherche donc $a, b \in \mathcal{E}$, avec a premier avec 26, tels que $4a + b \equiv 12 \bmod 26$ et $18a + b \equiv 6 \bmod 26$.
>
> Ce système de congruences implique par différence : $14a \equiv -6 \bmod 26$, donc $14a \equiv 20 \bmod 26$, donc $7a \equiv 10 \bmod 13$. Par multiplication par 2, il vient $14a \equiv 20 \bmod 13$, donc $a \equiv 7 \bmod 13$. Les deux seules solutions dans $\mathcal{E}$ sont $a = 7$ ou $a = 20$. Comme il faut de plus que a soit premier avec 26, on a nécessairement $a = 7$. On en déduit avec la seconde congruence du système que $b \equiv 10 \bmod 26$, qui a pour seule solution dans $\mathcal{E}$ la valeur $b = 10$.
>
> On a ainsi montré que le codage affine défini par $f(n) = 7n + 10$ vérifie bien $f(4) = 12$ et $f(18) = 6$, c'est-à-dire transforme bien E en M, et S en G. On applique ensuite ce codage aux autres lettres pour voir si l'on obtient un sens intelligible au message; il vient: CE MESSAGE EST TOP SECRET

d) Remarque historique. Les codages par transformation affine constituent une amélioration naturelle des codages par translation, mais d'autres perfectionnements du code de César ont été utilisés dans l'histoire. C'est le cas du système proposé par l'auvergnat Blaise de Vigenère,[9] dans lequel les différentes lettres sont translatées d'un nombre différents de crans suivant leur position dans le texte et les indications contenues dans un mot-clef connu du codeur et du décodeur.

> Supposons que le mot-clef soit LOIN. Il a 4 lettres, donc les différentes lettres du message sont, suivant leur rang x modulo 4 dans le texte, translatées d'un nombre de crans égal $g(\alpha)$ pour α la x-ième lettre du mot LOIN.
>
> les lettres de rang 1 modulo 4 (la 1ère, la 5ème, la 9ème,...) sont translatées de 11 crans modulo 26 car la première lettre du mot clef vérifie $g(L) = 11$;
>
> les lettres de rang 2 modulo 4 (la 2ème, la 6ème, la 10ème,...) sont translatées de 14 crans modulo 26 car la deuxième lettre du mot clef vérifie car $g(O) = 14$;
>
> les lettres de rang 3 modulo 4 (la 3ème, la 7ème, la 11ème,...) sont translatées de 8 crans modulo 26 car la troisième lettre du mot clef vérifie $g(I) = 8$;
>
> les lettres de rang 4 modulo 4 (la 4ème, la 8ème, la 12ème,...) sont translatées de 13 crans modulo 26 car la quatrième lettre du mot clef vérifie $g(N) = 13$.

[9] Blaise de Vigenère, 1523-1596, diplomate, astrologue et alchimiste, mais aussi cryptographe, auteur du "Traité des chiffres"

4.3 Codages polygraphiques

Le principe est de transformer par codage non pas chaque lettre par une lettre (ce qui résiste mal à la cryptoanalyse du fait des fréquences diverses d'apparition des lettres dans une langue donnée) mais des blocs de lettres d'une longueur donnée par des blocs de lettres de même longueur. Dans toute la suite, on se limitera (pour simplifier) à des blocs de deux lettres, suivant ce qu'on appelle un codage digraphique.

a) Exemple: code de Hill. Ce système est dû à L. S. Hill, dans les années 1930. On part d'un message à coder, dans lequel on regroupe d'abord les lettres deux par deux (s'il y a un nombre impair de lettres, on rajoute un X à la fin). On transforme ces groupes de deux lettres en groupes de deux entiers entre 0 et 25 par la bijection de numérotation g de $\mathcal{A}$ sur $\mathcal{E}$ déjà utilisée ci-dessus.

$$\begin{aligned} \text{ENVOYEZ L'ARGENT} &\longrightarrow \text{EN VO YE ZL AR GE NT} \\ &\xrightarrow{g} (4,13)\ (21,14)\ (24,4)\ (25,11)\ (0,17)\ (6,4)\ (13,19) \end{aligned}$$

Pour tout couple d'entiers (x, y) de $\mathcal{E} \times \mathcal{E}$, on note $x' = f(x, y)$ le reste de la division euclidienne de $5x + 17y$ par 26, et $y' = h(x, y)$ le reste de la division euclidienne de $4x + 15y$ par 26. En d'autres termes x' est l'unique entier de $\mathcal{E}$ et y' l'unique entier de $\mathcal{E}$ tels que:

$$\begin{cases} x' \equiv 5x + 17y \mod 26 \\ y' \equiv 4x + 15y \mod 26 \end{cases}$$

• *Principe.* Le point fondamental est que:

l'application $f \times h : (x, y) \mapsto (x' = f(x, y), y' = h(x, y))$ *est une bijection de* $\mathcal{E} \times \mathcal{E}$ *sur* $\mathcal{E} \times \mathcal{E}$.

> *Preuve.* Comme $\mathcal{E} \times \mathcal{E}$ est fini, il suffit de montrer l'injectivité pour conclure à la bijectivité. Soient donc (x_1, y_1) et (x_2, y_2) dans $\mathcal{E} \times \mathcal{E}$ tels que $f(x_1, y_1) = f(x_2, y_2)$ et $h(x_1, y_1) = h(x_2, y_2)$.
>
> On a: $\begin{cases} 5(x_1 - x_2) + 17(y_1 - y_2) \equiv 0 \mod 26 \\ 4(x_1 - x_2) + 15(y_1 - y_2) \equiv 0 \mod 26 \end{cases}$ d'où $\begin{cases} (5 \times 15 - 17 \times 4)(x_1 - x_2) \equiv 0 \mod 26 \\ (17 \times 4 - 15 \times 5)(y_1 - y_2) \equiv 0 \mod 26 \end{cases}$
>
> Ainsi, $7(x_1 - x_2)$ divise 26 et $7(y_1 - y_2)$ divise 26. Comme 7 et 26 sont premiers entre eux, il résulte du lemme de Gauss que $x_1 - x_2$ divise 26 et $y_1 - y_2$ divise 26. Or $-25 \leqslant x_1 - x_2 \leqslant 25$ et $-25 \leqslant y_1 - y_2 \leqslant 25$ puisque x_1, x_2, y_1, y_2 sont dans $\mathcal{E}$. On conclut que $x_1 - x_2 = y_1 - y_2 = 0$, ce qui prouve l'injectivité voulue et achève la preuve. □

• *Mode de codage.* On obtient donc un codage sans ambiguité en remplaçant chaque bloc (x, y) de deux éléments de $\mathcal{E}$ (correspondant à chaque bloc de deux lettres) en le bloc $(f(x, y), h(x, y))$. Par exemple:

$$\begin{array}{lll} (4,13) \longrightarrow (f(4,13), h(4,13)) = (7,3), & \text{donc le bloc EN se code en HD} \\ (21,14) \longrightarrow (f(21,14), h(21,14)) = (5,8), & \text{donc le bloc VO se code en FI} \\ (24,4) \longrightarrow (f(24,4), h(24,4)) = (6,0), & \text{donc le bloc YE se code en GA} \\ (25,11) \longrightarrow (f(25,11), h(25,11)) = (0,5), & \text{donc le bloc ZL se code en AF} \\ (0,17) \longrightarrow (f(0,17), h(0,17)) = (3,21), & \text{donc le bloc AR se code en DV} \\ (6,4) \longrightarrow (f(6,4), h(6,4)) = (20,6), & \text{donc le bloc GE se code en UG} \\ (13,19) \longrightarrow (f(13,19), h(13,19)) = (24,25), & \text{donc le bloc NT se code en YZ} \end{array}$$

Le message initial se code donc en HDFIGAAFDVUGYZ.

• *Mode de décodage.* C'est une question non triviale (voir plus loin) que de déterminer, au delà du procédé arithmétique de codage, un procédé analogue pour le décodage (qui ne se borne pas à un simple dictionnaire, éventuellement immense, de tous les codages obtenus de tous les blocs possibles). On peut dans le cas considéré ici expliciter un tel procédé:

Le problème est de déterminer, pour un couple quelconque donné (x', y') d'éléments de $\mathcal{E}$, l'unique couple (x, y) tel que $x' = f(x, y)$ et $y' = h(x, y)$. Il s'agit donc de résoudre le système:

$$\begin{cases} 5x + 17y \equiv x' \mod 26 \\ 4x + 15y \equiv y' \mod 26 \end{cases}$$

où x', y' sont supposés arbitrairement fixés. Il équivaut à:

$$\begin{cases} (5 \times 15 - 4 \times 17)x \equiv (15x' - 17y') \mod 26 \\ (4 \times 17 - 5 \times 15)y \equiv (4x' - 5y') \mod 26 \end{cases}, \quad \text{donc} \quad \begin{cases} 7x \equiv (15x' - 17y') \mod 26 \\ -7y \equiv (4x' - 5y') \mod 26 \end{cases}$$

A ce stade, il est crucial de remarquer que les quatre coefficients du système définissant le codage vérifient que $5 \times 15 - 4 \times 17 = 7$ est premier avec 26. Donc, par le théorème de Bézout, il existe des entiers $u, v \in \mathbb{Z}$ tels que $7u + 26v = 1$; en particulier, il existe un unique entier $u \in \mathcal{E}$ tel que $7u \equiv 1 \mod 26$. Il s'agit de $u = 15$ (effectivement $7 \times 15 = 105 \equiv 1 \mod 26$).
Le système précédent donne donc en multipliant chaque membre par 15:

$$x \equiv 15(15x' - 17y') \mod 26 \quad \text{et} \quad y \equiv 15(5y' - 4x') \mod 26.$$

Il suffit de choisir pour x le seul représentant de la classe de congruence de $15(15x' - 17y')$ modulo 26 qui soit compris entre 0 et 25, et et pour y le seul représentant de la classe de congruence de $15(5y' - 4x')$ modulo 26 qui soit compris entre 0 et 25. Le couple (x, y) d'élément de $\mathcal{E}$ ainsi construit vérifie bien $f(x, y) = x'$ et $h(x, y) = y'$.

> *Exemple.* On veut décoder le bloc HD. Comme $g(H) = 7$ et $g(D) = 3$, il s'agit de trouver l'unique couple (x, y) d'éléments de $\mathcal{E}$ tel que $f(x, y) = 7$ et $h(x, y) = 3$. En appliquant ce qui précède à $x' = 7$ et $y' = 3$, on doit avoir:
>
> $$x \equiv 15(15 \times 7 - 17 \times 3) \mod 26 \quad \text{et} \quad y \equiv 15(5 \times 3 - 4 \times 7) \mod 26,$$
>
> donc $x \equiv 810 \mod 26$ et $y \equiv -195 \mod 26$, d'où finalement $x = 4$ et $y = 13$. En revenant aux lettres via g^{-1}, on conclut que HD se décode en EN. On fait de même pour les autres blocs.

b) Cas général des codes digraphiques. On peut chercher à généraliser ce qui précède en remplaçant les entiers particuliers 5, 17, 4, 15 par quatre entiers a, b, c, d quelconques. Il s'agit de savoir à quelle condition sur a, b, c, d le codage $(x, y) \mapsto (x', y')$ défini par le système de congruences:

$$\begin{cases} x' \equiv ax + by \mod 26 \\ y' \equiv cx + dy \mod 26 \end{cases}$$

correspond bien à une bijection de $\mathcal{E} \times \mathcal{E}$ sur $\mathcal{E} \times \mathcal{E}$. Il suffit de reprendre les raisonnements faits ci-dessus dans le cas particulier de 5, 17, 4, 15 (dont l'utilisation du théorème de Bézout et du lemme de Gauss, et le rôle joué par l'entier $5 \times 15 - 4 \times 17 = 7$) pour voir qu'il suffit de supposer que:

$$ad - bc \text{ est premier avec } 26,$$

pour que tout ce qui précède s'applique de façon identique. A noter que, si l'on veut coder par ce procédé un nombre de caractères m qui ne soit pas forcément 26, il suffit de choisir a, b, c, d qui vérifient que $ad - bc$ est premier avec m.

c) Remarque finale. On verra plus loin d'autres systèmes de codages plus élaborés utilisant, outre des congruences, certaines propriétés des nombres premiers (codages par exponentiation arithmétique, codages à clefs publiques type RSA,...)

Chapitre 4: nombres premiers

1 Propriétés élémentaires des nombres premiers

1.1 Notion de nombre premier.

a) Définition. On appelle NOMBRE PREMIER tout entier p supérieur ou égal à 2 dont les seuls diviseurs positifs sont 1 et p.

Exemples. 2 est le seul nombre premier pair; $3, 5, 7, 11, 13, 17, 19, 23...$ sont premiers; 6 700 417 est premier. *Attention:* 0 et 1 ne sont pas premiers.

b) Diviseurs premiers. La proposition suivante est simple mais fondamentale.

PROPOSITION.

(i) *Tout entier différent de 1 et de* -1 *admet au moins un diviseur premier.*

(ii) *Tout entier* n *supérieur ou égal à 2 qui n'est pas un nombre premier admet au moins un diviseur premier* p *tel que* $p^2 \leqslant n$.

Preuve. Il est clair qu'il suffit de prouver (i) pour un entier naturel n supérieur ou égal à 2. Notons $D(n)$ l'ensemble des diviseurs de n supérieurs ou égaux à 2. Il est non-vide car il contient n. Comme $\mathbb{N}$ est bien ordonné, $D(n)$ admet un plus petit élément p. C'est un diviseur de n, supérieur à 2; montrons qu'il est premier. Pour cela, considérons un entier naturel a divisant p. Par transitivité de la divisibilité, a divise n. Si $a \geqslant 2$, alors $a \in D(n)$, donc $p \leqslant a$ par minimalité de p; ainsi a divise p et $p \leqslant a$, donc $a = p$. Sinon, $a = 1$. Ceci prouve (i).

De plus, il existe $k \in \mathbb{N}$ tel que $n = kp$. Supposons que n n'est pas premier. Donc $k \neq 1$, c'est-à-dire $k \geqslant 2$. Ainsi $k \in D(n)$, ce qui implique $p \leqslant k$. On obtient $n = kp \geqslant p^2$, ce qui prouve (ii). □

c) Infinitude de l'ensemble des nombres premiers.

THÉORÈME. *Le sous-ensemble de* $\mathbb{N}$ *formé des nombres premiers est infini.*

Preuve. Par l'absurde, supposons que l'ensemble des nombres premiers soit fini. Notons alors N le produit de tous les nombres premiers. C'est un entier supérieur à 2. L'entier $N + 1$ est un entier supérieur à 3; d'après la proposition ci-dessus, il admet un diviseur premier p. Celui-ci apparaissant comme un des facteurs du produit N, on a à la fois: p divise $N + 1$ et p divise N, ce qui implique (par différence) que p divise 1, et contredit le fait que p est premier. □

Notations. On note $\mathcal{P}$ l'ensemble des nombres premiers. Comme c'est un sous-ensemble infini de $\mathbb{N}$, donc un ensemble infini dénombrable, on peut aussi noter ses éléments sous forme d'une suite $(p_n)_{n\geqslant 1}$, où p_n désigne le n-ième nombre premier, avec donc $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7...$.

Remarque. La proposition ci-dessous donne une autre preuve du fait que l'ensemble des nombres premiers est infini. Elle est constituée de deux cas très particuliers et faciles d'un théorème profond de Dirichlet selon lequel il existe une infinité de nombres premiers de la forme $an + b$ dès lors que a et b sont premiers entre eux.

PROPOSITION. *Il existe une infinité de nombres premiers de la forme* $4n + 3$ *avec* $n \in \mathbb{N}$, *et une infinité de nombre premiers de la forme* $6m + 5$, *avec* $m \in \mathbb{N}$.

Preuve. On ne démontre que le premier point, la preuve du second étant analogue et laissée au lecteur. Notons E l'ensemble des nombres premiers de la forme $4n+3$ avec $n \in \mathbb{N}$. Il est non-vide, car par exemple 3 ou 7 sont dans E. Par l'absurde, supposons que E soit fini. Appelons N le produit de tous les éléments de E et posons $a = 4N-1$. Soit p un diviseur premier de a. Il est de la forme $4n$ ou $4n+1$ ou $4n+2$ ou $4n+3$, avec $n \in \mathbb{N}$.

Mais p étant premier, les cas $4n$ ou $4n+2$ sont impossibles (notons qu'on ne peut pas avoir $p = 2$ puisque a est impair). Si p était du type $4n+3$, il appartiendrait à E, donc diviserait N, donc diviserait $4N$, et comme p divise $a = 4N-1$, on obtiendrait que p divise 1, ce qui est impossible. En résumé, tout diviseur premier de a est de la forme $4n+1$. Il en résulte que tout diviseur de a est de cette forme. En particulier il existe $q \in \mathbb{N}$ tel que $a = 4q+1$. Mais l'égalité $4q+1 = 4N-1$ est absurde. C'est donc que E est infini. □

d) Un algorithme pour déterminer si un entier naturel est ou non premier. Soit $n \geqslant 3$ un entier. Pour tout entier $i \geqslant 1$, considérons la division euclidienne de n par le i-ème nombre premier p_i:

$$n = p_i q_i + r_i, \quad q_i \in \mathbb{N},\ 0 \leqslant r_i < p_i.$$

Comme $n \geqslant p_i q_i$ pour tout $i \geqslant 1$ et comme la suite des p_i est strictement croissante, il existe un plus petit entier $k \geqslant 1$ tel que $p_j > q_j$ pour tout $j \geqslant k$.

• S'il existe un entier $i \leqslant k-1$ tel que $r_i = 0$, alors n n'est pas premier (en effet, on a alors $n = p_i q_i$ et $q_i \neq 1$ puisque $q_i \geqslant p_i$ du fait que $i \leqslant k-1$).

• Sinon, n n'est divisible par aucun des nombres premiers $p_1, \ldots, p_{k-1}$. Si n n'était pas premier, il existerait d'après la proposition b) un nombre premier p divisant n et tel que $p^2 \leqslant n$. L'entier q tel que $n = pq$ vérifierait $p \leqslant q$, donc p serait l'un des p_i pour $1 \leqslant i \leqslant k-1$; contradiction. C'est donc que n est premier.

Concrètement: on effectue les divisions euclidiennes de n par les p_i jusqu'à ce que $p_i > q_i$; si l'un des restes s'annule, n n'est pas premier. Sinon, n est premier.

EXEMPLE: considérons $n = 127$. On effectue les divisions euclidiennes successives: $127 = 2 \times 63 + 1$, $127 = 3 \times 42 + 1$, $127 = 5 \times 25 + 2$, $127 = 7 \times 18 + 1$, $127 = 11 \times 11 + 6$, $127 = 13 \times 9 + 10$. Comme $p_6 = 13 > q_6 = 9$, on s'arrête. Aucun reste n'étant nul, on conclut que 127 est premier.

e) Crible d'Eratosthène[10] Il s'agit d'un algorithme très simple pour déterminer les nombres premiers inférieurs à un entier naturel donné.

PROPOSITION. *Pour tout* $k \in \mathbb{N}^*$, *le* $(k+1)$*-ième nombre premier* p_k *est:*

$$p_{k+1} = \mathrm{Min}\Big(\mathbb{N} \setminus \big(\{0,1\} \cup p_1\mathbb{N} \cup p_2\,\mathbb{N} \cup \ldots \cup p_k\mathbb{N} \big) \Big).$$

Preuve. Notons $A_k = \mathbb{N} \setminus (\{0,1\} \cup p_1\mathbb{N} \cup p_2\mathbb{N} \cup \ldots \cup p_k\mathbb{N})$. Il est clair que $p_{k+1} \in A_k$. Comme $A_k \neq \emptyset$, il admet un plus petit élément a_k. D'après la proposition b), il existe un nombre premier p qui divise a_k. Comme $a_k \in A_k$, on a $p \notin \{p_1, p_2, \ldots, p_k\}$. On en déduit que $p_{k+1} \leqslant p \leqslant a_k$. Mais par ailleurs $a_k \leqslant p_{k+1}$ puisque $p_{k+1} \in A_k$. On conclut que $a_k = p = p_{k+1}$. □

Algorithme (dit "crible d'Eratosthène").

Soit n un entier, $n \geqslant 2$. Notons p_j le plus grand des nombres premiers vérifiant $p_j^2 \leqslant n$. On note $[\![2, n]\!]$ l'ensemble $\{2, 3, 4, \ldots, n\}$. On dresse la liste des nombres premiers de $[\![2, n]\!]$.

• étape 1: on barre tous les éléments de $[\![2, n]\!]$ qui sont des multiples stricts de $p_1 = 2$ (ie. des multiples de p_1 strictement supérieurs à p_1). D'après la proposition, le premier élément non barré après p_1 est $p_2 = 3$.

[10] Eratosthène de Cyrène (IIIème siècle av. J.C.), astronome, géographe, philosophe et mathématicien grec, passé à la postérité entre autres pour sa méthode de mesure de la circonférence terrestre.

• étape 2: on barre ensuite tous les éléments de $[\![2, n]\!]$ qui sont des multiples stricts de p_2. D'après la proposition, le premier élément non barré après p_2 est $p_3 = 5$.

...

• étape j: on barre enfin tous les éléments de $[\![2, n]\!]$ qui sont des multiples stricts de p_j.

Affirmation: les entiers de $[\![2, n]\!]$ qui restent non-barrés sont les nombres premiers inférieurs à n.

> *En effet.* Soit $m \in [\![2, n]\!]$ non premier. Il existe un nombre premier p_i et un entier $q \geqslant 2$ tels que $m = p_i q$. Ou bien $i \leqslant j$, c'est-à-dire $p_i \leqslant p_j$, de sorte que m a été barré à l'étape i. Ou bien $i > j$, c'est-à-dire $p_i > p_j$; on a alors $q < p_j$ (car sinon $q \geqslant p_j$ impliquerait $m = p_i q \geqslant p_i p_j > p_j^2 \geqslant n$) de sorte que tout diviseur premier de q est de la forme p_k pour $k < j$ et donc $m = p_i q$ est un multiple strict de p_k, qui a été barré à l'étape k. □

Exemple. On détermine les nombres premiers inférieurs à $n = 100$, en barrant successivement les multiples stricts et inférieurs à 100 de $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ et $p_4 = 7$ (plus grand nombre premier de carré inférieur à 100); les entiers restant non barrés sont ceux qui sont encadrés ci-dessous:

	[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	[31]	32	33	34	35	36	[37]	38	39	40
[41]	42	[43]	44	45	46	[47]	48	49	50	51	52	[53]	54	55	56	57	58	[59]	60
[61]	62	63	64	65	66	[67]	68	69	70	[71]	72	[73]	74	75	76	77	78	[79]	80
81	82	[83]	84	85	86	87	88	[89]	90	91	92	93	94	95	96	[97]	98	99	100

1.2 Décomposition en produit de facteurs premiers.

a) Résultats préliminaires.

LEMME. *Un nombre premier est premier avec tout entier qu'il ne divise pas.*

> *Preuve.* Soit p un nombre premier. Soient a un entier non divisible par p et d le pgcd de a et p. Comme d divise p, on ne peut avoir que $d = p$ ou $d = 1$. Comme d divise a et que p ne divise pas a par hypothèse, d ne peut pas valoir p . C'est donc que $d = 1$. □

► *Conséquence 1.* Deux nombres premiers distincts sont premiers entre eux.

► *Conséquence 2.* Tout nombre premier est premier avec tout entier naturel non-nul qui lui est strictement inférieur.

PROPOSITION.

(i) *Si un nombre premier divise un produit d'entiers, alors il divise l'un des facteurs de ce produit.*

(ii) *Si un nombre premier divise un produit de nombres premiers, alors il est égal à l'un d'entres eux.*

> *Preuve.* Soit p un nombre premier. Supposons que p divise le produit bc de deux entiers b et c. Supposons que p ne divise pas b. Alors, d'après le lemme, p est premier avec b. Ce qui, d'après le théorème de Gauss, implique que p divise c. Ceci prouve (i). Le point (ii) s'en déduit immédiatement. □

b) Le résultat fondamental.

THÉORÈME. *Soit n un entier supérieur ou égal à 2. Il existe, et ceci de façon unique, un entier $s \geqslant 1$, des nombres premiers $p_1, p_2, \ldots, p_s$ vérifiant que $p_1 < p_2 < \cdots < p_s$, et des entiers naturels non-nuls $\alpha_1, \alpha_2, \ldots, \alpha_s$ tels que:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}.$$

Preuve. Montrons l'existence d'une telle décomposition par récurrence sur n. C'est clair si $n = 2$. Supposons-la vraie pour tout entier strictement inférieur à n. Soit p un diviseur premier de n. Si $n = p$, il n'y a rien à démontrer. Sinon, il existe $2 \leqslant n_0 \leqslant n-1$ tel que que $n = pn_0$. En appliquant l'hypothèse de récurrence à n_0, on a $n = pp_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$. S'il existe $1 \leqslant j \leqslant s$ tel que $p = p_j$, alors $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_j^{\alpha_j+1}\dots p_s^{\alpha_s}$, d'où le résultat. Sinon, on obtient une décomposition du type voulu, avec $s+1$ facteurs, et un exposant 1 pour le facteur p.

Montrons l'unicité. Supposons pour cela que $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s} = q_1^{\beta_1}q_2^{\beta_2}\dots q_t^{\beta_t}$, avec $s \in \mathbb{N}^*$, $p_1 < p_2 < \dots < p_s$ premiers, $\alpha_i \in \mathbb{N}^*$ pour tout $1 \leqslant i \leqslant s$, et $t \in \mathbb{N}^*$, $q_1 < q_2 < \dots < q_t$ premiers, $\beta_j \in \mathbb{N}^*$ pour tout $1 \leqslant j \leqslant t$. D'après le point (ii) de la proposition précédente, chaque p_i $(1 \leqslant i \leqslant s)$ est égal à un des q_j $(1 \leqslant j \leqslant t)$, et chaque q_j est égal à l'un des p_i. Comme les p_i sont à deux distincts, ainsi que les q_j, on a nécessairement $s = t$. De plus la condition de croissance sur les p_i et les q_j implique que l'on a précisément $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$. Donc finalement: $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s} = p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s}$. Si $\beta_1 < \alpha_1$, on en déduit l'égalité $p_2^{\alpha_2}\dots p_s^{\alpha_s} = p_1^{\beta_1-\alpha_1}p_2^{\beta_2}\dots p_s^{\beta_s}$; celle-ci implique que p_1 divise le produit $p_2^{\alpha_2}\dots p_s^{\alpha_s}$, ce qui est impossible d'après le point (ii) de la proposition précédente. De même $\beta_1 > \alpha_1$ conduit à une contradiction. C'est donc que $\alpha_1 = \beta_1$. On prouve de façon analogue que $\alpha_i = \beta_i$ pour tout $1 \leqslant i \leqslant s$. □

Définitions. L'écriture de n sous la forme $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$ s'appelle la DÉCOMPOSITION DE n EN PRODUIT DE FACTEURS PREMIERS, ou encore la DÉCOMPOSITION PRIMAIRE de n.
Chaque p_i $(1 \leqslant i \leqslant s)$ s'appelle un FACTEUR PREMIER de la décomposition. Chaque $p_i^{\alpha_i}$ s'appelle un FACTEUR PRIMAIRE.

Attention à la notation. La notation p_i pour désigner les différents facteurs premiers dans la décomposition du théorème ci-dessus est traditionnelle, mais ne doit pas être confondue avec la même notation p_i pour désigner le i-ème nombre premier (voir ci-dessus 1.1.c).

Remarques. Il découle évidemment du théorème fondamental ci-dessus (dont on reprend les notations) que tout entier n dans $\mathbb{Z}$ qui ne vaut ni 0, ni 1, ni -1 se décompose de façon unique sous la forme $n = \varepsilon p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, où $\varepsilon = \pm 1$.

c) Application: ensemble des diviseurs d'un entier.

PROPOSITION. *Soit n un entier tel que $n \geqslant 2$, et $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$ sa décomposition primaire. Alors les diviseurs de n dans $\mathbb{N}$ sont tous les entiers de la forme:*

$$m = p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s}, \quad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i \text{ pour tout } 1 \leqslant i \leqslant s.$$

Preuve. Soit m un diviseur de n. Si $m = 1$, on a le résultat voulu avec $\beta_1 = \dots = \beta_s = 0$. Si $m \neq 1$, tout diviseur premier de m divise $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, donc est égal à l'un des p_i d'après la proposition du a) ci-dessus. Ceci prouve qu'il existe des entiers naturels $\beta_1, \dots, \beta_s$ tels que $m = p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s}$. L'entier $p_1^{\beta_1}$ divise m, qui divise n, donc est un diviseur de $n = p_1^{\alpha_1}q$, où l'on a posé $q = p_2^{\alpha_2}\dots p_s^{\alpha_s}$. Puisque $p_1^{\beta_1}$ est premier avec q, il résulte du théorème de Gauss que $p_1^{\beta_1}$ divise $p_1^{\alpha_1}$, et donc $\beta_1 \leqslant \alpha_1$. On montre de même que $\beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant s$. On a ainsi montré que tout diviseur de n est de la forme voulue; la réciproque est évidente. □

Attention ! Dans l'énoncé ci-dessus, les exposants β_i peuvent valoir 0 (ie. certains des p_i peuvent ne pas diviser m).

COROLLAIRE. *Soit n un entier supérieur ou égal à 2. Soit $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$ sa décomposition primaire. Alors le nombre $\sigma_0(n)$ des diviseurs de n dans $\mathbb{N}$ est égal à:*

$$\sigma_0(n) = (1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_s).$$

Preuve. Résulte immédiatement de la proposition précédente. □

Exemple élémentaire. Soit $n = 756 = 2^2 \times 3^3 \times 7$. Il admet $\sigma_0(756) = (2+1)\times(3+1)\times(1+1) = 24$ diviseurs, qui sont tous les entiers $m = 2^i \times 3^j \times 7^k$ pour $0 \leqslant i \leqslant 2$, $0 \leqslant j \leqslant 3$ et $0 \leqslant k \leqslant 1$. Donc:

$$D_{756} = \{1, 2, 3, 4, 6, 7, 9, 12, 14, 18, 21, 27, 28, 36, 42, 54, 63, 84, 108, 126, 189, 252, 378, 756\}$$

d) Application: calcul du pgcd et du ppcm de deux entiers.

PROPOSITION. *Soient a et b deux entiers naturels supérieurs ou égaux à 2.*

(i) *Il existe un entier $r \geqslant 1$, des nombres premiers deux à deux distincts $p_1, p_2, \ldots, p_r$, et deux r-uplets $(\alpha_1, \alpha_2, \ldots, \alpha_r) \in \mathbb{N}^r$ et $(\beta_1, \beta_2, \ldots, \beta_r) \in \mathbb{N}^r$ tels que:*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}.$$

(ii) *En posant $\gamma_i = \min(\alpha_i, \beta_i)$ et $\delta_i = \max(\alpha_i, \beta_i)$ pour tout $1 \leqslant i \leqslant r$, on a alors:*

$$\text{pgcd}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_r^{\gamma_r} \quad \text{et} \quad \text{ppcm}(a, b) = p_1^{\delta_1} p_2^{\delta_2} \ldots p_r^{\delta_r}.$$

Preuve. Notons $\{p_1, \ldots, p_r\}$ la réunion de l'ensemble des diviseurs premiers de a et de l'ensemble des diviseurs premiers de b. Pour tout $1 \leqslant i \leqslant r$, notons α_i l'exposant de p_i dans la décomposition primaire de a si p_i divise a, et posons $\alpha_i = 0$ si p_i ne divise pas a. Notons β_i l'exposant de p_i dans la décomposition primaire de b si p_i divise b, et posons $\beta_i = 0$ si p_i ne divise pas b. Le point (i) est alors clair. Le point (ii) résulte de la proposition du c) ci-dessus. □

Attention ! Dans l'énoncé de la proposition ci-dessus, les exposants α_i et β_i peuvent être nuls.

Exemple élémentaire. Soient $a = 756 = 2^2 \times 3^3 \times 7$ et $b = 240 = 2^4 \times 3 \times 5$.
On écrit $a = 2^2 \times 3^3 \times 5^0 \times 7^1$ et $b = 2^4 \times 3^1 \times 5^1 \times 7^0$
D'où $\text{pgcd}(a, b) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$ et $\text{ppcm}(a, b) = 2^4 \times 3^3 \times 5^1 \times 7^1 = 15120$.

Remarque. Cette proposition ne doit pas être considérée comme une méthode systématique pour calculer le pgcd de deux entiers. Dans la plupart des calculs numériques, l'algorithme d'Euclide (voir plus loin) reste beaucoup plus rapide et efficace sur le plan pratique.

e) Application: exemples de fonctions arithmétiques multiplicatives.

Définition. On appelle FONCTION ARITHMÉTIQUE MULTIPLICATIVE une application $f : \mathbb{N}^* \to \mathbb{N}$ telle que, quels que soient des éléments a et b de $\mathbb{N}^*$ *premiers entre eux*, on a $f(ab) = f(a)f(b)$.

PROPOSITION. *Une fonction arithmétique multiplicative f sur $\mathbb{N}^*$ est entièrement déterminée par ses valeurs sur les puissances des nombres premiers.*

Preuve. Pour tout entier $n \geqslant 2$, donné par sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, on a $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2} \ldots p_s^{\alpha_s})$, car $p_1^{\alpha_1}$ est premier avec $p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. D'où en réitérant: $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f(p_s^{\alpha_s})$. □

Exemple 1. L'application $\sigma_0 : \mathbb{N}^* \to \mathbb{N}$ qui, à tout entier $n \geqslant 1$, associe le nombre de diviseurs de n, est une fonction arithmétique multiplicative. Il est clair que, pour toute puissance p^α d'un nombre premier p, on a $\sigma_0(p^\alpha) = \text{card}\{1, p, p^2, \ldots, p^\alpha\} = \alpha + 1$. On retrouve le corollaire du c) ci-dessus.

Exemple 2. L'application $\sigma_1 : \mathbb{N}^* \to \mathbb{N}$ qui, à tout entier $n \geqslant 1$, associe la somme des diviseurs de n, est une fonction arithmétique multiplicative.

En effet. Pour toute puissance p^α d'un nombre premier p, on a $\sigma_1(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = (p^{\alpha+1} - 1)(p - 1)^{-1}$. Pour tout entier naturel $n \geqslant 2$, donné par sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, on a d'après la proposition 2.3, l'égalité:

$$\sigma_1(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_s + p_s^2 + \cdots + p_s^{\alpha_s}). \ \square$$

Exemple 3. On verra plus loin une fonction arithmétique multiplicative particulièrement importante: l'indicatrice d'Euler.

EXERCICE: fonction de Möbius[11]. Montrer que l'application $\mu : \mathbb{N}^* \to \mathbb{N}$ définie par: $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par un carré distinct de 1, et $\mu(n) = (-1)^k$ si $n = p_1 p_2 \dots p_k$ avec $p_1, \dots, p_k$ premiers deux à deux distincts, est une fonction arithmétique multiplicative.

1.3 Quelques caractérisations des nombres premiers

a) Inversibilité dans $\mathbb{Z}/p\mathbb{Z}$. On a vu dans le chapitre précédent que, pour tout $n \geqslant 2$, l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$ est muni d'une addition et d'une multiplication qui ont "toutes les bonnes propriétés" pour calculer dans $\mathbb{Z}/n\mathbb{Z}$ (plus rigoureusement: qui font de $\mathbb{Z}/n\mathbb{Z}$ un anneau). Il y a cependant une propriété qui pose problème, celle de l'inversibilité des éléments de $\mathbb{Z}/n\mathbb{Z}$. Dire qu'un élément $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ signifie qu'il existe un élément $\overline{b}$ de $\mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \times \overline{b} = \overline{1}$. On dit alors que $\overline{b}$ est l'inverse de $\overline{a}$.

- $\overline{1}$ est toujours inversible, car $\overline{1} \times \overline{1} = \overline{1}$,
- $\overline{0}$ n'est jamais inversible, car $\overline{0} \times \overline{b} = \overline{0} \neq \overline{1}$ pour tout $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$,
- en reprenant la table de la multiplication dans $\mathbb{Z}/6\mathbb{Z}$ (voir chapitre précédent), on voit que, dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{1}$ est inversible, $\overline{5}$ est inversible (car $\overline{5} \times \overline{5} = \overline{1}$), mais ni $\overline{2}$, ni $\overline{3}$, ni $\overline{4}$, ni bien sûr $\overline{0}$ ne sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$.
- en reprenant la table de la multiplication dans $\mathbb{Z}/5\mathbb{Z}$, on voit que, dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{1}$ est inversible, $\overline{2}$ et $\overline{3}$ sont inversibles (car $\overline{2} \times \overline{3} = \overline{1}$), $\overline{4}$ est inversible (car $\overline{4} \times \overline{4} = \overline{1}$). Donc tous les éléments non-nuls sont inversibles.

PROPOSITION: *Pour tout entier $p \geqslant 2$, les deux conditions suivantes sont équivalentes:*

(i) *p est premier;*

(ii) *tout élément non-nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$; on dit alors que $\mathbb{Z}/p\mathbb{Z}$ est un corps.*

Preuve. Supposons que p est premier. Soit $a \in \mathbb{Z}$ tel que $\overline{a} \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Cela signifie que p ne divise pas a, donc (lemme 1.2.a) que p est premier avec a. Par le théorème de Bézout, il existe u, v dans $\mathbb{Z}$ tels que $au + pv = 1$. D'où $\overline{au} = \overline{1}$, et donc $\overline{a}$ est inversible d'inverse $\overline{u}$.

Réciproquement, supposons que p n'est pas premier. Il s'écrit donc $p = ac$ avec $2 \leqslant a, c < p$. On a donc $\overline{a} \times \overline{c} = \overline{0}$ avec $\overline{a} \neq \overline{0}$ et $\overline{c} \neq \overline{0}$. Si $\overline{a}$ était inversible, il existerait $\overline{b}$ dans $\mathbb{Z}/p\mathbb{Z}$ tel que $\overline{b} \times \overline{a} = \overline{1}$. En multipliant par $\overline{c}$, on aurait $\overline{c} = \overline{b} \times \overline{a} \times \overline{c} = \overline{b0} = \overline{0}$. D'où une contradiction. Ainsi, si p n'est pas premier, il existe des éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$ qui sont non inversibles.□

b) Petit théorème de Fermat[12]

LEMME PRÉLIMINAIRE. *Si p est un nombre premier, alors p divise $\binom{p}{k}$ pour tout $1 \leqslant k \leqslant p-1$.*

Preuve. D'une part p divise le produit $k!\binom{p}{k}$ puisque $k!\binom{p}{k} = p(p-1)\cdots(p-k+1)$. D'autre part p est premier avec $k!$ puisque p est premier et $k < p$. D'après le lemme de Gauss, on conclut que p divise $\binom{p}{k}$. □

THÉORÈME (dit PETIT THÉORÈME DE FERMAT). *Si p est premier, alors, pour tout $n \in \mathbb{Z}$, on a:*

$$n^p \equiv n \bmod p.$$

[11] August Ferdinand Möbius, 1790-1868, mathématicien et astronome allemand, dont le nom est en resté en particulier associé à une surface topologiquement intéressante: le fameux ruban de Möbius

[12] Pierre de Fermat, 1601(?)-1685, mathématicien et juriste français, célèbre en particulier pour divers résultats d'arithmétique, dont le fameux "dernier théorème de Fermat", problème resté ouvert pendant des siècles jusqu'à sa résolution en 1995 par Andrew Wiles.

Preuve. Supposons p premier. Il résulte du lemme précédent et de la formule du binôme que $(a+b)^p \equiv a^p + b^p \bmod p$ pour tous $a, b \in \mathbb{Z}$. On en déduit que, si $n \geqslant 2$ est un entier fixé, et $a_1, a_2, \ldots, a_n$ des entiers quelconques, on a $(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \bmod p$. En particulier pour $a_1 = a_2 = \cdots = a_n = 1$, il vient $n^p \equiv n \bmod p$. Le résultat pour tout $n \in \mathbb{Z}$ s'en déduit immédatement. □

Ce résultat admet le perfectionnement suivant.

PROPOSITION: *Pour tout entier $p \geqslant 2$, les deux conditions suivantes sont équivalentes:*

(i) p *est premier;*

(ii) *pour tout $n \in \mathbb{Z}$ tel que $n \notin p\mathbb{Z}$, on a:* $n^{p-1} \equiv 1 \bmod p$.

Preuve. Supposons p premier. D'après le petit théorème de Fermat, on a: $n^p \equiv n \bmod p$. Comme de plus on suppose ici que p ne divise pas n, le fait que p divise $n(n^{p-1} - 1)$ implique avec le lemme de Gauss que p divise $n^{p-1} - 1$, d'où $n^{p-1} \equiv 1 \bmod p$.

Pour la réciproque, supposons que p vérifie $n^{p-1} \equiv 1 \bmod p$ pour tout $n \in \mathbb{Z}$ tel que $n \notin p\mathbb{Z}$. Cela signifie que $\overline{n}^{p-1} = \overline{1}$ pour tout $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\overline{n} \neq \overline{0}$. En d'autre terme, tout élément non-nul $\overline{n}$ de $\mathbb{Z}/p\mathbb{Z}$ admet $\overline{n}^{p-2}$ pour inverse dans $\mathbb{Z}/p\mathbb{Z}$. Il en résulte avec la proposition du a) ci-dessus que p est premier. □

ATTENTION ! Cette proposition est une caractérisation (CNS) des nombres premiers. Ce n'est pas le cas du petit théorème de Fermat, qui donne seulement une condition nécessaire pour qu'un nombre soit premier.

Et cette condition n'est pas suffisante ! Il existe des entiers $p \geqslant 2$ qui vérifient $n^p \equiv n \bmod p$ pour tout $n \in \mathbb{Z}$ et qui ne sont pas premiers (par exemple 561, 1105, 1729, 2465, 2821,...). On les appelle nombres de Carmichael[13]. On les étudiera plus en détail plus loin dans ce chapitre.

EXERCICE. Montrons que 561 est un nombre de Carmichael.

Il n'est pas premier car $561 = 3 \times 11 \times 17$. Fixons $n \in \mathbb{Z}$ quelconque et posons $N = n^{561} - n$.

$N = n(n^{560} - 1) = n((n^2)^{280} - 1)$. Or $((n^2)^{280} - 1)$ est divisible par $(n^2 - 1)$. Il existe donc $k_1 \in \mathbb{Z}$ tel que $((n^2)^{280} - 1) = (n^2 - 1)k_1$. Donc $N = (n^3 - n)k_1$. Mais, d'après le petit théorème de Fermat, le nombre premier 3 divise $(n^3 - n)$. On conclut que 3 divise N.

De même, $N = n(n^{560} - 1) = n((n^{10})^{56} - 1)$. Or $((n^{10})^{56} - 1)$ est divisible par $(n^{10} - 1)$. Il existe donc $k_2 \in \mathbb{Z}$ tel que $((n^{10})^{56} - 1) = (n^{10} - 1)k_2$. Donc $N = (n^{11} - n)k_2$. Mais, d'après le petit théorème de Fermat, le nombre premier 11 divise $(n^{11} - n)$. On conclut que 11 divise N.

De même, $N = n(n^{560} - 1) = n((n^{16})^{35} - 1)$. Or $((n^{16})^{35} - 1)$ est divisible par $(n^{16} - 1)$. Il existe donc $k_3 \in \mathbb{Z}$ tel que $((n^{16})^{535} - 1) = (n^{16} - 1)k_3$. Donc $N = (n^{17} - n)k_3$. Mais, d'après le petit théorème de Fermat, le nombre premier 17 divise $(n^{17} - n)$. On conclut que 17 divise N.

En résumé, 3, 11 et 17 divisent $N = n^{561} - n$, donc 561 divise $n^{561} - n$, pour tout $n \in \mathbb{Z}$.

La même méthode permet de montrer que 1105 est un nombre de Carmichael, en observant que $1105 = 5 \times 13 \times 17$ avec $1105 = 4 \times 276 + 1 = 12 \times 92 + 1 = 16 \times 69 + 1$.

c) Théorème de Wilson[14]

THÉORÈME: *Un entier $p \geqslant 2$ est premier si et seulement si* $(p-1)! \equiv -1 \bmod p$.

[13] Robert Daniel Carmichael, 1879-1967, mathématicien et physicien américain.

[14] John Wilson, 17411793, mathématicien britannique ; il a conjecturé ce théorème, qui était déjà connu du mathématicien irakien Alhazen (965-1039).

Preuve. Supposons d'abord qu'il existe $k \in \mathbb{N}$ tel que $(p-1)! + 1 = kp$. Soit r un diviseur de p distinct de p. On a $r \in \{1, 2, \ldots, p-1\}$, donc r divise $(p-1)!$. Ainsi r divise à la fois p et $(p-1)!$, donc divise $(p-1)! - kp = 1$. On conclut que $r = 1$; ce qui prouve que p est premier.

Réciproquement, supposons p premier. D'après la proposition du a) ci-dessus, $\mathbb{Z}/p\mathbb{Z}$ est un corps. D'après la proposition du b) ci-dessus, tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$ vérifie $a^{p-1} \equiv 1 \bmod p$. Ce qui se traduit par: tout $\overline{a} \in \mathbb{F}_p$ tel que $\overline{a} \neq \overline{0}$ vérifie $P(\overline{a}) = \overline{0}$, où l'on a noté $P(X) = X^{p-1} - \overline{1}$, polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Les zéros de $P(X)$ dans $\mathbb{Z}/p\mathbb{Z}$ sont donc tous les éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$. Le produit de ces $p-1$ zéros simples doit valoir au signe près le terme constant de $P(X)$. Plus précisément, $(-1)^{p-1}\overline{1} \times \overline{2} \times \cdots \times \overline{p-1} = -\overline{1}$. D'où le résultat puisque $(-1)^{p-1} = 1$ lorsque $p \geqslant 3$ et $-\overline{1} = \overline{1}$ lorsque $p = 2$. □

d) Une généralisation du petit théorème de Fermat.

Le but de ce paragraphe est d'introduire une généralisation du petit théorème de Fermat (dit théorème d'Euler) qui est à la base de certains procédés cryptographiques. On introduit pour cela une fonction arithmétique multiplicative (au sens du 1.2.e) précédent) particulièrement importante.

NOTATION ET DÉFINITION. Pour tout entier $n \geqslant 2$, on note $\varphi(n)$ le nombre d'entiers compris entre 1 et $n-1$ qui sont premiers avec n. Par exemple :

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2, \quad \varphi(7) = 6, \quad \varphi(8) = 4, \quad \varphi(9) = 6, \ldots$$

En convenant de plus de poser $\varphi(1) = 1$, on définit ainsi une application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, appelée *fonction indicatrice d'Euler*.

REMARQUE 1. *Si p est un nombre premier, alors $\varphi(p) = p - 1$.*

Preuve. Tout entier compris entre 1 et $p-1$ est premier avec p. □

REMARQUE 2. *Si p est un nombre premier, alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ pour tout entier $\alpha \geqslant 1$.*

Preuve. Il y a $p^\alpha - 1$ entiers compris (au sens large) entre 1 et $p^\alpha - 1$. Parmi eux, ceux qui ne sont pas premiers avec p sont exactement ceux qui sont divisibles par p (car p est premier), c'est-a-dire ceux qui sont de la forme mp avec $m \geqslant 1$ tel que $mp < p^\alpha$. Il y en a autant que de valeurs de m telles que $1 \leqslant m < p^{\alpha-1}$, à savoir $p^{\alpha-1} - 1$. On conclut que $\varphi(p) = (p^\alpha - 1) - (p^{\alpha-1} - 1)$, d'où le résultat voulu. □

On peut montrer (en utilisant le théorème des restes chinois) que φ est une fonction arithmétique multiplicative. Dès lors, on déduit de la remarque 2 ci-dessus et de la décomposition en facteurs premiers une formule permettant de calculer $\varphi(n)$ pour tout entier $n \geqslant 2$:

pour tout n donné par sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_S^{\alpha_s} = \prod_{i=1}^{s} p_i^{\alpha_i}$, on a :

$$\varphi(n) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{s} (1 - \tfrac{1}{p_i}).$$

On peut alors énoncer et démontrer le théorème suivant:

THÉORÈME (dit THÉORÈME D'EULER). *Soient a et n deux entiers $\geqslant 2$ premiers entre eux, alors:*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Preuve. Plaçons-nous dans $\mathbb{Z}/n\mathbb{Z}$ et raisonnons comme dans la preuve de la proposition 1.3.a). Parce que a est premier avec n, il existe u, v dans $\mathbb{Z}$ tels que $au + nv = 1$, et donc $\overline{a}.\overline{u} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. En d'autres termes, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. On peut de même vérifier la réciproque

immédiatement, de sorte l'ensemble G_n des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ compte autant d'éléments qu'il existe d'entiers premiers avec n qui sont compris entre 1 et $n-1$, c'est-à-dire $\varphi(n)$.

Considérons alors l'application $t : \overline{x} \mapsto \overline{ax}$ de G_n dans G_n. Elle est clairement bijective car $\overline{a}$ est inversible (la bijection réciproque est simplement $\overline{y} \mapsto \overline{a}^{-1}\overline{y}$). Donc, le produit de tous les éléments de G_n peut s'exprimer par:

$$\prod_{\overline{x}\in G_n} \overline{x} = \prod_{\overline{x}\in G_n} t(\overline{x}) = \prod_{\overline{x}\in G_n} \overline{ax} = \overline{a}^{\varphi(n)} \prod_{\overline{x}\in G_n} \overline{x}$$

puisque le nombre d'éléments de G_n est $\varphi(n)$. Ainsi $\overline{a}^{\varphi(n)} = \overline{1}$, ie. $a^{\varphi(n)} \equiv 1 \mod n$. □

REMARQUE IMPORTANTE. Dans le cas où n est un nombre premier p, dire que a est premier avec p signifie que a n'est pas multiple de p, et $\varphi(p) = p-1$. Le théorème d'Euler dans ce cas redonne donc exactement l'assertion (ii) de la proposition du 1.3.b) ci-dessus, qui découle du petit théorème de Fermat. *C'est en ce sens que le théorème d'Euler peut être vu comme une extension du petit théorème de Fermat.*

2 Nombres premiers et cryptographie[15]

2.1 Codages par exponentiation arithmétique

a) Principe. On fixe :

► un nombre premier p (que dans la pratique on choisit au moins égal à 29)

► un entier e premier avec $p-1$ (appelée clef de codage associée à p).

On déduit de ces deux données initiales:

► un entier d vérifiant $1 \leqslant d < p-1$ et $ed = 1 + k(p-1)$ avec $k \geqslant 1$ (appelé clef de décodage associée à p et e).

En effet, comme e et $p-1$ sont premiers entre eux, il résulte du théorème de Bézout qu'il existe des entiers d et v tels que $ed + v(p-1) = 1$. On peut toujours choisir d tel que $1 \leqslant d < p-1$, ce qui impose pour v d'être négatif. On note $k = -v \geqslant 1$. □

► un entier naturel m, déduit du choix de p de la façon suivante:

- si $25 < p < 2525$, on prend $m = 1$,
- si $2525 < p < 252525$, on prend $m = 2$,
- si $252525 < p < 25252525$, on prend $m = 3$,

etc...

• Comme dans le chapitre 3, on considère l'alphabet $\mathcal{A} = \{A, B, C, D, \ldots, Y, Z\}$ et on identifie chaque lettre par son "rang" dans l'alphabet, mais en numérotant cette fois chaque lettre avec deux chiffres. C'est-à-dire que l'en considère l'ensemble

$$\mathcal{F} = \{00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, \ldots, 24, 25\}$$

et la bijection naturelle g de $\mathcal{A}$ sur $\mathcal{F}$:

$$g(A) = 00,\ g(B) = 01,\ g(C) = 02,\ g(D) = 03, \ldots,\ g(Y) = 24,\ g(Z) = 25.$$

• Le message (à coder ou à décoder) est une suite de lettres dans $\mathcal{A}$, qui correspond par g à une suite de paires de chiffres dans $\mathcal{F}$, que l'on regroupe en blocs de $2m$ chiffres. Un bloc est du type:

[15] Cette section utilise largement le chapitre 5 de l'ouvrage collectif "Arithmétique" publié par l'IREM de Clermont-Ferrand et le CRDP d'Auvergne en 1998, dont on reprend la plupart des commentaires et exemples.

$$x = a_1a_2a_3a_4a_5a_6\ldots a_{2m-1}a_{2m} \quad \text{avec } a_{2i-1}a_{2i} \in \mathcal{F} \text{ pour tout } 1 \leqslant i \leqslant m \qquad (\star).$$

Il est crucial de remarquer que, d'après le choix de m que l'on a fait, tous les entiers x de la forme $(\star)$ sont strictement inférieurs à p. Par voie de conséquence, si deux tels entiers x et y sont congrus modulo p, ils sont nécessairement égaux. En d'autres termes:

$$\text{pour deux entiers } x \text{ et } y \text{ de la forme } (\star), \text{ on a: } \quad x \neq y \ \Leftrightarrow\ x \not\equiv y \mod p.$$

• FORMULE POUR LE CODAGE. *Pour tout entier x de la forme $(\star)$, le transformé de x par le codage de clef de codage e est l'unique entier entier x' compris entre 0 et $p-1$ tel que:*

$$x' \equiv x^e \mod p$$

A noter que, contrairement à x, l'entier x' ne s'écrit pas forcément avec $2m$ chiffres; en revanche, comme p s'écrit avec au plus $2(m+1)$ chiffres (d'après le choix fait au départ sur m par rapport à p) et que $x' < p$, l'entier x' s'écrit a priori avec au plus $2(m+1)$ chiffres.

Le point remarquable est que le petit théorème de Fermat fournit une méthode pour retrouver x à partir de x'. C'est le but de:

• FORMULE POUR LE DÉCODAGE. *Pour tout bloc x' de la forme ci-dessus, l'entier x de la forme $(\star)$ dont x' est le transformé, est l'unique entier x compris entre 0 et $p-1$ tel que:*

$$x \equiv x'^d \mod p,$$

où d désigne la clef de décodage associée à p et e.

Preuve. En élevant la congruence $x' \equiv x^e \mod p$ à la puissance d, il vient: $x'^d \equiv x^{ed} \mod p$. Par définition de d, ceci équivaut à $x'^d \equiv x^{1+k(p-1)} \mod p$, ou encore $x'^d \equiv x(x^{p-1})^k \mod p$. Or $x < p$, donc x n'est pas multiple de p, donc on peut appliquer le point (ii) de la proposition 1.3.b pour déduire: $x^{p-1} \equiv 1 \mod p$. D'où $(x^{p-1})^k \equiv 1 \mod p$, et finalement $x'^d \equiv x \mod p$. □

b) Exemple.

Choisissons $p = 2633$ et $e = 29$, qui vérifient bien les conditions requises. On a alors $m = 2$ donc le texte sera séquencé en blocs de 4 lettres.

Soit à coder la phrase: CECI EST UN EXEMPLE DE CODAGE EXPONENTIEL
on transforme d'abord via la bijection g en:
$\longrightarrow$ 0204 0208 0418 1920 1304 2304 1215 1104 0304 0214 0300 0604 0423 1514 1304 1319 0804 1123,
(en notant que, suivant une tradition en codage, l'on a ajouté un x au dernier bloc pour rectifier l'imparité).

Il s'agit de coder chaque bloc x de quatre chiffres par l'opération $x' \equiv x^{29} \mod 2633$, avec $0 \leqslant x' < 2633$.
Par exemple, pour le premier bloc, on calcule: $0204^{29} \equiv 1566 \mod 2633$ (voir c) ci-dessous). On faisant de même pour chaque bloc, on obtient le message codé:
$\longrightarrow$ 1566 1846 0177 0071 0960 2241 2059 1684 2435 0356 1144 2441 2437 1759 0960 0815 0951 1133.

Pour opérer réciproquement au décodage, il faut et il suffit de déterminer la clef d de décodage. On procède par divisions euclidiennes successives selon l'algorithme d'Euclide (voir plus loin).

$2632 = 90 \times 29 + 22$ donc $22 = 2632 - 90 \times 29$,
$29 = 22 + 7$ donc $7 = 29 - 22 = 29 + 90 \times 29 - 2632 = 91 \times 29 - 1 \times 2632$,
$22 = 3 \times 7 + 1$ donc $1 = (2632 - 90 \times 29) - 3 \times (91 \times 29 - 2632) = 4 \times 2632 - 363 \times 29$,
ainsi $1 \equiv -363 \times 29 \mod 2632$, ou encore $1 \equiv 2269 \times 29 \mod 2632$,

ce qui prouve que la clef de décodage cherchée est $d = 2269$.

c) Quelques caractéristiques de ce type de codages.

► Coûts en calculs raisonnables pour le codage.

Il s'agit du coût en calcul de l'élevation de chaque bloc x à la puissance e modulo p. Reprenons l'exemple du b) ci-dessus. Pour calculer x^{29} modulo 2633, on écrit 29 en base 2 [c'est-à-dire $29 = 16 + 8 + 4 + 1$] et on procède par élévations au carré successives de x modulo 2633.

Par exemple pour le premier bloc $x = 0204$, on calcule :

$204^2 \equiv 2121 \mod 2633 \Rightarrow 204^4 \equiv 2121^2 \equiv 1477 \mod 2633 \Rightarrow 204^8 \equiv 1477^2 \equiv 1405 \mod 2633$
$\Rightarrow 204^{16} \equiv 1405^2 \equiv 1908 \mod 2633$.

D'où : $204^{29} = 204^{16} \times 204^8 \times 204^4 \times 204^1 \equiv 1908 \times 1405 \times 1477 \times 204 \equiv 1566 \mod 2633$.

Le calcul de x^{29} modulo 2633 revient donc à quatre multiplications pour les élévations au carré successives, plus trois multiplications pour conclure.

► Coûts en calculs raisonnables pour le décodage.

Il s'agit d'élever chaque bloc x' à la puissance d modulo p. Dans l'exemple du b) ci-dessus, $d = 2269$, que l'on écrit en base 2 comme: $2269 = 2^{11} + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^0$. Donc:

$$(x')^{2269} = (x')^{2^{11}} \times (x')^{2^7} \times (x')^{2^6} \times (x')^{2^4} \times (x')^{2^3} \times (x')^{2^2} \times (x') \mod 2633.$$

Pour mener les élévations au carré successives, on utilise le fait que $(x')^{2^{n+1}} = ((x')^{2^n})^2$. Le calcul de $(x')^{2^{11}}$ se déduit par passage au carré de celui de $(x')^{2^{10}}$, qui lui-même se déduit par passage au carré de celui de $(x')^{2^9}$,... tout cela bien sûr modulo 2633.

En résumé, le calcul de $(x')^{2269}$ modulo 2633 revient donc à onze multiplications pour les élévations au carré successives, plus six multiplications pour conclure.

> **Estimation générale:** soit p un nombre premier, soit a est un entier tel que $0 < a < p$, soit k l'entier naturel tel que $2^{k-1} \leqslant a < 2^k$, et soit y un entier naturel non-nul. Le calcul modulo p de y^a utilise au plus $k-1$ multiplications pour déterminer les y^{2^i}, et au plus $k-1$ multiplications pour conclure en utilisant la décomposition de a en base 2 ; soit en tout au plus $2k-2$ multiplications modulo p.
> En remarquant que $k-1 \leqslant \log_2 a < k$, on conclut que le nombre de multiplications modulo p à effectuer pour calculer y^a modulo p est majoré par $2 \log_2 a$.
> Par ailleurs, une multiplication modulo p nécessite un nombre d'opérations élémentaires électroniques de l'ordre de $(\log_2 p)^2$. Donc le nombre d'opérations élémentaires nécessaires à une exponentiation par a est de l'ordre de $(\log_2 p)^2 \times \log_2 a$, ou encore $(\log_2 p)^3$ puisque $a < p$. Si p s'écrit avec n chiffres en base décimale, on a $p < 10^n$, donc $\log_2 p < n \log_2 10$.
> **Conclusion,** *le nombre d'opérations élémentaires nécessaires à une exponentiation modulo un nombre premier à n chiffres est de l'ordre de n^3.*

► Résistance à la cryptoanalyse.

Supposons qu'un analyste cherche à percer un codage par exponentiation. Supposons (cas favorable) qu'il connaisse le nombre premier p servant au codage. Supposons aussi que, par les procédés de fréquences statistiques évoquées au chapitre 3, il fasse l'hypothèse qu'un bloc codé x' soit la traduction d'un bloc x. Il lui reste à trouver la clef de codage e, c'est-à-dire à résoudre:

$$x' \equiv x^e \mod p, \quad \text{où } e \text{ est l'inconnue, et } p, x, x' \text{ sont connus.}$$

A priori, il suffit de tester tous les entiers e de 1 à $p-1$. Le coût en calculs est de l'ordre de 10^n où n est le nombre de chiffres de l'écriture de p en base 10. Même s'il existe des algorithme spécialisés permettant de réduire ce coût (qui est exponentiel en n), il est sans commune mesure avec celui du codage ou du décodage (qui est polynomial en n, de l'ordre de n^3 on vient de le voir). Pour un nombre premier p avec $n = 100$ chiffres, le temps de calcul pour trouver e peut atteindre plusieurs années, alors qu'il est de quelques fractions de secondes pour coder ou décoder un bloc. Et si l'on passe à un nombre premier p' de $n' = 200$ chiffres, on multiplie le temps de codage ou décodage par 8 (car $n'^3 = 8n^3$), mais le temps de recherche de la clef e par de 10^{100} (car $10^{n'} = (10^n)^2$) ! D'où une **bonne résistance de ce type de codage au décryptage.**

2.2 Codages à clefs publiques: exemple du système RSA[16]

a) Principe. C'est une variante du codage par exponentiation arithmétique vu au paragraphe précédent. On fixe au départ un couple d'entiers naturels (e, n):

► l'entier n, appelé le module, est le produit de deux premiers très grands (dans la pratique, quelques centaines de chiffres dans leur écriture décimale) ; on note $n = pq$.

► l'entier e, appelé l'exposant, est choisi premier avec $\varphi(n)$, où φ désigne l'indicatrice d'Euler.

On déduit du fait que e et $\varphi(n)$ sont premiers entre eux, en utilisant le théorème de Bézout comme dans le paragraphe précédent, la détermination de:

► un entier d vérifiant $1 \leqslant d < \varphi(n)$ et $ed = 1 + k\varphi(n)$ avec $k \geqslant 1$, appelé clef de décodage associée à n et e.

Comme précédemment, on découpe le texte à coder en blocs de lettres, transformés via la bijection g en blocs chiffrés d'éléments de $\mathcal{F}$. Un tel bloc x est transformé par codage en x' défini par:

$$x' \equiv x^e \mod n.$$

Réciproquement, pour décoder x', on calcule $x'^d \equiv x^{ed} \mod n$, donc: $x'^d \equiv x^{1+k\varphi(n)} \mod n$, donc: $x'^d \equiv x(x^{\varphi(n)})^k \mod n$. Or x est inférieur à p et q, donc premier avec p et q, et premier avec n. On peut donc appliquer le théorème d'Euler 1.3.d pour déduire que $x^{\varphi(n)} \equiv 1 \mod n$, donc $(x^{\varphi(n)})^k \equiv 1 \mod n$. On conclut que:

$$x'^d \equiv x \mod n.$$

b) Quelques caractéristiques du système RSA.

► Coût en calculs raisonnable.

Les coûts en temps de calcul du codage et du décodage sont de même nature que ceux vus à la fin du 2.1. Et les tests de primalités permettent de trouver rapidement des couples de nombres premiers p et q d'un nombre de chiffres suffisamment grands (en testant des couples arbitraires d'entiers et en utilisant la fréquences des nombres premiers parmi les entiers naturels, voir section suivante, avec par exemple un entier de 100 chiffres sur 115 qui est premier).

► Très forte résistance à la cryptoanalyse.

Le couple (e, n) peut être connu de tous (c'est pour cela qu'on parle de cryptographie "à clef publique". Mais pour décoder, il faut inverser e modulo $\varphi(n)$, donc connaître $\varphi(n)$. Comme $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, cela revient à déterminer les deux nombres premiers p et q connaissant leur produit n (c'est-à-dire à retrouver la factorisation de n en le produit de deux nombres premiers "grands"). Et c'est un problème très lourd, sur lequel on ne dispose pas d'algorithme rapide (si p et q ont chacun environ 100 chiffres, donc n de l'ordre de 200 chiffres, retrouver p et q à partir de n reprénte des milliers d'années de calcul).

► Capacité à assurer la confidentialité et l'authenticité des communications au sein d'un réseau.

A chaque individu N_i d'un réseau sont associées une clef publique e_i connue de tous et une clef secrète d_i connue d'elle seule. Lorsque N_i veut s'adresser confidentiellement à N_j, il code son message à l'aide de e_j (qui est publique), et seul N_j peut le décoder (à l'aide de sa clef d_j).

Mieux, pour assurer l'authenticité de l'expéditeur, si N_i veut envoyer une message x à N_j, il commence par le coder avec la clef publique e_j (le message x devient $x_1 \equiv x^{e_j} \mod n$), puis il code le message x_1 avec sa clef secrète d_i. Le message x_1 devient $x_2 \equiv x_1^{d_i} \equiv x^{d_i e_j} \mod n$. Lorsque N_j reçoit x_2, il le décode en appliquant d'abord la clef publique e_i de N_i, puis sa propre clef secrète d_j; il obtient $x_3 \equiv x_2^{e_i} \equiv x^{e_j d_i e_i} \equiv x^{e_j} \mod n$, puis $x_3^{d_j} \equiv x^{e_j d_j} \equiv x \mod n$. Ainsi nul ne peut communiquer à la place d'un individu du réseau sans disposer de sa clef secrète.

[16] du nom de R. Rivest, A. Shamir et L. Adleman en 1978, bien que le concept innovant de codes à clef publique apparaisse dès 1976 chez W. Diffie et M. Hellman.

3 Quelques thèmes complémentaires sur les nombres premiers

3.1 Sur la répartition des nombres premiers

a) Problématiques. On a démontré en 1.1.c qu'il existe une infinité de nombres premiers. Mais comment sont-ils répartis ? Gauss avait déjà établi que:

> *il y a 25 nombres premiers inférieurs 100 ; il y a 168 nombres premiers inférieurs 1000 ; il y a 1229 nombres premiers inférieurs 10000 ; il y a 9592 nombres premiers inférieurs 100000 ; il y a 78498 nombres premiers inférieurs 1000000 ; il y a 664579 nombres premiers inférieurs 10000000.*

• Par ailleurs; il est facile de démontrer qu'il existe dans la suite de tous les entiers naturels des "trous" (ie. des intervalles sans aucun nombres premiers) de longueur arbitrairement grande. Plus précisément: *pour tout entier* $n \geqslant 1$*, on peut trouver une liste de* n *entiers naturels consécutifs qui ne contient aucun nombre premiers.*

> *Preuve.* On construit les n entiers consécutifs: $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1$. Aucun n'est premier car, pour tout $2 \leqslant i \leqslant n+1$, l'entier i divise $(n+1)!$, et donc divise $(n+1)!+i$. □

• A contrario, il existe des nombres premiers "les plus rapprochés possibles", c'est-à-dire des couples $(p, p+2)$ où p et $p+2$ sont tous les deux premiers (on dit que ce sont des *nombres premiers jumeaux*), et il "semble bien" que l'on puisse en trouver "aussi loin que l'on aille". En clair, il est *conjecturé* (ce n'est qu'une conjecture, non encore résolue aujourd'hui mais qui fait l'objet de nombreux travaux) qu'*il existe une infinité de nombres premiers jumeaux.*

> les nombres premiers jumeaux inférieurs à mille sont : $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$, $(107,109)$, $(137,139)$, $(149,151)$, $(179,181)$, $(191,193)$, $(197,199)$, $(227,229)$, $(239,241)$, $(269,271)$, $(281,283)$, $(311,313)$, $(347,349)$, $(419,421)$, $(431,433)$, $(461,463)$, $(521,523)$, $(569,571)$, $(599,601)$, $(617,619)$, $(641,643)$, $(659,661)$, $(809,811)$, $(821,823)$, $(827,829)$, $(857,859)$, $(881,883)$.
>
> 1 269 989 et 1 269 991 forment le dix-millième couple de nombres premiers jumeaux.
>
> Le plus grand couple de nombres premiers jumeaux actuellement connu (E. Vautier 2007) est $2003663613 \times 2^{195000} \pm 1$; les deux nombres possèdent 58 711 chiffres en écriture décimale.

b) Le "théorème des nombres premiers"

Pour tout réel $x \geqslant 2$, on note $\pi(x)$ le nombre de nombres premiers qui sont inférieurs ou égaux à x.

$$\pi(x) = \text{Card}\{p\,;\ p \text{ premier et } p \leqslant x\}$$

De façon heuristique, on porte dans le tableau suivant, pour différentes valeurs de x, le nombre $\pi(x)$ de nombres premiers plus petits que x, la fréquence $\pi(x)/x$ de ceux-ci, l'inverse $x/\pi(x)$ de cette fréquence, et l'écart Δ de la valeur de $x/\pi(x)$ quand on multiplie x par 10. On obtient:

x	$\pi(x)$	$\pi(x)/x$	$x/\pi(x)$	Δ
100	25	0,25	4	
1000	168	0,17	5,95	1,95
10000	1229	0,12	8,14	2,8
100000	9592	0,1	10,43	2,29
1000000	78498	0,08	12,84	2,31
10000000	664579	0,07	15,05	2,31
100000000	5761455	0,06	17,36	2,31

Cette expérimentation numérique met en évidence que la fonction $u(x) := x/\pi(x)$ satisfait:

$$u(10x) - u(x) \approx 2,3\ldots \approx \ln 10.$$

Il est alors naturel de conjecturer que $u(x) \approx \ln x$ pour x assez grand, ou en d'autres termes que le rapport de $\pi(x)$ sur $x/\ln x$ tend vers 1 pour x tendant vers l'infini. C'est en fait un théorème:

THÉORÈME. *La fonction π est équivalente à la fonction $\frac{x}{\ln x}$ au voisinage de $+\infty$.*

- Le résultat avait été conjecturé par Gauss suivant les estimations numériques explicitées ci-dessus (en 1792, il avait alors 15 ans). Il n'a été démontré qu'en 1896 indépendamment et simultanément par Hadamard[17] et De La Vallée Poussin[18], par des méthodes d'analyse complexes qui dépassent largement le contexte de ce cours.

- A noter qu'auparavant, un progrès important avait été réalisé par Tchebychev[19] qui avait prouvé l'existence de deux constantes k et k' telles que $k' \leqslant \pi(x)\frac{\ln x}{x} \leqslant k$ pour x assez grand (voir exercice ci-dessous).

- A noter aussi qu'une meilleure approximation de π est donnée par la fonction $\mathrm{li}\,(x) = \int_2^x \frac{dt}{\ln t}$, qui est un autre équivalent de π au voisinage de $+\infty$. Ce résultat avait également été conjecturé par Gauss (en 1841, il avait alors 64 ans). Dans leurs preuves, Hadamard et De La Vallée Poussin montrent que π est bien approchée par li, et que l'erreur commise est inférieure à $x\exp(-\frac{\sqrt{\ln x}}{15})$. L'amélioration de ce terme d'erreur est encore une branche de la recherche de la théorie analytique des nombres, en lien avec la fonction ζ de Riemann et avec l'hypothèse de Riemann, l'une des plus importantes conjectures des mathématiques.

c) Exercice: un résultat de majoration de π du type inégalité de Tchebychev.

Le but est de montrer comment, par des procédés élémentaires, on peut obtenir des majorations de $\pi(x)$ de la forme $\pi(x) \leqslant k\frac{x}{\ln x}$ avec k une constante positive (il existe de très nombreuses variantes de ce type de calculs, et d'autres voisins pour obtenir des minorations de la même forme[20]). On utilisera la notation suivante: si $m < n$ sont deux entiers,

$$\prod_{m<p\leqslant n} p \text{ désigne le produit des nombres } \textit{premiers} \text{ compris entre } m \text{ et } n,$$

avec la convention que ce produit vaut 1 s'il n'existe pas de nombre premier p tels que $m < p \leqslant n$.

LEMME. *Pour tout entier $n \geqslant 2$, on a:* $\prod_{p\leqslant n} p \leqslant 4^n$.

Preuve. Soient $m \geqslant 1$ un entier et $M := \binom{2m+1}{m+1} = \frac{1}{m!}(m+2)(m+3)\cdots(2m+1)$. Parmi les facteurs du produit $(m+2)(m+3)\cdots(2m+1)$ apparaissent en particulier tous les nombres premiers p tels que $m+1 < p \leqslant 2m+1$. Il en résulte que le produit $P := \prod_{m+1<p\leqslant 2m+1} p$ divise $(m+2)(m+3)\cdots(2m+1)$. Par ailleurs, comme M est un entier, l'entier $m!$ divise aussi $(m+2)(m+3)\cdots(2m+1)$. Mais comme les facteurs de $m! = 1.2.3.\cdots m$ sont tous strictement inférieurs à $m+1$, les entiers $m!$ et P sont premiers entre eux. Ainsi $m!$ et P sont deux diviseurs de $(m+2)(m+3)\cdots(2m+1)$ qui sont premiers entre eux, donc leur produit est aussi un diviseur de $(m+2)(m+3)\cdots(2m+1)$. On a $P \times m!$ qui divise $(m+2)(m+3)\cdots(2m+1)$, donc P divise $\frac{1}{m!}(m+2)(m+3)\cdots(2m+1)$. On a montré que:

[17] Jacques Hadamard, 1865-1963, mathématicien français, connu en particulier pour ses travaux en analyse complexe et théorie des nombres.

[18] Charles-Jean de La Vallé Poussin, 1866 - 1962, mathématicien belge.

[19] Pafnouti Tchebychev, 1821-1894, mathématicien russe de tout premier plan, en particulier par ses travaux dans le domaine des probabilités et des statistiques.

[20] En particulier l'encadrement : $\frac{\ln 2}{4}\cdot\frac{x}{\ln x} \leqslant \pi(x) \leqslant 6\ln 2\frac{x}{\ln x}$

$$\prod_{m+1<p\leqslant 2m+1} p \text{ divise } \binom{2m+1}{m+1}. \qquad (1)$$

Effectuons maintenant à l'aide de la formule du binôme le calcul:

$2.4^m = (1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} \geqslant \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2.\binom{2m+1}{m+1}$, d'où l'on déduit:

$$\binom{2m+1}{m+1} \leqslant 4^m. \qquad (2)$$

On est maintenant en mesure de montrer par récurrence l'inégalité du lemme. Elle est clairement vérifiée pour $n = 2, 3$ et 4. Supposons par HR qu'elle est satisfaite jusqu'à un rang $2n$. On calcule d'abord:

$\prod_{p\leqslant 2n+1} p = (\prod_{p\leqslant n+1} p)(\prod_{n+1<p\leqslant 2n+1} p) \leqslant 4^{n+1}.4^n = 4^{2n+1}$ en utilisant (HR), (1) et (2),

puis, en utilisant le fait que $2n+2$ n'est pas premier: $\prod_{p\leqslant 2n+2} p = \prod_{p\leqslant 2n+1} p \leqslant 4^{2n+1} \leqslant 4^{2n+2}$,

ce qui prouve le résultat voulu au rang $2(n+1)$. □

PROPOSITION. *Pour tout entier $n \geqslant 4$, on a:* $\pi(n) \leqslant 7\,\dfrac{n}{\ln n}$.

Preuve. Introduisons un réel $t < n$ et remarquons avec le lemme que $\prod_{t<p\leqslant n} p \leqslant \prod_{p\leqslant n} p \leqslant 4^n$. Or $\prod_{t<p\leqslant n} p \geqslant t^{\pi(n)-\pi(t)}$ car le produit $\pi(n)-\pi(t)$ nombres premiers, tous supérieurs à t.

Donc: $t^{\pi(n)-\pi(t)} \leqslant 4^n$, d'où: $(\pi(n)-\pi(t))\ln t \leqslant n \ln 4$, puis: $\pi(n) \leqslant n\frac{\ln 4}{\ln t} + \pi(t) \leqslant n\frac{\ln 4}{\ln t} + t$.

Pour $t = \dfrac{n}{(\ln n)^2}$, il vient : $\pi(n) \leqslant \dfrac{n}{\ln n} \times \dfrac{\ln 4}{1 - 2\,\frac{\ln(\ln n)}{\ln n}} + \dfrac{n}{(\ln n)^2}$.

La fonction $f(x) = \dfrac{\ln x}{x}$, dont la dérivée est $f'(x) = \dfrac{1-\ln x}{x^2}$, est majorée par $1/e$.

Donc : $0 < \dfrac{\ln(\ln n)}{\ln n} \leqslant \dfrac{1}{e}$, d'où l'on tire : $\dfrac{\ln 4}{1 - 2\,\frac{\ln(\ln n)}{\ln n}} \leqslant \dfrac{\ln 4}{1-2/e} \approx 5,24... < 6$.

Ainsi : $\pi(n) \leqslant 6\,\dfrac{n}{\ln n} + \dfrac{n}{(\ln n)^2} \leqslant 6\,\dfrac{n}{\ln n} + \dfrac{n}{\ln 4 \ln n} \leqslant 7\,\dfrac{n}{\ln n}$. □

d) Commentaire. Indépendamment de leurs liens avec le théorème de Hadamard et De La Vallée Poussin, les inégalités de Tchebychev sont à la base de divers autres résultats sur la répartition des nombres premiers, comme par exemple:

► le postulat de Bertrand[21] (qui en fait n'est plus un postulat puisqu'il a été démontré, par Tchbychef en 1850, puis par Erdös[22] en 1932 avec une preuve beaucoup plus simple dont l'ingrédient essentiel est le lemme du c) ci-dessus), énoncé qui établit que, pour tout entier $n \geqslant 2$, il existe un nombre premier au moins entre n et $2n$;

► les théorèmes d'Ishikawa (1934) prouvant que, avec la notation usuelle p_n pour désigner le n-ième nombre premier, on a: $p_n + p_{n+1} > p_{n+2}$ et $p_n p_m > p_{n+m}$.

[21] Joseph Bertrand, 1822-1900, mathématicien, économiste et historien des sciences français.

[22] Paul Erdös, 1913-1996, mathématicien hongrois, célèbre avant tout pour l'ampleur de son œuvre mathématique, mais aussi pour une certaine excentricité source de nombreuses anecdotes.

3.2 Tests de primalité et nombres pseudo-premiers

Par définition, un entier $n \geqslant 2$ qui n'est pas un nombre premier est dit *composé.* On développe ici les principes théoriques de méthodes testant si un entier $n \geqslant 2$ donné est premier ou composé.

Rappelons tout d'abord qu'il résulte des résultats vus en 1.3.b que, pour tout entier $n \geqslant 2$:

(1) n *premier* $\implies$ *pour tout entier* a, *on a:* $a^n \equiv a \bmod n$,

(1') n *premier* $\implies$ *pour tout entier* a *premier avec* n, *on a:* $a^{n-1} \equiv 1 \bmod n$,

(2) n *premier* $\iff$ *pour tout entier* a *non divisible par* n, *on a:* $a^{n-1} \equiv 1 \bmod n$,

(2') n *premier* $\iff$ *pour tout entier* a *tel que* $1 \leqslant a \leqslant n-1$, *on a:* $a^{n-1} \equiv 1 \bmod n$,

les assertions **(1)** et **(1')** étant deux formulations équivalentes du petit théorème de Fermat, et les assertions **(2)** et **(2')** incluant des arguments complémentaires pour une réciproque.

a) Tests de Fermat. Etant donné un entier $n \geqslant 2$, on peut appliquer la procédure suivante, basée sur **(1)**, pour détecter *éventuellement* s'il est composé.

(i) On fait des essais préliminaires de division par 2,3,5,7,11... par exemple par tous les nombres premiers jusqu'à 1000 ; si n est divisible par l'un de ces nombres premiers, alors n est composé. Sinon, on passe à l'étape suivante.

(ii) On calcule $2^n \bmod n$; si le résultat n'est pas 2, alors n est composé. Sinon, on passe à l'étape suivante.

(iii) On calcule $3^n \bmod n$; si le résultat n'est pas 3, alors n est composé. Sinon, on passe à l'étape suivante.

(iv) On ne teste pas 4^n car on sait à cette étape que $2^n \equiv 2 \bmod n$ et donc $4^n \equiv 4 \bmod n$. On calcule $5^n \bmod n$; si le résultat n'est pas 5, alors n est composé. Sinon, on passe à l'étape suivante.

Et on répète le processus avec tous les nombres premiers de la première étape. Si à la fin du test l'entier n a passé toutes les étapes sans détecter qu'il est composé, on ne peut rien conclure car **(1)** ne donne qu'une condition nécessaire pour que n soit premier, et donc qu'une condition suffisante pour que n soit composé. Les nombres n posant problème sont ceux qui vérifient $a^n \equiv a \bmod n$ pour tous les entiers a utilisés dans la suite de tests. D'où l'intérêt de la notion suivante.

b) Nombres pseudo-premiers. On introduit d'abord la définition suivante, basée sur **(1')**.

DÉFINITION. Soit $b \geqslant 2$ un entier. On appelle *nombre pseudo-premier de base* b un entier impair $n \geqslant 9$, qui est composé, qui est premier avec b, et qui vérifie $b^{n-1} \equiv 1 \bmod n$.

NOTATION. On note $\mathrm{pp}(b)$ l'ensemble des nombres pseudo-premiers de base b.

Des questions simples se posent alors naturellement: peut-on donner des exemples de nombres pseudo-premiers pour tout b (l'ensemble $\mathrm{pp}(b)$ est-il non-vide quel que soit b) ? y en a-t-il un nombre fini (l'ensemble $\mathrm{pp}(b)$ est-il fini ou infini suivant les valeurs de b) ? On y répond ci-dessous.

EXEMPLES.

(i) $91 \in \mathrm{pp}(3)$. En effet: $91 = 7 \times 13$ est bien impair et composé. D'une part, $3^{90} = (3^6)^{15} \equiv 1^{15} \equiv 1 \bmod 7$ (en utilisant pour le fait que $3^6 = 729 = 7 \times 104 + 1$ l'avant-dernière étape, et le petit théorème de Fermat pour la dernière). D'autre part, $3^{90} = (3^3)^{30} = (2 \times 13 + 1)^{30} \equiv 1 \bmod 13$. Ainsi $3^{90} \equiv 1 \bmod 7$ et $3^{90} \equiv 1 \bmod 13$, donc $3^{90} \equiv 1 \bmod 91$

(ii) $341 \in \mathrm{pp}(2)$. En effet: $341 = 11 \times 31$ est bien impair et composé. D'une part, en utilisant le fait que $2^{10} = 2^{11-1} \equiv 1 \bmod 11$ d'après le petit théorème de Fermat, on a: $2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \bmod 11$. D'autre part, $2^{340} = (2^5)^{68} = (31+1)^{68} \equiv 1 \bmod 31$. Ainsi $2^{340} \equiv 1 \bmod 11$ et $2^{340} \equiv 1 \bmod 31$, donc $2^{340} \equiv 1 \bmod 341$.

(iii) $341 \notin \mathrm{pp}(3)$. En effet: d'une part, en utilisant le fait que $3^{10} = 3^{11-1} \equiv 1 \bmod 11$ d'après le petit théorème de Fermat, on a: $3^{340} = (3^{10})^{34} \equiv 1^{34} \equiv 1 \bmod 11$. D'autre part, comme $3^{30} \equiv 1 \bmod 31$ d'après le petit théorème de Fermat, on déduit $3^{340} = (3^{30})^{11} \times 3^{10} \equiv 3^{10} \bmod 31$; puis $3^{10} = (3^2 \times 3^3)^2 \equiv (9 \times (-4))^2 \equiv (-5)^2 \equiv 25 \bmod 31$. Ainsi $3^{340} \equiv 1 \bmod 11$ et $3^{340} \equiv 25 \bmod 31$, donc $3^{340} \equiv 25 \bmod 341$ et finalement $3^{340} \not\equiv 1 \bmod 341$.

THÉORÈME. *Pour tout entier* $b \geqslant 2$, *il existe une infinité d'éléments dans* $\mathrm{pp}(b)$.

Preuve. On fixe $b \geqslant 2$. Il existe une infinité de nombres premiers p strictement supérieurs à b^2-1, donc ne divisant pas b^2-1, pour chacun de ces nombres premiers p, on définit l'entier:

$$n_p := \tfrac{b^{2p}-1}{b^2-1} = b^{2(p-1)} + b^{2(p-2)} + \cdots + b^2 + 1. \qquad (*)$$

On va montrer que tous ces n_p sont dans $\mathrm{pp}(b)$, ce qui établira bien le théorème.

► Pour cela, on vérifie d'abord que n_p est un nombre composé en observant que:

$$n_p = \tfrac{b^p-1}{b-1} \cdot \tfrac{b^p+1}{b+1} = (b^{p-1} + b^{p-2} + \cdots + b + 1)((-b)^{p-1} + (-b)^{p-2} + \cdots + (-b) + 1).$$

► De plus, il résulte du théorème de Fermat que $b^p \equiv b \bmod p$, d'où $b^{2p} \equiv b^2 \bmod p$, donc p divise $b^{2p} - b^2$. Or, avec (*), on a :

$$b^{2p} - b^2 = b^2(b^{2(p-1)} - 1) = b^2(b^2-1)(b^{2(p-2)} + b^{2(p-1)} + \cdots + b^2 + 1) = (b^2-1)(n_p - 1),$$

d'où, comme p est premier avec b^2-1 par hypothèse, on déduit avec le théorème de Gauss que p divise $n_p - 1$. Il existe ainsi un entier m tel que $n_p - 1 = mp$, ou encore $n_p + (-m)p = 1$, ce qui prouve avec le théorème de Bézout que n_p est premier avec p.

► Par ailleurs, $n_p - 1$ est pair ; en effet, il apparaît dans (*) comme la somme d'un nombre pair de termes (à savoir $p-1$ termes) qui ont tous la même parité (à savoir celle de b). Dès lors, puisque 2 est divisible à la fois par p (qui est impair) et par 2, il est divisible par $2p$. Ainsi il existe un entier k (qui vérifie en fait $m = 2k$) tel que $n_p - 1 = 2pk$. On déduit:

$$b^{n_p-1} - 1 = b^{2pk} - 1 = (b^{2p} - 1)(b^{2p(k-1)} + b^{2p(k-2)} + \cdots + b^{2p} + 1),$$

de sorte que $b^{2p} - 1$ divise $b^{n_p-1} - 1$. Or n_p divise $b^{2p} - 1$ d'après (*), et donc n_p divise $b^{n_p-1} - 1$. En d'autres termes, $b^{n_p-1} \equiv 1 \bmod n_p$, ce qui achève la preuve. □

REMARQUES. On dispose d'algorithmes permettant de calculer b^{n-1} modulo n rapidement (voir plus haut 2.1.c). C'est ce qui fait l'intérêt des tests de primalité précédents, dans la mesure où ils permettent de dire que des entiers sont composés sans avoir besoin de déterminer explicitement leur décomposition comme produit de facteurs (problème beaucoup plus ardu, voir plus haut 2.2.b).

Cependant, le test de Fermat pour des valeurs successives de b afin de déterminer si un entier n est composé ne peut aboutir que si n n'appartient pas à tous les $\mathrm{pp}(b)$. Or de tels entiers composés n existent, comme on va le voir maintenant.

c) Nombres de Carmichael.

DÉFINITION. On appelle *nombre de Carmichael* un entier naturel positif impair, qui est composé, et qui vérifie $b^{n-1} \equiv 1 \bmod n$ pour tout entier naturel b premier avec n.

EXEMPLES. On a vu plus haut en 1.3.b que 561 est un nombre de Carmichael. Il en est de même de 1105, 1729, 2465, 2821,... Mais aussi de 997 633, qui est un cas particulier de la propriété générale suivante, qui est une source d'exemples.

PROPOSITION. *Soit n un entier composé impair. On suppose que sa décomposition primaire est de la forme $n = p_1 p_2 \dots p_s$ avec les p_i premiers impairs deux à deux distincts, et tels que $p_i - 1$ divise $n - 1$ pour tout $1 \leqslant i \leqslant s$. Alors n est un nombre de Carmichael.*

> *Preuve.* Soit $b \geqslant 2$ un entier premier avec n. Pour tout $1 \leqslant i \leqslant s$, le diviseur premier p_i de n ne divise pas b et donc, en appliquant le petit théorème de Fermat, vérifie $b^{p_i - 1} \equiv 1 \bmod n$. Or, par hypothèse $p_i - 1$ divise $n - 1$, donc il existe un entier $k_i \geqslant 1$ tel que $n - 1 = k_i(p_i - 1)$. Donc $b^{n-1} \equiv 1^{k_i} \equiv 1 \bmod p_i$. Ainsi tous les p_i pour $1 \leqslant i \leqslant s$ divisent $b^{n-1} - 1$. Comme ils sont premiers deux à deux distincts, il en résulte que n divise $b^{n-1} - 1$,ie. $b^{n-1} \equiv 1 \bmod n$. □

Comme annoncé ci-dessus, l'exemple de $997\,633 = 7 \times 13 \times 19 \times 577$ vérifie que $7-1 = 6$, $13-1 = 12$, $19 - 1 = 18$ et $577 - 1 = 576$ sont des diviseurs de $997\,633 - 1 = 997\,632$ (ceci car $997\,632 = 6 \times 166\,272 = 12 \times 83136 = 18 \times 55424 = 576 \times 1732$), et donc $997\,633$ est un nombre de Carmichael.

REMARQUES ET COMMENTAIRES.

(i) On peut montrer que les nombres de Carmichael ont au moins trois facteurs premiers dans leur décomposition primaire. Le premier nombre de Carmichael se décomposant en $k = 3, 4, 5, \dots$ facteurs premiers est (sequence A006931 in OEIS) :

$$\begin{aligned}
k = 3 &\rightarrow 561 = 3 \cdot 11 \cdot 17 \\
k = 4 &\rightarrow 41041 = 7 \cdot 11 \cdot 13 \cdot 41 \\
k = 5 &\rightarrow 825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73 \\
k = 6 &\rightarrow 321197185 = 5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137 \\
k = 7 &\rightarrow 5394826801 = 7 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 73 \\
k = 8 &\rightarrow 232250619601 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 73 \cdot 163 \\
k = 9 &\rightarrow 9746347772161 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641
\end{aligned}$$

(ii) Les premiers nombres de Carmichael possédant 4 facteurs premiers dans leurs décomposition primaires sont (sequence A074379 in OEIS):

$41041 = 7 \cdot 11 \cdot 13 \cdot 41$	$62745 = 3 \cdot 5 \cdot 47 \cdot 89$	$63973 = 7 \cdot 13 \cdot 19 \cdot 37$
$75361 = 11 \cdot 13 \cdot 17 \cdot 31$	$101101 = 7 \cdot 11 \cdot 13 \cdot 101$	$126217 = 7 \cdot 13 \cdot 19 \cdot 73$
$172081 = 7 \cdot 13 \cdot 31 \cdot 61$	$188461 = 7 \cdot 13 \cdot 19 \cdot 109$	$278545 = 5 \cdot 17 \cdot 29 \cdot 113$

(iii) Du point de vue de la problématique des tests de primalité du type Fermat évoquée ci-dessus, le point crucial est qu'il a été démontré (relativement récemment, en 1994, par Alford, Granville et Pomerance) qu'*il existe une infinité de nombres de Carmichael* !

Plus précisément, ils démontrent que, si l'on note $C(x)$ le nombre de nombres de Carmichael inférieurs à un réel x donné, on a: $C(x) > x^{2/7}$.

On peut avoir une idée de la répartition des nombres de Carmichael avec les données suivantes (par R. Pinch 2007) :

n	3	4	5	6	7	8	9	10	11	12	13
$C(10^n)$	1	7	16	43	105	255	646	1547	3605	8241	19279

n	14	15	16	17	18	19	20	21
$C(10^n)$	44706	105212	246683	585355	1401644	3381806	8220777	20138200

d) Test de Miller[23]. On commence par l'observation suivante. Soit $b \geqslant 2$ un entier. Soit $n = 2m+1$ un entier impair, que l'on suppose premier avec b et vérifiant $b^{n-1} \equiv 1 \bmod n$. Posons $c = b^{\frac{n-1}{2}} = b^m$, de sorte que $c^2 \equiv 1 \bmod n$. Ainsi n divise $c^2 - 1 = (c-1)(c+1)$. Si n est un nombre premier, cela implique que n divise $c-1$ ou n divise $c+1$, c'est-à-dire que $c \equiv \pm 1 \bmod n$. Par contraposition, on conclut que: $(b^{\frac{n-1}{2}} \not\equiv \pm 1 \bmod n) \Rightarrow (n \text{ composé})$.

DÉFINITION. Soit n un entier positif impair, de sorte que l'entier pair $n-1$ peut s'écrire sous la forme $n-1 = 2^s t$, avec $s \geqslant 1$ et t impair. Soit $b \geqslant 2$ un entier premier avec n. On dit que b *satisfait le test de Miller de base* b lorsque:

$$b^t \equiv 1 \bmod n, \quad \text{ou} \quad b^{2^i t} \equiv -1 \bmod n \text{ pour un certain } 0 \leqslant i \leqslant s-1.$$

PROPOSITION. *Tout nombre premier* $n \geqslant 3$ *satisfait le test de Miller de base* b *pour tout entier* $2 \leqslant b \leqslant n-1$.

> *Preuve.* Posons $n-1 = 2^r t$ avec $s \geqslant 1$ et t impair. Pour tout $0 \leqslant i \leqslant s-1$, posons $x_i = b^{2^i t}$. Comme $b < n$ et n est premier, les entiers n et b sont premiers entre eux, et il résulte donc du petit théorème de Fermat que $b^{n-1} \equiv 1 \bmod n$. Mais $b^{n-1} = x_s$, et donc $x_s \equiv 1 \bmod n$. Comme $x_s = x_{s-1}^2$, on a $x_{s-1}^2 \equiv 1 \bmod n$, ce qui implique, parce que n est premier (voir l'observation initiale ci-dessus), que $x_{s-1} \equiv \pm 1 \bmod n$. Si $x_{s-1} \equiv -1 \bmod n$, alors n satisfait le test de Miller de base b ; sinon on a $x_{s-1} \equiv 1 \bmod n$, c'est-à-dire $x_{s-2}^2 \equiv 1 \bmod n$, d'où $x_{s-2} \equiv \pm 1 \bmod n$. En réitérant, ou bien on trouve un entier $1 \leqslant j \leqslant s$ tel que $x_{s-j} \equiv -1 \bmod n$, et alors n satisfait le test de Miller de base b, ou bien $x_s \equiv x_{s-1} \equiv x_{s-2} \equiv \cdots \equiv x_0 \equiv 1 \bmod n$. Mais alors $x_0 = b^t$ donne $b^t \equiv 1 \bmod n$, et donc n satisfait le test de Miller de base b. □

PROPOSITION. *Si un entier naturel impair* $n \geqslant 3$ *est composé et satisfait le test de Miller de base* b *pour un entier* $b \geqslant 2$ *premier avec* n, *alors* n *est pseudo-premier de base* b.

> *Preuve.* Notons toujours $n-1 = 2^r t$ avec $s \geqslant 1$ et t impair. Si $b^t \equiv 1 \bmod n$, alors $b^{n-1} \equiv 1^{2^s} \equiv 1 \bmod n$, et donc $n \in \mathrm{pp}(b)$. Sinon, il existe $0 \leqslant i \leqslant s-1$ tel que $b^{2^i t} \equiv -1 \bmod n$, donc $b^{2^{i+1} t} \equiv (-1)^2 \equiv 1 \bmod n$. On en déduit que $b^{n-1} \equiv 1^{2^{s-i-1}} \equiv 1 \bmod n$, et l'on conclut de même que $n \in \mathrm{pp}(b)$. □

REMARQUE. La proposition précédente peut aussi se formuler en disant que *si un entier naturel impair* $n \geqslant 3$ *est composé et satisfait le test de Miller de base* b *pour un entier* $b \geqslant 2$ *premier avec* n, *alors il satisfait le test de Fermat de base* b.
La réciproque est fausse, comme le montre le contre-exemple suivant.

> *Contre-exemple.* L'entier $n = 561$ satisfait le test de Fermat de base b pour tout entier naturel b premier avec 561 (car c'est un nombre de Carmichael). Et pourtant il ne satisfait pas le test de Miller de base 2, car, en notant $n-1 = 560 = 2^4.35$, on a :
>
> $$2^{35} \equiv 263 \not\equiv \pm 1 \bmod (561), \qquad 2^{2.35} \equiv 166 \not\equiv -1 \bmod (561),$$
> $$2^{2^2.35} \equiv 67 \not\equiv -1 \bmod (561), \qquad 2^{2^3.35} \equiv 1 \not\equiv -1 \bmod (561).$$
>
> On pourrait démontrer de même que le nombre $n = 997\,633$, qui vérifie $n-1 = 997\,632 = 2^8.3897$ et dont on a vu précédemment qu'il est un nombre de Carmichael, ne satisfait pas lui non plus le test de Miller de base 2.

Ainsi, le test de Miller apparaît comme une version forte du test de Fermat et, de même que l'on a défini une notion de nombres-pseudo premier de base b pour désigner les entiers satisfaisant au test de Fermat de base b, de même il est naturel d'introduire une notion de nombres-pseudo premier fort de base b pour désigner les entiers satisfaisant au test de Miller de base b.

[23] Gary Lee Miller, informaticien et mathématicien américain, actuellement professeur à la Carnegie Mellon University de Pittsburgh. On lui doit la version originelle dans les années 70 du type de test présenté ici, modifiée pour obtenir un algorithme probabiliste par le mathématicien germano-polonais Michael Rabin.

e) Nombres pseudo-premiers forts.

DÉFINITION. Soit $b \geqslant 2$ un entier. On appelle *nombre pseudo-premier fort de base* b un entier impair $n \geqslant 9$, qui est composé, qui est premier avec b, et qui satisfait le test de Miller de base b.

NOTATION. On note $\mathrm{ppf}(b)$ l'ensemble des nombres pseudo-premiers de base b. D'après la dernière remarque ci-dessus, on a:

$$\mathrm{ppf}(b) \subset \mathrm{pp}(b),$$

l'inclusion pouvant être stricte comme on l'a vu ci-dessus avec $561 \in \mathrm{pp}(2)$ et $561 \notin \mathrm{ppf}(2)$.

EXEMPLE. On a: $2047 \in \mathrm{ppf}(2)$.

En effet: $n = 2047 = 23.89$ est composé et vérifie $n - 1 = 2046 = 2.1023$.

On peut d'abord observer que $2^{2046} = (2^{11})^{186} = 2048^{186} = (2047+1)^{186} \equiv 1 \bmod 2047$ en utilisant la formule du binôme ; ce qui montre que $2047 \in \mathrm{pp}(2)$.

De même, $2^{1023} = (2^{11})^{93} = 2048^{93} = (2047+1)^{93} \equiv 1 \bmod 2047$, donc $2047 \in \mathrm{ppf}(2)$.

La proposition suivante donne une famille d'exemples de nombres pseudo-premiers forts de base 2 (et montre au passage que $\mathrm{ppf}(2)$ est infini).

PROPOSITION. *Pour tout nombre premier* $p \geqslant 7$, *l'entier* $\dfrac{4^p+1}{5}$ *est dans* $\mathrm{ppf}(2)$.

Preuve. On pose $n = \frac{4^p+1}{5}$. Comme $4^p \equiv (-1)^p \bmod 5$ avec p est impair, on a $4^p+1 \equiv 0 \bmod 5$, de sorte que n est bien un entier. Par ailleurs, en notant que $\frac{p+1}{2}$ est lui aussi un entier, on a:

$$4^p + 1 = (2^p+1)^2 - 2^{p+1} = (2^p + 1 - 2^{(p+1)/2})(2^p + 1 + 2^{(p+1)/2}).$$

Comme 5 divise 4^p+1 et que 5 est premier, il divise forcément d'un des deux facteurs de cette décomposition, et l'entier $\frac{4^p+1}{5}$ est composé si et seulement si:

$$2^p + 1 + 2^{(p+1)/2} \neq 5 \quad \text{et} \quad 2^p + 1 - 2^{(p+1)/2} \neq 5.$$

Or d'une part: $2^p + 1 + 2^{(p+1)/2} \geqslant 2^p \geqslant 128$,

et d'autre part: $2^p + 1 - 2^{(p+1)/2} = 2^{(p+1)/2}(2^{(p-1)/2} - 1) + 1 \geqslant 2^4(2^3 - 1) + 1 \geqslant 17$,

ce qui prouve bien que $n = \frac{4^p+1}{5}$ est composé.

On cherche donc à exprimer $n-1$ sous la forme $2^s t$ avec t impair. Pour cela, notons que $n - 1 = \frac{4^p-1}{5} = \frac{2^{2p}-1}{5} = 4.\frac{2^{2p-2}-1}{5}$. Introduisons $t = \frac{2^{2p-2}-1}{5} = \frac{4^{p-1}-1}{5}$, qui est un entier (on le déduit de l'application du théorème de Bézout car 4 et 5 sont premiers entre eux) et qui est impair (car si t était pair, $5t = 4^{p-1} - 1$ serait pair !). On conclut que $s = 2$.

On montre maintenant que $2^{2t} \equiv -1 \bmod n$, ce qui prouvera bien que $n \in \mathrm{ppf}(2)$. Pour cela, observons d'abord que 4 et p étant premiers entre eux, le petit théorème de Fermat implique $4^{p-1} \equiv 1 \bmod p$, donc $5t = 4^{p-1} - 1 \equiv 0 \bmod p$. Comme 5 est premier et que $p \geqslant 7$, il s'ensuit que $t \equiv 0 \bmod p$, ce que l'on écrit $t = kp$ avec k un entier impair (car t l'est). Dès lors, l'égalité $2^{2p} + 1 = 5n$ implique $2^{2p} \equiv -1 \bmod n$, qui devient $2^{2t} = 2^{2pk} \equiv (-1)^k \equiv -1 \bmod n$. □

COROLLAIRE. *L'ensemble* $\mathrm{ppf}(2)$ *est infini.*

COMMENTAIRES.

(i) Pour tout entier $\ell \geqslant 1$, notons N_ℓ le plus petit entier qui appartient à $\mathrm{ppf}(b)$ pour tout $b \in \{p_1, p_2, \ldots, p_\ell\}$, avec la notation usuelle $p_1 = 2$, $p_2 = 3$, ..., $p_\ell =$ le ℓ-ième nombre premier. Si n est un entier impair $< N_\ell$ qui est dans $\mathrm{ppf}(b)$ pour toutes ces bases b, alors n est un premier. On a: $N_1 = 2047$, $N_2 = 1\,373\,653$, $N_3 = 25\,326\,001$, $N_4 = 3\,215\,031\,751$.

(ii) On a vu qu'il existe des entiers qui appartiennent à $\mathrm{pp}(b)$ pour toute base b (ce sont les nombres de Carmichael), mais un tel phénomène de se produit pas sur les nombres pseudo-premiers forts car il a été démontré que, *pour tout entier composé impair* $\geqslant 15$, *le nombre de bases* b *dans* $\{1, 2, \ldots, n-1\}$ *pour lesquelles que* $n \in \mathrm{ppf}(b)$ *est majoré par* $\frac{n-1}{4}$.

3.3 D'autres familles de nombres liées aux nombres premiers

a) Nombres de Mersenne[24]. Le point de départ est la question de savoir si un entier de la forme $a^n - 1$ avec a, n des entiers $\geqslant 2$ est un nombre premier.
$\rightarrow$ Si a est un entier $\geqslant 3$, on a $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$. Comme $a - 1 \geqslant 2$, ceci prouve que $a^n - 1$ n'est pas premier.
$\rightarrow$ Si n n'est pas premier, il s'écrit $n = pq$ avec $p, q \geqslant 2$. On a:

$$2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \cdots 2^p + 1).$$

Donc $2^p - 1$ divise $2^n - 1$, ce qui (comme $2^p - 1 \geqslant 1$ puisque $p \geqslant 2$) montre que $2^n - 1$ non premier.

$\rightarrow$ Le problème de savoir si un entier de la forme $a^n - 1$ est premier ou non ne se pose donc que pour $a = 2$ et n est premier. D'où la définition suivante:

DÉFINITION. On appelle *nombre de Mersenne* tout entier de la forme $M_p := 2^p - 1$, où p est un nombre premier.

Les premiers nombres de Mersenne sont: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{11} = 2047 = 23 \times 89$, de sorte que M_2, M_3, M_5, M_7 sont premiers mais M_{11} ne l'est pas. La question de départ se reformule donc en: *quels sont les nombres de Mersenne qui sont premiers ?*

(i) La question de savoir si l'ensemble des nombres de Mersenne qui sont premiers est ou non fini est encore ouverte aujourd'hui.

(ii) On connaît actuellement 47 nombres de Mersenne qui sont premiers. Les 17 premiers sont les M_p pour $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281. Le plus grand est $M_{43112609}$, qui s'écrit avec 12978189 chiffres en base 10. Le plus récemment découvert est $M_{42643801}$, en avril 2009, qui s'écrit avec 12837064 chiffres en base 10.

b) Nombres d'Euclide et nombres parfaits.

DÉFINITION. On appelle *nombre d'Euclide* tout un entier de la forme $E_p := \frac{1}{2}M_p(M_p + 1) = 2^{p-1}M_p = 2^{p-1}(2^p - 1)$, où p est un nombre premier tel que M_p est premier.

$E_2 = 2 \times M_2 = 2 \times 3 = 6$,
$E_3 = 2^2 \times M_3 = 4 \times 7 = 28$,
$E_5 = 2^4 \times M_5 = 16 \times 31 = 496$,
$E_7 = 2^6 \times M_7 = 64 \times 127 = 8128$,
le suivant n'est pas E_{11} car on a vu que M_{11} n'est pas premier,
$E_{13} = 2^{12} \times M_{13} = 4094 \times 8191 = 33\,550\,556$.

Il est évident qu'il existe autant de nombres d'Euclide que de nombres de Mersenne premiers, ce qui ramène à la question ouverte précédente. Une propriété caractéristique des nombres d'Euclide est fournie par la proposition suivante, pour laquelle on rappelle d'abord une définition.

DÉFINITION. On appelle *nombre parfait* tout entier naturel $n \geqslant 2$ qui est égal à la somme de ses diviseurs stricts (ie. strictement inférieurs à n).

En rappelant la notation $\sigma_1(n)$ pour désigner la somme de tous les diviseurs de n (voir 1.2.e), dire que n est parfait signifie donc que $\sigma_1(n) = 2n$.

Exemples. 6 est parfait car $6 = 1 + 2 + 3$, et 28 est parfait car $28 = 1 + 2 + 4 + 7 + 14$.

$496 = 16 \times 31 = 2^4 \times 31$ est parfait car $1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496$.

$8128 = 64 \times 127 = 2^6 \times 127$ est parfait car $1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8128$.

[24] Marin Mersenne, 1588-1648, religieux français passé à la postérité comme érudit, mathématicien et philosophe.

PROPOSITION. *Les nombres parfait pairs sont exactement les nombres d'Euclide.*

Preuve. Soit n un nombre d'Euclide. Il existe donc p premier tel que $n = 2^{p-1}(2^p - 1)$ avec $2^p - 1$ premier.

Parce que 2 et $2^p - 1$ sont premiers et distincts, l'écriture $n = 2^{p-1}(2^p - 1)$ est la décomposition de n ets produit de facteurs premiers. Cela permet d'expliciter l'ensemble des diviseurs de n : $D_n = \{1, 2, 4, \ldots, 2^{p-2}, 2^{p-1}, (2^p - 1), 2(2^p - 1), 4(2^p - 1), \ldots, 2^{p-2}(2^p - 1), 2^{p-1}(2^p - 1)\}$, d'où:

$$\begin{aligned}\sigma_1(n) - n &= 1 + 2 + 4 + \cdots + 2^{p-2} + 2^{p-1} + (2^p - 1) + 2(2^p - 1) + 4(2^p - 1) + \cdots + 2^{p-2}(2^p - 1) \\ &= 1 + 2 + 4 + \cdots + 2^{p-2} + 2^{p-1} + (2^p - 1)(1 + 2 + 4 + \cdots + 2^{p-2} + 2^{p-2}) \\ &= \tfrac{2^p}{2-1} + (2^p - 1)\tfrac{2^{p-1}-1}{2-1} = (2^p - 1) + (2^p - 1)(2^{p-1} - 1) = (2^p - 1)2^{p-1} = n,\end{aligned}$$

ce qui prouve que n est parfait.

Réciproquement supposons que n est parfait et pair. Il s'écrit $n = 2^a b$ avec $a \geqslant 1$ et b impair. Tout diviseur de n est le produit d'un diviseur de b par 2^i avec $0 \leqslant i \leqslant a$. Il en résulte que:

$$\sigma_1(n) = \sigma_1(b) \times (1 + 2 + 2^2 + \cdots + 2^a) = \sigma_1(b)(2^{a+1} - 1).$$

Or par hypothèse, n est parfait, c'est-à-dire $\sigma_1(n) - n = n$, donc $\sigma_1(n) = 2n = 2^{a+1}b$. Ces deux expressions de $\sigma_1(n)$ conduisent donc à : $2^{a+1}b = \sigma_1(b)(2^{a+1} - 1)$. Comme 2^{a+1} est premier avec $2^{a+1} - 1$ (puisque il est impair), on en déduit avec le théorème de Gauss que $2^{a+1} - 1$ divise b. Il existe donc $c \in \mathbb{N}^*$ tel que: $b = (2^{a+1} - 1)c$, d'où: $\sigma_1(b) = 2^{a+1}c$. Montrons par l'absurde que $c = 1$. Supposons que $c \geqslant 2$. Alors l'ensemble des diviseur de b contiendrait au moins les trois éléments distincts $1, c, (2^{a+} - 1)c$, de sorte que l'on aurait $\sigma_1(b) \geqslant 1 + c + (2^{a+1} - 1)c > 2^{a+1}c = \sigma_1(b)$: contradiction.

Ainsi $c = 1$, donc $\sigma_1(b) = 2^{a+1}$ et $b = 2^{a+1} - 1$; ceci implique que b a pour seul diviseur lui-même et 1, c'est-à-dire que b est premier. Finalement, $n = 2^a(2^{a+1} - 1)$ avec $(2^{a+1} - 1)$ premier. D'après le début du a) ci-dessus, cela implique que $a+1$ est premier. Posons $p = a+1$; on conclut que $n = 2^{p-1}(2^p - 1)$ avec $2^p - 1$ premier, ce qui montre le résultat voulu. □

CONJECTURE. La question de savoir s'il existe ou non des nombres parfaits impairs reste encore ouverte aujourd'hui. Les spécialistes s'accordent à conjecturer qu'il n'en existe pas. Il a été prouvé très récemment qu'il n'existe pas de nombres parfait impairs inférieurs à 10^{1500}.

c) Nombres de Fermat. Le point de départ est l'observation que, si un entier de la forme $2^k + 1$ avec $k \geqslant 1$ est un nombre premier, alors k est une puissance de 2.

En effet, en notant $k = 2^s t$ avec $s \geqslant 0$ et t impair, et en posant $x = 2^{2^s}$, on a: $2^k + 1 = x^t + 1 = (1 + x)\sum_{i=0}^{t-1}(-1)^i x^i$. Donc $x + 1$ divise $2^k + 1$. Donc si $2^k + 1$ est premier, alors $x + 1 = 2^k + 1$, donc $x = 2^k$, donc $k = 2^s$. □

DÉFINITION. On appelle *nombre de Fermat* tout entier de la forme $F_n := 2^{(2^n)} + 1$, où n est un entier naturel.

- $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Ils sont tous premiers.
- Fermat pensait que tous les F_n étaient premiers. Ce n'est pas le cas, puisqu'Euler a montré que F_5 n'est pas premier.

  Montrons que F_5 n'est pas premier. On peut vérifier directement $F_5 = 2^{32} + 1 = 2^{16} \times 2^{16} + 1 = (2^8)^2 \times (2^8)^2 + 1 = 256^2 \times 256^2 + 1 = 65536 \times 65536 + 1 = 4\,294\,967\,297 \times 641$.

  On peut aussi (méthode plus élégante) partir de : $641 = 5.2^7 + 1$ et $641 = 2^4 + 5^4$,

  donc $5.2^7 \equiv -1 \bmod 641$ et $5^4 \equiv -2^4 \bmod 641$,

  donc $(5.2^7)^4 \equiv 1 \bmod 641$ et $5^4 \equiv -2^4 \bmod 641$,

  donc $5^4.2^{28} \equiv -1 \bmod 641$ et $5^4 \equiv -2^4 \bmod 641$.

  On déduit $-2^4.2^{28} \equiv -1 \bmod 641$, d'où $2^{32} + 1 \equiv 0 \bmod 641$, donc F_5 divisible par 641.

► On conjecture maintenant (toujours ouvert) qu'en fait F_n n'est premier pour aucun $n \geqslant 5$. Il a été prouvé que les nombres de Fermat F_n pour $5 \leqslant\leqslant 32$ sont tous composés ; F_{33} est le plus petit nombre de Fermat dont on ne sait pas actuellement s'il est premier ou composé. Le plus grand nombre de Fermat dont on sait qu'il est composé est $F_{2543548}$.

PROPOSITION (dit théorème de Goldbach[25]). *Si m et n sont deux entiers naturels distincts, alors les nombres de Fermat F_m et F_n sont premiers entre eux.*

Preuve. Soient n, m distincts dans $\mathbb{N}$. Quitte à échanger de m et n, on peut supposer que $m < n$. On note $m = n + k$, avec $k \geqslant 1$. On a $F_n = 2^{(2^n)} + 1$ et $F_m = F_{n+k} = 2^{(2^{n+k})} + 1$.

Posons $x = 2^{(2^n)}$ de sorte que $F_n = x + 1$ et $F_m = x^{(2^k)} + 1$. Donc $F_m - 2 = x^{(2^n)} - 1 = (x+1)(x^{2^n-1} - x^{2^n-2} + x^{2^n-3} - \cdots + x - 1)$. Ceci prouve que $F_m - 2$ est divisible par $x - 1$ qui n'est autre que F_n. Ainsi: F_n divise $F_m - 2$.

Dès lors, si q un diviseur commun positif de F_n et F_m, alors c'est un diviseur commun de $F_m - 2$ et de F_m, donc un diviseur de 2. Mais $q = 2$ est impossible car F_n et F_m sont impairs. Donc $q = 1$, ce qui prouve bien que F_m et F_n sont premiers entre eux. □

[25] Christian Goldbach, 1690-1764, mathématicien allemand, célèbre en particulier pour la conjecture portant son nom, affirmant que *tout nombre entier pair $\geqslant 4$ peut être écrit comme la somme de deux nombres premiers*, qui demeure l'une des questions ouvertes majeures en théorie des nombres.