ALGÈBRE ET ARITHMÉTIQUE 1

Cours de l'Université de Rennes 1 (2016–2017).
Url : `https://lectures.lionel.fourquaux.org/2016-2017/ar1/`

Ce texte est une version légèrement modifiée du poly 2009–2010 du module AR1, par David Bourqui, sur la base de textes antérieurs de Christophe Mourougane et Antoine Chambert-Loir. Que ces auteurs soient ici remerciés. *Septembre 2016*

ALGÈBRE ET ARITHMÉTIQUE 1

TABLE DES MATIÈRES

PARTIE I

LOGIQUE, THÉORIE DES ENSEMBLES, NOMBRES ENTIERS NATURELS

CHAPITRE 1

LOGIQUE ET THÉORIE DES ENSEMBLES

1.1. Un peu de logique

1.1.1. Formules logiques. — Les mathématiques sont construites à l'aide de concepts (les définitions qui seront données au fil de ce cours) et des propriétés qui découlent de ces concepts, énoncées sous formes de théorèmes, lemmes ou propositions. L'outil qui permet de bâtir cet enchaînement est le raisonnement logique. Sans entrer dans une présentation approfondie de la logique, le but de ce chapitre est de donner au lecteur les notions élémentaires nécessaires pour construire des raisonnements.

Considérons des assertions mathématiques comme « l'entier 4 est pair » (une assertion vraie) ou « $1 = 8$ » (une assertion fausse). Il est possible de les combiner entre elles à l'aide d'*opérateurs logiques*, comme « et », « ou », ou encore « est équivalent à », pour construire des phrases logiques plus élaborées. Quand celles-ci deviennent un peu compliquées, il est souvent pratique d'introduire des *formules logiques*, analogues aux formules numériques que l'on utilise pour décrire des calculs sur les nombres.

Pour cela, considérons des variables $\mathcal{P}$, $\mathcal{Q}$, ... pouvant ensuite être remplacées (*évaluées*) par des assertions vraies ou fausses.

On sera également amené à considérer des variables décrivant des assertions dépendant d'un paramètre, comme « l'entier n est pair » (ce que l'on pourrait noter $\mathcal{P}(n)$).

Ces variables forment des formules logiques élémentaires. À partir de là, on peut construire de nouvelles formules à l'aide d'opérateurs logiques qui combinent entre elles plusieurs sous-formules (de la même manière que l'on peut utiliser l'addition ou la multiplication pour combiner entre elles plusieurs formules numériques).

Pour décrire le comportement de ces opérateurs vis-à-vis de l'évaluation, on utilise des *tables de vérité*, qui donnent la valeur (vrai ou faux) de la formule en fonction des valeurs possibles des sous-formules après leur évaluation.

1.1.1.1. La *négation* de $\mathcal{P}$ est la formule « non $\mathcal{P}$ » définie par

$\mathcal{P}$	non $\mathcal{P}$
Vraie	Fausse
Fausse	Vraie

Ainsi, si l'on évalue la formule non $\mathcal{P}$ en remplaçant $\mathcal{P}$ par une assertion vraie, on obtient une assertion fausse, et si l'on remplace $\mathcal{P}$ par une assertion fausse, on trouve une assertion vraie. Par exemple, l'assertion « non(2 est un multiple de 3) » est vraie.

1.1.1.2. La *disjonction* de deux formules $\mathcal{P}$ et $\mathcal{Q}$ est la formule « $\mathcal{P}$ ou $\mathcal{Q}$ » définie par

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$ ou $\mathcal{Q}$
Vraie	Vraie	Vraie
Vraie	Fausse	Vraie
Fausse	Vraie	Vraie
Fausse	Fausse	Fausse

Il est à noter que le « ou » n'est pas exclusif : en mathématiques, lorsque l'on vous propose « fromage ou dessert », vous avez le droit de prendre les deux...

1.1.1.3. La *conjonction* de deux formules $\mathcal{P}$ et $\mathcal{Q}$ est la formule « $\mathcal{P}$ et $\mathcal{Q}$ » définie par

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$ et $\mathcal{Q}$
Vraie	Vraie	Vraie
Vraie	Fausse	Fausse
Fausse	Vraie	Fausse
Fausse	Fausse	Fausse

1.1.1.4. L'*implication* entre deux formules $\mathcal{P}$ et $\mathcal{Q}$ est la formule « $\mathcal{P} \Rightarrow \mathcal{Q}$ » définie par

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Rightarrow \mathcal{Q}$
Vraie	Vraie	Vraie
Vraie	Fausse	Fausse
Fausse	Vraie	Vraie
Fausse	Fausse	Vraie

L'implication « $\mathcal{P} \Rightarrow \mathcal{Q}$ » est toujours vraie sauf si l'hypothèse est vraie sans que la conclusion soit vraie. Soulignons qu'en écrivant $\mathcal{P} \Rightarrow \mathcal{Q}$, on n'affirme *strictement rien de plus* que le fait que *si* $\mathcal{P}$ est vraie alors $\mathcal{Q}$ l'est aussi. On ne dit *absolument rien* sur la véracité de $\mathcal{P}$ et/ou de $\mathcal{Q}$.

La formule « $\mathcal{Q} \Rightarrow \mathcal{P}$ » est appelée *implication réciproque* de l'implication $\mathcal{P} \Rightarrow \mathcal{Q}$.

La formule « non $\mathcal{Q} \Rightarrow$ non $\mathcal{P}$ » est appelée *implication contraposée* de l'implication $\mathcal{P} \Rightarrow \mathcal{Q}$.

Si l'implication $\mathcal{P} \Rightarrow \mathcal{Q}$ est vraie, pour deux assertions $\mathcal{P}$ et $\mathcal{Q}$, on dit que $\mathcal{P}$ est une *condition suffisante* pour $\mathcal{Q}$, et que $\mathcal{Q}$ est une *condition nécessaire* pour $\mathcal{P}$.

1.1.1.5. L'*équivalence* entre deux formules $\mathcal{P}$ et $\mathcal{Q}$ est la formule « $\mathcal{P} \iff \mathcal{Q}$ » définie par

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \iff \mathcal{Q}$
Vraie	Vraie	Vraie
Vraie	Fausse	Fausse
Fausse	Vraie	Fausse
Fausse	Fausse	Vraie

Si l'équivalence $\mathcal{P} \iff \mathcal{Q}$ est vraie, pour deux assertions $\mathcal{P}$ et $\mathcal{Q}$, on dit que $\mathcal{P}$ est une *condition nécessaire et suffisante* pour $\mathcal{Q}$.

1.1.2. Les priorités d'écriture. — Le « non » est prioritaire devant « et », « ou », « $\Rightarrow$ » et « $\iff$ ». Les écritures (non $\mathcal{P}$ et $\mathcal{Q}$) et (non $\mathcal{P}$) et $\mathcal{Q}$ sont donc équivalentes. Les opérateurs « et », « ou » sont prioritaires devant « $\Rightarrow$ » et « $\iff$ ».

Puisque nous parlons de règles d'écriture, c'est le moment de rappeler que le symbole « $\Rightarrow$ » est un symbole mathématique qui *en aucun cas* ne doit être utilisé dans une phrase comme abréviation pour le mot « donc » ou toute autre expression similaire. Il en est de même des symboles de quantification « $\forall$ » et « $\exists$ » décrits ci-dessous.

1.1.3. Quelques théorèmes de logique. —

Théorème. —

- Sur la négation : *non*$(\mathcal{P}$ *et* $\mathcal{Q})$ $\iff$ *non* $\mathcal{P}$ *ou non* $\mathcal{Q}$.
- Le tiers exclu : $\mathcal{P}$ *ou non* $\mathcal{P}$.
- La règle d'inférence : *Si on sait que $\mathcal{P}$ et $\mathcal{P} \Rightarrow \mathcal{Q}$ sont vraies, on en déduit que $\mathcal{Q}$ est vraie.*

$$(\mathcal{P} \textit{ et } (\mathcal{P} \Rightarrow \mathcal{Q})) \Rightarrow \mathcal{Q}.$$

- Le principe de contraposition :

$$(\mathcal{P} \Rightarrow \mathcal{Q}) \iff (\textit{non}\, \mathcal{Q} \Rightarrow \textit{non}\, \mathcal{P}).$$

- Le raisonnement par l'absurde :

$$(\mathcal{P} \Rightarrow \mathcal{Q}) \iff non(\mathcal{P}\ et\ non\ \mathcal{Q}).$$

- « Équivalence = double implication » :

$$(\mathcal{P} \iff \mathcal{Q}) \iff (\mathcal{P} \Rightarrow \mathcal{Q}\ et\ \mathcal{Q} \Rightarrow \mathcal{P}).$$

Démonstration. — On démontre ces théorèmes à l'aide de tables de vérité. Voici un exemple.

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Rightarrow \mathcal{Q}$	non Q	P et non Q	non(P et non Q)	non($\mathcal{P}$ et non $\mathcal{Q}$) $\iff$ ($\mathcal{P} \Rightarrow \mathcal{Q}$)
V	V	V	F	F	V	V
V	F	F	V	V	F	V
F	V	V	F	F	V	V
F	F	V	V	F	V	V

□

1.1.4. Formules quantifiées. — On considère souvent une famille $(P(x))_{x\in E}$ de formules logiques, autrement dit des formules $P(x)$ dépendant d'un paramètre x qui parcourt un ensemble E. Par exemple, la famille $(P(n))_{n\in\mathbf{N}} = (n$ est pair $)_{n\in\mathbf{N}}$ est une famille d'assertions indexée par $\mathbf{N}$. Ici, $P(2)$ est vraie alors que $P(3)$ est fausse.

On peut alors construire des *formules logiques avec quantificateurs* :

- quantification universelle : « $\forall x \in E, \quad P(x)$ », qui se lit « pour tout élément x de E, $P(x)$ est vrai » (ou « quel que soit x dans E, ... ») ;
- quantification existentielle : « $\exists x \in E, \quad P(x)$ », qui se lit « il existe un élément x de E tel que $P(x)$ est vrai ».

La formule « $\forall x \in E, \quad P(x)$ » est vraie si *toutes* les assertions $P(x)$ sont vraies, quel que soit l'élément x de E.

La formule « $\exists x \in E, \quad P(x)$ » est vraie si $P(x)$ est vrai pour *au moins un* élément x de E (il peut n'y en avoir qu'un seul !).

On peut voir ces formules comme les formes évaluées de « $\forall x, \ P(x)$ » et « $\exists x, \ P(x)$ », l'évaluation d'une telle formule correspondant à indiquer dans quel ensemble (ici, E) doit se trouver la variable quantifiée (ici, x). Il est cependant important de noter que seule une formule entièrement évaluée a une valeur de vérité (c'est-à-dire est vraie ou fausse), et donc que les assertions écrites sous forme de formule dans les démonstrations doivent systématiquement préciser l'ensemble d'appartenance pour les variables quantifiées.

Il est également à noter que la négation de la formule « $\forall x \in E, \quad P(x)$ » est la formule « $\exists x \in E, \quad \mathrm{non}\, P(x)$ ». Autrement dit, on a

$$\mathrm{non}\Big(\forall x \in E, \quad P(x)\Big) \iff \Big(\exists x \in E, \quad \mathrm{non}\, P(x)\Big).$$

1.1.5. Comment faire une démonstration ?— On utilise dans ce paragraphe les théorèmes de logique.

Par déductions élémentaires. — On utilise simplement la règle d'inférence.

Théorème. — $\forall n \in \mathbf{N}, 3$ *divise* $6n+18$

Démonstration. — Soit $n \in \mathbf{N}$, $6n = 3 \times 2n$. Donc, 3 divise $6n$. $18 = 3 \times 6$. Donc 3 divise 18. On sait que (a divise b et a divise c) implique (a divise $b+c$). Par conséquent, 3 divise $6n+18$. □

Par des tables de vérité. — Il s'agit de montrer que pour toutes les valeurs des assertions élémentaires qui apparaissent dans l'assertion à démontrer, celle-ci est vraie. Ce procédé systématique est surtout utilisé pour démontrer des théorèmes de logique.

Démontrer une implication. — Pour démontrer un théorème du type $\mathcal{P} \Rightarrow \mathcal{Q}$,

- on peut supposer $\mathcal{P}$ et chercher à démontrer $\mathcal{Q}$.
- on peut montrer l'assertion contraposée $\text{non}\,\mathcal{Q} \Rightarrow \text{non}\,\mathcal{P}$, c'est-à-dire supposer que $\mathcal{Q}$ est fausse et chercher à démontrer que $\mathcal{P}$ est fausse.
- on peut faire un raisonnement par l'absurde, c'est-à-dire supposer $\mathcal{P}$ et non $\mathcal{Q}$ et chercher une contradiction ($\mathcal{R}$ et non $\mathcal{R}$). En particulier, pour démontrer un théorème $\mathcal{Q}$, on peut chercher à montrer que l'hypothèse « non $\mathcal{Q}$ » mène à une absurdité.

Démontrer une équivalence. — Pour démontrer l'équivalence $\mathcal{P} \iff \mathcal{Q}$ il suffit de démontrer les deux implications $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\mathcal{Q} \Rightarrow \mathcal{P}$.

Démontrer une assertion universelle. —

- Pour montrer qu'une assertion universelle $(\forall x \in E, \quad P(x))$ est vraie, on considère un élément quelconque de E, on le note x, et on cherche à démontrer que $P(x)$ est vraie. Attention au sens de l'adjectif « quelconque ». Pour démontrer que $(\forall x \in \mathbf{N}, \quad P(x))$ est vraie, il ne suffit pas d'étudier $P(5)$.
- Pour montrer qu'une assertion universelle $(\forall x \in E, \quad P(x))$ est fausse, il suffit de trouver un élément x dans E pour lequel $P(x)$ est fausse (on dit que x est un contre-exemple). Démontrer que $P(6)$ est fausse suffit à démontrer que $(\forall x \in \mathbf{N}, \quad P(x))$ est fausse.

Par récurrence. — Pour démontrer une assertion universelle indexée par l'ensemble $\mathbf{N}$, on peut utiliser le raisonnement par récurrence. Ceci sera expliqué dans le chapitre suivant, consacré à l'ensemble des entiers naturels.

1.2. Un peu de théorie des ensembles

Il est hors de question dans ce cours de fonder rigoureusement la théorie des ensembles et nous nous contenterons des quelques définitions informelles qui suivent. En particulier, nous ne définirons pas la notion d'ensemble, même si nous décrirons la notion d'égalité d'ensembles.

1.2.1. Ensembles, éléments, appartenance, inclusion. — On écrit $x \in A$ et on prononce « x appartient à A » pour dire que x est un élément de l'ensemble A. Par définition, deux ensembles sont égaux s'ils ont les mêmes éléments ; en particulier, il n'y a dans un ensemble ni ordre ni répétition d'éléments :

$$\{2, 9, 3, 3\} = \{2, 3, 9\}.$$

L'ensemble vide, noté $\varnothing$ ou $\{\}$, n'a pas d'élément.

Des diagrammes (« patates ») sont utilisés pour représenter des ensembles ainsi que leurs éléments. Les éléments y figurent comme des points ou des petites croix, entourés par une courbe fermée qui forme lensemble. Dans le cas où lensemble contient un trop grand nombre déléments, seul lensemble est représenté, par la partie du plan intérieure à la courbe.

On dit que A est une partie de B, on écrit $A \subset B$ et on prononce « A est inclus dans B » pour dire que tout élément de A appartient à B ; en termes de logique,

$$A \subset B \iff (\forall x \in A, \quad x \in B).$$

On a donc $A \subset A$ (tout élément de A appartient à A) et $\varnothing \subset A$.

L'ensemble des parties d'un ensemble A est souvent noté $\mathcal{P}(A)$. C'est ce qui sera fait dans ce cours.

Une propriété fondamentale est

Proposition. — *Si $A \subset B$ et $B \subset A$, alors $A = B$.*

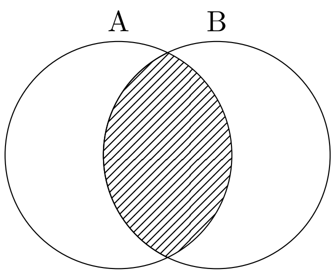
Démonstration. — Si $A \subset B$, les éléments de A sont dans B. Si de plus $B \subset A$, les éléments de B sont dans A. Si $A \subset B$ et $B \subset A$, les ensembles A et B ont les mêmes élements. Ils sont donc égaux, par la définition de l'égalité d'ensembles. □

Par exemple, pour résoudre l'équation $x^2 = 1$ dans $\mathbf{R}$, on peut d'abord montrer que toute solution est nécessairement dans $\{-1, 1\}$ et ensuite que -1 et 1 sont solutions. On aura ainsi montré que l'ensemble des solutions est l'ensemble $\{-1, 1\}$.

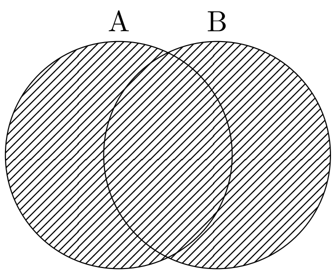
Proposition. — *Si $A \subset B$ et $B \subset C$, alors $A \subset C$.*

Démonstration. — La première inclusion dit que tout élément de A est un élément de B, l'autre que tout élément de B est un élément de C, si bien que les éléments de A sont des éléments de C. □

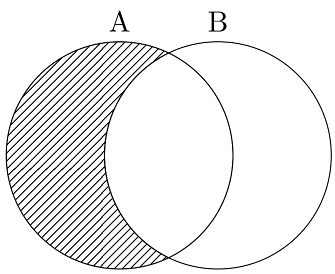
1.2.2. Opérations sur les ensembles. — La *réunion* de deux ensembles A et B est l'ensemble, noté $A \cup B$, (on prononce « A union B »), dont les éléments sont ceux qui appartiennent à A ou à B. L'*intersection* de deux ensembles A et B est l'ensemble formé des éléments qui appartiennent à la fois à A et à B ; on le note $A \cap B$ (« A inter B »). Ces définitions se généralisent sans peine à plus de deux ensembles. On dit que A et B sont disjoints si l'on a $A \cap B = \varnothing$, c'est-à-dire si A et B n'ont aucun élément en commun. Si, par exemple, $A = \{1, 2, 3\}$, $B = \{3, 4\}$ et $C = \{1, 4\}$, on a $A \cap B = \{3\}$, $A \cup B = A \cup C = \{1, 2, 3, 4\}$, $A \cap C = \{1\}$ et $A \cap B \cap C = \varnothing$. La *différence* de B dans A est l'ensemble, noté $A - B$ ou $A \setminus B$, des éléments de A qui ne sont pas dans B. Le *complémentaire* $\mathcal{C}_E A$ d'un sous-ensemble A d'un ensemble E est le sous-ensemble des éléments de E qui ne sont pas dans A. C'est $E \setminus A$, mais on n'utilise la notation $\mathcal{C}_E A$ que lorsque $A \subset E$.



$A \cap B$



$A \cup B$



$A \setminus B$

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

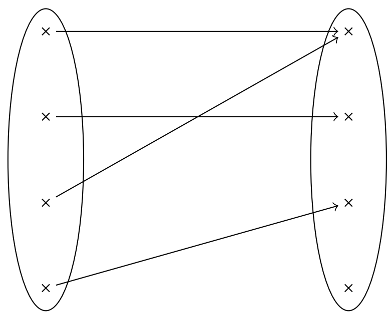
On note A^2 le produit cartésien $A \times A$, et plus généralement on note A^n l'ensemble des n-uplets d'éléments de A.

1.2.3. Applications. — Soit A et B des ensembles. Une *application* f de A dans B est la donnée, pour tout élément a de A, d'un élément de B qu'on note $f(a)$. On écrit

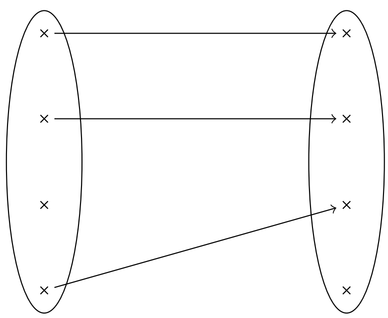
$$f\colon \begin{cases} A & \longrightarrow & B \\ a & \longmapsto & f(a). \end{cases}$$

On dit que A est l'*ensemble de départ de f* et que B est son *ensemble d'arrivée.* Si $b = f(a)$, on dit que b est l'*image* de a par f, et que a est un *antécédent* de b par f. Le *graphe de f* est l'ensemble des couples $(a, f(a))$, pour $a \in A$; c'est une partie de $A \times B$. Le diagramme du graphe fournit une représentation graphique de l'application.

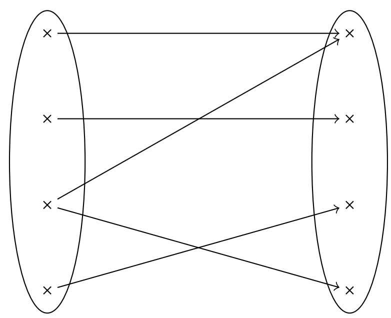
On note B^A l'ensemble des applications de A dans B.



Une application



Ceci n'est **pas** une application.



Ceci n'est **pas** une application.

Si A est un ensemble, il y a toujours au moins une application de A dans A : l'application *identité* de A, qui à tout $a \in A$ associe lui-même ; on la note Id_A :

$$\mathrm{Id}_A\colon \begin{cases} A & \longrightarrow & A \\ a & \longmapsto & a. \end{cases}$$

Si S est une partie de A, l'ensemble des $f(a)$ quand a parcourt S, est une partie de B qu'on appelle l'*image de S par f* et qu'on note $f(S)$.

$$f(S) := \{b \in B \mid \exists a \in S\ b = f(a)\}\,.$$

L'ensemble $f(A)$ est appelé l'image de l'application f. On le note aussi $\operatorname{im} f$.

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

$$f^{-1}(T) := \{a \in A \text{ tel que } f(a) \in T\}\,.$$

Soient $f\colon A \to B$ et $g\colon B \to C$ des applications. Noter qu'on suppose ici que l'ensemble d'arrivée de f coïncide avec l'ensemble de départ de g. On définit la *composée de f suivie de g* comme l'application $g \circ f\colon A \to C$ en posant $(g \circ f)(a) = g(f(a))$ pour tout $a \in A$.

Si $f\colon A \to B$ est une application, et si A' est une partie de A, la restriction de f à A', notée $f|_{A'}$, est l'application :

$$f|_{A'}\colon \begin{cases} A' & \longrightarrow & B \\ x & \longmapsto & f(x). \end{cases}$$

C'est une application de A' dans B. Son graphe est l'intersection du graphe de f avec $A' \times B$.

Si $f\colon A \to B$ est une application, et si B' est une partie de B *qui contient* $f(A)$, la corestriction de f à B', notée $f|^{B'}$, est l'application :

$$f|^{B'}\colon \begin{cases} A & \longrightarrow & B' \\ x & \longmapsto & f(x). \end{cases}$$

C'est une application de A dans B' qui a le même graphe que f.

1.2.4. Injectivité, surjectivité, bijectivité. —

Définition. — *Soit $f\colon A \to B$ une application. On dit que f est* injective *si des éléments de A distincts ont des images distinctes par f.*

$$f \text{ est injective} \iff \forall (x, x') \in A^2, \quad [x \neq x' \Rightarrow f(x) \neq f(x')] .$$

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

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

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

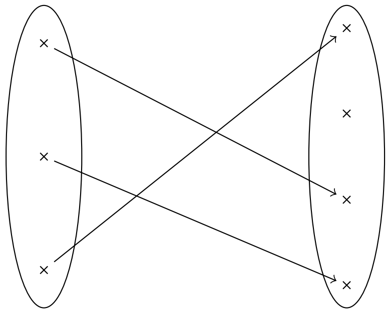
Exemples. L'application $f\colon \mathbf{N} \to \mathbf{N}$, $n \mapsto n^3 + n$ est injective. Démontrons ce fait. Soit n, $m \in \mathbf{N}$ tels que $f(n) = f(m)$; montrons que $n = m$. On a

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

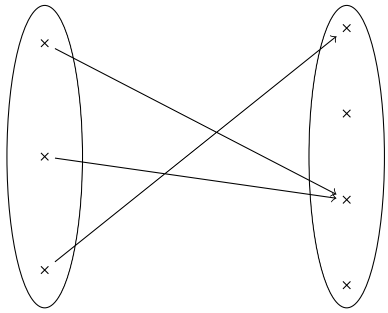
Comme $n^2 + nm + m^2 + 1 > 0$, on a $n = m$.

L'application $g\colon \mathbf{R} \to \mathbf{R}$, $x \mapsto x^2$ n'est pas injective car 1 et -1 ont même image par g ; autrement dit, $1 = 1^2 = (-1)^2$ a deux antécédents par g. Par contre, l'application $h\colon \mathbf{R}^+ \to \mathbf{R}$, $x \mapsto x^2$ est injective. En effet, soit y dans l'ensemble d'arrivée $\mathbf{R}$. Si y est strictement négatif, il n'a pas d'antécédent par h. Si y est positif, son seul antécédent par h est $\sqrt{y}$.

Si $f\colon A \to B$ est une application injective, les restrictions de f aux parties de A sont toutes injectives.



Une application injective



Une application non injective

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

$$f \textit{ est surjective} \iff \forall b \in B \quad \exists a \in A \textit{ tel que } b = f(a).$$

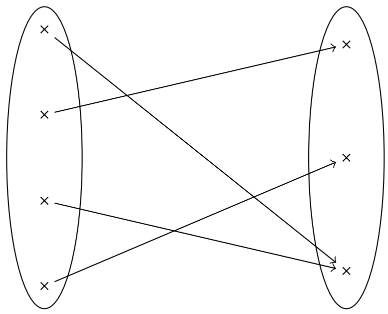
L'expression « au moins » est entre parenthèses, car par convention, il est toujours sous-entendu. Par exemple, un carré a un angle droit. Si on veut vraiment dire un unique, il faudra le préciser.

Exemples. L'application $f\colon \mathbf{R} \to \mathbf{R}$, $x \mapsto x^3$, est surjective, car tout nombre réel admet une racine cubique. Mais pas l'application $g\colon \mathbf{R} \to \mathbf{R}$, $x \mapsto x^2$. Par exemple -1 n'a pas d'antécédent par g.

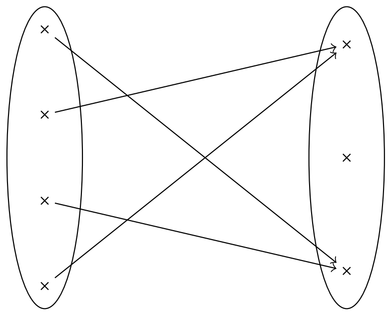
L'application $h\colon \mathbf{R} \to \mathbf{R}_+$, $x \mapsto x^2$ est surjective (tout nombre réel positif a une racine carrée).

Si $f\colon A \to B$ est une application, la corestriction de f à son image, c'est-à-dire $f|^{f(A)}$, est surjective.

Notons que la restriction d'une application surjective n'est pas forcément surjective.



Une application surjective



Une application non surjective

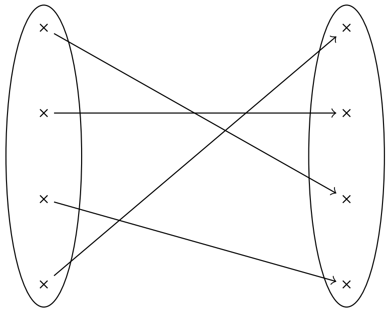
Définition. — *On dit qu'une application $f\colon A \to B$ est* bijective *si elle est à la fois injective et surjective.*

Cela revient à dire que tout élément de B a un antécédent et un seul par f. Si f est bijective, l'unique antécédent d'un élément $b \in B$ est noté $f^{-1}(b)$. Ceci construit la *bijection réciproque* f^{-1} de f. On a $f \circ f^{-1} = \mathrm{Id}_B$: pour tout $b \in B$, $f^{-1}(b)$ est un antécédent de b par f, donc $f(f^{-1}(b)) = b$. On a $f^{-1} \circ f = \mathrm{Id}_A$: pour tout $a \in A$, $f^{-1}(f(a))$ est l'unique antécédent de $f(a)$ par f ; comme a est un antécédent, on a $f^{-1}(f(a)) = a$. L'application f^{-1} est bijective. Si T est une partie de B, l'ensemble $f^{-1}(T)$, image réciproque de T par f, est aussi égal à l'image de T par f^{-1}. La notation est donc cohérente.

Exemples. Pour tout ensemble E, l'application identique Id_E, qui à tout élement x de E associe lui-même, est bijective.

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

Si $f\colon A \to B$ est une application injective, alors sa corestriction $f|^{f(A)}$ est une bijection de A sur $f(A)$.



Une application bijective

Proposition 1.2.1. — *Soit $f\colon A \to B$ et $g\colon B \to C$ des applications.*

1. *Si f et g sont injectives, $g \circ f$ est injective.*
2. *Si f et g sont surjectives, $g \circ f$ est surjective.*
3. *Si $g \circ f$ est injective, f est injective.*
4. *Si $g \circ f$ est surjective, g est surjective.*

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

Proposition 1.2.2. — *Soit $f\colon A \to B$ une application. Alors f est bijective si et seulement s'il existe une application $g\colon B \to A$ vérifiant $g \circ f = Id_A$ et $f \circ g = Id_B$.*

Démonstration. — La condition est nécessaire : si f est bijective, l'application $f^{-1}\colon B \to A$ vérifie ces propriétés.

La condition est suffisante : comme $g \circ f = \mathrm{Id}_A$ est injective, f est injective d'après la proposition précédente. Comme $f \circ g = \mathrm{Id}_B$ est surjective, f est surjective d'après la proposition précédente. L'application f étant injective et surjective est donc bijective. □

Remarquons que l'application g de l'énoncé est nécessairement unique si elle existe : on vérifie aussitôt que ce doit être alors l'application réciproque de f.

CHAPITRE 2

LES ENTIERS NATURELS

2.1. Les opérations élémentaires sur N

L'arithmétique est l'étude des propriétés des nombres entiers naturels ou relatifs. Notre but dans ce chapitre est de présenter les propriétés élémentaires des entiers et comment les manipuler.

On admet ici l'existence de l'ensemble $\mathbf{N} = \{0, 1, 2, \ldots\}$ des entiers naturels. Pour en savoir plus sur sa définition rigoureuse, on pourra consulter le chapitre sur les axiomes de Peano dans la partie « Pour aller plus loin ».

L'ensemble $\mathbf{N}$ est muni d'une opération appelée « addition », notée $+$, qui vérifie les propriétés suivantes.

Proposition. — *(i) L'entier naturel* 0 *est un* élément neutre *pour l'addition : si* a *est un entier naturel, on a* $a + 0 = 0 + a = a$.

(ii) L'addition est associative *: si* a, b, c *sont des entiers naturels, alors* $(a+b)+c = a+(b+c)$.

(iii) L'addition est commutative *: si* a *et* b *sont des entiers naturels, alors* $a + b = b + a$.

(iv) Si a *est un entier naturel, alors l'application* $\mathbf{N} \to \mathbf{N}, x \mapsto x + a$ *est injective, et* 0 *n'est dans son image que si* $a = 0$.

(v) Si a *et* b *sont deux entiers naturels, alors il existe un (unique) entier naturel* c *tel que* $a + c = b$ *ou* $b + c = a$.

Notons que 0 est alors l'unique élément neutre (car si $x \in \mathbf{N}$ est un élément neutre pour l'addition, alors on a $0+x = x+0 = 0$, et comme 0 est élément neutre on a aussi $x+0 = 0+x = x$, donc $x = 0$), et que l'application $\mathbf{N} \to \mathbf{N}, x \mapsto x + a$ est surjective si et seulement si $a = 0$ (auquel cas c'est l'identité).

L'ensemble $\mathbf{N}$ est également muni d'une opération appelée « multiplication », notée $\times$ ou $\cdot$ ou sans signe d'opération quand il n'y a pas d'ambiguïté, qui vérifie les propriétés suivantes.

Proposition. — *(i) Si* a *est un entier naturel, alors* $a \times 0 = 0 \times a = 0$.

(ii) L'entier naturel 1 *est un élément neutre pour la multiplication : si* a *est un entier naturel, on a* $a \times 1 = 1 \times a = a$.

(iii) La multiplication est associative : si a, b, c *sont des entiers naturels, alors* $(a \times b) \times c = a \times (b \times c)$.

(iv) La multiplication est distributive à gauche et à droite par rapport à l'addition : si a, b, c *sont des entiers naturels, alors* $a \times (b + c) = (a \times b) + (a \times c)$ *et* $(b + c) \times a = (b \times a) + (c \times a)$.

(v) La multiplication est commutative : si a *et* b *sont des entiers naturels, alors* $a \times b = b \times a$.

(vi) Si a *et* b *sont deux entiers naturels tels que* $a \times b = 0$, *alors* $a = 0$ *ou* $b = 0$.

(vii) Si a *et* b *sont deux entiers naturels tels que* $a \times b = 1$, *alors* $a = b = 1$.

2.2. Le principe de récurrence

Considérons une partie A de l'ensemble $\mathbf{N}$. Si :

- $0 \in A$;
- pour tout $x \in A$, on a $x + 1 \in A$;

alors $A = \mathbf{N}$. Cette propriété est appelée le *principe de récurrence*.

L'aspect remarquable du principe de récurrence est qu'il permet de démontrer une infinité de théorèmes en un temps fini. Si on doit par exemple démontrer qu'une certaine assertion $\mathcal{P}(n)$, qui dépend d'un entier naturel n, est vraie pour tout entier naturel, il suffit de procéder de la façon suivante :

Démonstration par récurrence. —

- initialisation *: on démontre l'assertion* $\mathcal{P}(0)$ *;*
- hérédité *: on considère un entier naturel n tel que l'assertion* $\mathcal{P}(n)$ *est vraie (*hypothèse de récurrence*) et on démontre que l'assertion* $\mathcal{P}(n+1)$ *est encore vraie.*

Le raisonnement par récurrence est une des façons de procéder ; il y en a d'autres.

Démontrons la validité de ce raisonnement. On montre que l'ensemble A des entiers naturels n pour lesquels l'assertion $\mathcal{P}(n)$ est vraie vérifie

- 0 appartient à A, puisque l'assertion $\mathcal{P}(0)$ est vraie ;
- Si n appartient à A, alors $\mathcal{P}(n)$ est vraie ; par hérédité $\mathcal{P}(n+1)$ aussi et donc $n+1$ appartient à A.

L'ensemble A est donc égal à $\mathbf{N}$ par le principe de récurrence. Les assertions $\mathcal{P}(n)$ sont donc vraies pour tous les entiers naturels n.

2.3. Quelques démonstrations par récurrence

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

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

Initialisation : cette formule est vraie pour $n=0$, car $1+\cdots+0=0=0(0+1)/2$; (elle l'est aussi pour $n=1$ car $1=1(1+1)/2$.)

Hérédité : Soit n un entier naturel tel que la formule $1+2+\cdots+n=n(n+1)/2$ soit vraie. Montrons qu'elle est encore vraie pour son successeur $n+1$. De fait, on a

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

ce qui est la formule au rang $n+1$.

Par récurrence, elle est donc vraie pour tout entier naturel n.

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

Initialisation : Pour $n=0$, cette formule qui s'écrit $1=\frac{a^1-1}{a-1}$ est donc vraie.

Hérédité : Soit n un entier naturel tel que la formule $1+a+\cdots+a^n = \dfrac{a^{n+1}-1}{a-1}$ soit vraie. On a alors

$$\begin{aligned}1+a+\cdots+a^{n+1} &= (1+\cdots+a^n)+a^{n+1}\\ &= \frac{a^{n+1}-1}{a-1}+a^{n+1}\\ &= \frac{(a^{n+1}-1)+a^{n+1}(a-1)}{a-1}\\ &= \frac{a^{n+1}-1}{a-1},\end{aligned}$$

ce qui montre qu'elle est vraie pour $n+1$.

Par récurrence, elle est vraie pour tout entier naturel n.

2.4. La relation d'ordre sur $\mathbf{N}$

2.4.1. Définitions. —

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

En particulier, comme pour tout entier naturel n, $n = 0 + n$, l'inégalité $0 \leq n$ est vraie pour tout entier naturel n : on dit que 0 est *le plus petit élément* de $\mathbf{N}$.

Proposition. — *La relation $\leq$ vérifie les trois propriétés suivantes*

1. *elle est* réflexive *: pour tout entier naturel m, on a $m \leq m$;*
2. *elle est* transitive *: si $m \leq n$ et $n \leq p$, alors $m \leq p$;*
3. *elle est* antisymétrique *: si $m \leq n$ et $n \leq m$, alors $m = n$.*

Démonstration. — 1. La première résulte de $m = m + 0$.

2. Supposons que m, n, p soient trois entiers naturels tels que $m \leq n$ et $n \leq p$; par hypothèse, il existe un entier naturel u tel que $n = m + u$ et un entier naturel v tel que $p = n + v$. Alors, par associativité, $p = m + (u + v)$, ce qui entraîne $m \leq p$.
3. Soit m et n deux entiers naturels tels que $m \leq n$ et $n \leq m$. Par définition de $\leq$, il existe deux entiers u et v tels que $n = m+u$ et $m = n+v$. Par suite $n = (n+v)+u = n+(v+u)$, par associativité. Par une des propriétés de l'addition, on en déduit que $v + u = 0$. Par une autre propriété de l'addition, on obtient finalement que u et v sont nuls. Donc, $m = n$.

□

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

4. deux entiers naturels m et n étant donnés, l'un des deux est inférieur ou égal à l'autre ;
5. soit m, n, p des entiers naturels ; si $m \leq n$, on a $m+p \leq n+p$; inversement, si $m+p \leq n+p$, alors $m \leq n$.
6. soit m, n, p des entiers naturels ; si $m \leq n$, alors $mp \leq np$; réciproquement, si $mp \leq np$ et que $p \neq 0$, alors $m \leq n$.

2.4.2. Éléments remarquables d'un ensemble ordonné. —

Définition. — *Soit E un ensemble. Une* relation d'ordre *$\preceq$ sur E est une assertion dépendant de deux éléments de E, que l'on note $x \preceq y$, pour $(x, y) \in E^2$, et qui est :*

- réflexive*, c'est-à-dire qu'elle vérifie*
$$\forall x \in E \qquad x \preceq x$$
- antisymétrique*, c'est-à-dire qu'elle vérifie*
$$\forall (x, y) \in E^2 \qquad x \preceq y \text{ et } y \preceq x \Rightarrow x = y$$
- transitive*, c'est-à-dire qu'elle vérifie*
$$\forall (x, y, z) \in E^3 \qquad x \preceq y \text{ et } y \preceq z \Rightarrow x \preceq z.$$

Par exemple, $\leq$ est une relation d'ordre sur $\mathbf{N}$.

Si A est un ensemble, $\subset$ est une relation d'ordre sur l'ensemble $\mathcal{P}(A)$ des parties de A.

Si quels que soient x et y dans E, on a $x \preceq y$ ou $y \preceq x$, on dit que l'ordre est *total*. Par exemple, $\leq$ est une relation d'ordre totale sur $\mathbf{N}$. En revanche, $\subset$ n'est en général pas une relation d'ordre totale sur $\mathcal{P}(A)$.

Définition. — *Soit E un ensemble muni d'une relation d'ordre $\preceq$. Soit A une partie de E et x un élément de E.*

- *On dit que x est* un majorant *de A si pour tout élément a de A, $a \preceq x$.*
- *On dit que x est* un plus grand élément *de A si x appartient à A et en est un majorant.*
- *On dit que x est* une borne supérieure *de A si x est un majorant de A et si pour tout majorant y de A on a $x \preceq y$.*
- *On dit que A est* majorée*, si elle admet un majorant.*

On peut bien sûr écrire des définitions analogues pour les minorants. Noter que par antisymétrie, un plus grand élément ou une borne supérieure, quand ils existent, sont uniques.

2.4.3. Retour sur le principe de récurrence. — Il y a plusieurs variantes du principe de récurrence qu'il est utile de connaître.

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

On peut se ramener au principe usuel en introduisant l'assertion $\mathcal{P}'(n)$ définie par $\mathcal{P}'(n) = \mathcal{P}(n + 10)$. Comme $\mathcal{P}'(0) = \mathcal{P}(0 + 10) = \mathcal{P}(10)$, cette assertion est vraie pour $n = 0$. Soit n un entier naturel tel que $\mathcal{P}'(n)$ soit vraie. Par définition, $\mathcal{P}(n+10)$ est vraie. L'assertion $\mathcal{P}'(n+1)$ est $\mathcal{P}((n+1)+10) = \mathcal{P}((n+10)+1)$. Comme $n + 10$ est plus grand que 10 et que $(n + 10) + 1$ est le successeur de $n + 10$, le point 2) permet d'affirmer que l'assertion $\mathcal{P}'(n + 1)$ est vraie.

Par récurrence, la propriété $\mathcal{P}'(n)$ est vraie pour tout n. Cela entraîne que $\mathcal{P}(n)$ est vraie pour tout $n \geq 10$.

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

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

Une autre variante du principe de récurrence s'énonce en termes de la relation d'ordre :

Proposition. — *Toute partie non vide de l'ensemble des entiers naturels possède un plus petit élément. En d'autres termes, pour toute partie non vide A de $\mathbf{N}$, il existe un entier naturel $a \in A$ tel que tout entier naturel $n \in A$ vérifie $n \geq a$.*

Démonstration. — Pour établir cette proposition, nous allons démontrer la propriété $\mathcal{P}(n)$ suivante : si A est une partie de $\mathbf{N}$ qui contient un élément inférieur ou égal à n, alors A possède un plus petit élément.

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

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

Inversement, on peut déduire le principe de récurrence de cette variante. Soit en effet A une partie de $\mathbf{N}$ qui contient 0 et qui, si elle contient un élément x, contient son successeur $x+1$. Montrons que $A = \mathbf{N}$. Soit B le complémentaire de A dans $\mathbf{N}$, c'est-à-dire l'ensemble des entiers naturels qui n'appartiennent pas à A. On veut montrer que B est vide. Raisonnons par l'absurde. Sinon, B possède un plus petit élément b. Comme $0 \in A$, $0 \notin B$, d'où $b \neq 0$. Par suite, b est le successeur d'un élément a de $\mathbf{N}$. Si $a \in A$, alors $b = a+1 \in A$, ce qui est faux ; mais si $a \in B$, on a l'inégalité $a < b$ qui contredit l'hypothèse que b est le plus petit élément de B.

On peut démontrer de façon analogue que

Proposition. — *Toute partie non vide et majorée de* $\mathbf{N}$ *admet un plus grand élément.*

2.4.4. Suites définies par récurrence. — Ce sont les suites (de nombres entiers naturels, réels, de points, de fonctions,...) dont chaque terme est défini en fonction du précédent, voire des deux précédents,...

Définition. — *Les suites* arithmétiques *sont définies par une relation de la forme :*

$$\forall n \in \mathbf{N}, u_{n+1} = u_n + a,$$

où a est un nombre (rationnel, réel, complexe...) appelé raison *de la suite. On démontre par récurrence que $u_n = u_0 + n\,a$ pour tout entier naturel n.*

De même, les suites géométriques *sont définies par une relation de la forme :*

$$\forall n \in \mathbf{N}, u_{n+1} = a\,u_n.$$

Le nombre a est appelé raison *de la suite, et l'on a $u_n = a^n u_0$ pour tout entier naturel n.*

On peut également s'intéresser aux suite *arithmético-géométriques*, définies par la relation de récurrence

$$\forall n \in \mathbf{N} \qquad u_{n+1} = au_n + b.$$

Si {a=1}, c'est une suite arithmétique.
Si $a \neq 1$, leur étude se ramène par translation à celle des suites géométriques. Plus précisément, il existe un nombre A tel que la suite $(u_n - A)$ soit géométrique de raison a. En effet, on a

$$\begin{aligned} u_{n+1} - A &= au_n + b - A \\ &= a(u_n - A) + aA + b - A \\ &= a(u_n - A) + (a-1)A + b, \end{aligned}$$

donc si $A = \frac{b}{1-a}$ on trouve $u_{n+1} - A = a(u_n - A)$ et la suite $(u_n - A)$ est géométrique. On en déduit

$$\begin{aligned} u_n &= A + a^n(u_0 - A) \\ &= a^n u_0 + \frac{1-a^n}{1-a} b. \end{aligned}$$

2.5. Un peu d'histoire

Kronecker [1] a dit un jour : « Le Bon Dieu a inventé les nombres entiers naturels, le reste est l'œuvre de l'homme ». [2] L'arithmétique a fasciné les humains probablement depuis la nuit des temps. On trouve en tout cas des textes d'arithmétique parmi les tout premiers textes écrits qui nous restent (la plus ancienne tablette dont on dispose est une reconnaissance de dettes).

Parmi les propriétés des nombres entiers naturels que nous allons étudier figurent des résultats très anciens : l'existence d'une infinité de nombres premiers est un théorème d'Euclide [3]. Certains problèmes remontent à Archimède [4] (les bœufs du soleil par exemple).

Pascal [5] avait déjà utilisé le principe de récurrence.

La nécessité d'une *définition* des nombres entiers naturels n'est apparue qu'au XIX$^{\text{e}}$ siècle qui fut un moment de bouleversement théorique en mathématique. C'est à ce moment que les mathématiciens commencèrent à ressentir fermement le besoin de définir plus précisément l'objet de leur science, faisant en particulier clairement la distinction entre axiomes, définitions, théorèmes,... Les mathématiciens durent aussi résoudre le problème de l'infini : qu'est-ce qu'un ensemble « infini » ? La possibilité d'appréhender mathématiquement l'infini fut d'ailleurs le sujet d'une controverse théologique — seul Dieu est infini. Pire, Cantor [6] découvrit qu'il existait des infinis plus grands que d'autres et, en un sens, l'ensemble des entiers naturels est le plus petit ensemble infini.

Ce n'est aussi qu'à la toute fin du XIX$^{\text{e}}$ siècle que Dedekind [7] puis, quelques années plus tard, Peano, énoncèrent des *axiomes* qui permettent de caractériser l'ensemble des nombres

---

1. Leopold Kronecker, mathématicien et logicien allemand (1823-1871).

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

3. Euclide, mathématicien grec (env. 325 av. J.-C.-env. 265 av. J.-C.), auteur principal d'un traité de mathématique, *Les Éléments*, dont l'influence jusqu'à nos jours sur le développement de la science en général et des mathématiques en particulier est considérée comme extrêmement importante (il est admis qu'il s'agit de l'ouvrage ayant connu le plus grand nombre d'éditions si l'on excepte la Bible). Le traité étudie des problèmes géométriques et arithmétiques. Du côté arithmétique, il contient de nombreux résultats qui seront étudiés dans ce cours : la division euclidienne, un algorithme de calcul de pgcd, baptisé depuis algorithme d'Euclide, la décomposition d'un entier en facteurs premiers, le fait que l'ensemble des nombres premiers est infini... La rationnalité de $\sqrt{2}$ y est également démontrée.

4. Archimède, mathématicien, physicien, ingénieur et astronome grec (287 av. J.-C.-212 av. J.-C.). Parmi ses abondantes contributions mathématiques, on peut citer le calcul de nombreux aires et volumes par une méthode dite d'exhaustion, consistant à subdiviser l'aire ou le volume considéré en une infinité d'aire ou de volumes dont le calcul est élémentaire. Cette méthode préfigure le calcul intégral, et d'après Archimède aurait été inventée par Eudoxe de Cnide

5. Blaise Pascal, mathématicien, physicien et philosophe français (1623 - 1662). Ses contributions mathématiques incluent notamment l'édification des fondements de la théorie des probabilités au cours d'une correspondance avec Pierre de Fermat. Nous verrons un peu plus loin le « triangle » qui porte son nom.

6. Georg Ferdinand Ludwig Philip Cantor, mathématicien allemand (1845-1918), fondateur de la théorie des ensembles.

7. Richard Dedekind, mathématicien allemand (1831-1916). Une grosse partie de ses travaux porte sur l'arithmétique. Il a montré en particulier comment l'utilisation de méthodes algébriques fournissait un outil puissant pour étudier des problèmes arithmétique. Il est ainsi l'un des fondateurs de ce qu'on appelle désormais la théorie algébrique des nombres.

entiers naturels. Du point de vue pratique, ces axiomes sont donc les « briques de base » que le mathématicien peut assembler pour démontrer une propriété liée aux nombres entiers naturels.

2.6. Ensembles finis, cardinal

Il serait dommage de consacrer un cours aux nombres entiers naturels sans passer un peu de temps à leur vocation première : *compter*, c'est-à-dire à dénombrer. Noter qu'ils servent aussi à ordonner, c'est-à-dire à numéroter. Dans de nombreuses formules, on aura besoin d'utiliser la fonction *factorielle* qui est définie comme suit. La factorielle d'un entier positif ou nul n est le produit de tous les entiers de 1 à n. On a $1! = 1$, $2! = 1 \times 2 = 2$, $3! = 1 \times 2 \times 3 = 6$, etc. Plus généralement,

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

On pose également [8] $0! = 1$. On rappelle que $n!$ se prononce *factorielle n*.

2.6.1. Définitions. — Si $n \geq 1$, notons F_n l'ensemble $\{1, \ldots, n\}$; on pose $F_0 = \varnothing$.

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

Démonstration. — Montrons ce lemme par récurrence sur n.
Initialisation : Pour $n = 0$, si $f : \varnothing \to F_m$ est une bijection, et si $m \geq 1$, on a $1 \in F_m$, mais 1 n'a pas d'antécédent dans $\varnothing$ (un antécédent serait un élément de l'ensemble vide). Cela montre que $m = 0$.
Hérédité : Soit n un entier naturel. Supposons le résultat vrai pour n et soit $f : F_{n+1} \to F_m$ une bijection. Posons $a = f(n+1)$ et définissons une application g de F_m sur lui-même en posant $g(x) = x$ pour $x < a$, $g(a) = m$, et $g(x) = x - 1$ pour $a + 1 \leq x \leq m$. Cette application est bijective, l'unique antécédent de x étant lui-même si $x < a$, $x + 1$ si $a \leq x \leq m - 1$, et a si $x = m$. L'application $h = g \circ f : F_{n+1} \to F_m$ est bijective et vérifie $h(n+1) = g(a) = m$. On en déduit que sa restriction à F_n définit une application bijective de F_n dans F_{m-1}. Par récurrence, $n = m - 1$, donc $n + 1 = m$, ce qu'il fallait démontrer. □

Définition. — *On dit qu'un ensemble A est* fini *s'il existe un entier $n \geq 0$ et une bijection de F_n sur A.*

Comme la composée de deux bijections en est une, il découle aussitôt de la définition que si A est un ensemble fini et que B est un ensemble en bijection avec A, alors B est fini.

De manière intuitive, un ensemble est fini si et seulement si on peut numéroter ses éléments, en partant de 1 et en s'arrêtant à un certain entier n.

Une remarque absolument cruciale est que cet entier n ne dépend que de A, et pas de la numérotation choisie : si $f : F_n \to A$ et $g : F_m \to A$ sont des bijections, $g^{-1} \circ f$ est une bijection de F_n sur F_m, donc $n = m$ d'après le lemme. Intuitivement, cela dit que si on numérote les éléments de A de deux façons différentes, on s'arrête en tout cas au même point.

Cet entier est appelé le *cardinal de A* ; on le note $\operatorname{card} A$ ou $|A|$. Le cardinal de l'ensemble vide est 0, celui d'un singleton 1, etc.

8. Le lecteur consciencieux se demandera certainement pourquoi attribuer la valeur 1 à $0!$. Voici un début de justification : on verra plus loin que $n!$ est égal au nombre de bijections d'un ensemble fini de cardinal n dans lui-même. Ainsi $0!$ représente le nombre de bijections de l'ensemble vide sur lui-même. Et même si le résultat pourra en surprendre certains, il est rigoureusement exact qu'il existe une et une seule bijection de l'ensemble vide sur lui-même, qui est en fait l'unique application de l'ensemble vide dans lui-même.

Deux ensembles finis qui sont en bijection ont même cardinal (et réciproquement). On dit alors qu'ils sont *équipotents*. Un ensemble qui n'est pas fini est dit *infini*.

Pour tout entier naturel n, l'ensemble F_n est fini par définition. On a en outre :

Proposition. — *Soit n un entier naturel. Alors toute partie de F_n est un ensemble fini.*

Démonstration. — Démontrons le par récurrence sur n. L'ensemble vide n'a qu'une partie, lui-même, qui est bien un ensemble fini. Supposons la propriété vraie pour un $n \in \mathbf{N}$. Soit A une partie de F_{n+1}. Si $A = F_{n+1}$, A est fini. Sinon il existe un élément b de F_{n+1} qui n'est pas dans A. Définissons une application $f : A \to F_n$ de la façon suivante : soit $a \in A$. Si on a $a < b$, on pose $f(a) = a$. Si on a $a > b$, on pose $f(a) = a - 1$. On vérifie que l'application f est bien définie et injective : elle induit donc une bijection de A sur une partie de F_n. Par hypothèse de récurrence, cette dernière partie est finie. Donc A est un ensemble fini. La propriété est donc vraie pour $n + 1$, ce qui clôt la démonstration. □

2.6.2. Dénombrement à l'aide de partitions. — Le principal moyen de dénombrer un ensemble est de le partager. La notion mathématique qui formalise ce partage est celle de partition.

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

Cela signifie que les parties $A_1, \dots, A_n$ sont deux à deux disjointes et que leur réunion est égale à A.

Proposition. — *Soit m un entier naturel. Soit X un ensemble et soit $(A_i)_{1 \leq i \leq m}$ une* partition *de X par m sous-ensembles finis. Alors, l'ensemble X est fini et*

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

La notation $\sum_{i=1}^{m} \operatorname{card} A_i$ indique $\operatorname{card} A_1 + \operatorname{card} A_2 + \cdots + \operatorname{card} A_m$. Pour compter les éléments de X, il suffit de compter les éléments de chaque paquet A_i et de sommer les entiers obtenus. La démonstration de cet énoncé se fait en construisant une bijection de $F_{\sum_{i=1}^{m} \operatorname{card} A_i}$ sur X à partir des m bijections données de $F_{\operatorname{card} A_i}$ sur A_i.

Cardinal d'un sous-ensemble. —

Proposition. — *Soit X un ensemble fini et A une partie de X. Alors A est fini et on a $\operatorname{card} A \leq \operatorname{card} X$; l'égalité entraîne que $A = X$.*

Démonstration. — Soit $n = \operatorname{card} X$ et $f : X \to F_n$ une bijection. Alors f induit une bijection de A sur une partie de F_n, donc sur un ensemble fini d'après la proposition ci-dessus. Ainsi A est fini.

Posons à présent $B = X \setminus A$ (c'est le complémentaire de A dans X, c'est-à-dire l'ensemble des éléments de X qui n'appartiennent pas à A). Par définition, A et B forment une partition de X. On a donc $\operatorname{card} X = \operatorname{card} A + \operatorname{card} B$, donc $\operatorname{card} A \leq \operatorname{card} X$. Si $\operatorname{card} A = \operatorname{card} X$, $\operatorname{card} B = 0$ donc $B = \varnothing$. □

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

Si tout élément de l'ensemble d'arrivée Y *a exactement* N *antécédents par* f*,* $\operatorname{card} X = N \operatorname{card} Y$*. Ce dernier énoncé est souvent appelé* principe des bergers. [9]

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

Démonstration. — Il suffit de remarquer que les sous-ensembles non-vides $(f^{-1}(\{y\}))_{y \in f(X)}$ forment une partition de l'ensemble de départ X. En effet, tout élément x de X appartient à exactement un de ces sous-ensembles, le sous-ensemble $f^{-1}(\{f(x)\})$. Donc, $\operatorname{card} X = \sum_{y \in f(X)} \operatorname{card} f^{-1}(\{y\})$. Comme ces sous-ensembles ont au moins un élément, on a $\operatorname{card} X \geq \operatorname{card} f(X)$. Si f est injective, ces sous-ensembles ont exactement un élément. Donc, $\operatorname{card} X = \sum_{y \in f(X)} 1 = \operatorname{card} f(X)$. Si f est surjective, $f(X) = Y$ et $\operatorname{card} X \geq \sum_{y \in f(X)} 1 = \operatorname{card} f(X) = \operatorname{card} Y$. Si tout élément de l'ensemble d'arrivée Y a exactement N antécédents par f, $\operatorname{card} X = \sum_{y \in f(X)} N = N \operatorname{card} Y$. □

Cardinal d'un produit cartésien. — Si X et Y sont deux ensembles finis, le cardinal de l'ensemble produit $X \times Y$ est égal à $\operatorname{card} X \times \operatorname{card} Y$. En effet, les parties $X \times \{y\}$ de $X \times Y$ forment une partition de $X \times Y$. Chacune de ces parties est en bijection avec X, donc est de cardinal $\operatorname{card} X$. Comme il y a $\operatorname{card} Y$ telles parties, on a $\operatorname{card}(X \times Y) = \operatorname{card} X \times \operatorname{card} Y$. On aurait aussi pu utiliser l'application $p : X \times Y \to X$, qui envoie tout couple sur sa première coordonnée. (On l'appelle première projection). Chaque élément de l'ensemble X a exactement $\operatorname{card} Y$ antécédents par p.

Cardinal d'une réunion. —

Principe d'inclusion-exclusion. — *Soit* X *un ensemble fini, soit* A *et* B *deux parties de* X*. Alors,*

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

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

Plus rigoureusement, $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ est une partition de $A \cup B$. Donc, $\operatorname{card}(A \cup B) = \operatorname{card}(A - B) + \operatorname{card}(B - A) + \operatorname{card}(A \cap B)$. De plus, $A = (A - B) \cup (A \cap B)$ est une partition de A. On en déduit que $\operatorname{card}(A - B) = \operatorname{card} A - \operatorname{card}(A \cap B)$. De même, $\operatorname{card}(B - A) = \operatorname{card} B - \operatorname{card}(A \cap B)$. On conclut en remplaçant ces deux dernières quantités dans la première égalité.

□

9. Il est généralement illustré par l'exemple suivant : pour compter les moutons d'un troupeau, il suffit de compter les pattes et de diviser par quatre. Le terme de « principe » se rapproche du langage courant et on lui préfère « proposition » ou « théorème ».

Cardinal de l'ensemble des fonctions de X dans Y. — Si X et Y sont deux ensembles finis, montrons que le cardinal de l'ensemble $\mathcal{F}(X,Y)$ des applications de X dans Y est égal à $(\operatorname{card} Y)^{\operatorname{card} X}$. Le plus simple est de le démontrer par récurrence [10] récurrence sur le cardinal de X.
Initialisation : si X est un singleton $\{a\}$, une application $X \to Y$ est déterminée par l'image de a. On a donc $\operatorname{card} \mathcal{F}(X,Y) = \operatorname{card} Y = (\operatorname{card} Y)^{\operatorname{card} X}$ dans ce cas.
Hérédité : Soit $n \in \mathbf{N}$. Supposons que cette formule soit vraie pour tout ensemble de cardinal strictement inférieur à n et montrons-la pour un ensemble X de cardinal n. On pose $X' = X \setminus \{a\}$, où a est un élément fixé de X. Pour se donner une application de X dans Y, il faut d'une part fixer l'image de a et d'autre part se donner une application de X' dans Y. Ces choix sont indépendants. Cela fait $(\operatorname{card} Y) \times (\operatorname{card} Y)^{n-1} = (\operatorname{card} Y)^n$ applications, d'où l'assertion voulue par récurrence sur n. Plus rigoureusement, définissons, si $y \in Y$, une partie $\mathcal{F}_y$ de $\mathcal{F}(X,Y)$ comme l'ensemble des $f : X \to Y$ tels que $f(a) = y$. Ces parties $\mathcal{F}_y$ forment une partition de $\mathcal{F}(X,Y)$; chacune est en bijection avec $\mathcal{F}(X',Y)$, donc de cardinal $(\operatorname{card} Y)^{\operatorname{card} X - 1}$. Comme il y a $(\operatorname{card} Y)$ parties, le cardinal de $\mathcal{F}(X,Y)$ vaut bien $(\operatorname{card} Y)^{\operatorname{card} X}$.

Principe des tiroirs. — Comme conséquence du calcul du cardinal d'une partition, on a le principe des tiroirs (utilisé pour la première fois par Dirichlet [11] au XIX$^{\text{e}}$ siècle) : « si une commode de trois tiroirs contient quatre paires de chaussettes, l'un des tiroirs en contient au moins deux. »

Principe des tiroirs. — *Soit X un ensemble fini et soit $(A_i)_{1\leq i\leq m}$ une partition de X. Si $\operatorname{card} X > m$, une des parties est de cardinal ≥ 2.*

Démonstration. — Montrons la contraposée. Si toutes les parties sont de cardinal inférieur à 1, on a $\operatorname{card} E = \sum_{i=1}^m \operatorname{card} A_i \leq \sum_{i=1}^m 1 \leq m$. ☐

2.6.3. Coefficients binômiaux. —

Cardinal de l'ensemble des parties d'un ensemble. — Soit X un ensemble fini, de cardinal n. Rappelons que l'on note ici $\mathcal{P}(X)$ l'ensemble des parties de X.

Par exemple, si X est l'ensemble $\{1,2,3\}$, l'ensemble de ses parties

$$\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, X\}$$

a huit éléments.

Proposition. — *Soit $n \in \mathbf{N}$. Si X est un ensemble de cardinal n, alors le cardinal de $\mathcal{P}(X)$ est 2^n.*

---

10. La récurrence ci-dessous démarre à $\operatorname{card}(X) = 1$, essentiellement pour des raisons psychologiques. Il n'y aurait aucun inconvénient d'ordre mathématique à la faire démarrer à $\operatorname{card}(X) = 0$. Il s'agit alors de remarquer que si X est vide, le nombre d'applications de X dans Y est toujours égal à 1 : il n'y a qu'une seule façon d'associer à tout élément de l'ensemble vide un et un seul élément de Y, elle consiste à ne… rien faire ! On notera quand même que pour la formule soit alors vraie même pour $Y = \varnothing$, il faut avoir convenu qu'on a $0^0 = 1$.

11. Johann Peter Gustav Lejeune Dirichlet, mathématicien allemand (1805-1859). Il a apporté d'importantes contributions dans la théorie des séries de Fourier et en arithmétique, notamment dans la résolution du célèbre problème de Fermat (cette résolution n'a d'ailleurs été achevée entièrement qu'en 1994 par le mathématicien anglais Andrew Wiles). On doit à Dirichlet le théorème remarquable suivant : soit a et b des entiers premiers entre eux, et soit (u_n) la suite arithmétique de premier terme a et de raison b. Alors une infinité de termes de la suite (u_n) sont des nombres premiers.

Démonstration. — Donnons d'abord une démonstration « intuitive ». Supposons que $X = \{1, \dots, n\}$. Pour construire une partie A de X, on peut décider si $1 \in A$ ou pas, d'où deux choix. Puis deux nouveaux choix (indépendants du résultat du choix précédent) pour décider si $2 \in A$ ou pas, et ainsi de suite.

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

Démontrons à présent la proposition par récurrence sur n.
Initialisation : l'ensemble vide n'a qu'une partie, lui-même. (Si $n = 1$ et si E est un ensemble à un élément, $E = \{a\}$. Par conséquent, E a deux parties , $\varnothing$ et $\{a\}$.)
Hérédité : soit n un entier naturel. Supposons (hypothèse de récurrence) que tout ensemble à n éléments a exactement 2^n parties. Soir X un ensemble à $n + 1$ éléments. Soit a un élément fixé de X et posons $Y = X \setminus \{a\}$, de sorte que $\operatorname{card} Y = n$. Par hypothèse de récurrence, l'ensemble Y possède 2^n parties. Parmi les parties de X, certaines contiennent a et d'autres non. Une partie A de X qui contient a est de la forme $\{a\} \cup B$, où $B = A \setminus \{a\}$ est une partie de Y ; il y a 2^n parties B de Y, d'où 2^n parties de X qui contiennent a. Une partie A de X qui ne contient pas a est une partie de Y ; il y en a donc 2^n. Finalement, l'ensemble X possède exactement $2^n + 2^n = 2^{n+1}$ parties. $\square$

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

Définition. — *Si $n = \operatorname{card} X$, le cardinal de $\mathcal{P}_p(X)$ est noté $\binom{n}{p}$ (ou C_n^p dans certains livres). On l'appelle le nombre de* combinaisons *(sans répétition) de p éléments parmi n.*

Noter que ces nombres ne dépendent pas de l'ensemble X choisi parmi les ensembles à n éléments. (Ceci se démontre en utilisant une bijection entre F_n et X.) On a ainsi $\binom{n}{p} = 0$ si $p < 0$ ou $p > n$ et $\binom{n}{0} = \binom{n}{n} = 1$. En dénombrant les complémentaires, on trouve que, pour tout couple d'entiers (n, p),

$$\binom{n}{p} = \binom{n}{n-p}.$$

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

Tout arrangement définit une combinaison (on oublie la numérotation) et le nombre d'arrangements qui définissent une combinaison donnée est précisément égal au nombre de numérotations possibles d'un ensemble à p éléments. Autrement dit, on considère l'application qui va de l'ensemble des arrangements à p éléments de F_n dans l'ensemble des parties à p éléments de F_n qui à $(e_1, e_2, \cdots e_p)$ associe $\{e_1, e_2, \cdots e_p\}$. Chaque élément $\{a_1, a_2, \cdots a_p\}$ de l'ensemble d'arrivée a autant d'antécédents qu'il y a d'arrangements de $\{a_1, a_2, \cdots a_p\}$, soit A_p^p. On trouve donc

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

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

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

En particulier,

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

d'où l'on déduit

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}, \qquad \text{pour tout } 0 \leq p \leq n.$$

Proposition 2.6.1. — *Soit p un entier naturel non nul*(12)*. Le nombre de bijections d'un ensemble à p éléments dans lui même (on dit aussi de permutations d'un ensemble à p éléments) est $p!$.*

Démonstration. — Soit E un ensemble à p éléments. Toute permutation de E est par définition injective. Réciproquement, soit f une application injective de E dans lui-même. Son image $f(E)$ est dans E. Comme f est injective, $\operatorname{card} f(E) = \operatorname{card} E$. Donc $f(E) = E$ et par conséquent f est bijective. Ainsi, il y a autant de permutations de E que d'applications injectives de E dans lui-même, c'est-à-dire $\mathrm{A}_p^p = p!$. □

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

$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}, \qquad \text{pour tout } 0 \leq p \leq n-1.$$

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

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

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

12. L'hypothèse de non nullité n'est là que pour des raisons psychologiques ; le résultat est vrai également pour $p = 0$, comme on l'a déjà expliqué

Formule du binôme de Newton. — [13] *Si a et b sont deux nombres réels et $n \geq 0$, on a*

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

Pour cette raison, les coefficients $\binom{n}{p}$ sont appelés *coefficients binomiaux*. On prendra comme convention [14] $0^0 = 1$.

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

On peut aussi le démontrer par récurrence :
Initialisation : la formule est vraie pour $n = 0$ car $(a+b)^0 = 1$ et $\binom{0}{0} a^0 b^0 = 1$. (Elle est vraie pour $n = 1$ car elle s'écrit alors $(a+b)^1 = a+b$).
Hérédité : supposons-la vraie pour un entier naturel n. Alors,

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

La formule est ainsi vraie pour tout entier n. □

13. Établie par Isaac Newton, mathématicien, physicien, philosophe et astronome anglais (1643-1727). L'une de ses découvertes les plus célèbres est sans doute la loi universelle de la gravitation. En mathématiques, il a fondé, avec Leibniz, le calcul infinitésimal.

14. Une autre justification de cette convention est expliquée dans l'une des notes de bas de page précédentes.

PARTIE II

ARITHMÉTIQUE

CHAPITRE 3

LA DIVISION EUCLIDIENNE

3.1. Construction des entiers relatifs

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

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

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

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

La meilleure méthode revient à introduire formellement « toutes » les soustractions $a-b$ et à identifier celles qui doivent donner les mêmes résultats, les mêmes différences. Ce procédé d'identification nécessite un peu de terminologie algébrique.

3.1.1. Relations d'équivalence. —

Définition. — *Le* graphe d'une relation $\mathcal{R}$ *sur un ensemble* E *est une partie* R *du produit cartésien* $E\times E$ *(aussi noté* E^2*). On définit alors une relation* $\mathcal{R}$ *associée en décrétant que l'assertion* $x\mathcal{R}y$ *est vraie si et seulement si le couple* (x,y) *appartient au graphe* R.

L'égalité dans E est une relation dont le graphe est la diagonale de $E\times E$.

Comme exemple concret de relations, prenons pour E l'ensemble des êtres vivants et pour relation $\mathcal{R}$ l'une des suivantes : « est né avant », « parle la même langue que », « n'est pas de la même nationalité que ».

Définition. — *La relation* $\mathcal{R}$ *sur un ensemble* E

1. *est dite* réflexive *si pour tout élément* x *de* E*, on a* $x\mathcal{R}x$ *;*
2. *est dite* symétrique *si pour tout élément* (x,y) *de* E^2 *tel que* $x\mathcal{R}y$*, on a* $y\mathcal{R}x$.
3. *est dite* anti-symétrique *si pour tout élément* (x,y) *de* E^2 *tel que* $x\mathcal{R}y$ *et* $y\mathcal{R}x$*, on a* $x=y$.
4. *est dite* transitive *si pour tout élément* (x,y,z) *de* E^3 *tel que* $x\mathcal{R}y$ *et* $y\mathcal{R}z$*, on a* $x\mathcal{R}z$ *;*
5. *Une relation réflexive, symétrique et transitive est appelée* relation d'équivalence.
6. *Une relation réflexive, anti-symétrique et transitive est appelée* relation d'ordre.

Les relations « est né avant » et « parle la même langue que » sont réflexives, mais pas la relation « n'est pas de la même nationalité que ». Les relations « parle la même langue que » et « n'est pas de la même nationalité que » sont symétriques, mais pas la relation « est né avant ». La relation « est né avant » est transitive, mais pas la relation « n'est pas de la même nationalité que ». La relation « parle la même langue que » est transitive si l'on suppose qu'un individu ne parle qu'une langue, mais pas sinon (si Alice parle anglais et français, Bernard anglais et allemand, Charles allemand, Alice et Bernard sont en relation, de même que Bernard et Charles, mais pas Alice et Charles). Dans l'ensemble des êtres humains vivants, la relation « est de la même nationalité que » est donc une relation d'équivalence (on exclut de cette discussion les problèmes liés à la double nationalité ou aux apatrides).

L'équivalence est une relation d'équivalence sur « l'ensemble » des assertions. L'inclusion est une relation d'ordre sur les « ensembles ». L'équipotence est une relation d'ordre sur « les ensembles ». (Pour avoir un énoncé rigoureux et retirer les guillemets, on peut restreindre les relations aux sous-ensembles d'un ensemble fixé.) Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, on peut d'une certaine manière « identifier » tous les éléments qui sont en relation : au moins de ce point de vue, ils sont équivalents. On appelle ainsi *classe d'équivalence d'un élément* x l'ensemble de tous les éléments de E qui sont équivalents à x. Notons $Cl(x)$ la classe d'équivalence de x ; c'est une partie de E.

$$Cl(x) := \{y \in E \text{ tels que } x\mathcal{R}y\}.$$

Pour la relation « est de la même nationalité que », la classe d'équivalence d'un individu est l'ensemble de ceux qui ont la même nationalité que lui. Les classes d'équivalences sont donc les ensembles des Français, des Allemands, des Polonais, etc.

Proposition 3.1.1. — *Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, deux classes d'équivalence sont ou bien disjointes ou bien égales. Ainsi, à condition de ne pas répéter deux fois une même classe, les classes d'équivalence des éléments de E définissent une partition de E.*

En particulier, les assertions $Cl(x) = Cl(y)$ et $x\mathcal{R}y$ sont équivalentes.

Démonstration. — Soit x et y des éléments de E dont les classes d'équivalence ont un élément commun, disons z. Par hypothèse, $x\mathcal{R}z$ et $y\mathcal{R}z$; comme la relation est symétrique, on a $z\mathcal{R}y$; comme elle est transitive, on a $x\mathcal{R}y$. Soit alors a un élément quelconque de $Cl(x)$; On a $x\mathcal{R}a$, d'où $y\mathcal{R}a$ par symétrie et transitivité, si bien que $a \in C(y)$. Cela démontre que $Cl(x) \subset Cl(y)$ et l'on démontre de même l'autre inclusion, si bien que $Cl(x) = Cl(y)$. □

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

Définition. — *Par définition, l'ensemble quotient de E par la relation d'équivalence $\mathcal{R}$ est l'ensemble de toutes les classes d'équivalence.*

C'est un ensemble dont les éléments sont des parties non vides de S, les classes d'équivalence. On le note souvent $E/\mathcal{R}$. Le passage à la classe d'équivalence définit une application Cl

$$\begin{array}{rccc} Cl : & E & \to & E/\mathcal{R} \\ & x & \mapsto & Cl(x) \end{array}$$

Cette application Cl est surjective.

Définition. — *Une application $f : E \to F$ entre deux ensembles E muni d'une relation $\mathcal{R}$ et F muni d'une relation $\mathcal{S}$ est dite* compatible aux relations *si*

$$\forall (x, x') \in E^2, x\mathcal{R}y \Rightarrow f(x)\mathcal{S}f(y).$$

Si les relations $\mathcal{R}$ et $\mathcal{S}$ sont des relations d'ordre, on parle d'application croissante. Si la relation $\mathcal{R}$ est une relation d'équivalence et $\mathcal{S}$ est la relation d'égalité, tous les éléments d'une même classe d'équivalence pour $\mathcal{R}$ ont la même image par une application compatible f. On dit alors que f est bien définie sur l'ensemble quotient $E/\mathcal{R}$.

C'est une démarche générale en mathématique de définir la notion de compatibilité des applications à chaque fois qu'on définit une nouvelle structure sur les ensembles. Par exemple, pour les ensembles munis de distances, on devra définir la notion d'isométrie.

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

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

Démonstration. — En effet, pour tout couple (a,b), $a+b=b+a$ et donc $(a,b)\mathcal{R}(a,b)$ (Réflexivité) Si un couple (a,b) est équivalent à un couple (c,d) (i.e. $a+d=b+c$), alors (c,d) est équivalent à (a,b) (i.e. $c+b=d+a$) (Symétrie). Si (a,b) est équivalent à (c,d) et (c,d) est équivalent à (e,f), alors (a,b) est équivalent à (e,f). En effet, si les deux premières assertions sont vérifiées, on a $a+d=b+c$ et $c+f=d+e$; alors, $a+c+f=a+d+e=b+c+e$, d'où $a+f=b+e$ en simplifiant par c, donc (a,b) est équivalent à (e,f) (Transitivité). □

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

Remarquons que l'application de $\mathbf{N}$ dans $\mathbf{Z}$ définie par $a\mapsto a-0$ est injective : si $a-0=b-0$, $a+0=0+b$, donc $a=b$. On peut donc identifier $\mathbf{N}$ à une partie de $\mathbf{Z}$. On prolonge alors l'addition des entiers naturels aux entiers relatifs par la formule : $(a-b)+(c-d)=(a+c)-(b+d)$. Comme les éléments de $\mathbf{Z}$ sont des parties de S, il faut vérifier une compatibilité ; c'est-à-dire que si les couples (a,b) et (a',b') sont dans la même classe d'équivalence, ainsi que (c,d) et (c',d'), alors la classe obtenue par $(a+c)-(b+d)$ et celle obtenue par $(a'+c')-(b'+d')$ coïncident. Par hypothèse, on a en effet $a+b'=a'+b$ et $c+d'=c'+d$, d'où

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

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

Proposition. — *L'addition dans $\mathbf{Z}$ vérifie les propriétés suivantes :*

- *il y a un élément neutre $0-0$, de sorte que $(a-b)+(0-0)=(0-0)+(a-b)=(a-b)$ pour tout entier relatif $a-b$;*
- *l'addition est associative : pour tous entiers relatifs $a-b$, $c-d$, $e-f$, $((a-b)+(c-d))+(e-f)=(a-b)+((c-d)+(e-f))$;*
- *l'addition est commutative : pour tous entiers relatifs $a-b$, $c-d$, $(a-b)+(c-d)=(c-d)+(a-b)$;*
- *tout élément $a-b$ a un opposé, $b-a$, tel que $(a-b)+(b-a)=(a+b)-(a+b)=(0,0)$.*

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

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

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

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

On peut aussi prolonger la relation d'ordre de **N** à **Z**, par

$$\forall (a, b, a', b') \in E^4, \quad a - b \leq a' - b' \iff a + b' \leq a' + b.$$

Elle reste un ordre total. Toute partie de **Z** non vide et minorée admet un plus petit élément. Toute partie de **Z** non vide et majorée admet un plus grand élément. Les compatibilités entre la relation d'ordre et l'addition restent formellement les mêmes que sur **N**. Mais la multiplication par un entier relatif négatif (i.e. inférieur à 0) n'est pas compatible avec la relation d'ordre (i.e. change le sens des inégalités).

3.2. Le théorème de la division euclidienne

Comme conséquence du fait que toute partie non-vide de **N** admet un plus petit élément, on obtient l'existence de la division euclidienne dans **Z**.

Théorème de la division euclidienne. — *Soit a et d deux entiers relatifs, avec $d \neq 0$. Il existe des entiers relatifs q et r, uniques, tels que $a = d\,q + r$ et $0 \leq r \leq |d| - 1$.*

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

Démonstration. — Soit R l'ensemble des entiers $r \in \mathbf{N}$ tels qu'il existe $q \in \mathbf{Z}$ avec $a = dq + r$. L'ensemble R n'est pas vide. En effet, si $a \geq 0$, la relation $a = d \cdot 0 + a$ montre que $a \in R$. Si $a \leq 0$, soit $\varepsilon \in \{-1, 1\}$ le signe de d ; on a la relation $a = \varepsilon d \cdot a + (1 - \varepsilon d)a$ dans laquelle $(1 - \varepsilon d)a \geq 0$ (car $\varepsilon d \geq 1$ et $a \leq 0$) ; par suite, $a(1 - \varepsilon d)$ appartient à R. Comme toute partie non vide de **N** admet un plus petit élément, on peut considérer r le plus petit élément de R. Soit $q \in \mathbf{Z}$ tel que $a = dq + r$. Par hypothèse, $r \geq 0$. Supposons par l'absurde que $r \geq |d|$. Notons encore ε le signe de d. On a donc $|d| = \varepsilon d$ d'où $r \geq \varepsilon d$. La relation $a = dq + r = d(q + \varepsilon) + (r - |d|)$ implique ainsi que $r - |d| \in R$, ce qui contredit la minimalité de r.

Pour montrer l'unicité, supposons qu'il existe deux couples (q, r) et (q', r') solutions. Alors $r - r' = d(q' - q)$. Or $-|d| < r - r' < |d|$. Comme d est non nul, on en déduit que l'entier $q' - q$ vérifie l'encadrement $-1 < q' - q < 1$. Donc, $q = q'$ et par suite $r = r'$. $\square$

3.3. Numération

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

Proposition. — *Soit b un entier supérieur ou égal à 2. Pour tout entier naturel n, il existe un entier $k \geq 0$ et des entiers $c_0, \dots, c_k \in \{0, \dots, b-1\}$ tels que l'on ait*

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

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

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

Démonstration. — On démontre l'existence par récurrence sur n. Pour $n = 0$, on peut écrire $n = 0$, avec $k = 0$ et $c_0 = 0$. Supposons qu'on puisse écrire de la sorte tout entier strictement inférieur à n. Soit alors q et r le quotient et le reste de la division euclidienne de n par b. On a bien $0 \leq r \leq b-1$. Comme $bq = n - r$ et $b \geq 2$, on a $q < n$. Par hypothèse de récurrence, l'entier q s'écrit sous la forme $d_m b^m + d_{m-1} b^{m-1} + \cdots + d_0$, où les d_i sont des entiers compris entre 0 et $b-1$, avec $m = 0$ si $q = 0$, et $c_m \neq 0$ si $q \neq 0$. Posons alors $c_0 = r$, $k = m+1$, et $c_i = d_{i-1}$ si $1 \leq i \leq m+1$. On a

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

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

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

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

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

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

Ce sont deux écritures en base b de l'entier q. Par hypothèse de récurrence, elles coïncident. Donc, $k - 1 = m - 1$, d'où $k = m$, et $c_i = d_i$ pour $1 \leq i \leq k$. □

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

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

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

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

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

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

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

Cela revient à écrire

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

méthode parfois appelée de Horner [1].

3.3.2. Addition et multiplication en base b. — Dans toutes les bases, la multiplication est une addition répétée. Formellement, ces opérations sont identiques à celles effectuées en base décimale. Le point important est de prendre garde aux retenues. Par exemple, en base 2, $1 + 1 = 10$ (On pose 0 et on retient 1) et en base hexadécimale $A + B = 15$ (On pose 5 et on retient 1). En guise d'exemple, vérifions qu'en base 5, on a $342 \times 43 = 32411$.

$$\begin{array}{cccccc} & & & 3 & 4 & 2 \\ \times & & & & 4 & 3 \\ \hline & & 2 & 1 & 3 & 1 \\ & 3 & 0 & 2 & 3 & \\ \hline & 3 & 2 & 4 & 1 & 1 \end{array}$$

3.4. Divisibilité, congruence

3.4.1. Divisibilité. —

Définition. — *On dit qu'un entier relatif d divise un entier relatif a s'il existe $q \in \mathbf{Z}$ tel que $a = dq$. On dit aussi que a est multiple de d et on note $d|a$.*

Quelques propriétés simples de la divisibilité :

Proposition. — *1. L'entier 0 ne divise que lui-même. Mais tout entier le divise.*

2. *Si d divise a, alors d divise au pour tout entier u. Si d divise a et b, alors d divise $a + b$ Plus généralement, si d divise a et b, alors d divise $au + bv$ pour tout couple (u, v) d'entiers relatifs.*
3. *Si a divise b et b divise c, alors a divise c. (Transitivité)*
4. *Si d divise a et $a \neq 0$, alors $|d| \leq |a|$.*
5. *Si a divise b et b divise a, on a $a = b$ ou $a = -b$.*
6. *Si d divise a et $n \in \mathbf{Z}$, alors nd divise na. Inversement, si $n \neq 0$ et si nd divise na, alors d divise a.*

Démonstration. — 1. résulte de $0 \times q = 0$ et $0 = d \times 0$.

2. Écrivons en effet $a = da'$ et $b = db'$, où $a' \in \mathbf{Z}$ et $b' \in \mathbf{Z}$. Alors, $au + bv = da'u + db'v = d(a'u + b'v)$; comme $a'u + b'v \in \mathbf{Z}$, d divise $au + bv$.
3. En effet, il existe $d \in \mathbf{Z}$ tel que $b = ad$ et $e \in \mathbf{Z}$ tel que $c = eb$. Alors, $c = e(ad) = a(ed)$; puisque $ed \in \mathbf{Z}$, a divise c.

1. William George Horner, mathématicien britannique (1786 - 1837). La méthode qui porte son nom était toutefois connue antérieurement.

4. Si $a = da'$ avec $a' \in \mathbf{Z}$, on a $a' \neq 0$ car $a \neq 0$, d'où $|a|' \geq 1$ et finalement $|a| = |d|\,|a|' \geq |d|$.
5. Si l'un des deux est nul, ils le sont tous deux et la propriété est vraie. S'ils sont tous deux non nuls, on a simultanément $|a| \leq |b|$ et $|b| \leq |a|$ d'où l'égalité $|a| = |b|$ et finalement $a = \pm b$.
6. Si l'on a $a = da'$ avec $a' \in \mathbf{Z}$, on a $na = nda'$, donc nd divise na. Dans l'autre sens, on peut supposer que n est strictement positif. Soit $a = dq + r$ la division euclidienne de a par d, avec $0 \leq r \leq |d| - 1$. On a $na = ndq + nr$. De plus, $0 \leq nr \leq n(|d| - 1) \leq n\,|d| - 1$. Par conséquent, nr est le reste de la division euclidienne de na par nd, supposé nul. On en déduit que r est nul, c'est-à-dire que d divise a.

□

3.4.2. Relation de congruence. —

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

Comme conséquence des propriétés simples de la divisibilité, on montre que c'est une relation d'équivalence sur $\mathbf{Z}$:

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

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

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

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

La relation de congruence est compatible avec l'addition et la multiplication. Plus précisément,

Proposition. — *Soit a, b, a', b' des entiers relatifs tels que $a \equiv b \pmod{m}$ et $a' \equiv b' \pmod{m}$.*

1. *pour tout entier $n \in \mathbf{Z}$, $na \equiv nb \pmod{nm}$ et par conséquent $na \equiv nb \pmod{m}$.*
2. *$a + a' \equiv b + b' \pmod{m}$.*
3. *$aa' \equiv bb' \pmod{m}$.*

Démonstration. — Par exemple, la troisième propriété résulte du fait que

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

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

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

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

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

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

$$n \equiv c_k + \dots + c_0 \pmod 9 :$$

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

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

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

3.5. Plus grand diviseur commun, algorithme d'Euclide

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

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

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

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

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

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

Pour démontrer cet algorithme, on utilise le lemme

Lemme. — *Si $a = bq + r$ est la division euclidienne de a par b alors* $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r)$.

Démonstration. — En effet si d divise a et b, il divise b et $r = a - bq$, et s'il divise b et r, il divise aussi $a = bq + r$ et b. Par suite, (a, b) et (b, r) ont les mêmes diviseurs, donc le même pgcd. □

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

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

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

$$\begin{aligned}
598 &= 1 \times 598 + 0 \times 414 & & \\
414 &= 0 \times 598 + 1 \times 414 & & \\
184 &= 598 - 414 = 1 \times 598 - 1 \times 414 & & q = 1 \\
46 &= 414 - 2 \times 184 = -2 \times 598 + 3 \times 414 & & q = 2.
\end{aligned}$$

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

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

Algorithme d'Euclide (étendu). — *Soit a et b deux entiers strictement positifs. On définit des suites (d_n), (u_n) et (v_n) par récurrence en posant*

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

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

$$d_{n+1} = d_{n-1} - q_{n+1} d_n \qquad u_{n+1} = u_{n-1} - q_{n+1} u_n \qquad v_{n+1} = v_{n-1} - q_{n+1} v_n.$$

Si $d_{n+1} = 0$, on a $d_n = \operatorname{pgcd}(a, b) = u_n a + v_n b$.

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

On va montrer par récurrence sur n que l'on a $d_n = au_n + bv_n$. C'est vrai pour $n = 0$ car $a = d_0 = a \times 1 + b \times 0 = au_0 + bv_0$; c'est aussi vrai pour $n = 1$ puisque $d_1 = b = a \times 0 + b \times 1$.

Supposons que ce soit vrai pour tout entier compris entre 0 et n et montrons que c'est vrai pour $n+1$. On a en effet, si q est le quotient de la division euclidienne de d_{n-1} par d_n,

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

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

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

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

Théorème de Bézout. — [2] *Soit a et b deux entiers relatifs. Alors, il existe des entiers relatifs u et v tels que* $\operatorname{pgcd}(a,b) = au + bv$.

(Le cas où a et b sont nuls est évident.)

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

Corollaire. — *Soit a, b et n trois entiers relatifs. L'entier n est un diviseur commun de a et b si et seulement si n est un diviseur de* $\operatorname{pgcd}(a,b)$.

Ou encore : *pour qu'un entier relatif divise deux entiers relatifs, il faut et il suffit qu'il divise leur pgcd.*

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

Par récurrence, on peut alors déterminer des entiers $u_1, \dots, u_n$ tels que $\operatorname{pgcd}(a_1, \dots, a_n) = a_1u_1 + \cdots + a_nu_n$. Faisons-le sur un exemple, disons $\operatorname{pgcd}(15, 10, 6)$. L'algorithme d'Euclide étendu appliqué au couple $(10, 6)$ s'écrit comme suit :

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

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

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

2. Étienne BÉZOUT, mathématicien français (1730-1783). La paternité de ce théorème doit semble-t-il être attribuée en fait à Claude Gaspard BACHET DE MÉZIRIAC. Il est d'ailleurs parfois baptisé théorème de Bachet-Bézout. BÉZOUT fut par contre le premier à montrer l'analogue de ce résultat pour les polynômes.

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

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

Voici une autre application importante :

Théorème de Gauss. — [3] *Soit a, b, c des entiers non nuls. Alors :*

1. *si a divise bc et si a est premier avec b, alors a divise c ;*
2. *si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.*

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

1. Supposons que a divise bc. L'entier a divise auc et bvc, donc leur somme qui est égale à c.
2. Soit x et y des entiers tels que $c = ax$ et $c = by$. On a $c = uac + vbc = uaby + vbax = ab(uy + vx)$, ce qui démontre que c est multiple de ab.

□

Une variante du second point est la propriété suivante

Proposition. — *Soit a un entier. Si n et m sont deux entiers premiers entre eux,*

$$\begin{cases} x \equiv a \pmod m \\ x \equiv a \pmod n \end{cases} \iff x \equiv a \pmod{mn}$$

3.6. Plus petit multiple commun

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

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

Calculons maintenant $\text{ppcm}(a, b)$ dans le cas général.

Lemme. — *Si $d = \text{pgcd}(a, b)$, on peut écrire $a = da'$ et $b = db'$; alors a' et b' sont premiers entre eux.*

Démonstration. — si $u > 1$ divise a' et b', on écrit $a' = ua''$, $b' = ub''$ et l'on a $a = (du)a''$, $b = (du)b''$, ce qui montre que du divise a et b, alors que $du > d$. □

Si m est multiple de a et de b, il est multiple de d ; écrivons donc $m = dm'$. Par hypothèse dm' est multiple de da' ; on en déduit, comme d n'est pas nul que m' est multiple de a'. De même, m' est multiple de b'. Par suite, m' est multiple de $a'b'$, car a' et b' sont premiers entre eux, donc m est multiple de $da'b'$ et en particulier, $m \geq da'b'$. Inversement, l'entier $da'b'$ vérifie

3. Johann Carl Friedrich Gauss, mathématicien, astronome et physicien allemand (1777–1855). Surnommé le « prince des mathématiques », il est universellement reconnu comme un des plus grands mathématiciens de tous les temps. Son ouvrage *Disquisitiones Arithmeticae* est considéré comme l'un des plus importants et influents traités d'arithmétique.

$da'b' = ab' = a'b$, donc est multiple à la fois de a et de b. Nous avons donc démontré que $\operatorname{ppcm}(a, b) = da'b'$. Remarquons que l'on a la formule

$$\operatorname{ppcm}(a, b) \operatorname{pgcd}(a, b) = d^2 a'b' = ab.$$

Notons aussi que la démonstration précédente prouve en fait qu'un multiple commun de a et b est non seulement plus grand que $\operatorname{ppcm}(a, b)$, mais aussi un multiple de $\operatorname{ppcm}(a, b)$.

Corollaire. — *Soit a, b et n trois entiers relatifs. L'entier n est un multiple commun de a et b si et seulement si n est un multiple de* $\operatorname{ppcm}(a, b)$.

Ceci démontre la

Proposition. — *Soit a un entier. Si n et m sont deux entiers naturels,*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv a \pmod{n} \end{cases} \iff x \equiv a \pmod{\operatorname{ppcm}(m, n)}.$$

Plus généralement, un entier est multiple commun des entiers non nuls $a_1, \dots, a_n$ si et seulement si c'est un multiple de leur plus petit multiple commun $\operatorname{ppcm}(a_1, \dots, a_n)$. Cela permet de déterminer le ppcm par récurrence ; par exemple, la relation $\operatorname{ppcm}(6, 10) = 30$ provient de la formule pour le ppcm de deux entiers et de ce que le pgcd de 6 et 10 est égal à 2. Ensuite

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

CHAPITRE 4

LES NOMBRES PREMIERS

4.1. Nombres premiers, crible d'Ératosthène

Définition. — *Un* nombre premier *est un entier naturel supérieur ou égal à* 2 *qui n'admet que deux diviseurs entiers naturels* 1 *et lui-même. Un entier qui n'est pas premier est dit* composé.

(On prendra garde à ne pas confondre cette notion avec la propriété que deux entiers sont premiers entre eux.)

Pour déterminer les entiers jusqu'à une certaine borne qui sont des nombres premiers, ÉRATOSTHÈNE [1] a inventé le procédé suivant, qu'on appelle *crible*.

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

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

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

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

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

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

Ensuite, il y a 5, d'où

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

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

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

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

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

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

4.2. Factorisation

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

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

1. ÉRATOSTHÈNE, astronome, géographe, philosophe et mathématicien grec (env. 276 av. J.-C.-env. 194 av. J.-C.). Il est connu notamment pour avoir déterminé, par une méthode géométrique, une estimation extrêmement précise de la longueur de la circonférence terrestre.

Lemme. — *Un nombre premier p qui ne divise pas un entier a est premier avec a.*

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

D'après le théorème de Gauss, on en déduit le

Lemme d'Euclide. — *Soit p un nombre premier et soit a, b deux entiers. Si p divise le produit ab et si p ne divise pas a, p divise b.*

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

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

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

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

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

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

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

Soit n un entier relatif. L'exposant du nombre premier p dans la décomposition en facteurs premiers de n est appelé *valuation p-adique de n* et est noté $v_p(n)$.

$$v_p(n) = \max\{v / p^v \text{ divise } n\}.$$

Cet exposant est nul si et seulement si p ne divise pas n. On peut alors écrire la formule précédente sous la forme

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

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

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

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

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

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

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

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

4.3. Petit théorème de Fermat

L'énoncé. — Voici la première propriété importante des nombres premiers.

Petit théorème de Fermat. — [2] *Soit p un nombre premier. Pour tout entier $n \in \mathbf{Z}$, on a $n^p \equiv n \pmod p$. Si de plus n n'est pas multiple de p, on a $n^{p-1} \equiv 1 \pmod p$.*

Démonstration. — Si k est un entier tel que $1 \leq k \leq p-1$, on a $k\binom{p}{k} = p\binom{p-1}{k-1}$. Donc, p divise $k\binom{p}{k}$. Mais p premier ne divise pas k. Par le lemme d'Euclide, p divise $\binom{p}{k}$.

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

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

On utilise ici la congruence pour $1 \leq k \leq p-1$, $\binom{p}{k} \equiv 0 \pmod p$. La propriété est donc vraie pour $n+1$. Par récurrence, elle est donc vraie pour tout entier naturel. Comme $(-n)^p \equiv -n^p \pmod p$ (c'est même vrai sans congruence si p est impair), le résultat s'en déduit pour tout entier négatif.

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

2. Pierre de Fermat, juriste et mathématicien français (env. 1605–1665). Le *grand théorème de Fermat* est le résultat suivant : si $n \geq 3$ est un entier et si x, y et z sont des entiers relatifs vérifiant la relation $x^n + y^n + z^n = 0$ alors x, y ou z est nul. Dans une note écrite dans la marge d'une page d'un ouvrage d'arithmétique, Fermat affirmait posséder une démonstration remarquable de ce fait, démonstration que la marge était malheureusement trop étroite pour contenir. La recherche d'une telle démonstration a mobilisé pendant plusieurs siècles un nombre incalculable de mathématiciens tant amateurs que professionnels. Il a fallu attendre 1994 et les travaux du mathématicien anglais Andrew Wiles pour avoir une démonstration complète (des cas particuliers du théorème avaient été démontrés auparavant). Les techniques utilisées par Wiles sont tout sauf élémentaires, et la majorité des outils mathématiques qu'il emploie ont été inventés au xxème siècle et n'étaient donc pas connus de Fermat. Il est généralement admis que la démonstration évoquée par Fermat devait être fausse.

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

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

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

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

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

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

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

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

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

Si l'on fixe la base, on ne peut pas espérer trop ; par exemple, $2^{340} \equiv 1 \pmod{341}$ (*le vérifier...*), alors que $341 = 31 \times 11$ n'est pas premier. On dira qu'un nombre entier p est pseudo-premier s'il est premier en toute base n qui est première à p. Les nombres premiers sont pseudo-premiers : c'est précisément ce qu'affirme le petit théorème de Fermat. Les nombres entiers qui sont pseudo-premiers sans être premiers sont appelés *nombres de Carmichael*[3]. Il en existe ; le plus petit d'entre eux est $561 = 3 \times 11 \times 17$. ALFORD[4], GRANVILLE[5] et POMERANCE[6] ont démontré en 1994 qu'il y a une infinité de nombres de Carmichael.

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

4.4. Combien y a-t-il de nombres premiers ?

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

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

---

3. Robert Daniel CARMICHAEL, mathématicien américain (1879–1967). Il a beaucoup étudié les nombres qui portent son nom.
4. William Robert ALFORD, mathématicien américain (1937–2003), spécialiste de théorie des nombres.
5. Andrew GRANVILLE, mathématicien anglais né en 1962, spécialiste de théorie des nombres.
6. Carl POMERANCE, mathématicien américain né en 1944, spécialiste de théorie des nombres.

On note alors, au moins depuis RIEMANN [7] (1859), $\pi(x)$ le nombre des nombres premiers inférieurs ou égaux à x. Le théorème d'Euclide affirme que $\lim_{x\to\infty} \pi(x) = +\infty$.

GAUSS avait conjecturé à la fin du XVIII$^{\text{e}}$ siècle, et HADAMARD [8] et DE LA VALLÉE-POUSSIN [9] ont démontré (simultanément et indépendamment) en 1896 le *théorème des nombres premiers*, à savoir que l'on a

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

Jusqu'aux années 1960 et la preuve d'ERDÖS [10] et SELBERG [11], les démonstrations de ce théorème utilisaient toutes des méthodes assez sophistiquées de la théorie des fonctions d'une variable complexe.

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

Depuis un article génial de RIEMANN (1859), on sait que la répartition des nombres premiers est liée à une fonction d'une variable complexe, appelée *fonction zêta de Riemann*, et précisément aux zéros de cette fonction. Ainsi, *l'hypothèse de Riemann*, toujours non démontrée à ce jour malgré la prime de 1 000 000 \$ qui lui est attachée par le milliardaire américain CLAY [12], équivaut à ce que pour tout $\alpha > 1/2$, on ait

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

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

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

---

7. Bernhard RIEMANN, mathématicien allemand (1826–1866). Il a notamment apporté d'importantes contribution à l'analyse et à la géométrie complexe, introduisant les surfaces qui portent désormais son nom. À l'instar de DIRICHLET, il a développé l'utilisation de méthodes d'analyse complexe pour étudier des problèmes d'arithmétique, en particulier la répartition des nombres premiers au moyen de ce qu'on appelle désormais la fonction zêta de Riemann.

8. Jacques HADAMARD, mathématicien français (1865–1963). Vous rencontrerez sans doute au cours de vos études l'inégalité qui porte son nom : dans le cas particulier de la dimension 3, elle affirme que le volume d'un parallélépipède est majoré par le produit des longueurs de ses côtés, avec égalité si et seulement si le parallélépipède est rectangle.

9. Charles-Jean DE LA VALLÉE-POUSSIN, mathématicien belge (1866–1963).

10. Paul ERDÖS, mathématicien hongrois (1913–1996), célèbre pour sa productivité mathématique impressionnante (il a signé, la plupart du temps en collaboration avec d'autres auteurs, plus de 1500 articles de recherche qui couvrent de nombreux domaines des mathématiques) et son excentrisme.

11. Atle SELBERG, mathématicien norvégien (1917–2007). Spécialiste de théorie analytique des nombres, il est l'un des récipiendaires de la médaille Fields (considérée comme la plus prestigieuse des distinctions attribuées à un mathématicien), qu'il reçut en 1950.

12. `http://www.claymath.org/millennium/`

CHAPITRE 5

CONGRUENCES

5.1. Équations (du premier degré) aux congruences

Dans ce paragraphe, il s'agit d'expliquer la résolution de l'équation $ax \equiv b \pmod{n}$, où a, b et n sont des entiers relatifs fixés.

5.1.1. Premières remarques, réduction au cas $pgcd(a, n) = 1$**.** — Si $a = 0$, l'équation est $b \equiv 0 \pmod{n}$. Tout entier est solution si b est multiple de n, et il n'y a pas de solution sinon. Nous supposons dans la suite que $a \neq 0$.

Par définition des congruences, on cherche donc à déterminer les entiers x tel que $ax - b$ soit multiple de n, c'est-à-dire s'écrive yn, avec $y \in \mathbf{Z}$. Cette relation peut s'écrire $b = ax - ny$. Posons $d = \operatorname{pgcd}(a, n)$. Comme d divise a et n, la somme d'un multiple de a et d'un multiple de n est un multiple de d. Une condition nécessaire pour qu'il existe des solutions est donc que b soit multiple de d : il n'y a pas de solution si b n'est pas un multiple de d.

Supposons donc que b soit multiple de d. Posons $A = a/d$, $B = b/d$, $N = n/d$ (comme $a \neq 0$, $d \neq 0$) ; ce sont des entiers. On a les équivalences

$$\begin{aligned} ax \equiv b \pmod{n} &\iff \exists k \in \mathbf{Z} \quad ax - b = kn \\ &\iff \exists k \in \mathbf{Z} \quad Ax - B = kN \\ &\iff Ax \equiv B \pmod{N} \end{aligned}$$

dans laquelle A et N sont des entiers *premiers entre eux.*

5.1.2. Inverse modulo n**.** —

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

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

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

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

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

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

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

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

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

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

Si b est multiple de d, écrivons $b = db'$. L'équation équivaut à $x \equiv b'u \pmod{n'}$, les solutions étant donc les entiers x de la forme $b'u + kn'$ avec $k \in \mathbf{Z}$.

5.2. Théorème chinois, système de congruences

On trouve dans un traité chinois (III–V[e] siècle ap. J.-C.) l'énoncé suivant :

Nous avons des choses dont nous ne connaissons pas le nombre ;
- si nous les comptons par paquets de trois, le reste est 2 ;
- si nous les comptons par paquets de cinq, le reste est 3 ;
- si nous les comptons par paquets de sept, le reste est 2.

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

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

Théorème chinois. — *Soit m et n deux entiers premiers entre eux. Soit a et b deux entiers. On considère le système d'équations aux congruences*

$$(S) \qquad \begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases} \qquad (x \in \mathbf{Z}).$$

1. *Soit c une solution du système (S). On a alors*

$$\forall x \in \mathbf{Z}, \quad x \text{ est solution de (S)} \iff x \equiv c \pmod{mn}.$$

2. *Il existe un entier c solution de (S). Plus précisément, soit r, s des entiers vérifiant $r\,m + s\,n = 1$. Soit $c = b\,r\,m + a\,s\,n$. Alors c est une solution de (S).*

Démonstration. — Si x et c sont solutions de (S), x et c sont tous les deux congrus à a modulo m et à b modulo n. On a donc $x \equiv c \pmod m$ et $x \equiv c \pmod n$. Ainsi $x - c$ est divisible à la fois par m et par n, donc par leur produit mn, *puisque m et n sont premiers entre eux.* Réciproquement, si c est solution de (S) et si on a $x \equiv c \pmod{mn}$, on a $x \equiv c \pmod m$ et $x \equiv c \pmod n$, ce qui se réécrit $x \equiv a \pmod m$ et $x \equiv b \pmod n$. Ainsi x est solution de (S). Ceci démontre le 1. Remarquons que nous n'avons pas encore démontré que (S) avait effectivement des solutions. C'est précisément l'objet du 2.

Nous donnons deux démonstrations du 2. La première utilise un argument combinatoire et est ineffective en ce sens qu'elle ne fournit pas de méthode pour trouver effectivement une solution de (S). La deuxième consiste simplement à vérifier que l'entier fourni par l'énoncé convient.

Première démonstration : Considérons l'application r de $\{0, \dots, mn - 1\}$ dans $\{0, \dots, m - 1\} \times \{0, \dots, n - 1\}$ qui, à un entier $x \in \{0, \dots, mn - 1\}$, associe le couple formé des restes des divisions euclidiennes de x par m et n. Montrons que cette application est injectivve Soient x et y deux éléments de $\{0, \dots, mn - 1\}$ ayant la même image (a', b') par r. Ceci signifie que x et y satisfont un système du type (S), où (a, b) est remplacé par (a', b'). D'après 1., on a $x \equiv y$

$\pmod{m} n$. Donc $x = y$. L'application r est injective et ses ensembles de départ et d'arrivée ont même cardinal, elle est donc surjective, ce qu'il fallait démontrer.

Deuxième démonstration : Posons $c = b\,r\,m + a\,s\,n$. On a donc $c \equiv b\,r\,n \pmod{n}$ et $c \equiv a\,s\,n \pmod{m}$ Comme $r\,m + s\,n = 1$, on a $r\,m \equiv 1 \pmod{n}$ et $s\,n \equiv 1 \pmod{m}$, d'où $c \equiv b \pmod{n}$ et $c \equiv a \pmod{m}$.

□

Ce théorème élucide la structure de l'ensemble des solutions du système (S). En particulier, (S) possède une et une seule solution élément de $\{0, \ldots, m\,n - 1\}$ (et toutes les autres solutions se déduisent de celle-ci lui ajoutant des multiples de $m\,n$).

Remarquons que tout système d'équations en congruences de la forme

$$\begin{cases} cx \equiv a' \pmod{m'} \\ dx \equiv b' \pmod{n'} \end{cases}$$

soit n'a pas de solution, soit est équivalent à un système du type (S). En effet d'après le paragraphe précédent, soit l'équation $cx \equiv a' \pmod{m'}$ n'admet pas de solution (quand a' n'est pas multiple de $\mathrm{pgcd}(c, m')$), soit cette équation est équivalente à une équation de la forme $x \equiv a \pmod{m}$.

On peut généraliser le théorème chinois à des systèmes de plus de deux équations aux congruences.

Théorème **(Généralisation du théorème chinois)**. — *Soit $m_1, \ldots, m_n$ des entiers naturels et soit $a_1, \ldots, a_n$ des entiers relatifs. Si les $m_1, \ldots, m_n$ sont deux à deux premiers entre eux, il existe un entier a tel qu'on ait l'équivalence*

$$\forall x \in \mathbf{Z}, \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \iff \begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \\ \vdots \\ x \equiv a \pmod{m_n} \end{cases}$$
$$\iff x \equiv a \pmod{m_1 m_2 \cdots m_n}.$$

Nous allons donner deux démonstrations de ce théorème, qui sont toutes les deux effectives (elles donnent chacune une méthode pour calculer effectivement un entier a vérifiant l'équivalence ci-dessus). Au moins une de ces deux méthodes est à connaître.

La première méthode est basée sur l'existence de la décomposition d'un entier en base mixte.

Théorème **(Décomposition d'un entier en base mixte)**. — *Soit $b_1, \ldots, b_k$ des entiers ≥ 2. Tout entier n s'écrit de manière unique sous la forme*

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

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

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

Démonstration du théorème chinois généralisé. — Première méthode. On cherche une solution x du système de congruences :

$$\forall 1 \leq k \leq n, \quad x \equiv a_k \pmod{m_k}.$$

On cherche x dans sa décomposition en base mixte $(m_1, m_2, \cdots, m_n)$

$$x = x_1 + x_2 m_1 + \cdots + x_n m_1 m_2 \ldots m_{n-1} + q m_1 m_2 \ldots m_n \text{ avec de plus } 0 \leq x_k < m_k.$$

La première condition $x \equiv a_1 \pmod{m_1}$ entraîne $x_1 = a_1 \pmod{m_1}$, car tous les autres termes sont multiples de m_1, d'où x_1 est le reste de la division euclidienne de a_1 par m_1. Si $x_1, \ldots, x_{k-1}$ sont déterminés, la condition $x \equiv a_k \pmod{m_k}$ s'écrit

$$x_k(m_1 \ldots m_{k-1}) \equiv a_k - x_1 - x_2 m_1 - \cdots - x_{k-1} m_1 \ldots m_{k-2} \pmod{m_k},$$

car tous les autres termes sont multiples de m_k. Il reste à résoudre cette équation (d'inconnue x_k) à l'aide des méthodes du paragraphe précédent. Sans hypothèses sur les m_k ce n'est pas toujours possible. Mais ici les m_k sont premiers entre eux deux à deux. Ainsi, $m_1 \ldots m_{k-1}$ est premier à m_k pour tout entier k tel que $1 \leq k \leq n$ (un nombre premier qui divise m_k ne divise aucun autre m_i, donc ne divise pas $m_1 \ldots m_{k-1}$). D'après le paragraphe précédent, l'équation $x_k(m_1 \ldots m_{k-1}) \equiv y_k \pmod{m_k}$ possède une unique solution modulo m_k, d'où l'existence d'un unique entier x_k qui vérifie cette congruence et tel que $0 \leq x_k < b_k$. À la fin de la résolution, on a déterminé l'*unique* entier X tel que $0 \leq X < m_1 \ldots m_n$ et $X \equiv x_k \pmod{b_k}$ pour tout k compris entre 1 et n. Les solutions du système de congruences sont alors les entiers de la forme $X + cm_1 \ldots m_n$, avec $c \in \mathbf{Z}$ (ceci se démontre de manière analogue au cas de deux équations).

Deuxième méthode. On regarde le système formé par les deux premières équations :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Comme m_1 et m_2 sont premiers entre eux, le théorème chinois nous dit qu'il existe un entier a_1' (que l'on peut déterminer explicitement à partir d'une relation de Bézout entre m_1 et m_2) tel qu'on ait

$$\forall x \in \mathbf{Z}, \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x_2 \equiv a_2 \pmod{m_2} \end{cases} \iff x \equiv a_1' \pmod{m_1 m_2}$$

On a donc

$$\forall x \in \mathbf{Z}, \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \iff \begin{cases} x \equiv a_1' \pmod{m_1 m_2} \\ x \equiv a_3 \pmod{m_3} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

On est donc ramené à un système comportant une équation de moins. On regarde alors le système formé par les deux premières équations de ce nouveau système :

$$\begin{cases} x \equiv a_1' \pmod{m_1 m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases}$$

Comme les m_k sont supposés premiers entre eux deux à deux, les entiers $m_1 m_2$ et m_3 sont premiers entre eux. On peut donc à nouveau appliquer le théorème chinois, ce qui fait encore diminuer d'une unité le nombre d'équations du système. De proche en proche, on montre ainsi que le système initiale est équivalent à une seule équation aux congruences. $\square$

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

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

Deuxième méthode. On résout d'abord le système

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Pour cela on détermine une relation de Bézout entre 3 et 5, par exemple $2.5 - 3.3 = 1$. On sait qu'alors $2.5.2 - 3.3.3 = -7$ est solution du système. On a donc

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \iff x \equiv -7 \pmod{15} \iff x \equiv 8 \pmod{15}.$$

Le système initial est donc équivalent au système

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7 \end{cases}$$

Une relation de Bézout entre 15 et 7 est $1.15 - 2.7 = 1$. Une solution de ce système est $2.1.15 - 8.2.7 = -82$ et on a

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7 \end{cases} \iff x \equiv -82 \pmod{105} \iff x \equiv 23 \pmod{105}.$$

5.2.1. Quand le théorème chinois ne s'applique pas. — Considérons un système d'équations en congruences

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

avec $d = \mathrm{pgcd}(m, n)$ différent de 1. Si le système admet une solution, disons x_0, alors comme d divise m et n, $x_0 \pmod d \equiv a \pmod d \equiv b \pmod d$.

Réciproquement, supposons que $a \pmod d \equiv b \pmod d$. Il existe donc un entier relatif c tel que $b - a = cd$. Considérons un couple de Bezout $(u, v) \in \mathbf{Z}^2$ pour (m, n) : $um + vn = d$. Alors,

$$\begin{aligned} a + cum &\equiv a \pmod m \\ a + cum &\equiv a + cum + cvn \equiv a + cd \equiv a + b - a \equiv b \pmod n. \end{aligned}$$

L'entier $a + kum$ est donc solution du système.

Le système devient alors équivalent à

$$\begin{cases} x \equiv a + cum \pmod{m} \\ x \equiv a + cum \pmod{n} \end{cases} \iff x - (a + cum) \text{ est multiple de } m \text{ et de } n,$$

dont les solutions sont les entiers de la forme $a + cum + k\,\mathrm{ppcm}(m, n)$ avec $k \in \mathbf{Z}$.

5.3. Équations polynomiales modulo p

Nous avons appris à résoudre des équations de la forme $ax \equiv b \pmod{n}$, où a, b et n sont des nombres entiers. Dans ce paragraphe, il s'agit d'expliquer comment trouver les solutions modulo n d'une équation polynomiale. Par souci de simplification, on se limitera essentiellement au cas d'une équation de degré 2 modulo un nombre premier, c'est-à-dire une équation de la forme $ax^2 + bx + c \equiv 0 \pmod{p}$ où p est premier.

Concernant l'équation générale de degré d arbitraire, le seul résultat que nous démontrerons est qu'il y a *au plus d* racines modulo p. Le chapitre « Pour aller plus loin » donne quelques éléments sur la démarche employée pour trouver les solutions d'une équation aux congruences polynomiale générale.

5.3.1. Le degré 2. — On considère une équation de la forme $ax^2 + bx + c \equiv 0 \pmod{p}$ où p est premier. On suppose que $a \not\equiv 0 \pmod{p}$; dans le cas contraire, l'équation est de degré au plus 1.

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

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

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

d'où finalement l'équation

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

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

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

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

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

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

Il convient aussi de remarquer que

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

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

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

Tout ceci nous amène à la question suivante : comment reconnaître si l'entier Δ est un carré modulo p ? La réponse n'est pas tout à fait évidente. Ainsi, -7 est un carré modulo 37 (c'est 17^2), alors que ce n'est pas un carré comme nombre réel. Avant d'aller plus loin sur ce sujet, nous allons avoir besoin d'en savoir un peu plus sur les équations de degré plus grand.

5.3.2. Le nombre maximum de solutions d'une équation polynomiale modulo p. —

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

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

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

avec $y=c$, on trouve

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

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

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

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

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

Théorème. — *Soit p un nombre premier et soit $A = X^d + a_{d-1}X^{d-1} + \dots + a_1 X + a_0$ un polynôme à coefficients entiers. Alors, le nombre d'entiers $k \in \{0, \dots, p-1\}$ tels que $A(k) \equiv 0 \pmod p$ est au plus égal à d.*

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

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

5.3.3. Être ou ne pas être un carré modulo p. — Soit p un nombre premier, supposons $p \geq 3$ de sorte que $p-1$ est pair.

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

Soit x un entier qui n'est pas multiple de p. D'après le petit théorème de Fermat, $x^{p-1} \equiv 1 \pmod{p}$, si bien que $a = x^{(p-1)/2}$ vérifie $a^2 \equiv 1 \pmod{p}$. Il est immédiat que 1 et -1 sont solutions modulo p de cette équation. Réciproquement, si $a^2 \equiv 1 \pmod{p}$, $a^2-1 = (a-1)(a+1)$ est multiple de p, donc $a-1$ ou $a+1$ est multiple de p, ce qui entraîne $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$). Donc $a \equiv \pm 1 \pmod{p}$.

Supposons qu'il existe un nombre entier y tel que $x \equiv y^2 \pmod{p}$. Alors, $x^{(p-1)/2} \equiv y^{p-1} \equiv 1 \pmod{p}$. Ainsi, si x est un carré modulo p, $x^{(p-1)/2}$ est congru à 1 modulo p. Les éléments de C sont donc des solutions de l'équation $x^{(p-1)/2} \equiv 1 \pmod{p}$. On peut alors montrer que tout $x \in \{0,\dots,p-1\}$ solution de cette dernière équation est dans C. En effet, le polynôme $X^{\frac{p-1}{2}} - 1$ est de degré $\frac{p-1}{2}$, donc l'équation aux congruences $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ a au plus $\frac{p-1}{2}$ solutions x dans $\{0,\dots,p-1\}$. Comme on en connaît déjà au moins $\frac{p-1}{2}$, à savoir les éléments de C, il n'y en a pas d'autres. On a ainsi le résultat suivant :

Proposition. — *Soit p un nombre premier, $p \neq 2$, et soit a un entier qui n'est pas multiple de p. L'entier a est congru modulo p au carré d'un nombre entier, si et seulement si $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Remarquons que si a n'est pas un carré modulo p, on a $a^{(p-1)/2} \equiv -1 \pmod{p}$. En effet, si on pose $b = a^{(p-1)/2}$, on a $b^2 \equiv 1 \pmod{p}$ et d'après ce qui précède on a $b \equiv -1 \pmod{p}$ ou $b \equiv 1 \pmod{p}$, ce dernier cas étant exclu si a n'est pas un carré modulo p.

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

Il est à noter que la proposition précédente fournit un moyen effectif de déterminer si un entier donné est ou non un carré modulo p. D'après le paragraphe précédent, ceci donne un moyen effectif de déterminer si une équation du second degré modulo p a ou non des solutions. Mais lorsque un entier x est un carré modulo p, nous n'avons pas donné de méthode pour trouver *effectivement* un entier y dont le carré est congru à x modulo p, en particulier pour calculer effectivement les solutions d'une équations du second degré modulo p lorsque ces solutions existent.

Bien sûr, il y a toujours la possibilité de calculer tous les carrés modulo p, mais ceci peut être assez long en pratique. Lorsque p est congru à 3 modulo 4, on peut donner un moyen simple et efficace de calculer une racine carrée modulo p.

Proposition. — *Soit p un nombre premier congru à 3 modulo 4 et a un entier qui est un carré modulo p. On a alors*

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a \pmod p$$

Démonstration. — En effet d'après la proposition précédente on a $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Par ailleurs on a

$$\begin{aligned}\left(a^{\frac{p+1}{4}}\right)^2 &\equiv a^{\frac{p+1}{2}} \pmod p \\ &\equiv a^{1+\frac{p-1}{2}} \pmod p \\ &\equiv a.a^{\frac{p-1}{2}} \pmod p \\ &\equiv a \pmod p\end{aligned}$$

□

5.4. Théorème d'Euler, ordre multiplicatif, cryptographie RSA

5.4.1. Théorème d'Euler. —

Définition. — *Soit n un entier ≥ 2. On note $\Phi(n)$ l'ensemble des entiers m avec $1 \leq m \leq n$ qui sont premiers à n et $\phi(n)$ leur nombre.*

La fonction ϕ s'appelle l'indicateur d'Euler [(1)]. Par exemple si p est un nombre premier, on a $\Phi(p) = \{1, 2, \cdots, p-1\}$ et $\phi(p) = p - 1$.

Calcul de ϕ. — *1. Si m et n sont deux entiers naturels premiers entre eux $\phi(mn) = \phi(n)\phi(n)$.*
2. Si p est un nombre premier et k un nombre naturel non nul, on a $\phi(p^k) = p^{k-1}(p-1)$.

Démonstration. — 1. Soit

$$\begin{array}{cccc} f & : & \Phi(mn) & \rightarrow & \Phi(m) \times \Phi(n) \\ & & x & \mapsto & (r_m, r_n) \end{array}$$

l'application qui a un entier x associe le couple formé du reste r_m de la division euclidienne de x par m et du reste r_n de la division euclidienne de x par m. Montrons que f est bien définie et que c'est une bijection.

Soit x dans $\Phi(mn)$. L'entier x est premier à mn donc à m. Par le lemme de l'algorithme d'Euclide $\text{pgcd}(r_m, m) = \text{pgcd}(x, m) = 1$. Donc, r_m appartient bien à $\Phi(m)$. De même, $r_n \in \Phi(n)$.

Soit (a, b) dans $\Phi(m) \times \Phi(n)$. Un antécédent de (a, b) par f est un entier x dans $\Phi(mn)$ dont le reste de la division euclidienne par m est a et par m est b. Par le théorème chinois, il existe un unique entier x dans $\{0, \cdots, mn-1\}$ tel que $x \equiv a \pmod m$ et $x \equiv b \pmod n$. Maintenant, $\text{pgcd}(x, m) = \text{pgcd}(a, m) = 1$ et $\text{pgcd}(x, n) = 1$. Par le lemme de Gauss, x est premier avec le produit mn. Ainsi, x est l'unique antécédent de (a, b) par f.

1. Leonhard Paul EULER, mathématicien et physicien suisse (1707–1783). À l'instar de GAUSS, il est reconnu comme l'un des plus grands mathématiciens de tous les temps. Ses contributions mathématiques couvrent de multiples domaines de la discipline, et son nom est resté associé à de nombreux objets et résultats mathématiques.

2. Soit x un entier de $\{1, 2, \cdots p^k - 1\}$. L'entier x n'est pas premier avec p^k si et seulement si p divise x, autrement dit si et seulement si il existe un entier q vérifiant $1 \leq q < p^{k-1}$ et $x = qp$. On en déduit que $\phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1)$.

□

Par exemple, si p et q sont deux nombres premiers disctincts, $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Théorème d'Euler. — *Soit $n \geq 2$ un entier naturel. Pour tout entier relatif a qui est premier à n, on a la congruence $a^{\phi(n)} \equiv 1 \pmod{n}$. En outre, le plus petit entier $m \geq 1$ tel que $a^m \equiv 1 \pmod{n}$ est un diviseur de $\phi(n)$.*

Cela généralise le théorème de Fermat déjà démontré au chapitre précédent lorsque n est un nombre premier.

Démonstration. — Soit a un entier premier à n et considérons l'application f de $\{0, \ldots, n-1\}$ dans lui-même qui, à un entier x, associe le reste de la division euclidienne de ax par n.

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

On rappelle que $\Phi(n)$ désigne l'ensemble des entiers m vérifiant $1 \leq m \leq n$ et qui sont premiers à n. Montrons qu'on a $f(\Phi(n)) \subset \Phi(n)$. Soit $x \in \{0, \ldots, n-1\}$. Soit d le plus grand diviseur commun de n et $f(x)$. Par définition de l'application f, il existe $q \in \mathbf{Z}$ tel que $ax = qn + f(x)$. Alors, d divise ax. Comme d divise n et que a est premier à n, d est premier à a, d'où d divise x. Si $x \in \Phi(n)$, cela entraîne $d = 1$, donc n et $f(x)$ sont premiers entre eux, c'est-à-dire $f(x) \in \Phi(n)$. Comme $\Phi(n)$ est fini, f définit une bijection de $\Phi(n)$ dans lui-même. Il en résulte l'égalité

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

Notons N cet entier. Ce produit d'entiers premiers à n est donc premier à n.

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

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

Autrement dit, $N(a^{\phi(n)} - 1)$ est multiple de n. Puisque N est premier à n, $a^{\phi(n)} \equiv 1 \pmod{n}$. □

5.4.2. Ordre multiplicatif. —

Définition et premières propriétés. — Soit n un entier naturel et soit a un entier qui est premier avec n. Il existe des entiers k tels que $a^k \equiv 1 \pmod{n}$, par exemple $k = \phi(n)$ convient. On peut donc poser la

Définition. — *Soit n un entier naturel et soit a un entier qui est premier avec n. L'*ordre (multiplicatif) de a modulo n, *noté* $\mathrm{ord}_n(a)$, *est le plus petit entier $k \geq 1$ tel que $a^k \equiv 1 \pmod{n}$.*

Si a et b sont congrus modulo n, $a^k \equiv b^k \pmod{n}$ pour tout entier k, si bien que a et b ont même ordre multiplicatif modulo p.

Proposition. — *L'ordre multiplicatif de a modulo n est un diviseur de $\phi(n)$.*

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

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

Comme d est le plus petit entier strictement positif tel que $a^d \equiv 1 \pmod n$ et que $0 \leq r < d$, on a nécessairement $r = 0$. Autrement dit, les entiers k tels que $n^k \equiv 1 \pmod p$ sont les multiples de d. Appliquons ce raisonnement à l'entier $\phi(n)$ □

L'ordre multiplicatif modulo p. — Soit n un entier supérieur à 2. Tout nombre entier x qui est premier à n possède un ordre multiplicatif modulo n. On a déjà démontré que cet entier divise $\phi(n)$. Ce paragraphe a pour objet de préciser quelles valeurs peut prendre cet entier.

Lemme. — *1. Soit x un nombre entier premier à n et soit a son ordre multiplicatif modulo n. Tout diviseur de a est l'ordre multiplicatif d'un nombre entier premier à n ; précisément, si $a = de$, alors d est l'ordre multiplicatif modulo n de x^e.*

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

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

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

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

3. Montrons d'abord que si a et b sont les ordres multiplicatifs modulo n de deux nombres entiers x et y, il existe un nombre entier relatif z, premier à n, dont l'ordre multiplicatif est égal à $\mathrm{ppcm}(a, b)$. Pour cela, écrivons la décomposition en facteurs premiers de a et b sous la forme $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$. On a donc $\mathrm{ppcm}(a, b) = \prod p_i^{\max(\alpha_i, \beta_i)}$. Posons $\alpha'_i = \alpha_i$ si $\alpha_i \geq \beta_i$, et $\alpha'_i = 0$ sinon. Posons aussi $\beta'_i = 0$ si $\alpha_i \geq \beta_i$ et $\beta'_i = \beta_i$ sinon. Posons $a' = \prod p_i^{\alpha'_i}$ et $b' = \prod p_i^{\beta'_i}$; par construction, $\mathrm{ppcm}(a, b) = a'b'$ puisque $\alpha'_i + \beta'_i = \max(\alpha_i, \beta_i)$ pour tout i. De plus, a' et b' n'ont aucun facteur commun.

   D'après *1*), a' et b' sont les ordres multiplicatifs modulo n d'entiers x' et y'. Comme ils sont premiers entre eux, $a'b' = \mathrm{ppcm}(a, b)$ est l'ordre multiplicatif d'un entier relatif premier à n.

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

□

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

Un tel élément ω est appelé *générateur multiplicatif* modulo p. Ce théorème est dû à GAUSS.

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

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

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

5.4.3. Chiffrement RSA. — À la fin des années 1970, RIVEST [2], SHAMIR [3] et ADLEMAN [4] ont utilisé ces résultats pour élaborer un *système de cryptographie à clef publique* : système depuis appelé RSA, du nom de ses auteurs.

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

Imaginons qu'un élément de A soit un message (ou un morceau de message) ; le message crypté sera $f(a)$. À moins de connaître f^{-1} explicitement, personne ne peut le décoder. Notons aussi qu'on peut même rendre la fonction f publique, de sorte que n'importe qui puisse coder des messages, sans rompre la sécurité du système.

Le principe. — Mais comment produire de telles fonctions f ? C'est là que réside l'astuce des auteurs de RSA : les congruences fournissent précisément ce genre d'applications.

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

Or, $\phi(N) = (p-1)(q-1)$. Soit ainsi e un entier petit, premier à $\phi(N)$ (en pratique, $e = 3$, ou 11) et d inverse de e modulo $\phi(n)$. La fonction f est la fonction $x \mapsto x^e \pmod N$; la fonction g est la fonction $x \mapsto x^d \pmod N$ [5]

Comme il existe $k \in \mathbf{N}$ tel que $de = 1 + \phi(N)k$, on a bien

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

2. Ronald RIVEST, cryptologue américain, né en 1947.
3. Adi SHAMIR, cryptologue israélien, né en 1952.
4. Leonard ADLEMAN, informaticien théoricien américain, né en 1945.
5. Les lettres e et d sont les premières lettres des mots anglais *encoding* et *decoding*.

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

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

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

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

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

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

3) On a aussi besoin de fabriquer de grands nombres premiers. Pour cela, on utilise des algorithmes qui permettent de reconnaître relativement rapidement les nombres premiers. On a vu que le petit théorème de Fermat permet de montrer qu'un entier n'est pas premier ; on a vu qu'il y a aussi des nombres de Carmichael pour lesquels ce test laisse croire que l'on a affaire à un nombre premier. Il existe cependant un raffinement assez simple de ce test de Fermat pour lequel il n'y a plus ce phénomène de nombres de Carmichael. On parle de *nombre fortement pseudo-premier en base a*. Un joli théorème de Rabin (6) montre que si un entier n'est pas premier, au moins $3/4$ des bases le mettent en évidence. La méthode consiste alors à tirer des bases au hasard et à regarder ce qui se passe ; au bout de 10 essais réussis, la *probabilité* que l'entier choisi ne soit pas premier est égale à 2^{-20}. C'est paraît-il bien moins que la probabilité qu'au même moment, un rayon cosmique ne provoque une erreur de calcul dans l'ordinateur...

Outre leur grande taille, il faut aussi prendre garde à éviter les nombres premiers p vérifiant des propriétés qui les rendraient faciles à repérer par certains algorithmes de factorisations. Par exemple, $p-1$ et $p+1$ doivent avoir de grands facteurs premiers. On ne peut donc pas utiliser de formules du genre de celles définissant les nombres de Fermat ou les nombres de Mersenne (7).

---

6. Michael Oser Rabin, informaticien et logicien israélien, né en 1931. Il reçut en 1976 le prix Turing, considéré comme la récompense la plus prestigieuse en informatique.

7. Marin Mersenne, religieux, mathématicien et philosophe français (1588–1648). Il est connu pour sa volumineuse correspondance avec d'autres mathématiciens de son époque (Descartes, Pascal…) Il a laissé son nom aux nombres de la forme $2^p - 1$, où p est un nombre premier, qui fournissent des candidats naturels pour trouver de grands nombres premiers. Actuellement (février 2013), 48 nombres de Mersenne premiers sont connus, le plus grand étant $2^{57885161} - 1$. Inutile de dire que les calculs ne se font pas à la main… On ignore s'il existe une

infinité de nombres de Mersenne premiers, tout comme on ignore d'ailleurs s'il existe une infinité de nombres de Mersenne qui ne sont pas premiers. . .

PARTIE III

POUR ALLER PLUS LOIN

Nous développons ici des thèmes liés à ceux étudiés dans le cours, mais qui ne seront pas vus en cours faute de temps.

Probabilités

Définition. — *Une probabilité sur un ensemble fini* Ω *est une application* $p : \mathcal{P}(\Omega) \to [0,1]$ *qui à toute partie* A *de* Ω *associe un nombre réel compris entre* 0 *et* 1*, sa* probabilité $p(A)$ *de sorte que l'on ait* $p(\varnothing) = 0$*,* $p(\Omega) = 1$*, et* $p(A \cup B) = p(A) + p(B)$ *si* A *et* B *sont deux parties* disjointes *de* Ω*.*

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

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

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

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

En particulier,

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

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

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

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

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

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

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

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

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

Les événements $A = \{a \leq 3\}$ et $B = \{a + b \geq 7\}$ ne sont par contre pas indépendants. La probabilité du premier est $\frac{3}{6} = \frac{1}{2}$. L'événement $\{a + b \geq 7\}$ se produit dans les cas $(6,b)$ avec b quelconque, $(5,b)$ avec $b \geq 2$, etc. jusque $(1,b)$ avec $b = 6$, d'où $6 + 5 + 4 + 3 + 2 + 1 = 21$ cas. Sa probabilité est ainsi de $\frac{21}{36} = \frac{7}{12}$. L'événement intersection correspond aux tirages $(1, b)$ avec $b = 6$, $(2, b)$ avec $b \geq 5$ et $(3, b)$ avec $b \geq 4$ et ces 6 tirages ont donc probabilité $\frac{6}{36} = \frac{1}{6}$. On constate que $p(A)p(B) = \frac{1}{2}\frac{7}{12} = \frac{7}{24}$ alors que $p(A \cap B) = \frac{1}{6} = \frac{4}{24}$. La probabilité pour B de survenir sachant que A est arrivé est ainsi $p(B|A) = p(A \cap B)/p(A) = \frac{1}{3}$. Intuitivement : comme la valeur de a est petite, on a moins de chance d'obtenir une valeur de $a + b$ qui soit au moins 7.

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

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

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

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

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

Finalement,

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

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

Plus généralement :

Formule de Bayes. — *Soit $A_1, \ldots, A_n$ une partition de Ω avec $p(A_i) > 0$ pour tout i. Soit E un événement quelconque de probabilité $p(E) > 0$. Alors,*

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

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

L'utilisation de cette formule est la suivante. Les événements A_i correspondent à des événements « réels » (le temps qu'il fait, le fait qu'on soit malade ou pas, qu'une pièce soit correctement usinée, etc.) et l'événement E est le résultat d'un test qui n'est pas totalement fiable (prévision météo, test de vaccination, contrôle aléatoire dans une chaîne de production, etc.). Les probabilités $p(E|A_i)$ représentent la fiabilité du test E : ce que dit E sachant que A_i se produit. Les probabilités $p(A_i)$

sont inconnues en général, mais peuvent être estimées sur une grande échelle (observations du temps, épidémiologique, etc.). La formule permet de calculer une estimation de la probabilité qu'on soit dans le cas A_i sachant que le test E est positif.

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

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

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

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

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

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

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

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

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

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

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

On peut ainsi espérer gagner $n\pi$.

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

Un exemple d'utilisation des suites arithmético-géométriques

Si vous devez acheter une maison, vous devrez probablement emprunter la somme correspondante à une banque. La banque avance alors l'argent et, chaque mois, vous devrez payer une somme fixée (la « mensualité »). Votre capital restant dû diminue d'autant, après avoir été majoré des intérêts sur la somme restant due.

Intéressons-nous aux intérêts. La littérature bancaire fait en général mention d'un *taux annuel* — pour un prêt immobilier, il est en ce moment l'ordre de 4,5 % par an. Mais comme vous remboursez chaque mois, vos intérêts sont aussi calculés chaque mois et le banquier doit utiliser un *taux mensuel.* On imaginerait a priori que ce taux mensuel est calculé de sorte que les intérêts d'un an (en l'absence de remboursement) correspondent au taux annuel.

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

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

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

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

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

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

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

L'inégalité précédente n'est pas propre au nombre 12. Nous allons montrer que pour tout entier naturel $n \geq 2$ et tout nombre réel $x > 0$, on a $(1 + x)^n > 1 + nx$. Si $n = 2$,

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

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

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

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

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

d'où

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

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

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

On pose $C_0 = C$ et, plus généralement, on note C_n le capital restant dû au bout de n mois. Au bout de chaque mois, la banque vous considère comme débiteur des intérêts mensuels sur le capital dû au début du mois mais vous crédite du montant de la mensualité, si bien que le capital restant dû au mois $(n+1)$ vérifie la relation Au bout d'un mois, vous devez à la banque $C + \tau_{\mathrm{m}} C - M$ et plus généralement, au bout de $n+1$ mois vous devez à la banque

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

La suite $(C_n)_{n\in\mathbf{N}}$ est donc une suite arithmético-géométrique. On a alors, pour tout entier naturel n,

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

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

Équations polynomiales modulo n

Un polynôme à coefficients entiers en une variable X est une expression de la forme $P(X) = a_0 + a_1 X + \cdots + a_d X^d$, où $a_0, \ldots, a_d$ sont des nombres entiers. Si $a_d \neq 0$, on dit que le polynôme P est de degré d ; quitte à ne pas écrire les termes dont le coefficient est nul, on peut facilement se ramener à ce cas.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'anneau $\mathbf{Z}/n\mathbf{Z}$

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

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

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

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

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

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

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

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

L'intérêt d'introduire $\mathbf{Z}/n\mathbf{Z}$, c'est que le calcul des classes permet de s'affranchir définitivement du choix des représentants : on utilise souvent les représentants compris entre 0 et $n-1$ mais on pourrait choisir les entiers compris entre $-n/2$ (exclu si n est pair) et $n/2$ (inclus si n est pair). Pire, à une ligne du calcul, le choix $n-1$ du représentant de la classe de -1 pourait être préférable, sans qu'il cesse d'être souhaitable, de vouloir revenir au représentant -1 à la ligne suivante. Avec le calcul des classes, cette question devient sans objet : dans $\mathbf{Z}/n\mathbf{Z}$, n (entendre « $\overline{n}$ », c'est-à-dire sa classe) est *égal* à 0, donc $n-1$ et -1 sont tout simplement égaux !

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

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

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

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

Construction des nombres entiers naturels

Notre but ici est d'expliquer comment rendre rigoureuses les manipulations que l'on fait sur les nombres entiers, pourquoi par exemple $3 + 5 = 5 + 3$.

Pour commencer, nous nous donnons quelques affirmations, prises comme vérités premières en arithmétique, appelées « axiomes ». Voici les axiomes, sous la présentation de Peano [(8)] (si ce n'est que Peano faisait débuter l'ensemble des entiers naturels à 1).

Axiomatique de Peano. —

AP1 zéro (0) est un entier naturel ;

AP2 tout entier naturel a un unique successeur parmi les entiers naturels ;

AP3 zéro n'est le successeur d'aucun entier naturel ;

AP4 si deux entiers naturels ont même successeur, ils sont égaux.

AP5 Soit A un ensemble d'entiers naturels. Supposons que A contienne 0 et que si un entier naturel n appartient à A, son successeur appartienne à A. Alors A est l'ensemble de tous les entiers naturels.

8. Giuseppe Peano, mathématicien italien (1858–1932). Ses travaux ont porté sur l'analyse et la logique mathématique. Avec l'axiomatisation présentée ici, son résultat le plus célèbre est la construction d'une courbe qui « remplit » entièrement un carré.

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

Avec le langage logique et celui de la théorie des ensembles, nous pouvons formuler de façon plus rigoureuse la construction de l'ensemble $\mathbf{N}$.

Définition. — *On dit qu'un triplet (N, o, s) composé d'un ensemble N, un objet o et une application s est un* système naturel *si*

1. *o est un élément de N.*
2. *s est une application de N dans N.*
3. *o n'est pas dans l'image de l'application s.*
4. *l'application s est injective.*
5. *le seul sous-ensemble A de N qui vérifie*
   (a) o appartient à A
   (b) $\forall n \in A, \quad s(n) \in A$

   est N lui même.

***Théorème* (admis)**. —

1. *Il exite un système naturel.*
2. *Si (N, o, s) et (N', o', s') sont deux systèmes naturels, il existe une unique bijection $f : N \to N'$ de N vers N' compatible avec l'élément distingué (i.e. $f(o) = o'$) et avec l'application successeur (i.e. $f \circ s = s' \circ f$.)*

À bijection près, il existe donc un seul système naturel. On l'appelle *ensemble des nombres naturels.* Ses éléments sont appelés *les nombres naturels.* Son élément distingué o est appelé *zéro* et noté 0.

Ainsi, les axiomes de Peano caractérisent l'ensemble des nombres naturels. Ils constituent la liste exhaustive de ses propriétés : tout théorème le concernant devra être démontré à partir d'eux et des règles du raisonnement logique.

L'ensemble de tous les entiers naturels est noté $\mathbf{N}$. On note 1 le successeur de 0, 2 le successeur de 1, 3 celui de 2, etc. Ici se cache une difficulté : comment écrire une infinité de nombres avec un nombre fini de symboles. Il y a des choix à faire, par exemple le choix d'une base.

Proposition. — *Tout entier naturel non nul est le successeur d'un unique entier.*

Démonstration. — Soit A la réunion du singleton $\{0\}$ et de l'ensemble des entiers naturels qui sont le successeur d'un entier. L'ensemble A contient 0, et s'il contient un entier naturel n, il contient son successeur, puisqu'il contient tous les successeurs. Donc, A est l'ensemble des entiers naturels. Ainsi, tout entier naturel, sauf zéro en vertu de l'axiome *(AP3)*, est le successeur d'un entier. Notons enfin qu'un entier naturel ne peut avoir deux prédécesseurs distincts, par l'axiome *(AP4)*. $\square$

Le principe de récurrence permet aussi de *définir* des objets dépendant d'un entier. Expliquons comment procéder et comment *démontrer* les propriétés élémentaires de l'addition et de la multiplication.

Si m et n sont deux entiers naturels, on veut définir l'entier naturel $m+n$. On va procéder par récurrence sur m.

Initialisation : Si $m = 0$, pour tout entier naturel n, on pose $0 + n = n$.
Hérédité : Soit m un entier. Supposons avoir défini l'entier naturel $m + n$ pour tout entier naturel n. Pour tout entier naturel n, on peut alors poser (puisque $m + n$ est déjà défini)

$$s(m) + n = s(m + n). \quad (*)$$

Cela définit l'addition de deux entiers naturels arbitraires.

Posons $1 := s(0)$. On a alors pour tout entier naturel n, $s(n) := 1 + n$. En effet on a

$$1 + n = s(0) + n = s(0 + n) = s(n).$$

Ainsi, la formule $(*)$ s'écrit $(1 + m) + n = 1 + (m + n)$. C'est un cas particulier de l'associativité de l'addition, qui sera démontrée ci-dessous en toute généralité.

Il est vrai qu'on a aussi pour tout entier naturel n l'égalité $s(n) = n + 1$ mais ce n'est pas évident a priori. Cela découle de la commutativité de l'addition, qui sera démontrée ci-dessous. On pourrait aussi le démontrer directement par récurrence.

Montrons à présent deux propriétés simples de l'addition

Proposition. — *Si deux entiers naturels a et b sont tels que $a + b = 0$, alors $a = 0$ et $b = 0$.*

Démonstration. — Nous allons faire un raisonnement par l'absurde. Supposons que a soit non nul. Par une proposition déjà obtenue, a est un successeur : il existe un entier a' tel que $a = s(a')$. Maintenant, par définition de l'addition,

$$a + b = s(a') + b = s(a' + b) = 0.$$

Or, 0 n'est pas un successeur par l'axiome *(AP3)*. Donc, a est nul. Maintenant, toujours par définition de l'addition, on obtient $a + b = 0 + b = b = 0$. □

Proposition. — *Si m, n et n' sont trois entiers naturels tels que $m + n = m + n'$, alors $n = n'$.*

Démonstration. — On procède par récurrence sur m.
Initialisation : soit n et n' deux entiers tels que $0 + n = 0 + n'$. Par définition de l'addition, $0 + n = n$ et $0 + n' = n'$. Donc, $n = n'$.
Hérédité : soit m un entier tel que si n et n' sont deux entiers naturels vérifiant $m + n = m + n'$ alors $n = n'$. Soit deux entiers naturels N et N' tels que $s(m) + N = s(m) + N'$. Par définition de l'addition, $s(m) + N = s(m + N)$ et $s(m) + N' = s(m + N')$. Donc, $m + N$ et $m + N'$ sont deux entiers naturels qui ont le même successeur. Par l'axiome *(AP4)*, ils sont donc égaux : $m + N = m + N'$. Par l'hypothèse de récurrence, on en déduit que $N = N'$.
Conclusion : la proposition est vraie quelque soit les entiers m, n et n'. □

Proposition. — *L'addition vérifie les propriétés suivantese :*

1. *elle admet* 0 *comme élément neutre : pour tout entier naturel n, $0 + n = n + 0 = n$;*
2. *elle est* commutative*, c'est-à-dire que pour tout couple (m, n) d'entiers naturels, on a $m + n = n + m$;*
3. *elle est* associative *: pour tout triplet (m, n, p) d'entiers naturels, on a $(m + n) + p = n + (m + p)$.*

Démonstration. — 1. Par définition, on a pour tout entier naturel n, $0 + n = n$. Nous allons démontrer par récurrence sur n que pour tout entier naturel n on a $n + 0 = n$.

Pour $n = 0$, on doit démontrer $0 = 0 + 0$, ce qui est vrai. Soit alors n un entier naturel tel que $n = n + 0$ (Hypothèse de récurrence). On a alors $s(n) + 0 = s(n + 0)$ par construction.

Par l'hypothèse de récurrence, $n+0=n$, donc $s(n)+0=s(n)$. Ceci qui montre la propriété pour le successeur de n. Par récurrence, la propriété $\mathcal{P}(0)$ est donc vraie.

2. Notons $\mathcal{Q}(m)$ la propriété : pour tout entier naturel n, $m+n=n+m$. Démontrons là par récurrence

   Initialisation : La propriété $\mathcal{Q}(0)$ s'écrit : pour tout entier naturel n, on a $n+0=0+n$. Ceci vient d'être démontré.

   Hérédité : soit m un entier naturel tel que la propriété $\mathcal{Q}(m)$ soit vérifiée et montrons que la propriété est encore vraie pour le successeur de m. Si n est un entier naturel, soit $\mathcal{R}(n)$ la propriété $s(m)+n=n+s(m)$; nous allons encore la démontrer par récurrence sur n ! Initialisation : Si $n=0$, on a $s(m)+0=0+s(m)$ car $\mathcal{Q}(0)$ (appliquée à l'entier naturel $s(m)$) est vraie.
   Hérédité : Si la propriété $\mathcal{R}(n)$ est vraie, alors

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

   Ainsi, la propriété $\mathcal{R}(s(n))$ est vraie. Par récurrence, elle est donc vraie pour tout entier naturel n, ce qui démontre la propriété $\mathcal{Q}(s(m))$. Par récurrence, la propriété $\mathcal{Q}(m)$ est vraie pour tout entier naturel m. Autrement dit, l'addition est commutative.

3. On note, pour tout entier naturel n, $\mathcal{P}(n)$ l'assertion

$$\text{pour tous entiers } l \text{ et } m, \quad (n+m)+l=n+(m+l).$$

   On va procéder par récurrence sur n.
   Initialisation : Soit l et m deux entiers naturels. Par définition de l'addition, $(0+m)+l=l+m$ et $0+(m+l)=l+m$. L'assertion $\mathcal{P}(0)$ est donc vraie.
   Hérédité : Soit n un entier naturel tel que pour tous entiers naturels l et m, $(n+m)+l=n+(m+l)$. Soit L et M deux entiers naturels. Par définition de l'addition, $(s(n)+M)+L=s(n+M)+L=s((n+M)+L)$. Toujours par définition de l'addition, $s(n)+(M+L)=s(n+(M+L))$. Par hypothèse de récurrence appliquée à L et M, on peut donc conclure que $(s(n)+M)+L=s(n)+(M+L)$. D'où l'hérédité.
   Conclusion : l'addition des nombres entiers naturels est associative.

□

Pour construire la multiplication, on utilise le fait que pour multiplier n par m, on doit effectuer l'addition $n+n+\cdots+n$, m fois. On procède par récurrence sur m. Posons ainsi, pour tout entier naturel n, $0\times n=0$. Si $m\times n$ est défini, on définit alors $s(m)\times n$ par la formule

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

Noter que 1 est élément neutre pour la multiplication : pour tout entier naturel n, $1\times n=s(0)\times n=0\times n+n=0+n=n$. On démontre alors par récurrence la commutativité et l'associativité de la multiplication. On peut aussi montrer par récurrence sur l, que la multiplication est distributive par rapport à l'addition :

$$\text{pour tous entiers naturels } l,\ m \text{ et } n, \text{ on a} \quad l \times (m+n) = l \times m + l \times n.$$

Deux bases d'exercices disponibles en ligne
`http://wims.univ-rennes1.fr/`
`http://braise.univ-rennes1.fr/`