Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Ensemble $\mathbb{N}$ des entiers positifs

En mathématiques, tout le monde connaît l'ensemble $\mathbb{N}$ des *entiers naturels* 0, 1, 2, 3, 4, 5, 6, 7, $\ldots$ On dit que ces entiers sont « *naturels* », car leur existence semble tout à fait claire sur la Terre (souffrante) qui nous environne — notamment lorsque le professeur compte le nombre (entier) de copies d'examen de ses étudiants. Dans notre atmosphère de plus en plus enrichie en molécules de CO_2, les nombres entiers existent partout, c'est bel et bien certain !

Mais à partir de la fin du XIX$^{\text{ième}}$ siècle, les mathématiciens ont désiré renforcer l'autonomie des mathématiques en créant des théories abstraites qui ne reposeraient ni sur la physique, ni sur la chimie, ni sur la biologie, ou que sais-je encore, sur l'espionnage nanométré de milliards de smartphones.

Et dans les mathématiques contemporaines, ce sont les axiomes dits *de Peano* [1] qui sont actuellement considérés comme un fondement rigoureux pour l'ensemble des nombres entiers, au sein de la branche reine des mathématiques, l'Arithmétique.

1. Giuseppe Peano (1858–1932) était un mathématicien et linguiste italien. Pionnier de l'approche formaliste des mathématiques, il développa, parallèlement à l'Allemand Richard Dedekind, une axiomatisation de l'arithmétique.

Au début de 1889, Giuseppe Peano publie un livret d'à peine 36 pages où il introduit pour la première fois les « axiomes de Peano » sur la construction des nombres entiers naturels. Il l'intitule « *Arithmetices principa nova metodo expositan* », et ses résultats seront, en grande partie, rapidement adoptés par la communauté mathématique.

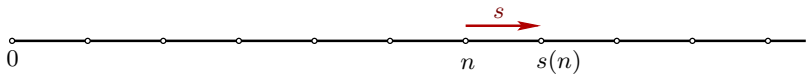
Dans le prolongement de sa contribution à l'axiomatique et à la logique symbolique, Peano formule un projet de langage logique universel grâce auquel il va pouvoir tout, ou presque, écrire et comprendre, avec son *Formulaire de mathématiques*. Les notations des mathématiques d'aujourd'hui doivent beaucoup à cet ambitieux projet de formalisation des mathématiques, écrit en français, que Peano conduit aidé de plusieurs de ses élèves, de 1895 à 1908.

À la fin de sa carrière, Peano finit par passer plus de temps à l'enseignement de ses notations originales, et à établir les définitions et concepts de base, qu'au programme d'enseignement qu'il devait traiter en face de ses étudiants. Convaincu des bénéfices de son formulaire et de ses symboles, Peano en vint même à exiger que les examens soient rédigés dans ce nouveau langage par ses étudiants !

Axiomes 2.1. [de Peano] Il existe un ensemble noté $\mathbb{N}$ contenant un élément distingué $0 \in \mathbb{N}$ appelé *zéro*, tel que $\mathbb{N}$ est muni d'une *application successeur :*

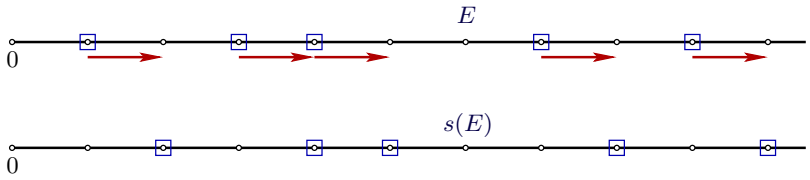
$$s\colon \quad \mathbb{N} \longrightarrow \mathbb{N},$$

laquelle vérifie les trois propriétés fondamentales suivantes.



(A1) 0 n'est le successeur d'aucun élément $n \in \mathbb{N}$, c'est-à-dire que $s(n) \neq 0$ pour tout $n \in \mathbb{N}$.

(A2) Deux nombres entiers m et n qui ont même successeur $s(m) = s(n)$ sont nécessairement égaux $m = n$, c'est-à-dire que l'application s est injective.



(A3) [Principe de récurrence] Si un sous-ensemble $E \subset \mathbb{N}$ contient $0 \in E$, et est *stable par* s, c'est-à-dire vérifie [2] :

$$s(E) \subset E,$$

alors en fait il remplit tout :

$$E = \mathbb{N}.$$

Les éléments de $\mathbb{N}$ sont appelés *entiers naturels* [3].

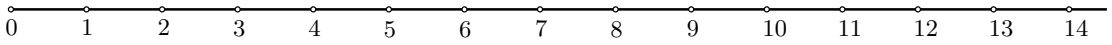
Parmi ces trois propriétés, la plus subtile et la plus importante, c'est **(A3)**, et nous y reviendrons dans quelques instants afin de justifier l'appellation « *Principe de récurrence* ».

Évidemment, il faut avoir à l'esprit que :

$$s(n) := n + 1,$$

et on pose :

$$1 := s(0), \qquad 2 := s(1), \qquad 3 := s(2), \qquad 4 := s(3), \qquad 5 := s(4), \qquad \ldots\ldots$$



Question 2.2. *Pourquoi formuler des axiomes ?*

2. Sur la figure illustrative au-dessus, on n'a *ni* $0 \in E$, *ni* $s(E) \subset E$.

3. On notera que ces axiomes ne disent pas véritablement comment construire $\mathbb{N}$. Heureusement, en théorie des ensembles, il est possible de construire $\mathbb{N}$ uniquement à partir de l'ensemble vide $\emptyset$, de la manière suivante : $0 := \emptyset$, puis $1 := \{\emptyset\}$ (l'ensemble dont l'unique élément est l'ensemble vide), puis :

$$2 := \big\{\emptyset,\, \{\emptyset\}\big\} = \{0, 1\},$$
$$3 := \Big\{\emptyset,\, \{\emptyset\},\, \big\{\emptyset,\, \{\emptyset\}\big\}\Big\} = \{0, 1, 2\}, \qquad \text{et ainsi de suite.}$$

De manière imagée, les axiomes doivent être envisagés comme des « règles du jeu », avant que ne débute le jeu véritable. Ce sont aussi des points de départ, des principes. Or les mathématiciens évoluent dans un monde essentiellement *incorporel*[4], et donc ils doivent impérativement créer et re-créer toutes les conséquences de leurs axiomes et de leurs principes, pour garantir que leur monde idéal existe véritablement.

Autrement dit, les axiomes vont servir de briques élémentaires pour de nombreuses démonstrations mathématiques. Notamment, il s'agira de *raisonner* avec logique, de *déduire* des conséquences, et de *démontrer* des résultats, tout cela, en prenant appui *seulement* sur les axiomes.

Nous pouvons donc commencer à décrire brièvement comment la théorie de Peano déduit *mathématiquement* toutes les propriétés évidentes ou connues des entiers naturels $n \in \mathbb{N}$.

Proposition 2.3. *Tout entier $a \neq 0$ est le successeur $a = s(c)$ d'un unique entier c.*

Démonstration. L'unicité de c est garantie par l'Axiome **(A2)**.

Pour ce qui est de l'existence de c, nous allons nous servir de l'Axiome crucial **(A3)**. Introduisons le sous-ensemble de $\mathbb{N}$:

$$E \,:=\, \{0\} \cup s(\mathbb{N}).$$

Premièrement, on a $0 \in E$. Deuxièmement, $E \subset \mathbb{N}$ implique $s(E) \subset s(\mathbb{N})$, et comme E contient visiblement $s(\mathbb{N})$, il vient :

$$s(E) \,\subset\, s(\mathbb{N}) \,\subset\, E.$$

Par conséquent, l'Axiome **(A3)** s'applique, il donne $E = \mathbb{N}$, et nous en déduisons que :

$$s(\mathbb{N}) \,=\, E \big\backslash \{0\} \,=\, \mathbb{N} \big\backslash \{0\}.$$

Si donc $a \in \mathbb{N}\backslash\{0\}$ est quelconque, cette égalité montre qu'il appartient aussi à $s(\mathbb{N})$, donc il existe bien $c \in \mathbb{N}$ tel que $s(c) = a$. □

Maintenant, définissons l'addition.

Proposition-Définition 2.4. [Addition] *Soit $n \in \mathbb{N}$. Il existe une application $m \longmapsto n+m$ de $\mathbb{N}$ dans $\mathbb{N}$ définie en posant :*

- $n + 0 := n$*;*
- $n + s(p) = s(n + p)$*, pour tout $p \in \mathbb{N}$.*

Cette application définit une opération sur $\mathbb{N}$, c'est-à-dire une application de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ qui, au couple (n, p) associe l'entier $n + p$.

Cette opération est appelée addition*, et l'entier $n + p$ est appelé* somme *de n et de p.*

Preuve résumée. Il s'agit de vérifier que l'ensemble E des entiers m pour lesquels cette application est définie est $\mathbb{N}$ tout entier. Comme E contient 0 et est stable par successeur, cela résulte de l'Axiome **(A3)**, *i.e.* du principe de récurrence. □

4. Les philosophes stoïciens estimaient qu'il y avait une différence entre les *principes* et les *éléments*. Les principes sont incréés et incorruptibles, tandis que les éléments se corrompent dans la conflagration. De plus, les principes sont incorporels et informes, tandis que les éléments sont pourvus d'une forme.

Grâce à cet énoncé, on a, par définition :

$$n+1 \;=\; n+s(0) \;=\; s(n+0) \;=\; s(n),$$

ce qui justifie pleinement notre intuition initiale que l'application de successeur $s(n)$ d'un entier n consiste à lui ajouter 1.

Cette observation permet de reformuler le principe de récurrence sous la forme la plus naturelle et la plus connue.

Théorème 2.5. [Principe de récurrence] *Soit $P(n)$ une propriété définie pour tout entier $n \in \mathbb{N}$. On suppose que :*

(1) Initialisation : *$P(0)$ est vraie ;*

(2) Hérédité : *$P(n)$ implique $P(n+1)$, quel que soit $n \in \mathbb{N}$.*

Alors $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Preuve résumée. Il suffit d'appliquer l'Axiome **(A3)** à l'ensemble E des entiers n qui vérifient la propriété $P(n)$. Les détails sont laissés en exercice (facile). □

À présent, les propriétés bien connues de l'addition peuvent être « dévoilées » comme *conséquences* des Axiomes **(A1)**, **(A2)**, **(A3)** de Peano.

Proposition 2.6. *Les quatre propriétés suivantes sont satisfaites.*

(1) Associativité de l'addition : *Pour tous $a, b, c \in \mathbb{N}$, on a $a+(b+c) = (a+b)+c$.*

(2) Commutativité de l'addition : *Pour tous $a, b \in \mathbb{N}$, on a $a+b = b+a$.*

(3) Règle de simplification : *Pour tous $a, b, c \in \mathbb{N}$, l'égalité $a+b = a+c$ implique $b = c$.*

(4) *Si $a+b=0$ est nul, alors $a=0$ et $b=0$ sont nuls.*

Attention ! En première approche, les étudiants sont invités à « sauter » la lecture de cette démonstration, et à reprendre la lecture à partir de « Sur notre route . . . ».

Démonstration concise. **(1)** On fixe $a, b \in \mathbb{N}$, et on applique le principe de récurrence à c. Soit E l'ensemble des c qui vérifient la propriété. On a $0 \in E$, car par définition $a+(b+0) = a+b$ et $(a+b)+0 = a+b$.

Ensuite, supposons que $c = s(p)$ soit le successeur d'un entier p, et que p vérifie l'associativité, *i.e* que $a+\big(b+p\big) = (a+b)+p$. Alors on calcule en appliquant la définition de l'addition :

$$\begin{aligned} a+(b+c) \;=\; a+\big(b+s(p)\big) \;=\; a+s(b+p) \;&=\; s\big(a+(b+p)\big) \\ \text{[Hypothèse de récurrence]} \qquad\qquad &= s\big((a+b)+p\big) \\ &= (a+b)+s(p) \\ &= (a+b)+c, \end{aligned}$$

pour constater que $c = s(p)$ vérifie encore l'associativité. On voit donc qu'on a bien $c \in E$, de sorte que E est stable par successeur, donc égal à $\mathbb{N}$, d'après l'Axiome **(A3)**.

(2) Commençons par établir deux lemmes.

Lemme 2.7. *Pour tout $a \in \mathbb{N}$, on a $a+0 = a = 0+a$.*

Indication de preuve. En partant de $0+0 = 0 = 0+0$, il suffit de raisonner par récurrence sur $a \in \mathbb{N}$. □

Lemme 2.8. *Pour tous $a, p \in \mathbb{N}$, on a $s(p)+a = s(p+a)$.*

On notera une différence d'ordre des termes à gauche, par rapport à l'identité connue $p + s(a) = s(p + a)$ de la Proposition-Définition 2.4.

Démonstration. On raisonne par récurrence sur $a \in \mathbb{N}$. Précisément, introduisons l'ensemble E des a qui vérifient $s(p) + a = s(p + a)$, pour tout $p \in \mathbb{N}$. Par définition de l'addition, 0 est dans E, c'est-à-dire $s(p) + 0 = s(p) = s(p + 0)$.

Soit $q \in E$. On a donc $s(p) + q = s(p + q)$, pour tout p. Montrons que $a := s(q)$ est aussi dans E, en calculant :

$$\begin{aligned} s(p) + a &= s(p) + s(q) \\ \text{[Définition de l'addition]} \qquad &= s\big(s(p) + q\big) \\ \text{[Hypothèse de récurrence]} \qquad &= s\big(s(p + q)\big) \\ \text{[Définition de l'addition]} \qquad &= s\big(p + s(q)\big) \;=\; s(p + a). \end{aligned}$$

Donc $E = \mathbb{N}$ grâce à l'Axiome **(A3)**. □

Nous pouvons maintenant prouver le point **(2)**. Raisonnons par récurrence sur b en introduisant l'ensemble E des $b \in \mathbb{N}$ qui vérifient la commutativité $a + b = b + a$ pour tout $a \in \mathbb{N}$. Grâce au Lemme 2.7, on a $0 \in E$

Supposons que $p \in E$ c'est-à-dire que $a+p = p+a$, et montrons $s(p) \in E$ en calculant :

$$a + s(p) \;=\; s(a + p) \;=\; s(p + a) \;=\; s(p) + a,$$

successivement : par définition ; par hypothèse de récurrence ; par le Lemme 2.8. Donc $s(p) \in E$, puis $E = \mathbb{N}$ grâce à **(A3)**, et cela termine **(2)**.

(3) Après commutation, ce point se montre par récurrence sur a (exercice).

(4) Ce dernier point est facile en raisonnant par l'absurde. Si, par exemple, b n'était pas égal à 0, par la Proposition 2.3, b serait successeur[5] $s(q) = b$ d'un q, d'où l'on déduirait par définition de l'addition :

$$0 \;=\; a + b \;=\; a + s(q) \;=\; s(a + q),$$

en contradiction avec l'Axiome **(A1)**, d'après lequel 0 n'est successeur de personne. □

Sur notre route, nous avons démontré, pour tout $a \in \mathbb{N}$, que :

$$1 + a \;=\; a + 1.$$

Mais le premier théorème vraiment important de l'arithmétique, que tous les écureuils connaissent, c'est : *deux et deux font quatre*, c'est-à-dire $2 + 2 = 4$. Et grâce à tout ce qui précède, nous pouvons le *démontrer* comme suit :

$$4 \;=\; s(3) \;=\; 3 + 1 \;=\; (2 + 1) + 1 \;=\; 2 + (1 + 1) \;=\; 2 + 2.$$

Parlons maintenant de la multiplication.

Proposition-Définition 2.9. *On définit une loi de multiplication sur $\mathbb{N}$, notée[6] $\cdot$, en posant :*

- $n \cdot 0 = 0$ *pour tout* $n \in \mathbb{N}$ *;*
- $n \cdot s(p) = (n \cdot p) + n$, *pour tout* $n \in \mathbb{N}$ *et tout* $p \in \mathbb{N}$.

Alors les sept propriétés suivantes sont satisfaites.

5. À ne pas confondre avec *cul*cesseur !

6. Parfois notée sans symbole opératoire lorsqu'il n'y a pas de risque de confusion, par exemple $n\,p$ au lieu de $n \cdot p$. La notation $n \times p$ apprise à l'école élémentaire sera très peu souvent utilisée.

(1) Associativité : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(2) Commutativité : $a \cdot b = b \cdot a$, *pour tous* $a, b \in \mathbb{N}$.

(3) Distributivité à gauche : $(a + b) \cdot c = a \cdot c + b \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(4) Distributivité à droite : $a \cdot (b + c) = a \cdot b + a \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(5) Élément neutre : $n \cdot 1 = n = 1 \cdot n$, *pour tout* $n \in \mathbb{N}$.

(6) Intégrité : $a \cdot b = 0$ *si et seulement si* $a = 0$ *ou* $b = 0$.

(7) Simplification : $a \cdot b = a \cdot c$ *avec* $a \neq 0$ *implique* $b = c$.

Indication de démonstration. Les preuves s'effectuent essentiellement par récurrence. Pour alléger ce cours polycopié, elles ne seront pas présentées en détail. □

3. Relation d'ordre sur les entiers naturels

Un aspect intuitif extrêmement important des nombres entiers, c'est qu'ils *croissent indéfiniment*, au fur et à mesure qu'on emploie l'application de successeur $s(\bullet)$. Il en découle que les entiers naturels $n \in \mathbb{N}$ peuvent être *ordonnés* d'une manière naturelle. Et la théorie de Peano est capable d'élaborer le concept d'*ordre* à partir des axiomes.

Définition 3.1. Soient deux entiers $p, q \in \mathbb{N}$. On dit que q *est supérieur ou égal à* p, et on écrit $q \geqslant p$, s'il existe $n \in \mathbb{N}$ tel que $q = n + p$.

On dit que q *est strictement supérieur à* p, et on écrit $q > p$, si on a $q \geqslant p$ avec de plus $q \neq p$.

Évidemment, on peut aussi définir les relations d'infériorité $\leqslant$ et d'infériorité stricte $<$, en écrivant $p \leqslant q$ si et seulement si $q \geqslant p$, ainsi que $p < q$ si et seulement si $q > p$.

Proposition 3.2. *La relation* $\geqslant$ *entre les entiers est une relation d'ordre, c'est-à-dire que pour tous* $p, q, r \in \mathbb{N}$*, elle satisfait les propriétés suivantes.*

(1) Réflexivité : *on a* $p \geqslant p$ *pour tout* $p \in \mathbb{N}$.

(2) Antisymétrie : *si* $q \geqslant p$ *et* $p \geqslant q$*, alors* $q = p$.

(3) Transitivité : *si* $r \geqslant q$ *et* $q \geqslant p$*, alors* $r \geqslant p$.

Indication de preuve. Cela résulte aussitôt des propriétés de l'addition (exercice). □

Voici maintenant des propriétés élémentaires connues qui seront extrêmement utiles dans de nombreuses démonstrations ultérieures de ce cours.

Proposition 3.3. **(1)** Ordre total : *Si* p, q *sont deux entiers quelconques, alors on a* $p \geqslant q$ *ou* $q \geqslant p$.

(2) Simplification : *Pour tous* $a, b, c \in \mathbb{N}$*, on a l'équivalence :* $a + b \geqslant a + c \iff b \geqslant c$.

(3) *Il n'existe pas d'entier* $n_* \in \mathbb{N}$ *tel que* $0 < n_* < 1$.

(4) *Il n'existe pas d'entier* $r^* \in \mathbb{N}$ *qui soit supérieur ou égal* $r^* \geqslant m$ *à tous les entiers* $m \in \mathbb{N}$.

(5) *Si* $q \geqslant p$*, alors* $n \cdot q \geqslant n \cdot p$*, pour tout* $n \in \mathbb{N}$.

À nouveau, les étudiants sont invités à « sauter » la lecture de cette démonstration. Mais ils doivent quand même se concentrer avec intensité pour construire leur compréhension intuitive de cette proposition.

Démonstration. **(1)** Pour p fixé, introduisons l'ensemble :

$$E_p := \big\{q \in \mathbb{N}\colon\ q \leqslant p \text{ ou } q \geqslant p\big\},$$

et montrons que cet ensemble E_p est égal à $\mathbb{N}$ tout entier, en utilisant l'Axiome **(A3)**. D'abord, 0 est dans E_p, car on a $0 \leqslant p$, c'est-à-dire $p \geqslant 0$, puisque par la Définition 3.1, on peut écrire $p = p + 0$

Ensuite, si q est dans E_p, deux cas sont à considérer.

Premier cas $q < p$. Autrement dit, $p = n+q$ avec $n \neq 0$, c'est-à-dire $n = s(m) = m+1$ avec $m \in \mathbb{N}$. On a alors $p = m + 1 + q = m + s(q)$, donc encore (par définition) $s(q) \leqslant p$. Ainsi, $s(q) \in E_p$.

Deuxième cas : $q \geqslant p$. Autrement dit $q = n + p$ avec $n \in \mathbb{N}$ par définition, donc $s(q) = q + 1 = n + 1 + p = (n + 1) + p$, et on a donc $s(q) \geqslant p$. Ainsi, $s(q) \in E_p$.

(2) Utiliser la définition de $\geqslant$ et la règle de simplification (laissé au lecteur).

(3) Par l'absurde, supposons qu'il existe un tel entier $0 < n_* < 1$. L'inégalité stricte $n_* < 1$ signifie par définition qu'il existe $p \neq 0$ avec $1 = n_* + p$. Comme p est non nul, il existe q tel que $p = s(q) = q + 1$, et on a donc $1 = n_* + q + 1$. Par simplification, on en déduit $0 = n_* + q$, donc $n_* = 0$ (et aussi $q = 0$) d'après la Proposition 2.6 **(4)**. Ceci contredit $0 < n_*$, et finit l'argumentation.

(4) Ce dernier point est aisé, en considérant r^* et son successeur (exercice).

(5) C'est une conséquence calculatoire (aussi laissée au lecteur) des définitions de $\cdot$ et de $\geqslant$. □

Au-delà de l'ensemble $\mathbb{N}$, on peut introduire le concept abstrait d'*ordre*.

Définition 3.4. Soit F un ensemble quelconque. Un *ordre partiel* sur F est une relation binaire, notée $\leqslant$, qui est réflexive, antisymétrique, et transitive :

(1) Réflexivité : $x \leqslant x$, pour tout $x \in F$;

(2) Antisymétrie : $x \leqslant y$ et $y \leqslant x$ impliquent $x = y$, pour tous $x, y \in F$;

(3) Transitivité : $x \leqslant y$ et $y \leqslant z$ impliquent $x \leqslant z$, pour tous $x, y, z \in F$.

L'ordre partiel $\leqslant$ est dit être un *ordre total* lorsque, de plus :

(4) Totalité : Deux éléments quelconques $x \in F$ et $y \in F$ sont toujours comparables, c'est-à-dire qu'on a $x \leqslant y$ ou $y \leqslant x$.

Il est clair que l'ordre $\leqslant$ sur $\mathbb{N}$ est total, d'après la Proposition 3.3 **(1)**.

Définition 3.5. Sur un ensemble F, un ordre $\leqslant$ est dit être un *bon ordre* si tout sous-ensemble non vide E de F possède un *plus petit élément*, c'est-à-dire un élément $m_* \in E$ tel que :

$$m_* \leqslant n \qquad (\forall\, n \in E).$$

Si $(F, \leqslant)$ est bien ordonné, alors $\leqslant$ est nécessairement un ordre total. En effet, l'ensemble $\{x, y\}$ possède un plus petit élément, donc on a $x \leqslant y$ ou $y \leqslant x$.

4. Élément minimal et élément maximal

Terminons cette présentation de l'ensemble $\mathbb{N}$ des entiers naturels par deux énoncés intuitivement évidents, mais qui possèderont une importance capitale dans les démonstrations ultérieures de la théorie arithmétique. La première assertion exprime que $\leqslant$ est un *bon ordre* sur $\mathbb{N}$.

Théorème 4.1. *Tout sous-ensemble non vide E contenu dans $\mathbb{N}$ possède un plus petit élément, c'est-à-dire un élément $m_* \in E$ tel que :*

$$m_* \leqslant n \qquad (\forall\, n \in E).$$

Il importe de faire remarquer ici que E peut tout à fait incorporer une infinité d'éléments.

Démonstration. Il revient au même de montrer que si E est un sous-ensemble de $\mathbb{N}$ qui n'a pas de plus petit élément, alors $E = \emptyset$ est vide.

Pour cela, introduisons la propriété :

$$P(n)\colon \quad i \notin E, \text{ pour tout } i \leqslant n.$$

Nous affirmons que $P(0)$ est vraie. Sinon, si $P(0)$ était fausse, *i.e.* si $i \in E$ pour au moins un $i \leqslant 0$, c'est-à-dire pour $i = 0$, d'où $0 \in E$, et alors 0 serait le plus petit élément de E, puisque 0 est le plus petit élément de $\mathbb{N}$.

Ensuite, supposons $P(n)$ et montrons $P(n+1)$. On sait qu'aucun des entiers $0, 1, \ldots, n$ n'est dans E, et il s'agit de voir que $n+1$ n'est pas non plus dans E. Mais sinon, si $n+1$ appartenait à E, il serait forcément le plus petit élément de E, contrairement à notre hypothèse.

Donc par récurrence, $P(n)$ est vraie pour tout $n \in \mathbb{N}$, donc $i \notin E$ pour tout $i \in \mathbb{N}$, donc $E = \emptyset$, ce qui termine l'argumentation. □

La deuxième assertion, au contraire, n'accepte pas une infinité d'éléments.

Théorème 4.2. *Tout sous-ensemble* fini *non vide E contenu dans $\mathbb{N}$ possède un plus grand élément, c'est-à-dire un élément $r^* \in E$ tel que :*

$$n \leqslant r^* \qquad (\forall\, n \in E).$$

Quand E possède un nombre *infini* d'éléments, la conclusion est en générale fausse — penser par exemple à $E := \mathbb{N}$, qui n'a *pas* de plus grand élément, d'après la Proposition 3.3 **(4)**.

Démonstration. Raisonnons par récurrence sur le cardinal $n := \mathsf{Card}\, E$ de E. Si $n = 1$, autrement dit s'il n'y a qu'un seul élément dans E, alors cet élément est bel et bien le plus grand !

Supposons que tout sous-ensemble E' de $\mathbb{N}$ de cardinal n possède un plus grand élément, et soit E contenu dans $\mathbb{N}$ de cardinal $n+1$. Grâce au Théorème 4.1, il existe un élément m_* qui est le plus petit parmi les éléments de E. Introduisons $E' := E \backslash \{m_*\}$. Comme $\mathsf{Card}\, E' = n$, l'hypothèse de récurrence s'applique, donc E' possède un plus grand élément, disons r^*, qui est évidemment aussi le plus grand élément de E. □

L'énoncé suivant, intéressant sur le plan logique, peut être laissé de côté en première lecture, car il ne sera pas utilisé dans la suite du cours.

Théorème 4.3. *Le principe de récurrence est équivalent à la propriété de bon ordre, c'est-à-dire qu'on a équivalence entre :*

(i) *$P(0)$ est vraie et $P(n) \Longrightarrow P(n+1)$ quel que soit n entraînent que $P(n)$ est vraie pour tout $n \in \mathbb{N}$;*

(ii) *Tout sous-ensemble E de $\mathbb{N}$ possède un plus petit élément.*

Démonstration. La démonstration du Théorème 4.1 a déjà fait voir l'implication **(i)** $\Longrightarrow$ **(ii)**, comme on peut s'en convaincre en la relisant.

Pour démontrer **(ii)** $\Longrightarrow$ **(i)**, on raisonne par l'absurde en supposant que $P(n)$ n'est pas vraie pour tous les entiers n, et on introduit l'ensemble des contre-exemples :

$$E \,:=\, \big\{n \in \mathbb{N} \colon\ P(n) \text{ n'est pas vraie}\big\}.$$

Ainsi, E est non vide.

Par conséquent, l'hypothèse **(ii)** garantit que E possède un plus petit élément m_*, qui est donc le contre-exemple minimal. On $m_* \neq 0$, car $P(0)$ est vraie par hypothèse. On considère alors $m_* - 1$, qui est encore dans $\mathbb{N}$, car $m_* > 0$, et qui est $< m_*$, donc n'est plus dans E, puisque m_* est le plus petit élément de E. Il s'ensuit que $P(m_* - 1)$ est vraie. Mais alors, comme on suppose que $P(n) \Longrightarrow P(n+1)$ quel que soit n, on doit forcément avoir que $P(m_*)$ est vraie, ce qui est une contradiction dans notre raisonnement.

En définitive, $E = \emptyset$ doit être vide, ce qui équivaut à **(i)** — terminé ! □

5. Anneau $\mathbb{Z}$ des entiers relatifs

L'ensemble $\mathbb{N}$ des entiers naturels, muni de l'addition, a un défaut : étant donné un entier quelconque $n \in \mathbb{N}$, il n'existe la plupart du temps *aucun* entier $m \in \mathbb{N}$ tel que :

$$n + m \,=\, 0.$$

Autrement dit, il n'existe pas d'opération *inverse* de l'addition.

À la fin du XIX$^{\text{ième}}$ siècle, les mathématiques abstraites et structurales, ont introduit la notion de *groupe commutatif*, que nous étudierons ultérieurement dans ce cours. Donnons-en toutefois la définition.

Définition 5.1. Un *groupe commutatif* est un ensemble G muni d'une relation binaire interne notée $(\bullet) * (\bullet)$ qui satisfait :

Associativité : $x * (y * z) = (x * y) * z$, pour tous $x, y, z \in G$;

Commutativité : $x * y = y * x$, pour tous $x, y \in G$;

Élément neutre : il existe un élément $e \in G$ tel que $e * x = x = x * e$, pour tout $x \in G$;

Existence d'un inverse : pour tout $x \in G$, il existe un unique élément $x' \in G$ tel que $x * x' = e = x' * x$.

Dans $\mathbb{N}$, l'opération $* \,=\, +$ est l'addition (commutative), l'élément neutre est $e = 0$. Mais *aucun* $n \in \mathbb{N}$ avec $n \neq 0$ n'admet un *inverse* n' pour l'addition, à savoir un n' satisfaisant $n + n' = 0 = n' + n$, à cause de la Proposition 2.6 **(4)**. Il s'agit là d'un défaut majeur de $\mathbb{N}$.

On a cependant une soustraction partielle.

Lemme 5.2. *Étant donné deux entiers $m, n \in \mathbb{N}$ avec $n \leqslant m$, il existe un unique entier p tel que $n + p = m$. On note alors $p = m - n$.*

Démonstration. Ceci est une reformulation de la Définition 3.1 même de la relation d'ordre ! □

L'objectif est maintenant de « plonger » $\mathbb{N}$ dans un ensemble plus « gros » $\mathbb{Z}$ pour lequel la soustraction $m - n$ entre deux entiers quelconques aura toujours un sens. La construction la plus naturelle de $\mathbb{Z}$ consiste simplement à adjoindre à tous les éléments $n \in \mathbb{N}$ leurs *opposés* $-n$. Autrement dit, à un entier, on va associer un signe.

On pose :

$$\mathbb{N}^* := \mathbb{N}\backslash\{0\} = \big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \dots\ \big\},$$

et on définit $\mathbb{Z}$ comme la réunion de $\mathbb{N}$ et d'une copie de $\mathbb{N}^*$, notée $-\mathbb{N}^*$:

$$\mathbb{Z} := -\mathbb{N}^* \cup \mathbb{N}.$$

Les éléments de $-\mathbb{N}^*$ seront notés $-n$, avec $n \in \mathbb{N}^*$. Pour le moment, ce signe $-$ est juste une notation formelle, car on n'a pas encore démontré qu'il correspond à l'opération *inverse* de l'addition.

On parlera des entiers de $\mathbb{N}$ comme des entiers *positifs*, et des entiers de $-\mathbb{N}^*$ comme des entiers *négatifs*.

Définition 5.3. La *valeur absolue* $|\bullet|$ d'un élément de $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ est :

- $|-n| := n$ pour tout $-n \in -\mathbb{N}^*$;
- $|n| := n$ pour tout $n \in \mathbb{N}$.

La définition de l'addition est alors bien naturelle et correspond bien à ce qu'on souhaite au final.

Définition 5.4. Sur $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$, on définit une addition comme suit.

- Pour $m, n \in \mathbb{N}$, la somme $m + n$ est prise au sens de $\mathbb{N}$.
- Pour $-m$ et $-n$ appartenant à $-\mathbb{N}^*$, on pose $(-m) + (-n) := -(m+n)$.
- Pour m dans $\mathbb{N}$ et $-n$ dans $-\mathbb{N}^*$, il y a deux sous-cas :

  ☐ lorsque $m < n$, d'où $n = m+p$ pour un entier unique p de $\mathbb{N}^*$, on pose $m+(-n) := -p = -(n-m)$.

  ☐ lorsque $m \geqslant n$, d'où $m+q = n$ pour un entier unique q de $\mathbb{N}$, on pose $m+(-n) := q$.
- Pour $-m$ dans $-\mathbb{N}^*$ et n dans $\mathbb{N}$, afin de définir $(-m) + n$, on procède de manière symétrique au cas précédent.

En réfléchissant sur ce dernier cas symétrique, on se convainc aisément (exercice de réflexion) que cette définition rend *commutative* l'addition $+$ dans $\mathbb{Z}$.

Théorème 5.5. *Muni de la loi $+$, l'ensemble $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ est un groupe commutatif, d'élément neutre $0 \in \mathbb{N}$, et dans lequel l'opposé, pour l'addition, d'un entier $n \in \mathbb{N}$ avec $n \neq 0$ est $-n \in -\mathbb{N}^*$, tandis que l'opposé de $-n$ est n.*

Cet énoncé justifie donc la notation $-n$, comme opposé de n, avec un signe $-$. Observons que $-(-n) = n$. Aux étudiants, il est conseillé de sauter la lecture de la démonstration, un peu aride et ardue.

Indication de démonstration. Seule l'associativité est non évidente, et nécessite de distinguer de nombreux cas. Il s'agit de montrer, pour tous $a, b, c \in \mathbb{Z}$, que l'on a $(a+b)+c = a+(b+c)$. Lorsque $a, b, c \in \mathbb{N}$, c'est l'associativité connue dans $\mathbb{N}$. Mais il y a des cas plus délicats.

Détaillons par exemple un cas « difficile », celui où a et b sont dans $\mathbb{N}$, tandis que $c = -d$ est dans $-\mathbb{N}^*$. Hélas, il faut encore distinguer trois sous-cas de figure.

(1) : $d \leqslant b$. On a donc $b = d+e$ avec $e \in \mathbb{N}$, et donc $e = b-d$, d'où aussi $a+b = d+(a+e)$, ce qui montre $d \leqslant a+b$. Par définition, on a :

$$a + (b + c) \ = \ a + (b - d) \ = \ a + e,$$

et il s'agit de faire voir que ceci est égal à $(a+b)+c=(a+b)-d$, autrment dit qu'on a $d+(a+e)=a+b$. Mais, vu l'égalité $b=d+e$, cela résulte des propriétés de l'addition dans $\mathbb{N}$.

(2) : $b<d\leqslant a+b$. Cette fois, on a $d=b+e$ et $a+b=d+f$, avec $e,f\in\mathbb{N}$. On en déduit $d+f=b+e+f=a+b$, d'où $a=e+f$, ce qui montre $e\leqslant a$. Alors on a $(a+b)+c=(a+b)+(-d)=f$ ainsi que $a+(b+c)=a+\big(b+(-d)\big)=a+(-e)=f$, d'où le résultat.

(3) : $a+b<d$. On a $d=a+b+e$, d'où $d-b=a+e$. On calcule alors $(a+b)+c=(a+b)+(-d)=-e$, puis $a+(b+c)=a+\big(b+(-d)\big)=a+\big(-(a+e)\big)=-e$.

Les autres cas se traitent de manière analogue, et nous nous dispenserons de les détailler. □

Ensuite, il s'agit de donner un sens à la multiplication dans $\mathbb{Z}$, *i.e.* de la *prolonger* de $\mathbb{N}$ à $\mathbb{Z}$.

Définition 5.6. La multiplication $a\cdot b$ entre deux éléments $a,b\in\mathbb{Z}$ est définie comme suit.

- Pour $a,b\in\mathbb{N}$, la multiplication $a\cdot b$ est prise au sens de $\mathbb{N}$.
- Pour $a\in\mathbb{N}$ et $b=-c$ dans $-\mathbb{N}^*$, on pose $a\cdot(-c):=-(a\cdot c)$.
- Symétriquement, pour $a=-c$ dans $-\mathbb{N}^*$ et $b\in\mathbb{N}$, on pose $(-c)\cdot b:=-(c\cdot b)$.
- Enfin, pour $a=-c$ dans $-\mathbb{N}^*$ et $b=-d$ dans $-\mathbb{N}^*$, on pose $(-c)\cdot(-d):=c\cdot d$.

De manière équivalente, la multiplication entre deux entiers est définie par la multiplication entre leurs valeurs absolues, et par la « *règle des signes* » :

□ $+$ fois $+$ égale $+$;

□ $+$ fois $-$ égale $-$;

□ $-$ fois $+$ égale $-$;

□ $-$ fois $-$ égale $+$.

Théorème 5.7. *Sur $\mathbb{Z}$, l'opération de multiplication $(\bullet)\cdot(\bullet)$ est associative, est commutative, a pour élément neutre 1, et est distributive à gauche et à droite par rapport à l'addition $(\bullet)+(\bullet)$.*

Autrement dit, la multiplication de $\mathbb{Z}$ hérite de toutes les propriétés dont elle jouissait sur $\mathbb{N}$, telles qu'énoncées dans la Proposition-Définition 2.9. À nouveau, il est conseillé de sauter la lecture de la démonstration.

Indication de démonstration. Pour toutes ces propriétés, il s'agit simplement d'effectuer une vérification directe, mais qui est parfois technique.

Contentons-nous de détailler un des cas nécessaires concernant la distributivité, en montrant la formule :

$$a\cdot\big(b+(-d)\big)\;=\;(a\cdot b)+\big(a\cdot(-d)\big),$$

où $a,b\in\mathbb{N}$ et $-d\in-\mathbb{N}^*$ sont quelconques. Hélas, il faut distinguer deux sous-cas.

(1) : $b<d$. On a donc $d=b+e$ avec $e\in\mathbb{N}$, d'où $a\cdot\big(b+(-d)\big)=a\cdot(-e)=-a\cdot e$. Mais on a par ailleurs $a\cdot d=a\cdot b+a\cdot e$, d'où le calcul conclusif :

$$a\cdot b+a\cdot(-d)\;=\;a\cdot b+(-a\cdot d)\;=\;-a\cdot e\;=\;a\cdot\big(b+(-d)\big).$$

(2) : $b \geqslant d$. On a donc $b = d + e$ avec $e \in \mathbb{N}$, d'où $b + (-d) = e$. Il s'agit de montrer :

$$a \cdot \big(b + (-d)\big) \;=\; a \cdot e \;\stackrel{?}{=}\; a \cdot b + \big(-(a \cdot d)\big),$$

ce qui revient à $a \cdot e + a \cdot b \stackrel{?}{=} a \cdot b$, et qui n'est autre que la distributivité (connue) dans $\mathbb{N}$. □

Quelle que soit la méthode employée pour construire $\mathbb{Z}$ et pour détailler tous les arguments des démonstrations, on obtient au final le résultat capital suivant.

Théorème 5.8. *Muni de ses deux lois* $(\bullet) + (\bullet)$ *d'addition et* $(\bullet) \cdot (\bullet)$ *de multiplication, l'ensemble* $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ *est un anneau commutatif.* □

Mais au fait — qu'entend-on ici par *anneau commutatif ?* Heureusement, les mathématiciens ont inventé la

Définition 5.9. [Anneau] Un *anneau commutatif* est un ensemble $\mathbb{A}$ muni de deux opérations internes, appelées *addition* et *multiplication*, notées en général $+$ et $\cdot$ (ou parfois $\times$), qui se comportent exactement comme celles $+$ et $\cdot$ de l'ensemble $\mathbb{Z}$ des entiers relatifs.

Plus précisément, toutes les conditions suivantes doivent être satisfaites.

Addition :

Associativité de l'addition : $a + (b + c) = (a + b) + c$, quels que soient $a, b, c \in \mathbb{A}$.

Commutativité de l'addition : $a + b = b + a$, quels que soient $a, b \in \mathbb{A}$.

Élément neutre pour l'addition : Il existe un élément spécial noté $0 \in \mathbb{A}$ satisfaisant $0 + a = a = a + 0$, quel que soit $a \in \mathbb{A}$.

Existence d'un inverse pour l'addition : Pour tout $a \in \mathbb{A}$, il existe un élément unique, noté $-a \in \mathbb{A}$, tel que $a + (-a) = 0 = (-a) + a$.

Multiplication :

Associativité de la multiplication : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

Commutativité de la multiplication : $a \cdot b = b \cdot a$, quels que soient $a, b \in \mathbb{A}$.

Élément neutre pour la multiplication : Il existe un élément spécial noté $1 \in \mathbb{A}$ satisfaisant $1 \cdot a = a = a \cdot 1$, quel que soit $a \in \mathbb{A}$.

Distributivité de la multiplication par rapport à l'addition :

Distributivité à gauche : $(a + b) \cdot c = a \cdot c + b \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

Distributivité à droite : $a \cdot (b + c) = a \cdot b + a \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

On parle alors de l'anneau commutatif $\big(\mathbb{A}, +, \cdot, 0, 1\big)$.

Il est important de faire observer qu'on ne demande *pas* ici l'existence d'un inverse pour la multiplication. D'ailleurs, dans $\mathbb{Z}$ lui-même, la plupart des nombres n'ont *pas* d'inverse multiplicatif, par exemple :

$$\frac{1}{25} \;=\; 0,04,$$

n'est *pas* un nombre entier !

La notion d'*anneau* est donc moins riche de structure que celle de *corps*.

Définition 5.10. [Corps] Un *corps* commutatif $\mathbb{K}$ est un anneau commutatif satisfaisant la condition supplémentaire suivante.

Existence d'un inverse pour la multiplication : Pour tout $x \in \mathbb{K}$, il existe un élément unique, noté $x^{-1} \in \mathbb{K}$, tel que $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Par exemple, l'ensemble $\mathbb{Q} = \left\{\frac{p}{q} :\ p \in \mathbb{Z},\ q \in \mathbb{N}_{\geqslant 1}\right\}$ des nombres *rationnels* est un corps. Mais dans ce chapitre, nous ne travaillerons qu'avec des *anneaux*, tels que $\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z}$ — à découvrir plus tard.

Il est temps maintenant d'introduire la relation d'ordre naturel sur $\mathbb{Z}$.

Définition 5.11. Étant donné deux entiers $m, n \in \mathbb{Z}$, on dit que $m \leqslant n$ est *inférieur ou égal* à n si $(-m) + n$ appartient à $\mathbb{N}$, et on dit que $m < n$ est strictement inférieur à n si on a de plus, $(-m) + n \geqslant 1$ — dans $\mathbb{N}$.

Comme sur $\mathbb{N}$, on peut aussi définir sur $\mathbb{Z}$ les relations duales de supériorité $\geqslant$ et de supériorité stricte $>$, lesquelles sont bien connues.

Nous ne détaillerons pas la démonstration de la proposition suivante, qui liste plusieurs propriétés de compatibilité entre les opérations algébriques et la relation d'ordre sur $\mathbb{Z}$. Les étudiants doivent vraiment apprendre et maîtriser cette proposition, car elle sera souvent utilisée dans les démonstrations du cours et dans les examens.

Proposition 5.12. [Importante] *Soient des entiers m, n, a, b, c, d dans $\mathbb{Z}$.*

(1) $m \geqslant 0$ *et* $n \geqslant 0$ *impliquent* $m + n \geqslant 0$ *et* $m \cdot n \geqslant 0$.

(2) $a \leqslant x \leqslant b$ *implique* $-b \leqslant -x \leqslant -a$.

(3) $a \leqslant x \leqslant b$ *et* $c \leqslant y \leqslant d$ *impliquent* $a + c \leqslant x + y \leqslant b + d$.

(4) $a \leqslant b$ *implique* $a + c \leqslant b + c$, *quel que soit le signe de* c.

(5) $0 \leqslant a \leqslant b$ *et* $0 \leqslant c$ *impliquent* $0 \leqslant a\,c \leqslant b\,c$.

(6) $0 \leqslant a \leqslant b$ *et* $c \leqslant 0$ *impliquent* $b\,c \leqslant a\,c \leqslant 0$ — *Attention ! a et b changent de place !*

(7) $a \in \mathbb{Z}$ *avec* $a \neq 0$ *implique* $|a| \geqslant 1$. □

Terminons cette présentation de l'anneau $\mathbb{Z}$ des entiers relatifs par trois énoncés qui sont des conséquences assez directes des Théorèmes 4.1 et 4.2.

Théorème 5.13. **(1)** *Tout sous-ensemble non vide* fini E *contenu dans $\mathbb{Z}$ possède un plus petit élément* et *un plus grand élément, c'est-à-dire deux éléments $m_* \in E$ et $r^* \in E$ avec $m_* \leqslant r^*$ tels que :*

$$m_* \leqslant n \leqslant r^* \qquad (\forall\, n \in E).$$

(2) *Tout sous-ensemble non vide* minoré E *de $\mathbb{Z}$, c'est-à-dire tel qu'il existe* $\mathrm{J} \in \mathbb{Z}$ *avec* $\mathrm{J} \leqslant n$ *pour tout $n \in E$, admet un plus petit élément $m_* \in E$, satisfaisant :*

$$m_* \leqslant n \qquad (\forall\, n \in E).$$

(3) *Tout sous-ensemble* majoré E *de $\mathbb{Z}$, c'est-à-dire tel qu'il existe* $\mathrm{K} \in \mathbb{Z}$ *avec* $n \leqslant \mathrm{K}$ *pour tout $n \in E$, admet un plus grand élément $r^* \in E$, satisfaisant :*

$$n \leqslant r^* \qquad (\forall\, n \in E).$$

Démonstration. Laissée au lecteur, sachant que le plus important est de se construire des *intuitions mentales et/visuelles* au sujet de **(1)**, **(2)**, **(3)**. □

6. Division à l'École élémentaire

Soit $\mathbb{Z}$ l'anneau des nombres entiers naturels positifs ou négatifs, et soit $\mathbb{N} = \mathbb{Z}_+ \subset \mathbb{Z}$ le sous-ensemble des entiers qui sont positifs.

Diviser *avec reste* un entier $a \geqslant 1$ par un entier $1 \leqslant b \leqslant a$ qui lui est inférieur, cela consiste à trouver un *quotient* entier $q \geqslant 0$ et un *reste* entier $r \geqslant 0$ tels que :

$$a \;=\; q\,b + r,$$

le quotient q étant maximal possible, de telle sorte que dans le reste r, on ne puisse plus extraire « du b » :

$$0 \leqslant r \leqslant b - 1.$$

Il est bien connu que diviser avec reste est toujours possible, le couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ étant alors déterminé de manière unique en partant de $a \geqslant 1$ et de b avec $1 \leqslant b \leqslant a$ quelconques.

Exemple 6.1. Comme à l'école élémentaire, soit à diviser $a = 126$ par $b = 35$:

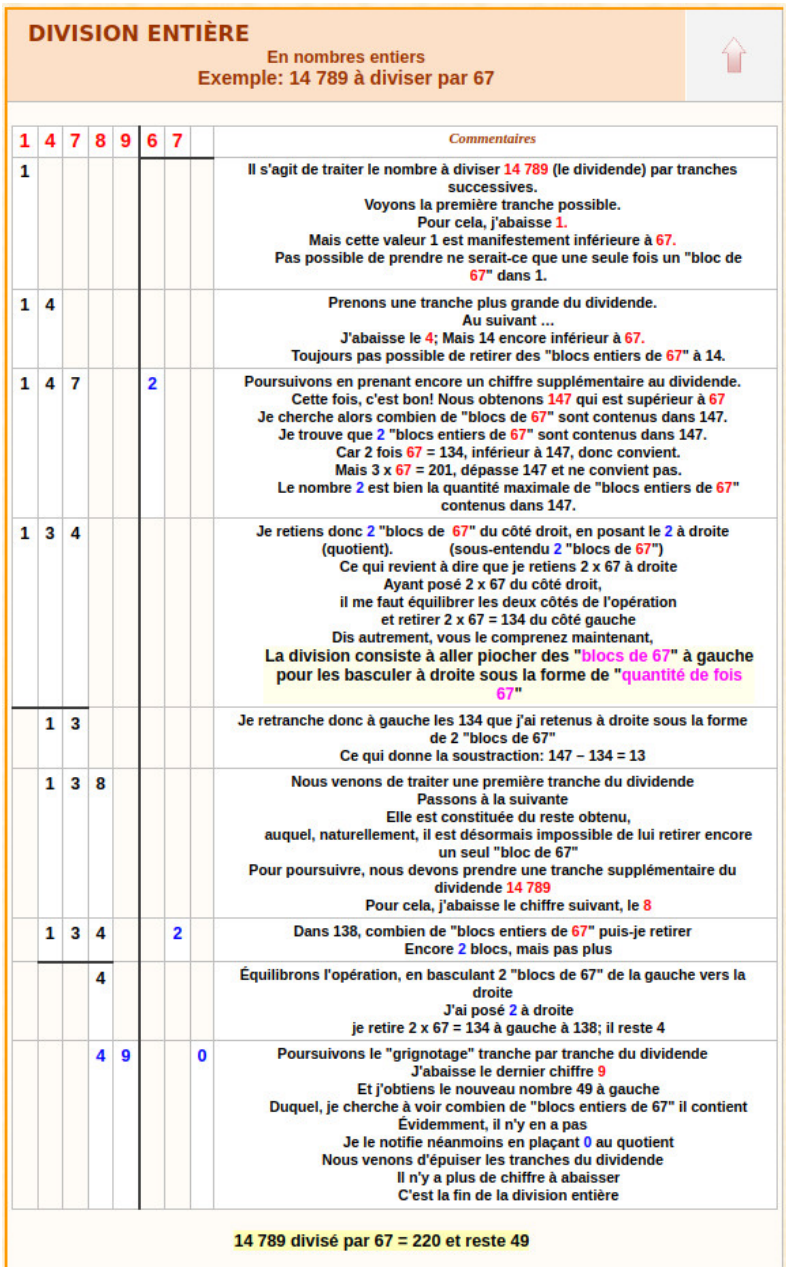
$$\begin{array}{r|l} 126 & 35 \\ \cline{2-2} -\,105 & 3 \\ 21 & \end{array}$$

Mentalement, on essaie de multiplier 35 successivement par 1, 2, 3, 4, et on trouve que $3 \times 35 = 105$ est le résultat maximum qui demeure inférieur à 126. On reporte alors $-\,105$ à gauche, on soustrait $126 - 105 = 21$, et on trouve :

$$\underbrace{126}_{a} \;=\; \underbrace{3}_{q} \cdot \underbrace{35}_{b} + \underbrace{21}_{r}.$$

Cet exemple s'inscrit dans un contexte général, connu depuis la Préhistoire sur Terre, sur Mars, sur Jupiter, sur Vénus, et sans doute aussi sur quelques exoplanètes dotées de mathématiques encore embryonnaires.

Voici un exemple plus élaboré.



DIVISION ENTIÈRE

En nombres entiers

Exemple: 14 789 à diviser par 67

1	4	7	8	9	6	7		*Commentaires*
1								Il s'agit de traiter le nombre à diviser 14 789 (le dividende) par tranches successives. Voyons la première tranche possible. Pour cela, j'abaisse 1. Mais cette valeur 1 est manifestement inférieure à 67. Pas possible de prendre ne serait-ce que une seule fois un "bloc de 67" dans 1.
1	4							Prenons une tranche plus grande du dividende. Au suivant ... J'abaisse le 4; Mais 14 encore inférieur à 67. Toujours pas possible de retirer des "blocs entiers de 67" à 14.
1	4	7			2			Poursuivons en prenant encore un chiffre supplémentaire au dividende. Cette fois, c'est bon! Nous obtenons 147 qui est supérieur à 67 Je cherche alors combien de "blocs de 67" sont contenus dans 147. Je trouve que 2 "blocs entiers de 67" sont contenus dans 147. Car 2 fois 67 = 134, inférieur à 147, donc convient. Mais 3 x 67 = 201, dépasse 147 et ne convient pas. Le nombre 2 est bien la quantité maximale de "blocs entiers de 67" contenus dans 147.
1	3	4						Je retiens donc 2 "blocs de 67" du côté droit, en posant le 2 à droite (quotient). (sous-entendu 2 "blocs de 67") Ce qui revient à dire que je retiens 2 x 67 à droite Ayant posé 2 x 67 du côté droit, il me faut équilibrer les deux côtés de l'opération et retirer 2 x 67 = 134 du côté gauche Dis autrement, vous le comprenez maintenant, **La division consiste à aller piocher des "blocs de 67" à gauche pour les basculer à droite sous la forme de "quantité de fois 67"**
	1	3						Je retranche donc à gauche les 134 que j'ai retenus à droite sous la forme de 2 "blocs de 67" Ce qui donne la soustraction: 147 – 134 = 13
	1	3	8					Nous venons de traiter une première tranche du dividende Passons à la suivante Elle est constituée du reste obtenu, auquel, naturellement, il est désormais impossible de lui retirer encore un seul "bloc de 67" Pour poursuivre, nous devons prendre une tranche supplémentaire du dividende 14 789 Pour cela, j'abaisse le chiffre suivant, le 8
	1	3	4			2		Dans 138, combien de "blocs entiers de 67" puis-je retirer Encore 2 blocs, mais pas plus
			4					Équilibrons l'opération, en basculant 2 "blocs de 67" de la gauche vers la droite J'ai posé 2 à droite je retire 2 x 67 = 134 à gauche à 138; il reste 4
			4	9			0	Poursuivons le "grignotage" tranche par tranche du dividende J'abaisse le dernier chiffre 9 Et j'obtiens le nouveau nombre 49 à gauche Duquel, je cherche à voir combien de "blocs entiers de 67" il contient Évidemment, il n'y en a pas Je le notifie néanmoins en plaçant 0 au quotient Nous venons d'épuiser les tranches du dividende Il n'y a plus de chiffre à abaisser C'est la fin de la division entière

14 789 divisé par 67 = 220 et reste 49

7. Divisibilité dans $\mathbb{Z}$

On commence par introduire une relation fondamentale entre les nombres entiers, quel que soit leur signe.

Définition 7.1. Soient deux entiers $a, b \in \mathbb{Z}$. On dit que a *divise* b s'il existe $u \in \mathbb{Z}$ tel que :

$$a\,u \;=\; b.$$

Dans ce cas, on dit que a *est un diviseur de* b, ou que b est un multiple de a. Cette propriété sera notée :

$$a \,|\, b.$$

Mais au fait, que se passe-t-il lorsque $a = 0$ ou $b = 0$? On sait qu'avec le nombre 0, il est souvent « aventureux », voire « interdit » de toucher au « bouton rouge » de la division !

En effet, avec $a = 0$ et pour $b \neq 0$, écrire que « 0 divise b », c'est-à-dire précisément que $0\,u = b$, semblerait impliquer que $u = \frac{b}{0}$ — Aïe ! On diviserait par 0 !

Observation 7.2. *Avec $b \in \mathbb{Z}$, la propriété $0 \mid b$ est impossible sauf lorsque $b = 0$.*

Démonstration. Avec $a = 0$, si $a\,u = b$, certainement $0\,u = 0 = b$. On confirme donc bien qu'un entier *non nul* $b \neq 0$ ne peut *jamais* être divisible par 0 — Ouf ! Toutes les mathématiques connues jusqu'à présent restent préservées et cohérentes ! □

Dans l'autre sens, tout se passe bien.

Observation 7.3. *On a toujours $a \mid 0$, quel que soit l'entier $a \in \mathbb{Z}$.*

Démonstration. Avec $b = 0$, il suffit de prendre $u := 0$ pour trouver effectivement $a\,0 = 0$. □

Heureusement, dans toutes les considérations qui suivront, nous n'aurons presque jamais à nous préoccuper de ces subtilités concernant les cas $a = 0$ et $b = 0$ dans le symbole binaire $a \mid b$. Presque toujours, lorsqu'on écrira $a \mid b$, il sera clair en fonction du contexte que $a \neq 0$ et $b \neq 0$.

Quelques exemples numériques simples de $a \mid b$:

$$2 \mid 4, \qquad 5 \mid -625, \qquad 17 \mid 323, \qquad -2 \mid 20,$$

semblent montrer que a est toujours plus petit que b. Mais il faut aussi tenir compte du fait que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ peuvent être négatifs. La valeur absolue doit intervenir, et pour un nombre réel $x \in \mathbb{R}$ quelconque, rappelons-en la définition :

$$|x| := \mathsf{max}\big\{-x,\ x\big\}.$$

Par exemple $|-19| = 19$. Intuitivement, la valeur absolue efface le signe $-$ des nombres négatifs.

Lemme 7.4. *Si $a \mid b$ avec $b \neq 0$, alors $|a| \leqslant |b|$.*

Démonstration. En effet, si $a \mid b$, il existe par définition $u \in \mathbb{Z}$ tel que $a\,u = b$. Comme b est non nul, u est non nul aussi — sinon, si $u = 0$ était nul, on aurait $a\,0 = 0 = b$. Comme u est un entier, on a $1 \leqslant |u|$, et donc :

$$\begin{aligned} |a| \;=\; |a| \cdot 1 \;&\leqslant\; |a| \cdot |u| \\ &=\; \big|a \cdot u\big| \\ &=\; |b|. \end{aligned}$$

□

Lemme 7.5. *Si $a \mid b$ et $b \mid a$, alors $b = \pm a$.*

Démonstration. Distinguons deux cas : $b = 0$, puis $b \neq 0$.

Premier cas : $b = 0$. On suppose donc $a \mid 0$ (toujours vrai) et $0 \mid a$. Mais nous venons de voir dans l'Observation 7.2 que cela force $a = 0$. Donc $a = 0 = b$, et on a bien $0 = \pm 0$.

Deuxième cas : $b \neq 0$, en supposant toujours $a \mid b$ et $b \mid a$. Autrement dit, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que :

$$a\,u = b \qquad \text{et} \qquad b\,v = a.$$

Mais alors, en multipliant la deuxième identité par u (en vert), on peut calculer :

$$\begin{aligned} &\big(b\,v = a\big)\,u \\ &b\,v\,u = a\,u = b, \end{aligned}$$

puis soustraire et factoriser :

$$b\,\big(v\,u-1\big)\;=\;0,$$

pour déduire ensuite, *puisque b est supposé non nul*, que :

$$v\,u\;=\;1.$$

En particulier, on en déduit que u et v sont tous deux non nuls. De plus, u et v doivent être de même signe, car $v\,u>0$.

Assertion 7.6. *On a $u=\pm 1$.*

Démonstration. Premier cas : u et v sont strictement positifs. Alors, comme ce sont des entiers, on a $u\geqslant 1$ et $v\geqslant 1$, d'où :

$$1\;\leqslant\;u\;\leqslant\;v\,u\;=\;1,$$

puis $u=1$ par encadrement entre deux gendarmes n°1.

Deuxième cas : u et v sont strictement négatifs. Alors $-u$ et $-v$ sont strictement positifs, satisfont aussi $(-v)(-u)=1$, donc le premier cas s'applique, et il donne $-u=1$, c'est-à-dire $u=-1$. □

En conclusion, puisque $u=\pm 1$, on a bien $a\,(\pm 1)=b$, ce qui était annoncé. □

Lemme 7.7. *Si $a\,|\,b$, alors pour tous entiers $k\in\mathbb{Z}$ et $\ell\in\mathbb{Z}$, on a aussi :*

$$a\,\Big|\,\big(k\,a+\ell\,b\big)$$

Démonstration. En effet, $a\,u=b$ implique que le nouveau nombre entier $B:=k\,a+\ell\,b$ est aussi multiple de a :

$$\begin{aligned}B\;=\;k\,a+\ell\,b\;&=\;k\,a+\ell\,a\,u\\&=\;a\,\big(\underbrace{k+\ell\,u}_{=:\,U\,\in\,\mathbb{Z}}\big),\end{aligned}$$

et cette égalité $a\,U=B$ exprime précisément que $a\,|\,B$. □

Même si cela paraît un peu stupide, observons que l'on a toujours :

$$a\,|\,a,$$

simplement parce que $a\,1=a$. Ensuite, énonçons la propriété de *transitivité* de la divisibilité.

Lemme 7.8. *Si $a\,|\,b$ et $b\,|\,c$, alors $a\,|\,c$.*

Démonstration. En effet :

$$\begin{aligned}\big(a\,u\;&=b\big)\,v\\b\,v\;&=\;c\end{aligned}\qquad\text{implique}\qquad a\,\underbrace{u\,v}_{=:\,w}\;=\;b\,v\;=\;c$$

et cette égalité $a\,w=c$ exprime précisément que $a\,|\,c$. □

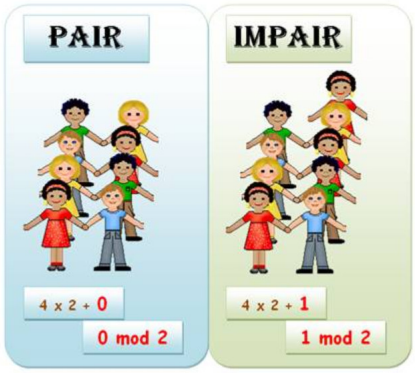
8. Idée de congruence et de périodicité dans le monde réel

Je connais ce domaine sans le savoir

Quand à l'école primaire vous avez fait connaissance avec les nombres pairs et impairs vous faisiez du calcul modulo 2 sans en connaître le nom.

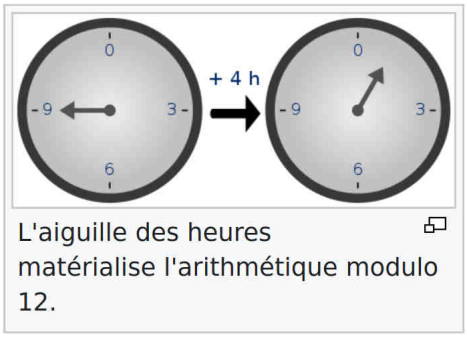
- un nombre pair est un nombre égal 0 modulo 2: divisé par 2 son reste est nul.
- un nombre impair est un nombre égal 1 modulo 2: divisé par 2 son reste est égal à 1.

Modulo est un mot qui signifie que l'on met en rang par 3, 4, ... n ...
En fait, une généralisation des nombres pairs et impairs.



8 est pair et 8 = 0 mod 2
9 est impair et 9 = 1 mod 2

Voici un autre exemple : l'« arithmétique de l'horloge », qui se réfère à l'« addition » des heures indiquées par la petite aiguille d'une horloge.



L'aiguille des heures matérialise l'arithmétique modulo 12.

Concrètement, si nous commençons à 9 heures et travaillons pendant 4 heures, alors plutôt que de terminer à 13 heures (comme dans l'addition normale), nous sommes à 1 heure. De la même manière, si nous commençons à minuit et nous attendons 7 heures trois fois de suite, nous nous retrouvons à 9 heures (au lieu de 21 heures).

Fondamentalement, quand nous atteignons 12, nous recommençons à zéro ; nous travaillons « *modulo 12* ». Pour reprendre l'exemple précédent, on dit que « *9 et 21 sont congrus modulo 12* ».

Les nombres 9, 21, 33, 45, *etc.* sont considérés comme égaux lorsqu'on travaille modulo 12.

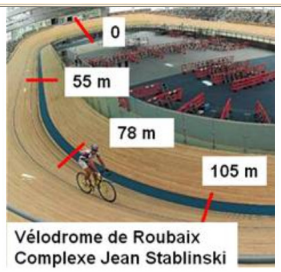
Plus généralement, l'« *arithmétique modulaire* » est un système arithmétique d'entiers modifiés, où les nombres sont « abaissés » lorsqu'ils atteignent une certaine valeur.

Imaginez un vélodrome avec un anneau de 250 m de long. Ce cycliste sait qu'en dix minutes il fait toujours un peu plus de vingt tours, mais il veut comparer ses records. Tous les jours, lorsque le chrono marque 10 minutes, il note de combien il dépasse: 55 m puis 78 m et aujourd'hui, c'est 105 m. Il vient de battre son record!

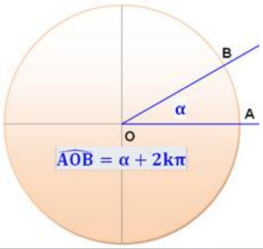
Ce cycliste fait un calcul en modulo sans le savoir.

En trigonométrie, seul l'angle sur le cercle compte. Le nombre tours que pourrait faire cet angle ne nous intéresse pas. Il peut tourner cent fois, mille fois ... on s'en fiche!

On dit que l'angle est connu à $2k\pi$ près; on aurait pu dire: modulo 2π.



Vélodrome de Roubaix
Complexe Jean Stablinski



En arithmétique, la congruence sur les entiers est une relation d'équivalence entre les entiers. Elle fut pour la première fois étudiée en tant que structure mathématique par le mathématicien allemand Carl Friedrich Gauss à la fin du XVIII$^{\text{ième}}$ siècle, dans un traité célèbre publié en 1801 et intitulé *Disquisitiones Arithmeticæ*. La congruence est aujourd'hui couramment utilisée en théorie des nombres, en algèbre générale, et en cryptographie.

C'est une arithmétique où l'on ne raisonne pas directement sur les nombres, mais sur leurs restes respectifs par la division euclidienne par un certain entier : le *module*.

9. Congruence modulo un entier

Définition 9.1. Soit un entier naturel $n \geqslant 1$. Deux entiers $a, b \in \mathbb{Z}$ sont dits *congrus modulo* n si leur différence $a - b$ est un multiple de n :

$$a \equiv b \mod n \quad \overset{\text{def}}{\Longleftrightarrow} \quad \exists\, k \in \mathbb{Z} \qquad a - b = k\,n,$$

ou, de manière équivalente, si $a - b$ est divisible par n :

$$n \mid a - b.$$

On notera que le symbole nouveau introduit ici avec trois traits horizontaux :

$$\equiv$$

est distinct du signe d'égalité $=$. Mais du point de vue définitionnel, ce symbole $\equiv$ de congruence repose sur le signe $=$ d'égalité :

$$\begin{array}{rl} \text{lire} & a \equiv b \mod n \\ \text{traduire} & a = b + k\,n \quad (\exists\, k \in \mathbb{Z}). \end{array}$$

Mentalement et intuitivement, il faudra toujours avoir à l'esprit qu'il existe toujours un « entier k caché » derrière le symbole $\equiv$. Et nous verrons bientôt pourquoi ce « k », il est très souvent préférable de le « cacher ».

Question 9.2. *Pourquoi ne pas définir la congruence $a \equiv b \bmod n$ aussi pour des entiers $n \leqslant -1$?*

On pourrait tout à fait définir la congruence avec un $n \leqslant -1$, mais comme :

$$a - b = k\,n \qquad \Longleftrightarrow \qquad a - b = (-k)\,(-n),$$

on aurait l'équivalence :

$$a \equiv b \bmod n \qquad \Longleftrightarrow \qquad a \equiv b \bmod (-n),$$

et donc, la congruence modulo un $n \leqslant -1$ se ramènerait à la congruence modulo $-n \geqslant 1$.

Question 9.3. *Pourquoi ne pas définir aussi la congruence modulo $n = 0$?*

Si, cela aurait du sens ! Mais cela serait inutile, car on retrouverait la notion connue d'égalité :

$$a - b = k\,0 = 0 \qquad \Longleftrightarrow \qquad a = b.$$

En définitive, dans la Définition 9.1, il est justifié de prendre des entiers $n \geqslant 1$.

Question 9.4. *À quoi ressemble la congruence modulo un entier n lorsque $n = 1$?*

Avec $n = 1$, par définition, deux entier $a, b \in \mathbb{Z}$ sont congrus modulo 1 s'il existe $k \in \mathbb{Z}$ tel que :

$$a - b = k \cdot 1.$$

Mais il suffit alors de prendre $k := a - b$ pour satisfaire cette égalité ! Donc deux entiers a et b quelconques sont toujours congrus entre eux modulo 1 ! Incroyable ! En particulier, tout entier a est congru à 0 modulo 1 :

$$a - 0 = a \cdot 1 \qquad \text{(prendre } k := a\text{)}.$$

Fait 9.5. [Peu intéressant] *Modulo $n = 1$, tous les entiers $a, b, c, d, e, \cdots \in \mathbb{Z}$ sont congrus entre eux, et congrus à 0.* □

Par conséquent, la notion de congruence modulo un entier n ne commence à être intéressante que pour $n \geqslant 2$.

D'ailleurs pour $n = 2$, par définition, deux entiers $a, b \in \mathbb{Z}$ sont congrus modulo 2 s'il existe $k \in \mathbb{Z}$ tel que :

$$a - b = k \cdot 2.$$

Et comme $2\,k \in 2\,\mathbb{Z}$ est un nombre *pair*, a et b sont congrus modulo 2 si et seulement si ils sont tous les deux pairs, ou tous les deux impairs. En base 10, comment fait-on pour différencier les nombres impairs des nombres pairs (de chaussettes) ?

Ensuite, au-delà de $n = 2$, voici deux exemples simples. Modulo 3, on a :

$$35 \equiv 2 \mod 3 \qquad \text{car} \qquad 35 = 2 + 11 \cdot 3.$$

Modulo 7, on a :

$$26 \equiv 12 \mod 7 \qquad \text{car} \qquad 26 - 12 = 2 \cdot 7.$$

Proposition 9.6. *Pour tout entier $n \geqslant 1$, et tout entier relatif $a \in \mathbb{Z}$, on a :*

$$a \equiv 0 \mod n \qquad \Longleftrightarrow \qquad a \text{ est multiple de } n.$$

Démonstration. En effet, $a - 0 = k\,n$ si et seulement si $a = k\,n$. □

La proposition suivante est importante, elle montre que le symbole binaire $\bullet \equiv \bullet \mod n$ se comporte comme l'égalité $\bullet = \bullet$.

Proposition 9.7. *Pour tout entier $n \geqslant 1$, la relation binaire $\bullet \equiv \bullet \mod n$ est une relation d'équivalence.*

(1) Réflexivité : $a \equiv a \mod n$, *quel que soit* $a \in \mathbb{Z}$.

(2) Symétrie : $a \equiv b \mod n$ *équivaut à* $b \equiv a \mod n$, *quels que soient* $a, b \in \mathbb{Z}$.

(3) Transitivité : $a \equiv b \mod n$ *et* $b \equiv c \mod n$ *entraîne* $a \equiv c \mod n$, *quels que soient* $a, b, c \in \mathbb{Z}$.

Démonstration. **(1)** Il est clair que $a - a = 0 = 0\,n$, avec $k = 0$.

(2) On a :

$$a - b = k\,n \qquad \Longleftrightarrow \qquad b - a = (-k)\,n.$$

(3) Effectivement :

$$\begin{aligned} a - b &= k\,n, \\ b - c &= \ell\,n, \end{aligned}$$

impliquent par addition verticale :

$$a - \underline{b}_{\circ} + \underline{b}_{\circ} - c = (k + \ell)\,n, \qquad \text{c'est-à-dire} \qquad a - c = j\,n. \qquad \square$$

On voit bien que l'entier k dans la Définition 9.1 change, puisqu'il devient ici $j := k + \ell$.

Une autre proposition importante garantit une *compatibilité* de la congruence $\bullet \equiv \bullet \mod n$ avec les opérations d'addition et de multiplication, c'est-à-dire de *compatibilité* avec la structure d'*anneau* de $\big(\mathbb{Z}, +, \times\big)$. Juste avant d'exposer de nombreux exemples concrets, intuitifs, et instructifs, cette compatibilité nous permettra de définir les *anneaux quotients* $\mathbb{Z}\big/n\mathbb{Z}$, qui constituent les domaines fondamentaux de l'*arithmétique modulaire*.

Proposition 9.8. *Pour tout entier $n \geqslant 1$ et tous entiers relatifs $a, b, a', b' \in \mathbb{Z}$ avec :*

$$\begin{aligned} a &\equiv b \mod n, \\ a' &\equiv b' \mod n, \end{aligned}$$

on a :

$$\begin{aligned} a + a' &\equiv b + b' \mod n, \\ a \cdot a' &\equiv b \cdot b' \mod n. \end{aligned}$$

Démonstration. En effet :

$$\begin{aligned} a &= b + k\,n, \\ a' &= b' + k'\,n, \end{aligned}$$

impliquent par addition et par multiplication verticales :

$$\begin{aligned} a + a' &= b + b' + (k + k')\,n, \\ a\,a' &= (b + k\,n)\,(b' + k'\,n) = b\,b' + \big(b\,k' + k\,b' + k\,k'\,n\big)\,n. \end{aligned}$$

À nouveau, l'entier k de la Définition 9.1 *change de visage*, il devient $k+k'$ pour l'addition, et $bk' + kb' + kk'n$ pour la multiplication. □

Et justement nous allons comprendre au fur et à mesure de notre progression que tout l'intérêt du calcul arithmétique modulo n est d'« oublier » volontairement ces entiers k qui peuvent devenir de plus en plus compliqués.

Théoriquement, on devrait employer des notations spécifiques pour l'addition et la multiplication modulo n, par exemple :

$$\overset{\text{mod}}{+} \qquad \text{et} \qquad \overset{\text{mod}}{\times},$$

mais pour des raisons de simplicité, tous les mathématiciens ré-utilisent la même notation $+$ et $-$ que dans $\mathbb{Z}$, en conservant à l'esprit que leur sens devient différent dans $\mathbb{Z}\backslash n\,\mathbb{Z}$, *i.e.* quand on travaille modulo n.

Ainsi en travaillant par exemple modulo 6, on écrira $3 + 2 \equiv 5 \mod 6$, et aussi $4 + 2 \equiv 0 \mod 6$, car la somme de 4 et 2 est égale à $1 \cdot 6$.

Modulo $n = 6$, on peut alors construire les deux tables d'opérations suivantes.

Table d'addition dans $\mathbb{Z}/6\mathbb{Z}$

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

10. Anneaux $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$

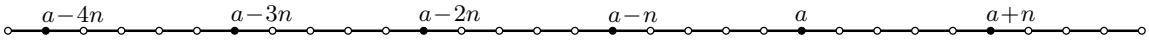
Nous pouvons maintenant introduire les domaines fondamentaux de l'arithmétique modulaire : les anneaux $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$. Quelques préliminaires s'avèrent nécessaires.

Proposition 10.1. *On fixe un entier $n \geqslant 2$. Alors modulo n, pour tout entier $a \in \mathbb{Z}$, il existe un entier a' tel que :*

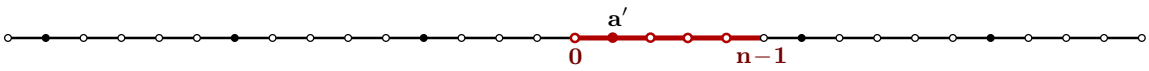
(1) $0 \leqslant a' \leqslant n - 1$*;*

(2) $a \equiv a' \mod$.

Autrement dit, tout entier relatif est toujours congru modulo n à au moins un entier $a' \in \big\{0, 1, 2, \ldots, n-2, n-1\big\}$.



Intuitivement, l'ensemble de tous les entiers $a' = a + k\,n$ congrus à a modulo n se représente comme une suite doublement infinie d'entiers situés à distance n l'un de l'autre.



L'intervalle entier :

$$[\![0,\, n-1]\!] = \{0, 1, 2, \ldots, n-2, n-1\},$$

étant de longueur (entière) égale à n, il existe forcément un nombre $a' = a + k\,n$ qui « tombe » dans cette « marmite » $[\![1, n-1]\!]$.

Démonstration. Donnons des arguments directs, simples, intuitifs. Pour tout entier $\mathrm{M} \in \mathbb{Z}$, l'entier $a + \mathrm{M}\,n$, est congru à a modulo n. En prenant $\mathrm{M} \gg 1$ positif assez grand, on peut garantir que $a + \mathrm{M}\,n \geqslant 0$. Donc on peut supposer depuis le début que $a \geqslant 0$.

Si $0 \leqslant a \leqslant n-1$, alors $a' := a$ convient.

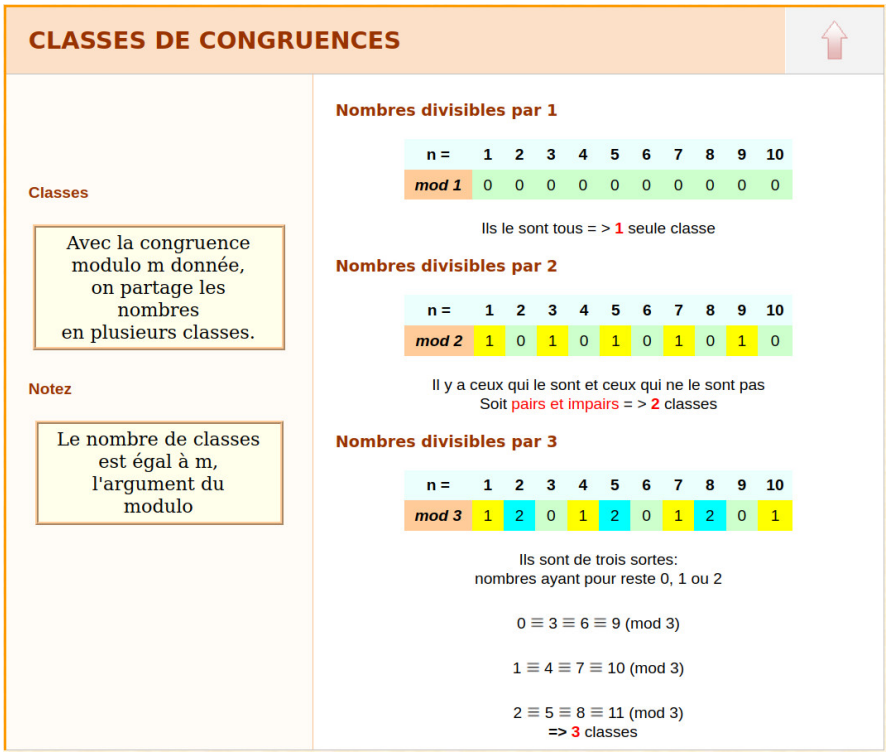
Sinon, $n \leqslant a$. Alors $a_1 := a - n$ est congru à a modulo n, et satisfait $0 \leqslant a_1$. Si $0 \leqslant a_1 \leqslant n-1$, alors $a' := a_1$ convient.

Sinon, $n \leqslant a_1$. Alors $a_2 := a_1 - n = a - 2\,n$ est congru à a modulo n, et satisfait $0 \leqslant a_2$. Si $0 \leqslant a_2 \leqslant n-1$, alors $a' := a_2$ convient.

Et ainsi de suite.

Puisque la suite $a_2 = a - 2\,n$, puis $a_3 = a - 3\,n$, *etc.*, tend vers $-\infty$, on ne peut pas toujours avoir $n \leqslant a_k = a - 2\,k$, et donc, il y a forcément un moment où $a' = a - 2\,k$, avec un certain $k \geqslant 0$, satisfera $0 \leqslant a' \leqslant n-1$. Cela achève la démonstration. □

Cette Proposition 10.1 importante sera aussi une conséquence de la division euclidienne classique, dont nous verrons plus tard une version élaborée dans la Section **17**.



Ensuite, il est intuitivement clair qu'à tout entier $a \in \mathbb{Z}$ est associé un *unique* entier $a' \equiv a \mod n$ avec $a' \in \{0, 1, 2, \ldots, n-2, n-1\}$.

Proposition 10.2. *On fixe un entier $n \geqslant 2$. Alors modulo n, les entiers :*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-2, \quad n-1,$$

sont mutuellement distincts, i.e. *aucun n'est congru à un autre.*

Démonstration. Soient donc deux tels entiers a et a' *distincts*, *i.e.* $a \neq a'$, avec :

$$\begin{aligned} 0 \leqslant a \leqslant n-1, \\ 0 \leqslant a' \leqslant n-1. \end{aligned}$$

En multipliant la deuxième ligne par -1, le sens des inégalités s'inverse (ou la gauche s'échange avec la droite) :

$$\begin{aligned} 0 \leqslant \quad a \leqslant n-1, \\ -(n-1) \leqslant -a' \leqslant 0. \end{aligned}$$

Ensuite, par addition verticale, on obtient :

$$-(n-1) \leqslant a - a' \leqslant n-1,$$

et enfin en prenant la valeur absolue :

$$|a - a'| \leqslant n-1. \tag{10.3}$$

Raisonnons par l'absurde. Si a et a' étaient congrus l'un à l'autre modulo n, c'est-à-dire si on avait :

$$a - a' = k \cdot n,$$

pour un certain entier $k \in \mathbb{Z}$, alors k serait non nul car on suppose $a \neq a'$, donc on aurait $|k| \geqslant 1$, donc en prenant la valeur absolue, on aurait :

$$\begin{aligned} |a - a'| &= |k| \cdot n \\ &\geqslant 1 \cdot n, \end{aligned}$$

ce qui contredirait (10.3). En conclusion, deux entiers distincts :

$$a, a' \in \{0, 1, 2, \ldots, n-2, n-1\}$$

ne peuvent jamais être congrus l'un à l'autre modulo n. □

Définition 10.4. L'ensemble « quotient [7] » de $\mathbb{Z}$ par la relation d'équivalence :

$$a \sim b \qquad \Longleftrightarrow \qquad a \equiv b \mod n,$$

sera noté :

$$\mathbb{Z}/n\mathbb{Z}.$$

La *classe d'équivalence* d'un entier $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, sera notée :

$$\overline{a} := \{a' \in \mathbb{Z} : \ a' \equiv a \mod n\}.$$

7. Cette notion mathématique quelque peu abstraite sera définie en détail ultérieurement dans un cadre très général.

On peut alors définir l'addition et la multiplication entre classes par :

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b}, \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b}, \end{aligned}$$

puis on peut vérifier, en utilisant la Proposition 9.8, que tout cela a du sens, mais ce point de vue n'est pas très pratique, car avec chaque classe $\overline{a}$, on manipule en fait simultanément une infinité de nombres $a' = a + k\,n$ congrus à a modulo n. Avec un unique symbole tel que $\overline{a}$, on préfèrerait en fait manipuler un seul objet à la fois, simple et concret.

Heureusement, il existe un meilleur point de vue. Grâce à la Proposition 10.1 et à la Proposition 10.2, nous savons qu'il existe une application de « *projection* » :

$$\begin{aligned} \pi\colon \quad \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ a &\longmapsto \text{unique } a' \in \big\{0,\, 1,\, 2,\, \ldots,\, n-2,\, n-1\big\} \\ &\qquad \text{tel que } a' \equiv a \mod n. \end{aligned}$$

On peut donc :

identifier $\quad \mathbb{Z}/n\mathbb{Z} \quad$ à $\quad \big\{0,\, 1,\, 2,\, \ldots,\, n-2,\, n-1\big\} \mod n.$

De plus, grâce à la Proposition 9.8, nous pouvons écrire pour tous $a, b \in \mathbb{Z}$:

$$\begin{aligned} \pi\big(a+b\big) &= \pi\big(\pi(a) + \pi(b)\big), \\ \pi\big(a \cdot b\big) &= \pi\big(\pi(a) \cdot \pi(b)\big), \end{aligned}$$

ce que nous pouvons expliquer concrètement au moyen des deux recettes suivantes concernant l'addition et la multiplication entre deux nombre quelconques :

$$a,\, b \,\in\, [\![0,\, n-1]\!] \,=\, \mathbb{Z}/n\mathbb{Z}.$$

Recette 10.5. [Addition dans $\mathbb{Z}/n\mathbb{Z}$] *Faire l'addition classique $a + b$ dans $\mathbb{Z}$, puis soustraire $a + b - k \cdot n$ avec le bon entier k pour « tomber » dans l'intervalle $[\![0, n-1]\!]$.*

L'opération de projection $\pi(\bullet)$, c'est justement la soustraction du bon multiple $k \cdot n$ de n à chaque étape de calcul. Pour additionner comme nous l'avons écrit plus haut, il faut d'ailleurs soustraire le bon $k \cdot n$ *trois fois*, d'abord pour avoir $\pi(a)$ et $\pi(b)$ dans $[\![0,\, n-1]\!]$, puis surtout, il faut ré-appliquer la projection $\pi\big(\pi(a) + \pi(b)\big)$, car l'addition $\pi(a) + \pi(b)$ peut « faire sortir de la marmite » $[\![0,\, n-1]\!]$.

Par exemple, avec $n := 17$, de telle sorte que :

$$\mathbb{Z}/17\mathbb{Z} \,=\, \big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16\big\} \mod 17,$$

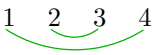
si on veut additionner $7 + 13 = 20$, en soustrayant $1 \cdot 17$ on trouve $20 - 1 \cdot 17 = 3$ qui appartient bien à $[\![0, 16]\!]$, et donc :

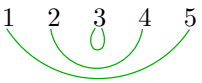
$$7 + 13 \,=\, 3 \qquad \text{(dans } \mathbb{Z}/17\mathbb{Z}\text{)}.$$

Parfois, on « reste dans la marmite » :

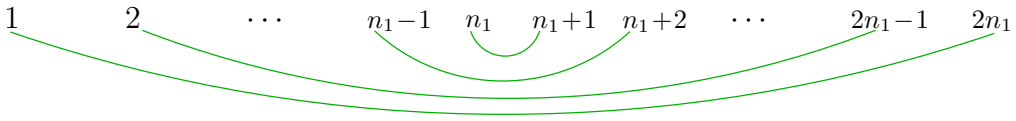
$$2 + 3 \,=\, 5 \qquad \text{(dans } \mathbb{Z}/17\mathbb{Z}\text{)}.$$

Pour l'addition, chaque élément $a \in \mathbb{Z}/n\mathbb{Z}$ possède l'inverse $a' := n - a$, puisque $a + (n - a) \equiv 0 \mod n$. On peut représenter les paires d'inverses additifs modulo n, d'abord dans $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$, puis dans $\mathbb{Z}/6\,\mathbb{Z}$:

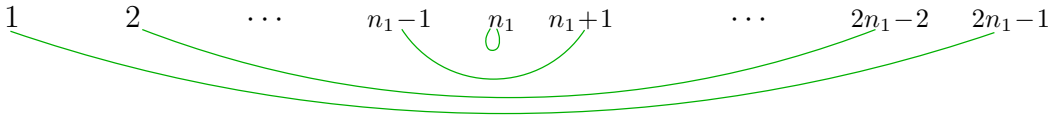




D'ailleurs, cette belle symétrie est valable généralement. Quand $n = 2\,n_1 + 1$ est *impair*, on peut représenter les paires d'inverses additifs comme suit :



et quand $n = 2\,n_1$ est pair, comme suit :



En revanche, pour la multiplication $\times$, il existe en général des éléments $a \in \mathbb{Z}/n\mathbb{Z}$ qui n'ont *pas* d'inverse multiplicatif.

*	**[0]**	**[1]**	**[2]**	**[3]**
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

En effet, la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$ montre par exemple qu'*aucun* nombre $a' \bmod 4$ ne parvient à faire que $2 \times a' \equiv 1 \bmod 4$.

Recette 10.6. [Multiplication dans $\mathbb{Z}/n\mathbb{Z}$] *Faire la multiplication classique $a \cdot b$ dans $\mathbb{Z}$, puis soustraire $a \cdot b - \ell \cdot n$ avec le bon entier ℓ pour « tomber » dans l'intervalle $[\![0, n-1]\!]$.*

La même nécessité d'appliquer plusieurs fois $\pi(\bullet)$ concerne aussi la multiplication. Par exemple, toujours $n := 17$, puique l'on a dans $\mathbb{Z}$:

$$7 \cdot 13 \;=\; 91 \;=\; 6 + 5 \cdot 17,$$

il vient :

$$7 \cdot 13 \;=\; 6 \qquad \text{(dans } \mathbb{Z}/17\mathbb{Z}\text{)}.$$

Afin de différencier les nombres dans $\mathbb{Z}$ des nombres dans $\mathbb{Z}/n\mathbb{Z}$, certains auteurs mettent une barre au-dessus des nombres, par exemple en écrivant :

$$\mathbb{Z}/17\mathbb{Z} \;=\; \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8},\ \overline{9},\ \overline{10},\ \overline{11},\ \overline{12},\ \overline{13},\ \overline{14},\ \overline{15},\ \overline{16}\} \bmod 17,$$

de telle sorte :

$$\overline{7} + \overline{13} \;=\; \overline{3},$$
$$\overline{7} \cdot \overline{13} \;=\; \overline{6},$$

mais nous préférons ne mettre aucun signe supplémentaire, tout en précisant bien le domaine, $\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z}$, dans lequel on effectue les calculs.

Corollaire 10.7. *On a :*

$$\mathsf{Card}\,\mathbb{Z}/n\mathbb{Z} \;=\; n.$$

Démonstration. En effet, il y a précisément n nombres dans l'ensemble $\{0,\ 1,\ 2,\ \ldots,\ n-2,\ n-1\}$ de tous les $\pi(\bullet)$ possibles modulo n. □

En résumé, pour tout entier $n \geqslant 1$, le quotient :

$$\begin{aligned}\big(\mathbb{Z}/n\mathbb{Z},\ +,\ \times\big) &= \mathbb{Z} \text{ modulo } n\,\mathbb{Z} \\ &= \big\{0,\ 1,\ 2,\ 3,\ \ldots,\ n-1,\ n-1\big\} \bmod n\end{aligned}$$

représente l'ensemble des nombres entiers $a \in \mathbb{Z}$ identifiés lorsqu'ils diffèrent d'un multiple de n :

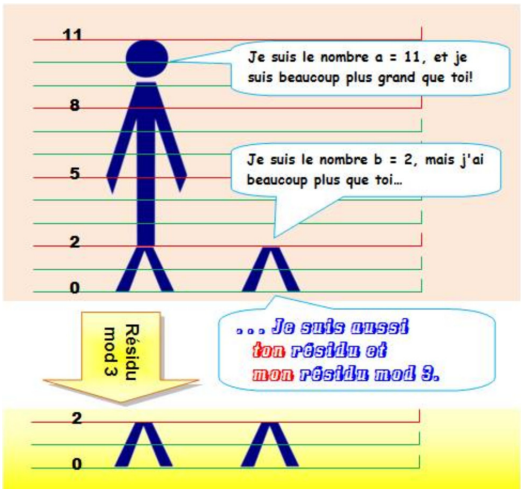
$$a \equiv a' \mod n \iff a - a' \text{ est divisible par } n.$$

Grâce à la Proposition 9.8, nous concluons que $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$ est un *anneau*, au sens abstrait de la Définition 5.9 déjà vue *supra*.

Théorème 10.8. *Pour tout entier (module) fixé $n \geqslant 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$, muni de ses deux lois d'addition et de multiplication modulo n :*

$$(\bullet) + (\bullet) \mod n, \qquad \textit{et} \qquad (\bullet) \cdot (\bullet) \mod n,$$

est un anneau commutatif. □



Terminologie 10.9. On fixe un entier $n \geqslant 2$. Pour tout entier $a \in \mathbb{Z}$, le *résidu de a modulo n* est l'entier unique $a' = \pi(a)$ tel que :

(1) $0 \leqslant a' \leqslant n-1$;

(2) $a' \equiv a \mod$.

Pour terminer cette section, donnons un exemple élémentaire d'application du calcul modulaire. Nous savons que modulo n, tout entier $a \in \mathbb{Z}$ est congru à exactement 1 entier parmi $\{0, 1, 2, \ldots, n-2, n-1\}$. Donc dans le cas $n = 3$, tout entier est congru ou bien à 0, ou bien à 1, ou bien à 2.

Proposition 10.10. *Pour tout entier $m \in \mathbb{Z}$, le produit $m(m+1)(m+2)$ est divisible par 3.*

Démonstration. Autrement dit, il s'agit de faire voir que :

$$m\,(m+1)\,(m+2) \equiv 0 \mod 3.$$

• Premier cas : $m \equiv 0 \mod 3$. Alors $m = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = 3\,m'(m+1)(m+2)$ aussi.

• Deuxième cas : $m \equiv 1 \mod 3$. Alors $m+2 \equiv 0 \mod 3$, donc $m+2 = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = m(m+1)\,3\,m'$ aussi.

• Troisième cas : $m \equiv 2 \mod 3$. Alors $m+1 \equiv 0 \mod 3$, donc $m+1 = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = m\,3\,m'\,(m+2)$ aussi. □

D'une manière similaire, $m(m+1)(m+2)(m+3)$ est toujours divisible par 4 (exercice). Au fait, que peut-on dire de $m(m+1)$? Plus généralement, on peut démontrer (exercice) la

Proposition 10.11. *Pour tout entier $n \geqslant 1$, le produit $m(m+1)\cdots(m+n-1)$ est divisible par n.* □

11. Multiplication modulaire et exponentiation modulaire

Avant de présenter de nombreux exemples très instructifs concernant le *calcul modulaire*, énonçons et démontrons deux propositions concernant le comportement de la congruence $\equiv$ modulo n vis-à-vis de la multiplication.

Proposition 11.1. *Pour tout entier $n \geqslant 1$, pour tous entiers relatifs $a, b \in \mathbb{Z}$, et pour tout multiplicateur $c \in \mathbb{Z}$, on a :*

$$a \equiv b \mod n \qquad \Longrightarrow \qquad a\,c \equiv b\,c \mod n.$$

Démonstration. En effet :

$$\big(a = b + k\,n\big)\,c \qquad \text{devient} \qquad a\,c = b\,c + (k\,c)\,n. \qquad \square$$

L'exponentiation est une forme généralisé de multiplication.

Proposition 11.2. *Pour tout entier $n \geqslant 1$, pour tous entiers relatifs $a, b \in \mathbb{Z}$, et pour tout exposant entier $r \geqslant 0$ on a :*

$$a \equiv b \mod n \qquad \Longrightarrow \qquad a^r \equiv b^r \mod n$$

Démonstration. Pour $r = 0$, puisque $a^0 = 1 = b^0$, on a bien, d'une manière tautologique, $1 \equiv 1 \mod n$.

Pour $r \geqslant 1$, la formule du binôme de Newton nous permet de développer la puissance r-ième :

$$\big(a = b + k\,n\big)^r \qquad \text{devient} \qquad \begin{aligned} a^r \;=\; & b^r + \tbinom{r}{1}\, b^{r-1}\,(k\,n)^1 \\ & + \tbinom{r}{2}\, b^{r-2}\,(k\,n)^2 \\ & + \cdots\cdots\cdots\cdots \\ & + \tbinom{r}{r-1}\, b^1\,(k\,n)^{r-1} \\ & + \tbinom{r}{r}\, b^0\,(k\,n)^r, \end{aligned}$$

et comme dans la colonne verticale à droite tous les termes $(k\,n)^*$ sont à une puissance $* \geqslant 1$ au moins égale à 1, on peut factoriser le tout par n pour obtenir :

$$a^r = b^r + \Big\{ \underbrace{\tbinom{r}{1}\, b^{r-1}\,k^1 + \tbinom{r}{2}\, b^{r-2}\,k^2\,n^1 + \cdots + \tbinom{r}{r-1}\, b^1\,k^{r-1}\,n^{r-2} + \tbinom{r}{r}\, b^0\,k^r\,n^{r-1}}_{=:\ \text{nouvel entier } \kappa} \Big\}\, n,$$

ce qui donne une relation :

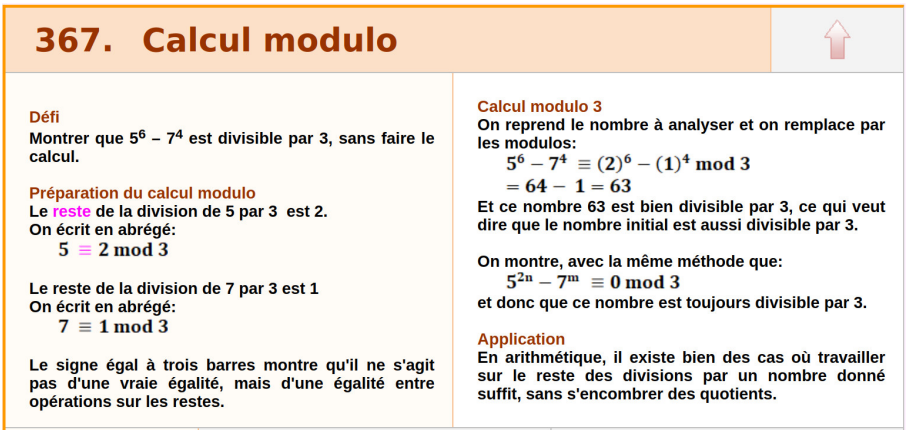
$$a^r \;=\; b^r + \mathrm{K}\, n,$$

exprimant bien que $a^r \equiv b^r \mod n$. □

On constate d'ailleurs manifestement dans ce dernier calcul que le fameux « entier k kaché » dans la relation de congruence peut absorber une complexité considérable de calculs annexes. Au travers de nombreux exemples « magiques » — et promis depuis bien longtemps —, nous allons enfin pouvoir vraiment dévoiler l'intérêt de « cacher » ces k intempestifs qui « explosent », et même mieux encore, nous allons montrer comment toujours s'épargner de nombreux calculs délicats.

« Neuf personnes sur dix aiment les mathématiques sans calculs », dit-on parfois en cours ou sur les bancs des écoles, et « La dizième *ment* », ajoute-t-on. Mais . . . rien n'est si sûr . . ., car dans les calculs se lovent toutes sortes de plaisirs gourmands et de découvertes impromptues.

12. Exemples de calculs modulo un entier



367. Calcul modulo

Défi
Montrer que $5^6 - 7^4$ est divisible par 3, sans faire le calcul.

Préparation du calcul modulo
Le reste de la division de 5 par 3 est 2.
On écrit en abrégé:
$5 \equiv 2 \bmod 3$

Le reste de la division de 7 par 3 est 1
On écrit en abrégé:
$7 \equiv 1 \bmod 3$

Le signe égal à trois barres montre qu'il ne s'agit pas d'une vraie égalité, mais d'une égalité entre opérations sur les restes.

Calcul modulo 3
On reprend le nombre à analyser et on remplace par les modulos:
$5^6 - 7^4 \equiv (2)^6 - (1)^4 \bmod 3$
$= 64 - 1 = 63$
Et ce nombre 63 est bien divisible par 3, ce qui veut dire que le nombre initial est aussi divisible par 3.

On montre, avec la même méthode que:
$5^{2n} - 7^m \equiv 0 \bmod 3$
et donc que ce nombre est toujours divisible par 3.

Application
En arithmétique, il existe bien des cas où travailler sur le reste des divisions par un nombre donné suffit, sans s'encombrer des quotients.

Question 12.1. *Étant donné un entier $m \in \mathbb{Z}$, peut-on l'écrire sous la forme $m = a^2 + b^2$, avec deux entiers relatifs a et b ?*

Par exemple, est-ce possible pour $m = 40\,003$? Une idée simple serait de tester toutes les sommes possibles $a^2 + b^2$ avec $a, b \leqslant \sqrt{40\,003}$, ce qui exigerait pas mal de calculs.

Mais une idée [8] plus astucieuse et plus économique consiste à examiner toutes les valeurs de carrés a^2 modulo 4, où $a \in \mathbb{Z}$ est quelconque, puis celles de $a^2 + b^2$ modulo 4.

En effet, tout entier a est congru modulo 4 à l'un des quatre nombres 0, 1, 2, 3. Donc a^2 est congru à 0^2, 1^2, 2^2, 3^3 modulo 4, c'est-à-dire à 0, 1, 0, 1 : il n'y a que deux valeurs possibles !

Par conséquent, une somme a^2+b^2 de deux carrés ne peut être congrue, modulo 4, qu'à :

$$0+0 \;\equiv\; 0, \qquad 0+1 \;\equiv\; 1, \qquad 1+1 \;\equiv\; 2,$$

c'est-à-dire à 0, 1, 2 : il n'y a que trois valeurs possibles !

8. On pourrait se demander : *Pourquoi le nombre* 4, *ici ?* Et la question est légitime.
En fait, l'Idée générale qui gouverne le calcul modulaire, c'est la possibilité de choisir divers *modules* $n \geqslant 1$, et de calculer modulo n afin de *contracter les calculs*. Si $n = 4$ ne marche pas, on essaie alors d'autres entiers $n = 5$, *etc.*, juste pour « tester », et souvent, cela finit par marcher.

Ainsi, la valeur 3 ne peut *jamais* être atteinte par une somme a^2+b^2 de deux carrés entiers !

Et comme $40\,003 \equiv 3 \bmod 4$, nous concluons qu'il n'est *pas* représentable comme somme de deux carrés.

Nous n'avons pas complètement répondu à la Question 12.1, mais nous avons au moins trouvé une *méthode* pour obtenir un *critère négatif*.

Proposition 12.2. **(1)** *Aucun entier de la forme $3+4k$ ne peut être représenté comme somme de deux carrés.*
(2) *Aucun entier de la forme $7+8k$ ne peut être représenté comme somme de trois carrés.*

Démonstration. Il reste à traiter **(2)**. En raisonnant modulo 8, les valeurs des carrés 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2 sont $0, 1, 4, 1, 0, 1, 4, 1$, c'est-à-dire $0, 1, 4$.

Si un entier $m = a^2+b^2+c^2$ est somme de trois carrés, ses valeurs modulo 8 ne peuvent être que :

$$\begin{aligned}
&0+0+0 \equiv 0,\\
&0+0+1 \equiv 1, \qquad 0+0+4 \equiv 4,\\
&0+1+1 \equiv 2, \qquad 0+4+4 \equiv 0, \qquad 1+1+4 \equiv 6,\\
&1+1+1 \equiv 3, \qquad 4+4+4 \equiv 4, \qquad 1+4+4 \equiv 1, \qquad 0+1+4 \equiv 5,
\end{aligned}$$

donc *jamais* 7 modulo 8. En conclusion, aucun entier de la forme $7+8k$ ne peut être atteint. □

13. Contraction de calculs avec des grands nombres

Grand nombre ...

Démontrez que $N = 10^{1\text{ million}} + 10$ est divisible par 13

Avec 10, il manque 3 pour arriver à 13.	$10 \equiv -3 \bmod 13$
Élévation au carré. **Effectivement 100 = 7x13 + 9**	$100 \equiv 9 \bmod 13$
Poursuivons en prenant le cube.	$1000 \equiv -27 \bmod 13$ $\equiv (-13-13-1) \bmod 13$ $\equiv -1 \bmod 13$
Super! Car le 1, élevé à une puissance quelconque, donne toujours 1.	$(10^3)^k \equiv (-1)^k \bmod 13$
Pour approcher le million proposé en exposant.	$(10^3)^{333\,333} \equiv (-1)^{333\,333} \bmod 13$
L'exposant est impair, le signe moins est conservé.	$10^{999\,999} \equiv -1 \bmod 13$
En multipliant par 10.	$10^{1\,000\,000} \equiv (-1)\times(-3) \bmod 13$ $\equiv 3 \bmod 13$
Reste à ajouter 10 pour avoir N.	$N = 10^{1\,000\,000} + 10$ $\equiv (3+10) \bmod 13$ $\equiv 0 \bmod 13$ ■

Un peu d'astuce avec les grands nombres	
Calculer le reste de la division par 5 de 2009^{2009}	$2^{2009} \equiv x? \bmod 7$
On note que	$2^2 \equiv 4 \bmod 7$ $2^3 = 8 \equiv 1 \bmod 7$
Or, 2009 = 3 x 669 + 2	$2^{2009} = 2^{3\times 669+2} = (2^3)^{669} \times 2^2$ $\equiv 1^{669} \times 4 \equiv 4 \bmod 7$
Calculer le reste de la division par 5 de 2009^{2009}	$2009^{2009} \equiv x? \bmod 5$
On note que 2009 = 2010 – 1 avec 2010 divisible par 5	$2009 \equiv -1 \bmod 5$
Rapidement, on obtient:	$2009^{2009} \equiv (-1)^{2009} = -1 \equiv 4 \bmod 5$
Vérification **par logiciel de calcul**	$2009^{2009} \bmod 5;$ 4

14. Carrés modulo un entier

Fixons un module $n \geqslant 1$. Rappelons comment nous avons établi que tout entier $a \in \mathbb{Z}$ est congru, modulo n, à exactement un entier parmi $\{0, 1, 2, \ldots, n-2, n-1\}$. L'argument-clé, c'était que les entiers :

$$\ldots,\ a-2\,n,\ a-n,\ a,\ a+n,\ a+2\,n,\ \ldots,$$

se situaient à distance exactement n l'un à la suite de l'autre, et que l'intervalle entier $[\![0, n-1]\!]$ était une « marmite » de même longueur n. En raisonnant de manière similaire, on établit la

Proposition 14.1. *Modulo n, tout entier $a \in \mathbb{Z}$ est congru à un et à un seul entier a' tel que :*

$$-\tfrac{n}{2} < a' \leqslant \tfrac{n}{2}.$$

Démonstration. Observons que l'inégalité à gauche est stricte, et que $\frac{n}{2}$ n'est pas toujours entier. Pour être plus précis, il vaut mieux distinguer deux cas :

• $n = 2\,n_1$ est pair, d'où $\frac{n}{2} = n_1$, puis $-n_1 < a' \leqslant n_1$ désigne l'intervalle entier $[\![-n_1 + 1, n_1]\!]$, de longueur égale à $2\,n_1 = n$;

• $n = 2\,n_1 + 1$ est impair, d'où $\frac{n}{2} = n_1 + \frac{1}{2}$, puis $-n_1 - \frac{1}{2} < a' \leqslant n_1 + \frac{1}{2}$ désigne l'intervalle entier $[\![-n_1, n_1]\!]$, de longueur égale à $2\,n_1 + 1 = n$;

Dans les deux cas, l'intervalle entier $\frac{n}{2} < a' \leqslant \frac{n}{2}$ est de longueur précisément égale à n, donc l'argument-clé déjà vu de la « marmite de longueur n » s'applique. □

Notation 14.2. La *partie entière*, notée $\lfloor x \rfloor$, d'un nombre réel $x \in \mathbb{R}$ est l'unique entier $\lfloor x \rfloor \in \mathbb{Z}$ satisfaisant :

$$\lfloor x \rfloor \leqslant x < 1 + \lfloor x \rfloor,$$

par exemple, $\lfloor \frac{2n_1+1}{2} \rfloor = n_1$.

Par souci de symétrie, nous considérerons l'intervalle entier $[\![-\lfloor \frac{n}{2} \rfloor,\ \lfloor \frac{n}{2} \rfloor]\!]$, sans inégalité stricte à gauche, sachant que pour $n = 2\,n_1$ pair, cet intervalle contient $n + 1$ nombres

entiers au lieu de n attendus (une tomate de plus), et que pour $n = 2\,n_1 + 1$, il en contient n comme voulu.

Proposition 14.3. *Les carrés modulo n sont les résidus modulo n de 0^2, 1^2, 2^2, …, $\lfloor \frac{n}{2} \rfloor^2$.*

Autrment dit, pour connaître les valeurs des carrés modulo n, on peut diviser par 2 le travail.

Démonstration. En effet, soit donc a' avec :

$$-\lfloor \tfrac{n}{2} \rfloor \leqslant a' \leqslant \lfloor \tfrac{n}{2} \rfloor.$$

Pour $a' = 0, 1, 2, \ldots \lfloor \frac{n}{2} \rfloor$, on obtient bien les carrés indiqués. Pour $a' = -1, -2, \ldots, -\lfloor \frac{n}{2} \rfloor$, quand on prend un carré, son signe s'évanouit, car $(-1)^2 \equiv 1 \bmod n$, et donc, on obtient forcément les mêmes carrés. □

Par exemple, modulo 10, il suffit de calculer :

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4, \qquad 3^2 \equiv 9, \qquad 4^2 \equiv 6, \qquad 5^2 \equiv 5.$$

15. Nombres de Fermat

En 1758, Euler a découvert que le cinquième nombre de Fermat :

$$2^{2^5} + 1 \;=\; 4\,294\,967\,297,$$

inférieur, en euros, aux plus grandes fortunes de France protégées de l'impôt avec le consentement des législateurs, n'est *pas* un nombre premier, et qu'il est divisible par :

$$641 \,\Big|\, 2^{2^5} + 1.$$

Pour voir cela de la manière la plus économique qui soit, Euler se propose un petit entraînement (échauffement) qui consiste à calculer — à la main ! — le nombre :

$$7^{160},$$

et Euler commence par calculer, toujours modulo 641, les nombres successifs :

$$7^2,\ 7^4,\ 7^8,\ 7^{16},\ 7^{32},\ 7^{64},\ 7^{128},$$

en prenant les carrés des nombres qui précèdent. Euler récupère le résultat intermédiaire 7^{32} qu'il n'a qu'à relire sur son manuscrit, pour calculer enfin :

$$7^{160} \;=\; 7^{128} \cdot 7^{32},$$

le tout modulo 641 *à chaque étape* [9].

Mais ce ne sont pas les puissances de 7 qui l'intéressent, c'est le cinquième nombre de Fermat.

9. Pour rendre transparente la difficulté, mentionnons que :

$$7^{32} \;=\; 1104427674243920646305299201,$$

et pour faire transpirer un peu plus les électrons-esclaves de notre ordinateur, ajoutons que :

$$7^{128} \;=\; 14878156471976116959103126817412735703323567171547989498984983050863873154233009996547575619286333058970368 01,$$

ce qui, au final, devrait donner quelque chose d'aussi astronomique que :

$$7^{160} \;=\; 16431847749381718579170004105565448063418374195995234970697646712332075655622878918775643238182544494869108389978714672980473696128960 01.$$

Théorème 15.1. [Euler 1732] *Contrairement à ce que Fermat affirmait, le nombre* $2^{2^5}+1$ *n'est* pas *un nombre premier, et il est divisible par le nombre premier* 641*, à savoir on a :*

$$2^{2^5} \equiv -1 \bmod 641.$$

Démonstration. Il suffit de partir d'un nombre encore trop petit pour que sa réduction modulo 641 commence à prendre effet, par exemple :

$$2^{2^3} = 2^8 = 256 \bmod 641,$$

pour monter ensuite deux crans plus haut tout en réduisant modulo 641 chaque fois que cela est possible :

$$\begin{aligned}
2^{2^5} &\equiv \left(\left(2^{2^3}\right)^2\right)^2 \bmod 641 \\
&\equiv \left(\left(256\right)^2 \bmod 641\right)^2 \bmod 641 \\
&\equiv \left(65536 \bmod 641\right)^2 \bmod 641 \\
&\equiv \left(154\right)^2 \bmod 641 \\
&\equiv 23716 \bmod 641 \\
&\equiv -1 \bmod 641.
\end{aligned}$$

□

DIVISIBILITÉ par 641

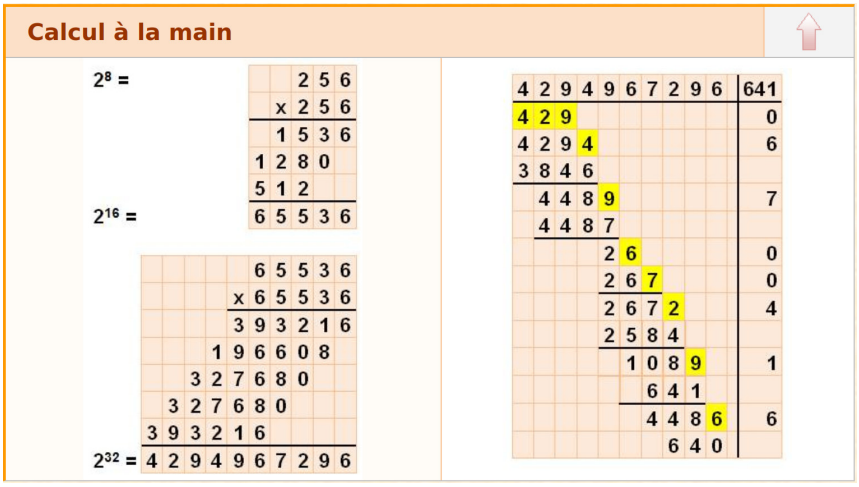
Nombre de Fermat n°5: divisible par 641.

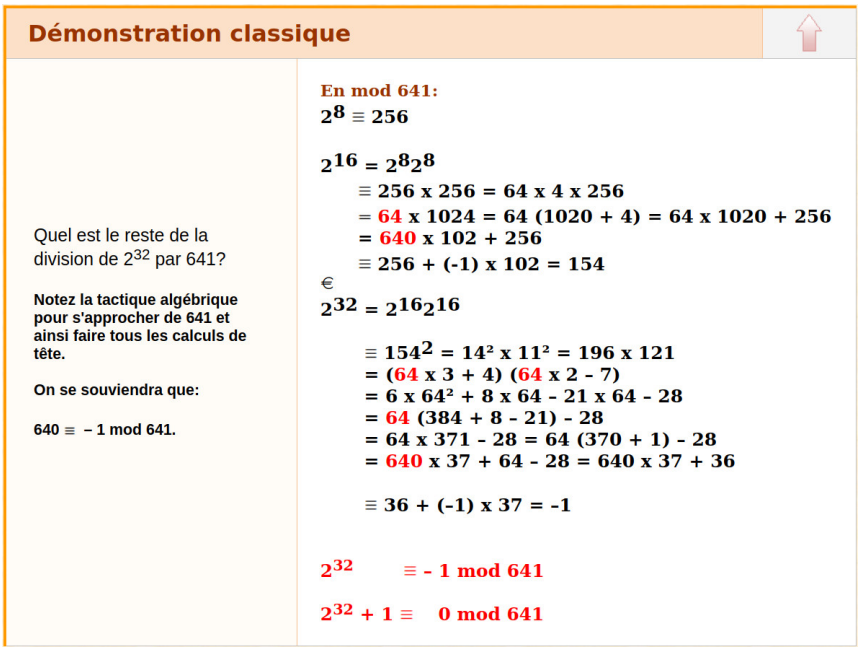
Enjeu historique: on savait que les nombres de Fermat inférieurs à F_5 étaient tous premiers. Fermat, lui-même, conjecturait qu'ils étaient tous premiers. On sait qu'ils sont tous composés à partir de F_5 et jusqu'à F_{31}.

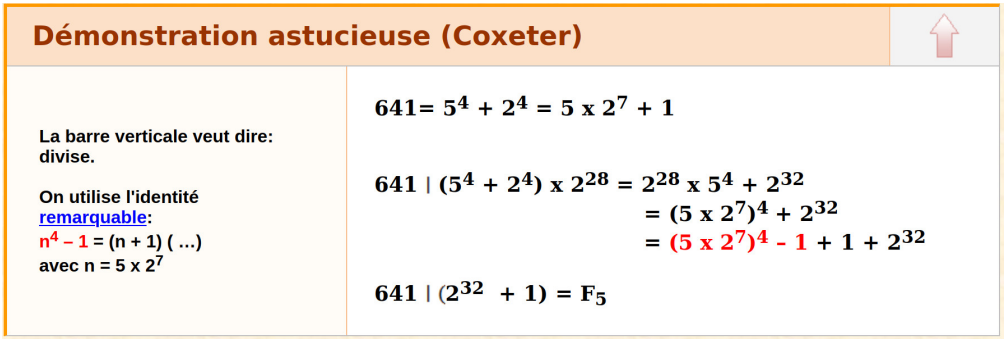
Aujourd'hui: Sachant que ce nombre est divisible par 641, plusieurs méthodes de calcul sont possibles: à la main, calculette ou via les congruences classiquement ou via une astuce. Ne connaissant pas 641, la méthode directe consisterait à écrire un programme pour détecter cette valeur.

Propriétés

Le nombre de Fermat F_5 est composé. Il est divisible par 641.	$\mathbf{F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641\ k}$
Autres puissances de 2 mod 641 N = r mod m veut dire que N divisé par m donne un reste r.	$\mathbf{2^{32} \equiv -1 \bmod 641}$ $\mathbf{2^{64} \equiv 1 \bmod 641}$ $\mathbf{2^{96} \equiv -1 \bmod 641}$ **etc.**







En effet, la découverte d'Euler était fantastique : arrêtons-nous quelques instants pour en dire plus.

Définition 15.2. Pour $n \geqslant 0$ entier, le n-ième *nombre de Fermat* est :

$$F_n := 2^{2^n} + 1.$$

Ces nombres doivent leur nom au mathématicien français Pierre de Fermat (1601–1665) qui émit la conjecture *erronée* que tous ces nombres étaient premiers.

Ironie cinglante : tous les nombres de Fermat connus, depuis F_5, F_6, F_7, …, jusqu'à :

$$F_{32} = 2^{2^{32}} + 1,$$

ne sont *pas* premiers.

Assertion 15.3. *Les seuls nombres de Fermat premiers connus sont donc :*

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537. \quad \square$$

En 1640, dans une lettre adressée à Bernard Frénicle de Bessy, Pierre de Fermat énonce son petit théorème, puis il commente :

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Dans cette même lettre, il émet la conjecture que ces nombres sont tous premiers, quoiqu'il reconnaisse :

> Je n'ai pu encore démontrer nécessairement la vérité de cette proposition.

Mais cette hypothèse le fascine littéralement. Deux mois plus tard en effet, dans une lettre àMarin Mersenne, Pierre de Fermat écrit :

> Si je puis une fois tenir la raison fondamentale que 3, 5, 17, *etc.* sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car j'ai déjà trouvé des choses merveilleuses dont je vous ferai part.

Il écrit encore à Blaise Pascal :

> Je ne vous demanderais pas de travailler à cette question si j'avais pu la résoudre moi-même.

Dans une lettre à Kenelm Digby, non datée mais envoyée en copie par Digby à John Wallis le 16 juin 1658, Fermat donne encore sa conjecture comme non démontrée. Toutefois, dans une lettre de 1659 à Pierre de Carcavi, il s'exprime en des termes qui, selon certains commentateurs, impliquent qu'il estime avoir trouvé une démonstration.

Mais en 1732, le jeune Leonhard Euler, à qui Christian Goldbach avait signalé cette conjecture trois ans auparavant, la réfute spectaculairement :

$$F_5 = 2^{2^5} + 1 \textit{ est divisible par } 641.$$

Or la motivation initiale de Fermat était de trouver une formule qui produise une infinité de nombres premiers [10]. Il connaissait la proposition élémentaire suivante.

Lemme 15.4. *Si $k \geqslant 1$ est un entier tel que le nombre $2^k + 1$ est premier, alors k est une puissance de 2.*

Démonstration. En divisant k pas à pas par 2 tant qu'on garde un nombre pair, on peut extraire k une puissance maximale de 2, et donc l'écrire comme $k = 2^b\, k'$, avec un entier $b \geqslant 0$, et avec un entier *impair* k'.

10. Il n'existe aucune formule ayant cette propriété qui soit *intéressante* ou *utile*.

Pour mémoire, on rappelle les factorisations classiques avec des puissances impaires :

$$\begin{aligned} 1+c^3 &= (1+c)\big(1-c+c^2\big),\\ 1+c^5 &= (1+c)\big(1-c+c^2-c^3+c^4\big). \end{aligned}$$

En posant $c := 2^{2^b}$, on dispose alors des égalités suivantes :

$$\begin{aligned} 1+2^k &= 1+2^{k'2^b}\\ &= 1+c^{k'}\\ &= (1+c)\big(1-c+c^2-\cdots-c^{k'-2}+c^{k'-1}\big), \end{aligned}$$

lesquelles montrent que $1+c$ serait un diviseur du nombre premier $1+2^k$ si on avait $k' \geqslant 3$, ce qui est impossible, donc $k'=1$ et enfin $k=2^b$. □

Fermat a conjecturé (erronément, comme on l'a vu) que la réciproque de ce lemme était vraie, après avoir confirmé (aisément) que les cinq (premiers) nombres :

$$\begin{aligned} F_0 &= 3,\\ F_1 &= 5,\\ F_2 &= 17,\\ F_3 &= 257,\\ F_4 &= 65537, \end{aligned}$$

sont tous premiers.

De nos jours encore, on ignore *cruellement* s'il existe d'autres nombres de Fermat qui sont premiers. On sait que F_5, F_6, …, F_{32} sont tous *composés*, mais on ne sait pas si F_{33} est premier ou composé.

Le plus grand nombre de Fermat dont on sait qu'il est composé est :

$$F_{2\,747\,499},$$

et on sait que l'un de ses diviseurs est :

$$57\cdot 2^{2\,747\,499}+1.$$

En fait, Euler avait démontré le :

Théorème 15.5. *Tout facteur premier p d'un nombre de Fermat F_n est de la forme :*

$$k\,2^{n+1}+1,$$

où k est un entier. □

Ceci permet d'ailleurs à Euler de trouver rapidement par une autre voie que F_5 est divisible par 641.

En effet, on cherche un entier k tel que le nombre :

$$p = k\,2^6+1 = 64\,k+1$$

soit à la fois premier et diviseur strict de F_5. Les premières valeurs de k ne conviennent pas, mais dès $k=10$, on constate que $p=641$ est premier et que modulo 641, on a :

$$5^4\cdot 2^{32} = \big(5\cdot 2^8\big)^4 = \big(5\cdot 128\cdot 2\big)^4 = \big(640\cdot 2\big)^4 \equiv (-2)^4 \bmod 641 \equiv 16 \bmod 641,$$

et par ailleurs :

$$5^4 \cdot 2^{32} \equiv \left(5^4 \bmod 641\right) \times 2^{32} \equiv \left(625 \bmod 641\right) \times 2^{32} \equiv -16 \times 2^{32} \bmod 641,$$

d'où en comparant ces deux résultats :

$$16 \bmod 641 \equiv -16 \times 2^{32} \bmod 641,$$

et enfin, après division par 16 qui est premier avec 641 :

$$1 \equiv -2^{32} \bmod 641,$$

ce qui montre bien que F_5 est divisible par 641. Plusieurs autres démonstration on déjà été données plus haut.

Le cas général est un problème difficile du fait de la taille des entiers F_n, même pour des valeurs relativement faibles de n.

Aujourd'hui, le plus grand nombre de Fermat dont on connaisse la factorisation complète est F_{11}, et le plus grand de ses cinq diviseurs premiers possède 560 chiffres. Les factorisations complètes des F_n, pour n entre 5 et 10, sont, elles aussi, entièrement connues.

En ce qui concerne F_{12}, on sait qu'il est composé mais c'est le plus petit nombre de Fermat dont on ne connaisse pas la factorisation complète.

Quant à F_{20}, c'est le plus petit nombre de Fermat composé dont on ne connaisse aucun diviseur premier.

16. Exponentiation rapide

Méthode de calcul de restes sur grands nombres

Calcul d'une puissance mod m.
Le calcul est accéléré en profitant de cette relation

$$a^k = \begin{cases} \left(a^{\frac{k}{2}}\right)^2 & \text{pour k pair} \\ a \cdot \left(a^{\frac{k-1}{2}}\right)^2 & \text{pour k impair} \end{cases}$$

Exemple: 3^{1304} **(mod 121)**

Étape 1 – Ligne 1: remplir les cellules de gauche à droite en commençant par l'exposant (1304). Si le nombre est pair, le suivant est sa moitié; sinon soustraire 1.

k	1304	652	326	163	162	81	80	40	20	10	5	4	2	1
3^k [121]	$(3^{652})^2$	$(3^{326})^2$	$(3^{163})^2$	$3 \cdot 3^{162}$	$(3^{81})^2$	$3 \cdot 3^{80}$	$(3^{40})^2$	$(3^{20})^2$	$(3^{10})^2$	$(3^5)^2$	243	81	9	3
	9^2	3^2	27^2	$3 \cdot 9$	3^2	$3 \cdot 1$	1^2	1^2	1^2	1^2				
	81	9	3	27	9	3	1	1	1	1	1	81	9	3

Étape 2 – Lignes 2, 3 et 4: on inscrit dans chaque cellule la valeur de $3^{\text{nombre du haut}}$ mod 121.
Le calcul est simplifié en remplissant les cellules de droite à gauche (donc dans l'autre sens). On profite des résultats précédents. Exemple: $3^{10} = 3^{5 \times 2} = (3^5)^2$ soit $(1)^2$ en mod 121.

Vérification avec logiciel de calcul

$$3^{1304} \bmod 121;$$
$$81$$

Exemple avec l'année 2021

Calculer le reste de la division par 13 de 2021^{2021}	$2021^{2021} \equiv x? \bmod 13$	
Premier pas	**Reduire la base 2021**	$2021 = 155 \times 13 + 6$ $2021 \equiv 6 \bmod 13$ $2021^{2021} \equiv 6^{2021} \bmod 13$
Conversion en binaire de 2021. **On se souvient que $2^{10} = 1024$**	N, k^2, k, B 2021 997, 1024, 10, 1 485, 512, 9, 1 229, 256, 8, 1 101, 128, 7, 1 37, 64, 6, 1 5, 32, 5, 1 5, 16, 4, 0 5, 8, 3, 0 1, 4, 2, 1 1, 2, 1, 0 0, 1, 0, 1	**En colonnes centrales toutes les puissances de 2 inférieures à 2021.** **En colonne de gauche, le nombre N puis sa valeur diminuée des valeurs successives de 2^k. Si le résultat reste positif, un 1 est placé en colonne de droite (binaire). Sinon, on conserve la valeur et on place un 0 à droite.** **La colonne de droite (B) indique la conversion en binaire de 2021.** **$2021_{10} = 111\ 1110\ 0101_2$**
Avec les puissances de 2	$2021^{2021} \equiv 6^{2\text{^}10} \times 6^{2\text{^}9} \times \ldots \times 6^{2\text{^}0} \bmod 13$	
Attention *Voir Puissances à étages*	$6^{2\text{^}10} = 6^{2^{10}} = 6^{1024} = 6,7124\ldots10^{796} \equiv 9\ mod\ 13$ $et\ non\ pas\ (6^2)^{10} = 36^{10} = 3,6561\ldots10^{15} \equiv 3\ mod\ 13$	

Attention *Voir Puissances à étages*	$6^{2\text{^}10} = 6^{2^{10}} = 6^{1024} = 6,7124\ldots10^{796} \equiv 9\ mod\ 13$ $et\ non\ pas\ (6^2)^{10} = 36^{10} = 3,6561\ldots10^{15} \equiv 3\ mod\ 13$	
Calcul des puissances de 6 mod 13	$6^{2^0} = 6^1 \equiv 6 \bmod 13$ $6^{2^1} = 6^2 = 36 \equiv 10 \bmod 13$ $6^{2^2} = 6^2 \times 6^2 = 100 \equiv 9 \bmod 13$ $6^{2^3} = 9 \times 9 = 81 \equiv 3 \bmod 13$ $6^{2^4} = 3 \times 3 = 9 \equiv 3 \bmod 13$ ... ð[6, 10, 9, 3, 9, 3, 9, 3, 9, 3, 9]	**Multiple de 13** **13, 26, 39, 52, 65, 78, 91, 104, 117, 130, ...**
Retour au calcul demandé	$2021^{2021} \equiv 9 \times 3 \times 9 \times 3 \times 9 \times 3 \times 9 \times 6 \bmod 13$ $\equiv 27 \times 27 \times 27 \times 54 \equiv 1 \times 1 \times 1 \times 2 \equiv$ **2 mod 13**	
Année 2021 en modulo	**2021 = [0, 1, 2, 1, 1, 5, 5, 5, 5, 1, 8, 5, 6, 5, 11, 5, 15, 5, 7, 1] mod (1, 2, 3,.., 13, ..., 20)** **2021^{2021} = [0, 1, 2, 1, 1, 5, 3, 5, 2, 1, 8, 5, 2, 3, 11, 5, 2, 11, 11, 1] mod (1, 2, 3,.., 13, ..., 20)**	

17. Division euclidienne générale dans $\mathbb{Z}$

Lorsque $a \geqslant 0$ et $b \geqslant 1$, la division euclidienne de a par b est intuitivement facile à effectuer. Le quotient q est le plus grand entier $q \geqslant 0$ tel que $0 \leqslant q\,b \leqslant a$, et le reste est alors $r := a - q\,b$.

Par exemple, la division euclidienne de 5 par 2 est :

$$5 \;=\; 2 \cdot 2 + 1.$$

Autrement dit, $q = 2$ et $r = 1$

Il faut en revanche faire un peu attention lorsqu'on travaille avec des entiers négatifs. Par exemple, la division euclidienne de -5 par 2 est :

$$-5 \;=\; 2\cdot(-3)+1.$$

Ainsi, dans ce cas, on a $q=-3$ et $r=1$.

Nous sommes maintenant prêts à démontrer un résultat fondamental pour toute l'arithmétique.

Théorème 17.1. [Division euclidienne dans $\mathbb{Z}$] *Soient $a,b\in\mathbb{Z}$ avec $b\neq 0$ non nul. Alors, il existe $q,r\in\mathbb{Z}$ tels que :*

(1) $a=q\,b+r$ *;*

(2) $0\leqslant r<|b|$.

De plus, les entiers q et r sont uniques.

Démonstration. Commençons par établir l'existence de q et de r. Comme $b\neq 0$ est supposé non nul, on peut diviser le travail en deux cas : $b\geqslant 1$, puis $b\leqslant -1$.

Premier cas : $b\geqslant 1$. Introduisons l'ensemble :

$$E \;:=\; \big\{m\in\mathbb{Z}\colon\; m\,b\leqslant a\big\}.$$

Assertion 17.2. *E est non vide et majoré.*

Preuve. Introduisons deux sous-cas : $a\geqslant 0$, puis $a\leqslant -1$.

Premier sous-cas : $a\geqslant 0$. Clairement, $0\in E$ car $0\cdot b=0\leqslant a$, donc $E\neq\emptyset$.

Ensuite, nous affirmons que a est un majorant de E, c'est-à-dire que $m\leqslant a$ pour tout $m\in E$. Pour cela, raisonnons par l'absurde. S'il existait $m_*\in E$ tel que $m_*\geqslant a+1$, alors on aurait $m_*\geqslant 1$ puisque $a\geqslant 0$, d'où nous déduirions les inégalités :

$$\begin{aligned} a+1 &\leqslant m_* \\ [b\geqslant 1] \qquad &\leqslant m_* b \\ [m_*\in E] \qquad &\leqslant a, \end{aligned}$$

dont la conséquence $a+1\leqslant a$, équivalente à $1\leqslant 0$, serait une contradiction fatale à toutes les mathématiques ! Donc on a bien $\max\limits_{m\in E} m\leqslant a$.

Deuxième sous-cas : $a\leqslant -1$. Clairement, $a\in E$ car $b\geqslant 1$ implique alors que $a\,b\leqslant a$, donc $E\neq\emptyset$.

Ensuite, nous affirmons que 0 est un majorant de E. Pour cela, raisonnons à nouveau par l'absurde. S'il existait $m_*\in E$ tel que $m_*\geqslant 1$, nous déduirions les inégalités :

$$\begin{aligned} [b\geqslant 1] \qquad 1 &\leqslant m_*\, b \\ [m_*\in E] \qquad &\leqslant a \\ &\leqslant -1, \end{aligned}$$

dont le résultat $1\leqslant -1$ serait très faux ! Donc on a bien $\max\limits_{m\in E} m\leqslant 0$. □

Grâce au Théorème 5.13 **(3)** concernant les sous-ensembles de $\mathbb{Z}$ majorés, E possède un plus grand élément, soit q. On a donc $q\in E$ et $q+1\notin E$, ce qui se traduit par :

$$q\,b\;\leqslant\; a\;<\;(q+1)\,b.$$

Posons alors $r:=a-q\,b$. L'encadrement précédent se ré-écrit $0\leqslant r<b=|b|$, d'où l'existence de q et de r dans ce premier cas $b\geqslant 1$.

Deuxième cas : $b \leqslant -1$. Alors $-b \geqslant 1$, et grâce à l'étude du premier cas, il existe $q, r \in \mathbb{Z}$ tels que :

$$\begin{aligned} a &= q\,(-b) + r \\ &= (-q)\,b + r, \end{aligned}$$

avec $0 \leqslant r < -b = |b|$, d'où le résultat.

Établissons maintenant l'unicité de (q, r). Supposons que $q, r, q', r' \in \mathbb{Z}$ vérifient :

$$\begin{aligned} a &= q\,b + r, \\ a &= q'\,b + r', \end{aligned}$$

avec :

$$\begin{aligned} 0 &\leqslant r < |b|, \\ 0 &\leqslant r' < |b|. \end{aligned}$$

Multiplions la deuxième ligne par -1, ce qui demande d'inverser les inégalités et d'échanger la droite avec la gauche :

$$\begin{aligned} 0 &\leqslant \quad r < |b|, \\ -|b| &< -r' \leqslant 0. \end{aligned}$$

Ensuite, par addition verticale, il vient — noter qu'après sommation, les inégalités sont *strictes* des deux côtés ! — :

$$-|b| < r - r' < |b|,$$

puis en prenant la valeur absolue :

$$|r - r'| < |b|. \tag{17.3}$$

Par ailleurs, en soustrayant verticalement les deux représentations de $a = q\,b + r$ et $a = q'\,b + r'$ écrites plus haut, on obtient :

$$0 = q\,b - q'\,b + r - r',$$

c'est-à-dire :

$$-(q - q')\,b = r - r'. \tag{17.4}$$

Nous affirmons que $q - q' = 0$. Sinon, si $q - q' \neq 0$, en prenant la valeur absolue de ce qui précède, on obtiendrait :

$$|q - q'|\,|b| = |r - r'|,$$

d'où à cause de $|q - q'| \geqslant 1$:

$$|b| \leqslant |r - r'|,$$

en contradiction manifeste avec (17.3).

Donc $q = q'$, et enfin en revenant à (17.4), nous concluons que $r = r'$. Cela achève la démonstration. □

Définition 17.5. Les entiers q et r définis par dans le Théorème 17.1 par $a = q\,b + r$ s'appellent respectivement le *quotient* et le *reste* de la division euclidienne de a par b.

Nous pouvons maintenant dévoiler un lien fondamental entre le calcul modulaire et la division euclidienne, dans $\mathbb{Z}$.

Proposition 17.6. *Pour tout entier $n \geqslant 1$, et tous entiers relatifs $a, b \in \mathbb{Z}$, on a équivalence entre :*

(i) $a \equiv b \bmod n$ *;*

(ii) a *et* b *ont le même reste dans leur division euclidienne par* n*.*

Démonstration. **(i)** $\Longrightarrow$ **(ii)** Si $a = b + k\,n$ est l'expression de la congruence, et si $b = q\,n + r$ est la division euclidienne de b par n, avec un reste $0 \leqslant r \leqslant n-1$, il en découle que :

$$a \;=\; (q+k)\,n + r,$$

et par unicité dans la division euclidienne, cette relation *est* la division de a par n, donc le reste r de b divisé par n est *aussi* le reste de a divisé par n.

(ii) $\Longrightarrow$ **(i)** En partant de :

$$\begin{aligned} a \;&=\; q_1\,n + r, \\ b \;&=\; q_2\,n + r, \end{aligned}$$

avec le *même reste* r pour ces deux petits pigeons a et b, il est clair que :

$$a \;\equiv\; r \;\bmod n \;\equiv\; b.$$

(i) $\Longleftrightarrow$ **(ii)** Donnons aussi une autre preuve directe de cette équivalence.

Écrivons les deux divisions de a et de b par n avec les deux restes incriminés :

$$\begin{aligned} a \;&=\; p\,n + r \qquad\qquad \text{avec} \quad 0 \;\leqslant\; r \;\leqslant\; n-1, \\ b \;&=\; q\,n + s \qquad\qquad \text{avec} \quad 0 \;\leqslant\; s \;\leqslant\; n-1, \end{aligned}$$

mutiplions la deuxième ligne par -1, puis additionnons verticalement :

$$\begin{aligned} 0 \;&\leqslant\; r \;&\leqslant\; n-1 \\ -(n-1) \;&\leqslant\; -s \;&\leqslant\; 0 \\ -(n-1) \;&\leqslant\; r-s \;&\leqslant\; (n-1). \end{aligned}$$

Ceci montre que l'entier $r - s$ appartient à l'intervalle entier $[\![-(n-1),\, (n-1)]\!]$.

Fait 17.7. *Aucun entier de l'intervalle $[\![-(n-1),\, (n-1)]\!]$, c'est-à-dire aucun entier parmi :*

$$-(n-1),\; -(n-2),\; \ldots,\; -2,\; -1,\; \mathbf{0},\; 1,\; 2,\; \ldots,\; n-2,\; n-1,$$

ne peut être congru à 0 *modulo* n*, excepté* **0** *au centre.*

Preuve. Soit $e \in [\![-(n-1),\, (n-1)]\!]$ avec $e \equiv 0 \bmod n$. Par la Proposition 9.6, $e = k\,n$ est un multiple de n, avec $k \in \mathbb{Z}$. Clairement, $k = 0$ marche et donne $e = \mathbf{0}$.

Pour $k \neq 0$, puisque $|k| \geqslant 1$, on minore $|e| = |k\,n| = |k|\,n \geqslant n$, donc $e = k\,n$ ne peut *pas* appartenir à l'intervalle $[\![-(n-1),\, (n-1)]\!]$. □

Ensuite, soustrayons les deux représentations de a et de b laissées sur le bord du chemin plus haut :

$$\begin{aligned} a - b \;&\equiv\; (p-q)\,n + r - s \\ &\equiv\; r - s \;\bmod n. \end{aligned} \tag{17.8}$$

En définitive :

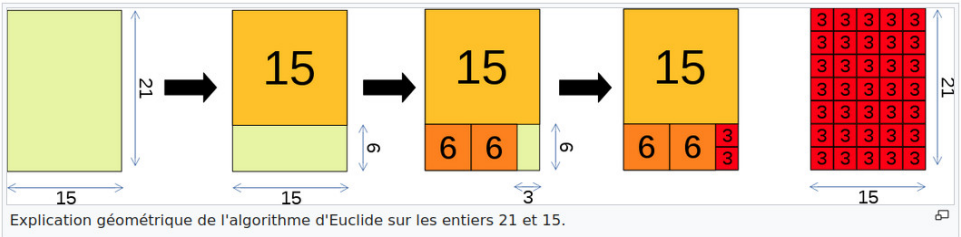
$$\begin{aligned} a \equiv b \mod n &\iff a - b \equiv 0 \mod n \\ \text{[Équation (17.8)]} &\iff r - s \equiv 0 \mod n \\ \text{[Fait 17.7]} &\iff r - s = 0 \\ &\iff r = s. \end{aligned}$$

□

Observons que la deuxième partie de la démonstration a effectivement établi l'équivalence **(ii)** $\Longleftrightarrow$ **(i)** *dans les deux sens*.

18. Algorithme d'Euclide : Histoire et Géométrie

L'algorithme de divisions successives d'Euclide est décrit dans le livre VII, Propositions 1 à 3, des *Éléments* d'Euclide (vers 300 av. J.-C.), sous la forme dite de l'*Anthyphérèse*[11]. Il est aussi décrit dans le livre X, Proposition 2, mais pour un problème de nature géométrique : comment trouver une « unité de mesure » commune pour deux longueurs de segments. L'algorithme procède par soustractions répétées de la longueur du plus court segment sur la longueur du plus long.



Explication géométrique de l'algorithme d'Euclide sur les entiers 21 et 15.

11. *Anthyphèrese* provient du grec $\alpha\nu\theta\upsilon\phi\alpha\iota\rho\varepsilon\iota\nu$, qui signifie « soustraire alternativement ». On appelle donc anthyphérèse une méthode qu'Euclide utilisait pour calculer le plus grand commun diviseur de deux nombres ou pour démontrer que deux longueurs sont incommensurables.

Dans le livre VII, Proposition 2, Euclide préconise en effet d'ôter au plus grand nombre le plus petit, autant que faire se pourra, puis d'ôter le reste au plus petit des nombres, et ainsi de suite.

L'Antyphérèse est de nouveau employée dans le livre X, Théorème 24 pour caractériser deux longueurs incommensurables (on parlerait de nos jours de longueurs dont le rapport est irrationnel). Si le processus se poursuit indéfiniment, les longueurs sont incommensurables. Cette méthode aurait pu être employée, par exemple, pour démontrer l'irrationalité de la racine carrée $\sqrt{2}$ de 2.

Considérons par exemple le rectangle de longueur $L = 21$ et de largeur $l = 15$, dans n'importe quelle unité de mesure. On peut y glisser un carré de côté 15, mais il reste alors un rectangle de côtés 15 et 6.

Qu'à cela ne tienne, glissons-y alors *deux* carrés de côté 6. Carrramba ! Encore rrraté ! Il reste encore un carré de côtés 6 et 3. Sans nous décourager, glissons enfin deux carrés de côté 3 : ouf ! tout est rempli !

Enfin, observons que nos carrés de côté 6 et celui de côté 15 peuvent aussi se carreler en carrés de côté 3. Par conséquent, le rectangle initial tout entier, de côtés 21 et 15, peut se carreler en carrés de côté 3. Et il n'existe pas de carré plus grand permettant un tel carrelage.

Cet algorithme *géométrique* n'a probablement pas été découvert par Euclide lui-même, qui aurait compilé des résultats d'autres mathématiciens dans ses *Éléments*. Pour le mathématicien et historien van der Waerden, le livre VII vient d'un livre de théorie des nombres écrit par un mathématicien de l'école de Pythagore. L'algorithme était probablement connu d'Eudoxe de Cnide (vers 375 av. J.-C.). Il se peut même que l'algorithme ait existé avant Eudoxe, sachant que le terme technique utilisé $\alpha\nu\theta\upsilon\phi\alpha\iota\rho\varepsilon\iota\nu$, soustraction réciproque — apparaît déjà dans les œuvres d'Aristote.

Quelques siècles plus tard, l'algorithme « d'Euclide » est (ré)inventé de manière indépendante à la fois en Inde et en Chine. L'objectif était de résoudre des équations diophantiennes issus de l'astronomie et de faire des calendriers plus précis. Au V$^{\text{ième}}$ siècle, le mathématicien et astronome indien Aryabhata a décrit cet algorithme comme le « *pulvérisateur* », à cause de son efficacité pour résoudre les équations diophantiennes.

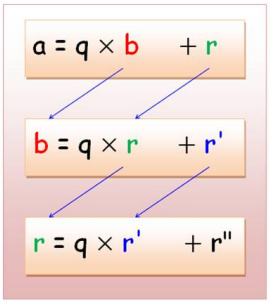
Exemple 18.1. Avant d'aborder l'algorithme général, présentons un autre calcul concret. Il est avisé de représenter synoptiquement la recherche du plus grand commun diviseur entre 126 et 35 :

$$\begin{aligned}
126 &\overset{126 \geqslant 35}{=} 3 \cdot 35 + 21 \\
35 &\overset{35 \geqslant 21}{=} 1 \cdot 21 + 14 \\
21 &\overset{21 \geqslant 14}{=} 1 \cdot 14 + 7 \\
14 &\overset{14 \geqslant 7}{=} 2 \cdot \boxed{7} + \mathbf{0},
\end{aligned}$$

et ici, puisque le dernier reste $\mathbf{0}$ est nul, l'avant-dernier reste $\boxed{7}$ est le pgcd recherché.

Exemple 18.2. De manière alternative, on peut représenter sous forme d'un tableau un autre calcul qui montre que 315 et 307 n'ont aucun facteur en commun, *i.e.* ont un plus grand commun diviseur égal à 1. En effet, le Théorème 20.2 de Bézout *infra* va nous expliquer dans un instant que cela est *démontré* par le fait que l'*avant-dernier* reste dans l'avant-dernière ligne $3 = 2 \times 1 + 1$ est égal à $\mathbf{1}$.

	Dividende	Diviseur	Reste
315 =1 x 307 + 8	315	307	8
307 = 8 x 38 + 3	307	8	3
8 = 2 x 3 + 2	8	3	2
3 = 2 x 1 + 1	3	2	1
2 = 2 x 1 + 0	2	1	0



Notre « plan T », *i.e.* Théorique, est le suivant.

☐ Décrire précisément l'algorithme d'Euclide

☐ Montrer qu'il permet naturellement de trouver facilement le *plus grand commun diviseur* entre deux entiers donnés.

☐ Montrer qu'il permet aisément de trouver une *relation de Bézout* $a\,u + b\,v = 1$ entre deux entiers a et b qui sont *premiers entre eux*.

Tous ces termes et concepts nouveaux vont être définis rigoureusement dans un instant, mais à travers les exemples qui précèdent, nous avons en fait déjà deviné plus de $50\,\%$ de ce qu'ils sont.

19. Algorithme d'Euclide : Plus Grand Commun Diviseur (PGCD)

Soient deux entiers relatifs quelconques $a, b \in \mathbb{Z}$. Quitte à les multiplier par -1 si besoin est, on peut les supposer positifs pour introduire la

Définition 19.1. Le *plus grand commun diviseur* de deux entiers $a \geqslant 0$ et $b \geqslant 0$ avec $(a,b) \neq (0,0)$, noté $\mathsf{pgcd}\,(a,b)$, est le plus grand entier $d \geqslant 1$ qui les divise tous les deux, à savoir :

$$\mathsf{pgcd}\,(a,b) \;:=\; \mathsf{max}\,\Big\{d \geqslant 1 :\;\; d \,|\, a \text{ et } d \,|\, b\Big\}.$$

Quand $a = 0$ et $b = 0$, on convient que $\mathsf{pgcd}\,(0,0) = 0$. Pour $a, b \in \mathbb{Z}$ éventuellement négatifs, on convient que :

$$\mathsf{pgcd}\,(a,b) \;:=\; \mathsf{pgcd}\,\big(|a|,\,|b|\big).$$

L'ensemble sur lequel on prend un maximum est non vide, car $d = 1$ lui appartient, et il est majoré, car pour des nombres positifs, $d \,|\, a$ implique $d \leqslant a$, d'où :

$$\mathsf{pgcd}\,(a,b) \;\leqslant\; \mathsf{min}\,(a,b).$$

Évidemment, on a :

$$\mathsf{pgcd}\,(b,a) \;=\; \mathsf{pgcd}\,(a,b).$$

Si $a = 0$ et $b \geqslant 1$, il est clair que le plus grand entier $d \geqslant 0$ divisant 0 et b est $d = b$. Par symétrie, on a donc :

$$\mathsf{pgcd}\,(0,b) \;=\; b \qquad\qquad \text{et} \qquad\qquad \mathsf{pgcd}\,(a,0) \;=\; a.$$

La notion de pgcd n'est donc intéressante que lorsque $a \geqslant 1$ et $b \geqslant 1$.

Par exemple, $\mathsf{pgcd}\,(10,30) = 10 = 2 \cdot 5$, parce que $20 = 2^2 \cdot 5$ et $30 = 2 \cdot 3 \cdot 5$, ce que nous comprendrons bientôt dans un contexte très général.

La Définition 19.1 se généralise aisément au $\mathsf{pgcd}\,(a,b,c)$ entre trois entiers quelconques $a, b, c \in \mathbb{N}$. Par exemple, $\mathsf{pgcd}\,(36,48,60) = 12 = 2^2 \cdot 3$, parce que $36 = 2^2 \cdot 3^2$, puis $48 = 2^4 \cdot 3$, et enfin $60 = 2^2 \cdot 3 \cdot 5$. Nous y reviendrons plus tard.

Question 19.2. *Comment déterminer le* $\mathsf{pgcd}\,(a,b)$ *entre deux entiers quelconques* $a \geqslant 1$ *et* $b \geqslant 1$ *?*

Réponse : grâce à l'algorithme d'Euclide !

Ainsi, on peut supposer $a \geqslant 1$ et $b \geqslant 1$. Quitte à les permuter, on peut aussi supposer que $a \geqslant b \geqslant 1$. Alors, *divisons avec reste* a par b :

$$a \;=\; q\,b + r,$$

avec des entiers naturels q et $0 \leqslant r < b$. Mais comme r est (strictement) inférieur à b, on peut spontanément avoir l'idée de re-diviser b par r ! Ce qui donne :

$$b \;=\; u\,r + s,$$

avec un certain reste $0 \leqslant s < r$. Mais alors pour la même raison, on peut donc encore re-diviser r par s :

$$r \;=\; v\,s + t,$$

avec encore un certain reste $0 \leqslant t < s$, et ainsi de suite.

Comme l'alphabet ne contient qu'un nombre limité de lettres, si on veut décrire complètement ce procédé, il est nécessaire d'introduire un formalisme mathématique avec des *indices*. Commençons alors par renommer :

$$r_0 := a, \qquad r_1 := b, \qquad q_1 := q, \qquad r_2 := r,$$

de telle sorte que nos deux premières divisions peuvent s'écrire :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \end{aligned}$$

en nommant r_3 le dernier reste qui apparaît.

Alors en poursuivant indéfiniment ces divisions successives, nous aboutissons à un résultat qui peut être représenté au moyen d'un diagramme en forme diagonale descendante :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \\ &\ddots \quad \ddots \quad \ddots \\ r_{i-1} &= q_i\,r_i + r_{i+1}, \\ &\ddots \quad \ddots \quad \ddots \\ r_{\ell-2} &= q_{\ell-1}\,r_{\ell-1} + \boxed{r_\ell}, \\ r_{\ell-1} &= q_\ell\,\boxed{r_\ell} + \mathbf{0}, \end{aligned}$$

avec, à chaque étape, un nouveau reste r_{i+1} strictement inférieur au précédent :

$$0 \leqslant r_{i+1} < r_i.$$

Assertion 19.3. *À partir d'un certain rang, le dernier reste obtenu devient égal à* $\mathbf{0}$.

Preuve. En partant du premier reste :

$$r = r_2 < b,$$

les restes suivants décroissent strictement à chaque étape :

$$0 \leqslant \cdots\cdots < r_3 < r_2 < b,$$

et comme ils sont tous positifs, ils sont minorés par 0.

Le nombre de restes r_i strictement positifs est donc nécessairement *fini*. Appelons alors ℓ ce nombre, avec $\ell \geqslant 1$ et $r_\ell \neq 0$, exactement comme cela était visible dans l'avant-dernière ligne du diagramme en diagonale descendante.

Par définition de ℓ, le prochain reste $r_{\ell+1} = \mathbf{0}$ est nécessairement nul. C'est bien ce que montre la dernière ligne écrite dans le diagramme. □

Ce dernier reste non nul $r_\ell \neq 0$ joue un rôle capital dans la théorie arithmétique.

Proposition 19.4. *On a* $r_\ell = \mathsf{pgcd}\,(a, b)$.

Démonstration. Notons de manière abrégée $d := \mathsf{pgcd}\,(a, b)$. Ainsi, $d \,|\, r_0$ et $d \,|\, r_1$, avec d maximal, d'ailleurs.

Comme $r_2 = r_0 - q_1\, r_1$, on voit que $d \,|\, r_2$ aussi, puisque r_0, r_1 multiples de d impliquent $r_0 - q_1\, r_1$ multiple de d.

Ensuite, $r_3 = r_1 - q_2\, r_2$ est aussi divisible par d, et ainsi de suite.

À la fin, $d \,|\, r_{\ell-2}$ et $d \,|\, r_{\ell-1}$ impliquent $d \,|\, r_\ell$, car $r_\ell = r_{\ell-2} - q_{\ell-1}\, r_{\ell-1}$. Autrement dit $\mathsf{pgcd}\,(a, b) \,|\, r_\ell$, et donc :

$$\mathsf{pgcd}\,(a, b) \leqslant r_\ell. \tag{19.5}$$

Maintenant, comme des saumons, remontons la cascade diagonale, en partant du bas (droite) vers le haut (gauche). L'égalité $r_{\ell-1} = q_\ell\, r_\ell$ dit que $r_{\ell-1}$ est divisible par r_ℓ.

Puis $r_{\ell-2} = q_{\ell-1}\, r_{\ell-1} + r_\ell$ entraîne que $r_{\ell-2}$ est divisible par r_ℓ.

Puis $r_{\ell-3} = q_{\ell-2}\, r_{\ell-2} + r_{\ell-1}$ entraîne que $r_{\ell-3}$ est divisible par r_ℓ, *et ainsi de suite*.

À la fin, c'est-à-dire en haut (regarder encore le diagramme), à l'avant-dernier étage supérieur, $r_1 = q_2\, r_2 + r_3$ entraîne que $r_1 = b$ est divisible par r_ℓ, puis, à la source du torrent tout en haut, $r_0 = q_1\, r_1 + r_2$ entraîne que $r_0 = a$ est divisible par r_ℓ.

Ainsi, $r_\ell \,|\, a$ et $r_\ell \,|\, b$. Comme le pgcd est le *plus grand* des diviseurs simultanés possibles, il est clair que :

$$r_\ell \leqslant \mathsf{pgcd}\,(a, b),$$

ce qui est l'inégalité *opposée* de celle, (19.5), déjà obtenue. En conclusion, on a bien :

$$\mathsf{pgcd}\,(a, b) = r_\ell.$$ □

Ensuite, on peut se convaincre en y réfléchissant que toutes ces opérations ne dépendent que des deux entiers a et b fournis au départ. En particulier, tous les restes r_i construits pas à pas ne dépendent que de a et de b. Et dans un instant, nous allons dévoiler des *formules* qui expriment les restes r_i comme *combinaison linéaires* de a et de b.

À cette fin, outre la suite connue :

$$r_0 := a, \qquad r_1 := b, \qquad r_{i+1} := r_{i-1} - q_i\, r_i \qquad (1 \leqslant i \leqslant \ell - 1),$$

introduisons les *deux* suites auxiliaires assez similaires :

$$u_0 := 1, \qquad u_1 := 0, \qquad u_{i+1} := u_{i-1} - q_i\, u_i \qquad (1 \leqslant i \leqslant \ell - 1),$$
$$v_0 := 0, \qquad v_1 := 1, \qquad v_{i+1} := v_{i-1} - q_i\, v_i \qquad (1 \leqslant i \leqslant \ell - 1).$$

Lemme 19.6. *Pour tout $i = 0, 1, 2, \ldots, \ell$, le reste r_i se représente comme la combinaison linéaire suivante de a et de b :*

$$u_i\, a + v_i\, b \;=\; r_i.$$

Démonstration. Pour $i = 0$, vérifions :

$$u_0\, a + v_0\, b \;=\; 1 \cdot a + 0 \cdot b \overset{?}{=} r_0,$$

ce qui est vrai car $a = r_0$ par définition.

Pour $i = 1$, vérifions :

$$u_1\, a + v_1\, b \;=\; 0 \cdot a + 1 \cdot b \overset{?}{=} r_1,$$

ce qui est à nouveau vrai car $b = r_1$ par définition.

En raisonnant par récurrence *double*, supposons que pour un certain indice i avec $1 \leqslant i \leqslant \ell - 1$, on ait démontré les *deux* formules :

$$u_{i-1}\, a + v_{i-1}\, b \;=\; r_{i-1},$$
$$u_i\, a + v_i\, b \;=\; r_i,$$

et demandons-nous si, à l'étage en-dessous, on a encore :

$$u_{i+1}\, a + v_{i+1}\, b \overset{?}{=} r_{i+1},$$

ou, de manière équivalente, si on a :

$$\big(u_{i-1} - q_i\, u_i\big)\, a + \big(v_{i-1} - q_i\, v_i\big)\, b \overset{?}{=} r_{i-1} - q_i\, r_i.$$

Mais après réorganisation, et factorisation de deux termes à gauche par q_i, ceci équivaut à l'identité vraie tautologiquement :

$$\underbrace{u_{i-1}\, a + v_{i-1}\, b}_{= r_{i-1}} - q_i \Big(\underbrace{u_i\, a + v_i\, b}_{= r_i} \Big) \overset{\text{oui}}{=} r_{i-1} - q_i\, r_i. \qquad \square$$

À la fin tout en bas, pour $i = \ell$, on obtient donc une représentation :

$$u_\ell\, a + v_\ell\, b \;=\; \mathsf{pgcd}\,(a, b),$$

du $\mathsf{pgcd}\,(a, b) = r_\ell$ comme combinaison linéaire de a et de b.

Théorème 19.7. *Le* pgcd *entre deux entiers quelconques donnés $a \geqslant b \geqslant 1$ se calcule en effectuant l'algorithme d'Euclide, et en mémorisant les résultats intermédiaires jusqu'à obtenir :*

$$\mathsf{pgcd}\,(a, b) \;=\; u_\ell\, a + v_\ell\, b \qquad (\exists\, u_\ell \in \mathbb{Z},\ \exists\, v_\ell \in \mathbb{Z}). \quad \square$$

Toutefois, cet énoncé n'est pas assez précis, *techniquement*. Il sous-entend que l'on doit implémenter les trois suites $\{r_i\}_{i=0}^{\ell}$, $\{u_i\}_{i=0}^{\ell}$, $\{v_i\}_{i=0}^{\ell}$, ce qui fonctionne très bien sur ordinateur, mais comme les ordinateurs ne sont pas autorisés lors des examens universitaires, il est tout à fait légitime de se poser la

Question 19.8. *Comment calculer, concrètement et manuellement, une représentation linéaire du* pgcd *entre deux entiers sous la forme :*

$$\mathsf{pgcd}\,(a,b) \;=\; u\,a + v\,b \;\textbf{?}$$

Répondons à cette question en traitant un exemple, qui va nous faire comprendre comment les deux suites auxiliaires $\{u_i\}_{i=0}^{\ell}$, $\{v_i\}_{i=0}^{\ell}$ interviennent naturellement.

Soit, comme précédemment, à déterminer $\mathsf{pgcd}\,(126,\,35)$. Comme nous l'avons déjà vu, l'algorithme d'Euclide donne :

$$\begin{aligned} 126 \;&=\; 3\cdot 35 \,+\, 21 \\ 35 \;&=\; 1\cdot 21 \,+\, 14 \\ 21 \;&=\; 1\cdot 14 \,+\, \mathbf{7} \\ 14 \;&=\; 2\cdot \mathbf{7} + \mathbf{0}, \end{aligned}$$

un pgcd égal à $\mathbf{7}$, au bout de $\ell \,=\, 4$ lignes. Alors, *comment trouver* u_4 *et* v_4 *satisfaisant* $u_4\,126 + v_4\,35 = \mathbf{7}$ *?* En se ré-incarnant sous la peau d'un saumon !

Partons en effet de l'avant-dernière ligne, en ne conservant que $\mathbf{7}$ à droite — attention ! il faut lire ces calculs du bas-droite vers le haut-gauche ! —, et remplaçons via la commande $\underline{\quad}_{\text{rpl}}$:

$$\begin{aligned} 2\cdot 126 - 7\cdot 35 \;&=\; -1\cdot 35 + 2\cdot\big(126 - 3\cdot 35\big) \;= \\ -1\cdot 35 + 2\cdot \underline{21}_{\text{rpl}} \;&=\; 21 - 1\cdot\big(35 - 1\cdot 21\big) \;= \\ 21 - 1\cdot \underline{14}_{\text{rpl}} \;&=\; \mathbf{7}. \end{aligned}$$

Effectivement, on a bien en haut à gauche $252 - 245 = \mathbf{7}$.

« Pour le fun », et avant de clore cette section, toujours avec $r_0 = a$ et $r_1 = b$, expliquons ce qui se passe généralement lorsqu'on a 4 étages :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \\ r_2 &= q_3\,r_3 + \mathbf{r_4}, \\ r_3 &= q_4\,\mathbf{r_4} + \mathbf{0}, \end{aligned}$$

ce qui donne en remontant depuis l'avant-dernière ligne :

$$\underbrace{(1+q_3\,q_2)}_{=:\,u_4} r_0 + \underbrace{(-q_3 - q_1 - q_3\,q_2\,q_1)}_{=:\,v_4} r_1 = -\,q_3\,r_1 + \big(1+q_3\,q_2\big)\big(r_0 - q_1\,r_1\big) =$$

$$-\,q_3 r_1 + \big(1+q_3 q_2\big)\,\underline{r_2}_{\text{rpl}} \;=\; r_2 - q_3\big(r_1 - q_2 r_2\big) =$$

$$r_2 - q_3 \underline{r_3}_{\text{rpl}} \;=\; \mathbf{r_4}.$$

20. Théorème de Bézout

Cette valeur terminale $r_\ell \,=\, \mathsf{pgcd}\,(a,b)$ de l'algorithme d'Euclide vaut parfois $r_\ell \,=\, 1$, et parfois, elle satisfait $r_\ell \,\geqslant\, 2$. Ces deux cas sont extrêmement différents, et ils motivent une conceptualisation adéquate. Rappelons que pour deux entiers a et b éventuellement négatifs, on a défini :

$$\mathsf{pgcd}\,(a,b) \;:=\; \mathsf{pgcd}\,\big(|a|,\,|b|\big).$$

Définition 20.1. On dit que deux entiers relatifs $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont *premiers entre eux* lorsque [12] :

$$1 \;=\; \mathsf{pgcd}\,(a,b),$$

et on note cette propriété [13] :

$$a \wedge b \;=\; 1.$$

On dit parfois aussi que a *est premier à* b, ou que b *est premier à* a.

L'aboutissement ultime de l'algorithme d'Euclide, c'est le résultat hyper-important suivant, ultra présent dans tous les exercices et dans tous les examens de L1, L2, L3, M1, et dont le slogan mnémotechnique [14] pourrait être : « *Bézout partout* ».
i

Théorème 20.2. [Bézout] *Pour toute paire d'entiers $a, b \in \mathbb{Z}$ quelconques avec $(a,b) \neq (0,0)$, il existe $u, v \in \mathbb{Z}$ tels que :*

$$u\,a + v\,b \;=\; \mathsf{pgcd}\,(a,b).$$

De plus, on a équivalence entre :

(i) *a et b sont premiers entre eux,* i.e. $1 = a \wedge b$*;*

(ii) *il existe $u, v \in \mathbb{Z}$ tels que $1 = u\,a + v\,b$.*

Les entiers u et v ne sont *jamais* uniques, car en prenant $u' := u + \lambda\,b$ et $v' := v - \lambda\,a$, avec $\lambda \in \mathbb{Z}$ quelconque, on a encore :

$$\big(u + \lambda\,b\big)\,a + \big(v - \lambda\,a\big)\,b \;=\; u\,a + v\,b \;=\; \mathsf{pgcd}\,(a,b).$$

Démonstration. On a vu il y a un instant que :

$$u_\ell\,a + v_\ell\,b \;=\; r_\ell \;=\; \mathsf{pgcd}\,(a,b),$$

donc la première affirmation était en fait déjà « okay ».

(i) $\Longrightarrow$ **(ii)** revient alors à la Définition 20.1.

(ii) $\Longrightarrow$ **(i)** Si donc $1 = u\,a + v\,b$, soit $d \in \mathbb{N}$ un diviseur commun à a et à b. Puisque $d \,|\, a$ et $d \,|\, b$, il vient :

$$d \;\Big|\; \big(u\,a + v\,b\big),$$

c'est-à-dire $d \,|\, 1$, ce qui force $d = 1$. Le maximum des d divisant a et b ne peut donc qu'être égal à 1, donc en conclusion $\mathsf{pgcd}\,(a,b) = 1$. □

12. Ceci exclut $(a,b) = (0,0)$, dont le pgcd vaut 0 par convention
13. Certains auteurs utilisent la notation raccourcie $a \wedge b$ pour désigner $\mathsf{pgcd}\,(a,b)$, ce qui est cohérent.
14. Certains auteurs appellent ce résultat *Théorème de Bachet-Bézout.*

Mais la préciosité de notre langue nous retient avec pudeur d'oser utiliser une terminologie qui pourrait évoquer ou rappeler l'un des jurons compulsifs et dégueulatoires du Capitaine Haddock.

Étant donné deux entiers relatifs non nuls $a, b \in \mathbb{Z}^*$ premiers entre eux, à savoir avec $1 = \mathsf{pgcd}\,(a,b)$, on peut supposer, quitte à changer leurs signes, que $1 \leqslant a, b$, et alors, ce Théorème 20.2 de Bézout fournit $u, v \in \mathbb{Z}$ satisfaisant, quitte à remplacer $v \longmapsto -v$:

$$u\,a - v\,b \,=\, 1.$$

On peut aussi supposer $1 \leqslant a \leqslant b$. On sait qu'il n'y a pas unicité, puisque, pour tout entier $k \in \mathbb{Z}$, on a encore :

$$\big(u + k\,b\big)\,a - \big(v + k\,a\big)\,b \,=\, 1.$$

Question 20.3. *Peut-on restreindre le domaine des valeurs de u et de v, de façon à avoir quand même une certaine forme d'unicité ?*

Le cas $1 = a$ est inintéressant, car alors $1 \wedge b = 1$ est automatique, et en prenant $u := 1$ puis $v := 0$, il est trivial que :

$$1 \cdot 1 - 0 \cdot b \,=\, 1.$$

Donc on peut supposer que $2 \leqslant a \leqslant b$, avec en fait $a < b$ si $1 = a \wedge b$.

Théorème 20.4. *Soient deux entiers $2 \leqslant a \leqslant b$ premiers entre eux. Alors il existe u et v uniques avec :*

$$0 \,\leqslant\, u \,\leqslant\, b-1 \qquad\qquad \textit{et} \qquad\qquad 0 \,\leqslant\, v \,\leqslant\, a-1,$$

satisfaisant une identité de Bézout :

$$u\,a - v\,b \,=\, 1.$$

Démonstration. Unicité. Supposons qu'il y ait deux identités de Bézout :

$$u\,a - v\,b \,=\, 1,$$
$$u'\,a - v'\,b \,=\, 1,$$

avec $0 \leqslant u, u' \leqslant b-1$, et avec $0 \leqslant v, v' \leqslant a-1$. Alors par soustraction, il vient :

$$\big(u - u'\big)\,a \,=\, \big(v' - v\big)\,b, \tag{20.5}$$

avec, comme nous le savons de Marseille :

$$\big|u - u'\big| \,\leqslant\, b-1 \qquad\qquad \text{et} \qquad\qquad \big|v' - v\big| \,\leqslant\, a-1.$$

Mais alors, à cause de la primalité relative $1 = a \wedge b$, le Théorème 21.1 de la Section **21** suivante force dans l'équation (20.5) :

$$a \,\big|\, (v' - v), \qquad\qquad \text{d'où} \qquad\qquad v' \,=\, v,$$
$$b \,\big|\, (u - u'), \qquad\qquad \text{d'où} \qquad\qquad u \,=\, u'.$$

Existence. Répétons que si (u_0, v_0) est une solution quelconque, fournie par le Théorème 20.2 de Bézout :

$$u_0\,a - v_0\,b \,=\, 1,$$

alors pour tout $k \in \mathbb{Z}$, on a encore une solution :

$$\big(\underbrace{u_0 + k\,b}_{=:\,u}\big)\,a - \big(\underbrace{v_0 + k\,a}_{=:\,v}\big)\,b \,=\, 1.$$

Grâce à ce que nous connaissons de la congruence modulo l'entier $a \geqslant 2$, nous pouvons choisir k afin que :

$$0 \,\leqslant\, v_0 + k\,a \,\leqslant\, a-1.$$

Nous avons donc trouvé u et v satisfaisant :

$$u\,a - v\,b \;=\; 1 \qquad\qquad \text{avec} \qquad\qquad 0 \;\leqslant\; v \;\leqslant\; a-1.$$

Assertion 20.6. *Alors automatiquement, on a* $0 \leqslant u \leqslant b-1$.

Preuve. Écrivons :

$$\begin{aligned} u\,a \;&=\; 1 + v\,b && \text{[Implique } u \geqslant 0\text{]} \\ &\leqslant\; 1 + (a-1)\,b \\ &=\; a\,b - (b-1) \\ &\leqslant\; a\,b - 1, && \text{[}2 \leqslant b\text{]} \end{aligned}$$

donc :

$$0 \;\leqslant\; u \;\leqslant\; b - \tfrac{1}{a},$$

et comme u est entier, on a bien $u \leqslant b-1$. □

En conclusion, nous avons bien $u\,a - v\,b = 1$, avec $0 \leqslant u \leqslant b-1$ et avec $0 \leqslant v \leqslant a-1$ uniques. □

21. Théorème de Gauss et applications

Voici un énoncé extrêmement célèbre et universellement utile en arithmétique.

Théorème 21.1. [Gauss] *Si deux entiers* $a, b \in \mathbb{Z}$ *sont premiers entre eux* $a \wedge b = 1$*, alors pour tout* $c \in \mathbb{Z}$ *:*

$$a \;\Big|\; b\,c \qquad\qquad \Longrightarrow \qquad\qquad a \mid c.$$

Informellement : si a est « étranger » à b, il ne peut posséder de « points communs » qu'avec c.

Démonstration. Par le Théorème 20.2 du Bizou, il existe deux entiers $u, v \in \mathbb{Z}$ tels que $u\,a + v\,b = 1$. On a alors $u\,a\,c + v\,b\,c = c$. Comme $a \mid a\,c$ trivialement et comme $a \mid b\,c$ par hypothèse, on obtient :

$$a \;\Big|\; \big(u\,a\,c + v\,b\,c\big),$$

c'est-à-dire $a \mid c$. □

Le Théorème 21.1 de Gauss est très utile, car il permet souvent de simplifier certaines situations. Par exemple si on sait que $3 \mid 2\,n$, alors on peut en conclure que $3 \mid n$. Voici d'autres énoncés parfois bien utiles.

Proposition 21.2. *Soient* a*,* b*,* c *trois entiers quelconques. Si* a *et* b *sont tous les deux premiers à* c*, alors leur produit* $a\,b$ *est aussi premier à* c*.*

Démonstration. Il s'agit de faire voir que :

$$d \;:=\; \mathsf{pgcd}\,\big(ab,\, c\big)$$

est égal à 1.

Comme $d \mid c$, il y a un entier e avec $d\,e = c$. Ensuite, grâce au Théorème 20.2 de Bézout, l'hypothèse $1 = a \wedge c$ s'exprime par une identité :

$$1 \;=\; u\,a + v\,c \;=\; u\,a + (v\,e)\,d,$$

qui montre que a et d sont aussi premiers entre eux.

Par ailleurs, comme $d \,|\, a\,b$ par définition et comme nous venons de dire $1 = d \wedge a$, le Théorème 21.1 de Gauss force $d \,|\, b$. Or par hypothèse, $d \,|\, c$ aussi. Enfin, comme b et c sont premiers entre eux, on a bien $d = 1$.

Une autre preuve plus directe-mécanique consiste à multiplier deux relations de Bézout exprimant les primalités relatives $1 = a \wedge c$ et $1 = b \wedge c$:

$$\begin{aligned} 1 &= a\,u + c\,v, \\ 1 &= b\,r + c\,s, \end{aligned}$$

pour en déduire, grâce à la formule transcendantale de l'unité qui se reproduit elle-même :

$$1 \cdot 1 = 1,$$

une relation de Bézout entre $a\,b$ et c :

$$\begin{aligned} 1 &= \big(a\,u + c\,v\big)\,\big(b\,r + c\,s\big) \\ &= a\,u\,b\,r + a\,u\,c\,s + c\,v\,b\,r + c\,v\,c\,s \\ &= a\,b\,(u\,r) + c\,\big(a\,u\,s + v\,b\,r + v\,c\,s\big). \end{aligned}$$ □

Proposition 21.3. *Si a et b sont deux entiers premiers entre eux, et s'ils divisent tous deux un certain entier c, alors leur produit $a\,b$ divise aussi c.*

Démonstration. En effet, on peut écrire $a\,u = c$ avec un entier u.

Ensuite, comme b divise c et que b est premier à a, le Théorème 21.1 de Gauss nous dit que b doit diviser u, c'est-à-dire $b\,v = u$ avec un entier v.

Enfin, on conclut bien que ab divise c grâce à :

$$c = a\,u = ab\,v.$$ □

Encore une fois, ce dernier résultat est très intuitif : si a et b divisent c, une raison pour laquelle $a\,b$ ne doit pas forcément diviser c est que a et b auront peut-être des diviseurs en commun, et le produit $a\,b$ peut être « trop gros » pour diviser c. Par exemple 6 et 3 divisent 12, mais *pas* leur produit $3 \cdot 6 = 18$ [15].

Mais si on suppose a et b premiers entre eux, ils n'ont par définition aucun diviseur en commun, et on s'attend alors bien à ce que $a\,b$ divise c.

On peut aisément généraliser l'énoncé précédent pour obtenir le résultat suivant, très pratique.

Proposition 21.4. *Soient $a_1, \ldots, a_r$ avec $r \geqslant 2$ des entiers premiers entre eux deux à deux, c'est-à-dire satisfaisant :*

$$1 = \mathsf{pgcd}\,\big(a_{i_1},\, a_{i_2}\big) \qquad (\forall\, 1 \leqslant i_1 \neq i_2 \leqslant r).$$

S'ils divisent tous $a_1 \,|\, n$, …, $a_r \,|\, n$ un entier n donné, alors leur produit $a_1\,a_2 \cdots a_r$ divise aussi l'entier n.

Indication de preuve. Raisonner par récurrence sur le nombre $r \geqslant 2$ d'entiers a_i, en appliquant à chaque fois la Proposition 21.3. □

15. Tout le monde aura maintenant bien compris l'intérêt incomparable du cours d'arithmétique : deux étudiants ayant obtenu 3 sur 20 et 6 sur 20 à l'examen partiel de chimie des matériaux n'auront qu'à entrer en réaction multiplicative afin d'augmenter superbement leur note !

Pour terminer cette Section **21**, revenons maintenant au Théorème 20.2 de « *Bézout-partout*[16] », afin de mieux présenter ce qu'il exprime véritablement.

Considérons le cas général où a et b sont deux entiers quelconques, non nécessairement premiers entre eux, et introduisons :

$$d \,:=\, \mathsf{pgcd}\,(a,b).$$

Comme $d \,|\, a$ et $d \,|\, b$ par définition, on peut factoriser :

$$a \,=\, d\,a' \qquad\qquad \text{et} \qquad\qquad b \,=\, d\,b',$$

au moyen de deux entiers uniques a' et b'. *Que dire alors de a' et de b' ?* Attention ! On doit tenir compte du fait que d est *maximal* parmi les diviseurs communs de a et de b !

Souvenons-nous en effet que le pgcd entre deux entiers représente *tout* ce que ces entiers ont en commun d'un point de vue arithmétique. On doit donc s'attendre à ce que a' et b' soient premiers entre eux — et c'est bien le cas !

Proposition 21.5. *Toute paire d'entiers $a, b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$ se factorise sous la forme :*

$$a \,=\, a' \cdot \mathsf{pgcd}\,(a,b), \qquad\qquad a \,=\, b' \cdot \mathsf{pgcd}\,(a,b), \qquad\qquad \textit{avec} \qquad\qquad 1 \,=\, a' \wedge b'.$$

Preuve. En effet, d'après le Théorème 20.2 de Bézout, $d := \mathsf{pgcd}\,(a,b)$ est combinaison linéaire entière de a et de b :

$$\begin{aligned} d \,&=\, u\,a + v\,b \\ &=\, u\,d\,a' + v\,d\,b', \end{aligned}$$

et après division par d de cette égalité, on voit bien que a' et b' sont premiers entre eux :

$$1 \,=\, u\,a' + v\,b'. \qquad\qquad \square$$

22. Équations linéaires à coefficients entiers

Grâce à toutes ces études préparatoires basées sur l'Algorithme d'Euclide, nous pouvons maintenant étudier un type de problèmes très anciens, auquel le pgcd est très fortement lié : les *équations linéaires à coefficients entiers*. Il s'agit d'équations de la forme :

$$a\,x + b\,y \,=\, c,$$

où a, b, c sont des entiers constants fixés dans $\mathbb{Z}$, et où on cherche des solutions (x,y) telles que $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ soient tous deux entiers.

Exemple 22.1. On dispose de billets de 20 et 50 euros. Combien y a-t-il de façons, et quelles sont-elles, de réunir la somme de 240 euros ?

Après quelques instants de réflexion, on comprend que la question revient précisément à trouver tous les entiers naturels $x \geqslant 0$ et $y \geqslant 0$ tels que :

$$20\,x + 50\,y \,=\, 240.$$

Sans s'aider d'un distributeur de billets, le lecteur est invité à résoudre ce petit exercice par lui-même. Mais pour la question mathématique générale, on admet que x et y puissent être négatifs, *i.e.* avoir un compte en banque à découvert.

16. — c'est-à-dire partout dans les exercices de Travaux Dirigés, les Devoirs à la Maison, les Examens Partiels, et les Examens Terminaux —

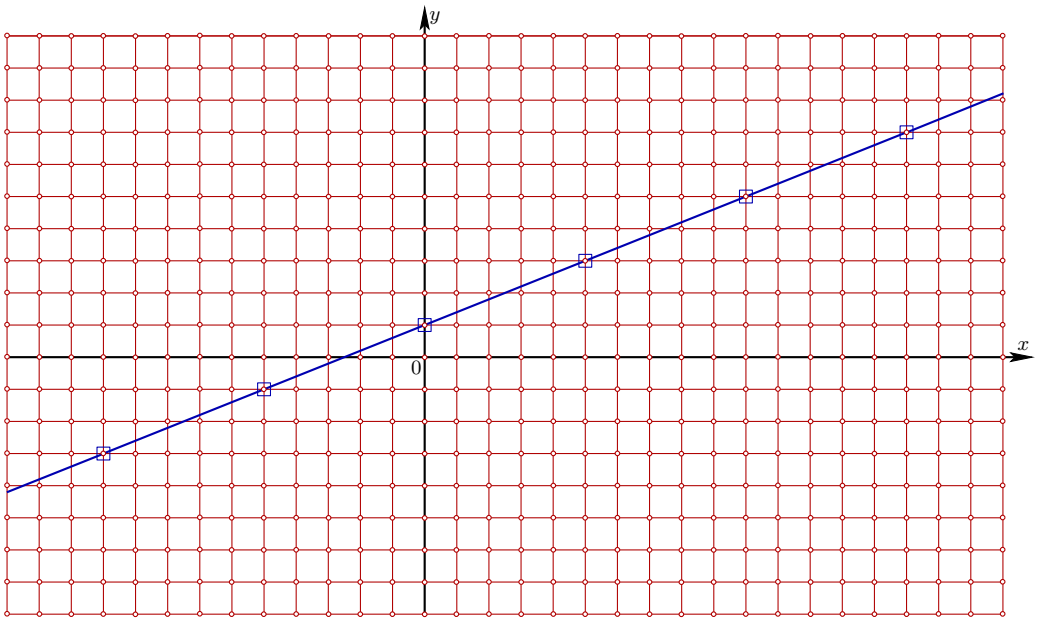
PIÈCES DE MONNAIE

Utilisation des congruences (modulo) pour résoudre un problème de pièces de monnaie

J'achète 351 euros avec un lot de pièces de 17 et 18 euros.
Combien de pièces de chaque?

On pose l'équation	18 x + 17 y = 351
On cherche une solution simple, en utilisant le fait que 17 et 18 sont deux nombres consécutifs	18 – 17 = 1 18 x 351 – 17 x 351 = 351
Retranchons membre à membre les deux équations	18 x + 17 y = 351 18 x 351 – 17 x 351 = 351
Résultat	18(x - 351) = – 17(y + 351)
Et pour x	x = – 17(y + 351)/18 + 351
Si on divise x par 17, on obtient les restes suivants (x mod 17)	x mod 17 = 0 + 351 mod 17
Or, le reste de 351 par 17 est 11	x mod 17 = 11
Autrement dit x est un multiple de 17 plus 11	x = 17 k + 11
Même chose pour y	y = – 18(x - 351) /17 – 351
En reste par 18	y mod 18 = 9 (ou -9)
Valeur de y	y = – 18 k' + 9
Essayons k= k' = 0	18 x 11 + 17 x 9 = 198 + 153 = 351
Avec d'autres valeurs, on trouve des valeurs trop grandes pour x ou négatives pour y	18 x 28 + 17 x 9 = 657 18 x 11 – 17 x 9 = 45
Seule solution	x = 11 et y = 9

En fait, on sait bien que l'équation $a\,x + b\,y = c$ représente une *droite* dans le plan $\mathbb{R}^2$ muni des coordonnées (x, y). Ce plan est un *continu* 2*-dimensionnel*, c'est-à-dire que partout et à tous les endroits, il y a une infinité de points arbitrairement proches les uns des autres. Et nous savons bien qu'au voisinage de chacun de ses points, une droite dans le plan contient *aussi* une infinité de points arbitrairement proches les uns des autres.



Mais si on ne recherche que les solutions *entières* de $a\,x + b\,y = z$, on voit qu'on ne s'intéresse qu'à l'intersection de cette droite avec le *réseau* des nombres entiers :

$$\mathbb{Z} \times \mathbb{Z} \;=\; \big\{(x, y) \in \mathbb{R}^2 \colon\; x \in \mathbb{Z},\; y \in \mathbb{Z}\big\}.$$

Sur la figure, l'équation de la droite est $y = 1 + \frac{2}{5}\,x$, c'est-à-dire $-\,2\,x + 5\,y = 5$, et de cinq en cinq en montant du bas-gauche vers le haut-droite, les petits carrés bleus capturent les points dont les *deux* coordonnées sont entières.

Fixons donc $a, b, c \in \mathbb{Z}$, et examinons tout d'abord, le cas dégénéré où $a = b = 0$ pour lequel l'équation à résoudre :

$$a\,x + b\,y \;=\; 0\,x + 0\,y \;=\; 0 \;\overset{?}{=}\; c,$$

n'a de solutions que si $c = 0$, et dans ce cas :

$$0\,x + 0\,y \;\overset{\text{oui}}{=}\; 0 \qquad\qquad (\forall\, x,\, \forall\, y),$$

est trivialement satisfaite. L'ensemble des solutions est donc (doublement) infini.

On peut donc supposer dorénavant que a et b ne sont pas tous les deux nuls. Alors grâce au Grand Bézout, nous allons pouvoir résoudre totalement cette équation à inconnues entières.

Comme à l'accoutumée, notons $d := \mathsf{pgcd}\,(a, b)$, avec $d \neq 0$ puisque $(a, b) \neq (0, 0)$. Alors $a = d\,a'$ et $b = d\,b'$, avec a' et b' premiers entre eux, comme cela a été vu dans la Proposition 21.5. L'équation à résoudre :

$$a\,x + b\,y \;=\; c \qquad\qquad \Longleftrightarrow \qquad\qquad d\,a'\,x + d\,b'\,y \;=\; c,$$

force visiblement c, à droite, à être multiple de d, à gauche. Donc elle n'a *aucune* solution lorsque c n'est pas divisible par d — *Argl !*

Qu'à cela ne tienne, supposons dorénavant que $c = d\,c'$ est multiple de $d = \mathsf{pgcd}\,(a, b)$. L'équation à résoudre équivaut alors à :

$$d\,a'\,x + d\,b'\,y \;=\; d\,c', \qquad\qquad \Longleftrightarrow \qquad\qquad a'\,x + b'\,y \;=\; c'.$$

Alors le fait que $a' \wedge b' = 1$ *améliore énormément la situation.* Car si jamais on avait $c' = 1$, on reconnaîtrait une relation de Bézout :

$$a'\,x + b'\,y \;=\; 1,$$

dont on sait qu'il existe au moins une solution (x_*, y_*), d'après le Théorème 20.2.

Proposition 22.2. *Soient trois constantes entières quelconques* $a, b, c \in \mathbb{Z}$ *avec* $(a, b) \neq (0, 0)$. *Alors si* $d := \mathsf{pgcd}\,(a, b)$ *divise* c, *l'équation* $a\,x + b\,y = c$ *possède au moins une solution entière* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$

Démonstration. En multipliant par c' une telle solution « *bézoutique* » (x_*, y_*) :

$$c'\,\big(\,a'\,x_* + b'\,y_* \;=\; 1\,\big) \qquad \text{devient} \qquad a'\,\underbrace{(c'\,x_*)}_{=:\,x_0} + b'\,\underbrace{(c'\,y_*)}_{=:\,y_0} \;=\; c',$$

on trouve au moins une solution (x_0, y_0) de $a'\,x_0 + b'\,y_0 = c'$, et enfin après multiplication par d :

$$d\,\big(\,a'\,x_0 + b'\,y_0 \;=\; c'\,\big) \qquad \text{devient} \qquad d\,a'\,x_0 + d\,b'\,y_0 \;=\; d\,c',$$

on trouve une solution (x_0, y_0) de l'équation proposée au début $a\,x_0 + b\,y_0 = c$. □

Et c'est encore de Bézout (partout) que nous allons nous servir pour établir le

Théorème 22.3. *Soient trois constantes entières quelconques* $a, b, c \in \mathbb{Z}$ *avec* $(a, b) \neq (0, 0)$. *Alors l'équation* $a\,x + b\,y = c$ *possède au moins une solution entière* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, *si et seulement si* $d := \mathsf{pgcd}\,(a, b)$ *divise* c.

Dans ce cas, en posant $a = d\,a'$, $b = d\,b'$ *avec* $a' \wedge b' = 1$, *et* $c = d\,c'$, *et en partant d'une solution particulière quelconque* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *de l'équation* [17] :

$$a\,x_0 + b\,y_0 \;=\; c,$$

l'ensemble de toutes *les solutions de* $a\,x + b\,y = c$ *est infini, et est égal précisément à :*

$$\mathsf{Sol} \;:=\; \Big\{\big(x_0 + b'k,\;\; y_0 - a'\,k\big) :\;\; k \in \mathbb{Z}\Big\}.$$

Effectivement, cet ensemble est infini, car il contient autant d'éléments qu'il y a d'entiers quelconques $k \in \mathbb{Z}$. Autrement dit, Sol est *paramétré* par $\mathbb{Z}$.

Démonstration. Quitte à échanger $a \longleftrightarrow b$, on peut supposer que $a \neq 0$. On suppose donc aussi que $c = d\,c'$, sinon, comme nous venons de le constater, il n'y aurait *aucune* solution.

Prenons alors une solution entière quelconque (x, y) de $a\,x + b\,y = c$. L'astuce intersidérale, utilisé dans toutes les galaxies mathématiques autant en Algèbre Linéaire que dans la théorie des Équations Différentielles, consiste à lui *soustraire* une solution particulière :

$$\begin{aligned} a\,x + b\,y \;&=\; c, \\ a\,x_0 + b\,y_0 \;&=\; c \end{aligned} \qquad \Longrightarrow \qquad a\,\big(x - x_0\big) + b\,\big(y - y_0\big) \;=\; 0,$$

afin de se ramener à une équation *plus simple* de second membre égal à 0, et avec *seulement deux termes*.

Dans cette équation, remplaçons $a = d\,a'$ (avec $a' \neq 0$ puisque $a \neq 0$), remplaçons $b = d\,b'$, puis divisons par d (non nul), pour obtenir une égalité :

$$a'\big(x - x_0\big) \;=\; b'\,\big(y_0 - y\big), \tag{22.4}$$

17. — nous venons d'argumenter qu'il en existe au moins une —

qui montre que a' *divise* $b'(y_0 - y)$. Mais comme $a' \wedge b' = 1$, le Théorème 21.1 de Gauss force $y_0 - y$ à être divisible par a'.

Autrement dit, il existe $k \in \mathbb{Z}$ tel que :

$$y_0 - y \;=\; a'\,k,$$

ce qui montre que $y = y_0 - a'k$ est de la forme annoncée dans Sol.

Ensuite, en remplaçant dans (22.4), nous obtenons $a'(x - x_0) = b'a'k$, et après division par a' qui est non nul, nous obtenons aussi l'expression de x annoncée dans Sol :

$$x \;=\; x_0 + b'\,k.$$

En définitive, nous venons d'achever de faire voir que si (x, y) est une solution entière quelconque de $a\,x + b\,y = c$, alors elle est nécessairement de la forme annoncée dans Sol. Yep !

Mais pour terminer rigoureusement la démonstration, il reste encore à vérifier que $x = x_0 + b'k$, $y = y_0 - a'k$ avec $k \in \mathbb{Z}$ *arbitraire* est *effectivement* une solution, ce qui est vrai grâce à une annihilation couplée :

$$\begin{aligned} c &\overset{?}{=} a\,x + b\,y \\ &= d\,a'\,\big(x_0 + b'\,k\big) + d\,b'\,\big(y_0 - a'\,k\big) \\ &= a\,x_0 + \underline{d\,a'\,b'\,k}_{\circ} + b\,y_0 - \underline{d\,b'\,a'\,k}_{\circ} \\ &= c \qquad \text{OUI.} \end{aligned}$$

□

23. Plus Petit Commun Multiple ppcm

La notion de *plus petit commun multiple* est très proche de celle de *plus grand commun diviseur* — elle est en quelque sorte « *duale* ».

Définition 23.1. Le ppcm entre deux entiers positifs $a \geqslant 0$ et $b \geqslant 0$ avec $(a, b) \neq (0, 0)$ est l'entier :

$$\begin{aligned} \mathsf{ppcm}\,(a, b) \;&:=\; \mathsf{min}\,\Big\{n \in \mathbb{N}^* :\;\; n \text{ multiple de } a,\;\; n \text{ multiple de } b\Big\} \\ &=\; \mathsf{min}\,\Big\{n \in \mathbb{N}^* :\;\; a \,|\, n,\;\; b \,|\, n\Big\}. \end{aligned}$$

On convient que $\mathsf{ppcm}\,(0, 0) := 0$, et pour $a, b \in \mathbb{Z}$ de signe quelconque, on pose :

$$\mathsf{ppcm}\,\big(|a|,\, |b|\big) \;:=\; \mathsf{ppcm}\,(a, b).$$

Évidemment, on a pour $a, b \geqslant 0$:

$$\mathsf{ppcm}\,(a, b) \;=\; \mathsf{ppcm}\,(b, a), \qquad\qquad \mathsf{ppcm}\,(a, 0) \;=\; a, \qquad\qquad \mathsf{ppcm}\,(0, b) \;=\; b.$$

Donc puisque le signe ne compte pas, nous pouvons supposer à partir de maintenant que $a \geqslant 1$ et $b \geqslant 1$.

Il existe effectivement un lien fort entre pgcd et ppcm. Déjà, il est clair que $a\,b$ est toujours un multiple commun à a et à b, mais ce n'est cependant pas toujours leur ppcm, car on peut voir qu'il existe souvent des multiples communs à a et à b qui sont plus petits.

Soit en effet $d := \mathsf{pgcd}\,(a, b)$. On peut écrire $a = d\,a'$ et $b = d\,b'$, où a' et b' sont premiers entre eux. Alors $d\,a'\,b'$ est toujours un multiple de a, car il s'agit de $a\,b'$. Mais c'est aussi toujours un multiple de b, puisqu'on peut aussi l'écrire $b\,a'$. C'est donc un multiple commun à a et à b !

Or on voit bien que $d\,a'\,b'$ est en général [18] plus petit que :

$$a\,b \;=\; d^2\,a'\,b'.$$

En fait, nous pouvons démontrer que cet entier $d\,a'\,b'$ *est* le ppcm de a et de b.

Théorème 23.2. *Soient deux entiers $a \geqslant 1$ et $b \geqslant 1$. Soient aussi a', b' avec $1 = a' \wedge b'$ définis par $a = d\,a'$, $b = d\,b'$. Alors :*

$$d \;:=\; \mathsf{pgcd}\,(a,b) \qquad\qquad \textit{et} \qquad\qquad m \;:=\; \mathsf{ppcm}\,(a,b),$$

satisfont :

$$m \;=\; \frac{a\,b}{d} \;=\; d\,a'\,b'.$$

Démonstration. Comme $a \,|\, m$, il existe un entier $k \geqslant 1$ tel que :

$$m \;=\; a\,k \;=\; d\,a'\,k. \tag{23.3}$$

Or $b = d\,b'$ divise aussi m, c'est-à-dire $d\,b' \,\big|\, d\,a'\,k$, d'où $b' \,|\, a'\,k$ après division (simplification) par $d \geqslant 1$. Mais comme b' est premier à a', le Théorème 21.1 de Gauss force $k = b'\,k'$ à être multiple de b', avec $k' \geqslant 1$ entier.

En revenant à (23.3), il vient alors :

$$m \;=\; d\,a'\,b'\,k'.$$

Autrement dit, nous venons de démontrer que tout entier m qui est multiple de a et de b est un multiple, au moyen de $k' \geqslant 1$, de $d\,a'\,b'$.

Mais comme nous avons compris plus haut que $d\,a'\,b'$ *est déjà* multiple de a et de b, et comme m est par définition le *plus petit* multiple commun, il faut choisir $k' := 1$, ce qui conclut l'argumentation. □

Corollaire 23.4. *Avec $a \geqslant 1$ et $b \geqslant 1$ entiers, le produit $a\,b$ coïncide avec* $\mathsf{ppcm}\,(a,b)$ *lorsque, et seulement lorsque* $\mathsf{pgcd}\,(a,b) = 1$. □

24. Décomposition des entiers en facteurs premiers

Introduisons maintenant une notation primordiale, et toujours très riche en mystères mathématiques inexpugnables.

Définition 24.1. Un nombre entier $p \in \mathbb{N}$ est dit *premier* si $p \geqslant 2$ et si ses seuls diviseurs positifs sont $d = 1$ et $d = p$.

Par exemple, 37 est un nombre premier. Il est important de faire remarquer que 1 n'est *pas* considéré comme étant un nombre premier. La plupart du temps, les nombres premiers seront désignés au moyen de la lettre p.

L'ensemble des nombres premiers sera noté :

$$\mathscr{P} \;:=\; \big\{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ \ldots\ \big\},$$

18. — dès que $d \geqslant 2$, car alors $d^2 > d$, strictement —

Voici d'ailleurs la liste complète de tous ceux qui sont inférieurs à 1 000 :

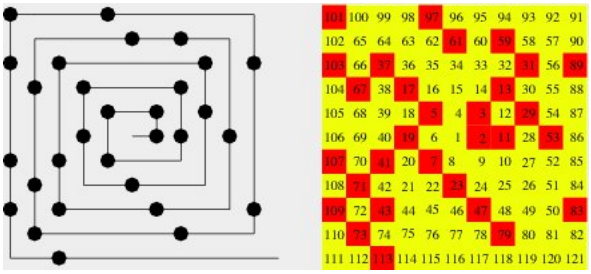
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137,
139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211,
223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283,
293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461,
463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563,
569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643,
647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739,
743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829,
839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937,
941, 947, 953, 967, 971, 977, 983, 991, 997.

Certaines représentations imagées sont plus parlantes.

2 3 5 7 11 13 17
19 23 29 31 37 41
43 47 53 59 61 67
71 73 79 83 89 97

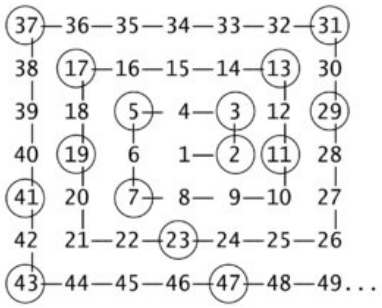
					0				
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

En mathématiques, la *spirale d'Ulam*, ou spirale des nombres premiers est une méthode simple pour représenter les nombres premiers qui révèle un motif qui n'a jamais été pleinement expliqué. Elle fut découverte par le mathématicien Stanislaw Ulam, lors d'une conférence scientifique en 1963.

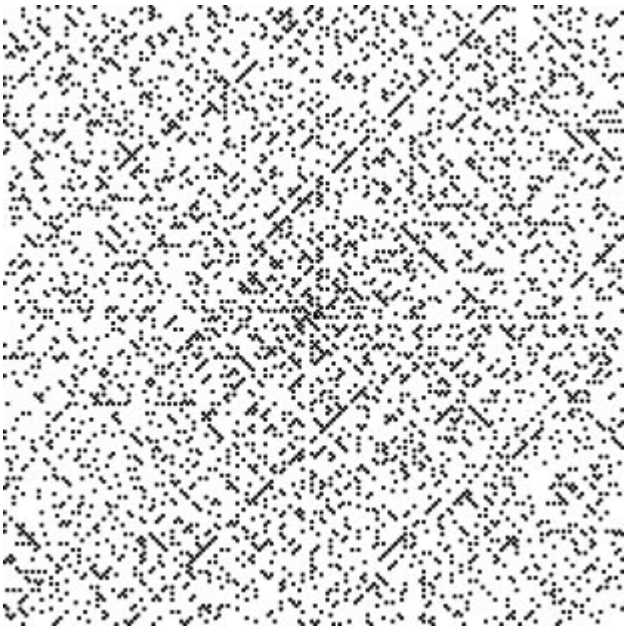


Ulam se trouvait coincé, contraint d'écouter « un exposé très long et très ennuyeux ». Il passa son temps à crayonner et se mit à gribouiller des entiers consécutifs, commençant par 1 au centre, dans une espèce de spirale tournant dans le sens inverse des aiguilles d'une montre. Il obtint une grille régulière de nombres, démarrant par 1 au centre, et spiralant vers l'extérieur, comme ci-dessous. Puis, Ulam entoura tous les nombres premiers, et il obtint alors l'image suivante.

```
37─36─35─34─33─32─31
│                  │
38 17─16─15─14─13 30
│  │           │  │
39 18  5─ 4─ 3  12 29
│  │  │     │  │  │
40 19  6   1─ 2  11 28
│  │  │        │  │
41 20  7─ 8─ 9─10 27
│  │              │
42 21─22─23─24─25─26
│
43─44─45─46─47─48─49...
```



À sa surprise, les nombres entourés tendaient à s'aligner le long de lignes diagonales. L'image suivante illustre ceci. C'est une spirale d'Ulam de 200×200, où les nombres premiers sont des points noirs. Des *diagonales noires* sont clairement visibles.



Il apparaît donc des lignes diagonales comportant une grande quantité de nombres premiers. Ceci semble rester vrai, même si le nombre central au départ est plus grand que 1. On remarque donc qu'il semble exister une infinité d'entiers naturels a, b et c tels que la fonction :

$$f(n) := a\,n^2 + b\,n + c$$

génère un nombre extraordinairement grand de nombres premiers. Néanmoins, aucune démonstration n'est connue sur Terre qu'il existe une *infinité* de nombres premiers de la forme $a\,n^2 + b\,n + c$ pour $a \neq 0$, b, c bien choisis.

Pour les traqueurs de nombres premiers, ces nombres étaient familiers. Au XVIII$^{\text{ième}}$ siècle, Euler avait avancé la formule n^2+n+17 qui, pour des valeurs successives de n, donnait des nombres premiers de $n = 0$ à $n = 15$. En fait, ces seize nombres premiers sont ceux qui apparaissent sur la diagonale principale de la spirale d'Ulam avec 17 comme nombre central de départ : 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227 et 257.

Euler proposa une autre formule, $n^2 - n + 41$ qui, pour des valeurs successives de n entre 1 et 40, ne produit que des nombres premiers.

Par calcul sur ordinateur, on montra que la formule d'Euler $n^2 - n + 41$ était étonnamment bonne, puisqu'elle engendre des nombres premiers inférieurs à dix millions dans 47,5% des cas.

Après cette parenthèse culturelle, revenons au cours formel.

Proposition 24.2. *Deux nombres premiers $p \neq p' \in \mathscr{P}$* distincts *sont toujours premiers entre eux $p \wedge p' = 1$.*

Autrement dit, leur pgcd est égal à 1.

Démonstration. Notons donc $d := \mathsf{pgcd}\,(p, p')$. On a $d \,|\, p$ et $d \,|\, p'$, et comme les seuls diviseurs d'un nombre premier sont 1 et lui-même, il vient :

$$\Big(\ d = 1 \quad \text{ou} \quad d = p\ \Big) \qquad \text{et} \qquad \Big(\ d = 1 \quad \text{ou} \quad d = p'\ \Big).$$

La seule possibilité commune — c'est-à-dire satisfaisant ce « et » — est $d = 1$. □

Ensuite, nous pouvons obtenir l'énoncé suivant, dans lequel le symbole $\nmid$ signifie « *ne divise pas* ».

Proposition 24.3. *Soit un nombre premier $p \in \mathscr{P}$. Alors, pour tout $a \in \mathbb{Z}$, on a équivalence entre :*

(i) *p et a sont premiers entre eux ;*

(ii) *$p \nmid a$.* □

Démonstration. L'implication **(i)** $\Longrightarrow$ **(ii)** est évidente, car en partant de $1 = p \wedge a$, si on avait non **(ii)**, c'est-à-dire si p divisait a, alors $\mathsf{pgcd}\,(p, a) = p$ serait > 1 !

Montrons maintenant **(ii)** $\Longrightarrow$ **(i)**. Soit $d := \mathsf{pgcd}\,(p, a)$, d'où $d \,|\, p$, donc $d = 1$ ou $d = p$ car p est premier. Mais $d = p$ est impossible, car $d \,|\, a$ et $p \nmid a$ par l'hypothèse **(ii)**. Donc $d = 1 = p \wedge a$, c'est-à-dire que p et a sont premiers entre eux. □

On en déduit un troisième énoncé, classique et célèbre.

Théorème 24.4. [Euclide] *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous $a, b \in \mathbb{Z}$, on a :*

$$p \,\big|\, a\,b \qquad \Longrightarrow \qquad \Big(\ p \mid a \quad \textit{ou} \quad p \mid b\ \Big).$$

Si de plus a et b sont premiers, alors $p = a$ ou $p = b$.

Autrement dit, un « atome » donné ne peut se trouver que dans une seule des deux molécules, et si les molécules elles-mêmes sont des atomes, alors l'atome donné est *égal* à l'une des deux.

Démonstration. Soient $a, b \in \mathbb{Z}$ avec $p \,|\, a\,b$. Si $p \,|\, a$, il n'y a rien à faire.

Si $p \nmid a$, alors la Proposition 24.3 précédente montre que a et p sont premiers entre eux. Mais alors le Théorème 21.1 de Gauss garantit que $p \,|\, b$, ce qui était annoncé.

Quand a et b sont premiers, par définition, leurs seuls diviseurs sont 1, a et 1, b. On vient d'obtenir $p \,|\, a$ ou $p \,|\, b$. Si c'est $p \,|\, a$, alors $p = a$. Si c'est $p \,|\, b$, alors $p = b$. □

La généralisation suivante du Théorème 24.4 d'Euclide va s'avérer d'une utilité extrêmement importante sur le plan technique dans ce qui va suivre.

Proposition 24.5. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous $a, b, c, \ldots, \ell \in \mathbb{Z}$, on a :*

$$p \,\big|\, a\,b\,c \cdots \ell \qquad \Longrightarrow \qquad \Big(\ p \mid a \quad \textit{ou} \quad p \mid b \quad \textit{ou} \quad p \mid c \quad \textit{ou} \quad \cdots \quad \textit{ou} \quad p \mid \ell\ \Big).$$

Si de plus tous les facteurs $a, b, \ldots, \ell$ sont premiers, alors $p = a$, ou $p = b$, …, ou $p = \ell$.

Démonstration. Il suffit de raisonner par récurrence sur le nombre de facteurs en appliquant successivement le Théorème 24.4 précédent. □

Terminologie 24.6. Étant donné un nombre entier $n \geqslant 2$, on appelle *diviseur* de n tout entier $d \mid n$ qui divise n. On dit que d est un *diviseur strict* lorsqu'on a de plus $1 < d < n$.

Alors on peut écrire $n = d\,m$ avec $m \in \mathbb{N}$. Dans le cas strict $1 < d < m$, observons que l'on a aussi $1 < m < n$. En effet, si on avait $m = 1$, on aurait $n = d$, ce qui n'est pas. Si on avait $m = n$, on aurait $1 = d$, ce qui n'est pas non plus.

Nous pouvons dorénavant énoncer et démontrer le résultat principal de ce chapitre, « découpé » en deux théorèmes, d'existence, puis d'unicité.

Théorème 24.7. *Tout entier $n \geqslant 2$ se décompose comme produit d'un nombre fini $r \geqslant 1$ de puissances de nombres premiers :*

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $2 \leqslant p_1 < \cdots < p_r$ premiers, et avec des exposants $\alpha_1 \geqslant 1$, …, $\alpha_r \geqslant 1$.

Voici trois exemples de telles décompositions :

$$\begin{aligned} 888 &= 2^3 \cdot 3 \cdot 37, \\ 1\,235 &= 5 \cdot 13 \cdot 19, \\ 5\,040 &= 5 \cdot 2^4 \cdot 3^2 \cdot 7. \end{aligned}$$

Il s'agit donc de décompositions « atomiques » de chaque « nombre entier-molécule ». Ce théorème s'appelle *Théorème fondamental de l'arithmétique*, car la structure arithmétique d'un nombre entier dépend uniquement de sa décomposition en produit de nombres premiers. Les nombres premiers sont ainsi les « particules élémentaires » qui constituent l'arithmétique (labyrinthique) des nombres entiers.

Rappelons que l'entier 1 n'est pas un nombre premier. Pourquoi ? Parce que multiplier un entier n par 1 ne le change en rien : $n \cdot 1 = n$, et donc, 1 ne peut en aucun cas être considéré comme une « brique » de construction.

Démonstration. Expliquons donc l'*existence* d'une telle décomposition.

À cet effet, introduisons l'ensemble $\overline{E}$ des entiers naturels $\overline{n} \geqslant 2$ qui ne s'écrivent *pas* comme un produit (fini) $\prod p_i^{\alpha_i}$ de nombres premiers, avec certaines puissances lorsqu'il y a des répétitions. Notre but est de montrer que $\overline{E} = \emptyset$.

Supposons alors par l'absurde que $\overline{E} \neq \emptyset$. Grâce au Théorème 4.1, $\overline{E}$ admet alors un *plus petit élément*, disons $\overline{n} \in \overline{E}$.

Clairement, $\overline{n}$ ne peut pas être égal à un nombre premier $p \in \mathscr{P}$. Mais alors, comme $\overline{n}$ n'est *pas* un nombre premier, il existe forcément (et logiquement), d'après la Définition 24.1, un diviseur *strict* d de $\overline{n}$, qui satisfait l'inégalité $1 < d < \overline{n}$. On a ainsi $\overline{n} = d\,m$, avec $m \in \mathbb{N}$ satisfaisant aussi $1 < m < \overline{n}$.

D'après la minimalité de $\overline{n}$, ces deux entiers $d < \overline{n}$ et $m < \overline{n}$ n'appartiennent *pas* à $\overline{E}$, et donc eux, il *peuvent* tous deux s'écrire comme un produit fini de puissances de nombres premiers :

$$d \;=\; p_1^{\gamma_1} \cdots p_i^{\gamma_i} \qquad \text{et} \qquad d \;=\; q_1^{\delta_1} \cdots q_j^{\delta_j}.$$

Mais alors, il clair et évident que leur *produit* $d\,m \;=\; \overline{n}$ devient aussi un produit fini $\prod p_i^{\gamma_i} \prod q_j^{\delta_j}$ de puissances de nombres premiers — ce qui est une contradiction manifeste. Donc $\overline{E} = \emptyset$, comme voulu. □

Ensuite, traitons de l'*unicité* de la décomposition en nombres premiers.

Théorème 24.8. *La décomposition de tout entier $n \geqslant 2$ en produit de nombres premiers :*

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $2 \leqslant p_1 < \cdots < p_r$ premiers et $\alpha_1, \ldots, \alpha_r \geqslant 1$, est unique*, au sens où si l'on a aussi :*

$$n \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s},$$

avec $2 \leqslant q_1 < \cdots < q_s$ premiers et $\beta_1, \ldots, \beta_s \geqslant 1$, alors en fait, tous ces citoyens entiers sont égaux :

$$s \;=\; r, \qquad q_1 = p_1, \;\ldots\; q_r = p_r, \qquad \beta_1 = \alpha_1, \;\ldots\; \beta_r = \alpha_r.$$

Ce théorème constitue le *fondement absolu* de toute l'arithmétique, mais il cache encore de très grands mystères mathématiques toujours non résolus actuellement.

Démonstration. Ainsi, supposons que :

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} \;=\; n \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

Pour tout indice $i = 1, \ldots, r$, si on écrit $p_i^{\alpha_i} = p_i \, p_i^{\alpha_i - 1}$, alors cette identité :

$$p_i \underbrace{p_1^{\alpha_1} \cdots p_i^{\alpha_i - 1} \cdots p_r^{\alpha_r}}_{=:\, u \text{ nombre entier}} \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s},$$

montre que p_i divise $q_1^{\beta_1} \cdots q_s^{\beta_s}$, qui est un produit de nombres premiers. Et grâce à la Proposition 24.5 — encore elle ! —, nous déduisons que p_i doit être égal à l'un des nombres premiers $q_1, \ldots, q_s$.

En raisonnant de manière symétrique, on déduit aussi que chaque q_j avec $1 \leqslant j \leqslant s$ doit être égal à l'un des p_i. Par conséquent, ces deux ensembles de nombres premiers doivent coïncider :

$$\big\{p_1, \ldots, p_r\big\} \;=\; \big\{q_1, \ldots, q_s\big\}.$$

Or comme ces deux collections de nombres premiers distincts $p_1 < \cdots < p_r$ et $q_1 < \cdots < q_s$ sont ordonnées de manière strictement croissante, cela force $r = s$ ainsi que $p_1 = q_1$, …, $p_r = q_r$.

Nous avons donc obtenu l'identité :

$$p_1^{\alpha_1} \cdots p_i^{\alpha_i} \cdots p_r^{\alpha_r} \;=\; n \;=\; p_1^{\beta_1} \cdots p_i^{\beta_i} \cdots p_r^{\beta_r},$$

et il nous reste encore à montrer l'égalité $\alpha_i \stackrel{?}{=} \beta_i$ des exposants, pour tout $i = 1, \ldots, r$.

Si on avait $\alpha_i > \beta_i$, en divisant cette identité par $p_i^{\beta_i}$, on obtiendrait une égalité :

$$\underbrace{p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_r^{\alpha_r}}_{= p_i \text{ fois un nombre entier}} \;=\; n \;=\; p_1^{\beta_1} \cdots p_{i-1}^{\beta_{i-1}} \cdot 1 \cdot p_{i+1}^{\beta_{i+1}} \cdots p_r^{\beta_r},$$

qui montrerait que p_i à gauche *divise* le nombre entier à droite, et alors la Proposition 24.5 — encore et toujours elle ! — forcerait p_i à être *égal* à l'un des nombres premiers :

$$p_1, \;\ldots,\; p_{i-1}, \;p_{i+1}, \;\ldots,\; p_r,$$

ce qui n'est pas.

En raisonnant de manière symétrique, on trouve aussi que $\alpha_i < \beta_i$ est absurde. En conclusion, $\alpha_i = \beta_i$, pour tout $i = 1, \ldots, r$. Cela achève la démonstration. □

Question 24.9. *Y a-t-il un nombre fini, ou un nombre infini, de nombres premiers ?*

En explorant les nombres premiers « à la main » — c'est-à-dire sur papier ou sur ordinateur —, on devine qu'il est toujours possible de trouver des nombres premiers de plus en plus grands, toujours nouveaux. Cependant de simples observations expérimentales ne constituent pas une véritable démonstration mathématique. Une argumentation rigoureuse très élégante du fait qu'il existe une infinité de nombres premiers est connue depuis Euclide — la voici.

Théorème 24.10. *Il existe une infinité de nombres premiers.*

Démonstration. Supposons par l'absurde qu'il n'y ait qu'un nombre *fini* $\mathrm{K} < \infty$ de nombres premiers, et notons-les alors :

$$q_1 < \cdots < q_k < \cdots < q_{\mathrm{K}},$$

avec évidemment $q_1 = 2$, $q_2 = 3$, $q_3 = 5$, *etc.*, puisque tout le monde connaît les tous *premiers* nombres premiers !

Par une immense astuce, introduisons alors l'entier :

$$\mathrm{N} := 1 + 2 \cdot 3 \cdot 5 \cdots q_k \cdots q_{\mathrm{K}},$$

qui a la propriété forte d'être congru à 1 modulo *tous* ces nombres premiers :

$$\mathrm{N} \equiv 1 \mod q_k, \qquad \forall\ 1 \leqslant k \leqslant \mathrm{K}. \tag{24.11}$$

Mais alors le Théorème 24.7 fondamental de l'arithmétique s'appliquerait à cet entier N pour le représenter comme un produit fini :

$$\mathrm{N} = q_{i_1}^{\alpha_1} \cdots q_{i_r}^{\alpha_r},$$

de certaines puissances $\alpha_1, \ldots, \alpha_r \geqslant 1$ de nombres premiers $q_{i_1} < \cdots < q_{i_r}$ qui *appartiendraient forcément tous* à cette liste finie $\{q_1, \ldots, q_{\mathrm{K}}\}$, ce qui impliquerait par exemple :

$$\mathrm{N} \equiv 0 \mod q_{i_1},$$

en contradiction manifeste avec (24.11) pour $k = i_1$.

Notre hypothèse était donc fausse, ce qui démontre bien qu'il existe une *infinité* de nombres premiers. □

Proposition 24.12. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tout exposant $\alpha \geqslant 1$, les seuls diviseurs de p^α sont :*

$$1,\ p,\ p^2,\ \ldots,\ p^{\alpha-1},\ p^\alpha.$$

Démonstration. Soit donc un diviseur $d \,|\, p^\alpha$. Grâce au Théorème 24.7, on sait maintenant que d est un produit de nombres premiers. Prenons alors un facteur premier quelconque q de d, d'où $q \,|\, d$. Par transitivité de la relation de divisibilité $q \,|\, d \,|\, p^\alpha$, il vient $q \,|\, p^\alpha$. Autrement dit, q divise $p \cdot p \cdots p$, avec α facteurs identiques.

Mais alors grâce à la Proposition 24.5, q doit être égal à l'un de ces facteurs premiers identiques, donc forcément $q = p$!

Ainsi, tous les diviseurs premiers q de p^α sont égaux à p, donc d est de la forme $d = p^\beta$, avec $\beta \leqslant \alpha$ puisque $d \,|\, p^\alpha$ — c'est-à-dire $d\,u = p^\alpha$ — implique $d \leqslant p^\alpha$ et $p^\beta \leqslant p^\alpha$ implique $\beta \leqslant \alpha$.

Enfin, comme chaque p^β avec $0 \leqslant \beta \leqslant \alpha$ divise manifestement $p^\alpha = p^\beta\, p^{\alpha-\beta}$, le travail est terminé. □

Revenons à la factorisation générale :

$$n \,=\, p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Dans cette factorisation, on peut en fait « faire apparaître » *tous* les nombres premiers $p \in \mathscr{P}$, *y compris* ceux qui sont distincts de $p_1, \ldots, p_r$, simplement en les mettant à la puissance 0, car $p^0 = 1$ — par exemple :

$$10 \,=\, 2 \cdot 5 \,=\, 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots .$$

Notation 24.13. On note la décomposition d'un entier $n \in \mathbb{Z}$ quelconque :

$$n \,=\, \varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)},$$

où :

☐ $\varepsilon = \pm 1$ est le *signe* de n ;

☐ $\mathsf{v}_p(n)$ est un exposant entier, appelé la *valuation p-adique* de n, et qui vaut presque toujours 0, sauf pour un nombre *fini* de nombres premiers $p \in \mathscr{P}$.

Par convention, on pose aussi $\mathsf{v}_p(0) := \infty$.

En effet, dans $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, il y a toujours un nombre *fini* de facteurs premiers. Tous les $p \neq p_1, \ldots, p_r$ sont mis à la puissance 0, ce qui donne la neutralité Suisse $1 = p^0$.

Proposition 24.14. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous entiers relatifs $m, n \in \mathbb{Z}$, les trois propriétés suivantes sont satisfaites.*

(1) *On a l'égalité :*

$$\mathsf{v}_p\big(m+n\big) \;\geqslant\; \mathsf{min}\,\big(\mathsf{v}_p(m),\, \mathsf{v}_p(n)\big).$$

(2) *On a :*

$$\mathsf{v}_p\big(m\,n\big) \,=\, \mathsf{v}_p(m)\,\mathsf{v}_p(n).$$

(3) *On a $m \,|\, n$ si et seulement si $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$ pour tout premier $p \in \mathscr{P}$.*

Démonstration. Expliquons seulement **(3)**, laissant **(1)** et **(2)** en exercice.

$\Longrightarrow$ Supposons donc $m \,|\, n$, c'est-à-dire $m\,u = n$, pour un entier $u \in \mathbb{Z}$. Décomposons chacun de ces trois entiers en facteurs premiers :

$$\begin{aligned}
m \,&=\, \varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(m)}, & \varepsilon \,&=\, \pm 1,\\
n \,&=\, \delta \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)}, & \delta \,&=\, \pm 1,\\
u \,&=\, \gamma \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(u)}, & \gamma \,&=\, \pm 1,
\end{aligned}$$

et écrivons vraiment l'égalité $m\,u = n$:

$$\varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(m)}\; \gamma \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(u)} \;=\; \delta \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)}.$$

Les signes doivent s'accorder (diplomatie oblige), c'est-à-dire $\varepsilon\,\gamma = \delta$. Ensuite, par la règle d'additivité des puissances, $p^\alpha \cdot p^{\alpha'} = p^{\alpha+\alpha'}$, il vient :

$$\mathsf{v}_p(m) + \mathsf{v}_p(u) \,=\, \mathsf{v}_p(n),$$

donc puisque $\mathsf{v}_p(u) \geqslant 0$ est toujours vrai car $\mathsf{v}_p(u) \in \mathbb{N}$ par définition, on a bien $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$, pour tout premier $p \in \mathscr{P}$.

$\Longleftarrow$ Réciproquement, en supposant que $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$ pour tout $p \in \mathscr{P}$, on trouve facilement le multiplicateur u satisfaisant $m\,u = n$:

$$u \;:=\; \tfrac{\varepsilon}{\delta} \prod_{p\in\mathscr{P}} p^{\mathsf{v}_p(n)-\mathsf{v}_p(m)},$$

avec $\frac{\varepsilon}{\delta} = \frac{\pm 1}{\pm 1} = \pm 1$ (of course !), et avec u entier, puisque tous les exposants sont *entiers*. □

Enfin, énonçons une représentation très naturelle et très intuitive du pgcd et du ppcm, dont la vérification formelle est laissée en exercice d'assimilation du cours.

Théorème 24.15. *Pour $a, b \in \mathbb{Z}$ quelconques non tous les deux nuls, on a :*

$$\mathsf{pgcd}\,(a,b) \;=\; \prod_{p\in\mathscr{P}} p^{\mathsf{min}\,(\mathsf{v}_p(a),\,\mathsf{v}_p(b))},$$

$$\mathsf{ppcm}\,(a,b) \;=\; \prod_{p\in\mathscr{P}} p^{\mathsf{max}\,(\mathsf{v}_p(a),\,\mathsf{v}_p(b))}. \qquad \square$$

Les notions de pgcd et de ppcm se généralisent à 3, 4, 5, *etc.* entiers, comme dans les Définitions 19.1 et 23.1.

Grâce à une application directe du Théorème 24.15 qui précède, on vérifie alors que :

$$\mathsf{pgcd}\,\big(a,b,c\big) \;=\; \mathsf{pgcd}\,\big(\mathsf{pgcd}\,(a,b),\,c\big),$$

$$\mathsf{ppcm}\,\big(a,b,c\big) \;=\; \mathsf{ppcm}\,\big(\mathsf{ppcm}\,(a,b),\,c\big),$$

ce qui signifie qu'on peut ramener le calcul du pgcd et/ou du ppcm de *plusieurs* entiers à des calculs successifs de pgcd et/ou de ppcm *classiques* entre *paires* d'entiers.

25. Théorème de Fermat

En mathématiques, le (petit) théorème de Fermat est un résultat de l'arithmétique modulaire, qui peut aussi se démontrer avec les outils de l'arithmétique élémentaire. Il doit son nom à Pierre de Fermat, qui l'énonce pour la première fois [19] en 1640.

19. La première apparition connue de l'énoncé de ce théorème provient d'une lettre de Fermat à Frénicle de Bessy datée de 1640. On peut y lire ceci :

> *Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.*

En termes modernes, Fermat exprime que pour tout nombre premier p et tout nombre a premier avec p, il existe un entier t tel que p divise $a^t - 1$, et, t étant le plus petit entier vérifiant ceci, t divise $p-1$, et tous les multiples n de t vérifient que p divise $a^n - 1$.

Comme habituellement dans sa correspondance Fermat ne donne aucune démonstration de ce résultat, ni même, comme il le fait parfois, d'indications à propos de celle-ci, mais il précise :

> *Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.*

À cette époque, il est d'usage de ne pas publier les preuves des théorèmes. Ainsi Leibniz rédige une démonstration vers 1683 mais ne la publie pas. En 1741, 1750 et 1761, Euler en publie deux qui procèdent par récurrence et utilisent le développement du binôme, et une qui étudie la répartition des restes modulo le nombre premier considéré. On trouve cette dernière en 1801 dans les *Disquisitiones arithmeticae* de Gauss.

Ce théorème dispose de nombreuses applications, à la fois en arithmétique modulaire et en cryptographie.

Théorème 25.1. [de Fermat] *Si p est un nombre premier, alors pour tout entier $a \in \mathbb{Z}$ qui est* non divisible par *p, l'entier a^{p-1} est congru à 1 modulo p :*

$$a \wedge p \,=\, 1 \qquad\qquad \Longrightarrow \qquad\qquad a^{p-1} \,\equiv\, 1 \mod p.$$

Évidemment, il faut exclure $a \equiv 0 \mod p$, car $0^{p-1} \equiv 0 \mod p$ n'est pas congru à 1 !

Mais si on multiplie par a, on obtient un énoncé essentiellement équivalent qui est est vrai sans exception.

Théorème 25.2. [de Fermat-bis] *Si p est un nombre premier, alors pour tout entier $a \in \mathbb{Z}$:*

$$a^p \,\equiv\, a \mod p.$$

Voici quelques exemples non triviaux de ce second énoncé.

- Pour $p = 2$, les entiers $a \in \mathbb{Z}$ sont congrus, ou bien à 0, ou bien à 1, modulo 2, et on a $0^2 \equiv 0$ ainsi que $1^2 \equiv 1$ modulo 2 — trivialement.
- $5^3 - 5 = 120$ est bien divisible par 3.
- $2^5 - 2 = 30$ est bien divisible par 5.
- $(-3)^7 + 3 = -2184 - 7 \cdot 312$ est bien divisible par 7.
- Avec le nombre premier $p = 97$ et avec $a = 2$:

$$\begin{aligned} 2^{97} - 2 \,&=\, 158\,456\,325\,028\,528\,675\,187\,087\,900\,670 \\ &=\, 97 \cdot 1\,633\,570\,361\,118\,852\,321\,516\,370\,110, \end{aligned}$$

est bien divisible par 97.

Autre illustration : *Que vaut le reste de la division de 5^{400} par le nombre premier 397 ?* Le Théorème 25.2 de Fermat-bis donne :

$$5^{\,397} \,\equiv\, 5 \mod 397,$$

d'où :

$$5^{\,400} \,\equiv\, 5^{397+3} \,\equiv\, 5^{3+1} \,\equiv\, 5^4 \,\equiv\, 625 \,\equiv\, 328 \mod 397.$$

Assertion 25.3. *Les Théorèmes 25.1 de Fermat et 25.2 de Fermat-bis sont équivalents.*

Preuve. Si le premier énoncé est vrai, alors le deuxième aussi, grâce à la factorisation :

$$a^p - a \,=\, a\left(a^{p-1} - 1\right) \overset{?}{\equiv} 0 \mod p,$$

car si $a \equiv 0 \mod p$, on a clairement $a^p - a \equiv 0 \mod p$, et si $a \not\equiv 0 \mod p$, c'est le deuxième facteur $a^{p-1} - 1 \equiv 0 \mod p$ qui fait le travail.

Inversement, si le deuxième énoncé est vrai, alors le premier aussi, car avec $a \not\equiv 0 \mod p$, donc avec $1 = p \wedge a$, en partant de la factorisation :

$$\mod p \;\; 0 \,\equiv\, a^p - a \,\equiv\, \underline{a}_{\circ}\left(a^{p-1} - 1\right) \text{ est divisible par } p,$$

le Théorème 24.4 d'Euclide force p à devoir diviser $a^{p-1} - 1$. Autrement dit, $a^{p-1} - 1 \equiv 0 \mod p$. □

Concentrons-nous donc sur le deuxième énoncé.

Démonstration du Théorème 25.1 de Fermat. Il s'agit d'arguments dus à Leibniz et à Euler, qui reposent sur une utilisation astucieuse de la formule du binôme de Newton (club des grands).

Tout d'abord, pour $a = 0$, on a bien $0^p \equiv 0 \mod p$. En partant de 0, et en ajoutant $+1$ pas à pas pour couvrir tous les éléments de $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\} \mod p$, nous allons raisonner par récurrence en appliquant le

Lemme 25.4. *Si $p \in \mathscr{P}$ est premier, alors tout entier $a \in \mathbb{Z}$ satisfait :*

$$\big(a+1\big)^p \equiv a^p + 1 \mod p.$$

Démonstration. Développons :

$$\big(a+1\big)^p = a^p + \tbinom{p}{1} a^{p-1}\, 1^1 + \tbinom{p}{2} a^{p-2}\, 1^2 + \cdots + \tbinom{p}{p-2} a^2\, 1^{p-2} + \tbinom{p}{p-1} a^1\, 1^{p-1} + 1^p,$$

avec, pour tout $1 \leqslant k \leqslant p-1$, les coefficients binomiaux :

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in \mathbb{N},$$

dont on sait qu'ils sont *entiers*. Extrayons p via $p! = p \cdot (p-1)!$:

$$\mathbb{N} \ni \frac{p\,(p-1)!}{k!\,(p-k)!} = p\, \underbrace{\frac{(p-1)!}{k!\,(p-k)!}}_{\text{doit être entier}},$$

et observons au dénominateur que :

- aucun facteur premier de $k! = 1 \cdot 2 \cdots k$ ne peut être égal à p, parce que $k \leqslant p-1$;
- aucun facteur premier de $(p-k)! = 1 \cdot 2 \cdots (p-k)$ ne peut être égal à p non plus, parce que $p - k \leqslant p - 1$, vu que $1 \leqslant k$.

Donc le p au numérateur ne peut se simplifier avec *aucun* nombre premier au dénominateur : il reste *intact*, et alors, les facteurs de $k!$ et de $(p-k)!$ ne peuvent se simplifier qu'avec $(p-1)!$. Nous avons en fait démontré le

Lemme 25.5. *Si $p \in \mathscr{P}$ est premier, alors pour tout $1 \leqslant k \leqslant p-1$:*

$$\binom{p}{k} = p\,\frac{(p-1)!}{k!\,(p-k)!} \equiv 0 \mod p.$$

En réduisant modulo p l'équation plus haut, nous obtenons bien :

$$\big(a+1\big)^p \equiv a^p + 0 + 0 + \cdots + 0 + 0 + 1^p \equiv a^p + 1 \mod p. \qquad \square$$

Par récurrence ascendante, en partant de $a = 0$, on peut appliquer ce lemme :

$$\begin{aligned} 1^p &\equiv \big(1+0\big)^p \equiv 1^p + 0^p \equiv 1 \mod p, \\ 2^p &\equiv \big(1+1\big)^p = 1^p + 1 \equiv 1 + 1 \equiv 2 \mod p, \\ 3^p &\equiv \big(2+1\big)^p = 2^p + 1 \equiv 2 + 1 \equiv 3 \mod p, \end{aligned}$$

et ainsi de suite pour obtenir $a^p \equiv a \mod p$, quel que soit l'entier $a \geqslant 0$.

Pour attraper tous les entiers $a \leqslant 0$ négatifs, on raisonne de manière similaire [20] avec :

$$\begin{aligned}(a-1)^p &= a^p + \tbinom{p}{1} a^{p-1}(-1)^1 + \cdots + \tbinom{p}{p-1} a^1 (-1)^{p-1} + (-1)^p \\ &\equiv a^p + (-1)^p \mod p.\end{aligned}$$

□

26. Théorème de Wilson

En arithmétique élémentaire, le théorème de Wilson énonce qu'un entier $n \geqslant 2$ est un nombre premier *si et seulement si* la factorielle de $n-1$ est congrue à -1 modulo n. Cette caractérisation des nombres premiers est assez anecdotique et ne constitue pas un test de primalité efficace. Son principal intérêt réside dans son histoire [21], et dans la relative simplicité de son énoncé et de ses preuves.

Rappelons que la *factorielle* d'un entier $m \geqslant 1$ est :

$$m! = 1 \cdot 2 \cdot 3 \cdots (m-1) \cdot m.$$

Théorème 26.1. [de Wilson] *Pour tout entier $n \geqslant 2$, on a équivalence entre :*

(i) $n = p \in \mathscr{P}$ *est premier ;*

(ii) $(n-1)! \equiv -1 \mod n$.

Voici quelques exemples illustrant cet énoncé.

- Si p est égal à 2, alors $(p-1)!+1$ est égal à 2, un multiple de 2.
- Si p est égal à 3, alors $(p-1)!+1$ est égal à 3, un multiple de 3.
- Si p est égal à 4, alors $(p-1)!+1$ est égal à 7, qui n'est *pas* un multiple de 4.
- Si p est égal à 5, alors $(p-1)!+1$ est égal à 25, qui *est* un multiple de 5.
- Si p est égal à 6, alors $(p-1)!+1$ est égal à 121, qui n'est *pas* un multiple de 6.
- Si p est égal à 17, alors $(p-1)!+1$ est égal à $20\,922\,789\,888\,001$, qui *est* un multiple de 17, car :

$$17 \cdot 1\,230\,752\,346\,353 = 20\,922\,789\,888\,001.$$

Démonstration. Le cas $n = 2$, qui est premier, est clair, car $(2-1)! \equiv -1 \mod 2$. On peut donc supposer que $n \geqslant 3$.

Montrons **(i)** $\Longrightarrow$ **(ii)**. D'après le Théorème 27.5, on sait que $\mathbb{Z}/p\,\mathbb{Z}$ est un corps. Ainsi, tout élément non nul a dans l'ensemble :

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^\times = \big\{1,\, 2,\, \ldots,\, p-2,\, p-1\big\} \mod p,$$

20. Il y a néanmoins une petite subtilité technique : il faut s'arranger à l'avance que $p \geqslant 3$ afin d'avoir $(-1)^p = -1$, donc il faut avoir traité le cas $p = 2$ à part, auparavant, ce que nous avons en fait déjà fait !

Autre moyen de raisonner : comme l'application $a \longmapsto a \mod p$ de $\mathbb{N}$ dans $\mathbb{Z}/p\mathbb{Z}$ est surjective, et comme l'équation de Fermat $a^p \equiv a \mod p$ s'exprime véritablement non pas dans $\mathbb{Z}$, mais dans $\mathbb{Z}/p\mathbb{Z}$, le fait d'avoir traité tous les $a \geqslant 0$ suffit largement.

21. Le premier texte actuellement connu qui fait référence à ce résultat est dû au mathématicien arabe Alhazen (965–1039). Ce théorème est connu à partir du XVII$^{\text{ième}}$ siècle en Europe. Leibniz (1646–1716) fait référence à ce résultat sans le démontrer. John Wilson (1741–1793) redécouvre ce qu'il croit être une conjecture, et en partage la découverte avec son professeur Edward Waring, qui publie cette conjecture en 1770.

En définitive, John Wilson est connu pour avoir énoncé (ou conjecturé) un théorème sur les nombres premiers qui porte son nom, alors qu'il ne l'a pas *du tout* démontré …

Lagrange en présente deux premières démonstrations en 1771, puis Euler une troisième en 1773. Utilisant les notations de l'arithmétique modulaire, Gauss reformule la démonstration d'Euler et donne une quatrième preuve, la plus élégante, celle que nous détaillons.

possède un inverse multiplicatif a', *qui appartient nécessairement au même ensemble*.

Or le cardinal de cet ensemble est égal à $p-1$, car tout nombre premier $p \geqslant 3$ est *impair*. Mais $1 = 1^{-1}$ est son propre inverse, et $(p-1) = (p-1)^{-1}$ aussi, car :

$$1 \cdot 1 \;=\; 1 \mod p, \qquad \text{et} \qquad (p-1)\cdot(p-1) \;=\; p^2 - 2\,p + 1 \;\equiv\; 1 \mod p.$$

Assertion 26.2. *Les éléments* 1 *et* $p-1$ *de* $\mathbb{Z}/p\mathbb{Z}$ *sont les seuls* x *satisfaisant :*

$$x^2 \;\equiv\; 1 \mod p.$$

Preuve. Soit un tel x. Certainement, $x \not\equiv 0 \mod p$, car $0^2 \equiv 1 \mod p$ est faux. On factorise :

$$(x-1)\,(x+1) \;\equiv\; 0 \mod p,$$

c'est-à-dire :

$$(x-1)\,\big(x-(p-1)\big) \;\equiv\; 0 \mod p.$$

Alors oui, $x = 1$ et $x = p-1$ satisfont bien cette congruence.

Mais alors, *aucun* $x = a$ parmi les éléments restants $a \in \{2, \ldots, p-2\}$ ne peut satisfaire cette congruence, car les inégalités :

$$\begin{aligned} 2 \;\leqslant\; a \;\leqslant\; p-2 \qquad &\Longrightarrow \qquad 1 \;\leqslant\; a-1 \;\leqslant\; p-3 \\ \text{et} \qquad &-(p-3) \;\leqslant\; a-(p-1) \;\leqslant\; -1, \end{aligned}$$

montrent que les deux entiers $a - 1 \;\not\equiv\; 0 \mod p$, ainsi que $a - (p-1) \;\not\equiv\; 0 \mod p$ ne peuvent *pas* être congrus à 0 modulo p.

Assertion 26.3. [Intégrité de $\mathbb{Z}/p\mathbb{Z}$] *Avec* $p \in \mathscr{P}$ *premier, on a toujours, pour* $a, b \in \mathbb{Z}$ *:*

$$\Big(\; a \;\not\equiv\; 0 \mod p \quad \textit{et} \quad b \;\not\equiv\; 0 \mod p \;\Big) \qquad \Longrightarrow \qquad a\,b \;\not\equiv\; 0 \mod p.$$

Preuve. Traitons plutôt l'implication contraposée, qui lui est équivalente :

$$\Big(\; a \;\equiv\; 0 \mod p \quad \text{ou} \quad b \;\equiv\; 0 \mod p \;\Big) \qquad \Longleftarrow \qquad a\,b \;\equiv\; 0 \mod p.$$

Supposons donc qu'il existe $k \in \mathbb{Z}$ tel que :

$$a\,b \;=\; k\,p,$$

de telle sorte que $a\,b$ soit divisible par p. Mais le Théorème 24.4 d'Euclide garantit alors que :

$$\big(\,p \,|\, a \quad \text{ou} \quad p \,|\, b\,\big) \qquad \text{c'est-à-dire} \qquad \big(\; a \;\equiv\; 0 \mod p \quad \text{ou} \quad b \;\equiv\; 0 \mod p\,\big).$$ □

Enfin, grâce à l'*intégrité* de $\mathbb{Z}/p\mathbb{Z}$, nous concluons que le produit de nos deux entiers est *aussi* non congru à zéro modulo p :

$$a^2 - 1 \;\equiv\; (a-1)\,\big(a-(p-1)\big) \;\not\equiv\; 0 \mod p.$$

En conclusion, pour tout $a \;\neq\; 1$ et $\neq\; p-1$, on a bien vérifié que $a^2 \;\not\equiv\; 1 \mod p$. En particulier, a ne peut *pas* être son propre inverse modulo p. □

Par conséquent, dans l'ensemble restant $\big\{2, \ldots, p-2\big\}$ de cardinal égal à $p-3$ *pair*, chaque élément $a \in \big\{2, \ldots, p-2\big\}$ trouve son inverse $a^{-1} \in \big\{2, \ldots, p-2\big\}$ *qui est différent de* a. Autrement dit, les éléments de $\big\{2, \ldots, p-2\big\}$ s'accouplent par paires annihilatrices — pour la multiplication …

Par exemple, modulo 7 et modulo 11, relions en rouge les paires d'inverses multiplicatifs :

et constatons que la combinatoire semble moins simple que pour les paires d'inverses additifs, qui exhibaient une symétrie très agréable dans la Section **10**. Dans ces deux exemples, les produits complets :

$$\begin{aligned} 2\cdot 3\cdot 4\cdot 5 &\equiv 2\cdot 3\cdot 2^{-1}\cdot 3^{-1} \\ &\equiv 1 \mod 7, \\ 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9 &\equiv 2\cdot 3\cdot 3^{-1}\cdot 5\cdot 2^{-1}\cdot 7\cdot 7^{-1}\cdot 5^{-1} \\ &\equiv 1 \mod 11, \end{aligned}$$

sont congrus à 1, c'est-à-dire généralement :

$$2\cdot 3\cdots(p-3)\cdot(p-2) \equiv 1 \mod p.$$

Enfin, on atteint la propriété **(ii)** :

$$\begin{aligned} (p-1)\,! &= 1\cdot\big[2\cdot 3\cdots(p-3)\cdot(p-2)\big]\cdot(p-1) \\ &\equiv 1\cdot\big[1\big]\cdot(p-1) \mod p \\ &\equiv p-1 \mod p \\ &\equiv -1 \mod p. \end{aligned}$$

Ensuite, montrons la réciproque **(ii)** $\Longrightarrow$ **(i)**. Par contraposition, cela revient à montrer :

$$\text{non } \textbf{(i)} \quad\Longrightarrow\quad \text{non } \textbf{(ii)}.$$

Supposons donc non **(i)**. Soit donc un entier $n \geqslant 4$ *non premier*, c'est-à-dire décomposé comme produit $n = d\,m$, avec $1 < d < n$ et $1 < m < n$. Clairement [22], l'écriture :

$$(n-1) = 1\cdot 2\cdots d\cdots(n-1),$$

fait voir que $(n-1)!$ est congru à 0 modulo d, donc *pas* congru à -1 :

$$(n-1)! \not\equiv -1 \mod d.$$

Enfin, grâce à la contraposée de la Proposition 33.2, qui a été énoncée comme le Corollaire 33.3, nous attteignons aussitôt non **(ii)** :

$$(n-1)\,! \not\equiv -1 \mod \underbrace{d m}_{=n}. \qquad \square$$

27. Intégrité et non-intégrité de $\mathbb{Z}/n\mathbb{Z}$

Dans $\mathbb{Z}/4\mathbb{Z} = \big\{0,1,2,3\big\} \mod 4$, les éléments inversibles sont :

$$\begin{aligned} 1 \text{ d'inverse } 1, &\quad \text{car } 1\cdot 1 \equiv 1 \mod 4, \\ 3 \text{ d'inverse } 3, &\quad \text{car } 3\cdot 3 \equiv 1 \mod 4, \end{aligned}$$

tandis que 2 n'a *pas* d'inverse, puisque modulo 4 :

$$0\cdot 2 \equiv 0, \qquad 1\cdot 2 \equiv 2, \qquad 2\cdot 2 \equiv 0, \qquad 3\cdot 2 \equiv 2.$$

Dans $\mathbb{Z}/8\mathbb{Z} = \big\{0,1,2,3,4,5,6,7\big\} \mod 8$, les éléments inversibles sont :

22. L'écriture symétrique $(n-1)! = 1\cdot 2\cdots m\cdots(n-1)$, qui montre que $(n-1)!$ est aussi divisible par m, n'est pas utilisée dans l'argumentation.

$$1 \text{ d'inverse } 1, \quad \text{car} \quad 1 \cdot 1 \equiv 1 \mod 8,$$
$$3 \text{ d'inverse } 3, \quad \text{car} \quad 3 \cdot 3 \equiv 1 \mod 8,$$
$$5 \text{ d'inverse } 5, \quad \text{car} \quad 5 \cdot 5 \equiv 1 \mod 8,$$
$$7 \text{ d'inverse } 7, \quad \text{car} \quad 7 \cdot 7 \equiv 1 \mod 8,$$

tandis que 2, 4, 6 n'ont *pas* d'inverse modulo 8, comme le montre la table de multiplication complète.

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Dans $\mathbb{Z}/11\mathbb{Z}$, *tous* les éléments non nuls 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 sont inversibles, comme on peut le voir en constatant dans la table de multiplication que chaque ligne (ou chaque colonne) concernée contient le nombre 1.

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**	**[10]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]	[0]	[4]	[8]	[1]	[5]	[9]	[2]	[6]	[10]	[3]	[7]
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]
[6]	[0]	[6]	[1]	[7]	[2]	[8]	[3]	[9]	[4]	[10]	[5]
[7]	[0]	[7]	[3]	[10]	[6]	[2]	[9]	[5]	[1]	[8]	[4]
[8]	[0]	[8]	[5]	[2]	[10]	[7]	[4]	[1]	[9]	[6]	[3]
[9]	[0]	[9]	[7]	[5]	[3]	[1]	[10]	[8]	[6]	[4]	[2]
[10]	[0]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Il y a quelques secondes, nous avons « laissé passer[23] » le fait — absolument non-anodin ! — que dans $\mathbb{Z}/4\mathbb{Z}$:

$$2 \cdot 2 \equiv 0 \mod 4.$$

Autrement dit, dans un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ au sens de la Définition 5.9, il peut exister des $a \neq 0$ et des $b \neq 0$ dont le *produit* $a \times b = 0_A$ est *nul ! Aïe !*

Définition 27.1. Un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ est dit *intègre* si, pour tous a et b dans $\mathbb{A}$:

$$a\,b = 0 \qquad \Longrightarrow \qquad \Big(a = 0 \quad \text{ou} \quad b = 0 \Big).$$

De manière équivalente :

$$\Big(a\,b = 0 \quad \text{avec} \quad a \neq 0 \Big) \qquad \Longrightarrow \qquad b = 0.$$

De manière encore équivalente, la contraposée de la première implication est :

$$a\,b \neq 0 \qquad \Longleftarrow \qquad \Big(a \neq 0 \quad \text{et} \quad b \neq 0 \Big).$$

Certainement, les anneaux $\mathbb{A} = \mathbb{Z}/n\mathbb{Z}$ sont commutatifs, *mais pas forcément intègres*.

23. Attention ! À l'aéorort de Sidney en Australie,

Proposition 27.2. [Règle de simplification] *Si $a \neq 0$, alors $a\,b = a\,c$ implique $b = c$.*

Démonstration. Ceci équivaut à $a\big(b-c\big) = 0$, et par intégrité, comme $a \neq 0$, il vient $b - c = 0$, c'est-à-dire $b = c$. □

Pire ! Dans $\mathbb{Z}/4\mathbb{Z}$, on a même un élément a, le nombre 2, qui satisfait $a^2 \equiv 0 \bmod 4$.

En tout cas, l'anneau classique $\big(\mathbb{Z}, +, \times\big)$ est intègre (et honnête !), c'est bien connu, tandis que l'anneau $\mathscr{M}_{2\times 2}(\mathbb{R})$, tout comme $\mathbb{Z}/4\mathbb{Z}$, n'est *pas* intègre, ce que montre la matrice :

$$M := \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right),$$

qui satisfait :

$$M^2 = M \cdot M = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right).$$

Maintenant, souvenons-nous de la Définition 5.10 de *corps commutatif* $\mathbb{K}$, qui demandait que tout élément non nul $x \in \mathbb{K}\backslash\{0\}$ ait un inverse x' pour la multiplication, c'est-à-dire satisfaisant $x'x = 1$. Nous avions dit que $\mathbb{Z}$ n'est *pas* un corps, car aucun élément $a \in \mathbb{Z}$, excepté $a = \pm 1$, n'a d'inverse pour la multiplication, *e.g.* $\frac{1}{137} \notin \mathbb{Z}$.

Question 27.3. *Un anneau $\mathbb{Z}/n\mathbb{Z}$ d'entiers modulo n peut-il être un corps ?*

Avec tous ces $\mathbb{Z}/4\mathbb{Z}$ et autres $\mathbb{Z}/8\mathbb{Z}$ trublionnaires, il semblerait que non. En tout cas, rappelons-nous qu'un corps est toujours un anneau commutatif, et qu'il a de meilleures propriétés. Par exemple, $\mathbb{Q} = \big\{\frac{p}{q} :\ p \in \mathbb{Z},\ q \in \mathbb{N}^*\big\}$, qui est un corps, est aussi un anneau, comme $\mathbb{Z}$, mais il est « mieux » que $\mathbb{Z}$, car l'inverse de $\frac{p}{q}$ est $\frac{q}{p}$, lorsque $p \neq 0$. Or, tous les corps sont intègres !

Proposition 27.4. *Tout corps commutatif $\big(\mathbb{K}, +, \times\big)$ est un anneau* intègre.

Démonstration. Étant donné $a, b \in \mathbb{K}$ quelconques avec $a \neq 0$, satisfaisant $a\,b = 0$, il s'agit de montrer que $b = 0$.

Comme $\mathbb{K}$ est un corps, un inverse multiplicatif (unique) a^{-1} de a existe, avec $a^{-1}\,a = 1$, et donc, il suffit de l'utiliser :

$$a^{-1}\,\big(\ a\,b = 0\ \big) \qquad \text{donne} \qquad a^{-1}\,a\,b = 1 \cdot b = b = 0. \qquad \square$$

Théorème 27.5. *Pour $n \geqslant 2$ entier, les assertions suivantes sont équivalentes.*

(i) *$n = p \in \mathscr{P}$ est un nombre premier.*

(ii) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.*

(iii) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Observons que $\mathbb{Z}/n\mathbb{Z} = \big\{0, 1, \ldots, n-1\big\} \bmod n$ possède au moins les deux éléments $0 \neq 1$, puisque $n \geqslant 2$.

Démonstration. Nous allons démontrer ces équivalences « en yo-yo » :

$$\begin{array}{cc} \textbf{(i)} & \textbf{(i)} \\ \Downarrow & \Uparrow \\ \textbf{(ii)} & \textbf{(ii)} \\ \Downarrow & \Uparrow \\ \textbf{(iii)} & \textbf{(iii)} \end{array}$$

Montrons **(i)** $\Longrightarrow$ **(ii)**. Supposons donc que $n = p$ est premier. Soient deux éléments $x, y \in \mathbb{Z}/p\mathbb{Z}$ satisfaisant $x \cdot y = 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Pour avoir l'*intégrité* de $\mathbb{Z}/p\mathbb{Z}$, il s'agit de faire voir que $x = 0$ ou $y = 0$, dans $\mathbb{Z}/p\mathbb{Z}$.

Autrement dit, x et y appartiennent à $\{0, 1, 2, \ldots, p-1\} \bmod p$ et satisfont :

$$x \cdot y \equiv 0 \bmod p \qquad \Longleftrightarrow \qquad x\,y = k\,p \qquad (k \in \mathbb{Z}).$$

Mais alors, ceci montre que p *divise* le produit $x\,y$, et par conséquent, le Théorème 24.4 d'Euclide force p à diviser x ou à diviser y.

Enfin, comme p ne peut aucunement diviser les nombres $1, 2, \ldots, p-1$ qui lui sont inférieurs [24], et qu'il ne peut donc diviser que 0, on conclut bien que $x = 0$ ou $y = 0$.

Montrons **(ii)** $\Longrightarrow$ **(iii)**. Supposons donc $\mathbb{Z}/n\mathbb{Z}$ intègre. Prenons $x \in \{1, 2, \ldots, n-1\}$ quelconque, différent de 0. Pour avoir que $\mathbb{Z}/n\mathbb{Z}$ est un corps, il s'agit de trouver un *inverse multiplicatif* $x' \in \mathbb{Z}/n\mathbb{Z}$ satisfaisant :

$$x\,x' \equiv 1 \bmod n.$$

Certainement, x' doit se trouver parmi $\{1, 2, \ldots, n-1\}$, car $x' = 0$ est exclu. Regardons alors *tous* les produits $x\,k$ modulo n, pour $k = 0, 1, 2, \ldots, n-1$, en espérant y trouver x', y compris pour $k = 0$.

Assertion 27.6. *Modulo n, les n produits $x\,0$, $x\,1$, $x\,2$, …, $x\,(n-1)$ prennent des valeurs deux à deux distinctes :*

$$x\,k_1 \not\equiv x\,k_2 \qquad (\forall\, 0 \leqslant k_1 \neq k_2 \leqslant n-1).$$

Preuve. Supposons qu'il existe k_1 et k_2 avec $x\,k_1 \equiv x\,k_2 \bmod n$, c'est-à-dire :

$$x\,(k_1 - k_2) \equiv 0 \bmod n. \tag{27.7}$$

On peut supposer $k_2 \leqslant k_1$. Puisqu'on a déjà vu que :

$$0 \leqslant k_2 \leqslant k_1 \leqslant n-1 \qquad \Longrightarrow \qquad 0 \leqslant k_1 - k_2 \leqslant n-1,$$

il est clair que $k_1 - k_2$ est un élément de $\{0, 1, \ldots, n-1\}$. Mais comme $\mathbb{Z}/n\mathbb{Z}$ est supposé *intègre*, et comme on a pris $x \not\equiv 0$, l'équation (27.7) force $k_1 - k_2 = 0$, c'est-à-dire $k_1 = k_2$.

Ainsi, $x\,k_1 \equiv x\,k_2 \bmod n$ implique $k_1 = k_2$. Par contraposition [25], $k_1 \neq k_2$ implique $x\,k_1 \not\equiv x\,k_2 \bmod n$. □

Comme les n éléments $x\,0$, $x\,1$, $x\,2$, …, $x\,(n-1)$ sont donc deux à deux distincts, on a égalité entre les deux ensembles :

$$\{x\,0,\ x\,1,\ x\,2,\ \ldots,\ x\,(n-1)\} \bmod n \ = \ \{0,\ 1,\ 2,\ \ldots,\ n-1\} \bmod n,$$

et par conséquent, parmi tous ces $x\,k$ à gauche, il doit forcément y en avoir un qui est égal au 1 à droite modulo n, et ce k-là, c'est l'inverse x' de x que nous recherchions — nous l'avons trouvé !

La première implication **(iii)** $\Longrightarrow$ **(ii)** du yo-yo qui remonte est évidente, car tout corps est un anneau intègre, comme nous la Proposition 27.4 nous l'a déjà fait voir.

24. Rappelons en effet qu'avec deux entiers $a \geqslant 1$ et $b \geqslant 1$, la définition de $a \,|\, b$ s'exprime par $a\,u = b$ avec $u \geqslant 1$ entier, ce qui implique aussitôt $a \leqslant b$.

25. Rappelons l'équivalence logique générale valable pour deux propositions P et Q, appelée *contraposition :*

$$\big(\,\mathsf{P} \implies \mathsf{Q}\,\big) \qquad \Longleftrightarrow \qquad \big(\,\text{non } \mathsf{P} \impliedby \text{non } \mathsf{Q}\,\big)$$

Terminons en établissant **(ii)** $\Longrightarrow$ **(i)**. Par contraposition (notion qui vient d'être rappelée en note de bas de page), cela revient à établir non **(ii)** $\Longleftarrow$ non **(i)**.

Autrement dit, en partant d'un entier n non premier, c'est-à-dire décomposable en produit $n = d\,m$ avec $1 < d < n$ et $1 < m < n$, il s'agit d'établir que $\mathbb{Z}/n\mathbb{Z}$ n'est *pas* intègre. Et comme nous l'avons déjà vu, cela est clair !

En effet, $d \mod n$ et $m \mod n$ sont alors tous deux différents de 0 dans $\mathbb{Z}/n\mathbb{Z}$, puisqu'ils appartiennent d'emblée à l'ensemble $\{2, \ldots, n-1\}$, tandis que leur produit $d\,m = n \equiv 0 \mod n$ est stupidement nul dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, d et m détruisent l'intégrité éventuelle de $\mathbb{Z}/n\mathbb{Z}$.

Cela achève complètement la démonstration du Théorème 27.5. □

Quand le module n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est donc *pas* un corps. Toutefois, certains éléments spéciaux peuvent quand même avoir un inverse multiplicatif. Voici une caractérisation générale très claire de ces éléments sympathiques.

Théorème 27.8. *Soit $n \geqslant 2$. Pour tout $a \in \mathbb{Z}$, on a équivalence entre :*

(i) *$a \wedge n = 1$ est premier avec n ;*

(ii) *$a \mod n$ possède un inverse $a' \mod n$, avec $a\,a' \equiv 1 \mod n$.*

Ce théorème est en fait essentiellement équivalent au Grand Théorème 20.2 de Bézout.

Démonstration. En effet :

$$\begin{aligned} a \wedge n \,=\, 1 \qquad &\overset{\text{Bézout}}{\Longleftrightarrow} \qquad u\,a + v\,n \,=\, 1 \qquad && (\exists\, u \in \mathbb{Z},\, \exists\, v \in \mathbb{Z}) \\ &\Longleftrightarrow \qquad u\,a \,\equiv\, 1 \mod n, \end{aligned}$$

ce qui montre que le « u » de Bézout n'est autre que l'inverse a^{-1} de a. □

En principe, donc, c'est l'algorithme d'Euclide [26] qui permet de trouver l'inverse d'un élément a de $\mathbb{Z}/n\mathbb{Z}$, lorsqu'il existe.

Définition 27.9. Pour un entier $n \geqslant 2$, on appelle *groupe multiplicatif* de $\mathbb{Z}/n\mathbb{Z}$ l'ensemble noté :

$$\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times} := \Big\{ a \in \mathbb{Z}/n\mathbb{Z} \colon \text{ il existe } a' \in \mathbb{Z}/n\mathbb{Z} \text{ satisfaisant } a\,a' \equiv 1 \mod n \Big\}.$$

Autrement dit :

$$\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times} \,=\, \big\{ a \in \{0, 1, \ldots, n-1\} \colon \; a \wedge n = 1 \big\}.$$

Définition 27.10. On appelle *fonction indicatrice d'Euler* la fonction notée :

$$\varphi \colon \quad \mathbb{N}^* \longrightarrow \mathbb{N}^*,$$

qui est définie pour tout entier $n \geqslant 2$ par :

$$\begin{aligned} \varphi(n) \,&:=\, \mathsf{Card}\,\big\{ 1 \leqslant a \leqslant n \colon \; a \wedge n = 1 \big\} \\ &=\, \mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times}, \end{aligned}$$

en posant $\varphi(1) := 1$ par convention.

26. — débouchant sur une relation de Bézout $u\,a + v\,b = \mathsf{pgcd}\,(a, b)$, d'après le Théorème 19.7 —

On voit que $\varphi(2) = 1$. Lorsque $n = p \in \mathscr{P}$ est premier, *tous* les entiers $1 \leqslant a \leqslant p-1$ sont premiers avec p, et donc :

$$\varphi(p) \,=\, p-1 \qquad (p \text{ premier}).$$

Ensuite, voici les valeurs de $\varphi(n)$ pour n *non* premier jusqu'à 10 (doigts ?) :

$$\begin{aligned}
\varphi(4) \,&=\, 2, && \text{car } 1,\, 3 \text{ premiers avec } 4,\\
\varphi(6) \,&=\, 2, && \text{car } 1,\, 5 \text{ premiers avec } 6,\\
\varphi(8) \,&=\, 4, && \text{car } 1,\, 3,\, 5,\, 7 \text{ premiers avec } 8,\\
\varphi(9) \,&=\, 6, && \text{car } 1,\, 2,\, 4,\, 5,\, 7,\, 8 \text{ premiers avec } 9,\\
\varphi(10) \,&=\, 4, && \text{car } 1,\, 3,\, 7,\, 9 \text{ premiers avec } 10.
\end{aligned}$$

Plus tard, dans la Section **33**, nous établirons une propriété fondamentale de *multiplicativité* de cette indicatrice pour des entiers premiers entre eux :

$$\varphi\big(m\,n\big) \,=\, \varphi(m)\,\varphi(n) \qquad (\forall\, m \wedge n = 1).$$

28. Théorème des restes chinois

Sur un exemple très simple, commençons par rappeler l'intérêt du *calcul modulaire*, *i.e.* du calcul modulo un entier $n \geqslant 2$. Imaginons-nous que nous sommes un jeudi, jour du cours en amphithéâtre. *Quel jour serons-nous dans 2 583 jours ?*

Un moyen de répondre joliment à cette question est de numéroter les jours : jeudi $= 1$; vendredi $= 2$, et ainsi de suite. Maintenant, on additionne 2583 jours à 1, puisque jeudi $= 1$, ce qui donne $2\,584$ jours. Comme il n'y a que 7 jours dans la semaine, on peut retrancher autant de fois des multiples de 7 que l'on veut ; autrement dit, on peut retrancher autant de semaines que l'on veut. Par une division, on a donc que $2\,584 = 369 \times 7 + 1$, d'où nous concluons que dans $2\,584$ jours, nous serons encore un jeudi !

Comme le calcul modulo 7 nous semble dorénavant réservé aux « bébés » du Lycée qui n'ont pas encore commencé à apprendre les vraies mathématiques universitaires, voici un autre problème, plus complexe, d'origine chinoise et datant de l'Antiquité.

Problème 28.1. *Mon panier peut contenir au plus cent œufs.*

- *Si je le vide par trois œufs à la fois, il en reste un.*
- *Si je le vide par huit œufs à la fois, il en reste deux.*
- *Si je le vide par sept œufs à la fois, il en reste cinq.*

Combien ai-je d'œufs ?

Grâce aux entiers modulaires, et aux théorèmes arithmétiques que nous avons démontrés, nous pouvons résoudre ce problème. En effet, les informations se traduisent en 3 équations modulaires, avec 3 modules distincts (et premiers entre eux), d'inconnue le nombre x d'œufs :

$$x \,\leqslant\, 100 \qquad \text{et} \qquad x \,\equiv\, \begin{cases} 1 \mod 3,\\ 2 \mod 8,\\ 5 \mod 7. \end{cases}$$

Par la première congruence, on a $x = 1 + 3\,k$, avec $k \in \mathbb{N}$. Pour tenir compte de la deuxième contrainte, $x = 2 + 8\,k'$ avec $k' \in \mathbb{N}$, partons de $x = 1 + 3\,k$ avec l'astuce de

multiplier cette équation par 3, car $3 \cdot 3 = 9 \equiv 1 \mod 8$:

$$\begin{aligned} \big(\, 1+3k \;=\; 2+8k' \,\big) \cdot 3 \mod 8 \quad \text{donne} \quad 3+9k &\equiv 6 \mod 8 \\ k &\equiv 3 \mod 8 \\ k &\equiv 3+8\ell \quad (\text{avec } \ell \in \mathbb{N}), \end{aligned}$$

valeur de k que nous pouvons remplacer dans :

$$\begin{aligned} x &= 1+3\big(3+8\ell\big) \\ &= 10+24\ell. \end{aligned}$$

Ensuite, pour tenir compte de la troisième contrainte $x \equiv 5 \mod 7$:

$$10+24\ell \;=\; 5+7k'' \qquad (\text{avec } k'' \in \mathbb{N}),$$

si on veut raisonner de manière analogue, on doit raisonner modulo 7. Comme $24 \equiv 3 \mod 7$, et comme 5 est l'inverse de 3 dans $\mathbb{Z}/7\mathbb{Z}$, car $5 \cdot 3 = 15 \equiv 1 \mod 7$, on doit multiplier cette équation par 5, puis réduire modulo 7, en utilisant $7 \cdot 19 = 119$:

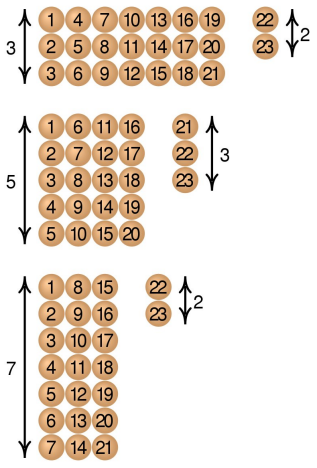
$$\begin{aligned} \big(\, 10+24\ell \;=\; 5+7k'' \,\big) \cdot 5 \mod 7 \quad \text{donne} \quad 50+120\ell &\equiv 25 \mod 7 \\ 1+\ell &\equiv 4 \mod 7 \\ \ell &\equiv 3 \mod 7 \\ \ell &= 3+7m \quad (\text{avec } m \in \mathbb{N}). \end{aligned}$$

Enfin, on remplace cette valeur de ℓ dans :

$$\begin{aligned} x &= 10+24\big(3+7m\big) \qquad 28.2 \\ &= 82+168m \qquad (m \in \mathbb{Z} \text{ quelconque.}) \end{aligned}$$

En conclusion, puisque l'on cherche $x \leqslant 100$, il faut choisir $m = 0$, et il y avait exactement 82 œufs dans le panier de la belle maraîchère.

Voici un autre exemple, dû à Sun Zi. La forme originale du théorème des restes chinois apparaît sous forme de problème dans le livre de Sun Zi, le Sunzi suanjing, datant du III$^{\text{ième}}$ siècle après Jésus-Chirst. Il est repris par le mathématicien chinois Qin Jiushao dans son ouvrage le Shushu Jiuzhang, *Traité mathématique en neuf chapitres*, publié en 1247. Le résultat concerne les systèmes de congruences.



Problème 28.3. *Soient des chevaux ailés en nombre inconnu.*

- *Si on les aligne par* 3 *au-dessus des nuages, il en reste* 2.
- *Si on les aligne par* 5, *il en reste* 3.
- *Si on les range par* 7, *il en reste 2.*

Combien y a-t-il de chevaux dans cet attelage céleste ?.

Cette énigme est parfois associée au général Han Xin comptant son armée (moins poétique). La résolution proposée par Sun Zi est la suivante.

> Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.

Cette solution, difficile à comprendre, n'explique qu'imparfaitement la méthode utilisée. Après un moment de concentration, on constate bien que le nombre indiqué par Sun Zi :

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15$$

a effectivement pour restes respectifs 2, 3, 2, dans les divisions par 3, 5, 7. Et comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors 23.

Question 28.4. *Mais pourquoi ces trois nombres* 70, 21, 15 *?*

On peut observer, et nous y reviendrons, que :

$$\begin{array}{lll} 70 \equiv 1 \mod 3, & 70 \equiv 0 \mod 5, & 70 \equiv 0 \mod 7, \\ 21 \equiv 0 \mod 3, & 21 \equiv 1 \mod 5, & 21 \equiv 0 \mod 7, \\ 15 \equiv 0 \mod 3, & 15 \equiv 0 \mod 5, & 15 \equiv 1 \mod 7. \end{array}$$

On retrouve ce problème presque à l'identique en 1202 dans le Liber Abbaci de Fibonacci, au sein du chapitre XII qui concerne les problèmes et énigmes où l'on trouve également le problème des lapins de la suite de Fibonacci. Le problème avait aussi été étudié par Ibn al-Haytham (Alhazen), dont Fibonacci a pu lire les œuvres. Euler s'est également intéressé à cette question, ainsi que Gauss.

Enfin, nous ne pouvons pas résister au fait de présenter un problème attrayant concernant des pirates et un trésor.

> Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

La réponse est 785. Les nombres 17, 11 et 6 étant premiers entre eux deux à deux, les solutions sont distantes d'un multiple de $1\,122 = 17 \cdot 11 \cdot 6$; par ailleurs, 785 vérifie bien l'énoncé : $785 = 17 \cdot 46 + 3 = 11 \cdot 71 + 4 = 6 \cdot 130 + 5$. Il s'ensuit que 785 est bien le plus petit des nombres possibles.

Avec son formalisme efficace, l'arithmétique modulaire a rendu ce type de problème plus facile à résoudre.

Théorème 28.5. [des restes chinois] *Soient $n_1, \ldots, n_r$ des entiers premier entre eux deux à deux, c'est-à-dire tels que :*

$$1 \;=\; n_i \wedge n_j \qquad (\forall\, 1 \leqslant i \neq j \leqslant r).$$

Alors pour tous entiers $a_1, \ldots, a_r$ quelconques, il existe un entier x satisfaisant les r équations de congruence :

$$\begin{aligned} x \;&\equiv\; a_1 \mod n_1, \\ &\cdots\cdots\cdots\cdots\cdots \\ x \;&\equiv\; a_r \mod n_r. \end{aligned}$$

De plus, toute autre solution x' est congrue $x' \equiv x \mod n_1 \ldots n_r$ à x modulo le produit *des n_i.*

Démonstration. Une solution x, au moins, peut être trouvée comme suit. En notant n le produit complet de tous les n_i :

$$n \;:=\; n_1 \cdots n_{i-1}\, n_i\, n_{i+1} \cdots n_r,$$

pour chaque entier fixé i compris entre 1 et r, les deux entiers :

$$n_i \qquad \text{et} \qquad \widehat{n}_i \;:=\; \frac{n}{n_i} \;=\; n_1 \cdots n_{i-1}\, n_{i+1} \cdots n_r,$$

sont clairement premiers entre eux. Rappelons alors comment, grâce au Théorème 20.2 de Bézout, on peut déterminer l'inverse v_i de $\widehat{n}_i$ modulo n_i.

Pour cela, on applique l'algorithme d'Euclide, jusqu'à obtenir deux entiers u_i et v_i satisfaisant :

$$u_i\, n_i + v_i\, \widehat{n}_i \;=\; 1.$$

Si on pose alors :

$$e_i \;:=\; v_i\, \widehat{n}_i \;=\; v_i\, n_1 \cdots n_{i-1} n_{i+1} \cdots n_r,$$

il vient :

$$e_i \;\equiv\; 1 \mod n_i \qquad \text{ainsi que} \qquad e_i \;\equiv\; 0 \mod n_j \text{ pour tout } j \neq i.$$

Une solution particulière de tout ce système de r équations de congruence s'offre alors tendrement à nous :

$$x \;:=\; a_1\, e_1 + \cdots + a_r\, e_r.$$

Assertion 28.6. *Toute autre solution $x' \equiv a_i \mod n_i$ pour $i = 1, \ldots, r$ satisfait nécessairement :*

$$x' - x \;\equiv\; 0 \mod n_1 \cdots n_r.$$

Preuve. Pour $i = 1, \ldots, r$, soustrayons :

$$x' \;\equiv\; a_i \mod n_i \qquad \text{terme à terme avec} \qquad x \;\equiv\; a_i \mod n_i,$$

pour obtenir :

$$x' - x \;\equiv\; 0 \mod n_i \qquad (i = 1, \ldots, r).$$

Ainsi, $x' - x$ est divisible séparément par les r entiers $n_1, \ldots, n_r$, qui sont premiers entre eux, et donc par conséquent, grâce aux théorèmes que nous avons démontrés [27], $x' - x$ est divisible par leur *produit* $n_1 \cdots n_r$. □

Une fois que notre douce solution particulière $x = a_1\, e_1 + \cdots + a_r\, e_r$ a été trouvée, cette assertion conclut la démonstration d'*unicité*, modulo $n = n_1 \cdots n_r$, des solutions. □

27. Euclide, Gauss, Obélix, et Compagnie …

Devinette – Solution

Problème
Trouver le nombre qui:
- divisé par 11 a un reste 4,
- divisé par 15 a un reste 10, et
- divisé par 19 a un reste 16.

Solution
Avec un tableur, la solution est simple !
- Colonne 1, les nombres k successifs
- Colonne 2, les nombre n = 11k + 4
- Colonne 3, valeurs de (n – 10) mod 15
- Colonne 4, valeurs de (n – 16) mod 19
- Colonne 5, test si mod = 0 en colonne 3 et 4. Si oui, c'est la bonne réponse.

Le nombre n = 1 555 est la solution.

Extrait tableur

=SI(ET(F142=0;G142=0);"Bingo";"n")

	D	E	F	G	H
		11	15	19	Test
1		15	5	18	n
2		26	1	10	n
3		37	12	2	n
140		1544	4	8	n
141		1555	0	0	Bingo
142		1566	11	11	n

Vérification
11 x 141 + 4 = 1 555
1 555 – 10 est divisible par 15 (= 103)
1 555 – 16 est divisible par 19 (= 81)

29. Anneaux commutatifs

À partir de maintenant, nous allons vouloir présenter et développer des aspects plus abstraits et plus généraux de la théorie mathématique des *structures algébriques*. Souvenons-nous que dans la Section **5**, lorsque nous avons construit $\mathbb{Z}$, nous avons déjà introduit le concept d'*anneau commutatif*, à travers la Définition 5.9, que nous reformulons ici de manière plus concise comme suit [28].

Définition 29.1. Soit $\mathbb{A}$ un ensemble muni de deux *lois de composition internes* $+$ et $\times$, c'est-à-dire $a+b \in \mathbb{A}$ et $a \times b \in \mathbb{A}$ pour tous $a, b \in \mathbb{A}$. On dit que $\mathbb{A}$ est un *anneau commutatif* s'il vérifie les propriétés suivantes.

(1) Le couple $(\mathbb{A}, +)$ est un *groupe commutatif*, au sens de la Définition 5.1 vue au chapitre précédent [29], d'élément neutre $0_{\mathbb{A}}$.

(2) La loi de multiplication $\times$ est associative et commutative d'élément neutre $1_{\mathbb{A}}$.

(3) La loi $\times$ est distributive par rapport à $+$:

$$a \times (b+c) \;=\; a \times b + a \times c \qquad (\forall\, a, b, c \in \mathbb{A}).$$

Le cas d'un anneau dans lequel $0_{\mathbb{A}} = 1_{\mathbb{A}}$ est très dégénéré : l'Exercice 2 propose de vérifier qu'alors tous les éléments $a \in \mathbb{A}$ sont égaux à $0_{\mathbb{A}}$, de telle sorte que $\mathbb{A} = \{0_{\mathbb{A}}\}$. On dit alors que $\mathbb{A}$ est l'*anneau nul*. Mais comme tout ce qui est nul est « *nul* », on supposera toujours à partir de maintenant que $0_{\mathbb{A}} \neq 1_{\mathbb{A}}$.

Clairement :

$$\big(\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Z}/n\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Q}, +, \times\big), \qquad \big(\mathbb{R}, +, \times\big), \qquad \big(\mathbb{C}, +, \times\big),$$

sont des anneaux commutatifs. Qui plus est, il y a des inclusions qui respectent les structures respectives.

Définition 29.2. Soit $\big(\mathbb{A}, +_{\mathbb{A}}, \times_{\mathbb{A}}\big)$ un anneau commutatif. On dit qu'un sous-ensemble $\mathbb{B} \subset \mathbb{A}$ est un *sous-anneau* de $\mathbb{A}$ lorsque :

(1) $(\mathbb{B}, +)$ est un *sous-groupe commutatif* de $(\mathbb{A}, +_{\mathbb{A}})$, c'est-à-dire que :

$$b,\, b' \in \mathbb{B} \qquad \Longrightarrow \qquad b +_{\mathbb{A}} b' \in \mathbb{B},$$

28. Plus tard, nous formulerons une définition dans laquelle nous ne demanderons pas forcément que la multiplication $\times$ soit commutative.

29. Rappelons en effet que dans groupe commutatif G, on a $x * (y * z) = (x * y) * z$, puis $x * y = y * x$, et enfin surtout $x * x^{-1} = e = x^{-1} * x$ pour tout $x \neq 0$, où $e \in G$ est l'élément neutre. Ici dans un anneau commutatif, la loi $* := +$ dispose bien de toutes ces bonnes propriétés, mais pas la loi $\times$.

où l'addition est prise dans $\mathbb{A}$, de telle sorte que $(\mathbb{B}, +_{\mathbb{A}})$ est un groupe commutatif en lui-même.

(2) pour tous $b, b' \in \mathbb{B}$, on a $b \times_{\mathbb{A}} b' \in \mathbb{B}$ aussi ;

(3) $1_{\mathbb{A}} \in \mathbb{B}$.

En jouant avec la logique (trop) pure (et peu intéressante), on vérifie que $\big(\mathbb{B}, +, \times_{\mathbb{A}}\big)$ est alors un anneau en lui-même.

Par exemple, les inclusions suivantes sont des inclusions de sous-anneaux :

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

pour l'addition $+$ et la multiplication $\times$ classiques. Enfin, rappelons la Définition 5.10 a déjà introduit le concept de corps commutatif, que nous pouvons reformuler comme suit.

Définition 29.3. [Corps] Un *corps commutatif* $\mathbb{K}$ est un anneau commutatif pour lequel $(\mathbb{K}, \times)$ est un groupe commutatif.

Autrement dit, tout élément non nul $x \in \mathbb{K}\backslash\{0_{\mathbb{K}}\}$ admet un élément inverse $x' \in \mathbb{K}$ satisfaisant $x'x = 1_{\mathbb{K}}$, ce qui garantit que la loi $* := \times$ est une loi de groupe, tout aussi bien que la loi $+$ de l'anneau sous-jacent.

30. Groupe des inversibles d'un anneau commutatif

Soit un anneau commutatif quelconque $\big(\mathbb{A}, +, \times\big)$, par exemple n'importe quel $\mathbb{Z}/n\mathbb{Z}$, ou $\mathbb{Z}$ lui-même. En général, $\mathbb{A}$ n'est *pas* un corps, et on sait d'ailleurs déjà, grâce au Théorème 27.5, que $\mathbb{Z}/n\mathbb{Z}$ n'est *jamais* un corps, dès que l'entier $n = d\,m$ est *composé*, avec $1 < d < n$ et $1 < m < n$.

Autrement dit, il y a certains éléments $a \in \mathbb{A}$ qui n'ont (malheureusement) pas d'*inverse* $a' \in \mathbb{A}$ pour l'opération de multiplication $\times$. Toutefois, on peut décider de sélectionner seulement les éléments de $\mathbb{A}$ qui sont inversibles, pour la multiplication.

Définition 30.1. On appelle *groupe des inversibles* d'un anneau $\big(\mathbb{A}, +, \times\big)$ l'ensemble noté :

$$\mathbb{A}^{\times} := \big\{a \in \mathbb{A} : \text{ il existe } a' \in \mathbb{A} \text{ satisfaisant } a\,a' = 1_{\mathbb{A}}\big\}.$$

Par exemple :

$$\mathbb{Z}^{\times} = \big\{-1, +1\big\}.$$

Évidemment, l'inverse d'un élément $a \in \mathbb{A}^{\times}$ est unique, car si a'' est un *autre* inverse, en multipliant à gauche par a' :

$$a' \big(\, a\,(a' - a'') = 0 \,\big),$$

on trouve instantanément $a' = a''$.

Alors $A^{\times}$ est un groupe commutatif en lui-même pour l'opération $\times$, au sens de la Définition 5.1, essentiellement parce que :

$$a,\, b \in \mathbb{A}^{\times} \qquad \text{implique} \qquad a \times b \in \mathbb{A}^{\times} \qquad \text{avec} \qquad \big(a \times b\big)' = b' \times a',$$

puisque :

$$\begin{aligned} (a \times b)\,\big(b' \times a'\big) &= a \times \underline{b \times b'}_{\circ} \times a' \\ &= \underline{a \times a'}_{\circ} \\ &= 1. \end{aligned}$$

Mais attention ! On dit bien « *groupe* » (multiplicatif) des inversibles, et non pas « *anneau* » (faux !) des inversibles, car $\mathbb{A}^\times$ n'est jamais invariant pas addition/soustraction, comme le montre l'exemple stupide :

$$1 \in \mathbb{Z}^\times \quad \text{et} \quad -1 \in \mathbb{Z}^\times \qquad \stackrel{?}{\Longrightarrow} \qquad 1+(-1) = 0 \in \mathbb{Z}^\times \ \text{(ah non !)}.$$

Proposition 30.2. *L'ensemble* $(\mathbb{A}^\times, \times)$ *muni de la multiplication est un groupe commutatif.*

Démonstration. Comme la loi $\times$ est associative sur $\mathbb{A}$, elle l'est également sur $\mathbb{A}^\times$. L'élément neutre $1_\mathbb{A}$ est tautologiquement inversible, donc on a $1_\mathbb{A} \in \mathbb{A}^\times$, et $1_\mathbb{A}$ est élement neutre pour $\times$.

Enfin, tout élément $a \in \mathbb{A}^\times$ admet un inverse *dans* $\mathbb{A}^\times$, car l'existence de $a' \in \mathbb{A}$ avec $a\,a' = a'a = 1_\mathbb{A}$ montre que a' lui-même est inversible, avec a pour inverse, c'est-à-dire appartient aussi à $\mathbb{A}^\times$. □

31. Anneaux commutatifs produits

Dans la Section **33** suivante, nous allons comparer :

$$\mathbb{Z}/mn\mathbb{Z} \stackrel{?}{\longleftrightarrow} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

où m, n sont deux entiers *premiers entre eux*. À cette occasion, nous aurons besoin du concept de *produit* entre anneaux commutatifs, dont voici une

Définition 31.1. Étant donné deux anneaux commutatifs $\big(\mathbb{A}, +_\mathbb{A}, \times_\mathbb{A}\big)$ et $\big(\mathbb{B}, +_\mathbb{B}, \times_\mathbb{B}\big)$, l'*anneau produit* $\big(\mathbb{A}\times\mathbb{B},\, +,\, \times\big)$ est l'ensemble produit constitué de couples d'éléments :

$$\mathbb{A}\times\mathbb{B} := \big\{(a,b)\colon\ a \in \mathbb{A} \text{ quelconque},\ b \in \mathbb{B} \text{ quelconque}\big\},$$

pour lequel les deux lois de compositions interne $+$ et $\times$ sont définies par :

$$(a,b) + (a',b') := \big(a +_\mathbb{A} a',\, b +_\mathbb{B} b'\big) \qquad \text{d'élément neutre } \big(0_\mathbb{A}, 0_\mathbb{B}\big),$$
$$(a,b) \times (a',b') := \big(a \times_\mathbb{A} a',\, b \times_\mathbb{B} b'\big) \qquad \text{d'élément neutre } \big(1_\mathbb{A}, 1_\mathbb{B}\big).$$

On vérifie par le raisonnement (tauto)logique que $\big(\mathbb{A}\times\mathbb{B},\, +,\, \times\big)$ est effectivement un anneau commutatif, au sens de la Définition 29.1.

Plus généralement, étant donné un nombre fini $\nu \geqslant 1$ d'anneaux commutatifs $\mathbb{A}_1, \dots, \mathbb{A}_\nu$, on peut construire l'*anneau-produit :*

$$\mathbb{A}_1 \times \cdots \times \mathbb{A}_\nu := \big\{\big(a_1, \dots, a_\nu\big)\colon\ a_1 \in \mathbb{A}_1 \text{ quelconque},\ \dots,\ a_\nu \in \mathbb{A}_\nu \text{ quelconque}\big\},$$

muni des opérations :

$$\big(a_1, \dots, a_\nu\big) + \big(a'_1, \dots, a'_\nu\big) := \big(a_1 +_{\mathbb{A}_1} a'_1, \dots, a_\nu +_{\mathbb{A}_\nu} a'_\nu\big),$$
$$\big(a_1, \dots, a_\nu\big) \times \big(a'_1, \dots, a'_\nu\big) := \big(a_1 \times_{\mathbb{A}_1} a'_1, \dots, a_\nu \times_{\mathbb{A}_\nu} a'_\nu\big).$$

Par exemple, avec :

$$\mathbb{Z}/2\mathbb{Z} = \big\{0,\, 1\big\} \ \mathsf{mod}\, 2,$$
$$\mathbb{Z}/3\mathbb{Z} = \big\{0,\, 1,\, 3\big\} \ \mathsf{mod}\, 3,$$

on a :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \big\{(0,0),\ (0,1),\ (0,2),\ (1,0)\ (1,1),\ (1,2)\big\}.$$

Proposition 31.2. *Le groupe des inversibles de l'anneau-produit* $\mathbb{A}\times\mathbb{B}$ *est :*

$$\big(\mathbb{A}\times\mathbb{B}\big)^\times = \mathbb{A}^\times \times \mathbb{B}^\times.$$

Preuve. Cela provient directement du fait que la loi de multiplication :

$$\big(a,\, b\big) \times \big(b,\, b'\big) \;=\; \big(aa',\, bb'\big),$$

s'effectue composante par composante. □

32. Isomorphismes entre anneaux commutatifs

Sur le plan didactique général, le terme « *isomorphisme* » désigne une relation entre des corps ou des objets de formes analogues, ou encore, entre des réalisations de même structure sous-jacente.

> La notion d'isomorphisme vient de la constatation qu'un individu tend à reconstruire autour de lui une constellation relationnelle qui reste relativement invariable même quand on le change de milieu.

En cristallographie, les corps dits « *isomorphes* » ont généralement une grande parenté dans leur constitution chimique, et notamment, ils ont la propriété de pouvoir se remplacer mutuellement dans la formation d'un même cristal, appelé parfois « *solution solide* ».

En linguistique aussi, « *isomorphisme* » est un concept avéré : il désigne une relation existant entre deux langues ou deux structures linguistiques, quand elles présentent toutes deux le même type de relations combinatoires.

En mathématiques enfin, un « *isomorphisme* » entre deux ensembles structurés est une application *bijective* qui *préserve* les structures respectives, et dont la réciproque *préserve aussi* ces structures.

> Le lecteur nous accordera que deux édifices mathématiques d'apparences fort dissemblables puissent, quand on examine leurs « secrètes architectures » conduire à des structures identiques, indiscernables. Chacun d'eux est la réalisation concrète d'un même groupe abstrait : on dit qu'ils sont « *en isomorphie* ». François LE LIONNAIS, Les grands courants de la pensée mathématique.

Un *isomorphisme* est donc une bijection pour laquelle les relations « algébriques » entre les éléments de l'ensemble d'arrivée sont les mêmes que celles entre leurs antécédents respectifs : la structure algébrique est préservée. Ce « méta-concept » mathématique admet une définition formelle.

Avec des symboles, soient E et F deux ensembles dont les éléments généraux sont notés e et f, respectivement. De plus, soient $\oplus$ et $\otimes$ leurs lois internes respectives. S'il existe une application bijective $\Phi\colon\, E \longrightarrow F$ satisfaisant :

$$\Phi\big(e_1 \oplus e_2\big) \;=\; \Phi(e_1) \otimes \Phi(e_2) \qquad (\forall\; e_1, e_2 \in E),$$

de telle sorte que la bijection réciproque $E \longleftarrow F \;:\Phi^{-1}$ satisfait de même :

$$\Phi^{-1}(f_1) \oplus \Phi^{-1}(f_2) \;=\; \Phi^{-1}\big(f_1 \otimes f_2\big) \qquad (\forall\; f_1, f_2 \in F),$$

alors on dit que les deux ensembles munis de structures $(E, \oplus)$ et $(F, \otimes)$ sont *isomorphes*. On dit que Φ et son inverse Φ^{-1} sont des *isomorphismes*. Quand $E = F$ et $\oplus = \otimes$, on dit que Φ est un *automorphisme*.

Parce qu'un isomorphisme préserve les aspects structuraux d'un ensemble, d'un groupe, d'un anneau, d'un corps, ou autres, on cherche souvent à *trouver* des isomorphismes qui envoient un objet « compliqué » vers un objet plus « simple » ou mieux connu, afin de comprendre, ou de mieux « pénétrer », ses propriétés mathématiques intimes.

Définition 32.1. Soient $\big(\mathbb{A}, +_{\mathbb{A}}, \times_{\mathbb{A}}\big)$ et $\big(\mathbb{B}, +_{\mathbb{B}}, \times_{\mathbb{B}}\big)$ deux anneaux commutatifs. Un *morphisme d'anneaux* de $\mathbb{A}$ vers $\mathbb{B}$ est une application $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ satisfaisant [30] :

(1) $f\big(a +_{\mathbb{A}} a'\big) = f(a) +_{\mathbb{B}} f(a')$ pour tous $a, a' \in \mathbb{A}$;

(2) $f(0_{\mathbb{A}}) = 0_{\mathbb{B}}$;

(3) $f\big(a \times_{\mathbb{A}} a'\big) = f(a) \times_{\mathbb{B}} f(a')$, pour tous $a, a' \in \mathbb{A}$;

(4) $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

Quand f est bijectif, on dit que f est un *isomorphisme* [31].

> Certains auteurs — français — disent *morphisme*, plutôt que *homomorphisme*. Les anglais/américains disent *homomorphism*, les italiens *omomorfismo*, les espagnols *homomorfismo*, les allemands *Homomorphismus*, ou *Gruppenhomomorphismus*. Depuis quelques années, certains français disent *morphisme* — bon, . . . Thomas Delzant

Lorsque seules les conditions **(1)** et **(2)** sont satisfaites, on parle de morphismes de groupes commutatifs sous-jacents

Par exemple, l'application $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $x \longmapsto -x$ est un isomorphisme entre les deux groupes commutatifs $(\mathbb{Z}, +)$ et $(\mathbb{Z}, +)$, d'application inverse $-y \longleftarrow y$.

Terminologie 32.2. Quand $\mathbb{A} = \mathbb{B}$, on dit que f est un *endomorphisme* de $\mathbb{A}$. Quand $f\colon \mathbb{A} \longrightarrow \mathbb{A}$ est de plus bijectif, on dit que f est un *automorphisme* de $\mathbb{A}$.

Par (contre-)exemple, avec une constante non nulle $\lambda \in \mathbb{Z}\backslash\{0\}$, l'application $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $f(x) := \lambda\, x$ est un morphisme de groupes commutatifs $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, mais dès que $\lambda \neq 1$, ce n'est *pas* un morphisme d'anneaux, car :

$$f\big(a\, a'\big) \;=\; \lambda\, a\, a' \;\neq\; (\lambda\, a)\, (\lambda\, a').$$

Définition 32.3. Le *noyau* d'un morphisme d'anneaux commutatifs $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ est l'ensemble :

$$\mathsf{Ker}\, f \;:=\; \big\{a \in \mathbb{A}\colon\;\; f(a) = 0_{\mathbb{B}}\big\}.$$

Son *image* est l'ensemble :

$$\mathsf{Im}\, f \;:=\; \big\{b \in \mathbb{B}\colon\;\; \text{il existe } a \in \mathbb{A} \text{ tel que } f(a) = b\big\}.$$

L'Exercice 3 propose de vérifier que $\mathsf{Im}\, f$ est toujours un sous-anneau de $\mathbb{B}$.

Mais comme $\mathsf{Ker}\, f$ ne contient pas toujours $1_{\mathbb{A}}$, et comme on *demande* dans la Définition 29.1 d'anneau commutatif (unitaire) que la multiplication $\times$ ait un élément neutre 1, le noyau $\mathsf{Ker}\, f$, qui ne contient en général pas $1_{\mathbb{A}}$, n'est pas toujours un sous-anneau de $\mathbb{A}$.

Proposition 32.4. *Tout morphisme d'anneaux commutatifs $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ induit, en restriction au groupe des inversibles $\mathbb{A}^\times \subset \mathbb{A}$, un morphisme de groupes commutatifs :*

$$f\colon \quad \mathbb{A}^\times \;\longrightarrow\; \mathbb{B}^\times.$$

Observons que nous n'avons pas encore formellement défini le concept de *morphisme entre groupes commutatifs*, mais le lecteur-étudiant aura certainement déjà deviné de quoi il s'agit.

30. On peut montrer que **(2)** est conséquence de **(1)**.

31. On peut vérifier que la bijection inverse $\mathbb{A} \longleftarrow \mathbb{B} : f^{-1}$ satisfait quatre axiomes similaires, par exemple $f^{-1}(b) +_{\mathbb{A}} f^{-1}(b') = f^{-1}(b +_{\mathbb{B}} b')$ ainsi que $f^{-1}(b) \times_{\mathbb{A}} f^{-1}(b') = f^{-1}(b \times_{\mathbb{B}} b')$.

Démonstration. Comme f est un morphisme d'anneaux, on sait déjà qu'il transfère (traduit) la multiplication dans $\mathbb{A}$ en la multiplication dans $\mathbb{B}$, et que $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$. La seule chose qui manque, c'est que f envoie bien les inversibles de $\mathbb{A}$ vers les inversibles de $\mathbb{B}$:

$$f\big(\mathbb{A}^\times\big) \overset{?}{\subset} \mathbb{B}^\times \ \textbf{?}$$

Mais si $a \in \mathbb{A}^\times$ admet l'inverse $a^{-1} \in \mathbb{A}^\times$ avec $a\,a^{-1} = 1_{\mathbb{A}}$, l'égalité suivante, vraie grâce au fait que f est un morphisme :

$$f(a)\,f(a^{-1}) \;=\; f\big(a\,a^{-1}\big) \;=\; f(1_{\mathbb{A}}) \;=\; 1_{\mathbb{B}},$$

montre aussitôt que $f(a^{-1}) := b'$ est un inverse de $f(a) = b$, unique en fait, que l'on peut d'ailleurs noter aussi b^{-1}.

Donc on a bien $f(a)$ inversible, quel que soit $a \in \mathbb{A}^\times$. □

33. Isomorphisme $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ pour $m \wedge n = 1$

Question 33.1. *Comment comparer les divers $\mathbb{Z}/n\mathbb{Z}$, lorsque $n \in \mathbb{Z}$ varie ?*

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x mod 3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
x mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Par exemple, la première ligne (en caractères gras) du tableau ci-dessus liste les quinze éléments de $\mathbb{Z}/15\mathbb{Z}$, puis la seconde et la troisième ligne représentent tous les couples d'éléments du produit $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. On y constate que chaque paire d'éléments apparaît exactement une seule fois, et donc, que $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ possède *aussi* quinze éléments. Bientôt, nous allons expliquer de manière générale ce phénomène.

Commençons par une observation naturelle, élémentaire, et très utile.

Proposition 33.2. *Étant donné deux entiers $m \geqslant 1$ et $n \geqslant 1$, quels que soient $a, b \in \mathbb{Z}$, on a :*

$$a \;\equiv\; b \mod m\,n \qquad \Longrightarrow \qquad \begin{cases} a \;\equiv\; b \mod m, \\ a \;\equiv\; b \mod n. \end{cases}$$

Preuve. Cela est tout à fait clair :

$$a \;=\; b + m\,n\,k \qquad \Longrightarrow \qquad \begin{cases} a \;=\; b + m\,(n\,k), \\ a \;=\; b + n\,(m\,k). \end{cases}$$ □

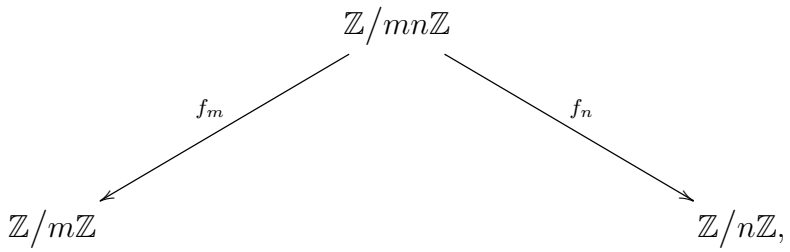
Corollaire 33.3. *Par contraposition de la première ligne :*

$$a \;\not\equiv\; b \mod m\,n \qquad \Longleftarrow \qquad a \;\not\equiv\; b \mod m.$$ □

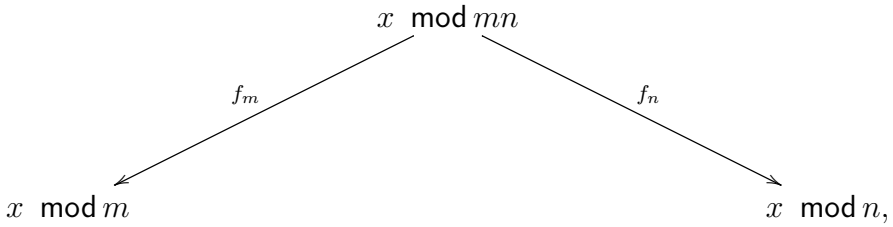
Nous pouvons illustrer cette proposition avec $m := 5$ et $n := 2$, où les $5 \cdot 2 = 10$ éléments de $\mathbb{Z}/10\mathbb{Z}$, sont réduits modulo 5 :

$$\begin{aligned} &\big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\big\} \mod 10 \\ \text{deviennent}\quad &\big\{0,\ 1,\ 2,\ 3,\ 4,\ 0,\ 1,\ 2,\ 3,\ 4\big\} \mod 5. \end{aligned}$$

Proposition 33.4. *Soient deux entiers arbitraires $m \geqslant 1$ et $n \geqslant 1$. Alors il existe deux applications de réduction :*



définies par :



qui sont de plus des morphismes d'anneaux.

Par symétrie, on peut étudier seulement f_m. Ici, f_m prend un entier modulo $m\,n$ et le « réduit » modulo m, comme dans l'exemple des deux mains à cinq doigts ci-dessus.

D'abord, il faut vérifier que f_m est bien définie, ce que nous allons faire. Ensuite aussi, que l'on a bien, quels que soient $a, b \in \mathbb{Z}/mn\mathbb{Z}$:

$$\begin{aligned} f_m(a+b) &= f_m(a) + f_m(b), \\ f_m(a \times b) &= f_m(a) \times f_m(b). \end{aligned}$$

Attention ! Les opérations $+$, $\times$ *à gauche* s'effectuent modulo mn, c'est-à-dire dans $\mathbb{Z}/mn\mathbb{Z}$, tandis que les opérations $+$, $\times$ *à droite* s'effectuent modulo m, dans $\mathbb{Z}/m\mathbb{Z}$, qui comporte *moins* d'éléments — n fois moins, précisément.

Avec $m = 5$, $n = 2$, explicitons concrètement le fait que f_5 est un morphisme d'anneaux, sur deux exemples numériques :

$$\begin{aligned} 7+9 \underset{10}{\equiv} 6 \overset{f_5}{\longmapsto} \underset{5}{\equiv} 1 \quad &\overset{\text{OUI}}{=} \quad 1 \underset{5}{\equiv} 2+4 = f_5(7) + f_5(9), \\ 4 \times 7 \underset{10}{\equiv} 8 \overset{f_5}{\longmapsto} \underset{5}{\equiv} 3 \quad &\overset{\text{OUI}}{=} \quad 3 \underset{5}{\equiv} 4 \times 2 = f_5(4) \times f_5(7). \end{aligned}$$

Démonstration de la Proposition 33.4. Rappelons que :

$$\mathbb{Z}/mn\mathbb{Z} = \big\{0,\, 1,\, 2,\, \ldots,\, mn-1\big\} \mod mn.$$

Autrement dit, dans les calculs, tous les entiers de $\mathbb{Z}$ sont considérés modulo mn, et « ramenés dans la marmite », l'ensemble $\{0, 1, \ldots, mn-1\}$.

Un élément $a \in \mathbb{Z}/mn\mathbb{Z}$, c'est un $a \in \big\{0, 1, \ldots, mn-1\big\}$ avec la collection de tous les $a + mn\,k$, où $k \in \mathbb{Z}$ est quelconque. Et l'on identifie $a + mn\,k$ avec $a + mn\,k'$ *parce que* leur différence :

$$a + mn\,k - \big(a + mn\,k'\big) = m\,n\,\big(k - k'\big),$$

est un multiple de $m\,n$.

Commençons par montrer que l'application :

$$\begin{array}{rccc} f_m\colon & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & a \mod mn & \longmapsto & a \mod m, \end{array}$$

est *bien définie*. Il faut vérifier que f_m prend la même valeur sur deux éléments quelconques :

$$a + mn\,k \qquad \text{et} \qquad a + mn\,k',$$

et cela est clair, parce que un multiple de $m\,n$ est toujours un multiple de m :

$$\begin{array}{rc} & a + mn\,k \overset{?}{\equiv} a + mn\,k' \mod m \\ \iff & 0 \overset{\text{OUI}}{\equiv} m\,(n\,k' - n\,k) \mod m. \end{array}$$

Ensuite, montrons que f_m est un morphisme d'anneaux. Soient $a, b \in \mathbb{Z}/mn\mathbb{Z}$ quelconques. Quel que soient les quatre éléments de $\mathbb{Z}$:

$$\begin{array}{ll} a + m\,n\,k, & a + m\,n\,k', \\ b + m\,n\,\ell, & b + m\,n\,\ell', \end{array}$$

il vient par addition verticale :

$$a + \underline{m\,n\,k}_{\circ} + b + \underline{m\,n\,\ell}_{\circ} \mod m \;\equiv\; a + \underline{m\,n\,k'}_{\circ} + b + \underline{m\,n\,\ell'}_{\circ} \mod m,$$

donc on a bien :

$$f_m\big(\underbrace{a+b}_{\substack{\text{addition}\\ \text{modulo } mn}}\big) \;=\; \underbrace{f_m(a) + f_m(b)}_{\substack{\text{addition}\\ \text{modulo } m}}.$$

Pour ce qui est des deux multiplications possibles :

$$\begin{aligned} \big(a + m\,n\,k\big)\,\big(b + m\,n\,\ell\big) &= a\,b + a\,m\,n\,\ell + m\,n\,k\,b + m\,n\,k\,m\,n\,\ell, \\ \big(a + m\,n\,k'\big)\,\big(b + m\,n\,\ell'\big) &= a\,b + a\,m\,n\,\ell' + m\,n\,k'\,b + m\,n\,k'\,m\,n\,\ell', \end{aligned}$$

leur résultat est *identique modulo* m, car les 3 derniers termes de chaque ligne sont visiblement tous multiples de m !

Donc on a bien aussi :

$$f_m\big(\underbrace{a\times b}_{\substack{\text{multiplication}\\ \text{modulo } mn}}\big) \;=\; \underbrace{f_m(a) + f_m(b)}_{\substack{\text{multiplication}\\ \text{modulo } m}}. \qquad \square$$

Répétons que les opérations $+$ et $\times$ ont un sens *différent* de part et d'autre du signe '='. Et dans la Définition 32.1 générale, nous avions bien spécifié que les additions et les multiplications pouvaient être *différentes* dans $\mathbb{A}$ et dans $\mathbb{B}$, lorsque nous avons écrit :

$$\begin{aligned} f\big(a +_{\mathbb{A}} a'\big) &= f(a) +_{\mathbb{B}} f(a'), \\ f\big(a \times_{\mathbb{A}} a'\big) &= f(a) \times_{\mathbb{B}} f(a'). \end{aligned}$$

Nous parvenons enfin à un point de maturité théorique où nous pouvons exprimer une version mathématique abstraite et plus complète du Théorème 28.5 des restes chinois, déjà exposé avec des outils rudimentaires.

Le produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ étant encore un anneau, grâce à la Section **31**, nous pouvons « mettre ensemble » nos deux applications f_m et f_n, ce qui nous donne l'application :

$$\begin{aligned} f: \qquad \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto \big(f_m(x),\, f_n(x)\big). \end{aligned}$$

Théorème 33.5. *Si $m \wedge n = 1$ sont premiers entre eux, alors le morphisme d'anneaux :*

$$\begin{aligned} f: \qquad \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x \bmod mn &\longmapsto \Big(x \bmod m,\ \ x \bmod n\Big), \end{aligned}$$

est un isomorphisme.

Démonstration. Il s'agit de montrer que f est *bijectif*. Mais comme :

$$q \,=\, \mathsf{Card}\,\big\{0,\, 1,\, 2,\, \ldots,\, q-1\big\},$$

tous ces anneaux sont de cardinal fini, *i.e.* ont un nombre fini d'éléments [32] :

$$\begin{aligned} mn \,&=\, \mathsf{Card}\,\mathbb{Z}/mn\mathbb{Z}, \qquad\qquad m \,=\, \mathsf{Card}\,\mathbb{Z}/m\mathbb{Z}, \qquad\qquad n \,=\, \mathsf{Card}\,\mathbb{Z}/n\mathbb{Z} \\ &=\, \mathsf{Card}\,\Big(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\Big), \end{aligned}$$

donc f est un morphisme entre anneaux de cardinaux *égaux*. Super !

Or puisque l'on sait qu'une application entre ensembles de même cardinal est bijective si et seulement si elle est injective, il va nous suffire de démontrer que :

$$f(x) \,=\, f(x') \qquad\qquad \overset{?}{\Longrightarrow} \qquad\qquad x \,=\, x'.$$

Mais comme f respecte l'addition, *i.e.* est un morphisme de groupes pour les lois $+$ respectives, ceci équivaut à [33] :

$$f(x - x') \,=\, (0, 0).$$

Avec $y := x - x'$, montrons donc que :

$$f(y) \,=\, \big(0 \bmod m,\ \ 0 \bmod n\big),$$

implique $y = 0$ dans $\mathbb{Z}/mn\mathbb{Z}$.

Or les deux équations $y \equiv 0 \bmod m$ et $y \equiv 0 \bmod n$ signifient qu'il existe $i \in \mathbb{Z}$ et $j \in \mathbb{Z}$ avec :

$$y \,=\, m\,i \qquad\qquad \text{et} \qquad\qquad y \,=\, n\,j.$$

Mais alors, l'égalité $m\,i = n\,j$ montre que $m\,i$ est divisible par n, et comme par hypothèse n est premier avec m, le Théorème 21.1 de Gauss force n à diviser i, c'est-à-dire $i = n\,k$, avec $k \in \mathbb{Z}$, d'où en remplaçant :

$$y \,=\, m\,n\,k \,=\, 0 \quad \text{ dans } \mathbb{Z}/mn\mathbb{Z}.$$

Donc f est injective, donc f est bijective, donc f établit un isomorphisme d'anneaux. Cela *achève* — à coups de hash ? — la démonstration. □

32. Rappelons en effet que si $E = \{e_1, \ldots, e_m\}$ et $F = \{f_1, \ldots, f_n\}$ sont deux ensembles finis, leur produit $E \times F$ a pour éléments tous les couples (e_i, f_j) avec $i = 1, \ldots, m$ et $j = 1, \ldots, n$, donc $\mathsf{Card}\, E \times F = \mathsf{Card}\, E \cdot \mathsf{Card}\, F$.

33. Oui, il y a bien deux zéros $(0, 0)$ à droite, le 0 de $\mathbb{Z}/m\mathbb{Z}$ et le 0 de $\mathbb{Z}/n\mathbb{Z}$ — pas d'erreur !

La Proposition 31.2 offre alors un corollaire direct de ce Théorème 33.5 chinois *occidentalisé*.

Théorème 33.6. *En restriction aux groupes d'inversibles respectifs, l'isomorphisme d'anneaux du théorème précédent offre un isomorphisme de groupes commutatifs :*

$$\begin{aligned} f\colon \qquad \big(\mathbb{Z}/mn\mathbb{Z}\big)^\times &\longrightarrow \big(\mathbb{Z}/m\mathbb{Z}\big)^\times \times \big(\mathbb{Z}/n\mathbb{Z}\big)^\times \\ x \mod mn &\longmapsto \Big(x \mod m,\ x \mod n\Big). \end{aligned}$$

Enfin, énonçons un résultat général, sans en détailler la démonstration puisqu'une simple récurrence sur le nombre de facteurs fonctionne sans obstacle.

Théorème 33.7. *Étant donné un nombre $r \geqslant 1$ d'entiers $n_1, \dots, n_r$ mutuellement premiers entre eux $n_i \wedge n_j = 1$ pour $i \neq j$, il existe un isomorphisme d'anneaux commutatifs :*

$$\begin{aligned} f\colon \qquad \mathbb{Z}/n_1 \cdots n_r\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ x \mod n_1 \cdots n_r &\longmapsto \Big(x \mod n_1,\ \dots,\ x \mod n_r\Big), \end{aligned}$$

qui, en restriction aux groupes des inversibles respectifs, fournit aussi un isomorphisme de groupes commutatifs :

$$\begin{aligned} f\colon \qquad \big(\mathbb{Z}/n_1 \cdots n_r\mathbb{Z}\big)^\times &\longrightarrow \big(\mathbb{Z}/n_1\mathbb{Z}\big)^\times \times \cdots \times \big(\mathbb{Z}/n_r\mathbb{Z}\big)^\times \\ x \mod n_1 \cdots n_r &\longmapsto \Big(x \mod n_1,\ \dots,\ x \mod n_r\Big). \end{aligned}$$

□

34. Multiplicativité de la fonction indicatrice φ d'Euler

Rappelons la Définition 27.10 de la fonction indicatrice d'Euler :

$$\begin{aligned} \varphi(n) &:= \mathsf{Card}\,\big\{1 \leqslant a \leqslant n\colon\ a \wedge n = 1\big\} \\ &= \mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^\times, \end{aligned}$$

Le résultat suivant, qui va découler du (très) beau Théorème 33.7, permet de calculer rapidement $\varphi(n)$ pour un entier n arbitraire.

Théorème 34.1. **(1)** *Si $m \geqslant 1$ et $n \geqslant 1$ sont premiers entre eux,* i.e. *vérifient $m \wedge n = 1$, alors :*

$$\varphi\big(m\,n\big) \,=\, \varphi(m)\,\varphi(n).$$

(2) *Si $p \in \mathscr{P}$ est premier, alors pour tout exposant $\alpha \geqslant 1$, on a :*

$$\varphi\big(p^\alpha\big) \,=\, p^\alpha - p^{\alpha-1}.$$

(3) *Pour un entier n arbitraire décomposé en facteurs premiers :*

$$n \,=\, p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $p_1 < \cdots < p_r$ premiers et avec des exposants $\alpha_1 \geqslant 1$, …, $\alpha_r \geqslant 1$, on a :

$$\begin{aligned} \varphi(n) \,&=\, \varphi\big(p_1^{\alpha_1}\big) \cdots \varphi\big(p_r^{\alpha_r}\big) \\ &=\, \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big) \cdots \big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \end{aligned}$$

Par exemple :

$$\begin{aligned}\varphi\big(1\,235\big) &= \varphi(5)\,\varphi(13)\,\varphi(19)\\ &= (5-1)\,(13-1)\,(19-1)\\ &= 4\cdot 12\cdot 18 \;=\; 864.\end{aligned}$$

Autre exemple :

$$\begin{aligned}\varphi\big(22\,500\,000\big) &= \varphi\big(2^5\big)\,\varphi\big(3^2\big)\,\varphi\big(5^7\big)\\ &= \big(2^5-2^4\big)\,\big(3^2-3^1\big)\,\big(5^7-5^6\big)\\ &= 16\cdot 6\cdot 625\,000\\ &= 6\,000\,000 \qquad \text{(d'euromillions).}\end{aligned}$$

Démonstration. Montrons **(1)**, appelée *propriété de multiplicativité* de la fonction indicatrice φ d'Euler.

Grâce à la Proposition 32.4, et à la Proposition 31.2, l'isomorphisme d'anneaux du Théorème 33.5 :

$$f\colon\quad \mathbb{Z}/mn\mathbb{Z} \;\xrightarrow{\sim}\; \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z},$$

induit par restriction aux groupes des inversibles respectifs un isomorphisme de groupes commutatifs :

$$\begin{aligned}\big(\mathbb{Z}/mn\mathbb{Z}\big)^\times \;&\xrightarrow{\sim}\; \big(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\big)^\times\\ &= \big(\mathbb{Z}/m\mathbb{Z}\big)^\times\times\big(\mathbb{Z}/n\mathbb{Z}\big)^\times,\end{aligned}$$

donc en particulier, une *bijection*. Par conséquent :

$$\mathsf{Card}\,\big(\mathbb{Z}/mn\mathbb{Z}\big)^\times \;=\; \mathsf{Card}\,\big(\mathbb{Z}/m\mathbb{Z}\big)\times\cdot\mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^\times,$$

c'est-à-dire précisément $\varphi(m\,n)=\varphi(m)\,\varphi(n)$, ce qui offre **(1)**.

Ensuite, montrons **(2)**. Soit donc un nombre premier $p\in\mathscr{P}$, et soit un exposant $\alpha\geqslant 1$. Observons que dans la formule à démontrer :

$$\varphi\big(p^\alpha\big) \;\overset{?}{=}\; p^\alpha - p^{\alpha-1},$$

il y a un signe « $-$ ».

Or rappelons que pour un ensemble *fini* E, et un sous-ensemble quelconque $F\subset E$, on a :

$$\mathsf{Card}\,\big(E\backslash F\big) \;=\; \mathsf{Card}\,E - \mathsf{Card}\,F.$$

Ici, l'ensemble E concerné a pour cardinal :

$$\mathsf{Card}\,\big\{1\leqslant k\leqslant p^\alpha\big\} \;=\; p^\alpha.$$

Alors plutôt que de déterminer directement :

$$\varphi\big(p^\alpha\big) \;=\; \mathsf{Card}\,\big\{1\leqslant k\leqslant p^\alpha\colon\ k \text{ est premier avec } p^\alpha\big\},$$

comptons les *autres* k, c'est-à-dire ceux qui ne sont *pas* premiers avec p^α.

Assertion 34.2. *Toujours avec $\alpha\geqslant 1$, pour un entier $1\leqslant k\leqslant p^\alpha$, on a équivalence entre :*

(i) *k est divisible par p, c'est-à-dire $k=p\,\ell$, avec $\ell\in\mathbb{N}$;*

(ii) *k n'est* pas *premier avec p^α.*

Preuve. L'implication **(i)** $\Longrightarrow$ **(ii)** est claire, puisque p est alors un facteur commun entre $k = p\,\ell$ et p^α car $\alpha \geqslant 1$.

Montrons maintenant **(ii)** $\Longrightarrow$ **(i)**. Par hypothèse, $d := \mathsf{pgcd}\,(k, p^\alpha)$ est > 1. Or d divise p^α. Grâce à la Proposition 24.12, on sait que $d = p^\beta$ pour un exposant $0 \leqslant \beta \leqslant \alpha$. Comme $d > 1$, nécessairement $\beta \geqslant 1$.

Enfin, comme d divise aussi k, c'est-à-dire $k = d\,\ell = p^\beta\,\ell$ avec $\ell \in \mathbb{N}$, nous concluons que k est bien divisible par p :

$$k \;=\; p^\beta\,\ell \;=\; p\,\big(p^{\beta-1}\,\ell\big). \qquad \square$$

Nous obtenons donc bien **(2)** :

$$\begin{aligned}
\varphi\big(p^\alpha\big) \;&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant k \leqslant \alpha\colon\ k \text{ n'est } \textit{pas} \text{ premier avec } p^\alpha\big\} \\
&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant k \leqslant p^\alpha\colon\ k = p\,\ell\big\} \\
&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant \ell \leqslant p^{\alpha-1}\big\} \\
&=\; p^\alpha - p^{\alpha-1}.
\end{aligned}$$

Pour terminer, montrons **(3)** en utilisant **(1)** et **(2)** :

$$\begin{aligned}
\varphi\big(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\big) \;&=\; \varphi\big(p_1^{\alpha_1}\big)\,\varphi\big(p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}\big) \\
&=\; \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\,\varphi\big(p_2^{\alpha_2}\big)\,\varphi\big(p_3^{\alpha_3} \cdots p_r^{\alpha_r}\big) \\
&=\; \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\,\big(p_2^{\alpha_2} - p_2^{\alpha_2-1}\big) \cdots \big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \qquad \square
\end{aligned}$$

35. Théorème d'Euler

Le Théorème d'Euler généralise le Théorème 25.1 de Fermat, qui ne traitait que le cas où $n = p$ était un nombre premier. Ce théorème d'arithmétique modulaire, publié [34] en 1761 par le mathématicien suisse Leonhard Euler, s'énonce comme suit.

Théorème 35.1. [Euler] *Pour tout entier $n \geqslant 1$, et tout entier $a \wedge n = 1$ premier avec n,* i.e. *inversible modulo n, on a :*

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

Par exemple, en base 10, proposons-nous de trouver le chiffre des unités de :

$$7^{222},$$

c'est-à-dire de trouver quel nombre (chiffre) entre 0 et 9 est congru à 7^{222} modulo 10. C'est facile ! Il suffit de voir que 7 et 10 sont premiers entre eux, et de savoir que $\varphi(10) = 4$, ce que l'on peut constater à partir de la table de multiplication suivante :

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[2]	[0]	[2]	[4]	[6]	[8]	[0]	[2]	[4]	[6]	[8]
[3]	[0]	[3]	[6]	[9]	[2]	[5]	[8]	[1]	[4]	[7]
[4]	[0]	[4]	[8]	[2]	[6]	[0]	[4]	[8]	[2]	[6]
[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]
[6]	[0]	[6]	[2]	[8]	[4]	[0]	[6]	[2]	[8]	[4]
[7]	[0]	[7]	[4]	[1]	[8]	[5]	[2]	[9]	[6]	[3]
[8]	[0]	[8]	[6]	[4]	[2]	[0]	[8]	[6]	[4]	[2]
[9]	[0]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

34. L. EULER, *Theoremata arithmetica nova methodo demonstrata*, Novi Comment. Acad. Sci. Imp. Petrop., vol. 8, 1763, pp. 74–104.

Le Théorème 35.1 d'Euler nous indique donc que :

$$7^4 \equiv 1 \mod 10,$$

d'où :

$$\begin{aligned} 7^{222} = 7^{4\cdot 55+2} &= \left(7^4\right)^{55} \cdot 7^2 \\ &\equiv 1^{55} \cdot 7^2 \\ &\equiv 49 \equiv 9 \mod 10. \end{aligned}$$

Le chiffre recherché est donc 9.

Démonstration. Les arguments, simples et élégants, sont essentiellement dus à Lagrange. Soit donc $n \geqslant 1$. On fixe $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ avec $a \wedge n = 1$, d'où $a \in \{2, \ldots, n-1\}$.

Assertion 35.2. [Point-clé] *Pour a premier avec n, l'application suivante est une bijection :*

$$\begin{array}{ccc} \left(\mathbb{Z}/n\mathbb{Z}\right)^\times & \longrightarrow & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\ x & \longmapsto & a\,x. \end{array}$$

Preuve. Comme $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est inversible, il existe $a^{-1} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ avec $a^{-1}a = 1$, dans $\mathbb{Z}/n\mathbb{Z}$.

Comme l'espace de départ et l'espace d'arrivée sont tous deux égaux — à $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ — et de cardinal fini, il suffit de vérifier que cette application est *injective*.

Si donc $a\,x \equiv a\,x' \mod n$, c'est-à-dire $a\,(x-x') \equiv 0$, utilisons a^{-1} pour déduire la coïncidence $x = x'$ témoignant de l'injectivité :

$$a^{-1}\,\big(\; a\,(x-x') \equiv 0 \;\big) \qquad \text{donne} \qquad x - x' \equiv 0. \qquad \square$$

Par conséquent, les deux ensembles suivant sont égaux, *i.e.* ont exactement les mêmes éléments :

$$\left\{x\colon\ x \in (\mathbb{Z}/n\mathbb{Z})^\times\right\} = \left\{a\,x\colon\ x \in (\mathbb{Z}/n\mathbb{Z})^\times\right\},$$

dont le nombre total est bien sûr égal à $\varphi(n)$. Très astucieusement, introduisons alors le produit :

$$\begin{aligned} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} a\,x \\ &= a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x, \end{aligned}$$

le signe '$=$' étant entendu *dans l'anneau* $\mathbb{Z}/n\mathbb{Z}$, puis multiplions l'égalité obtenue par le produit de tous les inverses x^{-1} possibles :

$$\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x^{-1} \left(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x = a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x \right),$$

ce qui offre la conclusion :

$$1 = a^{\varphi(n)}. \qquad \square$$

36. Appendice : Injections, Surjections, Bijections

Fill ??

37. Exercices

Exercice 1. [Caractérisation linéaire du pgcd] Étant donné deux constantes entières $a, b \in \mathbb{Z}$, on considère l'ensemble de leurs combinaisons linéaires à coefficients entiers :

$$\mathbb{Z}\,a + \mathbb{Z}\,b \;:=\; \big\{u\,a + v\,b\colon\;\; u \in \mathbb{Z},\;\; v \in \mathbb{Z}\big\}.$$

(a) Que dire lorsque $a = b = 0$?

(b) On suppose dorénavant $(a, b) \neq (0, 0)$ non tous les deux nuls. Soit $d := \mathsf{pgcd}\,(a, b)$. On introduit aussi :

$$\mathbb{Z}\,d \;:=\; \big\{w\,d\colon\;\; w \in\; \mathbb{Z}\big\}.$$

Montrer que $\mathbb{Z}\,d \subset \mathbb{Z}\,a + \mathbb{Z}\,b$.

(c) Inversement, montrer que $\mathbb{Z}\,a + \mathbb{Z}\,b \subset \mathbb{Z}\,d$. Indication: Dieu Bézout, aidez-nous !

(d) Conclure en énonçant un théorème soigné, clair, précis.

Exercice 2. Soit un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ dans lequel $1_{\mathbb{A}} = 0_{\mathbb{A}}$. Montrer que $\mathbb{A} = \{0_{\mathbb{A}}\big\}$. Indication: Utiliser les axiomes.

Exercice 3. Soit un morphisme $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ d'anneaux commutatifs. Montrer que $\mathsf{Im}\, f$ est un sous-anneau de $\mathbb{B}$.

Exercice 4. EE