MT 282

Groupes et Arithmétique

Chapitres choisis

B. Keller

Contents

1. Construction de Z à partir de N

En supposant connues les propriétés élémentaires de l'ensemble $\mathbf{N}$ et de l'addition des entiers naturels, nous allons donner une construction rigoureuse de $\mathbf{Z}$ et de l'addition des entiers relatifs. Dans cette construction, $\mathbf{Z}$ apparaîtra sous forme d'un quotient de $\mathbf{N} \times \mathbf{N}$ par une relation d'équivalence. Ce paragraphe est aussi l'occasion de rappeler les notions de relation d'équivalence et d'ensemble quotient, notions centrales pour le reste du cours.

Définition 1.1 *Soit X un ensemble. Une* relation sur X *est un ensemble $R \subset X \times X$ de couples d'éléments de X. On écrit xRx' au lieu de $(x, x') \in R$. Une relation R est une* relation d'équivalence *si elle est*

a) réflexive (i.e. pour tout $x \in X$, on a xRx)

b) symétrique (i.e. on a équivalence entre xRx' et $x'Rx$ quels que soient $x, x' \in X$)

c) transitive (i.e. les conditions xRx' et $x'Rx''$ impliquent que xRx'' quels que soient $x, x', x'' \in X$)

Exemples 1.2

1) Soit V l'ensemble des villes de France. On définit une relation R sur V en déclarant que vRv' signifie que v et v' se trouvent dans la même région. Il est facile de vérifier qu'il s'agit d'une relation d'équivalence.
2) Soit $X = \mathbf{N} \times \mathbf{N}$ et définissons R par

$$(x, y)R(x', y') \Leftrightarrow x + y' = y + x'.$$

Par exemple, on a $(0, 1)R(1, 2)$ et $(1, 2)R(2, 3)$. La réflexivité et la symétrie de R résultent de la commutativité de l'addition des entiers positifs. Montrons que R est transitive. En effet, par définition, les conditions $(x, y)R(x', y')$ et $(x', y')R(x'', y'')$ équivalent aux équations

$$\begin{aligned} x + y' &= y + x' \\ x' + y'' &= y' + x'' \end{aligned}$$

En rajoutant la première à la seconde on obtient

$$x + y' + x' + y'' = y + x' + y' + x''$$

ou encore

$$x + y'' + (x' + y') = x'' + y + (x' + y').$$

Or on sait que la loi d'addition sur $\mathbf{N}$ est *régulière* c'est-à-dire qu'une égalité $a+c = b+c$ implique $a = b$ quels que soient $a, b, c \in \mathbf{N}$. Il s'ensuit que $x+y'' = x''+y$ c'est-à-dire que $(x, y)R(x'', y'')$. Notons que dans cette démonstration, nous avons utilisé l'associativité, la commutativité et la régularité des entiers naturels.

Définition 1.3 *Soit X un ensemble et R une relation d'équivalence sur X. Pour $x \in X$, on pose*

$$^R\overline{x} = \{x' \in X \mid xRx' \} \subset X$$

et on appelle classe d'équivalence de x par rapport à R *cette partie de X. Par définition, l'ensemble X/R est formé des classes $^R\overline{x}$ d'éléments $x \in X$. On appelle X/R* le quotient de X par la relation d'équivalence R. *On définit* l'application quotient *(=*la projection canonique*) $q : X \to X/R$ par $q(x) = {}^R\overline{x}$. Une partie de X est un* système de représentants *pour R si elle contient un élément de chaque classe d'équivalence et un seul.*

Exemples 1.4

1) Dans l'exemple des villes de France (voir ci-dessus) la classe d'équivalence d'une ville v est formée de toutes les villes qui se trouvent dans la même région que v. En particulier deux classes $\overline{v}$ et $\overline{v'}$ sont égales ssi v et v' se trouvent dans la même région. Les éléments de V/R sont des ensembles de villes, deux villes étant regroupé dans un même ensemble ssi elles se trouvent dans la même région. On a donc une bijection

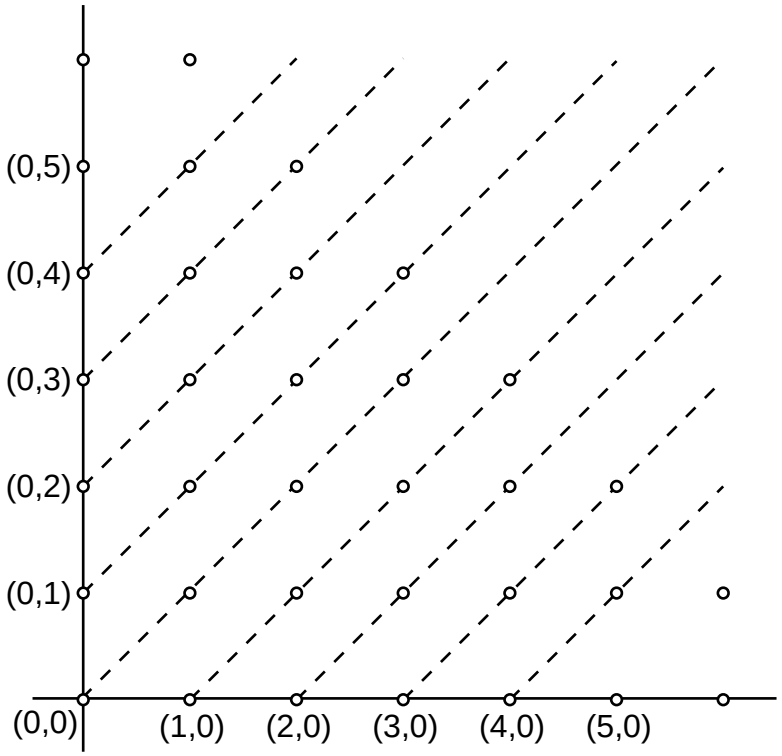
$$X/R \xrightarrow{\sim} \{\text{régions de France}\}\ ,\ \overline{v} \mapsto \text{la région où se trouve v.}$$

Il existe *beaucoup* de systèmes de représentants. Par exemple, l'ensemble V_0 formé des capitales des régions en est un. L'ensemble V_1 formé des villes les plus éloignées de la capitale dans leur région en est un autre.

2) Dans le cas de l'exemple $X = \mathbf{N} \times \mathbf{N}$ et de la relation R introduite ci-dessus on vérifie que $(x, y)R(x', y')$ si et seulement si l'une des deux conditions suivantes est remplie

- il existe $d \in \mathbf{N}$ tel que $x' = x + d$ et $y' = y + d$
- il existe $d \in \mathbf{N}$ tel que $x = x' + d$ et $y = y' + d$.

Ainsi, deux éléments appartiennent à une même classe d'équivalence si on peut passer de l'un à l'autre en ajoutant un même entier naturel aux deux coordonnées. Les classes sont donc des 'parties diagonales' du plan $\mathbf{N} \times \mathbf{N}$:

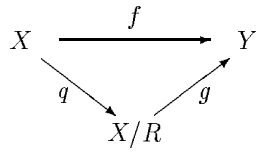


Il y a beaucoup de systèmes de représentants. Par exemple

$$X_0 = \{0\} \times \mathbf{N} \cup \mathbf{N} \times \{0\} = \{\ldots, (0,3), (0,2), (0,1), (0,0), (1,0), (2,0), \ldots\}$$

en est un. On définit l'ensemble $\mathbf{Z}_{ax}$ ($\mathbf{Z}$ axiomatique) comme étant l'ensemble quotient $(\mathbf{N} \times \mathbf{N})/R$.

Lemme 1.5 (Propriété universelle de X/R) *Soit X un ensemble, R une relations d'équivalence sur X et $f : X \to Y$ une application constante sur les classes d'équivalence par rapport à R (c'est-á-dire qu'on a $f(x) = f(x')$ à chaque fois que xRx'). Alors il existe une application $g : X/R \to Y$ et une seule telle que $f = g \circ q$. Réciproquement, toute application de la forme $g \circ q$ est constante sur les classes d'équivalence.*



Remarque 1.6 Le lemme signifie que la règle $g(\overline{x}) = f(x)$ définit une application $g : X/R \to Y$ si et seulement si on a $f(x) = f(x')$ quels que soient $x, x' \in X$ vérifiant xRx'.

Démonstration. On pose $g(\overline{x}) = f(x)$. Il s'agit de vérifier que $f(x)$ est indépendant du représantant x de la classe $\overline{x}$. Or si x' en est un autre, c'est-à-dire que $\overline{x} = \overline{x'}$, alors par définition, on a xRx' et donc $f(x) = f(x')$. $\surd$

Exemple 1.7 Il existe une application $g : \mathbf{Z}_{ax} \to \mathbf{Z}$ et une seule telle que $g(\overline{(x,y)}) = x - y$. En effet, si $(x,y)R(x',y')$ alors $x + y' = y + x'$ et donc $x - y = x' - y'$. L'application g est bijective : En effet, elle est surjective car si $n \in \mathbf{Z}$, on a $n = g(\overline{(n,0)})$ si $n \geq 0$ et $n = g(\overline{(0,-n)})$ si $n < 0$. Elle est injective car si on a $x - y = x' - y'$, alors $x + y' = x' + y$ c'est-à-dire que $(x,y)R(x',y')$ et que $\overline{(x,y)} = \overline{(x',y')}$.

Lemme 1.8 (Addition sur $\mathbf{Z}_{ax}$) *Il existe une application*

$$\mathbf{Z}_{ax} \times \mathbf{Z}_{ax} \to \mathbf{Z}_{ax}$$

et une seule telle que

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$

Démonstration. Il s'agit de montrer que $\overline{(a+c,b+d)} = \overline{(a'+c',b'+d')}$ si $(a,b)R(a',b')$ et $(c,d)R(c',d')$. Nous laissons au lecteur le soin de cette vérification. $\surd$

Définition 1.9 *Un* groupe *est un couple $(G, \star)$ formé d'un ensemble G et d'une application*

$$\star : G \times G \to G\ ,\ (g,h) \mapsto g \star h$$

appelée la loi *du groupe telle que*

a) la loi $\star$ est associative (i.e. on a $(x \star y) \star z = x \star (y \star z)$ quels que soient $x, y, z \in G$)

b) la loi $\star$ admet un élément neutre (i.e. il existe $e \in G$ tel que $x \star e = e \star x = x$ quel que soit $x \in G$)

c) tout élément x de G admet un inverse x' pour la loi $\star$ (i.e. on a $x \star x' = e = x' \star x$)

Un groupe $(G, \star)$ est commutatif *si on a $x \star y = y \star x$ quels que soient $x, y \in G$.*

Remarques 1.10

1) Si les conditons a) et b) sont vérifiées, alors l'élément neutre e est unique. En effet, soient e et e' deux éléments neutres. Alors on a $e = e \star e'$ (car e' est neutre) et $e \star e' = e'$ (car e est neutre) et donc $e = e'$.

2) Si les conditions a), b) et c) sont vérifiées, l'élément inverse x' de la conditon c) est unique. En effet, supposons que x' et x'' sont deux éléments inverses à x. Alors on a

$$x' = x' \star e = x' \star (x \star x'') = (x' \star x) \star x'' = e \star x'' = x''.$$

On note x^{-1} l'élement inverse de x.

(Non-)exemples 1.11

1) Le couple $(\mathbf{N}, +)$ vérifie a) et b) (pour $e = 0$) mais non pas c) car l'équation $n + n' = 0$ n'admet pas de solution $n' \in \mathbf{N}$ si $n > 0$.

2) Le couple $(\mathbf{Z}_{ax}, +)$ est un groupe. En effet, on vérifie facilement l'associativité. L'élément neutre est la classe de $(0, 0)$. L'inverse de la classe de (a, b) est la classe de (b, a) ! En effet, nous avons
$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, a + b)} = \overline{(0, 0)}.$$

Lemme 1.12 (Propriété universelle de $\mathbf{Z}_{ax}$) *Soit ι l'application*

$$\iota : \mathbf{N} \to \mathbf{Z}_{ax}\ ,\ n \to \overline{(n, 0)}.$$

On a $\iota(n + n') = \iota(n) + \iota(n')$ et si $\phi : \mathbf{N} \to G$ est une autre application de $\mathbf{N}$ vers un groupe G telle que $\phi(n + n') = \phi(n) \star \phi(n')$, alors il existe une application $\psi : \mathbf{Z}_{ax} \to G$ et une seule telle que a) $\psi \circ \iota = \phi$ et b) $\psi(x + x') = \psi(x) \star \psi(x')$ quels que soient $x, x' \in \mathbf{Z}_{ax}$.

Remarque 1.13 On peut interpréter ce lemme en disant que $\mathbf{Z}_{ax}$ (et donc $\mathbf{Z}$) est *le groupe universel contenant* $\mathbf{N}$.

Démonstration. Il est immédiat que ι est additive. Supposons donnée une application ϕ comme dans l'énoncé. Définissons $f : \mathbf{N} \times \mathbf{N} \to G$ par $f((a, b)) = \phi(a) \star \phi(b)^{-1}$. Montrons que f induit une application $\mathbf{Z}_{ax} \to G$, Supposons que $(a, b) R (a', b')$ et donc que $a + b' = b + a'$. Alors pour montrer que
$$\phi(a)\phi(b)^{-1} = \phi(a')\phi(b')^{-1}$$
il suffit de montrer que

$$\phi(a)\phi(b)^{-1}\phi(b)\phi(b') = \phi(a')\phi(b')^{-1}\phi(b)\phi(b').$$

En utilisant que $\phi(b)\phi(b') = \phi(b + b') = \phi(b')\phi(b)$ nous sommes ramenés à montrer que

$$\phi(a)\phi(b') = \phi(a')\phi(b)$$

ce qui est clair car $\phi(a)\phi(b') = \phi(a + b')$ et $\phi(a')\phi(b) = \phi(a' + b)$. Montrons l'unicité de ψ. En effet, si ψ et ψ' vérifient les hypothèses, nous avons

$$\psi(\overline{(n, 0)}) = \psi \circ \iota(n) = \phi(n) = \psi' \circ \iota(n) = \psi'(\overline{(n, 0)}).$$

En outre, si $x' = \overline{(0, n)}$, alors $\psi(x')$ et $\psi'(x')$ sont tous les deux inverses de $\psi(x) = \psi'(x)$ où $x = \overline{(n, 0)}$. Donc $\psi(x') = \psi'(x')$. Comme les $(0, n)$ et les $(n, 0)$, $n \in \mathbf{N}$, forment un système de représentants des classes d'équivalence par rapport à R, il s'ensuit que $\psi = \psi'$. $\surd$

2. La division euclidienne et ses conséquences

Lemme 2.1 (division euclidienne) *Soient $a \in \mathbf{Z}$ et $b \in \mathbf{Z} \setminus \{0\}$. Alors il existe $q \in \mathbf{Z}$ et $r \in \{0, 1, \ldots, |b| - 1\}$ tels que*

$$a = qb + r.$$

En outre, q et r sont uniques.

Exemples. On a $15 = 2 \times 7 + 1$ ce qui est une division euclidienne. On a aussi $-15 = (-2) \times 7 + (-1)$ ce qui *n'est pas* une division euclidienne, car le reste d'une division euclidienne est positif, par définition. Par contre, $-15 = (-3) \times 7 + 6$ est bien une division euclidienne.

Démonstration. On considère l'ensemble R formé des entiers $a - p\,b$, où $p \in \mathbf{Z}$. Puisque b est non nul, l'ensemble R contient des nombres positifs. Donc l'intersection $R \cap \mathbf{N}$ est non vide. Elle admet donc un élément minimal. Appelons r cet élément et définissons q par l'égalité $a - q\,b = r$. Montrons que $r < |b|$. Soit ε le signe de b ($\varepsilon = 1$ si $b > 0$ et $\varepsilon = -1$ si $b < 0$). Si nous avions $r > |b|$, nous pourrions enlever $\varepsilon\,b$ des deux côtés de l'égalité $a - q\,b = r$ pour trouver un nombre

$$r - \varepsilon\,b = a - (q + \varepsilon)b$$

qui appartiendrait encore a $R \cap \mathbf{N}$ mais qui serait strictement inférieur à r. Contradiction. On a donc bien $r \in \{0, 1, \ldots, |b| - 1\}$.

Montrons l'unicité. Si nous avons

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

alors $(q - q')\,b = r - r'$. Puisque r et r' sont positifs et strictement inférieurs à $|b|$, il s'ensuit que $|q - q'|\,|b| = |r - r'| < |b|$. Comme $|b| \neq 0$, nous avons $|q - q'| < 1$. Or, $|q - q'|$ est un entier positif et donc $|q - q'| = 0$ et $q = q'$. Par conséquent, nous avons aussi $r = a - q\,b = a - q'\,b = r'$. $\surd$

Définition 2.2 *Soit $(G, *)$ un groupe. Un* sous-groupe *de $(G, *)$ est une partie $H \subset G$ telle que*

a) L'élément neutre e de G appartient à H.

b) On a $h * h' \in H$ quels que soient $h, h' \in H$.

c) On a $h^{-1} \in H$ quel que soit $h \in H$.

Remarques 2.3

a) Si H est une sous-groupe de $(G, *)$, on définit une loi $*_H : H \times H \to H$ par

$$h *_H h' = h * h'.$$

Il est clair que $(H, *_H)$ est un groupe.

b) Quel que soit le groupe $(G, *)$, les parties G et $\{e\}$ sont toujours des sous-groupes.

c) Pour tout $n \in \mathbf{Z}$, la partie

$$n\mathbf{Z} = \{nx \mid x \in \mathbf{Z}\}$$

est un sous-groupe de $(\mathbf{Z}, +)$. D'après le théorème ci-dessus, on obtient ainsi *tous* les sous-groupes de $(\mathbf{Z}, +)$.

Théorème 2.4 *Tout sous-groupe H de $(\mathbf{Z}, +)$ est de la forme $H = n\mathbf{Z}$ pour un $n \in \mathbf{Z}$ unique au signe près.*

Démonstration. Si $H = \{0\}$, alors $H = 0\mathbf{Z}$ et il n'y a rien à démontrer. Supposons donc que $H \neq \{0\}$. Alors l'ensemble des normes $|x| > 0$ d'éléments de H est non-vide. Soit $n \in H$ tel que $|n|$ est non nul et minimal. Je dis que $H = n\mathbf{Z}$. En effet, puisque H est un sous-groupe qui contient n, il contient $n\mathbf{Z}$. Réciproquement, soit $a \in H$ et soit $a = qn + r$ la division euclidienne de a par n (rappelons que $n \neq 0$). Si on avait $r \neq 0$, alors $r = q - qn$

serait un élément de H non nul et de norme strictement inférieure à celle de n. Donc nous avons $r = 0$ et $a = qn$ appartient à $n\mathbf{Z}$.

Montrons l'unicité. En effet, si $n\mathbf{Z} = n'\mathbf{Z}$, nous avons $n = xn'$ pour un $x \in \mathbf{Z}$ et $n' = x'n$ pour un $x' \in \mathbf{Z}$. Donc $n = xx'n$. Nous avons soit $n = 0$, et alors $n\mathbf{Z} = \{0\}$ et $n' = 0$, soit $n \neq 0$ et alors $1 = xx'$ et donc $x = \pm 1$ et $n' = \pm n$. $\surd$

Remarque 2.5 Si H et H' sont deux sous-groupes de $(\mathbf{Z}, +)$, on pose

$$H + H' = \{x + x' \mid x \in H \text{ et } x' \in H'\}.$$

On vérifie aussitôt que $H + H'$ est encore un sous-groupe de $(\mathbf{Z}, +)$. D'après le théorème, si a et b sont deux entiers, il existe un entier c unique au signe près tel que

$$a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}.$$

Nous allons voir que c est en fait *le plus grand commun diviseur* de a et b.

Définition 2.6 *Soient $a, b \in \mathbf{Z}$. On dit que a est* divisible *par b s'il existe $q \in \mathbf{Z}$ tel que $a = q\,b$. Dans ce cas, on dit aussi que a est* multiple *de b, que b* divise *a ou que b est* diviseur *de a. On écrit $a|b$.*

Remarques 2.7

a) Le nombre 15 est divisible par $1, 3, 5, 15, -1, -3, -5$ et -15 !

b) Le nombre 0 est divisible par tout entier. Par contre le nombre 1 n'est divisible que par 1 et -1. En effet, si on a $1 = qb$, alors $1/|b|$ est un entier non nul et ≤ 1. Donc $b = \pm 1$.

c) Supposons $b \neq 0$. Alors la division euclidienne de a par b est bien définie et a est divisible par b ssi le reste de la division euclidienne de a par b s'annule.

Définition 2.8 *Soient $a, b \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$. Alors le module d'un diviseur commun à a et b est borné par* $\max(|a|, |b|)$ *et il existe donc un* plus grand diviseur commun *à a et b. On le note $PGCD\,(a, b)$. Les nombres a et b sont* premiers entre eux *si $PGCD\,(a, b) = 1$. Si $a = b = 0$, on pose $PGCD\,(a, b) = 0$.*

Lemme 2.9 (Bézout) *Soient $a, b \in \mathbf{Z}$. Alors*

$$a\,\mathbf{Z} + b\,\mathbf{Z} = PGCD\,(a, b)\,\mathbf{Z}.$$

En particulier, on a équivalence entre

i) Les entiers a et b sont premiers entre eux.

ii) On a $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$.

iii) L'équation $ax + by = 1$ admet une solution $(x, y) \in \mathbf{Z}^2$.

Remarques 2.10

a) L'équation $ax + by = 1$ est dite *équation de Bézout*. Si $(a, b) \neq (0, 0)$, elle admet toujours des solutions $(x, y) \in \mathbf{Q}^2$ mais pas nécessairement dans $\mathbf{Z}^2$.

b) Il s'ensuit du lemme que tout diviseur commun c de a et b divise $\mathrm{PGCD}\,(a, b)$ (car il divise $ax + by$ quels que soient $x, y \in \mathbf{Z}$).

Démonstration. Supposons que $a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}$ avec c positif. Comme $a \in c\mathbf{Z}$ et $b \in c\mathbf{Z}$, le nombre c est un diviseur commun de a et b. Donc $c \leq \mathrm{PGCD}\,(a, b)$. De l'autre côté, $\mathrm{PGCD}\,(a, b)$ divise a et b et donc tout élément de $a\mathbf{Z} + b\mathbf{Z}$. En particulier, $\mathrm{PGCD}\,(a, b)$ divise c. Il s'ensuit que $c = \mathrm{PGCD}\,(a, b)$.

Il est ainsi clair que i) est équivalent à ii). Il est aussi clair que i) implique iii). Réciproquement, si iii) est vérifié et $z \in \mathbf{Z}$, il suffit de multiplier l'équation $ax + by = 1$ par z pour conclure que $z = a(zx) + b(zy)$ appartient à $a\mathbf{Z} + b\mathbf{Z}$ et donc que $\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$. $\surd$

Lemme 2.11 (Gauss) *Soient $a, b, c \in \mathbf{Z}$. Si a divise bc et que a et b sont premiers entre eux, alors a divise c.*

Démonstration. D'après le lemme de Bézout, il existe $x, y \in \mathbf{Z}$ tels que $ax + by = 1$. Nous multiplions cette ǵalité par c pour obtenir

$$acx + bcy = c.$$

Puique a divise acx et bcy, il doit diviser $axc + bcy = c$. $\surd$

Définition 2.12 *Un nombre premier est un entier > 1 dont les seuls diviseurs positifs sont 1 et lui-même.*

Remarques 2.13

a) Le nombre 1 *n'est pas premier.*

b) Les nombres $2, 3, 5 \ldots$ sont premiers.

c) Un nombre premier est un entier positif qui admet exactement deux diviseurs positifs.

Lemme 2.14 (Euclide) *Soit p un nombre premier et $a, b \in \mathbf{Z}$. Si p divise ab alors p divise a ou p divise b.*

Démonstration. Si p ne divise pas a, alors a et p sont premiers entre eux, car les seuls diviseurs de p sont 1 et lui-même. D'après le lemme de Gauss, p doit alors diviser b. De même, si p ne divise pas b, il doit diviser a. $\surd$

Remarques 2.15

a) L'affirmation de ce lemme est *fausse* si on omet l'hypothèse que p est premier. Par exemple le nombre 3×5 divise le produit $(2 \times 3) \times (5 \times 7)$ mais il ne divise ni 2×3 ni 5×7.

b) Soient p et $p_1, \ldots, p_r$ des nombres premiers. Montrons que si p divise $p_1 \cdots p_r$, alors $p = p_i$ pour un i. En effet, si $r = 1$, il n'y a rien a démontrer. Si $r > 1$, et que p divise le produit $p_1 \times (p_2 \cdots p_r)$, alors d'après le lemme d'Euclide, p divise p_1 ou p divise $p_2 \cdots p_r$. Dans le premier cas, nous avons $p = p_1$ et dans le second $p = p_i$ pour un $i \geq 2$, d'après l'hypothèse de récurrence.

Théorème 2.16 (Décomposition en facteurs premiers) *Soit $n \geq 1$ un entier et soit $p_1, p_2 \ldots$ la liste des nombres premiers (exhaustive et sans répétitions). Alors il existe des entiers $m_i \in \mathbf{N}$ uniques et nuls sauf pour un nombre fini d'entre eux tels que*

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots.$$

Remarque 2.17 Comme presque tous les m_i sont nuls, presque tous les facteurs dans l'écriture $p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots$ valent un. Il s'agit donc en effet d'un produit avec un nombre *fini* de facteurs.

Démonstration. Montrons l'existence de l'écriture par un raisonnement récursif : Si $n = 1$, on pose $m_i = 0$ pour tous les i. Si $n > 1$ alors soit n est premier, soit $n = n'n''$ pour deux nombres strictement inférieurs à n. Dans le premier cas, il existe un nombre premier p_j dans la liste et un seul tel que $n = p_j$. On pose $m_i = 0$ pour $i \neq j$ et $m_j = 1$. Dans le second cas, l'hypothèse de récurrence nous donne les écritures

$$\begin{aligned} n' &= p_1^{m_1'} p_2^{m_2'} \cdots \\ n'' &= p_1^{m_1''} p_2^{m_2''} \cdots. \end{aligned}$$

En multipliant nous trouvons

$$n = p_1^{m_1'+m_1''} p_2^{m_2'+m_2''} \cdots .$$

Montrons l'unicité de l'écriture. Supposons donc que

$$n = p_1^{m_1} p_2^{m_2} \cdots = p_1^{m_1'} p_2^{m_2'} \cdots .$$

Montrons que $m_1 = m_1'$ (la démonstration pour les autres m_i est la même). Nous procédons par récurrence. Si $m_1 = 0$, alors p ne divise pas n (sinon il serait égal à l'un des p_i d'après la remarque ci-dessus). Donc $m_1' = 0$. Si $m_1 > 0$, alors p_1 divise n. D'après la remarque ci-dessus, p_1 doit apparaître dans l'écriture

$$n = p_1^{m_1'} p_2^{m_2'} \cdots .$$

Donc $m_1' > 0$. En divisant par p_1 nous trouvons

$$p_1^{m_1-1} p_2^{m_2} \cdots = p_1^{m_1'-1} p_2^{m_2'} \cdots .$$

et par l'hypothèse de récurrence, il s'ensuit que $m_1 - 1 = m_1' - 1$. Donc $m_1 = m_1'$. $\surd$

Remarques 2.18

a) Ce théorème a des conséquences étonnantes. Par exemple, d'après l'unicité, l'application

$$\mathbf{N} \times \mathbf{N} \times \mathbf{N} \to \mathbf{N} \ , \ (m_1, m_2, m_3) \mapsto 2^{m_1} \times 3^{m_2} \times 5^{m_3}$$

est injective ! Donc le cardinal de $\mathbf{N} \times \mathbf{N} \times \mathbf{N}$ est inférieur à celui de $\mathbf{N}$. (Bien sûr, on sait par ailleurs que ces deux cardinaux sont égaux).

b) Si nous avons

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots .$$

comme dans le théorème, alors les diviseurs positifs de n sont exactement les nombres

$$n' = p_1^{m_1'} p_2^{m_2'} p_3^{m_3'} \cdots$$

où $m_i' \leq m_i$ pour tout i. En effet, il est clair que ces nombres divisent n. Réciproquement supposons que $n = n'n''$ et que nous avons les décompositions

$$\begin{aligned} n' &= p_1^{m_1'} p_2^{m_2'} \cdots \\ n'' &= p_1^{m_1''} p_2^{m_2''} \cdots . \end{aligned}$$

En multipliant nous trouvons

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots = p_1^{m_1'+m_1''} p_2^{m_2'+m_2''} \cdots .$$

Par l'unicité, il s'ensuit que $m_i = m_i' + m_i''$ pour tout i. Donc on a bien $m_i \geq m_i'$.

c) Nous déduisons de b) que le nombre de diviseurs de n est égal à $(m_1 + 1)(m_2 + 1) \cdots$.

d) Supposons que nous avons les décompositions

$$\begin{aligned} n &= p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots \\ n' &= p_1^{m_1'} p_2^{m_2'} p_3^{m_3'} \cdots . \end{aligned}$$

Alors il s'ensuit de b), que nous avons

$$\begin{aligned} \mathrm{PGCD}\,(n, n') &= p_1^{\min(m_1, m_1')} p_2^{\min(m_2, m_2')} \cdots \\ \mathrm{PPCM}\,(n, n') &= p_1^{\max(m_1, m_1')} p_2^{\max(m_2, m_2')} \cdots \end{aligned}$$

où $\mathrm{PPCM}\,(n, n')$ désigne le plus petit commun multiple de n et n'. On en déduit que

$$n \times n' = \mathrm{PPCM}\,(n, n') \times \mathrm{PGCD}\,(n, n').$$

3. Congruences

Définition 3.1 *Soient $n \geq 1$ un entier et $a, b \in \mathbf{Z}$. On dit que a est congru à b modulo n s'il existe un $k \in \mathbf{Z}$ tel que $a = b + k\,n$. On écrit alors*

$$a \equiv b\ (n) \text{ ou } a \equiv_n b \text{ ou } a = b \bmod n.$$

Remarque 3.2 On a $a \equiv b\ (n)$ si et seulement si a et b ont le même reste dans la division euclidienne par n. En effet, si nous avons $a = qn + r$ et $b = q'n + r$, alors $a = b + (q - q')\,n$ et $a \equiv b\ (n)$. Réciproquement, si $a = q\,n + r$ et $b = q'\,n + r'$ et que $a = b + k\,n$, alors

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

et par l'unicité de la division euclidienne, il s'ensuit que $r = r'$ (et $q = q' + k$).

Exemple 3.3 Nous avons $6 \equiv -15\ (7)$ car $6 = -15 + 3 \times 7$. Notons que -15 a effectivement le même reste que 6 pour la division euclidienne par 7 car $-15 = (-3) \times 7 + 6$.

Lemme 3.4 *a) La relation $\equiv_n$ est une relation d'équivalence.*

b) Si $a \equiv a'\ (n)$ et $b \equiv b'\ (n)$, alors $a + b \equiv a' + b'\ (n)$ et $a\,b \equiv a'\,b'\ (n)$. Dans ce cas, on a aussi $a^m \equiv a'^m\ (n)$ pour tout $m \in \mathbf{N}$.

c) Les nombres $0, 1, \ldots, n-1$ forment un système de représentants des classes par rapport à $\equiv_n$.

Démonstration. a) La relation est réflexive car nous avons $a = a + 0 \times n$ pour tout $a \in \mathbf{Z}$. Elle est symétrique car si nous avons $a = b + k\,n$ alors nous avons $b = a + (-k)\,n$. Elle est transitive, car si nous avons $a = b + k\,n$ et $b = c + l\,n$, alors nous avons $a = (c + l\,n) + k\,n = c + (l + k)\,n$.

b) Supposons que $a = a' + k\,n$ et que $b = b' + l\,n$. Alors $a + b = a' + b' + (k + l)\,n$ et

$$a\,b = (a' + k\,n)(b' + l\,n) = a'\,b' + a'ln + knb' + klnn = a'\,b' + (a'l + kb' + kln)\,n.$$

La dernière affirmation s'ensuit par récurrence sur m.

c) Tout $a \in \mathbf{Z}$ est équivalent par $\equiv_n$ à un et un seul des nombres $0, 1, \ldots, n-1$. En effet, cette affirmation est une reformulation de l'existence et de l'unicité du reste dans la division euclidienne de a par n. $\surd$

Définition 3.5 *On pose*

$$\mathbf{Z}/n\mathbf{Z} \;=\; \mathbf{Z}/\equiv_n .$$

On note ${}^n\overline{a}$ ou $\overline{a}$ (ou même a) la classe de $a \in \mathbf{Z}$. Les éléments de $\mathbf{Z}/n\mathbf{Z}$ sont donc les $\overline{a}$, $a \in \mathbf{Z}$. On munit $\mathbf{Z}/n\mathbf{Z}$ des deux lois

$$\begin{aligned} + &: \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}, \qquad (\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a + b} \\ \cdot &: \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}, \qquad (\overline{a}, \overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b} \end{aligned}$$

Remarques 3.6

a) Grâce au lemme ci-dessus les deux lois sont bien définies.

b) Par définition de la notion de 'classe d'équivalence', nous avons

$${}^n\overline{a} = {}^n\overline{b} \text{ si et seulement si } a \equiv b\ (n).$$

Par conséquent, deux classes $\overline{a}$ et $\overline{b}$ sont égales ssi les restes de a et b par la division euclidienne par n sont égaux.

c) D'après le lemme ci-dessus, les classes

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}$$

sont distinctes deux à deux et toute classe est égale à une d'entre elles. Ces classes constituent donc la liste (exhaustive et sans répétitions) des éléments de $\mathbf{Z}/n\mathbf{Z}$. En particulier, $\mathbf{Z}/n\mathbf{Z}$ *est de cardinal* n.

4. Critères de divisibilité

Soit

$$N = 1001001001001001001001001.$$

Le nombre N est-il premier ? Non. Il est divisible par 3 car la somme de ses chiffres est divisible par 3. De façon générale, on sait qu'un nombre est divisible par 3 ssi la somme de ses chiffres l'est. De même pour 9 au lieu de 3. On sait aussi qu'un nombre est divisible par 11 ssi la somme alternée $c_0 - c_1 + c_2 - \ldots$ de ses chiffres l'est (c_0 est le chiffre des unités, c_1 celui des dizaines, ...). La divisibilité par 7, par contre, ne semble être reliée ni à la divisibilité par 7 de la somme ni à celle de la somme alternée de ses chiffres comme le montrent les exemples $7, 14, 21, \ldots$.

En fait, nous allons voir qu'un nombre est divisible par 7 si et seulement si c'est le cas pour le nombre

$$c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + 2c_8 - c_9 - 3c_{10} - \ldots$$

Par exemple, le nombre 100100100100 est divisible par 7. Plus généralement, tout nombre dont l'écriture décimale est 3-périodique et comporte un nombre de chiffres divisible par 6 est divisible par 7.

Ces faits trouvent leur explication à l'aide de deux outils : 1) le calcul des congruences et 2) le calcul des restes de puissances. Le lemme suivant élucide le rôle que joue le calcul des congruences :

Lemme 4.1 *Soit $n \geq 2$ un entier et $a_i, i \in \mathbf{N}$ une suite d'entiers telle que*

$$a_i \equiv 10^i \ (n) \ \textit{pour tout} \ i \in \mathbf{N}.$$

Soit $N \in \mathbf{N}$ et soient $c_0, c_1, \ldots, c_s \in \{0, \ldots, 9\}$ les chiffres de son écriture décimale (c_0=unités, ...). Alors nous avons

$$N \equiv \ a_0c_0 + a_1c_1 + a_2c_2 + \ldots + a_sc_s \ (n).$$

En particulier, N est divisible par n si et seulement si $a_0c_0 + a_1c_1 + \ldots + a_sc_s$ est divisible par n.

Démonstration. Par définition de l'écriture décimale, on a

$$N = c_0 + c_1 \times 10 + c_2 \times 10^2 + c_3 \times 10^3 + \cdots + c_s \times 10^s.$$

Puisque $10^i \equiv a_i \ (n)$, les règles du calcul des congruences nous permettent de conclure que

$$N \equiv \ c_0a_0 + c_1a_1 + c_2a_2 + c_3a_3 + \ldots + c_ra_r \ (n).$$

√

Exemple 4.2 Déduisons le critère de divisibilité par 7 que nous avons évoqué plus haut. Pour pouvoir appliquer le lemme, il nous faut calculer une suite d'entiers a_i tels que $a_i \equiv 10^i \ (7)$. La suite des a_i vérifie donc les congruences

$$\begin{aligned} a_0 &\equiv 1 \ (7) \\ a_{i+1} &\equiv 3\,a_i \ (7) \end{aligned}$$

(car $10 \equiv 3$ (7)). Pour $a_0, \dots a_6$, nous trouvons

$$1, 3, 2, -1, -3, -2, 1.$$

Donc $a_6 \equiv a_0$ (7) et par récurrence, on trouve que $a_i \equiv a_{i+6}$ (7) pour tout $i \in \mathbf{N}$. Pour la suite des a_i, on peut donc choisir la suite 6-périodique suivante

$$1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, \dots$$

D'après le lemme, il s'ensuit que N est divisible par 7 ssi c'est le cas pour le nombre

$$c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + 2c_8 - c_9 - 3c_{10} - \dots$$

où les c_i sont les chiffres de l'écriture décimale de N (c_0=unités, c_1=dizaines, ...).

5. Généralisation à d'autres systèmes de numération

Le fondement mathématique des systèmes de numération est le lemme suivant :

Lemme 5.1 *Soit $b \geq 2$ un entier. Pour tout entier $N \in \mathbf{N}$, il existe des entiers uniques $c_i \in \{0, \dots, b-1\}$, $i \in \mathbf{N}$, nuls sauf pour un nombre fini d'entre eux, tels que*

$$N = c_0 + c_1 b + c_2 b^2 + \dots + c_i b^i + \dots$$

Notation. Dans la situation du lemme, si $N \neq 0$ et que c_s est le dernier coefficient non nul, nous écrivons

$$N = [c_s, c_{s-1}, \dots, c_1, c_0]_b.$$

et nous appelons l'expression à droite *l'écriture de N en base b*. Il nous arrivera d'omettre les crochets et les virgules comme dans l'exemple suivant

$$1995_{10} = 11111001011_2 = 133023_8.$$

Dans les cas de $b = 2$, 8 et 16, on parle de l'écriture *binaire*, *octale* et *hexadécimale*, respectivement. Si b excède 10, les 'chiffres' de 10 à b sont représentés par les premières lettres de l'alphabet. Par exemple, les chiffres du système hexadécimal sont $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$. Ainsi on a

$$1995_{10} = 7CB_{16}.$$

Démonstration. On prouve d'abord l'existence par récurrence sur n. Pour $n = 0$ on pose $c_i = 0$ pour tout $i \in \mathbf{N}$. Supposons $n > 0$. Effectuons la division euclidienne par b

$$n = qb + r.$$

D'après l'hypothèse de récurrence, le nombre q s'écrit

$$q = c'_0 + c'_1 b + \dots + c'_t b^t$$

et donc

$$n = r + c'_0 b + c'_1 b^2 + \dots + c'_t b^{t+1}$$

On pose donc $c_0 = r$ et $c_i = c'_{i-1}$ pour $i > 0$. Montrons l'unicité. Si nous avons

$$n = c_0 + c_1 b + c_2 b^2 + \dots = d_0 + d_1 b + d_2 b^2 + \dots$$

alors $c_0 = d_0$ car les deux apparaissent comme le reste de la division euclidienne de n par b. Nous enlevons $c_0 = d_0$ des deux côtés et nous divions par b pour obtenir

$$(n - c_0)/b = c_1 + c_2 b + \dots = d_1 + d_2 b + \dots.$$

L'unicité s'ensuit par récurrence sur n. $\surd$

Lemme 5.2 *Soit $n \geq 2$ un entier et a_i, $i \in \mathbf{N}$, une suite d'entiers tels que*

$$b^i \equiv a_i \ (n).$$

Soit $N \in \mathbf{N}$ et c_i, $i \in \mathbf{N}$, les chiffres de son écriture en base b (c_0=unités, ...). Alors on a

$$N \equiv a_0 c_0 + a_1 c_1 + a_2 c_2 \cdots \ (n).$$

En particulier, N est divisible par n, si c'est le cas pour $a_0 c_0 + a_1 c_1 + a_2 c_2 \cdots$.

Démonstration. La démonstration est analogue à celle du cas $b = 10$. $\surd$

Exemples 5.3

a) Nous avons $8^i \equiv 1 \ (7)$. Donc un nombre est divisible par 7 ssi la somme des chiffres de son écriture octale est divisible par 7.

b) Nous avons $16^i \equiv (-1)^i \ (16)$. Donc un nombre est divisible par 17 ssi la somme alternée des chiffres de son écriture hexadécimale est divisible par 17.

6. L'algorithme d'Euclide-Bézout

Soient $a, b, c \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$. L'algorithme suivant sert à calculer le PGCD (a, b) et la solution générale $(x, y) \in \mathbf{Z}^2$ de l'équation de Bézout

$$a\,x + b\,y = c.$$

L'algorithme se présente sous forme d'un tableau. Dans une première étape on remplit les deux premières lignes comme indiquées dans le tableau ci-dessous. Le coefficient q_1 n'est pas défini; le coefficient q_2 est le quotient de la division euclidienne de a par b. Les lignes suivantes se calculent chacune en fonction des deux précédentes comme indiquée ci-dessous.

k	r_k	q_k	x_k	y_k	
1	a	$*$	1	0	
2	b	q_2	0	1	$a = q_2\,b + r_3$ est une div. eucl.
3	r_3	...	...	...	
$\vdots$					
$k-1$	r_{k-1}	q_{k-1}	x_{k-1}	y_{k-1}	
k	r_k	q_k	x_k	y_k	$r_{k-1} = q_k\,r_k + r_{k+1}$ est une div. eucl.
$k+1$	r_{k+1}	q_{k+1}	x_{k+1}	y_{k+1}	$x_{k+1} = x_{k-1} - q_k x_k$, $y_{k+1} = y_{k-1} - q_k y_k$
$\vdots$					
N	r_N	q_N	x_N	y_N	
$N+1$	$r_{N+1} = 0$	$*$	x_{N+1}	y_{N+1}	

La première colonne contient donc les restes des divisions euclidiennes successives, la deuxième colonne les quotients et les deux dernières colonnes des coefficients x_k, y_k tels que $a\,x_k + b\,y_k = r_k$ (voir la démonstration ci-dessous).

Les coefficients de la première colonne forment une suite strictement décroissante de nombres positifs entiers. Par définition, N est le plus petit entier avec $r_{N+1} = 0$.

Théorème. *On a $r_N = PGCD\,(a, b)$. Si $PGCD\,(a, b)$ divise c, la solution générale de l'équation*

$$ax + by = c$$

est donnée par

$$\begin{aligned} x &= \frac{c}{PGCD\,(a,b)} x_N + l x_{N+1} \\ y &= \frac{c}{PGCD\,(a,b)} y_N + l y_{N+1} \end{aligned}$$

où $l \in \mathbf{Z}$. Si PGCD(a,b) ne divise pas c, l'équation $ax+by=c$ n'admet pas de solution $(x,y) \in \mathbf{Z}^2$.

Exemple. Nous cherchons le PGCD $(198, 75)$ et toutes les solutions de l'équation $198x + 75y = \text{PGCD}\,(198, 75)$. Nous obtenons le tableau

k	r_k	q_k	x_k	y_k
1	198	$*$	1	0
2	75	2	0	1
3	48	1	1	-2
4	27	1	-1	3
5	21	1	2	-5
6	6	3	-3	8
7	3	2	11	-29
8	0	$*$	-25	66

Ainsi PGCD $(198, 75) = 3$ et la solution générale de l'équation $198x + 75y = 3$ est donnée par

$$\begin{aligned} x &= 11 - 25l \\ y &= -29 + 66l \end{aligned}$$

où $l \in \mathbf{Z}$.

Notons que $25 = 75/3$ et $66 = 198/3$. Notons aussi que les dernières deux colonnes sont des suites alternées et que les modules de x_k, y_k sont strictement croissants pour $k \geq 3$. En particulier, nous avons $0 \leq x_N < -(-25)$ et $-66 < y_N \leq 0$. La solution (x_N, y_N) est la seule avec ces propriétés. Les coefficients q_k apparaissent dans l'identité

$$\frac{198}{75} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}}} \quad .$$

Voir les exercices après la démonstration.

Démonstration. Notons d'abord que l'algorithme s'arrête. En effet, r_{k+1} est le reste d'une division euclidienne par r_k. Donc r_{k+1} est compris entre 0 et $r_k - 1$. Les r_k forment donc une suite strictement décroissante de nombres positifs entiers. Une telle suite doit aboutir à zéro après un nombre fini d'étapes.

Montrons que $r_N = \text{PGCD}\,(a, b)$. Montrons d'abord que nous avons

$$\text{PGCD}\,(r_{k-1}, r_k) = \text{PGCD}\,(r_k, r_{k+1}).$$

En effet, par construction, nous avons une équation

$$r_{k-1} = q_k r_k + r_{k+1}.$$

Elle montre que l'ensemble des diviseurs communs à r_{k-1} et r_k est égal à l'ensemble des diviseurs communs à r_k et r_{k+1}. En particulier, les plus grands éléments de ces ensembles sont égaux. La formule pour r_N s'ensuit par récurrence :

$$\begin{aligned} \text{PGCD}\,(a, b) &= \text{PGCD}\,(b, r_3) = \ldots \\ &= \text{PGCD}\,(r_{N-1}, r_N) = \text{PGCD}\,(r_N, r_{N+1}) = \text{PGCD}\,(r_N, 0) = r_N. \end{aligned}$$

Pour montrer la deuxième affirmation, nous introduisons les matrices

$$S_k = \begin{bmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{bmatrix}, \; k \geq 1.$$

Nous avons

$$S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ et } S_{k+1} = S_k \begin{bmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{bmatrix}.$$

Par récurrence, il s'ensuit que

$$[a \;\; b]S_k = [r_k \;\; r_{k+1}] \quad \text{et} \quad \det S_k = -(-1)^k.$$

En particulier, nous avons $[a \;\; b]S_N = [r_N \;\; 0]$ et la matrice

$$S_N^{-1} = -(-1)^N \begin{bmatrix} y_{N+1} & -x_{N+1} \\ -y_N & x_N \end{bmatrix}$$

est *à coefficients entiers*. Donc si nous posons

$$\begin{bmatrix} u \\ v \end{bmatrix} = S_N^{-1} \begin{bmatrix} x \\ y \end{bmatrix},$$

alors u, v sont des *entiers*. Nous avons

$$[a \;\; b] \begin{bmatrix} x \\ y \end{bmatrix} = [a \;\; b]S_N S_N^{-1} \begin{bmatrix} x \\ y \end{bmatrix} = [r_N \;\; 0] \begin{bmatrix} u \\ v \end{bmatrix}$$

de façon que l'équation

$$[a \;\; b] \begin{bmatrix} x \\ y \end{bmatrix} = c \quad (\text{resp. } ax + by = c)$$

est équivalente à l'équation

$$[r_N \;\; 0] \begin{bmatrix} u \\ v \end{bmatrix} = c \quad (\text{resp. } r_N u + 0\, v = c).$$

Or il est clair que cette dernière équation admet des solutions si et seulement si r_N divise c et que dans ce cas la solution générale est

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} c/r_N \\ l \end{bmatrix},$$

où $l \in \mathbf{Z}$. Donc l'équation $ax + by = c$ admet des solutions si et seulement si r_N divise c et dans ce cas la solution générale est

$$\begin{bmatrix} x \\ y \end{bmatrix} = S_N \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} x_N & x_{N+1} \\ y_N & y_{N+1} \end{bmatrix} \begin{bmatrix} c/r_N \\ l \end{bmatrix} = \begin{bmatrix} \frac{c}{r_N} x_N + l x_{N+1} \\ \frac{c}{r_N} y_N + l y_{N+1} \end{bmatrix}.$$

Exercices. 1) Trouver toutes les solutions $(x, y) \in \mathbf{Z}^2$ des équations suivantes : a) $5x + 3y = 2$, b) $4x + 9y = 1$, c) $17x + 68y = 3$, d) $20x + 30y = 0$, e) $1789x + 1994y = 1$ f) $1994x + 666y = 2$.

2) Avec les notations de l'algorithme d'Euclide-Bézout, montrer que

$$x_{N+1} = (-1)^N \frac{c}{\text{PGCD}\,(a, b)} \text{ et } y_{N+1} = -(-1)^N \frac{a}{\text{PGCD}\,(a, b)}.$$

Indication : On pourra utiliser l'identité

$$\begin{bmatrix} a & b \\ -y_N & x_N \end{bmatrix} S_N = \begin{bmatrix} r_N & 0 \\ 0 & -(-1)^N \end{bmatrix}.$$

3) Supposons $a > b > 0$. Avec les notations de l'algorithme d'Euclide-Bézout, montrer que

$$\frac{a}{b} = q_2 + \frac{r_3}{b} = q_2 + \frac{1}{q_3 + \frac{r_4}{r_3}} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{r_5}{r_4}}} = \dots$$

4) Nous allons caractériser la solution (x_N, y_N) fournie par l'algorithme d'Euclide-Bézout parmi toutes les solutions de l'équation de Bézout. Supposons, pour simplifier, que $a > b > 0$ et que $\mathrm{PGCD}\,(a, b) = 1$.

a) Montrer qu'il existe une solution $(x_+, y_+) \in \mathbf{Z}^2$ de $ax + by = 1$ et une seule telle que $0 \leq x_+ < b$. Montrer qu'on a $-a < y_+ \leq 0$.

b) Montrer qu'il existe une solution $(x_-, y_-) \in \mathbf{Z}^2$ de $ax + by = 1$ et une seule telle que $-b < x_- \leq 0$. Montrer qu'on a $0 \leq y_+ < a$.

c) Montrer qu'on a $(x_N, y_N) = (x_+, y_+)$ si N est impair et $(x_N, y_N) = (x_-, y_-)$ si N est pair. Indication : on pourra commencer par montrer que les suites $-(-1)^k x_k$ et $(-1)^k y_k$ sont strictement croissantes pour $k \geq 3$.

5) Nous allons estimer le nombre d'étapes de l'algorithme d'Euclide-Bézout. Pour un couple d'entiers (a, b) avec $a > b \geq 0$ notons $N(a, b)$ le nombre N apparaissant comme nombre d'étapes de l'algorithme d'Euclide-Bézout appliqué à (a, b).

a) Montrer que $N(a, b) \leq 1 + \log_2 a$.

b) Soit $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour tout $n > 1$. Par définition, le nombre F_n est le *n-ième nombre de Fibonacci*. Montrer que $N(F_n, F_{n-1}) = n$, que $N(a, b) \leq n$ si $a \leq F_n$ et que l'égalité ne se présente que pour $a = F_n$ et $b = F_{n-1}$.

7. Une autre approche de l'équation de Bézout

Soient $a, b, c \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$. *L'équation de Bézout* est l'équation

$$ax + by = c$$

où x, y désignent deux entiers relatifs. Si $c \neq 0$ on dit qu'il s'agit d'une *équation inhomogène d'inhomogénéité* c. Dans ce cas, l'équation *homogène* associée est l'équation

$$ax + by = 0.$$

Notons $d = \mathrm{PGCD}\,(a, b)$.

Théorème 7.1 *a) La solution générale de l'équation homogène $ax + by = 0$ est donnée par*

$$\begin{array}{rcl} x_h & = & l\,\frac{b}{d} \\ y_h & = & -l\,\frac{a}{d} \end{array} \quad l \in \mathbf{Z}.$$

b) Si d divise c et que (x_p, y_p) est une solution (dite "particulière") de l'équation inhomogène $ax + by = c$, alors la solution générale de l'équation inhomogène est donnée par

$$\begin{array}{rcl} x & = & x_p + l\,\frac{b}{d} \\ y & = & y_p - l\,\frac{a}{d} \end{array}$$

Remarque 7.2 La construction de la solution générale de l'équation de Bézout se fait donc suivant le même schéma que la construction de la solution d'une équation différentielle linéaire :

sol. gén. de l'éq. inhomogène = sol. part. de l'éq. inhomogène+sol. gén. de l'éq. homogène.

Démonstration. a) Regardons d'abord le cas où $b = 0$. Alors l'équation se réduit à $ax + 0\ y = 0$ où $a \neq 0$ (car $(a, b) \neq (0, 0)$). Clairement la solution générale est donnée par $x = 0$, $y = l$, $l \in \mathbf{Z}$. De l'autre côté, on a $d = |a|$, donc $a/d = \pm 1$ et $b/d = 0$. L'affirmation est donc vraie dans ce cas.

Supposons maintenant $b \neq 0$. L'équation $ax + by = 0$ équivaut à

$$\frac{a}{d}\ x = -\frac{b}{d}\ y.$$

Notons que les deux fractions qui apparaissent ici sont en fait des entiers, car $d = \mathrm{PGCD}\,(a, b)$ divise a et b. Cette dernière équation montre que b/d divise le produit $x\ a/d$. Or, nous avons $\mathrm{PGCD}\,(a/d, b/d) = 1$. Par le lemme de Gauss, il s'ensuit que b/d divise x. Donc il existe un $l \in \mathbf{Z}$ tel que $x = l\ b/d$. Nous avons donc

$$\frac{a}{d}\ l\ \frac{b}{d} = -\frac{b}{d}\ y.$$

Puisque $b \neq 0$, nous pouvons conclure que $y = -l\ a/d$.

b) Supposons que $(x, y) \in \mathbf{Z}^2$ est une solution de l'équation inhomogène. Si nous formons la différence des deux équations

$$\begin{aligned} ax + by &= c \\ ax_p + by_p &= c \end{aligned}$$

nous trouvons

$$a(x - x_p) + b(y - y_p) = 0$$

c'est-à-dire que $(x - x_p, y - y_p)$ est une solution de l'équation homogène. D'après a), il existe donc un $l \in \mathbf{Z}$ tel que

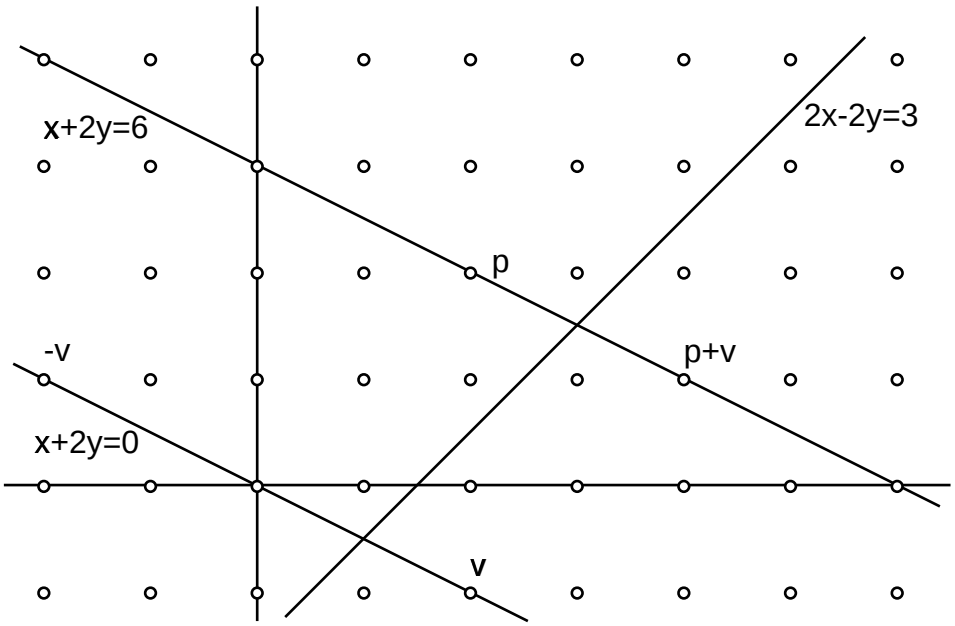
$$\begin{aligned} x - x_p &= l\ \frac{b}{d} \\ y - y_p &= -l\ \frac{a}{d} \end{aligned}$$

L'affirmation en résulte. $\surd$

8. Interprétation géométrique

Nous considérons le plan $\mathbf{R}^2$ et nous appelons *points entiers* les points $(x, y) \in \mathbf{R}^2$ à coordonnées entières $x, y \in \mathbf{Z}$. Soient $a, b, c \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$. Notons $D = D(a, b, c)$ la droite dans $\mathbf{R}^2$ formée des points $(\xi, \eta) \in \mathbf{R}^2$ tels que $a\xi + b\eta = c$. Alors *l'ensemble des solutions* $(x, y) \in \mathbf{Z}^2$ *de l'équation de Bézout* $ax + by = c$ *s'identifie à l'ensemble des points*

entiers de la droite D.



D'après les théorèmes cités ci-dessus, deux cas seulement sont possibles

- soit la droite D ne contient aucun point entier
- soit la droite D contient une infinité de points entiers.

Dans le deuxième cas, l'ensemble des points entiers est obtenu en rajoutant un multiple entier d'un vecteur $v = (x_h, y_h)$ à un point entier $p = (x_p, y_p)$ fixé de la droite. Le vecteur (x_h, y_h) peut être identifié avec un point entier de distance minimale à l'origine sur la droite $D(a, b, 0)$. Notons que cette droite contient exactement deux tels points (à savoir v et $-v$).

9. Le lemme chinois en termes de congruences

Lemme 9.1 (lemme chinois) *Soient $n_1, n_2 \geq 2$ deux entiers premiers entre eux et $u_1 n_1 + u_2 n_2 = 1$ une équation de Bézout. Soient $a_1, a_2 \in \mathbf{Z}$ et $a \in \mathbf{Z}$ tel que $a \equiv a_1 u_2 n_2 + a_1 u_1 n_1 (n_1 n_2)$. Alors pour $x \in \mathbf{Z}$ on a l'équivalence*

$$\left.\begin{array}{rcl} x & \equiv & a_1 \ (n_1) \\ x & \equiv & a_2 \ (n_2) \end{array}\right\} \iff x \equiv a \ (n_1 n_2).$$

Remarque 9.2 On peut réinterpréter le lemme en disant que la solution générale $x \in \mathbf{Z}$ du système de congruences à gauche est donnée par

$$x = a + k n_1 n_2 \ , \ k \in \mathbf{Z}.$$

Démonstration. Vérifions d'abord que a est bien une solution du système de congruences. En effet, d'après l'hypothèse, nous avons

$$a = a_1 u_2 n_2 + a_2 u_1 n_1 + k n_1 n_2$$

pour un $k \in \mathbf{Z}$ et donc

$$a \equiv a_1 u_2 n_2 \equiv a_1 (u_2 n_2 + u_1 n_1) \equiv a_1 \ (n_1)$$

et de même

$$a \equiv a_2 u_1 n_1 \equiv a_2(u_1 n_1 + u_2 n_2) \equiv a_2 \ (n_2).$$

Montrons maintenant l'équivalence. Supposons que $x \equiv a \ (n_1 n_2)$. Alors $x = a + k n_1 n_2$ pour un $k \in \mathbf{Z}$ et donc $x \equiv a \equiv a_1 \ (n_1)$ et $x \equiv a \equiv a_2 \ (n_2)$. Réciproquement, supposons que x vérifie $x \equiv a_1 \ (n_1)$ et $x \equiv a_2 \ (n_2)$. Alors nous avons $(x - a) \equiv 0 \ (n_1)$ et $(x - a) \equiv 0 \ (n_2)$. Donc $x - a$ est divisible par n_1 et par n_2. Puisque les deux sont premiers entre eux, il s'ensuit (lemme de Gauss) que $x - a$ est divisible par $n_1 n_2$, c'est-à-dire que $x \equiv a \ (n_1 n_2)$. $\surd$

Exemple 9.3 Considérons le système

$$\begin{aligned} x &\equiv 1 \ (17) \\ x &\equiv 2 \ (28) \\ x &\equiv 3 \ (31) \end{aligned}$$

Nous avons l'équation de Bézout $5 \times 17 - 3 \times 28 = 1$. Le système formé des deux premières équations est donc équivalent à la congruence $x \equiv a \ (17 \times 28)$ où $a = 1 \times (-3 \times 28) + 2 \times (5 \times 17) = 86$. Le système des trois équations se réduit donc à

$$\begin{aligned} x &\equiv 86 \ (476) \\ x &\equiv 3 \ (31). \end{aligned}$$

Nous avons l'équation de Bézout $(-14) \times 476 + 215 \times 31 = 1$. Donc le système est équivalent à la congruence $x \equiv b \ (476 \times 31)$ où $b = 86 \times (215 \times 31) + 3 \times (-14 \times 476) = 553198$. Si nous réduisons b modulo $476 \times 31 = 14756$, nous trouvons que le système des trois équations est équivalent à la congruence

$$x \equiv 7226 \ (14756);$$

Nous invitons le lecteur à vérifier que 7226 donne les restes 1, 2 et 3 dans la division par 17, 28 et 31.

10. Systèmes de congruences

Soient r et $n_1, \ldots, n_r$ des entiers ≥ 2 et $a_1, \ldots, a_r$ des entiers quelconques. Considérons le système

$$\begin{aligned} x &\equiv a_1 \ (n_1) \\ x &\equiv a_2 \ (n_2) \\ &\vdots \\ x &\equiv a_r \ (n_r). \end{aligned}$$

Supposons que $x = a$ et $x = a'$ sont deux solutions. Alors la différence $a - a'$ est divisible par tous les n_i et donc par leur plus petit commun multiple $n = \mathrm{PPCM}\,(n_1, \ldots, n_r)$. Donc *s'il existe une solution*, sa classe modulo n est unique.

Il peut ne pas exister de solution comme le montre l'exemple du système

$$\begin{aligned} x &\equiv 1 \ (6) \\ x &\equiv 2 \ (8) \end{aligned}$$

ou encore celui du système

$$\begin{aligned} x &\equiv 1 \ (2) \\ x &\equiv 0 \ (2). \end{aligned}$$

Notons que nous n'avons pas exclu ce genre de contradictions banales.

L'application systématique du lemme chinois nous permettra de réduire tout système de congruences soit à un système contradictoire soit à une seule congruence modulo le plus petit commun multiple des modules. Nous ne développons pas ici la méthode dans le cas général mais nous limitons à la décrire dans un exemple simple.

Considérons le système

$$\begin{aligned} x &\equiv 3\ (18) \\ x &\equiv c\ (12). \end{aligned}$$

Il s'agit de déterminer tous les entiers c pour lesquels le sytème admet des solutions et de calculer les solutions dans ce cas. Constatons tout d'abord que les nombres 18 et 12 ne sont pas premiers entre eux de façon que le lemme chinois ne s'applique pas immédiatement. Pour résoudre le problème, nous allons dans une première étape *augmenter* le nombre d'équations pour obtenir des modules qui sont des puissances de nombres premiers. Nous avons ainsi $18 = 2 \times 3^2$ et d'après le lemme chinois la première congruence est équivalente au système

$$\begin{aligned} x &\equiv 1\ (2) \\ x &\equiv 3\ (9). \end{aligned}$$

De même, puisque nous avons $12 = 3 \times 4$, la seconde congruence est équivalente au système

$$\begin{aligned} x &\equiv c\ (3) \\ x &\equiv c\ (4). \end{aligned}$$

Nous avons ainsi trouvé un système de quatre congruences qui est équivalent au système de départ. Nous le réécrivons dans un ordre où les puissances de chaque nombre premier sont regroupées ensemble et les puissances les plus élevées apparaissent en premier lieu :

$$\begin{aligned} x &\equiv c\ (4) && (1) \\ x &\equiv 1\ (2) && (2) \\ x &\equiv 3\ (9) && (3) \\ x &\equiv c\ (3) && (4) \end{aligned}$$

Rappelons-nous que si nous avons $a \equiv b\ (n)$ alors nous avons aussi $a \equiv b\ (d)$ pour tout diviseur d de n (en effet, si $n = q\,d$ et $a = b + k\,n$ alors $a = b + (k\,q)\,d$). L'équation (1) implique donc que $x \equiv c\ (2)$ de façon que les équations (1) et (2) sont contradictoires sauf si $c \equiv 1\ (2)$. De même, les équations (3) et (4) sont contradictoires sauf si $c \equiv 0\ (3)$. Nous avons donc les conditions

$$\begin{aligned} c &\equiv 1\ (2) \\ c &\equiv 0\ (3) \end{aligned}$$

qui sont nécessaires pour qu'une solution existe. Réciproquement, ces conditions sont aussi suffisantes car si elles sont vérifiées, la congruence (2) est une conséquence de (1), et (4) est une conséquence de (3) de façon que le système tout entier est équivalent à un système de deux congruences

$$\begin{aligned} x &\equiv c\ (4) \\ x &\equiv 3\ (9) \end{aligned}$$

Nous avons l'équation de Bézout $-2 \times 4 + 9 = 1$. Donc, d'après le lemme chinois, ce système est équivalent à la congruence $x \equiv c \times 9 + 3 \times (-8)\ (36)$ ou encore $x \equiv 3c + 12\ (36)$. En conclusion, *le système de départ admet une solution si et seulement si* $c \equiv 3\ (6)$ *et dans ce cas l'ensemble des solutions est l'ensemble des entiers* x *tels que* $x \equiv 3c + 12\ (36)$.

11. Classes de congruence inversibles

Définition 11.1 *Soit $n \geq 2$ un entier. Une classe de congruence $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ est* inversible *s'il existe une classe $\overline{b}$ telle que $\overline{a}\overline{b} = \overline{1}$. On note $(\mathbf{Z}/n\mathbf{Z})^*$ l'ensemble des classes inversibles.*

Lemme 11.2 *Muni de la multiplication naturelle, l'ensemble des classes inversibles est un groupe d'élément neutre $\overline{1}$.*

Remarque 11.3 Le lemme implique que si la classe $\overline{a}$ est inversible, alors la classe $\overline{b}$ telle que $\overline{a}\overline{b} = \overline{1}$ est unique. On l'appelle la *classe inverse de $\overline{a}$.*

Démonstration. Il s'agit d'abord de vérifier que la loi de multiplication est bien définie, c'est-à-dire que le produit de deux classes inversibles est encore inversible. En effet, si $\overline{a}\overline{b} = \overline{1}$ et $\overline{a'b'} = \overline{1}$, alors $(\overline{a}\overline{a'})(\overline{b'b}) = \overline{1}$. La loi est associative car la multiplication de $\mathbf{Z}/n\mathbf{Z}$ est associative. Elle admet l'élément $\overline{1}$ pour élément neutre. Finalement, par définition, tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ admet un inverse. $\surd$

Lemme 11.4 *Une classe $\overline{a}$ est inversible ssi a et n sont premiers entre eux.*

Démonstration. En effet, la classe a est inversible, ssi l'équation $ab = 1 + kn$ admet des solutions $b, k \in \mathbf{Z}$. Or cette équation est une variante de l'équation de Bézout $ab + (-n)k = 1$ aux inconnues b, k. L'affirmation en résulte. $\surd$

Lemme 11.5 *Supposons que la classe $\overline{x}$ est inversible. Alors la congruence $a \equiv b\ (n)$ est équivalente à $ax \equiv bx\ (n)$.*

Remarque 11.6 L'affirmation du lemme est fausse si la classe $\overline{x}$ n'est pas inversible.

Démonstration. Supposons que $\overline{xy} = \overline{1}$. Alors $xy \equiv 1\ (n)$ et donc la congruence $axy \equiv bxy\ (n)$ implique $a \equiv b\ (n)$. $\surd$

12. Anneaux, groupes et lemme chinois

Définition 12.1 *Un* anneau *est un triplet $(A, +, \cdot)$ formé d'un ensemble A et deux deux applications*

$$+ : A \times A \to A\ ,\ (a, b) \mapsto a + b \quad \text{et} \quad \cdot : A \times A \to A\ ,\ (a, b) \mapsto ab$$

appelées l'addition *et la* multiplication *de A et qui vérifient les axiomes suivants*

(1) Le couple $(A, +)$ est un groupe commutatif. On note 0_A ou 0 son élément neutre.

(2) La multiplication $\cdot$ est associative et admet un élément neutre noté 1_A ou 1.

(3) L'addition et la multiplication vérifient les règles de distributivité

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}$$

quels que soient a, b, c éléments de A.

Un anneau est commutatif *si sa multiplication est commutative.*

Exemples. Les ensembles $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ munis de leurs opérations d'addition et de multiplication habituelles sont des anneaux commutatifs. L'anneau $M_2(\mathbf{R})$ des matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

avec l'addition et la multiplication des matrices est un anneau non-commutatif. En effet, si on pose

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \ , \ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

on a $AB \neq BA$.

Définition 12.2 *Soit $A = (A, +, \cdot)$ un anneau. Un élément $a \in A$ est* inversible *s'il existe un élément $b \in A$ tel que $ab = 1_A = ba$. On note A^* l'ensemble des éléments inversibles de A. L'anneau A est un* corps *si $A^* = A \setminus \{0\}$, c'est-à-dire que tout élément non nul de A est inversible (et que $A \neq \{0_A\}$).*

Exemples. Pour le cas de l'anneau $A = \mathbf{Z}/n\mathbf{Z}$, cette définition est celle de la section précédente. Les anneaux $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont des corps.

L'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier. Soit p un nombre premier. Alors $(\mathbf{Z}/p\mathbf{Z})^*$ est formé des $p-1$ classes $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. Soit n un entier ≥ 1. Alors $(\mathbf{Z}/p^n\mathbf{Z})$ est le *complémentaire* dans $\mathbf{Z}/p^n\mathbf{Z}$ des p^{n-1} classes $\overline{p}, \overline{2p}, \ldots, \overline{(p^{n-1}-1)p}$. Donc

$$|(\mathbf{Z}/p\mathbf{Z})^*| = p - 1 \text{ et } |(\mathbf{Z}/p^n\mathbf{Z})^*| = p^n - p^{n-1} = p^{n-1}(p-1).$$

Remarque 12.3 Si l'élément 0_A est inversible dans l'anneau A, alors nous avons $0_A = 1_A$ et $A = \{0_A\} = \{1_A\}$. En effet, supposons que $0\ b = 1$. Nous affirmons que $0b = 0$; en effet, il suffit de rajouter $-0\ b$ des deux côtés de léquation $0\ b = (0+0)\ b = 0\ b + 0\ b$.

Lemme 12.4 *Soit $A = (A, +, \cdot)$ un anneau. Alors si deux éléments sont inversibles, leur produit l'est encore. L'ensemble A^* muni de la multiplication déduite de celle de A est un groupe d'élément neutre 1_A.*

Remarque 12.5 Il s'ensuit que l'inverse d'un élément inversible d'un anneau est unique (car l'inverse d'un élément d'un groupe est unique).

Démonstration. Supposons que a et b sont inversibles et que $aa' = 1 = a'a$ et $bb' = 1 = b'b$. Alors nous avons $(ab)(b'a') = 1 = (b'a')(ab)$ de façon que ab est inversible. L'associativité de la multiplication est conséquence de la même propriété pour la multiplication dans un anneau et de même l'existence d'un élément neutre. L'existence des inverses résulte de la définition de A^*. $\surd$

Lemme-Définition 12.6 *Soient $(A_1, +, \cdot)$ et $(A_2, +, \cdot)$ deux anneaux. L'ensemble $A_1 \times A_2$ muni des lois définies par*

$$(a_1, a_2) + (a_1', a_2') = (a_1 + a_1', a_2' + a_2')$$
$$(a_1, a_2) \cdot (a_1', a_2') = (a_1 a_1', a_2 a_2')$$

est un anneau appelé l'anneau produit *de A_1 par A_2. L'élément neutre pour l'addition de $A_1 \times A_2$ est le couple $(0,0)$ et celui pour la multiplication le couple $(1,1)$.*

Remarque 12.7 En appliquant plusieurs fois ce résultat nous obtenons un grand nombre de nouveaux exemples d'anneaux. Par exemple, tous les anneaux suivants sont de cardinal 24

$$\mathbf{Z}/24\mathbf{Z} \ , \ \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z} \ , \ \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \ , \ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

Nous allons voir que certains de ces anneaux sont "isomorphes", c'est-à-dire qu'ils ne se distinguent pas de façon essentielle.

Démonstration. Il s'agit de vérifier les trois groupes d'axiomes pour les lois définies sur $A_1 \times A_2$. A titre d'exemple, vérifions que la multiplication est associative. En effet, en

utilisant la définition de la multiplication sur $A_1 \times A_2$ et l'accociativité de la multiplication dans A_1 et A_2, nous avons

$$\begin{aligned}((a_1,a_2)\cdot(a_1',a_2'))\cdot(a_1'',a_2'') &= (a_1a_1',a_2a_2')\cdot(a_1'',a_2'') = ((a_1a_1')a_1'',(a_2a_2')a_2'')\\ &= (a_1(a_1'a_1''),a_2(a_2'a_2'')) = (a_1,a_2)\cdot(a_1'a_1'',a_2'a_2'')\\ &= (a_1,a_2)\cdot((a_1',a_2')\cdot(a_1'',a_2'')).\end{aligned}$$

Nous laissons au lecteur le soin d'écrire les démonstrations des autres propriétés. $\surd$

Lemme-Définition 12.8 *Soient $(G_1,\star)$ et $(G_2,\star)$ deux groupes. L'ensemble $G_1\times G_2$ muni de la loi*

$$(g_1,g_2)\star(g_1',g_2') = (g_1\star g_1', g_2g_2')$$

est un groupe d'élément neutre le couple (e,e).

Démonstration. La démonstration est analogue à celle du lemme-définition précédent. $\surd$

Lemme 12.9 *Soient $(A_1,+,\cdot)$ et $(A_2,+,\cdot)$ deux anneaux. Alors nous avons l'égalité*

$$(A_1\times A_2)^\star = A_1^\star\times A_2^\star.$$

En outre la loi de groupe sur $(A_1\times A_2)^\star$ est celle du groupe produit $A_1^\star\times A_2^\star$.

Démonstration. Soit (a_1,a_2) un couple d'éléments inversibles. Soient a_1' et a_2' les inverses de a_1 et a_2. Alors nous avons

$$(a_1',a_2')\cdot(a_1,a_2) = (1,1) = (a_1,a_2)\cdot(a_1',a_2')$$

ce qui signifie que (a_1,a_2) est inversible dans $A_1\times A_2$ d'inverse (a_1',a_2'). Ainsi l'ensemble $A_1^\star\times A_2^\star$ est inclus dans $(A_1\times A_2)^\star$. Réciproquement, soit (a_1,a_2) un élément inversible de $A_1\times A_2$ et soit (a_1',a_2') son inverse. Alors on vérifie aussitôt que a_1' est inverse à a_1 dans A_1 et que a_2' est inverse à a_2 dans A_2. La dernière affirmation est une conséquence immédiate des définitions. $\surd$

Définition 12.10 *Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux. Une application $f:A\to B$ est un* homomorphisme d'anneaux *si elle vérifie*

$$\begin{aligned}f(a+a') &= f(a)+f(a')\\ f(a\cdot a') &= f(a)\cdot f(a')\\ f(1_A) &= 1_B\end{aligned}$$

quels que soient $a,a'\in A$. C'est un isomorphisme d'anneaux *si en plus, elle est bijective. Les anneaux A et B sont* isomorphes *s'il existe un isomorphisme de A vers B.*

Exemple 12.11 Soient A_1 et A_2 deux anneaux. Considérons l'application

$$f: A_1\times A_2\to A_2\times A_1\ ,\ (a_1,a_2)\mapsto(a_2,a_2).$$

Alors on vérifie que f est un isomorphisme.

Lemme 12.12 *Soient A et B deux anneaux et $f:A\to B$ un isomorphisme. Soit $g:B\to A$ l'application réciproque de f. Alors g est un homomorphisme et même un isomorphisme.*

Démonstration. En effet, soient b, b' des éléments de B. Pour vérifier qu'on a égalité entre $g(b\,b')$ et $g(b)\,g(b')$ il suffit de voir que les images par f de ces deux éléments coïncident. Or nous avons

$$f(g(b\,b')) = b\,b' = f(g(b))\,f(g(b')) = f(g(b)\,g(b')).$$

De même on vérifie que $g(b+b') = g(b) + g(b')$. Finalement, l'égalité $f(1_A) = 1_B$ entraîne que $1_A = g(1_B)$. $\surd$

Définition 12.13 *Soit G et H deux groupes. Une application $f : G \to H$ est un* homomorhisme de groupes *si elle vérifie*

$$f(g_1 \star g_2) = f(g_1) \star f(g_2)$$

quels que soient $g_1, g_2 \in G$. C'est un isomorphisme *si en plus elle est bijective. Les groupes G et H sont* isomorphes *s'il existe un isomorphisme de G vers H.*

Remarques 12.14

a) On peut s'étonner de ne pas trouver l'axiome $f(e_G) = f(e_H)$ dans cette définition. Or cet axiome est une *conséquence* de la définition. En effet, nous avons

$$f(e_G) = f(e_G \star e_G) = f(e_G) \star f(e_G).$$

Si nous multiplions cette égalité des deux côtés à gauche par l'inverse de $f(e_G)$ dans H, nous trouvons $e_H = f(e_G)$. Notons que cette démonstration utilise l'existence des inverses et qu'elle n'a donc pas d'analogue pour les lois de multiplication des anneaux.

b) Si $f : G \to H$ est un isomorphisme de groupes et que $g : H \to G$ est l'application réciproque à f, alors g est un homomorphisme de groupes et même un isomorphisme. Nous laissons au lecteur le soin d'adapter au cadre des groupes la démonstration donnée ci-dessus pour les anneaux.

Lemme 12.15 *Soient A et B deux anneaux et $f : A \to B$ un homomorphime d'anneaux. Alors nous avons $f(A^\star) \subset B^\star$ et l'application*

$$f^\star : A^\star \to B^\star, a \mapsto f(a)$$

est un homomorphisme de groupes. C'est un isomorphisme de groupes si f est un isomorphisme d'anneaux.

Démonstration. Supposons que $a \in A$ est inversible d'inverse a'. Alors $f(a')$ est inverse à $f(a)$. En effet, nous avons

$$f(a)f(a') = f(aa') = f(1_A) = 1_B = f(a')f(a).$$

Ainsi, l'application f nous fournit bien une application entre les groupes des éléments inversibles

$$f^\star : A^\star \to B^\star\ ,\ a \mapsto f(a).$$

Il est immédiat de constater que cette application est un homomorphisme de groupes. Supposons maintenant que f est un isomorphisme d'anneaux et soit $g : B \to A$ son application réciproque. Alors g est un homomorphisme et donc $g(B^\star)$ est contenu dans $A^\star$. Ceci montre que $a \in A$ est inversible si et seulement si $f(a)$ est inversible dans B. Donc dans ce cas f^* est bijective et c'est donc un isomorphisme de groupes. $\surd$

Lemme 12.16 (Lemme chinois en termes d'anneaux résiduels) *Soient r et s deux entiers ≥ 2 et premiers entre eux. Alors l'application*

$$\Phi : \mathbf{Z}/rs\mathbf{Z} \to \mathbf{Z}/r\mathbf{Z} \times \mathbf{Z}/s\mathbf{Z}\ ,\ {}^{rs}\overline{a} \mapsto ({}^{r}\overline{a}, {}^{s}\overline{a})$$

est un isomorphisme d'anneaux.

Remarque 12.17 Ainsi nous voyons que tous les anneaux suivants sont isomorphes

$$\mathbf{Z}/24\mathbf{Z}\ ,\ \mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}\ ,\ \mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}.$$

Nous verrons plus tard que ces anneaux *ne sont pas* isomorphes à $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$.

Démonstration. Vérifions que Φ est un homomorphisme. En effet pour $a,b\in\mathbf{Z}$, nous avons

$$\begin{aligned}\Phi({}^{rs}\overline{a}+{}^{rs}\ \overline{b}) &= \Phi({}^{rs}\overline{a+b}) = ({}^{r}\overline{a+b},{}^{s}\ \overline{a+b})\\ &= ({}^{r}\overline{a}+{}^{r}\ \overline{b},{}^{s}\ \overline{a}+{}^{s}\ \overline{b})\\ &= ({}^{r}\overline{a},{}^{s}\ \overline{a})+({}^{r}\overline{b},{}^{s}\ \overline{b}).\end{aligned}$$

De même, on vérifie que Φ est compatible à la multiplication. Vérifions que Φ est injective. En effet, si $\Phi({}^{rs}\overline{a})=\Phi({}^{rs}\overline{b})$, alors nous avons $({}^{r}\overline{a},{}^{s}\ \overline{a})=({}^{r}\overline{b},{}^{s}\ \overline{b})$ et donc

$$\begin{aligned}a &\equiv b\ (r)\\ a &\equiv b\ (s).\end{aligned}$$

Ainsi la différence $a-b$ est divisible par r est s et donc par le produit $r\,s$, puisque r et s sont premiers entre eux. Donc les classes ${}^{rs}\overline{a}$ et ${}^{rs}\overline{b}$ sont égales. Vérifions que Φ est surjective. En effet soient $a_1,a_2\in\mathbf{Z}$. Alors nous cherchons $a\in\mathbf{Z}$ tel que $({}^{r}\overline{a},{}^{s}\ \overline{a})=({}^{r}\overline{a_1},{}^{s}\ \overline{a_2})$. De façon équivalente, nous cherchons $a\in\mathbf{Z}$ solution du système

$$\begin{aligned}a &\equiv a_1\ (r)\\ a &\equiv a_2\ (s)\end{aligned}$$

Or, puisque r et s sont premiers entre eux, d'après le lemme chinois pour les congruences, il existe une solution $a\in\mathbf{Z}$. $\surd$

Remarque 12.18 Les anneaux $\mathbf{Z}/rs\mathbf{Z}$ et $\mathbf{Z}/r\mathbf{Z}\times\mathbf{Z}/s\mathbf{Z}$ ont même cardinal (égal à $r\,s$). Dans la démonstration, il aurait donc suffi de montrer soit la surjectivité soit l'injectivité de l'application Φ pour conclure qu'elle est en fait bijective. Nous avons donné les deux démonstrations pour mieux établir le lien avec le lemme chinois en termes de congruences.

Corollaire 12.19 *Soient r,s des entier ≥ 2 et premiers entre eux. Alors l'application*

$$\Phi^{\star}:(\mathbf{Z}/rs\mathbf{Z})^{\star}\to(\mathbf{Z}/r\mathbf{Z})^{\star}\times(\mathbf{Z}/s\mathbf{Z})^{\star}\ ,\ {}^{rs}\overline{a}\mapsto({}^{r}\overline{a},{}^{s}\ \overline{a})$$

est un isomorphisme de groupes. En particulier, elle est bijective et le deux groupes sont donc du même ordre.

Démonstration. Le corollaire résulte du lemme précédent et du lemme (12.15). $\surd$

Définition 12.20 *Soit n un entier ≥ 2. On définit $\phi(n)$ comme le cardinal du groupe des éléments inversibles de l'anneaux $\mathbf{Z}/n\mathbf{Z}$. La fonction ϕ est* l'indicatrice d'Euler.

Corollaire 12.21 *Si r et s sont deux entiers ≥ 2 et premiers entre eux on a*

$$\phi(rs)=\phi(r)\,\phi(s).$$

Démonstration. Ceci résulte aussitôt de la définition de $\phi(rs)$ et du corollaire (12.19). $\surd$

Remarque 12.22 Le corollaire précédent nous permet de calculer la valeur de $\phi(n)$ pour tout entier dont nous connaissons la décompositions en facteurs premiers. En effet, si nous avons

$$n=p_1^{e_1}\,p_2^{e_2}\,\ldots\,p_r^{e_r}$$

alors en applicant le corollaire plusieurs fois nous trouvons

$$\phi(n) = \phi(p_1^{e_1}\,\phi(p_2^{e_2}) \ldots \phi(p_r^{e_r}).$$

Mais d'après **??**, nous savons que pour un nombre premier p nous avons

$$\phi(p^k) = p^k - p^{k-1}.$$

Donc

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \ldots (p_r^{e_r} - p_r e_r - 1).$$

Par exemple,

$$\phi(36) = \phi(4 \times 9) = \phi(4)\,\phi(9) = (4-2) \times (9-3) = 12$$

et

$$\phi(1995) = \phi(3 \times 5 \times 7 \times 19) = 864.$$

13. Notion d'ordre d'un élément d'un groupe

Lemme 13.1 *Soit $(G, \star)$ un groupe et g un élément de G. Alors il existe une application*

$$\exp_g : \mathbf{Z} \to G$$

et une seule telle que

$$\begin{aligned} \exp_g(1) &= g \\ \exp_g(k+l) &= \exp_g(k) \star \exp_g(l) \end{aligned}$$

quels que soient $k, l \in \mathbf{Z}$.

Démonstration. Nous admettons ce résultat. √

Remarques 13.2

a) La seconde condition de la définition signifie que $\exp_g$ est un homomorphisme de groupes de $\mathbf{Z}$ vers G.

b) Supposons que $(G, \cdot)$ est un groupe dont la loi est notée multiplicativement. Alors pour tout n entier positif, nous avons

$$\begin{aligned} \exp_g(n) &= \underbrace{g \cdot g \cdots g}_{n} = g^n \\ \exp_g(-n) &= \exp_g(n)^{-1} = (g^{-1})^n. \end{aligned}$$

Nous écrirons g^n pour $exp_g(n)$ pour tout n entier.

c) Supposons que $(A, +)$ est un groupe dont la loi est notée additivement. Alors pour tout n entier positif, nous avons

$$\begin{aligned} \exp_a(n) &= \underbrace{a + a + \cdots + a}_{n} = n\,a \\ \exp_a(-n) &= -\exp_a(n) = -n\,a. \end{aligned}$$

Nous écrirons $n\,a$ pour $\exp_a(n)$ pour tout n entier.

Corollaire 13.3 *a) Soit $(G,\cdot)$ un groupe dont la loi est notée multiplicativement et g un élément de G. Pour $k,l \in \mathbf{Z}$, on a les égalités suivantes*

$$\begin{aligned} g^1 &= g \\ g^{k+l} &= g^k \star g^l \\ g^0 &= e_G \\ (g^k)^l &= g^{kl} \end{aligned}$$

b) Soit $(A,+)$ un groupe commutatif dont la loi est notée additivement et a un élément de A. Pour $k,l \in \mathbf{Z}$ on a les égalités suivantes

$$\begin{aligned} 1\,a &= a \\ (k+l)\,a &= k\,a + l\,a \\ 0\,a &= 0_A \\ k\,(l\,a) &= (kl)\,a \end{aligned}$$

Démonstration. Les deux parties sont des traductions dans la nouvelle notation de certaines propriétés de la fonction exp. Montrons-les dans les notations de a). Les premières deux égalités ne font que traduire dans la nouvelle notation les propriétés de la définition de $\exp_g$. La troisième propriété résulte du fait que $\exp_g$ est un homomorphisme. Pour la dernière propriété, fixons $k \in \mathbf{Z}$ et considérons l'application

$$f : \mathbf{Z} \to G, \ , \ l \mapsto g^{kl}.$$

Nous avons clairement $f(1) = g^k$ et

$$f(l+l') = g^{k(l+l')} = g^{kl+kl'} = g^{kl} \star g^{kl'} = f(l) \star f(l').$$

Par l'unicité de l'application $\exp_{g^k}$ nous pouvons conclure que $f(l) = \exp_{g^k}(l)$ pour tout $l \in \mathbf{Z}$ et donc que $f(l) = (g^k)^l$ pour tout $l \in \mathbf{Z}$. $\surd$

Définition 13.4 *Soit $(G,\star)$ un groupe et g un élément de G.* L'ordre de g *est le plus petit entier $n \geq 1$ tel que $\exp_g(n) = e_G$ s'il existe un tel entier. Sinon, l'ordre de g est infini. On note $\mathrm{ord}_G(g)$ ou $\mathrm{ord}\,(g)$ l'ordre de g dans G.*

Remarques 13.5

a) Supposons que $(G,\cdot)$ est un groupe dont la loi est notée multiplicativement et soit $g \in G$. Alors nous avons

$$\mathrm{ord}_G\,(g) = \inf\{n \in \mathbf{N} \mid n \geq 1 \text{ et } g^n = e\}.$$

Supposons que $(A,+)$ est un groupe commutatif dont la loi est notée additivement et soit $a \in A$. Alors nous avons

$$\mathrm{ord}_G\,(a) = \inf\{n \in \mathbf{N} \mid n \geq 1 \text{ et } na = 0_A\}.$$

b) Soit $(G,\cdot)$ un groupe dont la loi est notée multiplicativement (pour alléger les notations). Supposons que $g \in G$ est d'ordre fini n. Alors nous avons

$$g^{k+n} = g^k \cdot g^n = g^k \cdot e = g^k$$

pour tout entier k et n est le plus petit entier ≥ 1 avec cette propriété. Autrement dit, *la suite des puissances de g*

$$g^0 = e\ ,\ g\ ,\ g^2\ ,\ \ldots, g^k, \ldots$$

est périodique de période n. Nous avons aussi

$$g^{a+kn} = g^a g^{kn} = g^a (g^n)^k = g^a e^k = g^a$$

pour tout entier $a \in \mathbf{Z}$ et tout entier $k \in \mathbf{Z}$. Autrement dit *la valeur de g^a ne dépend que de la classe de congruence de a modulo n.*

Lemme 13.6 *Soit n un entier ≥ 2 et soit $\overline{a}$ une classe modulo n considérée comme élément du groupe $(A, +) = (\mathbf{Z}/n\mathbf{Z}, +)$. Alors*

$$\mathrm{ord}_{\mathrm{Z}/n\mathrm{Z}}(\overline{a}) = \frac{PPCM\,(a,n)}{a} = \frac{n}{PGCD\,(a,n)}.$$

Démonstration. Nous avons $k\overline{a} = \overline{0}$ ssi ka est un multiple de n, c'est-à-dire un multiple commun à a et n. Donc ka doit être un multiple de $\mathrm{PPCM}\,(a,n)$ et k un multiple de $\mathrm{PPCM}\,(a,n)/a$. Compte tenu de l'égalité

$$\mathrm{PPCM}\,(a,n) = \frac{a\,n}{\mathrm{PGCD}\,(a,n)}$$

nous obtenons aussi la seconde égalité. $\surd$

Remarque 13.7 Il *n'existe pas* de formule analogue pour l'ordre d'un élément $\overline{x}$ dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$. Cependant nous verrons que cet ordre est toujours un diviseur de $\phi(n)$, l'ordre du groupe $(\mathbf{Z}/n\mathbf{Z})^*$.

Lemme 13.8 *Soit $(G, \star)$ un groupe et g élément de G. Alors g est d'ordre infini ssi l'application*

$$\exp_g : \mathbf{Z} \to G$$

est injective. En particulier, tous les éléments d'un groupe fini sont d'ordre fini.

Démonstration. Si l'application $\exp_g$ est injective nous avons $\exp_g(n) \neq \exp_g(0)$ pour tout $n > 0$. Puisque $\exp_g(0) = e$, nous avons donc $\exp_g(n) \neq e$ pour tout $n > 0$ et g est d'ordre infini.

Réciproquement supposons g d'ordre infini. Soient $k \leq l$ des entiers tels que $\exp_g(k) = \exp_g(l)$. Alors nous avons $\exp_g(l-k) = e$. Puisque $l - k \geq 0$ et que g est d'ordre infini, il s'ensuit que $k = l$ et donc que $\exp_g$ est injective. $\surd$

Lemme 13.9 *Soit $(G, *)$ un groupe et $g \in G$ un élément d'ordre fini n. Alors l'application*

$$\mathbf{Z}/n\mathbf{Z} \to G\ ,\ \overline{a} \mapsto \exp_g(a)$$

est bien définie et injective. En particulier, l'ensemble des éléments de la forme $\exp_g(a)$, $a \in \mathbf{Z}$, est de cardinal n.

Démonstration. Supposons pour alléger les notations que la loi de G est notée multiplicativement. Nous avons donc

$$exp_g(a) = g^a \text{ et } g^n = e$$

pour tout $a \in \mathbf{Z}$. Donc

$$exp_g(a + kn) = g^{a+kn} = g^a g^{kn} = g^a (g^n)^k = g^a e^k = g^a.$$

L'application est donc bien définie. Supposons que $a \leq b$ sont deux entiers dont les classes ont même image. Alors nous avons $g^a = g^b$ et donc $g^{b-a} = e$. Pour montrer que n divise $b - a$, effectuons la division euclidienne $b - a = qn + r$ de $b - a$ par n. Par définition, nous avons $0 \leq r \leq (n-1)$. De l'autre côté, nous avons $e = g^{b-a} = g^r$. Puisque g est d'ordre n, il s'ensuit que n divise $b - a$ et donc que $\overline{a} = \overline{b}$. $\surd$

Théorème 13.10 (Lagrange) *Soit $(G,*)$ un groupe fini. L'ordre de tout élément de G divise l'ordre de G.*

Exemple 13.11 Considérons le groupe $G = (\mathbf{Z}/11\mathbf{Z})^*$. L'ordre de G est de 10. Voici les ordres des éléments de G :

g	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
ord (g)	1	10	5	5	5	10	10	10	5	2

Notons que le nombre d'éléments d'ordre 10 est de $4 = \phi(10)$, le nombre d'éléments d'ordre 5 est de $4 = \phi(5)$ et le nombre d'élments d'ordre 2 est de $1 = \phi(2)$. Nous verrons que ce n'est pas un hasard (17.5). Nous verrons aussi comment calculer facilement ce tableau (exemples 15.3)

Démonstration. Pour alléger les notations, supposons que la loi de G est notée multiplicativement. Soit $g \in G$. La démonstration se fait en plusieurs étapes :

Première étape : la relation définie par

$$x \equiv x' \ (g) \Longleftrightarrow x = x'\, g^k \ \textit{pour un}\ k \in \mathbf{Z}\,,$$

est une relation d'équivalence. Nous laissons cette vérification au lecteur. Notons $\overline{x}$ la classe d'équivalence d'un élément x. Par définition, la classe de x est formée de tous les éléments de la forme $x\, g^k$, $k \in \mathbf{Z}$.

Seconde étape : le cardinal de la classe de e est l'ordre de g. En effet, la classe de e est formée de tous les éléments de la forme g^k, $k \in \mathbf{Z}$. C'est donc l'image de l'application $\exp_g : \mathbf{Z} \to G$. Nous avons vu au lemme (13.9) qu'elle est en bijection avec $\mathbf{Z}/n\mathbf{Z}$ où n est l'ordre de g.

Troisième étape : toutes les classes d'équivalence ont même cardinal que la classe de e. En effet, si x est un élément de G, nous avons des bijections inverses l'une de l'autre entre $\overline{e}$ et $\overline{x}$ données par les applications $y \mapsto xy$ resp. $z \mapsto x^{-1}z$.

Quatrième étape : le cardinal de la classe de e divise l'ordre de G. En effet, nous savons que G est la réunion disjointe des classes d'équivalence. L'ordre de G est donc la somme des cardinaux des classes. Or toutes les classes ont même cardinal que $\overline{e}$. L'ordre de G est donc égal au cardinal de la classe de e multiplié par le nombre de classes d'équivalence.

Conclusion : l'ordre de g, qui est égal au cardinal de la classe de e (seconde étape), divise l'ordre de G (troisième étape). √

Corollaire 13.12 (Théorème d'Euler) *Soit n un entier ≥ 2 et a un entier premier avec n. Alors on a*

$$a^{\phi(n)} \equiv 1 \ (n),$$

où ϕ est l'indicatrice d'Euler.

Démonstration. Comme a est premier avec n, la classe $g = \overline{a}$ appartient au groupe $G = (\mathbf{Z}/n\mathbf{Z})^*$. L'affirmation résulte du théorème de Lagrange car $\phi(n)$ est l'ordre du groupe $(\mathbf{Z}/n\mathbf{Z})^*$ par définition. √

Corollaire 13.13 (Petit Théorème de Fermat) *Si p est un nombre premier et a un entier qui n'est pas divisible par p, on a*

$$a^{p-1} \equiv 1 \ (p).$$

Démonstration. On applique le théorème d'Euler en utilisant que $\phi(p) = p - 1$ pour un nombre premier. √

Remarque 13.14 Les théorèmes de Fermat (petit) et d'Euler permettent de calculer très rapidement certains restes de puissances. Dans les exemples suivants, on cherche le reste r de la division euclidienne de a par b :

Exemples 13.15

a) $a = 67^{100}$, $b = 101$: le nombre 101 est premier et 67 n'est pas divisible par 101. D'après le petit théorème de Fermat, on a $67^{100} \equiv 1\ (101)$ et donc $r = 1$.

b) $a = 1995^{540}$, $b = 541$: le nombre 541 est premier et 1995 n'est pas divisible par 541. D'après le petit théorème de Fermat, on a $1995^{540} \equiv 1\ (541)$ et donc $r = 1$.

c) $a = 25^{24}$, $b = 72$: nous avons $\phi(72) = \phi(8 \times 9) = \phi(8)\phi(9) = 4 \times 6 = 24$. Les nombres 72 et 25 sont premiers entre eux. Nous pouvons donc appliquer le théorème d'Euler pour conclure que $25^{24} \equiv 1\ (72)$. Donc $r = 1$.

d) $a = 51^{24}$, $b = 72$: nous avons $\phi(72) = 24$ (voir le numéro précédent). Or, *les nombres 51 et 72 ne sont pas premiers entre eux et nous ne pouvons pas appliquer le théorème d'Euler.* Cependant, soit $x = 51^{24}$. D'après le lemme chinois, pour connaître la classe de x modulo 72, il suffit de connaître les restes de x modulo 8 et modulo 9. Or

$$\begin{aligned} x &\equiv 51^{24} \equiv 3^{24} \equiv 1\ (8) \\ x &\equiv 51^{24} \equiv 6^{24} \equiv 0\ (9). \end{aligned}$$

Ici, nous avons appliqué le théorème d'Euler à 3 et 8 ($\phi(8) = 4$) et nous avons utilisé le fait que $6^2 \equiv 0\ (9)$. Le lemme chinois nous permet de conclure que $x \equiv 9\ (72)$ et le reste recherché est donc $r = 9$.

14. Algorithme de calcul rapide des puissances

Soit G un groupe dont la loi est notée multiplicativement. Soit g un élément de G et n un entier ≥ 2. Pour calculer g^n, on utilise l'algorithme suivant qui consiste à construire récursivement des suites x_k, y_k, q_k, $k \geq 1$, où $x_k, y_k \in G$ et $q_k \in \mathbf{N}$:

1) Initialisation : on pose $x_1 = g$, $y_1 = e$, $q_k = n$.

2) Passage à l'étape k : on pose $x_k = x_{k-1}^2$, on prend pour q_k le quotient de la division de q_{k-1} par 2 et on pose

$$y_k = \begin{cases} y_{k-1} & \text{si } q_{k-1} \text{ est pair} \\ x_{k-1}y_{k-1} & \text{si } q_{k-1} \text{ est impair} \end{cases}$$

3) Arrêt : quand $q_k = 1$, l'algorithme s'arrête et la puissance recherchée est $g^n = x_k y_k$.

Dans la pratique, on organise les suites x_k, y_k, q_k dans un tableau. Voir les exemples ci-dessous.

Exemples. Calculons 2^{50} dans $(\mathbf{Z}/101\mathbf{Z})^*$:

k	x_k	y_k	q_k
1	2	1	50
2	4	1	25
3	16	4	12
4	54	4	6
5	88	4	3
6	68	49	1
		100	

Nous trouvons donc que $2^{50} \equiv -1$ (101). La première colonne ne dépend que de $g = 2$ et nous pouvons la réutiliser. Dans le tableau suivant, nous utilisons deux fois la même première colonne pour calculer 3^{50} et 3^{20} dans $(\mathbf{Z}/101\mathbf{Z})^*$.

x_k	y_k	q_k	y_k	q_k
3	1	50	1	20
9	1	25	1	10
81	9	12	1	5
97	9	6	81	2
16	9	3	81	1
54	43	1		
	100		84	

Lemme 14.1 *L'algorithme décrit ci-dessus est correct.*

Démonstration. Nous allons montrer par récurrence que nous avons $x_k^{q_k}\, y_k = g^n$. Ceci entraînera l'affirmation car pour $q_k = e$, cette égalité se spécialise en $x_k y_k = g^n$.

A l'étape $k = 1$, l'affirmation est vraie par définition de l'initialisation de l'algorithme. Supposons qu'elle est vraie pour l'étape $k-1$ et montrons-la pour l'étape k. Soit $q_{k-1} = 2\, q_k + r_k$ la division euclidienne de q_{k-1} par 2. Par l'hypothèse de récurrence, nous avons

$$x_{k-1}^{q_{k-1}} y_{k-1} = g^n.$$

Si nous substituons le résultat de la division euclidienne pour q_{k-1}, nous trouvons

$$g^n = x_{k-1}^{2\,q_k + r_k}\, y_{k-1} = (x_{k-1}^2)^{q_k} (x_{k-1}^{r_k}) y_{k-1} = x_k^{q_k}\, y_k.$$

Pour la dernière égalité, nous avons utilisé la définition de x_k et y_k (le nombre q_{k-1} est pair ssi $r_k = 0$). $\surd$

15. Calcul de l'ordre d'un élément

Soit n un entier. Un diviseur positif d de n est *maximal* s'il est de la forme n/p où p est un diviseur premier de n. Soit G un groupe fini dont la loi est notée multiplicativement. Soit g un élément de G. Soit n un entier positif.

Lemme 15.1 *a) On a $g^n = e$ si et seulement si n est un multiple de l'ordre de g.*

b) L'élément g est d'ordre n si et seulement si $g^n = e$ et $g^d \neq e$ pour tout diviseur maximal de n.

c) Si g est d'ordre n et d divise n, alors g^d est d'ordre n/d.

d) Plus généralement, si g est d'ordre n et a un entier quelconque, alors g^a est d'ordre $n/PGCD\,(a,n)$.

Démonstration. a) Ceci est clair d'après le lemme 13.9 qui affirme que l'application $\mathbf{Z}/\mathrm{ord}(g)\mathbf{Z} \to G$, $\overline{k} \mapsto g^k$ est injective.

b) La condition est clairement nécessaire. Supposons réciproquement qu'elle est vérifié. Alors n est multiple de l'ordre de g d'après a), mais aucun diviseur propre de n n'est multiple de l'ordre de g. (tout diviseur propre divise un diviseur maximal de n). Donc $n = \mathrm{ord}(g)$.

c) Nous avons $(g^d)^k = g^{dk}$ ce qui donne immédiatement l'affirmation.

d) D'après le lemme 13.9, nous avons $g^k = e$ ssi $\overline{k} = \overline{0}$ dans $\mathbf{Z}/n\mathbf{Z}$. Donc l'ordre de g^a est égal à l'ordre de $\overline{a}$ dans $\mathbf{Z}/n\mathbf{Z}$. Ce dernier est égal à $n/\mathrm{PGCD}\,(a,n)$ d'après le lemme 13.6. $\surd$

Remarque 15.2 Pour déterminer l'ordre de g, on calcule les puissances g^d pour les diviseurs maximaux d de n. Si on a $g^d \neq e$ pour tout diviseur maximal, alors g est d'ordre n (et G est cyclique engendré par g voir ci-dessous). Sinon, on a $g^d = e$ pour un diviseur maximal d de n et on recommence avec n remplacé par d. Dans le calcul des puissances $g^{d'}$ pour les diviseurs maximaux d' de d on pourra cependant omettre tous ceux qui divisent un diviseur maximal d'' de n pour lequel $g^{d''} \neq e$. Voir l'exemple suivant.

Exemples 15.3

a) Calculons l'ordre de 2 dans $(\mathbf{Z}/113\mathbf{Z})^*$. Ce groupe est d'ordre $n = 112 = 7 \times 16$. Les diviseurs maximaux de n sont 16 et 56. Calculons donc 2^{56} et 2^{16}.

x_k	y_k	q_k	y_k	q_k
2	1	56	1	16
4	1	28	1	8
16	1	14	1	4
30	1	7	1	2
109	30	3	1	1
16	106	1		
	1		109	

Ainsi $2^{16} \neq e$ et $2^{56} = e$. Les diviseurs maximaux de 56 sont 8 et 28. Puisque $2^{16} \neq e$ nous avons $2^8 \neq e$ et il suffit de calculer 2^{28}. On trouve $2^{28} = 1$. Les diviseurs maximaux de 28 sont 4 et 14. Puisque $2^8 \neq 1$, nous avons $2^4 \neq 1$ et il suffit de calculer 2^{14}. On trouve $2^{14} = -1$ et *l'ordre de* 2 *dans* $(\mathbf{Z}/113\mathbf{Z})^*$ *est donc de* 28.

b) Déterminons les ordres des éléments de $(\mathbf{Z}/11\mathbf{Z})^*$. Calculons l'ordre de 2. Nous avons $2^{10} \equiv 1\ (11)$ par le petit théorème de Fermat. Les diviseurs maximaux de 10 sont 2 et 5. Nous avons

$$2^2 = 4\,,\ 2^5 \equiv 2 \times 4 \times 4 \equiv -1\ (11).$$

Donc 2 est d'ordre 10 et tout élément de $(\mathbf{Z}/11\mathbf{Z})^*$ est une puissance de 2 d'après le lemme (13.9). Calculons ces puissances

k	0	1	2	3	4	5	6	7	8	9
2^k	1	2	4	8	5	10	9	7	3	6

Maintenant, on calcule facilement les ordres de tous les éléments à l'aide des parties b) et c) du lemme. Par exemple, on a

$$\begin{aligned} \mathrm{ord}(3) &= \mathrm{ord}(2^8) = \frac{10}{\mathrm{PGCD}\,(10,8)} = 5 \\ \mathrm{ord}(4) &= \mathrm{ord}(2^2) = \frac{10}{2} = 5. \end{aligned}$$

On trouve la table suivante (voir)

g	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\mathrm{ord}\,(g)$	1	10	5	5	5	10	10	10	5	2

16. Groupes cycliques

Définition 16.1 *Soit* $(G, *)$ *un groupe. Un* sous-groupe *de* G *est une partie* H *de* G *vérifiant les trois conditions suivantes*

- $e_G \in H$,
- $h \star k \in H$ *pour tous les* $h, k \in H$,
- $h^{-1} \in H$ *pour tous les* $h \in H$.

Exemples 16.2

a) Les parties $\{e_G\}$ et G de G sont toujours des sous-groupes. L'intersection de toute famille de sous-groupes est un sous-groupe.

b) Pour tout $n \in \mathbf{Z}$, la partie $n\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z}, +)$. Réciproquement, tout sous-groupe de $\mathbf{Z}$ est de cette forme : en effet, soit $S \subset \mathbf{Z}$ un sous-groupe. Si $S = \{0\}$, alors $S = 0\mathbf{Z}$ et il n'y a rien à démontrer. Sinon, la partie S contient un entier non nul et donc un entier non nul positif (car x appartient à S si $-x$ appartient à S). Soit n le plus petit des entiers strictements positifs contenus dans S. Alors on a clairement $n\mathbf{Z} \subset S$. Réciproquement, si x appartient à S et que $x = q\,n + r$ est la division euclidienne de x par n, alors $r = x - q\,n$ appartient à S et est positif et inférieur à n. Donc $r = 0$ et $x \in n\mathbf{Z}$.

c) Si n est un entier ≥ 2 et d un diviseur de n, alors $d\mathbf{Z}/n\mathbf{Z} = \{\overline{dx} \mid x \in \mathbf{Z}\}$ est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z}, +)$ et tout sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ est de cette forme : en effet, si $\tilde{A} \subset \mathbf{Z}/n\mathbf{Z}$ est un sous-groupe alors $\tilde{A} \subset \mathbf{Z}$ est un sous-groupe qui contient $n\mathbf{Z}$. Donc $\tilde{A} = d\mathbf{Z}$ pour un entier d. La condition $n\mathbf{Z} \subset d\mathbf{Z}$ montre que n est un multiple de d.

Définition 16.3 *Soit G un groupe et X une partie de G. On note $< X >$ et on appelle* sous-groupe engendré par X *la partie de G formée de tous les produits d'éléments de X et de leurs inverses (par convention on pose $< X >= \{e_G\}$ si X est vide).*

Remarque 16.4 Il s'agit bien d'un sous-groupe.

Exemple 16.5 Soit G un groupe (dont la loi est notée multiplicativement) et g un élément de G. Alors le sous-groupe engendré par la partie $X = \{g\}$ est égale à $\{g^k \mid k \in \mathbf{Z}\}$. Ce sous-groupe est isomorphe à $\mathbf{Z}$ si g est d'ordre infini et isomorphe à $\mathbf{Z}/n\mathbf{Z}$ si g est d'ordre fini n d'après les lemmes (13.8) et (13.9).

Définition 16.6 *Un groupe est* cyclique *s'il contient un élément qui l'engendre : un* générateur.

Remarque 16.7 D'après l'exemple précédent, un groupe cyclique est soit isomorphe à $\mathbf{Z}$ soit à $\mathbf{Z}/n\mathbf{Z}$ pour un entier $n \geq 1$. Réciproquement, un groupe isomorphe à $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$ est cyclique (engendré par l'image de 1 resp. $\overline{1}$ par un isomorphisme choisi). Un groupe fini d'ordre n est cyclique si et seulement si il contient un élément d'ordre n.

Théorème 16.8 *Soit p un nombre premier. Alors le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.*

Démonstration. Le théorème sera démontré plus tard (18.4). $\surd$

Remarque 16.9 Le théorème ne donne pas de générateur de ce groupe et c'est un problème ouvert de construire un 'générateur universel et explicite'. On ignore par exemple si la classe de 2 engendre $(\mathbf{Z}/p\mathbf{Z})^*$ pour une infinité de nombres premiers p ou non.

17. Racines de l'unité

Définition 17.1 *Soit G un groupe et l un entier ≥ 1. Nous appellerons racine l-ièmes de l'unité dans G les solutions $g \in G$ de l'équation $g^l = e$.*

Remarque 17.2 Les racines l-ièmes de l'unité sont exactement les éléments de G dont l'ordre est un diviseur de l.

Lemme 17.3 *Soit G un groupe cyclique d'ordre fini n et g un générateur de G. Soit l un entier ≥ 2 et R l'ensemble des solutions de l'équation*

$$x^l = e$$

dans G.

a) Si l divise n, on a

$$R = \{g^{k\,(n/l)} \mid k = 0, 1, \ldots, l-1\}.$$

b) Si l est premier avec n, on a

$$R = \{e\}.$$

c) Dans le cas général, posons $l' = PGCD(n, l)$. Alors

$$R = \{g^{k\,(n/l')} \mid k = 0, 1, \ldots, l'-1\}.$$

Exemple 17.4 On cherche les solutions de l'équation $x^5 = 1$ dans $\mathbf{Z}/2011\mathbf{Z}$. Si $x \in \mathbf{Z}/2011\mathbf{Z}$ est solution de cette équation, alors $xx^4 = 1$ et donc x est inversible (d'inverse x^4). Ainsi, il revient au même de chercher les solutions de cette équation dans $(\mathbf{Z}/2011\mathbf{Z})^*$. Or le nombre $p = 2011$ est premier et le groupe $G = (\mathbf{Z}/2011\mathbf{Z})^*$ est donc cyclique (16.8). En outre 5 divise l'ordre de G qui est 2010. L'équation admet donc exactement 5 solutions et ces solutions sont de la forme

$$g^0\ ,\ h = g^{402}\ ,\ h^2 = g^{804}\ ,\ h^3 = g^{1206}\ ,\ h^4 = g^{1608}\ ,$$

où g est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. Il reste à trouver un générateur et à calculer ces puissances. Si on calcule les puissances maximales de 2, on trouve que $2^{2010/5} = 1$. Donc 2 n'est pas un générateur. Par contre, les puissances maximales de 3 sont toutes différentes de 1 et 3 engendre donc $(\mathbf{Z}/2011\mathbf{Z})^*$. Si on calcule $h = 3^{402}$, on trouve $h = 1328$. L'ensemble des solutions de l'équation $x^5 = 1$ est donc formé de

$$1\ ,\ h = 1328\ ,\ h^2 = 1948\ ,\ h^3 = 798\ ,\ h^4 = 1958.$$

Démonstration. Comme G est cyclique, toute solution x de $x^l = e$ est de la forme $x = g^a$ pour un $a \in \mathbf{Z}$. Dans le cas de a), on a donc $al \equiv 0\ (n)$ d'après le lemme (13.9). Cela signifie que a est multiple de n/l.

Dans le cas de b), la congruence $al \equiv 0\ (n)$ implique $a \equiv 0\ (n)$ car l est inversible modulo n.

Finalement, dans le cas de c), écrivons $l = l'l''$ où l'' et n sont premiers entre eux. Alors la congruence $al'l'' \equiv 0\ (n)$ est équivalente à $al' \equiv 0\ (n)$ qui, elle, exprime que a est multiple de n/l'. $\surd$

Lemme 17.5 *Soit G un groupe cyclique d'ordre $n < \infty$ et g un générateur de G. Soit d un diviseur de n. Alors l'ensemble des éléments d'ordre d de G est formé des puissances*

$$g^{k\,n/d}$$

où k parcourt les classes inversibles modulo d. Ces éléments sont deux à deux distincts. En particulier, le nombre d'éléments d'ordre d dans G est égal à $\phi(d)$, le nombre de générateurs de G est égal à $\phi(n)$ et on a

$$n = \sum_{d|n} \phi(d).$$

Exemple 17.6 Le nombre $p = 2011$ est premier et le groupe $G = (\mathbf{Z}/p\mathbf{Z})^*$ est donc cyclique (théorème 16.8) d'ordre $2010 = 2 \times 3 \times 5 \times 67$. Ce groupe contient donc $\phi(2010) = 2 \times 4 \times 66 = 528$ générateurs.

Démonstration. Soit $x = g^a$ un élément d'ordre d de G. Alors d'après le théorème 17.3, nous avons $a = k\,n/d$ pour un $k \in \mathbf{Z}$. Si f est un facteur commun à k et d, alors on a $(g^a)^{(d/f)} = e$. Puisque g^a est d'ordre d, il s'ensuit $f = \pm 1$. Les éléments de l'affirmation sont deux à deux distincts d'après le lemme (13.9). La dernière affirmation s'ensuit parce que G est la réunion disjointe de ses parties formées des éléments d'ordre d, où d parcourt les diviseurs d de n, d'après le théorème de Lagrange (13.10). √

18. Structure du groupe des classes inversibles modulo un nombre premier

Nous démontrerons dans cette section le théorème (16.8) qui affirme que le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique lorsque p est premier. Nous aurons besoin du

Lemme 18.1 *Soit p un nombre premier. Si*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

est un polynôme de degré n à coefficients a_i dans $\mathbf{Z}/p\mathbf{Z}$, alors l'équation $P(x) = 0$ admet au plus n solutions x dans $\mathbf{Z}/p\mathbf{Z}$.

Remarque 18.2 On appelle *racines* de $P(X)$ les solutions x de $P(x) = 0$.

Démonstration. Nous procédons par récurrence sur n. Si $n = 1$, l'équation $P(x) = 0$ devient $a_1 x + a_0 = 0$. Elle admet $x = -a_0/a_1$ pour unique solution (le coefficient a_1 est non nul car $P(X)$ est de degré 1). Supposons l'affirmation démontrée pour des polynômes de degré $< n$ et soit $P(X)$ de degré n. Supposons que $P(x) = 0$. Comme pour des polynômes à coefficients réels (ou à coefficients dans tout autre corps) nous pouvons écrire la division euclidienne du polynôme $P(X)$ par le polynôme $(X - x)$

$$P(X) = (X - x)\,Q(X) + R(X)\,,$$

où $Q(X)$ est un polynôme de degré $n - 1$ (le quotient) et $R(X)$ un polynôme de degré < 1 (le reste) car $X - x$ est de degré 1. Donc $R(X) = c_0$ pour un $c_0 \in \mathbf{Z}/p\mathbf{Z}$. Si nous remplaçons X par x dans l'équation de la division euclidienne nous trouvons

$$0 = 0 \times Q(x) + c_0$$

et donc $c_0 = 0$. Ainsi, nous avons $P(X) = Q(X)\,(X - x)$. Si $P(X)$ s'annule en y, alors on a $Q(y) = 0$ ou $y - x = 0$ car $\mathbf{Z}/p\mathbf{Z}$ est un corps. Ainsi toute solution $y \neq x$ de $P(X) = 0$ est solution de $Q(X) = 0$ et par l'hypothèse de récurrence on conclut que $P(X)$ admet au plus $n - 1$ racines différentes de x, c'est-à-dire n racines au total. √

Lemme 18.3 *Soit G un groupe d'ordre fini n et tel que l'équation $x^d = e$ admet au plus d solutions dans G pour tout diviseur d de n. Alors G est cyclique.*

Démonstration. Pour un diviseur d de n, notons $\psi(d)$ le nombre d'éléments d'ordre d de G. Supposons que d est un diviseur de n et qu'il existe dans G un élément g d'ordre d. Considérons le sous-groupe $< g >$ engendré par cet élément. Il est cyclique d'ordre d et chacun de ses éléments est solution de l'équation $x^d = e$ dans G. Ainsi, d'après l'hypothèse sur G, toute solution de $x^d = e$ dans G se trouve en fait dans le sous-groupe $< g >$. En particulier, tout élément d'ordre d de G se trouve dans ce sous-groupe. Or nous savons qu'un groupe cyclique contient exactement $\phi(d)$ éléments d'ordre d (lemme 17.5). Ainsi, le groupe G contient exactement $\phi(d)$ éléments d'ordre d. Nous avons donc $\psi(d) = \phi(d)$ si

$\psi(d) > 0$ et $\psi(d) = 0$ sinon. De toute façon, nous avons $\psi(d) \leq \phi(d)$. Par conséquent, nous avons

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \phi(d) = n\,,$$

où la dernière égalité provient du lemme (17.5). Nous avons donc $\psi(d) = \phi(d)$ pour tout diviseur d de n et en particulier, le groupe G contient $\phi(n)$ éléments d'ordre n. Il nous aurait suffi d'un seul pour conclure que G est cyclique d'ordre n. $\surd$

Corollaire 18.4 *(=Théorème 16.8) Si p est premier, le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.*

Démonstration. En effet, appliquons le lemme précédent à $G = (\mathbf{Z}/p\mathbf{Z})^*$. D'après le lemme (18.1), l'équation $X^d - 1 = 0$ admet au plus d solutions pour tout diviseur d de n (et même pour tout $d \in \mathbf{N}$). $\surd$

19. Structure du groupe des classes inversibles modulo une puissance d'un nombre premier

Lemme 19.1 *Soit p un nombre premier et $1 \leq k \leq p-1$. Alors le coefficient binomial C_p^k est divisible par p.*

Démonstration. En effet, nous avons

$$C_p^k = \frac{p!}{k!\,(p-k)!} = \frac{p\,(p-1)\,(p-2)\,\ldots\,(p-k+1)}{1 \times 2 \times 3 \times \ldots \times k}.$$

Puisque $0 < k < p$, le numérateur comporte un facteur p, mais le dénominateur n'en comporte pas. $\surd$

Théorème 19.2 *a) Soit p un nombre premier > 2 et k un entier ≥ 1. Alors le groupe $G = (\mathbf{Z}/p^k\mathbf{Z})^*$ est cyclique d'ordre $(p-1)\,p^{k-1}$. La classe de $1+p$ est un élément d'ordre p^{k-1} dans G.*

b) Le groupe $(\mathbf{Z}/2\mathbf{Z})^*$ est trivial, le groupe $(\mathbf{Z}/4\mathbf{Z})^*$ est cyclique d'ordre 2 et pour $k \geq 2$, le groupe $(\mathbf{Z}/2^k\mathbf{Z})^*$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{k-2}\mathbf{Z}$. Dans ce dernier cas, l'élément 5 est d'ordre 2^{k-2} dans $(\mathbf{Z}/2^k\mathbf{Z})^*$ et tout élément de ce groupe est de la forme $\pm 5^a$, $a \in \mathbf{Z}$.

Démonstration. Posons $G = (\mathbf{Z}/p^k\mathbf{Z})^*$ resp. $G = (\mathbf{Z}/2^k\mathbf{Z})^*$.

a) *Première étape : pour $e \geq 0$, nous avons*

$$(1+p)^{(p^e)} \equiv 1 + p^{e+1}\ (p^{e+2}).$$

Procédons par récurrence sur e. Pour $e = 0$ l'affirmation est trivialement vraie. Supposons la démontrée pour e. Nous avons donc

$$(1+p)^{(p^e)} = 1 + p^{e+1}(1+xp)$$

pour un $x \in \mathbf{Z}$. Alors

$$\begin{aligned}(1+p)^{p^{e+1}} &= ((1+p)^{(p^e)})^p = (1+p^{e+1}(1+xp))^p \\ &= 1 + p\,p^{e+1}(1+xp) + (\sum_{k=2}^{p-1} C_p^k p^{k(e+1)}(1+xp)^k) + p^{p(e+1)}(1+xp)^p.\end{aligned}$$

Si nous réduisons modulo p^{e+3} nous trouvons $1 + p^{e+2}$ car les C_p^k sont divisibles par p et $p(e+1) \geq 3$ puisque $p \geq 3$.

Notons $\phi : (\mathbf{Z}/p^k\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ l'application qui à x associe sa classe modulo p. Clairement, ϕ est un homomorphisme de groupe. Notons H le *noyau* de ϕ, c'est-à-dire l'ensemble de $x \in G$ tels que $\phi(x) = e$. C'est clairement un sous-groupe.

Seconde étape : L'élément $1+p$ est un générateur de H. En particulier, il est d'ordre p^{k-1}. Clairement, H est formé des éléments $1+x$ où x est divisible par p (dans $\mathbf{Z}/p^k\mathbf{Z}$). Donc H est d'ordre p^{k-1}. L'élément $1+p$ appartient à H. Son ordre est donc une puissance de p. D'après la première partie c'est p^{k-1}.

Troisième étape : construction d'un élément d'ordre $p-1$. Soit x_0 un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ et $x_1 \in G$ un élément tel que $\phi(x_1) = x_0$. Si on a $x_1^k = e$ alors on a $\phi(x_1)^k = e$ et l'ordre de x_1 est donc un multiple de l'ordre de x_0. Par conséquent, l'ordre de x_1 est de la forme $(p-1)\,p^l$ pour un $l \in \mathbf{N}$. Posons $x = x_1^{p^l}$. Alors x est d'ordre $p-1$ d'après le lemme 15.1.

Quatrième étape : l'affirmation. Avec les notations introduites ci-dessus, considérons l'élément $x\,(1+p)$. Il est d'ordre $(p-1)\,p^{k-1}$ d'après le lemme ci-dessous.

b) *Première étape : pour $e \geq 0$, nous avons*

$$5^{(2^e)} \equiv 1 + 2^{e+2}\ (2^{e+3}).$$

Procédons par récurrence. Pour $e = 0$, l'affirmation est trivialement vraie. Supposons-la démontrée pour e. Alors nous avons

$$\begin{aligned} 5^{(2^{e+1})} &= (1 + 2^{e+2}(1+2\,x))^2 \\ &= 1 + 2 \times 2^{e+2}(1+2\,x) + 2^{2\,e+4}(1+2\,x)^2. \end{aligned}$$

Si nous réduisons modulo 2^{e+4}, nous trouvons bien $1 + 2^{e+3}$.

Notons $\phi : (\mathbf{Z}/2^k\mathbf{Z})^* \to (\mathbf{Z}/4\mathbf{Z})^*$ l'application qui à x associe sa classe modulo 4. Clairement, ϕ est un homomorphisme de groupe. Notons H le *noyau* de ϕ, c'est-à-dire l'ensemble de $x \in G$ tels que $\phi(x) = e$. C'est clairement un sous-groupe.

Seconde étape : L'élément 5 est un générateur de H. En particulier, il est d'ordre 2^{k-2}. Clairement, H est formé des éléments $1+x$ où x est divisible par 4 (dans $\mathbf{Z}/2^k\mathbf{Z}$). Donc H est d'ordre 2^{k-2}. L'élément 5 appartient à H. Son ordre est donc une puissance de 2. D'après la première partie c'est 2^{k-2}.

Troisième étape : l'affirmation. Considérons l'application

$$f : \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{k-2}\mathbf{Z} \to (\mathbf{Z}/2^k\mathbf{Z})^*\ ,\ (\overline{a}, \overline{b}) \mapsto (-1)^a\ 5^b.$$

On vérifie aisément que c'est un homomorphisme de groupe. En outre, f est surjectif (quel que soit $x \in G$, on a $x \in H$ ou $-x \in H$). Comme les deux groupes sont d'ordre 2^{k-1}, il s'ensuit que f est bijectif. Donc f est un isomorphisme.

$\surd$

Lemme 19.3 *Soit G un groupe noté multiplicativement et soient g, h deux éléments d'ordre fini a, b de G tels que $gh = hg$ et a, b sont premiers entre eux. Alors gh est d'ordre ab.*

Démonstration. En effet, pour $k \in \mathbf{Z}$, nous avons $(gh)^k = g^k\,h^k = e$ si et seulement si $g^k = h^{-k}$. L'ordre de l'élément $g^k = h^{-k}$ est donc un diviseur commun à ord$g$ et ord$h$. Comme ces nombres sont premiers entre eux, l'ordre de $g^k = h^{-k}$ est égal à 1 et $g^k = h^{-k} = e$. Cela veut dire que k est multiple de a et de $-b$. Puisque les deux sont premiers entre eux, k doit être multiple du produit ab. Réciproquement, nous avons $(gh)^{ab} = (g^a)^b\,(h^b)^a = e$. $\surd$

Remarque 19.4 En combinaison avec le lemme chinois, le théorème 19.2 permet de déterminer la structure du groupe $(\mathbf{Z}/n\mathbf{Z})^*$ pour tout entier n dont on connaît la décomposition en produit de facteurs premiers. Par exemple, considérons $n = 3 \times 5^3 \times 7^2$. Alors, par le théorème chinois, nous avons un isomorphisme

$$(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} (\mathbf{Z}/3\mathbf{Z})^* \times (\mathbf{Z}/5^3\mathbf{Z})^* \times (\mathbf{Z}/7^2\mathbf{Z})^*.$$

Le théorème 19.2 donne des isomorphismes $(\mathbf{Z}/3\mathbf{Z})^* \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$, $(\mathbf{Z}/5^3\mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}/100\mathbf{Z}$, $\mathbf{Z}/7^2\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/42\mathbf{Z}$. Donc on a

$$(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/100\mathbf{Z} \times \mathbf{Z}/42\mathbf{Z}.$$

Cela montre par exemple que le nombre de solutions de l'équation $x^4 = 1$ dans $\mathbf{Z}/n\mathbf{Z}$ est égal à $2 \times 4 \times 2 = 16$. Nous laissons au lecteur le soin de calculer explicitement ces 16 solutions.

20. L'indicatrice de Carmichael

Définition 20.1 *Soit n un entier ≥ 2. On définit $\lambda(n)$ comme le maximum des ordres des éléments du groupe $(\mathbf{Z}/n\mathbf{Z})^*$. On appelle* indicatrice de Carmichael *l'expression $\lambda(n)$.*

Exemple 20.2 Si p est premier, on a $\lambda(p) = \phi(p) = p - 1$ car le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p - 1$.

Lemme 20.3 (Théorème de Carmichael) *On a $a^{\lambda(n)} \equiv 1\ (n)$ pour tout entier a premier à n. Réciproquement, si m vérifie $a^m \equiv 1\ (n)$ pour tout entier a premier à n, alors m est multiple de $\lambda(n)$.*

Démonstration. Soit $a \in (\mathbf{Z}/n\mathbf{Z})^*$ un élément d'ordre $u = \lambda(n)$ et $b \in (\mathbf{Z}/n\mathbf{Z})^*$ un élément d'ordre v. Nous allons montrer que $(\mathbf{Z}/n\mathbf{Z})^*$ contient un élément dont l'ordre est PPCM (u, v). Il s'ensuivra que $\lambda(n) = \text{PPCM}\,(u, v)$ et donc que v divise $\lambda(n)$.

Pour cela, écrivons PPCM $(u, v) = u'v'$, où u' divise u, v' divise v et u', v' sont premiers entre eux. Alors $a^{u/u'}$ est d'ordre u', $b^{v/v'}$ est d'ordre v' et donc leur produit est d'ordre $u'v' = \text{PPCM}\,(u, v)$ d'après le lemme 19.3.

La deuxième affirmation est claire. √

Lemme 20.4 *a) On a $\lambda(2) = 1$, $\lambda(4) = 2$ et $\lambda(2^k) = 2^{k-2}$ pour tout $k \geq 3$.*

b) Si p est un nombre premier impair, on a $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.

c) Si $n = rs$ où r et s sont premiers entre eux, on a $\lambda(n) = PPCM(\lambda(r), \lambda(s))$.

Remarque 20.5 Ce lemme permet de calculer l'indicatrice de Carmichael de tout nombre dont on connaît la décomposition en facteurs premiers. Par exemple, on a

$$\lambda(561) = \lambda(3 \times 11 \times 17) = \text{PPCM}\,(2, 10, 16) = 80.$$

En particulier, comme 80 divise 560, nous avons

$$a^{560} \equiv 1\ (561)$$

pour tout a premier à 561 (comme dans le petit théorème de Fermat). Un nombre n tel que $a^{n-1} \equiv 1\ (n)$ pour tout entier a premier à p s'appelle un *nombre de Carmichael.* Voici le tableau des premiers 17 nombres de Carmichael non premiers.

i	n	décomposition	$\lambda(n)$
1	561	$3 \times 11 \times 17$	80
2	1105	$5 \times 13 \times 17$	48
3	1729	$7 \times 13 \times 19$	36
4	2465	$5 \times 17 \times 29$	112
5	2821	$7 \times 13 \times 31$	60
6	6601	$7 \times 23 \times 41$	1320
7	8911	$7 \times 19 \times 67$	198
8	10585	$5 \times 29 \times 73$	504
9	15841	$7 \times 31 \times 73$	360
10	29341	$13 \times 37 \times 61$	180
11	41041	$7 \times 11 \times 13 \times 41$	120
12	46657	$13 \times 37 \times 97$	288
13	52633	$7 \times 73 \times 103$	1224
14	62745	$3 \times 5 \times 47 \times 89$	2024
15	63973	$7 \times 13 \times 19 \times 37$	36
16	75361	$11 \times 13 \times 17 \times 31$	240
17	101101	$7 \times 11 \times 13 \times 101$	300

Démonstration. Les parties a) et b) résultent du théorème 19.2. Pour c), nous avons l'isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} (\mathbf{Z}/r\mathbf{Z})^* \times (\mathbf{Z}/s\mathbf{Z})^*$$

donné par le lemme chinois. L'ordre d'un couple $(a,b) \in (\mathbf{Z}/r\mathbf{Z})^* \times (\mathbf{Z}/s\mathbf{Z})^*$ est clairement égal au PPCM des ordres des deux composantes. Ceci implique que l'ordre maximal d'un couple sera le PPCM des ordres maximaux atteints dans chaque composante. $\surd$

21. Résidus quadratiques

Définition 21.1 *Soit $n \geq 2$ un entier. Une classe $a \in (\mathbf{Z}/n\mathbf{Z})^*$ est un* résidu quadratique *modulo n si $a = b^2$ pour une classe b. Dans le cas contraire, la classe a est un* non-résidu quadratique.

Exemples. Dressons les listes des résidus quadratiques modulo quelques nombres premiers

$$\begin{array}{rcl} 2 & : & 1 \\ 3 & : & 1 \\ 5 & : & 1,4 \\ 7 & : & 1,2,4 \\ 11 & : & 1,3,4,5,9 \\ 13 & : & 1,3,4,9,10,12 \\ 17 & : & 1,2,4,8,9,13,15,16 \\ 19 & : & 1,4,5,6,7,9,11,16,17 \\ 23 & : & 1,2,3,4,6,8,9,12,13,16,18 \\ 29 & : & 1,4,5,6,7,9,13,16,20,22,23,24,25,28 \end{array}$$

Notons qu'il y a $(p-1)/2$ résidus quadratiques pour chacun de ces nombres premiers et que -1 est un résidu quadratique pour $5, 13, 29$.

Lemme 21.2 *Soit $p = 2l+1$ un nombre premier impair.*

a) Parmi les $2l$ éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ la moitié exactement sont des résidus quadratiques.

a) Pour tout $a \in (\mathbf{Z}/p\mathbf{Z})^*$ on a $a^l \equiv \pm 1\ (p)$. On $a^l \equiv 1\ (p)$ si et seulement si a est un résidu quadratique modulo p.

b) La classe de -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1\ (4)$.

Exemple 21.3 Le nombre 2011 est premier et congru à 3 modulo 4. Donc -1 n'est pas résidu quadratique modulo 2011. Par contre, à l'aide de l'algorithme de calcul rapide des puissances, on vérifie aisément que $1848^{1005} \equiv 1\ (2011)$. Donc 1848 est un résidu quadratique modulo 2011.

Démonstration. a) Nous savons que $(\mathbf{Z}/p\mathbf{Z})^*$ est isomorphe à $\mathbf{Z}/2l\mathbf{Z}$. Or ce dernier groupe contient exactement l classes multiples de 2.

b) Nous avons $(a^l)^2 \equiv a^{p-1} \equiv 1\ (p)$ d'après le petit théorème de Fermat (13.13). Donc $a^l \equiv \pm 1\ (p)$ (car l'équation $x^2 = 1$ admet exactement 2 solutions dans $\mathbf{Z}/p\mathbf{Z}$, d'après 17.3).

Si $a = b^2$, alors $a^k = b^{2k} = b^{p-1} = 1$ modulo p, par le petit théorème de Fermat. Réciproquement, si $a^l = 1$ modulo p, alors si g est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$, nous avons $a = g^{2k}$ pour un $k \in \mathbf{Z}$ d'après le lemme (17.3). Donc a est un carré.

c) D'après a), la classe de -1 est un résidu quadratique ssi $(-1)^l \equiv 1\ (p)$, c'est-à-dire que l est pair ou encore que $p = 2l+1$ vérifie $p \equiv 1\ (4)$.

$\surd$

Théorème 21.4 (Conjecture d'Euler) *Soit a un entier non nul et p un nombre premier impair. Le fait que a soit résidu quadratique modulo p ou non ne dépend que de la classe de p modulo $4a$.*

Remarque 21.5 La conjecture, due à Euler, fut démontrée pour la première fois par C. F. Gauss en 1796 sous le nom de 'théorème d'or'. Nous allons donner la démonstration dans une section ultérieure.

Exemples. Nous avons déjà vu que -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4, ou encore modulo $-4 = 4(-1)$.

D'après le théorème, le fait que 2 soit un carré modulo p ne dépend que de la classe de p modulo 8. Or 2 est non résidu quadratique pour 3 et 5, il est résidu quadratique pour 7 ($4^2 = 2$) et pour 17 ($6^2 = 2$). Donc 2 *est un carré modulo p ssi* $p \equiv \pm 1$ (8).

Nous verrons plus tard que le calcul des classes de nombres premiers p modulo lesquels a est un résidu quadratique peut toujours se ramener à $a = 2$ et $a = -1$.

22. Le symbole de Legendre

Définition 22.1 *Soit p un nombre premier et a un entier. On pose*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a \\ 1 & \text{si } a \text{ est résidu quadratique modulo } p \\ -1 & \text{si } a \text{ est non résidu quadratique modulo } p \end{cases}$$

On appelle symbole de Legendre *l'expression* $(\frac{a}{p})$.

Remarque 22.2 Par définition, le symbole de Legendre $(\frac{a}{p})$ ne dépend que de la classe de a modulo p.

Pour un nombre premier impair, onn a $(\frac{-1}{p}) = 1$ ssi p est congru à 1 modulo 4 et $(\frac{2}{p}) = 1$ ssi p est congru à ± 1 modulo 8. Si on tient à des formules explicites, on peut écrire

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} \quad (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

Lemme 22.3 *Soit $p = 2l + 1$ un nombre premier impair.*

a) On a $(\frac{a}{p}) \equiv (-1)^l$ (p).

b) On a $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ pour tous entiers a, b et $(\frac{a^2 b}{p}) = (\frac{b}{p})$ si a n'est pas divisible par p.

Démonstration. a) résulte du lemme 21.2 a) et b) de a). √

Définition 22.4 *Pour deux entiers a, b, on pose*

$$\theta(a, b) = \begin{cases} -1 & \text{si } a \equiv 3\ (4) \text{ et } b \equiv 3\ (4) \\ 1 & \text{sinon} \end{cases}$$

Remarque 22.5 On peut vérifier aisément que pour a et b impairs, on a

$$\theta(a, b) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

Théorème 22.6 (Loi de réciprocité quadratique) *Si p et q sont deux nombres premiers impairs distincts, on a*

$$(\frac{p}{q})(\frac{q}{p}) = \theta(p, q).$$

Remarque 22.7 Le théorème est équivalent à la conjecture d'Euler. Il signifie que $(\frac{p}{q}) = (\frac{q}{p})$ si p ou q est congru à 1 modulo 4, et $(\frac{p}{q}) = -(\frac{q}{p})$ dans le cas contraire.

Démonstration. On a toujours $p - q = 4a$ ou $p + q = 4a$ pour un $a \in \mathbf{Z}$. Supposons d'abord que $p - q = 4a$. Alors on a

$$(\frac{p}{q}) = (\frac{q + 4a}{q}) = (\frac{4a}{q}) = (\frac{a}{q}).$$

où nous avons utilisé le lemme 22.3. De l'autre côté, nous avons

$$(\frac{q}{p}) = (\frac{p - 4a}{p}) = (\frac{-4a}{p}) = (\frac{-1}{p})(\frac{a}{p}).$$

Or, d'après la conjecture d'Euler, nous avons $(\frac{a}{p}) = (\frac{a}{q})$. Puisque p et q ont même reste par 4, il s'ensuit que $\theta(p, q) = (\frac{-1}{p})$ ce qui termine la démonstration dans ce cas.

Supposons maintenant que $p + q = 4a$. Alors nous avons

$$(\frac{p}{q}) = (\frac{4a - q}{q}) = (\frac{4a}{q}) = (\frac{a}{q})$$

et de même

$$(\frac{q}{p}) = (\frac{4a - p}{p}) = (\frac{4a}{p}) = (\frac{a}{p}).$$

Donc d'après la conjecture d'Euler, nous avons $(\frac{p}{q}) = (\frac{q}{p})$. $\surd$

Résumé des propriétés du symbole de Legendre. *Les règles suivantes permettent de calculer tout symbole de Legendre (p et q sont des nombres premiers impairs distincts; a, a', b sont des entiers)*

(1) Modularité :

$$(\frac{a}{p}) = (\frac{a'}{p})$$

si $a \equiv a'\ (p)$.

(2) Multiplicativité :

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$$

(3) Réciprocité :

$$(\frac{p}{q}) = \begin{cases} -(\frac{q}{p}) & \textit{si } p \equiv 3\ (4) \textit{ et } q \equiv 3\ (4) \\ (\frac{q}{p}) & \textit{sinon} \end{cases}$$

(4) Valeurs particulières :

$$(\frac{-1}{p}) = \begin{cases} 1 & \textit{si } p \equiv 1\ (4) \\ -1 & \textit{si } p \equiv 3\ (4) \end{cases}, \qquad (\frac{2}{p}) = \begin{cases} 1 & \textit{si } p \equiv \pm 1\ (8) \\ -1 & \textit{sinon} \end{cases}.$$

Exemple 22.8 Nous montrons comment les règles ci-dessus permettent de calculer $(\frac{541}{2011})$:

$$\begin{aligned} (\frac{541}{2011}) &= (\frac{2011}{541}) \quad \text{(réciprocité, } 541 \equiv 1\ (4))) \\ &= (\frac{388}{541}) \quad \text{(modularité, } 2011 \equiv 388\ (541)) \\ &= (\frac{2}{541})^2 (\frac{97}{541}) \quad \text{(multiplicativité, } 388 = 2^2 \times 97) \\ &= (\frac{541}{97}) \quad \text{(réciprocité, } 541 \equiv 1\ (4)) \end{aligned}$$

$$
\begin{aligned}
&= (\frac{56}{97}) \quad \text{(modularité, } 541 \equiv 56\ (97)) \\
&= (\frac{7}{97})\,(\frac{2}{97})^3 \quad \text{(multiplicativité)} \\
&= (\frac{97}{7})\,(\frac{2}{97})^3 \quad \text{(réciprocité, } 97 \equiv 1\ (4)) \\
&= (\frac{-1}{7})\,(\frac{2}{97})^3 \quad \text{(modularité)} \\
&= -1 \quad \text{(valeurs particulières, } (\tfrac{-1}{7}) = -1,\ (\tfrac{2}{97}) = 1)
\end{aligned}
$$

23. Démonstration de la conjecture d'Euler

Lemme 23.1 *Soit $p = 2\,l+1$ un nombre premier impair et a un entier qui n'est pas divisible par p. Pour $1 \leq k \leq l$, soit r_k le reste de la division de ka par p et soit ν le nombre de restes $r_k > l$. Alors*

$$a^l \equiv (-1)^\nu\ (p)$$

et en particulier, a est un résidu quadratique modulo p si et seulement si ν est pair.

Démonstration. Si $a\,i \equiv \pm a\,j\ (p)$, alors comme a est inversible modulo p, nous avons $i \equiv \pm j\ (p)$ ce qui est impossible si i et j sont compris entre 1 et l. Donc si nous posons

$$s_i = \begin{cases} r_i & \text{si } 1 \leq r_i \leq l \\ p - r_i & \text{si } l < r_i \end{cases}$$

les s_i sont deux à deux distincts et compris entre 1 et l. Puisque ils sont au nombre de l, tout entier entre 1 et l est égal à un s_j. Nous avons

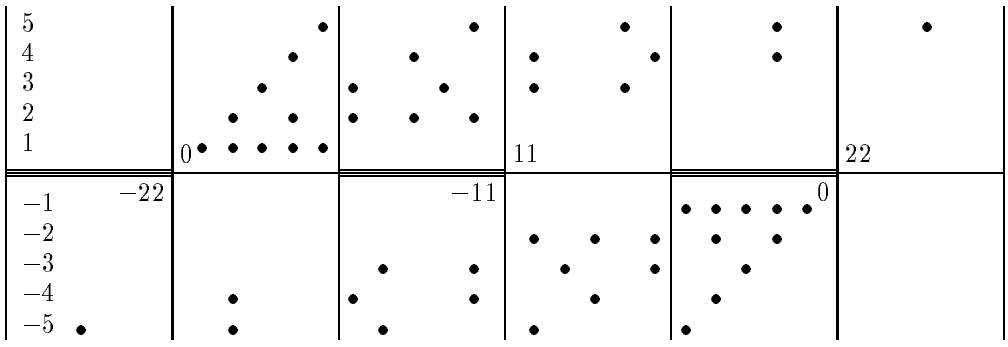
$$r_1 r_2 \cdots r_l \equiv (-1)^\nu s_1 s_2 \cdots s_l \equiv (-1)^\nu l\,!\ (p).$$

De l'autre côté, nous avons

$$r_1 r_2 \cdots r_l \equiv l\,!\ a^l\ (p).$$

Puisque $l\,!$ est inversible modulo p, nous obtenons l'affirmation. La dernière partie résulte du lemme précédent. $\surd$

Exemple 23.2 Prenons $p = 11$ et donc $l = 5$. Dans le dessin suivant, nous calculons ν pour a variant entre -5 et 5. Par exemple, la ligne qui commence par le nombre 2 comporte $l = 5$ points aux abscisses $2, 4, 6, 8, 10$. Le nombre de points qui se trouvent dans des intervalles 'sous-lignés' est égal à ν. Donc $\nu = 3$ et 2 est un non-résidu quadratique modulo 11. Les résidus quadratiques modulo 13 sont $-2, 1, 3, 4, 5$.



Théorème 23.3 (Conjecture d'Euler) *Soit a un entier non nul et p un nombre premier impair. Le fait que a soit résidu quadratique modulo p ou non ne dépend que de la classe de p modulo $4a$.*

Démonstration. D'après le lemme 23.1 et l'exemple qui le suit, il s'agit de compter le nombre ν de points ka, $1 \leq k \leq l$, qui se trouvent dans l'un quelconque des intervalles $I_i = [ip/2, (i+1)p/2]$, où i est impair et compris entre 1 et a. En effet, le dernier point, $la = (p-1)a/2$, se trouve dans l'intervalle $[(a-1)p/2, ap/2]$. Supposons que $p' = p + 4a$ et que ν' est le nombre de points correspondant (peu importe si p' n'est pas premier). Alors le nombre d'intervalles I_i' reste le même ($= a$), mais le nombre de points ka augmente de $l' - l = 2a$. Je dis que chacun des a intervalles I_i' comporte 2 points ka de plus que l'intervalle I_i correspondant. Ceci impliquera que $\nu' - \nu$ est pair et donc que $(-1)^{\nu'} = (-1)^{\nu}$. Comparons en effet l'intervalle I_i à l'intervalle I_i' : nous avons

$$\begin{aligned} I_i &= [i\,\frac{p}{2}, (i+1)\,\frac{p}{2}] \\ I_i' &= [i\,(\frac{p}{2} + 2a), (i+1)\,(\frac{p}{2} + 2a)] \\ &= [i\,\frac{p}{2} + 2ia, (i+1)\,\frac{p}{2} + 2ia] \cup [(i+1)\,\frac{p}{2} + 2ia, (i+1)\,\frac{p}{2} + 2ia + 2a]. \end{aligned}$$

L'intervalle I_i' est donc obtenu à partir de I_i par deux opérations : décalage de $2ia$ et rajout d'un intervalle disjoint de longueur $2a$ dont les extrémités ne sont pas multiples de a. Or le décalage d'un multiple de a laisse invariant le nombre de points ka contenus dans l'intervalle, et le rajout d'un intervalle disjoint de longueur $2a$ dont les extrémités ne sont pas multiples de a rajoute 2 points ka car tout intervalle de longueur $2a$ dont les extrémités ne sont pas des multiples de a comporte exactement 2 points ka (par mise à l'échelle, on peut supposer que $a = 1$: tout intervalle de longueur 2 dont les extrémités ne sont pas entières comporte exactement 2 points entiers.) $\surd$

24. Bibliographie

Les livres suivants peuvent servir à *approfondir* les connaissances sur certains sujets traités en cours. Le livre de Weiss [7] est rédigé de façon élémentaire et son contenu est relativement proche de celui du cours. Le livre de Gindikin [5] contient des biographies de mathématiciens et physiciens de la renaissance à nos jours et donne des explications élémentaires mais complètes d'un grand nombre de résultats qu'ils ont obtenus. Le chapitre sur Gauss est un trésor de perles d'arithmétique. Le cours de Michel Demazure [3] contient entièrement le programme de ce cours et le dépasse de loin. Il s'adresse à un public un peu plus avancé. Le livre d'Artin [9] est très complet, bien rédigé et peut servir du DEUG jusqu'à la maîtrise.

Les chiffres en gras se reportent à la bibliothèque de Mathématiques du second cycle, Tour 56, rez de chaussée.

References

[1] L. Koulikov, *Algèbre et théorie des nombres*, Chap. XI et XII, Moscou Ed. Mir, 1982. **10 KOU 82**.

[2] Paul-Jean Cahen, Touibi Chédly, *Arithmétique et Algèbre*, Scientifika, 1992. **03.5 CAH 92**.

[3] Michel Demazure, *Cours d'algèbre*, Notes d'un cours à l'Ecole Polytechnique en Majeure Algèbre et Informatique, Polycopié à paraître sous forme de livre chez Cassini Editeurs.

[4] Jacques Faraut, *Arithmétique : Cours, exercices et travaux pratiques sur micro-ordinateur*, Ellipse, 1990. **77.5 P FAR 90**.

[5] Simon Gindikin, *Horloges, pendules et mécanique céleste*, Diderot Editeur, 1995.

[6] Raymond Séroul, *math–info, Informatique pour mathématiciens, Chap. 2*, Interéditions, 1995.

[7] Edwin Weiss, *A first course in algebra and number theory*, Academic Press, 1971. **10 WEI 71**.

[8] Lindsay Childs, *A concrete introduction to higher algebra*, Undergraduate texts in Mathematics, Springer, 1979. **10 CHI 79**.

[9] Michael Artin, *Algebra*, Prentice Hall, 1991. **10 ART 91**.