MASTER MAIM (MATHÉMATIQUES GÉNÉRALES, 1ère année)

ARITHMÉTIQUE et COMBINATOIRE

COURS et EXERCICES

Emmanuel Fricain

- 2011–2012 -

La théorie des nombres est l'une des théories mathématiques les plus fascinantes car elle mêle à la fois des outils algébriques, des outils analytiques, des outils combinatoires, des outils géométriques et des outils probabilistes. L'objectif de ce cours d'introduction est d'illustrer cette diversité. Dans les trois premiers chapitres, nous traiterons de quelques questions élémentaires de nature plutôt algébrique (théorie des congruences, racines primitives et résidus quadratiques). Dans un quatrième chapitre, nous présenterons un résultat classique de Minkowski sur les réseaux de $\mathbb{R}^n$ et l'appliquerons au problème de la représentation des entiers en sommes de carrés. Ce théorème de Minkowski a donné naissance à ce qu'on appelle aujourd'hui la "théorie géométrique des nombres". Enfin dans les derniers chapitres, nous nous intéresserons au problème de la répartition des nombres premiers en utilisant diverses techniques d'analyse. Notamment nous introduirons la notion de séries de Dirichlet, si importante en théorie des nombres.

Les prérequis pour ce cours sont les cours d'algèbre et d'analyse de Licence (notamment le cours d'analyse complexe) et le cours d'algèbre de M1 sur les groupes et corps. Néanmoins, nous rappellerons le cas échéant les principales définitions et résultats utiles pour ce cours. On trouvera notamment une longue appendice d'arithmétique élémentaire qu'il est absolument indispensable de maitriser (notamment en vue de l'agrégation). Pour préparer ce cours, je me suis inspiré de notes de cours de Jean-Louis Nicolas que je tiens à remercier à cette occasion. Marc Deleglise m'a également légué sa précieuse "banque" d'exercices, qu'il en soit ici vivement remercié. Enfin, je me suis appuyé sur divers ouvrages ou cours en ligne dont voici une liste (non exhaustive) et que le lecteur pourra consulter pour des compléments ou plus de détails :

1. **Arithmetics**, Marc Hindry, Universitext, Springer, 2008. (pour le chapitre sur les résidus quadratiques et les sommes de Gauss).
2. **Elementary Methods in Number Theor**, Melvyn B. Nathanson, Graduate Texts in Mathematics, Springer, 2000.
3. **Théorie algébrique des nombres**, cours de Gaëtan Chenevier, cours en ligne : http ://www.math.polytechnique.fr/ chenevier/MAT552.html. (pour le chapitre sur la théorie géométrique des nombres).
4. **Introduction to Analytic Number Theory**, Tom Apostol, Undergraduate Texts in Mathematics, Springer, 1976.

Table des matières

Chapitre 1

Congruences

L'objectif de ce chapitre est de rappeler quelques notions et résultats élémentaires de théorie des congruences. Cette théorie conduit naturellement à introduire l'anneau $\mathbb{Z}/n\mathbb{Z}$ ainsi que le groupe de ses éléments inversibles (pour la multiplication), noté $(\mathbb{Z}/n\mathbb{Z})^*$. Nous rappelons la construction de ces objets et précisons leurs principales propriétés.

1.1 Quelques rappels sur les groupes finis

Soient G un groupe fini (noté multiplicativement) et H un sous-groupe de G. Un théorème de Lagrange affirme que le cardinal de H divise le cardinal de G. Maintenant, si g est un élément de G, alors il existe un plus petit entier $\omega \geq 1$ tel que $g^\omega = e$. Les éléments $e, g, g^2, \ldots, g^{\omega-1}$ sont alors tous distincts et l'ensemble

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{\omega-1}\}$$

est le plus petit sous-groupe de G contenant g. L'entier ω est appelé **l'ordre** de g. On vérifie facilement (en utilisant le théorème de la division euclidienne) que

$$g^m = e \Longleftrightarrow \omega | m.$$

En appliquant le théorème de Lagrange, on obtient immédiatement que ω divise le cardinal de G. En particulier, si G est un groupe de cardinal n, alors $g^n = e$ pour tout $g \in G$.

On rappelle qu'un groupe G est **cyclique** s'il existe $g \in G$ tel que le sous-groupe engendré par g est G tout entier. On dit dans ce cas que g est un **générateur** de G. Un élément g de G est un générateur de G si et seulement si l'ordre de g est maximal, c'est-à-dire exactement le cardinal de G.

Théorème 1.1.1 *Soit g un élément d'ordre n d'un groupe G. Pour tout entier naturel m, l'ordre de g^m est $n/(n,m)$, où (m,n) est le pgcd de m et n. En particulier, si G est un groupe cyclique d'ordre n et g un générateur de G, alors l'ensemble des générateurs de G est*

$$\{g^t : (t,n) = 1\}.$$

Preuve : Soit $d = (n,m)$ le pgcd de m et n, et écrivons $n = n'd$ et $m = m'd$. L'ordre de g^m est le plus petit entier naturel non nul k tel que

$$n|km \text{ ou encore } n'|km'.$$

Comme n' et m' sont premiers entre eux, la condition $n'|km'$ est satisfaite si et seulement si k est un multiple de $n' = n/d = n/(n,m)$. Ceci prouve le premier point.

L'élément g^t est générateur si et seulement si son ordre est n. Or d'après ce qui précède, l'ordre de g^t est $n/(n,t)$. On obtient donc que g^t est générateur si et seulement si $(t,n) = 1$.

□

Un autre résultat sur les groupes finis sera aussi utilisé.

Lemme 1.1.2 *Soient G un groupe fini commutatif et g, h deux éléments de G d'ordre respectif n et m. Si n et m sont premiers entre eux, alors l'élément gh est d'ordre mn.*

Preuve : Considérons l'intersection $M = \langle g \rangle \cap \langle h \rangle$. C'est un sous-groupe de $\langle g \rangle$ et $\langle h \rangle$. Le théorème de Lagrange implique alors que le cardinal de M divise n et m. Comme $(n,m) = 1$, on en déduit que nécessairement $M = \{e\}$. Vérifions maintenant que gh est d'ordre mn. Tout d'abord comme $gh = hg$, on a $(gh)^{mn} = g^{mn}h^{mn} = e$. Donc l'ordre de gh divise mn. Réciproquement si $(gh)^k = e$ alors $g^k = h^{-k} \in M$. Donc $g^k = h^k = e$. Ainsi $n|k$ et $m|k$. Une application du théorème 5.5.3 implique alors que le produit nm divise k. Finalement on conclut que l'ordre de gh est mn.

□

1.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soient $n \geq 2$ un entier fixé. On dit que les entiers a et b sont **congrus modulo** n, et on écrit

$$a \equiv b \,(\mathrm{mod}\, n),$$

si $a - b$ est un multiple de n. On vérifie que la relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$ compatible avec l'addition et la multiplication, c'est-à-dire que si $a \equiv a' \pmod{n}$ et si $b \equiv b' \pmod{n}$, alors

$$a + b \equiv a' + b' \pmod{n} \quad \text{et} \quad ab \equiv a'b' \pmod{n}.$$

Pour tout entier a, on note $a \bmod n$ la **classe de congruence** de a modulo n, et s'il n'y a pas d'ambiguité, on utilisera aussi la notation $\bar{a}$. Autrement dit,

$$a \bmod n = \bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ le quotient de $\mathbb{Z}$ avec cette relation d'équivalence.

Pour $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, on pose

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{et} \quad \bar{a}.\bar{b} = \overline{ab}.$$

On vérifie alors que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire. De plus, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est l'unique groupe cyclique à n éléments (à isomorphisme près) : il est engendré par $\bar{1}$, à savoir

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1}\}.$$

1.3 Congruences linéaires et théorème des restes chinois

Le théorème suivant, bien qu'élémentaire, est très utile pour résoudre des congruences linéaires.

Théorème 1.3.1 *Soient $a, b \in \mathbb{Z}$, $n \geq 2$. Soit $d = (a, n)$ le pgcd de a et n. L'équation*

$$ax \equiv b \pmod{n} \tag{1.1}$$

a (au moins) une solution si et seulement si d divise b. Si d divise b, alors l'équation (1.1) a exactement d solutions entières modulo n.

Preuve : L'équation (1.1) possède une solution si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que

$$ax - b = ny,$$

ou de manière équivalente

$$b = ax - ny.$$

Comme $(a, n) = d$, la dernière équation admet des solutions si et seulement si d divise b (voir appendice, théorème 5.4.1).

Maintenant si x et x_1 sont solutions de (1.1), on a

$$a(x_1 - x) = ax_1 - ax \equiv 0 \pmod{n},$$

d'où

$$a(x_1 - x) = nz$$

pour un certain entier z. On a alors $\frac{a}{d}(x_1 - x) = \frac{n}{d}z$. Comme $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, le lemme de Gauss implique alors que $\frac{n}{d}$ divise $x_1 - x$. D'où $x_1 = x + k\frac{n}{d}$ pour un certain $k \in \mathbb{Z}$. Autrement dit

$$x_1 \equiv x \left(\mod \frac{n}{d}\right).$$

De plus, chaque entier x_1 de cette forme est une solution de (1.1). Remarquons maintenant que les d entiers

$$x + i\frac{n}{d}, \qquad 0 \leq i \leq d-1,$$

sont deux à deux incongrus modulo n. En conséquence, l'équation (1.1) possède d solutions entières modulo n.

□

On en déduit immédiatement le corollaire suivant :

Corollaire 1.3.2 *Soient $a, b \in \mathbb{Z}$, $n \geq 2$ et supposons que $(a, n) = 1$. L'équation $ax \equiv b \pmod{n}$ a une unique solution modulo n.*

Dans la suite, nous allons nous intéresser au système de congruences suivant :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases}$$

où $k \geq 2$, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ et $m_1, m_2, \ldots, m_k$ sont des entiers ≥ 2.

Commençons par le cas $k = 2$.

Théorème 1.3.3 (des restes chinois) *Soient $a, b \in \mathbb{Z}$ et $m, n \geq 2$. Le système*

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

admet une solution x si et seulement si

$$a \equiv b \pmod{(m, n)}.$$

De plus, dans ce cas, si x est une solution du système (S), alors y est une solution de (S) si et seulement

$$y \equiv x \pmod{[m, n]}\ [1].$$

1. Dans tout le cours, $[m, n]$ désigne le ppcm de m et n et (m, n) désigne le pgcd de m et n.

Preuve : Si x est solution du système (S), alors il existe deux entiers u, v tels que $x = a + mu = b + nv$. D'où

$$a - b = nv - mu \equiv 0 \,(\mathrm{mod}(m, n)).$$

Réciproquement, si $a \equiv b \,(\mathrm{mod}(m, n))$, alors par la relation de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $a - b = nv - mu$. D'où $x := a + mu = b + nv$ est une solution du système (S). Cela conclut la première partie du théorème. Maintenant si x est une solution de (S), alors un entier y est solution de (S) si et seulement si

$$\begin{cases} y \equiv a \equiv x \,(\mathrm{mod}\, m) \\ y \equiv b \equiv x \,(\mathrm{mod}\, n) \end{cases}.$$

Par conséquent, $y - x$ est un multiple de m et n, donc de $[m, n]$. Autrement dit, $y \equiv x \,(\mathrm{mod}[m, n])$. Réciproquement, si $y \equiv x \,(\mathrm{mod}[m, n])$, alors $y \equiv x \,(\mathrm{mod}\, m)$ et $y \equiv x \,(\mathrm{mod}\, n)$. Donc y est solution de (S).

□

Remarque 1.3.4 On voit d'après la preuve du théorème 1.3.3 que si $a \equiv b \,(\mathrm{mod}(m, n))$, alors on construit une solution particulière du système (S) de la façon suivante. En utilisant l'algorithme d'Euclide, on commence par chercher une solution au système de Bezout suivant $d = mu + nv$ où $d = (m, n)$. Ensuite comme $a \equiv b \,(\mathrm{mod}\, d)$, il existe $k \in \mathbb{Z}$ tel que $a = b + dk$. Il suffit alors de considérer $x_0 = b + nkv$. L'ensemble des solutions du système (S) est alors donné par $x_0 \,\mathrm{mod}([m, n])$.

Théorème 1.3.5 (des restes chinois) *Soient k un entier ≥ 2, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ et $m_1, m_2, \ldots, m_k$ des entiers ≥ 2. Supposons que les entiers $m_1, m_2, \ldots, m_k$ soient deux à deux premiers entre eux. Notons $m = m_1 m_2 \ldots m_k$. Alors le système*

$$(S) \begin{cases} x \equiv a_1 \,(\mathrm{mod}\, m_1) \\ x \equiv a_2 \,(\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv a_k \,(\mathrm{mod}\, m_k), \end{cases}$$

possède une solution. De plus, si x est une solution du système (S), un entier y est aussi solution de (S) si et seulement si $y \equiv x \,(\mathrm{mod}\, m)$.

Preuve : On raisonne par récurrence sur l'entier k. Le cas $k = 2$ provient du lemme car $(m_1, m_2) = 1$ et $[m_1, m_2] = m_1 m_2$. Soit $k \geq 3$ et supposons que le résultat soit vrai pour $k - 1$ congruences. Alors il existe un entier z tel que $z \equiv a_i \,(\mathrm{mod}\, m_i)$, $1 \leq i \leq k - 1$. Comme $m_1, m_2, \ldots, m_k$ sont des entiers deux à deux premiers entre eux, on a $(m_1 m_2 \ldots m_{k-1}, m_k) = 1$. Donc le cas $k = 2$ permet de dire qu'il existe un entier x tel que

$$\begin{cases} x \equiv z \,(\mathrm{mod}\, m_1 m_2 \ldots m_{k-1}) \\ x \equiv a_k \,(\mathrm{mod}\, m_k). \end{cases}$$

D'où $x \equiv a_i \pmod{m_i}$, pour tout $1 \leq i \leq k$. Ainsi x est solution de (S). Ceci prouve la première partie du théorème. Maintenant, si y est une solution du système, alors $x - y$ est divisible par m_i, $1 \leq i \leq k$. Comme $m_1, m_2, \ldots, m_k$ sont deux à deux premiers entre eux, l'entier $x - y$ est divisible par $m_1 m_2 \ldots m_k$. Cela complète la preuve du résultat.

□

Remarque 1.3.6 Pour résoudre le système (S), on peut procéder de la façon suivante : pour chaque entier i, les entiers m_i et $\hat{m}_i = \frac{m}{m_i} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$ sont premiers entre eux et donc d'après le théorème de Bezout, on peut trouver (en utilisant par exemple l'algorithme d'Euclide) des entiers u_i et v_i tels que $u_i m_i + v_i \hat{m}_i = 1$. Si on pose $e_i = v_i \hat{m}_i$, alors on a

$$e_i \equiv 1 \pmod{m_i}$$

et

$$e_i \equiv 0 \pmod{m_j} \text{ pour } j \neq i.$$

Une solution particulière de (S) est alors donnée par $x_0 = \sum_{i=1}^{k} a_i e_i$. Les autres solutions sont congrues à ce x_0 modulo m.

On peut donner une formulation plus abstraite du théorème des restes chinois.

Corollaire 1.3.7 *Soient $m_1, m_2, \ldots, m_k \geq 2$ des entiers deux à deux premiers entre eux et notons $m = m_1 m_2 \ldots m_k$. Alors l'application*

$$\begin{array}{rccc} \psi : & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ & x \bmod m & \longmapsto & (x \bmod m_1, \ldots, x \bmod m_k) \end{array}$$

définit un isomorphisme d'anneaux unitaires.

Preuve : Remarquons tout d'abord que si $x \bmod m = y \bmod m$, alors $x \bmod m_i = y \bmod m_i$ pour tout $1 \leq i \leq k$, donc l'application ψ est bien définie. On vérifie que

$$\psi(x \bmod m + y \bmod m) = \psi(x \bmod m) + \psi(y \bmod m),$$

$$\psi((x \bmod m)(y \bmod m)) = \psi(x \bmod m)\psi(y \bmod m),$$

et $\psi(1_{\mathbb{Z}/m\mathbb{Z}}) = 1_{\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}}$. Donc ψ est un morphisme d'anneaux unitaires. De plus, étant donné $(a_1 \bmod m_1, a_2 \bmod m_2, \ldots, a_k \bmod m_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, il existe d'après le théorème des restes chinois un élement $x \in \mathbb{Z}$ tel que

$$x \equiv a_i \pmod{m_i} \qquad 1 \leq i \leq k.$$

D'où $x \bmod m_i = a_i \bmod m_i$, $1 \leq i \leq k$, c'est-à-dire

$$\psi(x \bmod m) = (a_1 \bmod m_1, a_2 \bmod m_2, \ldots, a_k \bmod m_k).$$

De plus, le théorème des restes chinois implique également que la solution x est unique modulo m. Ainsi ψ est un isomorphisme d'anneaux unitaires.

□

1.4 Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ et l'indicatrice d'Euler

L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication est un groupe. On le note $(\mathbb{Z}/n\mathbb{Z})^*$. Le résultat suivant caractérise ses éléments inversibles.

Proposition 1.4.1 *Pour que l'élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ soit inversible il faut et il suffit que $(a, n) = 1$. Dans ce cas, le calcul de l'inverse de $\bar{a}$ se fait à l'aide de l'algorithme d'Euclide étendu appliqué au couple (a, n).*

Preuve : Si $\bar{a}$ est inversible, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$. Il existe donc $v \in \mathbb{Z}$ tel que $ab - 1 = vn$, ou $ba - vn = 1$. Par le théorème de Bezout, a et n sont premiers entre eux. Réciproquement, si a et n sont premiers entre eux, il existe u et v entiers tels que $au + nv = 1$. Cela donne dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{au} = \overline{1 - nv} = \bar{1}$. Donc $\bar{a}$ est inversible, d'inverse $\bar{u}$.

□

On obtient immédiatement le corollaire suivant.

Corollaire 1.4.2 *Pour que l'anneau $\mathbb{Z}/p\mathbb{Z}$ soit un corps il faut et il suffit que p soit un nombre premier. On note parfois $\mathbf{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.*

La fonction **indicatrice d'Euler** φ associe à un entier $n \geq 2$ l'entier $\varphi(n)$ défini par

$$\varphi(n) = \operatorname{card}\left((\mathbb{Z}/n\mathbb{Z})^*\right).$$

Autrement dit, d'après la proposition 1.4.1, on a

$$\varphi(n) = \operatorname{card}\{a : 0 \leq a \leq n - 1 \,\&\, (a, n) = 1\}. \tag{1.2}$$

Proposition 1.4.3 *Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. On a*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

En particulier, $\varphi(p) = p - 1$.

Preuve : On a d'après (1.2)

$$\varphi(p^\alpha) = \text{card}\{a : 0 \leq a \leq p^\alpha - 1 \,\&\, (a, p^\alpha) = 1\}.$$

On vérifie facilement que si $0 \leq a \leq p^\alpha - 1$, alors $(a, p^\alpha) > 1$ si et seulement si $p|a$. Or les multiples de p dans l'intervalle $[\![0, p^\alpha - 1]\!]$ sont

$$0, p, 2p, \ldots, p(p^{\alpha-1} - 1).$$

Il y en a donc $p^{\alpha-1}$. D'où $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

□

Lemme 1.4.4 *Soient $m, n \geq 2$. Si $(m, n) = 1$, alors $\varphi(mn) = \varphi(n)\varphi(m)$.*

Preuve : Remarquons que si A_1, A_2, A_3 sont trois anneaux unitaires tel qu'il existe un isomorphisme $\psi : A_1 \longrightarrow A_2 \times A_3$, alors $\psi(A_1^*) = A_2^* \times A_3^*$, où A_i^* désigne le groupe des éléments inversibles de A_i, $i = 1, 2, 3$. En particulier, A_1^* est isomorphe à $A_2^* \times A_3^*$. Il suffit de combiner ce résultat et le corollaire 1.3.7 pour obtenir que les groupes $(\mathbb{Z}/mn\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ sont isomorphes. Ils ont donc même cardinal, ce qui donne le résultat.

□

Théorème 1.4.5 *Soit $n \geq 2$. On a*

$$\varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ p|n}} \left(1 - \frac{1}{p}\right),$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers.

Preuve : Soit $n = p_1^{r_1} \ldots p_k^{r_k}$ la décomposition canonique de n en produits de facteurs premiers. D'après le lemme 1.4.4, on a

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i}).$$

Or, avec la proposition 1.4.3, $\varphi(p_i^{r_i}) = p^{r_i} - p_i^{r_i - 1} = p_i^{r_i}(1 - \frac{1}{p_i})$, ce qui donne

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

□

1.5 Un théorème d'Euler et de Fermat

Théorème 1.5.1 (Euler) *Soient $n \geq 2$ et $a \in \mathbb{Z}$ tel que $(a, n) = 1$. Alors*

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

Preuve : On sait que l'ordre du sous-groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$. D'autre part, comme $(a, n) = 1$, la proposition 1.4.1 implique que $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et donc est un élément de $(\mathbb{Z}/n\mathbb{Z})^*$. Le théorème de Lagrange affirme alors que l'ordre de $\bar{a}$ divise l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$, ce qui implique en particulier que

$$\overline{a^{\varphi(n)}} = \bar{a}^{\varphi(n)} = \bar{1}.$$

Le résultat suit immédiatement.

□

On en déduit alors ce qu'on appelle le "petit théorème de Fermat".

Théorème 1.5.2 (Fermat) *Soient p un nombre premier et $a \in \mathbb{Z}$. On a*

$$a^p \equiv a \pmod{p}.$$

De plus, si p ne divise pas a, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Preuve : Si p est premier et ne divise pas a, alors on a $(a, p) = 1$ et $\varphi(p) = p - 1$. Le théorème d'Euler implique alors que

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

En multipliant cet congruence par a, on obtient que $a^p \equiv a \pmod{p}$. Si p divise a, alors on a clairement

$$a^p \equiv 0 \equiv a \pmod{p}.$$

□

1.6 Sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

La description des sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ est assez simple. Comme ici le groupe est additif, il faut prendre garde au fait que l'ordre d'un élément $x \bmod n$ est défini comme le plus petit entier $d \geq 1$ tel que $dx \equiv 0 \pmod{n}$. De plus, dans ce cas, les éléments $\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(d-1)x}$ sont tous distincts et

$$\langle x \rangle = \{\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(d-1)x}\}$$

est le plus petit sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ contenant $\bar{x}$. De plus, si $k \geq 1$, on a

$$k\bar{x} = \bar{0} \Longleftrightarrow k|d.$$

Lemme 1.6.1 *Soient x un entier et $n \geq 2$. L'élément $x \bmod n$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si $x \bmod n$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : Supposons que $x \bmod n$ soit un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Alors

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(n-1)x}\}$$

et donc il existe un entier $0 \leq k \leq n-1$ tel que $k\bar{x} = \bar{k}\bar{x} = \bar{1}$. D'où $x \bmod n$ est inversible d'inverse $k \bmod n$. Réciproquement, supposons que $x \bmod n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et notons d l'ordre de $x \bmod n$ dans le groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Alors $dx \equiv 0 \,(\bmod n)$. Autrement dit, n divise dx. Comme $x \bmod n$ est inversible, on a d'après la proposition 1.4.1, $(x,n) = 1$. Le lemme de Gauss implique alors que n divise d. Mais d'autre part, d'après le théorème de Lagrange, d divise n et donc $d = n$. Finalement on obtient que $x \bmod n$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$.

□

On déduit en particulier du lemme 1.6.1 que

$$\varphi(n) = \text{card}\{g : g \text{ générateur de } (\mathbb{Z}/n\mathbb{Z},+)\}. \tag{1.3}$$

Proposition 1.6.2 *Soit $n \geq 2$. Pour chaque entier $d \geq 1$ divisant n, il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ d'ordre d, c'est le sous-groupe cyclique engendré par la classe de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : Supposons que $n = kd$. Alors l'élément $x = \bar{k}$ est d'ordre d. En effet, d'une part, on a

$$dx = d\bar{k} = \overline{dk} = \bar{n} = \bar{0}.$$

D'autre part, si $cx = 0$, alors $\overline{ck} = \bar{0}$. Autrement dit, n divise ck. Ceci implique que d divise c. Par conséquent, x est bien d'ordre d. Ainsi, le sous-groupe $\langle x \rangle$ est d'ordre d. Montrons que c'est le seul. Soit donc H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ d'ordre d. Notons $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. On sait que $s^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. Donc il existe un entier $m \in \mathbb{N}$ tel que $s^{-1}(H) = m\mathbb{Z}$. Par conséquent, s étant surjective, on a $H = s(s^{-1}(H)) = s(m\mathbb{Z}) = \langle \bar{m} \rangle$. Comme l'ordre de H est d, on a $d\bar{m} = \bar{0}$. Donc $n|dm$, c'est-à-dire $k|m$. Ceci implique que $H = \langle \bar{m} \rangle \subset \langle \bar{k} \rangle$. Or l'ordre du sous-groupe engendré par $\bar{k}$ est d'ordre d, ce qui implique que

$$H = \langle \bar{k} \rangle.$$

□

Corollaire 1.6.3 *Soit $n \geq 2$. On a*

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

Preuve : On écrit

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} E_d,$$

où $E_d = \{x \bmod n : x \bmod dn \text{ est d'ordre } d\}$ et la réunion est disjointe. D'où

$$n = \sum_{d|n} \text{card}(E_d).$$

Or $x \bmod n \in E_d$ si et seulement si $x \bmod n$ est générateur d'un sous-groupe d'ordre d et d'après la proposition 1.6.2, ce sous-groupe d'ordre d est unique et isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Ainsi avec (1.3), on obtient que

$$\text{card}(E_d) = \text{card}\{g : g \text{ générateur de } (\mathbb{Z}/n\mathbb{Z}, +)\} = \varphi(d),$$

ce qui donne le résultat.

□

1.7 Exercices

Exercice 1.7.1 Calculer l'inverse de 13 modulo 100.

Exercice 1.7.2 Résoudre les équations

$$19x \equiv 2 \pmod{140} \qquad \text{et} \qquad 57x \equiv 87 \pmod{105}.$$

Exercice 1.7.3 Résoudre $42x + 150y = 18$.

Exercice 1.7.4

1. Résoudre $6u + 5z = 10$.
2. Résoudre $4x + 5y = u$.
3. En déduire les solutions de $24x + 30y + 5z = 10$.

Exercice 1.7.5 Soit p un nombre premier. Montrer que

$$x^2 \equiv 1 \,(\text{mod}\, p)$$

si et seulement si

$$x \equiv \pm 1 \,(\text{mod}\, p).$$

Exercice 1.7.6 (Théorème de Wilson) Soit p un nombre premier. Montrer que

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p).$$

Indication : vérifier d'abord le résultat pour $p = 2, 3$. On suppose alors que $p \geq 5$. Montrer que pour tout $a \in \{1, 2, \ldots, p-1\}$, il existe $a^\sharp \in \{1, 2, \ldots, p-1\}$ tel que $aa^\sharp \equiv 1 \,(\mathrm{mod}\, p)$. Remarquer alors que $a = a^\sharp$ si et seulement si $a = 1$ ou $a = p-1$ (voir exercice 1.7.5). Partitionner alors l'ensemble $\{2, \ldots, p-2\}$ en $(p-3)/2$ pairs d'entiers $(a_i, a_i^\sharp)$ tels que $a_i a_i^\sharp \equiv 1 \,(\mathrm{mod}\, p)$ pour $1 \leq i \leq (p-3)/2$. Conclure.

Exercice 1.7.7 Le produit de trois entiers consécutifs peut–il être un carré ?

Exercice 1.7.8

1. Montrer que, pour tout $n \in \mathbb{N}$, $n^{13} - n$ est multiple de 455.
2. Montrer qu'on peut améliorer ce résultat, c'est-à-dire qu'il existe un multiple non trivial de 455 qui divise tous les $n^{13} - n$.
3. En admettant que si p est un nombre premier, il existe un élément d'ordre $p-1$ dans $\mathbf{F}_p$, quel est le plus grand entier m qui divise tous les $n^{13} - n$?

Exercice 1.7.9 On définit la suite des nombres de Fermat par $F_n = 2^{2^n} + 1$.

1. Montrer que les F_n sont deux à deux premiers entre eux.
   Indication : si $m < n$ alors F_m divise $F_n - 2$.
2. En déduire qu'il existe une infinité de nombres premiers.

Exercice 1.7.10 Prouver qu'il existe une infinité de premiers de la forme $4k - 1$. Prouver de la même façon qu'il existe une infinité de nombres premiers de la forme $6k - 1$.

Exercice 1.7.11 Expliciter un n tel que $n, n+1, n+2, \ldots, n+9$ soient tous non premiers.

Indication : on pourra traduire le problème comme un système de congruences et utiliser le théorème des restes chinois.

Exercice 1.7.12 a et b sont premiers entre eux et $N \in \mathbb{N}$. On considère l'équation

$$ax + by = N \qquad (E)$$

1. Montrer que si N est assez grand l'équation (E) a une solution en entiers naturels.
2. Montrer que si $N = (a-1)(b-1) - 1$ l'équation (E) n'a pas de solutions en entiers naturels.

3. Montrer que si $N \geq (a-1)(b-1)$ l'équation (E) a une solution en entiers naturels.

Exercice 1.7.13 Soient $x_1, x_2, \ldots, x_n$ des entiers relatifs. Montrer qu'il existe i, j entiers, $1 \leq i < j \leq n$ tels que $x_i + x_{i+1} + \cdots + x_j \equiv 0 \pmod{n}$.

Indication : on pourra introduire

$$S_j = \sum_{0<i\leq j} x_j \bmod n$$

et appliquer le principe des tiroirs de Dirichlet.

Exercice 1.7.14 Vérifier que les 4 derniers chiffres (en base 10) de 9376^2 sont 9376. Déterminer tous les entiers x, $0 \leq x < 10000$ tels que $x^2 \equiv x \pmod{10000}$?

Indication : on pourra remarquer que x est solution de $X^2 - X \equiv 0 \pmod{N}$ si et seulement si $1 - x$ est solution.

Exercice 1.7.15 Résoudre le système de congruences

$$\begin{cases} 2x & \equiv & 3 & \pmod 5 \\ 4x & \equiv & 3 & \pmod 7 \\ 3x & \equiv & 5 & \pmod 8 \end{cases}$$

Exercice 1.7.16 Trouver les deux derniers chiffres de $39^{39^{39}}$. Même question avec $17^{17^{17}}$.

Exercice 1.7.17 Montrer que si n est impair alors $n \mid 2^{n!} - 1$.

Exercice 1.7.18 Pour un nombre réel x, on désigne par $\lfloor x \rfloor$ la partie entière de x, c'est-à-dire le plus petit entier k satisfaisant

$$k \leq x < k + 1.$$

Si $a \in \mathbb{Z}^*$ et p est un nombre premier, on appelle **valuation p-adique de a** le plus grand entier $\alpha \in \mathbb{N}$ tel que a est divisible par p^α mais pas par $p^{\alpha+1}$.

Soit n un entier positif ou nul.

1. Démontrer la formule de Legendre :

$$v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots \lfloor \frac{n}{p^k} \rfloor + \cdots$$

2. Prouver que chacun des termes de la suite $\left(\lfloor \frac{n}{p^k} \rfloor \right)$ est le quotient de la division euclidienne du précédent par p.

Exercice 1.7.19 Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers, où $p_1 < p_2 < \dots < p_k$.

1. Montrer que $k \leq \dfrac{\log n}{\log 2}$.
2. Pour $1 \leq i \leq k$, montrer que $p_i \geq i + 1$.
3. En déduire que
$$\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}.$$

Exercice 1.7.20 Un nombre entier m est appelé un **nombre de Carmichael** s'il vérifie les deux propriétés suivantes :

(i) m n'est pas premier ;

(ii) pour tout entier a premier avec m, on a
$$a^{m-1} \equiv 1 \pmod{m}.$$

Démontrer que $m = 561$ est un nombre de Carmichael (c'est en fait le plus petit nombre de Carmichael).

Indication : on pourra utiliser le théorème des restes chinois.

Exercice 1.7.21 Soit m entier tel que $6m + 1$, $12m + 1$, $18m + 1$ soient premiers. Démontrer que $n = (6m + 1)(12m + 1)(18m + 1)$ est un nombre de Carmichael.

Exercice 1.7.22 Soit n un entier non premier tel que

1. n est impair, sans facteurs carrés.
2. Pour tout diviseur premier p de n, $p - 1$ divise $n - 1$.

Démontrer que n est un nombre de Carmichael.

Exercice 1.7.23 Le but de cet exercice est de démontrer que la condition suffisante, obtenue dans l'exercice précédent pour qu'un entier soit un nombre de Carmichael, est aussi nécessaire. Considérons donc n un entier dont la factorisation (canonique) s'écrit
$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$
et supposons que n est un nombre de Carmichael.

1. Soit a un entier premier avec n. Prouver que son ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est un diviseur de $n - 1$.
2. Soit p un diviseur premier impair de n et $\alpha = v_p(n)$ la valuation p-adique de n.

(a) Prouver qu'il existe un entier a, premier avec n, dont l'ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $p^{\alpha-1}(p-1)$.

Indication : utiliser le fait que si p est un nombre premier impair, alors $(\mathbb{Z}/p^\alpha Z)^*$ est cyclique et utiliser le théorème des restes chinois.

(b) En déduire que $\alpha = 1$, que $p-1$ est un diviseur de $n-1$ et enfin que n est impair.

3. Démontrer qu'une puissance de 2 n'est jamais un nombre de Carmichael.

4. Déduire des questions précédentes que

   (a) n est impair, sans facteurs carrés.

   (b) Pour tout diviseur premier p de n, $p-1$ divise $n-1$.

Chapitre 2

Racines primitives

Ce chapitre est consacré à la notion importante de racines primitives, c'est-à-dire de l'existence d'un générateur pour le groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

2.1 Quelques rappels sur les équations diophantiennes polynomiales

Le résultat classique suivant affirme qu'un polynôme de degré n dans $\mathbf{F}_p[x]$ admet au plus n racines distinctes.

Théorème 2.1.1 (Lagrange, 1768) *Soient p un nombre premier, $a_1, a_2, \ldots, a_n$ des nombres entiers tels que p ne divise pas a_n. Alors l'équation*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p} \tag{2.1}$$

a au plus n solutions modulo p.

Preuve : On raisonne par récurrence sur n. Pour $n = 1$, on a

$$a_1 x \equiv -a_0 \pmod{p}.$$

Comme p ne divise pas a_1, on a $(a_1, p) = 1$ et donc a_1 est inversible modulo p. Autrement dit, il existe $a_1^{-1} \in \mathbb{Z}$ tel que $a_1^{-1}a_1 \equiv 1 \pmod{p}$. D'où

$$x \equiv -a_1^{-1}a_0 \pmod{p}.$$

Ainsi l'équation (2.1) possède une solution. Supposons que le résultat soit vrai au rang $n-1$. Soit x, x_1 deux solutions de (2.1). Alors

$$a_n(x^n - x_1^n) + a_{n-1}(x^{n-1} - x_1^{n-1}) + \cdots + a_1(x - x_1) \equiv 0 \pmod{p}.$$

En factorisant, on obtient

$$(x - x_1)Q(x) \equiv 0 \pmod{p},$$

où Q est un polynôme de degré égal à $n-1$ (dont le coefficient du terme en x^{n-1} est a_n). D'autre part, rappelons que p étant premier, on a $ab \equiv 0 \pmod{p}$ si et seulement si $a \equiv 0 \pmod{p}$ ou $a \equiv 0 \pmod{p}$. Ainsi on obtient que $x \equiv x_1 \pmod{p}$ ou $Q(x) \equiv 0 \pmod{p}$. D'après l'hypothèse de récurrence, l'équation $Q(x) \equiv 0 \pmod{p}$ possède au plus $n-1$ solutions donc l'équation (2.1) possède au plus n solutions modulo p.

□

On peut préciser le théorème de Lagrange dans un cas particulier important pour la suite.

Théorème 2.1.2 *Soit p un nombre premier et d un entier naturel tel que $d|(p-1)$. Alors l'équation*

$$x^d \equiv 1 \pmod{p}$$

a exactement d solutions modulo p.

Preuve : Ecrivons $p-1 = dk$, $k \in \mathbb{N}$. D'après le théorème de Fermat, l'équation

$$x^{p-1} \equiv 1 \pmod{p}$$

a exactement $p-1$ solutions modulo p. D'autre part,

$$x^{p-1} - 1 = x^{dk} - 1 = (x^d - 1)(x^{(k-1)d} + x^{(k-2)d} + \cdots + 1).$$

D'où

$$x^{p-1} \equiv 1 \pmod{p} \Longleftrightarrow x^d \equiv 1 \pmod{p} \text{ ou } x^{(k-1)d} + x^{(k-2)d} + \cdots + 1 \equiv 0 \pmod{p}.$$

D'après le théorème de Lagrange, l'équation

$$x^{(k-1)d} + x^{(k-2)d} + \cdots + 1 \equiv 0 \pmod{p}$$

a au plus $(k-1)d$ solutions modulo p et l'équation

$$x^d \equiv 1 \pmod{p}$$

a au plus d solutions modulo p. Comme au total, il y a $p-1 = (k-1)d+d$ solutions, on en déduit le résultat.

□

2.2 Racines primitives

Définition 2.2.1 *Soit $n \geq 2$. Un entier a est appelé une* **racine primitive** *modulo n si $(a,n) = 1$ et l'ordre de $a \bmod n$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$.*

Notons que si $(a,n)=1$, l'ordre de $a \bmod n$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ divise toujours $\varphi(n)$. Si a est une racine primitive modulo n, alors les $\varphi(n)$ entiers $1, a, a^2, \ldots, a^{\varphi(n)-1}$ sont premiers avec n et sont deux à deux incongrus modulo n. On a en particulier

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{1}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\varphi(n)-1}\}.$$

Autrement dit, un entier a premier avec n est une racine primitive de n si et seulement si $\bar{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^*$. Notons que si a est une racine primitive de n, alors tout entier de la forme $a+kn$, $k \in \mathbb{Z}$, est aussi une racine primitive de n.

Exemples :

(a) 3 est une racine primitive de 7 : on vérifie que $3 \bmod 7$ est d'ordre 6 dans $(\mathbb{Z}/7\mathbb{Z})^*$.

(b) 3 est une racine primitive de 10 : $3 \bmod 10$ est d'ordre 4 dans $(\mathbb{Z}/10\mathbb{Z})^*$.

(c) Certains entiers n'ont pas de racines primitives : ainsi $n=8$ n'a pas de racines primitives car aucun entier a tel que $(a,8)=1$ n'est d'ordre 4 modulo 8. On vérifie que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 (\bmod 8)$.

Par définition, l'entier n admet une racine primitive si et seulement le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique. Le résultat suivant montre que c'est le cas si $n=p$ est un nombre premier.

Théorème 2.2.2 (Gauss) *Soit p un nombre premier et $d \in \mathbb{N}$ tel que $d|(p-1)$. Alors il existe exactement $\varphi(d)$ classes modulo p d'ordre d. En particulier, l'entier p admet $\varphi(p-1)$ racines primitives incongrues modulo p.*

Preuve : On raisonne par récurrence sur d. Le cas $d=1$ est trivial. Supposons le résultat correct pour tout $d'|(p-1)$, avec $1 \leq d' < d$. D'après le théorème 2.1.2, l'équation $x^d \equiv 1 (\bmod p)$ a d solutions modulo p. Parmi ces solutions, d'après l'hypothèse de récurrence, le nombre de classes modulo p d'ordre $< d$ est

$$\sum_{\substack{d'<d \\ d'|d}} \varphi(d').$$

On en déduit donc qu'il y a $d - \sum_{\substack{d'<d \\ d'|d}} \varphi(d')$ solutions d'ordre d. Or d'après le corollaire 1.6.3, on a

$$d = \sum_{d'|d} \varphi(d').$$

D'où on en déduit qu'il y a $\varphi(d)$ classes modulo p d'ordre d. Le résultat est donc prouvé par récurrence.

Comme une racine primitive correspond à une classe modulo p d'ordre $p-1$, on en déduit qu'il y a $\varphi(p-1)$ racines primitives incongrues modulo p.

□

Si a est une racine primitive de p, alors on sait d'après le théorème 1.1.1 que les autres racines primitives sont de la forme a^k avec $(k, p-1) = 1$.

On peut reformuler ce qui précède sous la forme suivante :

Corollaire 2.2.3 *Soit p un nombre premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$. Il admet $\varphi(p-1)$ générateurs. Si g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, alors les autres générateurs sont de la forme g^k avec $(k, p-1) = 1$.*

2.3 Existence de racines primitives

L'objectif de cette section est de montrer qu'un entier $m \geq 2$ a une racine primitive si et seulement si $m = 2, 4, p^k$ ou $2p^k$, avec p un entier premier impair et k un entier ≥ 1.

Théorème 2.3.1 *Soit $m \geq 2$ un entier qui n'est pas une puissance de 2. Si m a une racine primitive, alors $m = p^k$ ou $m = 2p^k$, avec p un entier premier impair et $k \geq 1$.*

Preuve : Soient a et m des entiers tels que $(a, m) = 1$ et $m \geq 3$. Supposons que

$$m = m_1 m_2 \qquad \text{avec } (m_1, m_2) = 1 \text{ et } m_1 \geq 3,\ m_2 \geq 3. \tag{2.2}$$

Alors $(a, m_1) = (a, m_2) = 1$. De plus, si φ désigne l'indicatrice d'Euler, alors $\varphi(m)$ est paire pour $m \geq 3$ (voir Théorème 1.4.5). On peut donc considérer

$$n = \frac{\varphi(m)}{2}$$

et on a

$$n = \frac{\varphi(m_1)\varphi(m_2)}{2}.$$

D'après le théorème d'Euler, on a

$$a^{\varphi(m_1)} \equiv 1 \,(\mathrm{mod}\, m_1),$$

d'où

$$a^n = (a^{\varphi(m_1)})^{\varphi(m_2)/2} \equiv 1 \,(\mathrm{mod}\, m_1).$$

De façon similaire, on a

$$a^n = (a^{\varphi(m_2)})^{\varphi(m_1)/2} \equiv 1 \,(\mathrm{mod}\, m_2).$$

Comme $(m_1, m_2) = 1$ et $m = m_1 m_2$, le théorème des restes chinois implique que

$$a^n \equiv 1 \,(\mathrm{mod}\, m).$$

Donc l'ordre de a modulo m est strictement plus petit que $\varphi(m)$. Par conséquent, si m peut se factoriser sous la forme (2.2), alors m n'admet pas de racine primitive. En particulier, si m est divisible par deux nombres premiers distincts impairs alors m n'admet pas de racine primitive. De façon similaire, si $m = 2^\ell p^k$, avec $\ell \geq 2$ et p un entier premier impair, alors m n'admet pas non plus de racines primitives. Par conséquent, si m n'est pas une puissance de 2 et si m admet une racine primitive, alors m est nécessairement de la forme $m = p^k$ ou $m = 2p^k$ pour un certain entier premier impair et $k \geq 1$.

□

La réciproque du théorème précédent est aussi vraie. Commençons par le cas où $m = p^k$ avec p un entier premier impair. Pour cela, on utilisera le lemme suivant de congruence.

Lemme 2.3.2 *Soient k un entier naturel et p un nombre premier impair. On a*

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \,(\mathrm{mod}\, p^{k+2}).$$

Preuve : Commençons par une observation : si p est un nombre premier, et si $k \geq 1$, alors $a \equiv b \,(\mathrm{mod}\, p^k)$ entraîne $a^p \equiv b^p \,(\mathrm{mod}\, p^{k+1})$. En effet, si $a = b + \alpha p^k$ pour un certain $\alpha \in \mathbb{Z}$, alors, avec la formule du binôme de Newton, on a

$$a^p = b^p + \sum_{i=1}^{p} \binom{p}{i} \alpha^i p^{ki} b^{p-i}$$

Or comme p est premier, on a $\binom{p}{i} \equiv 0 \,(\mathrm{mod}\, p)$, pour tout $1 \leq i \leq p-1$, (voir appendice, application du lemme 5.6.3). D'où

$$\binom{p}{i} p^{ki} \equiv 0 \,(\mathrm{mod}\, p^{ki+1}).$$

Puisque $ki + 1 \geq k + 1$, on en déduit que pour tout $1 \leq i \leq p-1$, on a

$$\binom{p}{i} p^{ki} \equiv 0 \,(\mathrm{mod}\, p^{k+1}).$$

C'est aussi vrai pour $i = p$, d'où finalement, on obtient que

$$\binom{p}{i} p^{ki} \equiv 0 \,(\mathrm{mod}\, p^{k+1}) \qquad (1 \leq i \leq p) \tag{2.3}$$

et donc

$$a^p \equiv b^p \,(\mathrm{mod}\, p^{k+1}).$$

Prouvons maintenant le résultat. On raisonne par récurrence sur k. Pour $k = 0$, c'est trivial. Pour $k = 1$, on a

$$(1+p)^p = 1 + p^2 + \sum_{i=2}^{p} \binom{p}{i} p^i.$$

Or en utilisant une nouvelle fois que $\binom{p}{i} \equiv 0 \pmod{p}$ pour $1 \leq i \leq p-1$, on obtient

$$\binom{p}{i} p^i \equiv 0 \pmod{p^3}$$

pour $2 \leq i \leq p-1$. C'est aussi vrai pour $i = p$ car $p \geq 3$ (p est un nombre premier impair !). On obtient finalement

$$(1+p)^p \equiv 1 + p^2 \pmod{p^3}.$$

Cela prouve le résultat pour $k = 1$. Supposons maintenant le résultat vrai pour un entier $k \geq 1$ et montrons le résultat pour $k+1$. En utilisant l'observation et l'hypothèse de récurrence, on a

$$(1+p)^{p^{k+1}} \equiv (1 + p^{k+1})^p \pmod{p^{k+3}}.$$

Or

$$(1+p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} p^{(k+1)i} \equiv 1 + p^{k+2} \pmod{p^{k+3}},$$

ce qui donne le résultat.

□

Théorème 2.3.3 (Gauss) *Soit p un entier premier impair. Alors p^k admet une racine primitive.*

Preuve : On va utiliser l'entier $p+1$ et le lemme 2.3.2. Remarquons que comme $(p+1, p^k) = 1$, l'élément $(p+1) \bmod p^k$ est inversible dans $\mathbb{Z}/p^k\mathbb{Z}$. D'autre part, d'après le lemme 2.3.2, on a

$$(1+p)^{p^{k-1}} \equiv 1 \pmod{p^k}$$

et

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

Ceci prouve que l'élément $(p+1) \bmod p^k$ est d'ordre p^{k-1} dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. Soit maintenant a une racine primitive de p (qui existe d'après le théorème 2.2.2). Alors $a \bmod p$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Soit d l'ordre de $a \bmod p^k$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. On a $a^d \equiv 1 \pmod{p^k}$, d'où $a^d \equiv 1 \pmod{p}$. Par conséquent $p-1$ divise d. Le

théorème 1.1.1 implique alors que $a^{d/(p-1)} \bmod p^k$ est d'ordre $\frac{d}{(d,d/(p-1))} = p-1$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. Comme $(p-1,p^k)=1$, le lemme 1.1.2 implique alors que l'élément $(p+1)a^{d/(p-1)} \bmod p^k$ est d'ordre $p^{k-1}(p-1) = p^k - p^{k-1}$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. Comme $\varphi(p^k) = p^k - p^{k-1}$, on en déduit que $(p+1)a^{d/(p-1)}$ est une racine primitive de p^k.

□

Traitons maintenant le cas où $m = 2p^k$.

Théorème 2.3.4 *Soient p un entier premier impair. Alors $2p^k$ admet une racine primitive. Plus précisément, si a est une racine primitive de p^k, et si $a_1 \in \{a, a+p^k\}$ est impair, alors a_1 est une racine primitive de $2p^k$.*

Remarquons que comme p^k est impair, un des deux nombres a et $a+p^k$ est impair et l'autre est pair. De plus, si a est une racine primitive de p^k alors bien évidemment $a+p^k$ est aussi une racine primitive de p^k.

Preuve : Comme $(a+p^k, p^k) = (a,p^k) = 1$ et a_1 est impair, on en déduit que $(a_1, 2p^k) = 1$. Notons d l'ordre de $a_1 \bmod 2p^k$ dans $(\mathbb{Z}/2p^k\mathbb{Z})^*$. D'une part, d divise $\varphi(2p^k)$. D'autre part, comme $a_1^d \equiv 1 \,(\mathrm{mod}\, 2p^k)$, on a en particulier

$$a_1^d \equiv 1 \,(\mathrm{mod}\, p^k).$$

Comme a_1 est une racine primitive de p^k, on en déduit que $\varphi(p^k)$ divise d. Mais comme p est impair, on a $(2,p^k)=1$ et donc

$$\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k).$$

On obtient donc que $d = \varphi(2p^k)$, ce qui permet de conclure que a_1 est une racine primitive de $2p^k$.

□

Il reste le cas des puissances de 2.

Théorème 2.3.5 *Il existe une racine primitive de $m = 2^k$ si et seulement si $k = 1$ ou 2.*

Preuve : Il est facile de voir que 1 est une racine primitive de 2 et 3 est une racine primitive de 4. Montrons maintenant que si $k \geq 3$, alors 2^k n'admet pas de racines primitives. Comme $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$, il suffit de montrer que

$$a^{2^{k-2}} \equiv 1 \,(\mathrm{mod}\, 2^k) \tag{2.4}$$

pour tout nombre impair a et $k \geq 3$. On prouve cette relation de congruence par récurrence sur k. Pour $k=3$, la relation (2.4) provient de

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \,(\mathrm{mod}\, 8).$$

Soit $k \geq 3$ et supposons que (2.4) soit satisfaite. Alors l'entier $a^{2^{k-2}} - 1$ est divisible par 2^k. Comme a est impair, il suit que $a^{2^{k-2}} + 1$ est pair. Par conséquent, l'entier

$$a^{2^{k-1}} - 1 = (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1)$$

est divisible par 2^{k+1}. Ainsi

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}.$$

Cela prouve la congruence (2.4) et le théorème.

□

En résumé, on obtient le résultat suivant :

Théorème 2.3.6 *Soit m un entier ≥ 2. Les assertions suivantes sont équivalentes :*

1. *m admet une racine primitive.*
2. *$(\mathbb{Z}/m\mathbb{Z})^*$ est cyclique.*
3. *$m = 2, 4, p^k$ ou $2p^k$, avec p un entier premier impair et $k \geq 1$.*

Le théorème 2.3.6 donne une caractérisation des entiers qui admettent une racine primitive. En revanche, quand elle existe, il est difficile de construire une racine primitive. On verra dans l'exercice ?? une méthode permettant de construire une racine primitive d'un nombre premier. Mais il reste de nombreuses questions simples sur les racines primitives encore ouvertes de nos jours. Par exemple, on ne sait pas s'il existe un nombre fini ou infini de nombres premiers p pour lesquels 2 est une racine primitive. En fait, on ne connait pas d'entier qui soit une racine primitive pour une infinité de nombres premiers. Il existe un résultat surprenant de Gupta–Murty et Heath-Brown affirmant que tout premier, avec au plus deux exceptions, est une racine racine primitive pour une infinité de nombres premiers. Mais on ne connait pas ces exceptions ! Ainsi on sait qu'au moins un des nombres premiers 2, 3 et 5 est une racine primitive pour une infinité de nombres premiers, mais on ne sait pas lequel....Mentionnons à ce propos une conjecture célèbre due à Artin : *soit a un entier qui n'est pas un carré et tel que $a \neq -1$. Alors a est une racine primitive pour une infinité de nombres premiers.*

2.4 Les logarithmes discrets

Soit p un nombre premier et g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$. Si $a \in (\mathbb{Z}/p\mathbb{Z})^*$, le **logarithme discret** de a en base g, noté $\log_g a$, est l'unique entier α tel que

$$0 \leq \alpha \leq p - 2, \quad a = g^\alpha.$$

Lemme 2.4.1 *Soient p un nombre premier, g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et n un entier tel que $a = g^n$. Alors, le logarithme discret de a en base g est le reste de la division euclidienne de n par $p-1$.*

Preuve : Effectuons le reste de la division euclidienne de n par $p-1$. Alors il existe deux entiers q et r tels que

$$n = q(p-1) + r, \qquad 0 \leq r \leq p-2.$$

On a alors $a = g^n = g^{q(p-1)+r} = g^{q(p-1)}g^r = g^r$ car $g^{p-1} = 1$. Par définition, on en déduit que $\log_g a = r$.

□

Théorème 2.4.2 *Soit p un nombre premier et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Pour tous a, b dans $(\mathbb{Z}/p\mathbb{Z})^*$, on a*

$$\log_g(ab) \equiv \log_g a + \log_g b \,(\mathrm{mod}(p-1)).$$

Preuve : Soit $k_1 = \log_g(a)$ et $k_2 = \log_g(b)$. On a

$$a = g^{k_1} \quad \text{et} \quad b = g^{k_2}.$$

D'où $ab = g^{k_1+k_2}$. D'après le lemme 2.4.1, on en déduit que

$$\log_g(ab) \equiv k_1 + k_2 \,(\mathrm{mod}(p-1)).$$

□

2.5 Exercices

Exercice 2.5.1 Les nombres suivants possèdent-ils des racines primitives :

1. $m = 23$?
2. $m = 41$?

Si oui, en exhiber une.

Exercice 2.5.2 Montrer que 2 est une racine primitive de 101.

Exercice 2.5.3 Quel est l'ordre de 3 mod 101 ? Est-ce que 3 est une racine primitive de 101 ?

Exercice 2.5.4 (a) Prouver que 2 est une racine primitive de 53.

(b) Trouver toutes les solutions de

$$2^x \equiv 22 \,(\mathrm{mod}\, 53).$$

Exercice 2.5.5 Soit p un nombre premier impair et g une racine primitive de p.

(i) Montrer que $g^{(p-1)/2} \equiv -1 \,(\mathrm{mod}\, p)$.

(ii) Montrer que $(p-1)! \equiv g^{(p-2)(p-1)/2} \pmod{p}$.

(iii) Retrouver le théorème de Wilson.

Exercice 2.5.6 (a) Montrer que pour tout entier $k \in \mathbb{N}$, on a

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

(b) En déduire que l'élément $5 \bmod 2^m$ est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^*$.

(c) Soit $m \geq 3$ et soit

$$\begin{array}{rccc} \psi : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & (\mathbb{Z}/2^m\mathbb{Z})^* \\ & (p,q) & \longmapsto & (-1)^p 5^q \bmod 2^m. \end{array}$$

(i) Montrer que ψ est un morphisme de groupes tel que $\ker \psi = 2\mathbb{Z} \times 2^{m-2}\mathbb{Z}$.

(ii) En déduire que $(\mathbb{Z}/2^m\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Exercice 2.5.7 Soit $p = 7$ et $g = 3$.

(a) Montrer que g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

(b) Calculer $\log_g a$, pour tout a tel que $1 \leq a \leq 6$.

(c) Calculer $\log_g 30$.

Exercice 2.5.8 (Théorème de Lucas) Soient q, a deux entiers naturels > 1 tels que

1. $a^{q-1} \equiv 1 \bmod q$.
2. Pour tout diviseur premier p de $q-1$, $a^{\frac{q-1}{p}} \not\equiv 1 \bmod q$.

Démontrer que q est premier et, de plus a est un générateur de $\mathbf{F}_q$ (indication : considérer l'ordre de a dans $\mathbf{F}_q$).

Exercice 2.5.9 Etant donné un nombre premier p et a un nombre premier avec p, on notera $O_p(a)$ l'ordre de a dans $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que si 4 divise $O_p(a)$, alors $O_p(a) = O_p(-a)$. En déduire que si p est un nombre premier de la forme $4k+1$, et a un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ alors $-a$ est aussi un générateur.

Exercice 2.5.10 Si $p = 2q+1$ est premier, avec q premier impair, et a est un entier tel que $a^3 - a \not\equiv 0 \bmod p$, montrer que a ou bien $-a$ est un générateur de $\mathbf{F}_p$.

Chapitre 3

Résidus quadratiques

Dans ce chapitre, on s'intéresse à l'ensemble des carrés dans le corps $\mathbf{F}_p$, p premier. On introduit le symbole de Legendre qui permet de caractériser ces carrés et on développe les principales propriétés de ce symbole. On démontre notamment la "fameuse" loi de réciprocité quadratique due à Gauss. Cette formule admet de nombreuses démonstrations. Nous donnerons celle basée sur les sommes de Gauss. Ces sommes de Gauss seront également utilisées pour obtenir une formule pour le nombre de solutions d'une équation quadratique.

3.1 Résidus quadratiques modulo p.

Définition 3.1.1 *Soit p un nombre premier et a un entier tel que p ne divise pas a. Alors a est appelé un* **résidu quadratique** *modulo p si l'équation $x^2 \equiv a \pmod{p}$ possède une solution. Dans le cas contraire, a est appelé un* **non résidu quadratique** *modulo p.*

Autrement dit, un entier a est un résidu quadratique modulo p si et seulement si $a \bmod p$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$.

Commençons par un exemple simple. Dressons la table des carrés dans $\mathbb{Z}/p\mathbb{Z}$, avec $p = 7$.

$x \bmod 7$	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1

Parmi les 6 éléments non nuls, 3 sont des carrés $\{1, 2, 4\}$, les 3 autres ne sont pas des carrés. De plus, chaque carré non nul a deux racines carrées :

$$\sqrt{1} = \pm 1, \quad \sqrt{2} = \pm 3, \quad \sqrt{4} = \pm 2.$$

Les deux observations effectuées sur cet exemple sont en fait un théorème !

Théorème 3.1.2 *Soit p un nombre premier impair et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Un élément a de $(\mathbb{Z}/p\mathbb{Z})^*$ est un carré si et seulement si son logarithme en base g est pair. Parmi les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, la moitié exactement sont des carrés. Chaque carré a 2 racines carrés.*

Preuve : Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et k son logarithme en base g. Si $k = 2\ell$ est pair, alors on a

$$a = (g^\ell)^2$$

et donc a est un carré. Réciproquement, si a est le carré de g^t, pour un certain t, on a $a = g^{2t}$. Donc d'après le lemme 2.4.1, son logarithme discret est le reste de la division euclidienne de $2t$ par $p-1$. Ce reste est pair car $p-1$ est pair. On en déduit alors que les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ sont

$$\{g^t : 0 \leq t \leq p-2 : t \equiv 1 \,(\mathrm{mod}\, 2)\}.$$

On en déduit donc qu'il existe exactement $(p-1)/2$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

D'autre part, si a est un carré, $a = b^2$, l'élément $-b$ est aussi une racine du polynôme $x^2 - a$, distincte de la racine b (car $a \neq 0$). Le polynôme $x^2 - a$ de $\mathbf{F}_p[x]$ étant de degré 2, il n'admet pas d'autres racines.

□

En d'autres termes, le théorème 3.1.2 affirme qu'étant donné un nombre premier impair p, il existe exactement $(p-1)/2$ résidus quadratiques et $(p-1)/2$ non-résidus quadratiques modulo p.

Le résultat suivant fournit un critère pour qu'un entier soit un résidu quadratique modulo p.

Théorème 3.1.3 (Euler) *Soit p un nombre premier impair et a un entier tel que p ne divise pas a. Alors*

(a) a est un résidu quadratique modulo p si et seulement si $a^{(p-1)/2} \equiv 1 \,(\mathrm{mod}\, p)$.

(b) a est un non-résidu quadratique modulo p si et seulement si $a^{(p-1)/2} \equiv -1 \,(\mathrm{mod}\, p)$.

Preuve : D'après le théorème de Fermat (théorème 1.5.2), on a

$$\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Donc $a^{(p-1)/2}$ est une solution de la congruence $x^2 \equiv 1 \,(\mathrm{mod}\, p)$ et donc

$$a^{(p-1)/2} \equiv \pm 1 \,(\mathrm{mod}\, p).$$

Supposons que a soit un résidu quadratique modulo p. Alors $a \equiv b^2 \pmod{p}$, pour un certain entier b et donc

$$a^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

D'après le théorème 2.1.2, l'équation

$$x^{(p-1)/2} \equiv 1 \pmod{p}$$

a exactement $(p-1)/2$ solutions. Comme il y a $(p-1)/2$ résidus quadratiques modulo p, les solutions de l'équation précédente sont exactement les résidus quadratiques. Ainsi, pour un non-résidu quadratique a, on a $a^{(p-1)/2} \equiv -1 \pmod{p}$.

□

3.2 Le symbole de Legendre

Définition 3.2.1 *Soient p un nombre premier impair et $a \in \mathbb{Z}$. On définit le* **symbole de Legendre** *par*

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

Il est clair que, pour tout nombre premier impair p, on a

$$\left(\frac{1}{p}\right) = 1.$$

Le résultat suivant est une conséquence immédiate du résultat d'Euler.

Corollaire 3.2.2 (Critère d'Euler) *Soient p un nombre premier impair et a un entier. On a*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Théorème 3.2.3 (Périodicité du symbole de Legendre) *Soient p un nombre premier impair, $a \in \mathbb{Z}$ et $m \in \mathbb{Z}$. On a*

$$\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right).$$

Preuve : Il est clair que p divise a si et seulement si p divise $a + mp$. On peut donc supposer maintenant que p ne divise pas a. Alors $\left(\frac{a}{p}\right) = 1$ si et seulement si l'équation

$$x^2 \equiv a \pmod{p}$$

a une solution, ce qui est équivalent au fait que l'équation

$$x^2 \equiv a + mp \,(\mathrm{mod}\, p)$$

a une solution, c'est à dire que $\left(\frac{a+mp}{p}\right) = 1$.

□

Le théorème 3.2.3 permet d'étendre la définition du symbole de Legendre modulo p à $\mathbb{Z}/p\mathbb{Z}$. Ainsi, on pose

$$\left(\frac{a \bmod p}{p}\right) := \left(\frac{a}{p}\right).$$

Théorème 3.2.4 (Multiplicativité du symbole de Legendre) *Soient $a, b \in \mathbb{Z}$ et p un nombre premier impair. On a*

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

Preuve : En utilisant le critère d'Euler, on a

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \,(\mathrm{mod}\, p)\\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \,(\mathrm{mod}\, p)\\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \,(\mathrm{mod}\, p),\end{aligned}$$

ce qui donne le résultat.

□

Le théorème 3.2.4 implique que le symbole de Legendre est complètement déterminé par ses valeurs en -1, 2 et aux entiers impairs. En effet, si a est un entier non divisible par p, alors on peut écrire a sous la forme

$$a = \pm 2^{r_0} q_1^{r_1} q_2^{r_2} \dots q_k^{r_k},$$

où $q_1, \dots, q_k$ sont des entiers premiers impairs, distinct et différent de p. Alors on a

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{r_0}\left(\frac{q_1}{p}\right)^{r_1} \dots \left(\frac{q_k}{p}\right)^{r_k}.$$

On peut déterminer l'ensemble des nombres premiers p pour lesquels -1 est un résidu quadratique. D'après le résultat suivant, cela dépend uniquement de la classe de congruence de p modulo 4.

Théorème 3.2.5 (Caractère quadratique de -1) *Soit p un nombre premier impair. Alors*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 4) \\ -1 & \text{si } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

De façon équivalente, on a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Preuve : Observons que

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

D'autre part, en appliquant le critère d'Euler, on a

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$$

et le résultat suit immédiatement car chacun des termes de la congruence est ± 1.

□

Le résultat suivant donne un critère pour que 2 soit un carré modulo p.

Théorème 3.2.6 (Caractère quadratique de 2.) *Soit p un entier premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8). \end{cases}$$

Preuve : Soit ζ une racine primitive 8-ème de l'unité sur $\mathbf{F}_p$ et posons $y = \zeta + \zeta^{-1}$. On a $y^2 = \zeta^2 + \zeta^{-2} + 2$. D'autre part, comme $\zeta^8 = 1$, on a $\zeta^4 = \pm 1$; mais le cas $\zeta^4 = 1$ est exclu car sinon ζ ne serait pas une racine primitive. Il en résulte donc que $\zeta^4 = -1$. Cela implique que $\zeta^2 = -\zeta^{-2}$ et donc $y^2 = 2$. En utilisant la formule du binôme de Newton, on obtient également que

$$y^p = \zeta^p + \zeta^{-p} + \sum_{1 \le i \le p-1} \binom{i}{p} \zeta^i \zeta^{-p+i}.$$

Or $\binom{i}{p} \equiv 0 \pmod p$ pour tout $1 \le i \le p-1$, d'où

$$y^p = \zeta^p + \zeta^{-p}.$$

Comme $y^2 = 2$, on obtient que 2 est un carré modulo p si et seulement si $y \in \mathbf{F}_p$, ce qui est équivalent à $y^p = y$. Si $p \equiv \pm 1 \pmod 8$, alors on a

$$y^p = \zeta + \zeta^{-1} = y,$$

donc 2 est un carré modulo p et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$. Si $p \equiv \pm 3 \pmod 8$, on a

$$y^p = \zeta^3 + \zeta^{-3},$$

et en utilisant que $\zeta^4 = -1$, on obtient

$$y^p = -\zeta^{-1} - \zeta = -y$$

et donc 2 n'est pas un carré modulo p. D'où $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$.

□

Lemme 3.2.7 *On a*

$$\sum_{\bar{a}\in\mathbf{F}_p^*}\left(\frac{a}{p}\right)=0.$$

Preuve : Il suffit de se rappeler qu'il y a autant de carrés que de non-carrés dans $\mathbf{F}_p^*$ d'après le théorème 3.1.2.

□

3.3 Les sommes de Gauss

Les sommes de Gauss sont très importantes en arithmétique. Nous allons les utiliser pour donner une démonstration de la loi de réciprocité quadratique. Nous les utiliserons également pour calculer le nombre de solutions modulo p d'une équation quadratique. Dans cette section, nous introduisons ces sommes et donnons quelques formules utiles pour la suite.

Soient p un nombre premier impair, K un corps de caractéristique q différente de p et soit ζ une racine primitive p-ième de l'unité sur K. Pour $x\in\mathbb{Z}$, l'élément ζ^x ne dépend que de $x \bmod p$ et donc il garde un sens pour $x\in\mathbf{F}_p$. Pour $a\in\mathbf{F}_p^*$, on pose

$$\tau(a)=\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^{ax}.$$

L'élément $\tau(a)$, qui appartient à $\Sigma_p(K)$ (le corps des racines p-ième de l'unité sur K, voir appendice) s'appelle la **somme de Gauss** sur K associée à a.

Théorème 3.3.1 *Soient K un corps de caractéristique q, soit p un nombre premier impair, $p\neq q$. Alors, on a les propriétés suivantes :*

(i) pour tout $a\in\mathbf{F}_p^*$,

$$\tau(a)=\left(\frac{a}{p}\right)\tau(1).$$

(ii) $\tau(1)^2=\left(\frac{-1}{p}\right)p.$

(iii) si q est un nombre premier impair, pour tout $a\in\mathbf{F}_p^*$, on a

$$\tau(a)^{q-1}=\left(\frac{q}{p}\right).$$

Preuve : (i) : l'application $x\longmapsto ax$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$. On a donc

$$\begin{aligned}\tau(a) &= \sum_{y\in\mathbf{F}_p^*}\left(\frac{a^{-1}y}{p}\right)\zeta^y\\ &= \sum_{y\in\mathbf{F}_p^*}\left(\frac{a^{-1}}{p}\right)\left(\frac{y}{p}\right)\zeta^y\\ &= \left(\frac{a^{-1}}{p}\right)\tau(1).\end{aligned}$$

Or $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$ car $\left(\frac{a}{p}\right) \in \{-1, 1\}$. D'où $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$.

(ii) : pour simplifier, nous noterons $\tau = \tau(1)$. En utilisant le théorème 3.2.4, on a

$$\tau^2 = \left(\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^x\right)\left(\sum_{y\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^y\right) = \sum_{x,y\in\mathbf{F}_p^*}\left(\frac{xy}{p}\right)\zeta^{x+y}.$$

Si on effectue le changement de variable $t = x^{-1}y$, on a $y = xt$ et donc $xy = x^2t$. D'où

$$\left(\frac{xy}{p}\right) = \left(\frac{x^2t}{p}\right) = \left(\frac{x^2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{t}{p}\right).$$

Donc

$$\tau^2 = \sum_{x,t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)\zeta^{x(1+t)} = \sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)\left(\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)}\right).$$

Si $1 + t \equiv 0 \,(\mathrm{mod}\, p)$, alors $\zeta^{x(1+t)} = 1$ donc

$$\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)} = p - 1.$$

Si $1 + t \not\equiv 0 \,(\mathrm{mod}\, p)$, alors l'application $x \longmapsto x(1 + t)$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$, d'où

$$\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

Ainsi

$$\tau^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\neq -1}\left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right).$$

Il reste à appliquer le lemme 3.2.7 pour conclure la preuve du *(ii)*.

(iii) : remarquons que $\left(\frac{a}{p}\right)^{q-1} = 1$. Donc, d'après *(i)*, il suffit de prouver le résultat pour $a = 1$. En notant $\tau = \tau(1)$, comme la caractéristique de $\Sigma_p(K)$ est égale à q, on a

$$\tau^q = \sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)^q\zeta^{qx}.$$

Or comme q est impair, on a

$$\left(\frac{x}{p}\right)^q = \left(\frac{x}{p}\right),$$

d'où

$$\tau^q = \sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^{qx} = \left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{qx}{p}\right)\zeta^{qx}.$$

L'application $x \longmapsto qx$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$, d'où

$$\tau^q = \left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^x = \left(\frac{q}{p}\right)\tau.$$

Or d'après *(ii)*, $\tau \neq 0$, d'où on en tire que $\tau^{q-1} = \left(\frac{q}{p}\right)$.

□

Dans le cas où le corps K est $\mathbb{Q}$, une racine primitive p-ième de l'unité est donnée par $\zeta = e^{2i\pi/p}$. On peut alors donner une autre expression des sommes de Gauss qui nous sera utile dans les applications. Pour prouver ce lemme, nous aurons besoin de la formule suivante

$$\sum_{x\in\mathbf{F}_p} \exp\left(\frac{2i\pi xy}{p}\right) = \begin{cases} p & \text{si } y = 0 \bmod p \\ 0 & \text{sinon.} \end{cases} \tag{3.1}$$

dont la preuve (simple) est laissée en exercice.

Lemme 3.3.2 *On a*

$$\tau(a) = \sum_{y\in\mathbf{F}_p} \exp\left(\frac{2i\pi ay^2}{p}\right).$$

Preuve : On vérifie facilement que l'équation $y^2 = x$ admet $1 + \left(\frac{x}{p}\right)$ solutions. On en déduit, en utilisant (3.1) que

$$\begin{aligned} \tau(a) &= \sum_{x\in\mathbf{F}_p} \left(\frac{x}{p}\right) \exp\left(\frac{2i\pi ax}{p}\right) = \sum_{x\in\mathbf{F}_p} \left(1 + \left(\frac{x}{p}\right)\right) \exp\left(\frac{2i\pi ax}{p}\right) \\ &= \sum_{y\in\mathbf{F}_p} \exp\left(\frac{2i\pi ay^2}{p}\right). \end{aligned}$$

□

3.4 La loi de réciprocité quadratique

Le résultat fondamental suivant a été démontré par Gauss. Il existe de nombreuses preuves. Celle que nous utilisons est basée sur les "sommes de Gauss".

Théorème 3.4.1 (Loi de réciprocité quadratique) *Soient p et q des nombres premiers impairs distincts. On a*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Autrement dit, si $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, alors $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, sinon $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Preuve : Soit ζ une racine primitive p-ième de l'unité sur $\mathbf{F}_q$ et soit $\tau = \tau(1)$ la somme de Gauss associée dans $\Sigma_p(\mathbf{F}_q)$. En utilisant le corollaire 3.2.2 et le théorème 3.3.1, on obtient les égalités suivantes dans $\Sigma_p(\mathbf{F}_q)$:

$$\begin{aligned} \left(\frac{p}{q}\right) &= p^{(q-1)/2} = \left(\left(\frac{-1}{p}\right)\tau^2\right)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}\tau^{q-1} \\ &= (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right), \end{aligned}$$

ce qui donne le résultat.

□

3.5 Le symbole de Jacobi

Sachant que le nombre 239 est premier, proposons nous de calculer le symbole de Legendre $\left(\frac{143}{239}\right)$. Pour appliquer la loi de réciprocité quadratique, il faudrait que le symbole de Legendre $\left(\frac{239}{143}\right)$ soit défini donc que 143 soit premier. Ce n'est pas le cas car $143 = 11 \times 13$. Le seul moyen d'avancer dans le calcul est d'utiliser cette factorisation, et la multiplicativité du symbole de Legendre. On écrit alors

$$\left(\frac{143}{239}\right) = \left(\frac{11}{239}\right)\left(\frac{13}{239}\right).$$

La loi de réciprocité s'applique maintenant car 11 et 13 sont premiers et cela conduit à

$$\left(\frac{143}{239}\right) = -\left(\frac{239}{11}\right)\left(\frac{239}{13}\right) = -\left(\frac{8}{11}\right)\left(\frac{5}{13}\right) = -\left(\frac{2}{11}\right)^3\left(\frac{13}{5}\right).$$

Or d'après le théorème 3.2.6, $\left(\frac{2}{11}\right) = -1$, d'où

$$\left(\frac{143}{239}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Le calcul est très simple ici car la factorisation de 143 est évidente. Dans le cas général, le calcul du symbole de Legendre $\left(\frac{a}{p}\right)$ lorsque a est non premier nous ramène au problème de la factorisation de a qui est un problème difficile. Le symbole de Jacobi supprime cette difficulté.

Définition 3.5.1 *Soit n un entier positif impair dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Le* **symbole de Jacobi** $\left(\frac{m}{n}\right)$ *est défini par*

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1}\left(\frac{m}{p_2}\right)^{\alpha_2}\dots\left(\frac{m}{p_k}\right)^{\alpha_k}.$$

Théorème 3.5.2 *Soient m et n des entiers positifs impairs et $a, b, k \in \mathbb{Z}$. On a*

(a) $\left(\frac{a+kn}{n}\right) = \left(\frac{a}{n}\right)$.

(b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(c) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

(d) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

(e) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

Preuve : La preuve se déduit des propriétés analogues du symbole de Legendre et les détails sont laissés en exercice.

□

Il faut prendre garde au fait que le symbole de Jacobi ne caractérise pas les carrés modulo n (si a est premier avec n et est un carré modulo n alors $\left(\frac{a}{n}\right) = 1$ mais la réciproque est fausse si n est composé. Ceci montre que le symbole de Jacobi n'a pas de signification intéressante, contrairement au symbole de Legendre qui permet de distinguer les carrés. En revanche, c'est un outil de calcul indispensable. Reprenons l'exemple du calcul de $\left(\frac{143}{239}\right)$. On commence par appliquer la loi de réciprocité quadratique pour le symbole de Jacobi et on écrit

$$\begin{aligned}\left(\frac{143}{239}\right) &= -\left(\frac{239}{143}\right) = -\left(\frac{96}{143}\right) = -\left(\frac{2^5.3}{143}\right) \\ &= -\left(\frac{2}{143}\right)^5\left(\frac{3}{143}\right) = -\left(\frac{3}{143}\right) \\ &= \left(\frac{143}{3}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

Il n'est plus nécessaire de factoriser les entiers, sauf pour sortir les facteurs 2 lorsque l'argument figurant au dénominateur est pair. On utilise essentiellement la loi de réciprocité et la périodicité. Le calcul du symbole de Jacobi $\left(\frac{a}{b}\right)$ est semblable au calcul du pgcd de a et b par l'algorithme d'Euclide. Le calcul d'un symbole de Legendre en utilisant les symboles de Jacobi ne nécessite que $O(\log b)$ divisions.

3.6 Nombre de solutions d'une équation quadratique

On rappelle que si $Q(x) = \sum_{1\leq i,j\leq n} a_{i,j}x_ix_j$ est une forme quadratique sur $\mathbf{F}_p^n$, on dit qu'elle est non dégénérée si $\det(Q) := \det(a_{i,j}) \neq 0$.

Théorème 3.6.1 *Soit Q une forme quadratique en n variables non dégénérée à coefficients dans $\mathbf{F}_p$ où p est un nombre premier impair. Alors*

$$card\{x \in \mathbf{F}_p^n : Q(x) = 0\} = p^{n-1} + \varepsilon(p-1)p^{\frac{n}{2}-1},$$

où

$$\varepsilon = \begin{cases} 0 & \text{si } n \text{ est impair} \\ \left(\frac{(-1)^{\frac{n}{2}}\det(Q)}{p}\right) & \text{si } n \text{ est pair.}\end{cases}$$

Preuve : Etape 1 : on se ramène au cas où Q est diagonale, c'est-à-dire de la forme

$$Q(x) = a_1x_1^2 + a_2x_2^2 + \ldots a_nx_n^2.$$

Ecrivons $Q(x) = {}^txAx$. Comme

$$Q(x) = \sum_{1\leq i,j\leq n} \frac{1}{2}(a_{i,j} + a_{j,i})x_ix_j,$$

on peut supposer que la matrice A est symétrique (quitte à changer A en $\frac{1}{2}(A + {}^tA)$). En utilisant un résultat classique sur les formes quadratiques symétriques non dégénérées, on sait qu'il existe une matrice de changement de base U et il existe $a_1, a_2, \ldots, a_n \in \mathbf{F}_p$ tels que si $x = Uy$, alors

$$Q(x) = Q^\sharp(y) = a_1 y_1^2 + \cdots + a_n y_n^2.$$

De plus, comme ${}^txAx = {}^ty{}^tUAUy$, la matrice $A^\sharp := {}^tUAU$ est la matrice associée à $Q^\sharp$. Il reste à remarquer alors que

$$\det(Q^\sharp) = \det(A^\sharp) = (\det(U))^2 \det(Q),$$

ce qui implique

$$\left(\frac{\det(Q^\sharp)}{p}\right) = \left(\frac{\det(Q)}{p}\right),$$

et achève de prouver l'étape 1.

Etape 2 : on prouve le résultat dans le cas où Q est diagonale.

Notons

$$N_p = \mathrm{card}\{x \in \mathbf{F}_p^n : Q(x) = 0\}.$$

et montrons que

$$pN_p = \sum_{a=0}^{p-1} \sum_{x \in \mathbf{F}_p^n} \exp\left(\frac{2i\pi a Q(x)}{p}\right). \tag{3.2}$$

On a, tout d'abord,

$$\sum_{a=0}^{p-1} \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)=0}} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = \sum_{a=0}^{p-1} N_p = pN_p.$$

D'autre part, en utilisant (3.1), on a

$$\sum_{a=0}^{p-1} \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)\neq 0}} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)\neq 0}} \sum_{a=0}^{p-1} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = 0,$$

ce qui donne la formule (3.2). On écrit maintenant

$$\begin{aligned}
pN_p &= p^n + \sum_{a=1}^{p-1} \sum_{x \in \mathbf{F}_p^n} \exp\left(\frac{2i\pi a Q(x)}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \sum_{x_1, x_2, \ldots, x_n \in \mathbf{F}_p} \exp\left(\frac{2i\pi a(a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2)}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \sum_{x_j \in \mathbf{F}_p} \exp\left(\frac{2i\pi a a_j x_j^2}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \tau(a a_j).
\end{aligned}$$

D'où en utilisant le théorème 3.3.1, on en déduit que

$$pN_p = p^n + \tau(1)^n \left(\frac{a_1 \dots a_n}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n.$$

Or $\det(Q) = a_1 \dots a_n$ et

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n = \begin{cases} 0 & \text{si } n \text{ est impair} \\ p-1 & \text{si } n \text{ est pair.} \end{cases}$$

Donc si n est impair, on en déduit que $pN_p = p^n$, c'est-à-dire que $N_p = p^{n-1}$. Pour n pair, on obtient que

$$pN_p = p^n + \tau(1)^n \left(\frac{\det(Q)}{p}\right)(p-1),$$

et

$$\tau(1)^n = \left(\tau(1)^2\right)^{\frac{n}{2}} = \left(p\left(\frac{-1}{p}\right)\right)^{\frac{n}{2}} = \left(\frac{(-1)^{\frac{n}{2}}}{p}\right) p^{\frac{n}{2}}.$$

D'où

$$N_p = p^{n-1} + (p-1)\left(\frac{(-1)^{\frac{n}{2}} \det(Q)}{p}\right) p^{\frac{n}{2}-1},$$

ce qui donne le résultat.

□

3.7 Exercices

Exercice 3.7.1 Soit p un nombre premier impair. Déterminer $\left(\frac{\frac{p+1}{2}}{p}\right)$ et $\left(\frac{\frac{p-1}{2}}{p}\right)$.

Exercice 3.7.2

1. Déterminer les p premiers pour lesquels l'équation $x^2 \equiv 3 \pmod{p}$ admet au moins une solution ?
2. Pour quels p premiers l'équation $x^2 \equiv 5 \pmod{p}$ a-t-elle des solutions ?

Exercice 3.7.3 131 et 263 sont premiers. Calculer $O_{263}(131)$ avec un minimum de calculs.

Exercice 3.7.4 Montrer que les diviseurs premiers de $4n^2 + 1$ sont de la forme $4k + 1$.

Exercice 3.7.5 Résoudre l'équation $x^2 + 3x + 7 \equiv 0 \pmod{115}$.

Exercice 3.7.6 (La méthode de Hensel) Soit p un nombre premier impair, $n \geq 1$ et $a \in \mathbb{Z}$ tel que $(a, p) = 1$.

(a) Montrer que $\bar{a} \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

(b) On suppose que $x_1^2 \equiv a \pmod{p}$. Montrer que, pour tout entier $n \geq 1$, il existe un entier x_n, unique modulo p^n, qui vérifie

$$x_n \equiv x_1 \pmod{p}, \quad x_n^2 \equiv a \pmod{p^n}.$$

Indication : les x_n se construisent par récurrence, en cherchant x_{n+1} sous la forme

$$x_{n+1} = x_n + p^n u,$$

où u est un nombre entier à déterminer.

(c) En déduire que la congruence $x^2 \equiv a \pmod{p^n}$ admet des solutions si et seulement si $\left(\frac{a}{p}\right) = 1$, et dans ce cas, elle admet exactement deux solutions modulo p^n.

(d) **Application :** résoudre $x^2 + x + 3 \equiv 0 \pmod{125}$.

Exercice 3.7.7 (Résolution de $x^2 \equiv a \pmod{2^n}$ (a impair))

1. Soit $n \geq 3$, a un entier impair. Démontrer que si la congruence $x^2 \equiv a \pmod{2^n}$ a des solutions, alors $a \equiv 1 \pmod{8}$.
2. On suppose $a \equiv 1 \pmod{8}$. Démontrer que $x^2 \equiv a \pmod{8}$ admet exactement 4 solutions modulo 8.
3. Supposons que $a \equiv 1 \pmod{8}$ et supposons qu'il existe un entier x tel que $x^2 \equiv a \pmod{2^n}$.
   (a) Montrer que a est un carré modulo 2^{n+1}.
   Indication : on pourra calculer pour $y \in \mathbb{N}$, $(x + y2^{n-1})^2$.
   (b) En déduire que a possède au moins 4 racines carrés modulo 2^{n+1}.
4. Conclure par récurrence que, pour tout $n \geq 3$, si $a \equiv 1 \pmod{8}$, alors a possède exactement 4 racines carrées modulo 2^n.
   Indication : on pourra considérer $C_n = \{x \in (\mathbb{Z}/2^n\mathbb{Z})^* : x \equiv 1 \pmod{8}\}$ et

$$\begin{array}{rccc} \varphi : & (\mathbb{Z}/2^n\mathbb{Z})^* & \longrightarrow & C_n \\ & x & \longmapsto & x^2. \end{array}$$

Exercice 3.7.8 On s'intéresse à l'équation $x^2 + x + 1 \equiv 0 \pmod{n}$.

1. Soit $S(n)$ la fonction arithmétique qui associe à l'entier $n \geq 1$ le nombre de solutions modulo n de l'équation $x^2 + x + 1 \equiv 0 \pmod{n}$. Démontrer que la fonction S est une *fonction arithmétique multiplicative* c'est à dire que $S(mn) = S(m)S(n)$ chaque fois que m et n sont premiers entre eux.

2. Pour quels p premiers l'équation $x^2+x+1=0 \pmod p$ a-t-elle des solutions, c'est à dire tels que $S(p)>0$.
3. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ la valeur de $S(p^\alpha)$.
4. Quels sont les entiers n pour lesquels $x^2+x+1 \equiv 0 \pmod n$ a des solutions ?
5. Quel est le nombre de solutions de

$$x^2+x+1 \equiv 0 \pmod{2457}.$$

Exercice 3.7.9 1. Pour quels p premiers l'équation $x^2+6x+1=0 \pmod p$ a-t-elle des solutions ?
2. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ le nombre de solutions de

$$x^2+6x+1 \equiv 0 \pmod{p^\alpha}$$

3. Quels sont les entiers n pour lesquels $x^2+6x+1 \equiv 0 \pmod n$ a des solutions ?

Exercice 3.7.10 On appelle $n^{\text{ième}}$ nombre de Fermat le nombre $2^{2^n}+1$.

1. Montrer que si un nombre premier est de la forme 2^k+1 alors c'est un nombre de Fermat.
2. Soit $F_n = 2^{2^n}+1$ un nombre de Fermat. Montrer que les diviseurs premiers de F_n sont tous de la forme $k2^{n+1}+1$ (si p est un diviseur premier de F_n, on considèrera l'ordre de 2 modulo p et on montrera qu'il est exactement 2^{n+1}).
3. En considérant le caractére quadratique de 2 modulo p montrer qu'on a un peu mieux : les diviseurs premiers de F_n sont tous de la forme $k2^{n+2}+1$.
4. En marchant sur les traces d'Euler, en déduire que $F_5 = 2^{32}+1 = 4294967297$ n'est pas premier.

Exercice 3.7.11 Soit $p = F_n = 2^{2^n}+1$, avec $n \geq 1$.

1. On suppose que p est premier.
   (a) Montrer que g est un générateur $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $\left(\frac{g}{p}\right) = -1$.
   (b) Montrer que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Ici on ne suppose pas p premier, mais seulement que

$$3^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Montrer que p est premier. Ce test de primalité pour les nombres de Fermat est le test de Pepin.

Exercice 3.7.12 (Calcul d'une racine carrée modulo p) On donne dans cet exercice un algorithme efficace de calcul des racines carrées de a dans $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier impair.

1. Dans la cas ou $p \equiv 3 \pmod 4$ cet algorithme est particulièrement simple. Soit a un carré modulo p. Démontrer que $a^{\frac{p+1}{4}}$ est un racine carrée de a.
2. A partir de maintenant p est un nombre premier impair quelconque. Expliquer comment, en pratique, on peut trouver rapidement un entier b qui ne soit pas un carré modulo p. On choisit un tel entier. On considère alors l'ensemble E des couples (e_1, e_2) satisfaisant

$$a^{e_1} b^{e_2} \equiv 1 \bmod p. \tag{3.3}$$

3. Montrer que $\left(\frac{p-1}{2}, 0\right) \in E$
4. Montrer que si $(e_1, e_2) \in E$ alors e_2 est pair.
5. Montrer que si $(e_1, e_2) \in E$ et si e_1 est impair alors

$$x = a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$

est une racine carrée de a modulo p.

6. Soit $(e_1, e_2) \in E$ avec e_1 pair. Soit $u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}$. Que pouvez vous dire de u^2 ? En déduire un couple $(e_1', e_2') \in E$ avec $e_1' = e_1/2$.
7. En déduire un algorithme de calcul d'une racine carrée de a modulo p. Analyser la complexité de cet algorithme dans le pire des cas, c'est-à-dire le nombre maximum d'opérations à effectuer pour obtenir ainsi une racine carrée de a. Que se passe-t-il lorsque p est de la forme $p = 4k + 3$?.

Chapitre 4

Théorème de Minkowski et applications.

Ce chapitre a pour objectif d'introduire la "géométrie des nombres", théorie initiée par Minkowski en 1896. Elle consiste à donner une minoration du nombre de points d'un réseau de l'espace euclidien $\mathbb{R}^n$ qui appartiennent à un partie convexe donnée, la minoration s'effectuant en fonction du volume du réseau et du convexe. Appliquées à certains réseaux de nature arithmétique, ces estimations ont des conséquences nombreuses et spectaculaires en théorie des nombres. Nous en donnerons deux applications à travers la représentation d'entiers en sommes de carrés.

4.1 Réseaux de $\mathbb{R}^n$.

Fixons $n \geq 1$ un entier. Dans tout ce chapitre, on supposera que $\mathbb{R}^n$ est muni d'une norme $\|\cdot\|$ quelconque. On rappelle qu'une partie $D \subset \mathbb{R}^n$ est dite **discrète** si pour tout réel $r > 0$, l'ensemble

$$\{x \in D : \|x\| \leq r\}$$

est fini. Autrement dit, toute boule de centre 0 et de rayon $r > 0$ contient un nombre fini de points de D. Remarquons bien sûr que cette propriété ne dépend pas du choix de la norme (car toutes les normes sont équivalentes sur $\mathbb{R}^n$).

Définition 4.1.1 *Un* **réseau** *de $\mathbb{R}^n$ est un sous-groupe discret qui engendre $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel.*

Autrement dit, une partie non vide $L \subset \mathbb{R}^n$ est un réseau si elle vérifie les trois propriétés suivantes :

(i) L est discrète.

(ii) $\forall a, b \in L$, on a $a - b \in L$.

(iii) il existe $e_1, e_2, \ldots, e_n \in L$ qui est une base de $\mathbb{R}^n$.

Exemples :

- Le sous-groupe $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$.
- L'ensemble

$$L_0 = \{(a,b) \in \mathbb{Z}^2 : a \equiv 2b \,(\mathrm{mod}\, 3)\}$$

est un réseau de $\mathbb{R}^2$.

On rappelle qu'une famille $e_1, e_2, \ldots, e_r$ d'un groupe abélien G est dite $\mathbb{Z}$-**génératrice** si tout élément g de G s'écrit sous la forme

$$g = \sum_{i=1}^{r} m_i e_i,$$

avec $m_i \in \mathbb{Z}$ pour tout $i = 1, 2, \ldots, r$. On dit que c'est une $\mathbb{Z}$-**base** si de plus une telle écriture est unique.

Un troisième exemple fondamental de réseau est donné par le résultat suivant :

Lemme 4.1.2 *Soit $e = \{e_1, \ldots, e_n\}$ une base de $\mathbb{R}^n$, et notons*

$$L(e) = \{m_1 e_1 + m_2 e_2 + \cdots + m_n e_n : m_1, \ldots, m_n \in \mathbb{Z}\}$$

le sous-groupe engendré par e. Alors $L(e)$ est un réseau de $\mathbb{R}^n$.

Preuve : Considérons la norme sur $\mathbb{R}^n$ définie par

$$\left\| \sum_{i=1}^{n} x_i e_i \right\|_\infty = \max_{1 \le i \le n} |x_i|.$$

Pour tout $r > 0$, on a

$$m = (m_1, \ldots, m_n) \in L(e) \cap D(0,r) \Longleftrightarrow m_i \in \mathbb{Z} \text{ et } |m_i| \le r, \forall 1 \le i \le n.$$

Or le cardinal de $\mathbb{Z} \cap [-r, r]$ étant fini, cela implique que l'ensemble $L(e) \cap D(0,r)$ est aussi fini. Autrement dit, $L(e)$ est une partie discrète. Il est clair que $L(e)$ est un sous-groupe de $\mathbb{R}^n$ qui, par hypothèse, engendre $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel. Donc $L(e)$ est un réseau de $\mathbb{R}^n$.

□

Le résultat suivant affirme que cet exemple de réseau est en fait l'exemple canonique.

Théorème 4.1.3 (caractérisation algébrique des réseaux) *Soit $L \subset \mathbb{R}^n$ un sous-groupe. Les assertions suivantes sont équivalentes :*

(i) L est un réseau de $\mathbb{R}^n$.

(ii) il existe $e = \{e_1, \dots, e_n\}$ une base de $\mathbb{R}^n$ telle que $L = L(e)$.

En particulier, tout réseau admet une $\mathbb{Z}$-base à n éléments.

Pour prouver le théorème, nous allons être amenés à introduire le **pavé fondamental** de $\mathbb{R}^n$ associé à la base $e = \{e_1, \dots, e_n\}$ défini comme l'ensemble

$$\Pi(e) = \left\{ \sum_{i=1}^{n} x_i e_i : x_i \in [0,1[, 1 \leq i \leq n \right\}.$$

Lemme 4.1.4 *Soit $e = \{e_1, \dots, e_n\}$ une base de $\mathbb{R}^n$. Tout vecteur u de $\mathbb{R}^n$ s'écrit de manière unique sous la forme*

$$u = u_1 + u_2,$$

avec $u_1 \in L(e)$ et $u_2 \in \Pi(e)$.

Preuve : Rappelons que pour tout $t \in \mathbb{R}$, la partie entière $\lfloor t \rfloor$ désigne l'unique entier m tel que $m \leq t < m+1$. Si $u = \sum_{i=1}^{n} x_i e_i \in \mathbb{R}^n$, alors $u = u_1 + u_2$, avec

$$u_1 = \sum_{i=1}^{n} \lfloor x_i \rfloor e_i \quad \text{et} \quad u_2 = \sum_{i=1}^{n} (x_i - \lfloor x_i \rfloor) e_i.$$

Il est clair que $u_1 \in L(e)$ et $u_2 \in \Pi(e)$, ce qui prouve l'existence de la décomposition. Concernant l'unicité, supposons qu'il existe $u_1 \in L(e)$ et $u_2 \in \Pi(e)$ tel que $u = u_1 + u_2$. Comme $u_1 \in L(e)$, il existe $(m_1, \dots, m_n) \in \mathbb{Z}^n$ tel que

$$u_1 = \sum_{i=1}^{n} m_i e_i.$$

Comme $u_2 \in \Pi(e)$ il existe $(x_1', \dots, x_n') \in [0,1[^n$ tel que

$$u_2 = \sum_{i=1}^{n} x_i' e_i.$$

D'où, comme $(e_1, \dots, e_n)$ est une base de $\mathbb{R}^n$, on a, pour tout $1 \leq i \leq n$,

$$x_i = m_i + m_i'.$$

Ainsi $\lfloor x_i \rfloor = m_i$ et donc $x_i' = x_i - \lfloor x_i \rfloor$, ce qui prouve l'unicité de la décomposition.

□

Soit G un groupe abélien et H un sous-groupe de G. On rappelle que la relation binaire défini dans G par

$$x \sim y \Longleftrightarrow x - y \in H$$

est une relation d'équivalence. Muni de l'opération

$$\bar{x} + \bar{y} = \overline{x+y},$$

l'ensemble quotient $G/\sim$ est un groupe noté G/H et appelé le **groupe quotient** de G par H. On dit alors que H est d'**indice fini** dans G si ce groupe quotient est un groupe fini et on appelle **indice** de H dans G le nombre, noté $[G : H]$, défini par

$$[G : H] = \mathrm{card}(G/H).$$

Lemme 4.1.5 *Soit L un réseau de $\mathbb{R}^n$ et $e = \{e_1, e_2, \ldots, e_n\}$ une base de $\mathbb{R}^n$ telle que $e_i \in L$ pour tout $1 \leq i \leq n$. Alors $L(e)$ est d'indice fini dans L et il existe un entier $N \geq 1$ tel que $L \subset \frac{1}{N} L(e)$.*

Preuve : Il est clair que $L(e)$ est un sous-groupe de L. Soient $u, v \in L$. D'après le lemme 4.1.4, on a $u = u_1 + u_2$, $v = v_1 + v_2$, avec $u_1, v_1 \in L(e)$ et $u_2, v_2 \in \Pi(e)$. Par unicité de l'écriture, on a

$$u \sim v \Longleftrightarrow u - v \in L(e) \Longleftrightarrow u_2 = v_2.$$

Or si $u \in L$, on a $u_2 = u - u_1 \in L \cap \Pi(e)$. Mais L est discret et $\Pi(e)$ est borné donc $\mathrm{card}(L \cap \Pi(e))$ est fini. En particulier,

$$\mathrm{card}(L/L(e)) \leq \mathrm{card}(L \cap \Pi(e)) < +\infty,$$

ce qui prouve que $L(e)$ est d'indice fini dans L. Notons $N = \mathrm{card}(L/L(e))$. D'après le théorème de Lagrange, on a $N\bar{v} = \bar{0}$ pour tout $v \in L$. D'où $Nv \in L(e)$, ce qui achève la preuve du lemme.

□

Proposition 4.1.6 *Soit L un réseau de $\mathbb{R}^n$ et soit $\mathcal{B}$ l'ensemble des bases $e = \{e_1, \ldots, e_n\}$ de $\mathbb{R}^n$ telles que $e_i \in L$ pour tout $1 \leq i \leq n$. Alors $\mathcal{B}$ est non vide et il existe $e = \{e_1, \ldots, e_n\} \in \mathcal{B}$ tel que*

$$|\det(e_1, e_2, \ldots, e_n)|$$

est minimal. De plus, pour un tel élément e, on a $L = L(e)$.

Ici le déterminant de la famille de vecteurs est pris de manière sous-entendu par rapport à la base canonique.

Preuve : Comme L est un réseau de $\mathbb{R}^n$, l'ensemble $\mathcal{B}$ est non vide par définition. Fixons $f = \{f_1, \ldots, f_n\} \in \mathcal{B}$. Il est clair que $L(f) \subset L$. D'après le lemme 4.1.5, il existe $N \geq 1$ tel que

$$L(f) \subset L \subset \frac{1}{N} L(f).$$

Donc tout élément $x \in L$ s'écrit sous la forme

$$x = \sum_{i=1}^{n} \frac{m_i}{N} f_i,$$

où $m_i \in \mathbb{Z}$, $1 \leq i \leq n$. En particulier, pour tout $e = \{e_1, e_2, \ldots, e_n\} \in \mathcal{B}$, on a

$$\det(e) \in N^{-n} \det(f)\mathbb{Z}.$$

Or $N^{-n} \det(f)\mathbb{Z}$ est un sous-groupe discret de $\mathbb{R}$, donc on peut choisir $e \in \mathcal{B}$ tel que $|\det(e)|$ est minimal (nécessairement non nul car e est une base de $\mathbb{R}^n$).

Il reste à montrer que $L = L(e)$. D'après le lemme 4.1.4, si $u \in L$ alors il existe $u_1 \in L(e)$ et $u_2 \in \Pi(e) \cap L$ tel que $u = u_1 + u_2$. Il suffit de montrer que $\Pi(e) \cap L = \emptyset$. Soit $v = \sum_{i=1}^{n} v_i e_i \in \Pi(e) \cap L$. Comme $v \in \Pi(e)$, on a $v_i \in [0, 1[$ pour tout $i = 1, \ldots, n$. Il s'agit de montrer que $v_i = 0$ pour tout i. Raisonnons par l'absurde en supposant qu'il existe $1 \leq i \leq n$ tel que $v_i \neq 0$. On vérifie facilement que l'élément

$$f = \{e_1, \ldots, e_{i-1}, v, e_{i+1}, \ldots, e_n\}$$

est une base de $\mathbb{R}^n$ donc un élément de $\mathcal{B}$. Mais d'après les propriétés élémentaires du déterminant, on a

$$|\det(f)| = |v_i| |\det(e)| < |\det(e)|,$$

ce qui contredit la minimalité de $|\det(e)|$.

□

Preuve du théorème 4.1.3 : il suffit d'appliquer le lemme 4.1.2 et la proposition 4.1.6

□

Corollaire 4.1.7 *Soient L un réseau de $\mathbb{R}^n$ et $e = \{e_1, \ldots, e_m\}$ une famille $\mathbb{Z}$-génératrice de L. Alors $m \geq n$. De plus, les assertions suivantes sont équivalentes :*

(i) e est une $\mathbb{Z}$-base de L.

(ii) e est une base de $\mathbb{R}^n$.

(iii) $m = n$.

En particulier, toutes les $\mathbb{Z}$-bases de L ont même cardinal.

Preuve : Comme L engendre $\mathbb{R}^n$, on a nécessairement $m \geq n$.

$(i) \Longrightarrow (iii)$: supposons que e soit une $\mathbb{Z}$-base de L et considérons

$$\begin{array}{rccc} \psi : & \mathbb{Z}^m & \longrightarrow & L \\ & (\alpha_i)_{1 \leq i \leq m} & \longmapsto & \sum_{i=1}^{m} \alpha_i e_i. \end{array}$$

Il est facile de vérifier que ψ est un isomorphisme de groupes. De plus, d'après la proposition 4.1.6, il existe $f = \{f_1, f_2, \ldots, f_n\}$ une base de $\mathbb{R}^n$ telle que $L = L(f)$. En particulier, f est une $\mathbb{Z}$-base de L et donc $\psi^{-1}(f) = \{\psi^{-1}(f_1), \ldots, \psi^{-1}(f_n)\}$ est une $\mathbb{Z}$-base de $\mathbb{Z}^m$. Comme $\mathbb{Z}^m$ est un réseau de $\mathbb{R}^m$, on en déduit que $n \geq m$, d'où $m = n$.

$(iii) \Longrightarrow (ii)$: la famille $e = \{e_1, \ldots, e_n\}$ est une famille $\mathbb{Z}$-génératrice de L. Donc, en particulier, c'est une famille $\mathbb{R}$-génératrice de $\mathbb{R}^n$ et comme $\text{card}(e) = n$, on sait que c'est une base de $\mathbb{R}^n$.

$(ii) \Longrightarrow (i)$: on sait que pour tout $x \in L$, il existe $x_1, \ldots, x_n \in \mathbb{Z}$ tels que

$$x = \sum_{i=1}^{n} x_i e_i.$$

Il reste à montrer l'unicité de la décomposition, autrement dit, il suffit de montrer si

$$\sum_{i=1}^{n} x_i e_i = 0, \qquad x_i \in \mathbb{Z}$$

alors $x_1 = \ldots, x_n = 0$. Mais ceci découle du fait que e est une famille libre sur $\mathbb{R}^n$.

□

Considérons

$$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : \exists N \in M_n(\mathbb{Z}), MN = I_n\}.$$

Autrement dit, $GL_n(\mathbb{Z})$ est le sous-groupe de $GL_n(\mathbb{R})$, constitué des matrices à coefficients entiers, et dont l'inverse est aussi à coefficients entiers. Il est facile de vérifier qu'étant donné $M \in M_n(\mathbb{Z})$, on a

$$M \in GL_n(\mathbb{Z}) \Longleftrightarrow \det M = \pm 1.$$

Lemme 4.1.8 *Soit $e = \{e_1, \ldots, e_n\}$ et $f = \{f_1, \ldots, f_n\}$ des bases de $\mathbb{R}^n$ et $P = (p_{i,j})_{1 \leq i,j \leq n}$ la matrice de passage de la base e à la base f, c'est à dire*

$$f_j = \sum_{i=1}^{n} p_{i,j} e_i, \qquad 1 \leq j \leq n.$$

Alors $L(e) = L(f)$ si et seulement si $\det P = \pm 1$.

Preuve : On a $f_j \in L(e)$ si et seulement si la j-ème colonne de P est à coefficients entiers. Autrement dit,

$$L(f) \subset L(e) \Longleftrightarrow P \in M_n(\mathbb{Z}).$$

Si Q est la matrice de passage de la base f à la base e, on a de même

$$L(e) \subset L(f) \Longleftrightarrow Q \in M_n(\mathbb{Z}).$$

D'où

$$\begin{aligned} L(e) = L(f) &\iff P, Q \in M_n(\mathbb{Z}) \\ &\iff P \in GL_n(\mathbb{Z}) \\ &\iff \det P = \pm 1. \end{aligned}$$

□

4.2 Domaines fondamentaux pour un réseau.

On munit dans ce qui suit l'espace vectoriel $\mathbb{R}^n$ de la mesure de Lebesgue que l'on notera μ.

Définition 4.2.1 *Soient L un réseau de $\mathbb{R}^n$ et X un sous-ensemble mesurable de $\mathbb{R}^n$. On dit que X est un* **domaine fondamental** *de L si tout vecteur v de $\mathbb{R}^n$ s'écrit de manière unique sous la forme*

$$v = v_1 + v_2,$$

avec $v_1 \in L$ et $v_2 \in X$.

Un pavé fondamental est un domaine fondamental comme le montre le résultat suivant.

Lemme 4.2.2 *Soit $e = \{e_1, \ldots, e_n\}$ une base de $\mathbb{R}^n$. Alors $\Pi(e)$ est un domaine fondamental de $L(e)$ et*

$$\mu(\Pi(e)) = |\det(e_1, \ldots, e_n)|.$$

En particulier, on a $0 < \mu(\Pi(e)) < +\infty$.

Preuve : Notons

$$\begin{array}{rccc} J : & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & (v_1, \ldots, v_n) & \longmapsto & \sum_{i=1}^n v_i e_i. \end{array}$$

Par construction, $\Pi(e) = J([0,1[^n)$. Comme $[0,1[^n$ est mesurable et J est continue, on en déduit que $\Pi(e)$ est mesurable. Ainsi $\Pi(e)$ est un domaine fondamental d'après le lemme 4.1.4. De plus, J étant linéaire, on a

$$\begin{aligned} \mu(\Pi(e)) &= \mu(J([0,1[^n)) \\ &= |\det J|\, \mu([0,1[^n) = |\det J| = |\det(e_1, e_2, \ldots, e_n)|. \end{aligned}$$

□

Remarquons que si e et f sont deux bases de $\mathbb{R}^n$ et $P \in GL_n(\mathbb{R})$ est la matrice de passage de la base e à la base f, alors le lemme 4.2.2 implique que

$$\mu(\Pi(f)) = |\det P|\, \mu(\Pi(e)). \tag{4.1}$$

En particulier, si $L(e) = L(f)$, alors $\det P = \pm 1$ d'après le lemme 4.1.8 et donc

$$\mu(\Pi(f)) = \mu(\Pi(e)).$$

Cette observation est en fait un cas particulier du résultat suivant.

Théorème 4.2.3 (Blichfeldt) *Soient L un réseau et X, Y deux parties mesurables. On suppose que*

(i) X est un domaine fondamental de L.

(ii) pour tous $x, y \in Y$, $x - y \in L \Longrightarrow x = y$.

Alors $\mu(Y) \leq \mu(X)$. En particulier, tous les domaines fondamentaux de L ont même mesure, égale à celle d'un pavé fondamental de L.

Preuve : Pour une partie $A \subset \mathbb{R}^n$ et $v \in \mathbb{R}^n$, on notera $A + v = \{a + v : a \in A\}$. Comme X est un domaine fondamental de L, on a

$$\mathbb{R}^n = \bigcup_{\lambda \in L} (X + \lambda),$$

et la réunion est disjointe. Ainsi

$$Y = \bigcup_{\lambda \in L} (Y \cap (X + \lambda)).$$

Or $(Y \cap (X + \lambda)) - \lambda = X \cap (Y - \lambda)$ et comme la mesure de Lebesgue est invariante par translation, on a

$$\mu(Y) = \sum_{\lambda \in L} \mu(X \cap (Y - \lambda)).$$

Or si $\lambda_1, \lambda_2 \in L$, $\lambda_1 \neq \lambda_2$, alors $(Y - \lambda_1) \cap (Y - \lambda_2) = \emptyset$. En effet, sinon il existerait $x, y \in Y$ tel que $x - \lambda_1 = y - \lambda_2$, c'est-à-dire $x - y = \lambda_1 - \lambda_2 \in L$. L'hypothèse impliquerait alors que $x = y$ et donc $\lambda_1 = \lambda_2$, ce qui est en contradiction avec l'hypothèse. Ainsi on a $(Y - \lambda_1) \cap (Y - \lambda_2) = \emptyset$, ce qui implique que

$$\mu(Y) = \mu\left(\bigcup_{\lambda \in L} (X \cap (Y - \lambda))\right) \leq \mu(X).$$

Ceci prouve la première partie de l'énoncé. Pour prouver la deuxième assertion, remarquons que si X est un domaine fondamental de L, alors $x, y \in X$, $x - y \in L \Longrightarrow x = y$. En effet, on a

$$x = y + (x - y) = x + 0,$$

et $y \in X$ et $x - y \in L$. Par unicité de la décomposition, on en déduit donc que $x = y$. Maintenant si X et Y dont deux domaines fondamentaux, alors ce qui précède montre que $\mu(X) = \mu(Y)$.

□

Définition 4.2.4 *Soit L un réseau de $\mathbb{R}^n$. Le* **covolume** *d'un réseau L, noté* $\mathrm{covol}(L)$, *est la mesure d'un domaine fondamental de L. En particulier, si $e = \{e_1, e_2, \ldots, e_n\}$ est une $\mathbb{Z}$-base de L, alors*

$$\mathrm{covol}(L) = |\det(e_1, e_2, \ldots, e_n)|. \tag{4.2}$$

4.3 Le théorème du corps convexe de Minkowski

Théorème 4.3.1 (Minkowski) *Soit $C \subset \mathbb{R}^n$ une partie mesurable, symétrique et convexe et soit L un réseau de $\mathbb{R}^n$. Supposons que l'une des deux conditions supplémentaires soient vérifiées :*

(i) $\mathrm{covol}(L) < 2^{-n}\mu(C)$.

(ii) $\mathrm{covol}(L) \leq 2^{-n}\mu(C)$ *et C est compact.*

Alors il existe $x \in L \cap C$, $x \neq 0$.

Preuve : Soit $L' = 2L \subset L$. Il est clair que L' est un réseau de $\mathbb{R}^n$. De plus, si $e = \{e_1, \ldots, e_n\}$ engendre L, alors la base $2e = \{2e_1, \ldots, 2e_n\}$ engendre L'. D'où

$$\mathrm{covol}(L') = |\det(2e_1, \ldots, 2e_n)| = 2^n\,|\det(e_1, e \ldots, e_n)| = 2^n\,\mathrm{covol}(L).$$

Supposons que l'hypothèse (i) soit satisfaite, c'est-à-dire que $\mathrm{covol}(L') < \mu(C)$. Le lemme de Blichfeldt implique alors qu'il existe $x, y \in C$, $x - y \in L' = 2L$ et $x \neq y$. D'où

$$\frac{x-y}{2} \in L \cap C \quad \text{et} \quad \frac{x-y}{2} \neq 0,$$

ce qui prouve le résultat sous l'hypothèse (i). Supposons maintenant que l'hypothèse (ii) soit satisfaite, c'est-à-dire que C est compact et $\mathrm{covol}(L') \leq \mu(C)$. Soit $\varepsilon > 0$. On considère alors

$$C_\varepsilon = \{v \in \mathbb{R}^n : \mathrm{dist}(v, C) < \varepsilon\}.$$

On vérifie facilement que C_ε est une partie ouverte, bornée, convexe et symétrique. De plus, on a

$$\mathrm{covol}(L') \leq \mu(C) < \mu(C_\varepsilon).$$

Le cas précédent implique alors qu'il existe $x_\varepsilon \in C_\varepsilon \cap L$, $x_\varepsilon \neq 0$. Mais L étant discret et C_ε borné, l'ensemble $C_\varepsilon \cap L$ est fini. De plus, si $\varepsilon < \varepsilon'$, on a $C_\varepsilon \subset C_{\varepsilon'}$.

Ainsi il existe un élément $x \neq 0$ tel que $x \in L \cap C_\varepsilon$ pour tout ε suffisamment petit. En faisant tendre ε vers 0, on obtient que $x \in C$ (car C est compact).

□

Le résultat suivant sera très utile au calcul du covolume de certains réseaux.

Lemme 4.3.2 *Soient L un réseau de $\mathbb{R}^n$ et $L' \subset L$ un sous-groupe d'indice fini. Alors L' est un réseau de $\mathbb{R}^n$ et*

$$\mathrm{covol}(L') = [L : L']\,\mathrm{covol}(L).$$

Preuve : Vérifions que L' est un réseau. Tout d'abord, L' est évidemment un sous-groupe discret de $\mathbb{R}^n$. De plus, comme L' est un sous-groupe d'indice fini, L/L' est fini et notons $p = \mathrm{card}(L/L') = [L : L']$. Alors le théorème de Lagrange assure que $pL \subset L'$. Comme L engendre $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel puisque c'est un réseau, pL engendre aussi $\mathbb{R}^n$ et donc il en est de même de L'. Vérifions maintenant l'assertion sur covolume. Par définition de p, il existe des éléments $\lambda_1, \ldots, \lambda_p \in L$ tels que

$$L = \bigcup_{i=1}^{p} (L' + \lambda_i),$$

et la réunion est disjointe. Soit X un domaine fondamental pour L et considérons

$$X' = \bigcup_{i=1}^{p} (X + \lambda_i).$$

L'ensemble X' est clairement un ensemble mesurable et on a

$$\mu(X') = \sum_{i=1}^{p} \mu(X + \lambda_i) = \sum_{i=1}^{p} \mu(X) = p\mu(X).$$

Remarquons que X' est un domaine fondamental de L' car

$$\mathbb{R}^n = \bigcup_{\lambda \in L} (X + \lambda) = \bigcup_{i=1}^{p} \bigcup_{\lambda' \in L'} (X + \lambda_i + \lambda') = \bigcup_{\lambda' \in L'} (X' + \lambda').$$

D'où

$$\mathrm{covol}(L') = \mu(X') = p\mu(X) = p\,\mathrm{covol}(L).$$

□

4.4 Quelques applications en arithmétique

4.4.1 Somme de deux carrés.

Théorème 4.4.1 (Fermat-Euler) *Soit p un nombre premier. Si $p \equiv 1 \pmod 4$, alors il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.*

Preuve : Comme $p \equiv 1 \pmod 4$, on sait d'après le théorème 3.2.5 que -1 est un carré modulo p. Autrement dit, il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv -1 \pmod p$. Soit

$$L = \{(a,b) \in \mathbb{Z}^2 : a \equiv ub \pmod p\}$$

et soit

$$\begin{array}{rccc} \psi : & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & (a,b) & \longmapsto & a - bu \pmod p. \end{array}$$

On vérifie facilement que ψ est un morphisme de groupes surjectifs et on a $\ker \psi = L$. Donc ψ induit un isomorphisme entre $\mathbb{Z}^2/L$ et $\mathbb{Z}/p\mathbb{Z}$. On obtient ainsi que L est un sous-groupe d'indice fini de $\mathbb{Z}^2$. Le lemme 4.3.2 implique que L est un réseau de $\mathbb{R}^2$ et

$$\operatorname{covol}(L) = [\mathbb{Z}^2 : L] \operatorname{covol}(\mathbb{Z}^2).$$

Comme $\mathbb{Z}^2/L \simeq \mathbb{Z}/p\mathbb{Z}$, on a $[\mathbb{Z}^2 : L] = p$ et on vérifie facilement que $\operatorname{covol}(\mathbb{Z}^2) = 1$. D'où $\operatorname{covol}(L) = p$. Considérons maintenant le disque euclidien

$$C(r) = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 < r\}.$$

Il est clair que $C(r)$ est un ouvert, convexe, symétrique de mesure πr. D'après le théorème 4.3.1, il existe un élément non nul dans $L \cap C(r)$ dès que

$$\operatorname{covol}(L) < \frac{\mu(C(r))}{2^2},$$

soit $\frac{4p}{\pi} < r$. Ainsi par exemple, il existe un élément non nul $(a,b) \in L \cap C(2p)$. D'une part, on a

$$0 < a^2 + b^2 < 2p$$

et d'autre part, comme $(a,b) \in L$ et $u^2 + 1 \equiv 0 \pmod p$, on a

$$a^2 + b^2 \equiv u^2b^2 + b^2 \equiv b^2(u^2+1) \equiv 0 \pmod p.$$

Donc la seule possibilité est que $a^2 + b^2 = p$.

□

Corollaire 4.4.2 *Un nombre entier naturel n s'écrit comme la somme de deux carrés si et seulement si n vérifie la propriété suivante : pour tout nombre premier p impair de la forme $4k+3$, on a*

$$v_p(n) > 0 \Longrightarrow v_p(n) \in 2\mathbb{N}^*. \tag{4.3}$$

Preuve : Si m et n sont représentables en somme de deux carrés, disons $n = a^2 + b^2$ et $m = c^2 + d^2$, alors

$$mn = (ac + bd)^2 + (ad - bc)^2.$$

Supposons que l'entier n vérifie la condition (4.3). Alors n peut s'écrire

$$n = 2^k p_1^{k_1} \dots p_r^{k_r} q_1^{2\ell_1} \dots q_s^{2\ell_s},$$

avec p_j, q_j des nombres premiers tels que $p_j \equiv 1 \pmod 4$ et $q_j \equiv 3 \pmod 4$. Remarquons que $q_j^2 \equiv 1 \pmod 4$, $1 \leq j \leq s$. D'après le théorème 4.4.1, les nombres $p_1, \dots, p_r$ et $q_1^2, \dots, q_s^2$ peuvent s'écrire comme une somme de deux carrés. L'entier 2 peut aussi s'écrire comme une somme de deux carrés ($2 = 1^2 + 1^2$). Par la remarque faite au début de la preuve, on en déduit que l'entier n peut aussi s'écrire comme une somme de deux carrés.

Réciproquement, supposons que $n = a^2 + b^2$. Soit $d = (a, b)$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ et $n_1 = \frac{n}{d^2}$. On a $n_1 = a_1^2 + b_1^2$ avec $(a_1, b_1) = 1$. Supposons que q est un nombre premier de la forme $4k + 3$ et supposons que $v_q(n)$ est un nombre impair. On a

$$v_q(n) = v_q(n_1 d^2) = v_q(n_1) + 2v_q(d).$$

Comme $v_q(n)$ est impair, nécessairement $v_q(n_1)$ est impair, donc en particulier non nul. Autrement dit, l'entier q divise n_1. Comme $(a_1, b_1) = 1$, on a nécessairement que q ne divise pas a_1 ni b_1. Or $-b_1^2 \equiv a_1^2 \pmod q$, d'où on en déduit que

$$1 = \left(\frac{-b_1^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{b_1^2}{q}\right) = \left(\frac{-1}{q}\right).$$

Il suit alors du théorème 3.2.5 que $q \equiv 1 \pmod 4$, ce qui contredit l'hypothèse.

□

4.4.2 Somme de quatre carrés.

Théorème 4.4.3 (Lagrange) *Tout entier $n \geq 0$ est somme de quatre carrés.*

Preuve : La preuve va se décomposer en plusieurs étapes.

Etape 1 : on peut supposer que n est un nombre premier impair.

En effet, si m et n sont deux entiers représentables comme somme de quatre carrés, disons

$$m = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad n = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

alors on vérifie que

$$\begin{aligned} mn = &(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Donc mn est aussi représentable comme somme de 4 carrés, ce qui montre qu'il suffit de prouver le résultat pour un nombre premier $p \geq 3$ (remarquons que pour $n = 0, 1$ et 2, le résultat est trivial).

Etape 2 : il existe $x, y \in \mathbb{Z}$ tels que $x^2 + y^2 \equiv -1 \,(\mathrm{mod}\, p)$.

Considérons l'ensemble

$$E = \{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$$

des carrés modulo p. D'après le théorème 3.1.2, on sait que $\mathrm{card}(E) = \frac{p+1}{2}$. De même, l'ensemble $F = \{-1 - x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ a aussi $\frac{p+1}{2}$ éléments. Ainsi nécessairement, on a $E \cap F \neq \emptyset$. Autrement dit, il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ tel que $x^2 = -1 + y^2$, c'est-à-dire $x^2 + y^2 = -1$, ce qui prouve l'étape 2.

Etape 3 : soit $u, v \in \mathbb{Z}$ tel que $u^2 + v^2 = -1 \,(\mathrm{mod}\, p)$ et considérons

$$L = \{(a, bc, d) \in \mathbb{Z}^4 : c \equiv au + bv \,(\mathrm{mod}\, p) \,\&\, d \equiv av - bu \,(\mathrm{mod}\, p)\}.$$

Alors L est un réseau de $\mathbb{R}^4$ de covolume p^2.

En effet, considérons

$$\begin{array}{rccc} \psi : & \mathbb{Z}^4 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 \\ & (a, b, c, d) & \longmapsto & (c - au - bv \bmod p, d - av + bu \bmod p). \end{array}$$

On vérifie facilement que ψ est un morphisme de groupes surjectif et $\ker \psi = L$. D'où ψ induit un isomorphisme de groupes de $\mathbb{Z}^4/L$ sur $(\mathbb{Z}/p\mathbb{Z})^2$. Ceci implique que L est un sous-groupe de $\mathbb{Z}^4$ d'indice fini et $[\mathbb{Z}^4 : L] = p^2$. Donc le lemme 4.3.2 implique que L est un réseau de $\mathbb{R}^4$ de covolume p^2.

Etape 4 : l'entier p s'écrit comme une somme de 4 carrés.

Nous allons appliquer le théorème de Minkowski. A cet effet, introduisons maintenant

$$C(r) = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : \sum_{i=1}^{4} x_i^2 < r\}.$$

Il est clair que $C(r)$ est un ouvert convexe, symétrique et un calcul classique montre que $\mu(C(r)) = \frac{\pi^2 r^2}{2}$. Le théorème de Minkowski implique donc que si

$$\mathrm{covol}(L) < \frac{\mu(C(r))}{2^4}, \tag{4.4}$$

alors il existe un élément non nul dans $C(r) \cap L$. Or (4.4) équivaut à $16p^2 < \frac{\pi^2 r^2}{2}$, c'est-à-dire $r > \frac{4\sqrt{2}}{\pi} p$. En particulier, il existe un élément non nul $(a, b, c, d) \in L \cap C(2p)$. On a alors

$$0 < a^2 + b^2 + c^2 + d^2 < 2p,$$

et d'autre part,

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (au + bv)^2 + (av - bu)^2 \,(\mathrm{mod}\, p) \\ &\equiv a^2 + b^2 + a^2u^2 + b^2v^2 + a^2v^2 + b^2u^2 \,(\mathrm{mod}\, p) \\ &\equiv a^2(1 + u^2 + v^2) + b^2(1 + u^2 + v^2) \,(\mathrm{mod}\, p) \\ &\equiv 0 \bmod p. \end{aligned}$$

Donc la seule possibilité est $a^2 + b^2 + c^2 + d^2 = p$.

□

4.5 Exercices

Exercice 4.5.1 *Le but de cet exercice est de retrouver via une méthode connue sous le nom de* **descente infinie**, *le théorème d'Euler suivant :*

si p est un nombre premier congru à $1 \bmod 4$, alors p peut s'écrire comme la somme de deux carrés.

On suppose donc que $p \equiv 1 \pmod 4$.

(a) Montrer qu'il existe un entier $x_0 \in \mathbb{Z}$ *tel que* $-\frac{p}{2} < x_0 \leq \frac{p}{2}$ *et* $0 < \ell < p$ *tel que* $x_0^2 + 1 = \ell p$.

(b) Soit m *le plus petit entier naturel (non nul) tel que* mp *puisse s'écrire comme somme de deux carrés*

$$mp = x_1^2 + y_1^2.$$

Si $m = 1$, *le théorème est démontré. Supposons donc que* $m > 1$. *On a donc* $1 < m \leq \ell < p$. *Choisissons* $x_2, y_2 \in (-\frac{m}{2}, \frac{m}{2})$ *tels que*

$$x_2 \equiv x_1 \pmod m \quad et \quad y_2 \equiv y_1 \pmod m.$$

(i) Montrer qu'il existe $0 \leq r < m$ *tel que* $x_2^2 + y_2^2 = rm$.

(ii) Montrer que $r \neq 0$ *(on pourra raisonner par l'absurde).*

(iii) Montrer que

$$x_1 y_2 - x_2 y_1 \equiv 0 \pmod m \quad et \quad x_1 x_2 + y_1 y_2 \equiv 0 \pmod m$$

(iv) En déduire qu'il existe $x_3, y_3 \in \mathbb{Z}$ *tels que* $x_3^2 + y_3^2 = rp$.

(v) Conclure.

Exercice 4.5.2 *Le but de cet exercice est de retrouver via la méthode de la descente infinie le théorème de Girard, Fermat, Lagrange suivant :*

tout entier naturel peut s'écrire comme la somme de 4 carrés.

Comme on l'a vu dans la première étape de la preuve du théorème 4.4.3, on peut supposer que l'entier $n = p$ *est un nombre premier.*

(a) Si $p \equiv 1 \bmod 4$, *prouver le résultat.*

(b) On suppose maintenant dans toute la suite que $p \equiv 3 \bmod 4$. *Soit* z *le plus petit entier positif qui est un non résidu quadratique modulo* p.

(i) Vérifier que $z \geq 2$ *et que* $z-1$ *est un résidu quadratique.*

(ii) Montrer que $-z$ *est un résidu quadratique modulo* p.

(iii) Montrer qu'il existe $x_0, y_0, m_0 \in \mathbb{Z}$ *tels que* $x_0^2 + y_0^2 + 1 = m_0 p$ *et* $|x_0| < \frac{p}{2}$, $|y_0| < \frac{p}{2}$ *et* $1 \leq m_0 < p$.

(c) Soit m *le plus petit entier naturel (non nul) tel que* mp *puisse s'écrire comme la somme de* 4 *carrés. Si* $m = 1$, *le théorème est démontré. Supposons donc que* $m > 1$ *et* $mp = a^2 + b^2 + c^2 + d^2$. *Choisissons* $A, B, C, D \in (-\frac{m}{2}, \frac{m}{2}]$ *tels que*

$$a \equiv A \,(\mathrm{mod}\, m), \quad b \equiv B \,(\mathrm{mod}\, m), \quad c \equiv C \,(\mathrm{mod}\, m) \quad et \quad d \equiv D \,(\mathrm{mod}\, m).$$

(i) Montrer qu'il existe $0 \leq r \leq m$ *tel que*

$$A^2 + B^2 + C^2 + D^2 = rm.$$

(ii) Montrer que $r \neq 0$ *et* $r \neq m$ *(on pourra raisonner par l'absurde).*

(iii) Montrer qu'il existe $\alpha, \beta, \gamma, \delta \equiv 0 \,(\mathrm{mod}\, m)$ *tels que*

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

(iv) Montrer que rp *peut s'écrire comme la somme de* 4 *carrés et conclure.*

Exercice 4.5.3 *Le but de cet exercice est de donner une troisième démonstration du théorème d'Euler à travers la théorie des anneaux et plus particulièrement de* $\mathbb{Z}[i]$. *Rappelons que* $\mathbb{Z}[i]$ *est défini comme le sous-anneau de* $\mathbb{C}$ *formé des nombres complexes* $a + ib$, $a, b \in \mathbb{Z}$.

(a) Soit $N(a+ib) = a^2 + b^2$ *la norme de l'élément* $a + ib \in \mathbb{Z}[i]$.

(i) Montrer que $N(xy) = N(x)N(y)$, *pour tous* $x, y \in \mathbb{Z}[i]$.

(ii) En déduire que x *est inversible dans* $\mathbb{Z}[i]$ *si et seulement si* $N(x) = 1$.

(iii) En déduire que l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ *est*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

(b) Montrer que $\mathbb{Z}[i]$ *est euclidien donc principal.*

Indication : *on pourra montrer que si* $x, y \in \mathbb{Z}[i]$, *alors*

- *si* x *divise* y, *on a* $N(x) \leq N(y)$.
- *si* x *ne divise pas* y, *alors il existe* q *et* $r \in \mathbb{Z}[i]$ *tels que*

$$y = qx + r \quad avec\ N(r) < N(x).$$

(c) Soit p un nombre premier tel que $p \equiv 1 \bmod 4$. On sait qu'il existe $a \in \mathbb{Z}$ tel que $a^2 \equiv -1 \bmod p$.

(i) Montrer que l'élément p n'est pas premier dans $\mathbb{Z}[i]$. Donc il n'est pas irréductible et il existe $\alpha, \beta \in \mathbb{Z}[i]$ non inversibles tels que $p = \alpha\beta$.

(ii) En déduire que $N(\alpha) = p$, puis que p s'écrit comme la somme de deux carrés.

Exercice 4.5.4 *Pour tout entier naturel $n \geq 1$ on note $r_3(n)$ le nombre de triplets $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tels que*

$$n = x_1^2 + x_2^2 + x_3^2.$$

1. *Démontrer que si $n \equiv 7 \pmod 8$, $r_3(n) = 0$.*
2. *Démontrer que $r_3(4n) = r_3(n)$.*
3. *En déduire que si $n = 4^a(8b+7)$ où $a \in \mathbb{N}$, $b \in \mathbb{N}$, alors n n'est pas une somme de 3 carrés.*

Gauss a démontré la réciproque : tout entier naturel n qui n'est pas de la forme $n = 4^a(8b + 7)$ est une somme de 3 carrés.

Chapitre 5

Autour de la répartition des nombres premiers : approches élémentaires.

Les nombres premiers jouent un rôle important en théorie des nombres. Dans ce chapitre, nous discutons, via des approches élémentaires, de la répartition des nombres premiers. On s'intéresse plus précisément à la fonction

$$\pi(x) := \sum_{p \leq x} 1$$

qui compte le nombre de nombres premiers $p \leq x$.

5.1 Introduction

La preuve fournie par Euclide de l'infinité des nombres premiers permet de donner une minoration de $\pi(x)$.

Théorème 5.1.1 (Euclide) *La suite des nombres premiers* $p_1 = 2 < p_2 = 3 < p_3 < \cdots < p_n < \ldots$ *est infinie et pour tout entier* $n \geq 1$, *on a*

$$p_n \leq 2^{2^{n-1}}.$$

Preuve : On vérifie trivialement que $p_1 = 2 \leq 2^{2^0}$ et $p_2 = 3 \leq 2^{2^1}$. Supposons que pour un certain entier $n \geq 3$ et pour tout $k = 1, \ldots, n-1$, on ait $p_k \leq 2^{2^{k-1}}$. Le nombre entier $p_1 p_2 \ldots p_{n-1} - 1$ n'est divisible par aucun des nombres premiers $p_1, \ldots, p_{n-1}$. Donc

$$p_n \leq p_1 \ldots p_{n-1} \leq 2^{2^0+2^1+\cdots+2^{n-2}} = 2^{2^{n-1}-1} \leq 2^{2^{n-1}}.$$

□

On en déduit tout de suite une minoration de $\pi(x)$.

Corollaire 5.1.2 *Pour tout $x \geq 2$, on a*

$$\pi(x) \geq \ln \ln x.$$

Preuve : D'après le théorème d'Euclide, on a

$$\pi(2^{2^{n-1}}) \geq n.$$

Soit $x \geq 2$ et considérons l'entier n défini par $=$

$$n = 1 + \left\lfloor \frac{\ln(\ln x / \ln 2)}{\ln 2} \right\rfloor.$$

L'entier n satisfait les inégalités suivantes

$$2^{2^{n-1}} \leq x \leq 2^{2^n}.$$

La fonction π étant croissante, on en déduit que

$$\pi(x) \geq \pi(2^{2^{n-1}}) \geq n \geq \frac{\ln(\ln x / \ln 2)}{\ln 2}.$$

Il suffit maintenant de montrer que pour tout $x \geq 2$, on a $\frac{\ln(\ln x / \ln 2)}{\ln 2} \geq \ln \ln x$. Cette inégalité est clairement équivalente à

$$(1 - \ln 2) \ln \ln x \geq \ln \ln 2.$$

Or la fonction $x \longmapsto (1 - \ln 2) \ln \ln x$ est croissante, donc pour tout $x \geq 2$, on a

$$(1 - \ln 2) \ln \ln x \geq (1 - \ln 2) \ln \ln 2.$$

Il ne reste plus qu'à remarquer que $\ln \ln 2 \leq 0$, ce qui donne

$$(1 - \ln 2) \ln \ln 2 \geq \ln \ln 2.$$

□

L'approximation fournit par le théorème d'Euclide peut être grandement améliorée. C. Gauss a conjecturé en 1792 que

$$\pi(x) \sim \frac{x}{\ln x}, \qquad x \to +\infty.$$

En utilisant des méthodes d'analyse complexe et notamment l'étude des propriétés analytiques de la fonction ζ de Riemann (en particulier que $\zeta(s) \neq 0$, pour tout s tel que $\Re(s) \geq 1$), cette conjecture a finalement été prouvée en 1896 par J. Hadamard et C.J. de La Vallée Poussin (de façon indépendante) et est maintenant connue sous le nom de *théorème des nombres premiers*.

Théorème 5.1.3 (Théorème des nombres premiers) *On a*

$$\pi(x) \sim \frac{x}{\ln x}, \qquad x \to +\infty.$$

La preuve de ce théorème dépasse le cadre de ce cours. Nous nous contenterons ici d'estimations plus élémentaires.

5.2 Inégalités de type Chebyshev

Dans le résultat suivant, nous allons montrer que $\pi(x)$ peut être encadré par $c_1\frac{x}{\ln x}$ et $c_2\frac{x}{\ln x}$, où c_1 et c_2 sont deux constantes explicites. Avec le théorème des nombres premiers, on sait qu'asymptotiquement, ces constantes peuvent être choisies aussi proche de 1 qu'on veut. Ici, nous n'avons pas cherché à obtenir les meilleures constantes. Notre but est de montrer comment des méthodes "élémentaires" peuvent déjà conduire à des résultats intéressants.

Théorème 5.2.1 *Pour tout $x \geq 2$, on a*

$$\frac{\ln 2}{6}\frac{x}{\ln x} \leq \pi(x) \leq 4\frac{x}{\ln x}.$$

La preuve de ce théorème qui va nous occuper toute cette section est basée sur une série de 4 lemmes.

Lemme 5.2.2 *Soit $m \geq 1$. On a*

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 4^m.$$

Preuve : On a

$$\binom{2m+1}{m} = \frac{(2m+1)2m\ldots(2m+1-m+1)}{m!} = \frac{1}{m!}\prod_{k=m+2}^{2m+1} k.$$

Soit p un nombre premier, $m+1 < p \leq 2m+1$. D'après l'égalité précédente, p divise $m!\binom{2m+1}{m}$. Comme p ne divise pas $m!$, nécessairement p divise $\binom{2m+1}{m}$. Autrement dit, $\binom{2m+1}{m}$ est un multiple de chacun des nombres premiers p, $m+1 < p \leq 2m+1$, donc de leur produit. Ainsi

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m},$$

ce qui démontre la première inégalité.

Pour la deuxième inégalité, remarquons que

$$2^{2m+1} = (1+1)^{2m+1} = \sum_{k=0}^{2m+1}\binom{2m+1}{k} \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m}.$$

Ceci implique que $2 \times 4^n \geq 2\binom{2m+1}{m}$, ce qui donne l'inégalité désirée.

□

Lemme 5.2.3 *Pour tout entier $n \geq 1$, on a*

$$\prod_{p\leq n} p < 4^n.$$

Preuve : Raisonnons par récurrence. Pour $n = 1, 2$, l'inégalité est évidente. Supposons le résultat vrai pour un certain entier n et tout $k = 1, 2, \ldots, n-1$. Si n est pair, on a

$$\prod_{p \leq n} = \prod_{p \leq n-1} p < 4^{n-1} < 4^n.$$

Si n est impair, $n = 2m+1$, en utilisant le lemme 5.2.2,

$$\prod_{p \leq n} p = \left(\prod_{p \leq m+1} p \right) \left(\prod_{m+1 < p \leq 2m+1} p \right) \leq 4^m \prod_{p \leq m+1} p.$$

L'hypothèse de récurrence implique que

$$\prod_{p \leq m+1} p < 4^{m+1}.$$

D'où

$$\prod_{p \leq n} p < 4^{2m+1} = 4^n.$$

□

Corollaire 5.2.4 *Pour tout $x \geq 1$, on a*

$$\prod_{p \leq x} p < 4^x.$$

Preuve : Soit $x \geq 1$ et $n = \lfloor x \rfloor$. En utilisant le lemme 5.2.3, on a

$$\prod_{p \leq x} p = \prod_{p \leq n} p < 4^n \leq 4^x.$$

□

Lemme 5.2.5 *Pour tout entier $n \geq 1$, on a*

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Preuve : Pour la première inégalité, il suffit de remarquer que

$$\binom{2n}{n} < (1+1)^{2n} = 2^{2n} = 4^n.$$

Pour la seconde inégalité, écrivons que

$$2^{2n-1} = \sum_{k=0}^{2n-1} \binom{2n-1}{k}$$

et remarquons que $\binom{2n-1}{k} \leq \binom{2n-1}{n-1}$, pour tout $k = 0, 1, \ldots, 2n-1$. D'où

$$2^{2n-1} \leq 2n \binom{2n-1}{n-1},$$

soit

$$\frac{4^n}{2n} \leq 2\binom{2n-1}{n-1} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = \binom{2n}{n}.$$

□

Lemme 5.2.6 *Supposons que p^α divise $\binom{2n}{n}$, pour un certain nombre premier p et un certain entier $\alpha \geq 1$. Alors*

$$p^\alpha \leq 2n.$$

Preuve : La formule de Legendre (voir exercice 1.7.18) implique que

$$v_p(m!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{m}{p^k} \right\rfloor.$$

Or $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. D'où

$$v_p\left(\binom{2n}{n}\right) = v_p((2n)!) - 2v_p(n!) = \sum_{k=1}^{+\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Notons que dès que $k > \frac{\ln(2n)}{\ln p}$, on a

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor = 0.$$

De plus, la fonction $x \longmapsto \lfloor 2x \rfloor - 2\lfloor x \rfloor$ est 1-périodique et on a

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0 & \text{si } 0 \leq x < 1/2 \\ 1 & \text{si } 1/2 \leq x < 1. \end{cases}$$

D'où

$$\begin{aligned} \alpha \leq v_p\left(\binom{2n}{n}\right) &= \sum_{k=1}^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right) \\ &\leq \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor \leq \frac{\ln(2n)}{\ln p}. \end{aligned}$$

Ceci implique alors que $p^\alpha \leq 2n$.

□

Nous sommes maintenant prêt pour prouver le théorème.

Preuve du théorème 5.2.1 : Montrons tout d'abord que $\pi(x) < 4x/\ln x$.

On écrit

$$\prod_{p \leq n} p > \prod_{\sqrt{n} < p \leq n} p \geq \sqrt{n}^{\,\pi(n) - \pi(\sqrt{n})}.$$

En utilisant le lemme 5.2.3, on obtient

$$n^{\frac{1}{2}(\pi(n) - \pi(\sqrt{n}))} < 4^n,$$

soit

$$\pi(n) - \pi(\sqrt{n}) < \frac{2n \ln 4}{\ln n} < \frac{3n}{\ln n}.$$

Puisque, pour $n \geq 2$, on a $\pi(\sqrt{n}) \leq \sqrt{n} < n/\ln n$, on obtient finalement

$$\pi(n) \leq 4\frac{\ln n}{n}.$$

Par conséquent, en utilisant la croissance de la fonction $t \longmapsto t/\ln t$ sur $[e, +\infty[$, on en déduit que

$$\pi(x) = \pi(\lfloor x \rfloor) < 4\frac{\lfloor x \rfloor}{\ln \lfloor x \rfloor} \leq 4\frac{x}{\ln x},$$

pour tout $x \geq 2$.

Montrons maintenant que $\pi(x) > \frac{\ln 2}{6}\frac{x}{\ln x}$.

D'une part, le lemme 5.2.6 implique que

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{v_p(\binom{2n}{n})} \leq \prod_{p \leq 2n} 2n = (2n)^{\pi(2n)}.$$

D'autre part, d'après le lemme 5.2.5, on a

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n},$$

d'où

$$(2n)^{\pi(2n)} \geq \frac{2^{2n}}{2n},$$

soit

$$\pi(2n) \geq \frac{2n \ln 2}{\ln(2n)} - 1, \qquad n \geq 1.$$

On vérifie alors facilement que

$$\frac{2n \ln 2}{\ln(2n)} - 1 \geq \frac{n \ln 2}{\ln(2n)},$$

ce qui donne

$$\pi(2n) \geq n\frac{\ln 2}{\ln(2n)}.$$

Pour conclure, remarquons que l'inégalité $\pi(x) > \frac{\ln 2}{6}\frac{x}{\ln x}$ est triviale si $2 \leq x < 3$. On peut donc supposer que $x \geq 3$ et on pose $n = \lfloor x/2 \rfloor$. On a donc

$$2n \leq x < 2(n+1),$$

ce qui implique

$$\begin{aligned}
\pi(x) &\geq \pi(2n) \geq \frac{n \ln 2}{\ln(2n)} \\
&\geq \frac{\ln 2}{\ln x}\left(\frac{x}{2} - 1\right) \\
&= \frac{x}{\ln x}\ln 2\left(\frac{1}{2} - \frac{1}{x}\right) \\
&\geq \frac{x}{\ln x}\ln 2\left(\frac{1}{2} - \frac{1}{3}\right) = \frac{\ln 2}{6}\frac{x}{\ln x}.
\end{aligned}$$

□

5.3 Les fonctions de Chebyshev

En dehors de $\pi(x)$, deux autres sommes apparaissent naturellement dans l'étude de la répartition des nombres premiers. Il s'agit des deux fonctions de Chebyshev

$$\Theta(x) := \sum_{p \leq x} \ln p$$

et

$$\Psi(x) := \sum_{p^m \leq x} \ln p.$$

Dans cette section, nous allons montrer comment les fonctions $\Theta(x)$, $\Psi(x)$ et $\pi(x)$ sont intimement reliées entre elles. Donnons une première estimation élémentaire qui découle du corollaire 5.2.4.

Lemme 5.3.1 *On a*

$$\Theta(x) \leq (2 \ln 2)x.$$

Preuve : Il suffit d'écrire que

$$e^{\Theta(x)} = \prod_{p \leq x} p \leq 4^x.$$

D'où

$$\Theta(x) \leq x \ln 4 = (2 \ln 2)x.$$

□

Le résultat suivant donne le lien entre $\Theta(x)$ et $\Psi(x)$.

Lemme 5.3.2 *Pour tout $x \geq 2$, on a*

$$\Theta(x) \leq \Psi(x) \leq \Theta(x) + 2\sqrt{x} \ln x.$$

Preuve : Soit k le plus grand entier tel que $x^{1/k} \geq 2$, c'est-à-dire $k = \lfloor \ln x / \ln 2 \rfloor$. On a alors

$$\Psi(x) = \sum_{m=1}^{k} \sum_{p \leq x^{1/m}} \ln p = \sum_{m=1}^{k} \Theta(x^{1/m}).$$

En particulier, on a donc

$$\Psi(x) = \Theta(x) + \sum_{m=2}^{k} \Theta(x^{1/m}) \geq \Theta(x).$$

D'autre part, en utilisant le lemme 5.3.1, on obtient que

$$\Psi(x) \leq \Theta(x) + 2 \ln 2 \sum_{m=2}^{k} x^{1/m} \leq \Theta(x) + 2 \ln 2 k \sqrt{x}.$$

Comme $k \leq \ln x / \ln 2$, on en déduit que

$$\Psi(x) \leq \Theta(x) + 2\sqrt{x} \ln x.$$

□

On peut maintenant donner le lien entre les fonctions Θ et π.

Lemme 5.3.3 *Pour tout $x \geq 2$, on a*

$$\frac{\Theta(x)}{\ln x} \leq \pi(x) \leq \frac{\Theta(x)}{\ln x - 2\ln\ln x} + \frac{x}{(\ln x)^2}.$$

Preuve : La première inégalité découle de l'estimation suivante

$$\Theta(x) = \sum_{p \leq x} \ln p \leq \ln x \sum_{p \leq x} 1 = \pi(x) \ln x.$$

Pour la deuxième inégalité, notons que pour $2 \leq y < x$, on a

$$\begin{aligned} \pi(x) - \pi(y) &= \sum_{y < p \leq x} 1 \leq \frac{1}{\ln y} \sum_{y < p \leq x} \ln p \\ &\leq \frac{1}{\ln y} \left(\Theta(x) - \Theta(y)\right). \end{aligned}$$

On en tire

$$\pi(x) \leq \frac{\Theta(x)}{\ln y} + \pi(y) \leq \frac{\Theta(y)}{\ln y} + y.$$

En choisissant $y = x/(\ln x)^2$, on en déduit que

$$\pi(x) \leq \frac{\Theta(x)}{\ln x - 2\ln\ln x} + \frac{x}{(\ln x)^2},$$

ce qui prouve la deuxième inégalité.

□

Théorème 5.3.4 *Les assertions suivantes sont équivalentes :*

(i) $\pi(x) \sim x/\ln x$, *lorsque* $x \to +\infty$.

(ii) $\Theta(x) \sim x$, *lorsque* $x \to +\infty$.

(iii) $\Psi(x) \sim x$, *lorsque* $x \to +\infty$.

Preuve : En utilisant les lemmes 5.3.2 et 5.3.3, on a

$$\frac{\Theta(x)}{x} \leq \frac{\psi(x)}{x} \leq \frac{\Theta(x)}{x} + \frac{2\ln x}{\sqrt{x}}$$

et

$$\frac{\Theta(x)}{x} \leq \frac{\pi(x)\ln x}{x} \leq \frac{\Theta(x)}{x} \frac{\ln x}{\ln x - 2\ln\ln x} + \frac{1}{\ln x}.$$

Le résultat suit alors immédiatement.

□

5.4 Estimations de fonctions sommatoires

Si a est une fonction de $\mathbb{N}$ dans $\mathbb{C}$, on posera pour tout $x \in \mathbb{R}_+$,

$$A(x) = \sum_{n \leq x} a(n).$$

Le résultat suivant découle facilement de la transformation d'Abel.

Théorème 5.4.1 (Formule d'Abel) *Soient $0 < y < x$, $f : [y, x] \longrightarrow \mathbb{C}$ une fonction de classe C^1 et $a : \mathbb{N} \longrightarrow \mathbb{C}$. Alors*

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t)\, dt.$$

En particulier, pour $x > 1$ et f de classe C^1 sur $[1, x]$, on a

$$\sum_{n \leq x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t)\, dt.$$

Preuve : Introduisons $p = \lfloor y \rfloor$ et $q = \lfloor x \rfloor$ et remarquons tout d'abord que

$$\sum_{y < n \leq x} a(n) f(n) = \sum_{n=p+1}^{q} a(n) f(n).$$

En utilisant que $a(n) = A(n) - A(n-1)$ et en effectuant une transformation d'Abel, on obtient alors

$$\begin{aligned} \sum_{y < n \leq x} a(n) f(n) &= \sum_{n=p+1}^{q} A(n) f(n) - \sum_{n=p+1}^{q} A(n-1) f(n) \\ &= \sum_{n=p+1}^{q-1} A(n)(f(n) - f(n+1)) + A(q) f(q) - A(p) f(p+1). \end{aligned}$$

Or, la fonction f étant supposée de classe C^1, on peut écrire

$$f(n) - f(n+1) = -\int_n^{n+1} f'(t)\, dt$$

et pour $t \in [n, n+1[$ on a $A(t) = A(n)$. D'où

$$\begin{aligned} \sum_{y < n \leq x} a(n) f(n) &= -\sum_{n=p+1}^{q-1} \int_n^{n+1} A(t) f'(t)\, dt + A(q) f(q) - A(p) f(p+1) \\ &= -\int_{p+1}^{q} A(t) f'(t)\, dt + A(q) f(q) - A(p) f(p+1). \end{aligned}$$

Or

$$\int_{p+1}^{q} A(t) f'(t)\, dt = \int_{p+1}^{y} A(t) f'(t)\, dt + \int_y^x A(t) f'(t)\, dt + \int_x^q A(t) f'(t)\, dt,$$

et en utilisant une nouvelle fois que pour $t \in [n, n+1[$, $A(t) = A(n)$, on en déduit que

$$\int_{p+1}^{q} A(t)f'(t)\,dt = \int_{y}^{x} A(t)f'(t)\,dt + A(p)(f(y) - f(p+1)) + A(q)(f(q) - f(x)).$$

D'où

$$\sum_{y<n\leq x} a(n)f(n) = -\int_{y}^{x} A(t)f'(t)\,dt + A(q)f(x) - A(p)f(y).$$

Pour conclure, il reste à utiliser (une nouvelle fois) que $A(q) = A(x)$ et $A(p) = A(y)$.

La deuxième formule découle immédiatement de la première en écrivant que

$$\sum_{n\leq x} a(n)f(n) = a(1)f(1) + \sum_{1<n\leq x} a(n)f(n)$$

et en remarquant que $a(1) = A(1)$.

□

Nous allons maintenant montrer comment cette formule permet d'estimer $A(x)$ pour certaines fonctions arithmétiques a liées aux nombres premiers, et dont le comportement asymptotique est plus facilement accessible que celui de la fonction $\pi(x)$.

Théorème 5.4.2 (Mertens) *On a*

$$\sum_{p\leq x} \frac{\ln p}{p} = \ln x + O(1). \tag{5.1}$$

De plus, il existe une constante $C > 0$ telle que

$$\sum_{p\leq x} \frac{1}{p} = \ln\ln x + C + O(1/\ln x). \tag{5.2}$$

En particulier, les deux séries

$$\sum_{p\in\mathbb{P}} \frac{\ln p}{p} \quad \text{et} \quad \sum_{p\in\mathbb{P}} \frac{1}{p}$$

divergent.

Preuve : Pour démontrer la formule (5.1), on va calculer $\ln(\lfloor x\rfloor!)$ de deux manières. Tout d'abord on utilise la formule d'Abel avec $a(n) = 1$, $n \geq 1$, $f(t) = \ln t$ et $x > 1$. On vérifie immédiatement que $A(t) = \lfloor t\rfloor$, ce qui donne

$$\ln(\lfloor x\rfloor!) = \sum_{n\leq x} \ln n = \lfloor x\rfloor \ln x - \int_{1}^{x} \lfloor t\rfloor \frac{dt}{t}.$$

En introduisant $\{t\} = t - \lfloor t\rfloor$ la partie fractionnaire du réel t, on obtient

$$\begin{aligned} \ln(\lfloor x\rfloor!) &= (x - \{x\})\ln x - \int_{1}^{x} \frac{t - \{t\}}{t}\,dt \\ &= x\ln x - \{x\}\ln x - (x-1) + \int_{1}^{x} \frac{\{t\}}{t}\,dt. \end{aligned}$$

Comme $0 \leq \{t\} < 1$, on a

$$\left| \int_1^x \frac{\{t\}}{t}\, dt \right| \leq \int_1^x \frac{dt}{t} = \ln x.$$

D'où, on en déduit

$$\ln(\lfloor x \rfloor !) = x \ln x - x + O(\ln x). \tag{5.3}$$

D'autre part, en écrivant

$$\begin{aligned} \ln(\lfloor x \rfloor !) &= \ln \left(\prod_{p \leq x} p^{v_p(\lfloor x \rfloor !)} \right) \\ &= \sum_{p \leq x} v_p(\lfloor x \rfloor !) \ln p, \end{aligned}$$

et en utilisant la formule de Legendre (voir exercice 1.7.18), on obtient

$$\ln(\lfloor x \rfloor !) = \sum_{p \leq x} \ln p \sum_{m \geq 1} \left\lfloor \frac{\lfloor x \rfloor}{p^m} \right\rfloor.$$

Or on vérifie immédiatement que

$$\left\lfloor \frac{\lfloor x \rfloor}{p^m} \right\rfloor = \left\lfloor \frac{x}{p^m} \right\rfloor.$$

D'où

$$\begin{aligned} \ln(\lfloor x \rfloor !) &= \sum_{p \leq x} \sum_{m \geq 1} \left\lfloor \frac{x}{p^m} \right\rfloor \ln p \\ &= \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor \ln p + \sum_{p \leq x} \sum_{m \geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \ln p \\ &= x \sum_{p \leq x} \frac{\ln p}{p} - \sum_{p \leq x} \left\{ \frac{x}{p} \right\} \ln p + \sum_{p \leq x} \sum_{m \geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \ln p. \end{aligned}$$

Remarquons en utilisant le lemme 5.3.1 que

$$\sum_{p \leq x} \left\{ \frac{x}{p} \right\} \ln p \leq \sum_{p \leq x} \ln p = \Theta(x) \leq (2 \ln 2) x.$$

De plus,

$$\begin{aligned} \sum_{p \leq x} \sum_{m \geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \ln p &\leq x \sum_{p \leq x} \sum_{m \geq 2} \frac{\ln p}{p^m} \\ &= x \sum_{p \leq x} \ln p \left(\frac{1}{p^2} \frac{1}{1 - \frac{1}{p}} \right) \\ &= x \sum_{p \leq x} \frac{\ln p}{p(p-1)}. \end{aligned}$$

Comme la série $\sum_n \frac{\ln n}{n(n-1)}$ converge, on en déduit que

$$\sum_{p \leq x} \sum_{m \geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \ln p = O(x),$$

ce qui entraine que

$$\ln(\lfloor x \rfloor !) = x \sum_{p \leq x} \frac{\ln p}{p} + O(x). \tag{5.4}$$

En comparant (5.3) et (5.4), on en déduit finalement la formule (5.1).

Pour prouver l'estimation (5.2), on introduit la fonction

$$R(x) = \sum_{p \leq x} \frac{\ln p}{p} - \ln x,$$

et on applique la formule d'Abel à $f(t) = 1/\ln t$ et

$$a(n) := \begin{cases} \frac{\ln p}{p} & \text{si } n = p \\ 0 & \text{sinon.} \end{cases}$$

On vérifie facilement que

$$A(x) = \sum_{n \leq x} a(n) = \sum_{p \leq x} \frac{\ln p}{p} = R(x) + \ln x,$$

ce qui donne

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \frac{1}{2} + \sum_{2 < p \leq x} \frac{1}{p} = \frac{1}{2} + \frac{A(x)}{\ln x} - \frac{A(2)}{\ln 2} - \int_2^x A(t) f'(t)\, dt \\ &= \frac{1}{2} + \frac{R(x)}{\ln x} - \frac{R(2)}{\ln 2} + \int_2^x \frac{R(t)}{t(\ln t)^2}\, dt + \int_2^x \frac{dt}{t \ln t}\, dt \\ &= \ln\ln x - \ln\ln 2 + \frac{1}{2} - \frac{R(2)}{\ln 2} + \frac{R(x)}{\ln x} + \int_2^x \frac{R(t)}{t(\ln t)^2}\, dt. \end{aligned}$$

Remarquons tout d'abord que $R(2) = \frac{\ln 2}{2} - \ln 2 = -\frac{1}{2}\ln 2$, d'où

$$\sum_{p \leq x} \frac{1}{p} = \ln\ln x + 1 - \ln\ln 2 + \frac{R(x)}{\ln x} + \int_2^x \frac{R(t)}{t(\ln t)^2}\, dt.$$

D'autre part, d'après (5.1), on a $R(t) = O(1)$, ce qui implique en particulier que l'intégrale

$$\int_2^{+\infty} \frac{R(t)}{t(\ln t)^2}\, dt$$

converge et si on note A sa valeur, on obtient

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \ln\ln x + 1 - \ln\ln 2 + A + \frac{R(x)}{\ln x} - \int_x^{+\infty} \frac{R(t)}{t(\ln t)^2}\, dt \\ &= \ln\ln x + C + \frac{R(x)}{\ln x} - \int_x^{+\infty} \frac{R(t)}{t(\ln t)^2}\, dt, \end{aligned}$$

où $C = 1 - \ln\ln 2 + A$. Il reste à remarquer, en notant $R = \sup_{t \geq 2} |R(t)|$, que

$$\left| \frac{R(x)}{\ln x} - \int_x^{+\infty} \frac{R(t)}{t(\ln t)^2}\, dt \right| \leq \frac{R}{\ln x} + R \int_x^{+\infty} \frac{dt}{t(\ln t)^2}$$

et

$$\int_x^{+\infty} \frac{dt}{t(\ln t)^2} = \left[-\frac{1}{\ln t} \right]_x^{+\infty} = \frac{1}{\ln x}.$$

D'où

$$\left|\frac{R(x)}{\ln x} - \int_x^{+\infty} \frac{R(t)}{t(\ln t)^2}\, dt\right| \leq \frac{2R}{\ln x},$$

ce qui implique l'estimation (5.2) et achève la preuve du théorème.

□

5.5 Exercices

Exercice 5.5.1 Dans cet exercice, on admettra le théorème des nombres premiers, c'est à dire que $\pi(x) \sim x/\ln x$, $x \to +\infty$. On note p_n le n-ième nombre premier. Montrer que $p_n \sim n \ln n$, $n \to +\infty$.

Exercice 5.5.2 Soit $P^+(n)$ le plus grand facteur premier d'un entier n. Calculer

$$\sum_{P^+(n)\leq 5} \frac{1}{n}.$$

Exercice 5.5.3 (Postulat de Bertrand) En partant de l'encadrement

$$\forall x \geq 30, \qquad 0.9\, \frac{x}{\log x} \leq \pi(x) \leq 1.2\, \frac{x}{\log x},$$

prouver que pour tout $n \geq 30$, il existe un nombre premier strictement compris entre n et $2n$. En déduire le résultat [1] suivant :

$$\forall n \geq 2, \text{il existe un nombre premier } p \text{ satisfaisant } n < p < 2n.$$

Exercice 5.5.4 Montrer que, pour $n > 1$, $n!$ n'est pas de la forme a^b avec $b > 1$. *Indication :* on considérera le plus grand premier $p \leq n$ et on utilisera le théorème de Bertrand.

Exercice 5.5.5 Soit x un réel, $x > 1$. Démontrez les estimations suivantes :

$$(a)\ \ln x \leq \sum_{d\leq x} \frac{1}{d} \leq 1 + \ln x \qquad (b)\ \sum_{d>x} \frac{1}{d^2} \leq \frac{1}{x-1}.$$

Exercice 5.5.6 Pour $n \geq 1$, on note $d(n)$ le nombre de diviseur de l'entier n,

$$d(n) = \sum_{d|n} 1.$$

Montrer que

$$\frac{1}{x} \sum_{n\leq x} d(n) = \ln x + O(1).$$

1. Remarquons une conjecture analogue due à Legendre : pour tout entier $n \geq 1$, il existe un nombre premier entre n^2 et $(n+1)^2$. En 2012, on ne sait toujours pas si cette conjecture est vraie ou non.

Exercice 5.5.7 En utilisant la méthode dite de *l'hyperbole de Dirichlet*, le but de l'exercice est d'améliorer l'estimation démontrée dans l'exercice précédent.

(a) Montrer que $\sum_{n\leq x} d(n)$ est le nombre de points à coordonnées entières situés dans le quart de plan $u \geq 1$, $v \geq 1$ et sous l'hyperbole d'équation $uv = x$.

(b) En utilisant la symétrie du graphe de l'hyperbole $uv = x$, en déduire que

$$\sum_{n\leq x} d(n) = 2 \sum_{d\leq\sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor\sqrt{x}\rfloor^2.$$

(c) En utilisant la formule d'Abel, retrouver le résultat bien connu suivant :

$$\sum_{n\leq x} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right),$$

où γ est la constante définie par

$$\gamma = 1 - \int_1^{+\infty} \frac{\{t\}}{t^2}\, dt.$$

(d) En déduire que

$$\frac{1}{x}\sum_{n\leq x} d(n) = \ln x + (2\gamma - 1) + O\left(\frac{1}{\sqrt{x}}\right).$$

Exercice 5.5.8 On note p_n le n-ième nombre premier.

(a) Sans utiliser le théorème des nombres premiers, montrer que la série

$$\sum_n \frac{1}{p_n \ln p_n}$$

converge.

(b) En utilisant le théorème des nombres premiers, donner un équivalent du reste

$$R_n := \sum_{k=n+1}^{+\infty} \frac{1}{p_k \ln p_k}$$

Exercice 5.5.9 (a) Montrer que si $f : [2, +\infty[\longrightarrow \mathbb{R}$ est une fonction de classe C^1, alors

$$\sum_{p\leq x} f(p) = \pi(x)f(x) - \int_2^x f'(t)\pi(t)\, dt.$$

(b) On admet dans cette question que

$$\pi(x) = \frac{x}{\ln x} + O\left(\frac{x}{(\ln x)^2}\right), \qquad x \geq 2.$$

Retrouver alors le fait qu'il existe une constante $C > 0$ telle que

$$\sum_{p\leq x} \frac{1}{p} = \ln\ln x + C + O\left(1/\ln x\right)$$

Exercice 5.5.10

1. Montrer que
$$\lim_{x\to+\infty} \sum_{\sqrt{x}<p\leq x} \frac{1}{p} = \ln 2.$$
2. Notons pour un entier n, $P^+(n)$ le plus grand facteur premier de n et posons
$$A_x = \left\{n \leq x : P^+(n) > \sqrt{n}\right\}.$$
   (i) Montrer que $n \in A_x$ si et seulement s'il existe un nombre premier p et un entier q tel que $n = pq$ et $q < p \leq \frac{x}{q}$. Montrer de plus qu'un telle décomposition est unique.
   (ii) Montrer que
$$\mathrm{card}(A_x) = \sum_{p\leq\sqrt{x}} (p-1) + \sum_{\sqrt{x}<p\leq x} \left\lfloor \frac{x}{p} \right\rfloor.$$
3. En déduire, que lorsque $x \to +\infty$, une proportion positive des entiers $n \leq x$ ont leur plus grand facteur premier $> \sqrt{n}$.

Exercice 5.5.11 Le but de l'exercice est d'évaluer
$$\sum_{pq\leq x} \frac{1}{pq}$$
où p et q désignent des nombres premiers.

1. Montrer qu'il existe une constante C telle que
$$\sum_{pq\leq x} \frac{1}{pq} = (\ln\ln x + C) \sum_{p\leq\frac{x}{2}} \frac{1}{p} + O\left(\sum_{p\leq\frac{x}{2}} \frac{1}{p} \ln\left(\frac{\ln x}{\ln(x/p)}\right)\right).$$
2. En déduire que
$$\sum_{pq\leq x} \frac{1}{pq} = (\ln\ln x)^2 + 2C\ln\ln x + O\left(1 + \sum_{p\leq\frac{x}{2}} \frac{1}{p} \ln\left(\frac{\ln x}{\ln(x/p)}\right)\right).$$
3. Montrer que
$$\sum_{p\leq\frac{x}{2}} \frac{1}{p} \ln\left(\frac{\ln x}{\ln(x/p)}\right) \leq \int_1^{\ln x/\ln 2} \sum_{x^{\frac{v-1}{v}}<p\leq x/2} \frac{1}{p}\frac{dv}{v}.$$
4. En utilisant que $\int_1^{+\infty} \ln\left(\frac{v}{v-1}\right)\frac{dv}{v}$ converge, en déduire que
$$\sum_{p\leq\frac{x}{2}} \frac{1}{p} \ln\left(\frac{\ln x}{\ln(x/p)}\right) = O(1).$$
5. En déduire que
$$\sum_{pq\leq x} \frac{1}{pq} = (\ln\ln x)^2 + 2C\ln\ln x + O(1).$$

Chapitre 6

Fonctions arithmétiques multiplicatives

6.1 Fonctions multiplicatives

Une fonction *arithmétique* est une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{C}$. On dit que f est *multiplicative* si

$$f(1) \neq 0 \quad \text{et} \quad f(mn) = f(m)f(n)$$

pour toute paire d'entiers (m, n) premiers entre eux. Enfin, la fonction f est dite *complètement multiplicative* si

$$f(1) \neq 0 \quad \text{et} \quad f(mn) = f(m)f(n)$$

pour toute paire d'entiers (m, n).

Exemples :

(a) Rappelons qu'à la section 1.4, nous avons introduit la fonction indicatrice d'Euler φ par

$$\varphi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^*), \qquad n \geq 2.$$

En prolongeant la définition et en posant $\varphi(1) = 1$, le lemme 1.4.4 implique que la fonction d'Euler φ est multiplicative.

(b) La fonction $\mathbf{I}$, définie par $\mathbf{I}(n) = 1$, $n \geq 1$, est une fonction complètement multiplicative.

(c) La fonction δ, définie par $\delta(1) = 1$ et $\delta(n) = 0$, $n \geq 2$, est aussi complètement multiplicative.

(d) Enfin, si $a \in \mathbb{R}$, la fonction N_a, définie par $N_a(n) = n^a$, $n \geq 1$, est complètement multiplicative. Notons que $N_0 = \mathbf{I}$.

Le résultat suivant montre que pour connaitre une fonction multiplicative f (respectivement complètement multiplicative), il suffit de connaitre $f(p^k)$ (respectivement $f(p)$), pour tout entier $k \geq 1$ et tout nombre premier p.

Théorème 6.1.1 *Soit f une fonction arithmétique.*

(a) Si f est multiplicative, alors $f(1) = 1$. De plus, elle est entièrement déterminée par ses valeurs aux puissances des nombres premiers.

(b) Si f est complètement multiplicative, alors elle est entièrement déterminée par ses valeurs aux nombres premiers.

Preuve : Tout d'abord supposons que f soit multiplicative et remarquons que $f(1) = f(1)f(1)$. Comme $f(1) \neq 0$, on en déduit immédiatement que $f(1) = 1$. Maintenant soit $n \in \mathbb{N}^*$. Ecrivons la factorisation canonique de n en produit de facteurs premiers,

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Comme f est multiplicative, on a

$$f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r}),$$

ce qui prouve l'assertion (a). Si, on suppose de plus que f est complètement multiplicative, alors on obtient que si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, on a

$$f(n) = f(p_1)^{k_1} f(p_2)^{k_2} \dots f(p_r)^{k_r},$$

ce qui prouve que f est déterminée par les valeurs $f(p)$, p premier.

□

6.2 Convolution des fonctions arithmétiques

Si f et g sont deux fonctions arithmétiques, on définit le produit de convolution $f * g$ par

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{d_1, d_2 \\ d_1 d_2 = n}} f(d_1) g(d_2).$$

Proposition 6.2.1 *Pour toute fonction arithmétique f, g, h, on a :*

(a) $f * g = g * f$.

(b) $(f * g) * h = f * (g * h)$.

(c) $f * \delta = f$.

Preuve : Il n'y a pas de difficultés et la preuve est laissée en exercice.

□

Si on définit la somme de deux fonctions arithmétiques f et g par

$$(f+g)(n) = f(n) + g(n), \qquad n \geq 1,$$

on vérifie facilement que l'ensemble des fonctions arithmétiques, muni de l'addition et du produit de convolution, est un anneau commutatif unitaire, dont l'unité est δ.

Théorème 6.2.2 *Soient f, g deux fonctions arithmétiques multiplicatives. Alors la fonction arithmétique $f * g$ est aussi multiplicative.*

La preuve est basée sur le lemme suivant.

Lemme 6.2.3 *Soient $(m,n) = 1$ et d un diviseur de mn. Alors d s'écrit de façon unique sous la forme $d = d_1 d_2$ où $d_1 | m$ et $d_2 | n$.*

Preuve : Prouvons d'abord l'existence de d_1 et d_2. Ecrivons

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad \text{et} \quad n = p_{k+1}^{\alpha_{k+1}} \dots p_{k+r}^{\alpha_{k+r}}.$$

Notons que comme $(m,n) = 1$, les premiers qui interviennent dans la factorisation de m sont tous différents de ceux qui interviennent dans la factorisation de n. On a alors

$$mn = p_1^{\alpha_1} \dots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \dots p_{k+r}^{\alpha_{k+r}}.$$

Si d est un diviseur de mn, l'entier d s'écrit nécessairement sous la forme

$$d = p_1^{\beta_1} \dots p_k^{\beta_k} p_{k+1}^{\beta_{k+1}} \dots p_{k+r}^{\beta_{k+r}},$$

où $\beta_i \leq \alpha_i$, pour tout $i = 1, 2, \dots, k+r$. Définissons alors

$$d_1 = p_1^{\beta_1} \dots p_k^{\beta_k} \quad \text{et} \quad d_2 = p_{k+1}^{\beta_{k+1}} \dots p_{k+r}^{\beta_{k+r}}.$$

On a $d = d_1 d_2$ et $d_1 | m$, $d_2 | n$, ce qui prouve l'existence de la décomposition.

Il reste à prouver l'unicité. Soit $d = d_1 d_2 = d_1' d_2'$, avec $d_1, d_1' | m$ et $d_2, d_2' | n$. Soit $\delta = (d_1, d_2')$. Alors δ divise d_1 et donc m et δ divise d_2' et donc n. Ainsi $\delta | (m,n) = 1$ et donc $(d_1, d_2') = 1$. Comme d_2' divise $d_1 d_2$, le lemme de Gauss implique alors que $d_2' | d_2$. Par symétrie, on obtient que $d_2 | d_2'$ et donc $d_2 = d_2'$. On en déduit alors aussi que $d_1 = d_1'$, ce qui achève de prouver l'unicité.

□

Preuve du théorème 6.2.2 : soit m et n deux entiers premiers entre eux et notons $h = f * g$. D'après le lemme 6.2.3, on a

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{d_1|m, d_2|n} f(d_1d_2)g\left(\frac{mm}{d_1d_2}\right).$$

Remarquons que $(m,n) = 1$ implique que $(d_1,d_2) = 1$ et $\left(\frac{m}{d_1}, \frac{n}{d_2}\right) = 1$. D'où $f(d_1d_2) = f(d_1)f(d_2)$ et $g\left(\frac{mm}{d_1d_2}\right) = g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)$. Donc

$$\begin{aligned} h(mn) &= \sum_{d_1|m, d_2|n} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right) \\ &= \left(\sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right)\right) \\ &= h(m)h(n). \end{aligned}$$

□

6.3 Fonction somme de diviseurs et nombres parfaits

Notons

$$d(n) = \sum_{d|m} 1 \qquad \text{et} \qquad \sigma(n) = \sum_{d|n} d.$$

La fonction d s'appelle la fonction *nombre de diviseurs* et la fonction σ s'appelle la fonction *somme de diviseurs*. Le résultat suivant montre que ces deux fonctions arithmétiques sont multiplicatives.

Corollaire 6.3.1 *Les fonctions d et σ sont multiplicatives.*

Preuve : Il suffit de remarquer que $d = \mathbf{I} * \mathbf{I}$ et $\sigma = N_1 * \mathbf{I}$ et d'appliquer le théorème 6.2.2.

□

Le résultat suivant donne une formule explicite pour $d(n)$ et $\sigma(n)$ lorsqu'on connait la factorisation canonique de l'entier n.

Proposition 6.3.2 *Si $n = p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ est la factorisation canonique d'un entier n, on a*

$$d(n) = \prod_{j=1}^{r}(k_j + 1)$$

et

$$\sigma(n) = \prod_{j=1}^{r} \frac{p_j^{k_j} + 1}{p_j - 1}.$$

Preuve : On a, pour tout nombre premier p et tout entier $k \geq 1$, on a

$$d(p^k) = \sum_{d|p^k} 1 = \text{card}\{1, p, \ldots, p^k\} = k+1$$

et

$$\sigma(p^k) = \sum_{d|p^k} d = \sum_{i=0}^{k} p^i = \frac{p^{k+1}+1}{p-1},$$

ce qui donne le résultat en appliquant le théorème 6.1.1.

□

Un entier n est dit *parfait* si $\sigma(n) = 2n$, autrement dit si

$$n = \sum_{\substack{d|n \\ d<n}} d.$$

Exemple : $6 = 1+2+3$ et $28 = 1+2+4+7+14$ sont des nombres parfaits.

Théorème 6.3.3 (Euclide–Euler) *(a) Si $2^k - 1$ est premier, alors $2^{k-1}(2^k-1)$ est parfait.*

(b) Si n est pair et parfait, alors il existe un entier $k \geq 2$ tel que $n = 2^{k-1}(2^k-1)$ et $2^k - 1$ est premier.

Preuve : Il est clair que $(2^{k-1}, 2^k - 1) = 1$, d'où σ étant multiplicative, on a

$$\sigma(2^{k-1}(2^k-1)) = \sigma(2^{k-1})\sigma(2^k-1).$$

Si 2^k-1 est premier, on a $\sigma(2^k-1) = 1+(2^k-1) = 2^k$ et d'après la proposition 6.3.2, on a

$$\sigma(2^{k-1}) = \frac{2^k+1}{2-1} = 2^k+1.$$

Donc on obtient que

$$\sigma(2^{k-1}(2^k-1)) = 2^k(2^k-1) = 2 \times 2^{k-1}(2^k-1),$$

ce qui prouve que $2^{k-1}(2^k-1)$ est parfait.

Supposons que l'entier n est pair et parfait. Ecrivons alors $n = 2^{k-1}m$, avec $k \geq 2$ et m impair. Comme n est parfait, on a $\sigma(n) = 2n$, ce qui donne

$$2^k m = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k-1)\sigma(m).$$

Puisque $(2^k, 2^k-1) = 1$, le lemme de Gauss implique que 2^k-1 divise m et 2^k divise $\sigma(m)$. Ecrivons $\sigma(m) = 2^k\ell$, $\ell \geq 1$. D'où $2^k m = 2^k(2^k-1)\ell$, c'est-à-dire $m = (2^k-1)\ell$. Supposons que $\ell > 1$. Alors $1, \ell$ et m sont trois diviseurs distincts de m. D'où

$$\sigma(m) \geq 1 + \ell + m > \ell + m = 2^k\ell = \sigma(m),$$

ce qui est absurde. D'où $\ell = 1$ et $m = 2^k - 1$. Ainsi on obtient que $n = 2^{k-1}(2^k - 1)$. De plus, comme $\sigma(m) = 2^k$ et $m = 2^k - 1$, on en déduit que m est premier.

□

Le théorème 6.3.3 donne une caractérisation des entiers pairs qui sont parfait. En revanche, on ne sait pas s'il existe des nombres impairs parfaits.

6.4 Inversibilité des fonctions arithmétiques

Rappelons que pour toute fonction arithmétique f, on a

$$f * \delta = f,$$

où $\delta(1) = 1$ et $\delta(n) = 0$, $n \geq 2$. Si $\mathbb{A}$ désigne l'ensemble des fonctions arithmétiques, l'ensemble $(\mathbb{A}, +, *)$ est un anneau commutatif unitaire, dont l'unité est δ. Le résultat suivant caractérise les éléments inversibles de cet anneau.

Théorème 6.4.1 *Soit f une fonction arithmétique. Alors f est inversible si et seulement si $f(1) \neq 0$.*

Preuve : Supposons que f soit inversible, c'est-à-dire qu'il existe $g \in \mathbb{A}$ telle que $f * g = \delta$. D'où

$$(f * g)(1) = \delta(1) = 1,$$

et comme

$$(f * g)(1) = \sum_{d|1} f(d) g\left(\frac{1}{d}\right) = f(1)g(1),$$

on en déduit que $f(1)g(1) = 1$. En particulier, nécessairement $f(1) \neq 0$.

Réciproquement, supposons $f(1) \neq 0$. On cherche $g \in \mathbb{A}$ telle que $f * g = \delta$, c'est-à-dire $f(1)g(1) = 1$ et pour tout $n \geq 2$,

$$0 = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

On va construire g par récurrence. On commence par définir $g(1) = 1/f(1)$. Supposons avoir construit $g(1), \ldots, g(n-1)$. Alors on veut

$$0 = f(1)g(n) + \sum_{\substack{1 < d \leq n \\ d|n}} f(d) g\left(\frac{n}{d}\right).$$

D'où on pose

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{1 < d \leq n \\ d|n}} f(d) g\left(\frac{n}{d}\right).$$

Par récurrence, on construit $g \in \mathbb{A}$ telle que $g * f = \delta$.

□

Corollaire 6.4.2 *Soit $f \in \mathbb{A}$ une fonction multiplicative. Alors f est inversible et f^{-1} est multiplicative.*

Preuve : Comme f est multiplicative, le théorème 6.1.1 implique que $f(1) = 1$. Donc d'après le théorème 6.4.1, f est inversible. Il reste à montrer que $g = f^{-1}$ est multiplicative. Soit h la fonction multiplicative qui est égale à g sur les nombres premiers, c'est-à-dire que

$$h(p^k) = g(p^k),$$

pour tout nombre premier p et tout entier $k \geq 1$. D'après le théorème 6.1.1, la fonction h est uniquement déterminée et le théorème 6.2.2 implique que la fonction arithmétique $u = f * h$ est multiplicative. Pour chaque nombre premier p et tout entier $k \geq 1$, on a

$$\begin{aligned} u(p^k) &= \sum_{d|p^k} f(d)g\left(\frac{p^k}{d}\right) \\ &= \sum_{j=0}^{k} f(p^j)h(p^{k-j}) \\ &= \sum_{j=0}^{k} f(p^k)g(p^{k-j}) \\ &= (f * g)(p^k) = \delta(p^k). \end{aligned}$$

Donc u et δ coïncident sur les puissances des nombres premiers. Comme elles sont multiplicatives, le théorème 6.1.1 implique qu'elles sont identiques. D'où

$$f * h = u = \delta.$$

Par unicité de l'inverse, on a $f^{-1} = h$ et f^{-1} est multiplicative.

□

Corollaire 6.4.3 *L'ensemble des fonctions arithmétiques multiplicatives, muni du produit de convolution, forme un groupe abélien.*

Preuve : découle immédiatement du corollaire 6.4.2 et de la proposition 6.2.1.

□

6.5 La fonction de Möbius et la formule d'inversion

La fonction $\mathbf{I}$ est multiplicative. Donc d'après le corollaire 6.4.2, elle est inversible et son inverse est multiplicative. On note $\mu = \mathbf{I}^{-1}$ et μ s'appelle la *fonction de Möbius*. Le résultat suivant donne une expression explicite de $\mu(n)$.

Théorème 6.5.1 *On a*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers disctincts}, \\ 0 & \text{si } n \text{ est divisible par un carré.} \end{cases}$$

Un entier n tel que $\mu(n) \neq 0$ est appelé un *entier sans facteur carré.*

Preuve : Comme μ est multiplicative, on a $\mu(1) = 1$. De plus, pour tout premier p, on a

$$0 = \delta(p) = (\mu * \mathbf{I})(p) = \mu(1)\mathbf{I}(p) + \mu(p)\mathbf{I}(1),$$

ce qui implique que

$$\mu(p) = -\mu(1) = -1.$$

De plus, pour tout entier $k \geq 2$, on a

$$\begin{aligned} 0 &= \delta(p^k) = \sum_{j=0}^{k} \mu(p^j)\mathbf{I}(p^{k-j}) = \sum_{j=0}^{k} \mu(p^j) \\ &= \mu(1) + \mu(p) + \sum_{j=2}^{k} \mu(p^j). \end{aligned}$$

Ce qui précède implique alors que

$$\sum_{j=2}^{k} \mu(p^j) = 0$$

pour tout entier $k \geq 2$. Un raisonnement par récurrence montre alors immédiatement que $\mu(p^k) = 0$, pour tout $k \geq 2$ et tout premier p. Le théorème 6.1.1 permet alors de conclure.

□

Théorème 6.5.2 (Formule d'inversion de Möbius) *Soit f une fonction arithmétique et notons pour tout $n \geq 1$,*

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

On a

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Preuve : Par hypothèse, on a $F = f * \mathbf{I}$. D'où

$$f = \delta * f = \mu * \mathbf{I} * f = \mu * f * \mathbf{I} = \mu * F,$$

ce qui donne immédiatement le résultat.

□

6.6 Exercices

On rappelle que :

1. μ représente la fonction de Möbius.
2. φ la fonction d'Euler : $\varphi(n) = \sum_{\substack{1 \leq m \leq n \\ (m,n)=1}} 1$.
3. $d(n) = \sum_{d|n} 1$ le nombre des diviseurs de l'entier n.
4. $\sigma(n) = \sum_{d|n} d$ la somme des diviseurs de l'entier n.

Exercice 6.6.1 Déterminer toutes les fonctions arithmétiques f complètement multiplicatives telles que $F = \mathbf{1} * f$ soit encore complètement multiplicative.

Exercice 6.6.2 Montrer que la fonction arithmétique f définie par $f(n) = (-1)^{n+1}$ pour $n \geq 1$ est multiplicative. Soit g l'inverse de f pour la convolution. Expliciter $g(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}$ puis $g(n)$ pour un entier $n \geq 1$ quelconque.

Exercice 6.6.3 On désigne par $\Omega(n)$ le nombre de facteurs premiers de n, *comptés avec leur ordre de multiplicité* c'est-à-dire

$$\Omega(n) = \sum_{i=1}^{k} \alpha_i, \text{ où } n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

est la décomposition en facteurs premiers de n. La *fonction λ de Liouville* est définie par $\lambda(n) = (-1)^{\Omega(n)}$. Montrer que λ est complètement multiplicative, et que le produit de convolution $\lambda * \mathbf{1}$ est la fonction caractéristique des carrés c'est-à-dire que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n \text{ est un carré} \\ 0 & \text{si } n \text{ n'est pas un carré.} \end{cases}$$

Exercice 6.6.4

1. Montrer que pour tout $n > 1$ on a $\varphi(n)\sigma(n) < n^2$.
2. Montrer que pour tout $n > 1$ on a $\varphi(n)d(n) \geq n$ avec égalité si et seulement si $n = 2$.

Exercice 6.6.5 On dit qu'un entier n est **abondant** si $\sigma(n) \geq 2n$. Montrer que si n est abondant et impair il admet au moins 3 facteurs premiers.

Exercice 6.6.6

1. Montrer que $\varphi(mn) \geq \varphi(m)\varphi(n)$, avec égalité seulement si $(m, n) = 1$.

2. Montrer que $d(mn) \leq d(m)d(n)$ avec égalité si et seulement si $(m,n) = 1$.

Exercice 6.6.7 La fonction d prend elle plus souvent des valeurs paires ou impaires ?

Exercice 6.6.8 Montrer que pour tout n, $\sigma(3n-1)$ est un multiple de 3.

Exercice 6.6.9 Soient $F : [1, +\infty[\longrightarrow \mathbb{C}$ et

$$G(x) = \sum_{n \leq x} F\left(\frac{x}{n}\right).$$

Montrer que

$$F(x) = \sum_{n \leq x} \mu(n) G\left(\frac{x}{n}\right).$$

Cette formule est connue sous le nom de *deuxième formule d'inversion de Möbius.*

Exercice 6.6.10 Soit x un réel $x \geq 1$.

1. Montrer, par exemple en utilisant la deuxième formule d'inversion de Möbius (voir exercice précédent), que

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1.$$

2. En déduire que

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

Exercice 6.6.11

1. Montrer que $\mu * N_1 = \varphi$.
2. En déduire que, pour tout $n \geq 1$, on a

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

3. Montrer que

$$\sigma(n) = \sum_{k|n} d(k) \varphi\left(\frac{n}{k}\right).$$

Exercice 6.6.12 Montrer que

$$\frac{1}{x} \sum_{n \leq x} \frac{\sigma(n)}{n} = \frac{\pi^2}{6} + O\left(\frac{\log x}{x}\right).$$

Exercice 6.6.13 On définit la *fonction de von Mangoldt* $\Lambda(n)$ par

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k \text{ est une puissance d'un nombre premier,} \\ 0 & \text{sinon.} \end{cases}$$

Remarquons alors que si ψ désigne la fonction de Chebyshev, on a

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

1. Montrer que
$$\sum_{d|n} \Lambda(d) = \log n.$$
2. Montrer que pour $x \geq 2$, on a
$$\sum_{m \leq x} \psi\left(\frac{x}{m}\right) = \sum_{d \leq x} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor.$$
3. Montrer que
$$\sum_{m \leq x} \psi\left(\frac{x}{m}\right) = x \log x - x + O(\log x).$$
4. Montrer que
$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$
5. En déduire une nouvelle preuve de la formule de Mertens :
$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Chapitre 7

Séries de Dirichlet

7.1 Définition et premières propriétés

Soit $(a_n)_{n\geq 1}$ une suite à coefficients complexes. On appelle *série de Dirichlet* une série de la forme

$$\sum_{n\geq 1} \frac{a_n}{n^s}, \qquad s \in \mathbb{C}.$$

Théorème 7.1.1 *Supposons que la série de Dirichlet*

$$\sum_{n\geq 1} \frac{a_n}{n^s}, \qquad s \in \mathbb{C}.$$

converge pour un $s_0 \in \mathbb{C}$. Alors elle converge dans le demi-plan $\Re(s) > \Re(s_0)$. De plus, elle converge uniformément sur tout secteur du type

$$\Delta_{s_0,\alpha} = \{s \in \mathbb{C} : \Re(s) > \Re(s_0) \,\&\, |\arg(s - s_0)| \leq \alpha\},$$

où $0 < \alpha < \frac{\pi}{2}$.

La preuve utilise le lemme élémentaire suivant.

Lemme 7.1.2 *Soient $0 < \alpha < \beta$. Alors, pour tout $z \in \mathbb{C}$, $x = \Re(z) > 0$, on a*

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq \frac{|z|}{x}\left(e^{-\alpha x} - e^{-\beta x}\right).$$

Preuve : On a

$$e^{-\alpha z} - e^{-\beta z} = z\int_\alpha^\beta e^{-tz}\,dt.$$

D'où

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq |z|\int_\alpha^\beta |e^{-tz}|\,dt = |z|\int_\alpha^\beta e^{-tx}\,dt = \frac{|z|}{x}\left(e^{-\alpha x} - e^{-\beta x}\right).$$

□

Preuve du théorème 7.1.1 : soit $s \in \mathbb{C}$, $\Re(s) > \Re(s_0)$. Posons $u_n = a_n n^{-s_0}$, $v_n = n^{s_0 - s}$, et pour $q \geq p$

$$S_{p,q} = \sum_{n=p}^{q} u_n v_n = \sum_{n=p}^{q} \frac{a_n}{n^s}$$

et

$$U_{p,q} = \sum_{n=p}^{q} u_n = \sum_{n=p}^{q} \frac{a_n}{n^{s_0}}.$$

Par hypothèse, pour tout $\varepsilon > 0$, il existe un entier $N(\varepsilon)$ tel que

$$q \geq p \geq N(\varepsilon) \Longrightarrow |U_{p,q}| \leq \varepsilon.$$

De plus, si $\Re(s) > \Re(s_0)$, remarquons que

$$|v_n| = \frac{1}{n^{\Re(s)-\Re(s_0)}} < 1.$$

En utilisant une transformation d'Abel (avec la convention que $U_{p,p-1} = 0$), on a

$$\begin{aligned}
\sum_{n=p}^{q} \frac{a_n}{n^s} &= \sum_{n=p}^{q} u_n v_n = \sum_{n=p}^{q} (U_{p,n} - U_{p,n-1}) v_n \\
&= \sum_{n=p}^{q} U_{p,n} v_n - \sum_{n=p}^{q} U_{p,n-1} v_n \\
&= \sum_{n=p}^{q} U_{p,n} v_n - \sum_{k=p-1}^{q-1} U_{p,k} v_{k+1} \\
&= U_{p,q} v_q + \sum_{n=p}^{q-1} U_{p,n} (v_n - v_{n+1}).
\end{aligned}$$

D'où, pour $q > p \geq N(\varepsilon)$, on a

$$\left| \sum_{n=p}^{q} \frac{a_n}{n^s} \right| \leq \varepsilon |v_q| + \varepsilon \sum_{n=p}^{q-1} |v_n - v_{n+1}| \leq \varepsilon \left(1 + \sum_{n=p}^{q-1} |v_n - v_{n+1}| \right).$$

Or

$$|v_n - v_{n+1}| = \left| \frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right| = \left| e^{-(s-s_0)\ln n} - e^{-(s-s_0)\ln(n+1)} \right|.$$

En appliquant le lemme 7.1.2 à $z = s - s_0$, $\alpha = \ln n$ et $\beta = \ln(n+1)$, on obtient

$$|v_n - v_{n+1}| \leq \frac{|s - s_0|}{\sigma - \sigma_0} \left(\frac{1}{n^{\sigma-\sigma_0}} - \frac{1}{(n+1)^{\sigma-\sigma_0}} \right),$$

où $\sigma = \Re(s)$ et $\sigma_0 = \Re(s_0)$. D'où

$$\begin{aligned}
\left| \sum_{n=p}^{q} \frac{a_n}{n^s} \right| &\leq \varepsilon \left[1 + \frac{|s - s_0|}{\sigma - \sigma_0} \sum_{n=p}^{q-1} \left(\frac{1}{n^{\sigma-\sigma_0}} - \frac{1}{(n+1)^{\sigma-\sigma_0}} \right) \right] \\
&= \varepsilon \left[1 + \frac{|s - s_0|}{\sigma - \sigma_0} \left(\frac{1}{p^{\sigma-\sigma_0}} - \frac{1}{q^{\sigma-\sigma_0}} \right) \right] \\
&\leq \varepsilon \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right). \qquad (7.1)
\end{aligned}$$

Ceci montre donc que la série $\sum_n a_n n^{-s}$ vérifie le critère de Cauchy donc elle converge.

Il reste à montrer la convergence uniforme dans $\Delta_{s_0,\alpha}$ où $0 < \alpha < \pi/2$. Remarquons que si $s \in \Delta_{s_0,\alpha}$, il existe $\theta = \theta(s)$ tel que

$$\cos(\theta) = \frac{\sigma - \sigma_0}{|s - s_0|} \quad \text{et} \quad |\theta| \leq \alpha.$$

D'où

$$\frac{|s - s_0|}{\sigma - \sigma_0} = \frac{1}{\cos(\theta)} \leq \frac{1}{\cos(\alpha)},$$

ce qui avec (7.1) implique que, pour tout $s \in \Delta_{s_0,\alpha}$, on a

$$\left| \sum_{n=p}^{q} \frac{a_n}{n^s} \right| \leq \varepsilon \left(1 + \frac{1}{\cos(\alpha)} \right).$$

Ainsi la série $\sum_n a_n n^{-s}$ vérifie le critère de Cauchy uniforme sur $\Delta_{s_0,\alpha}$, donc elle converge uniformément sur $\Delta_{s_0,\alpha}$.

□

Le résultat suivant est un analogue de l'existence du rayon de convergence pour les séries entières.

Corollaire 7.1.3 *Soit $\sum_n a_n n^{-s}$ une série de Dirichlet. On note*

$$E_c = \left\{ \sigma \in \mathbb{R} : \sum_n a_n n^{-\sigma} \text{ converge} \right\}$$

et

$$\sigma_c = \begin{cases} \inf E_c & \text{si } E_c \neq \emptyset \\ +\infty & \text{si } E_c = \emptyset. \end{cases}$$

Alors

- *si $\Re(s) > \sigma_c$, la série $\sum_n a_n n^{-s}$ converge ;*
- *si $\Re(s) < \sigma_c$, la série $\sum_n a_n n^{-s}$ diverge.*

On appelle σ_c l'abscisse de convergence de la série de Dirichlet et le demi-plan $\Re(s) > \sigma_c$ le demi-plan de convergence.

Preuve : Supposons tout d'abord que $E_c = \emptyset$ et soit $s_0 \in \mathbb{C}$. Il s'agit de montrer que la série $\sum_n a_n n^{-s_0}$ diverge. Supposons au contraire qu'elle converge. Alors le théorème 7.1.1 implique que, pour tout $s \in \mathbb{C}$, $\Re(s) > \Re(s_0)$, la série $\sum_n a_n n^{-s}$ converge. En particulier, $\sigma = \Re(s) \in E_c$, ce qui est contraire à l'hypothèse.

Supposons maintenant que $E_c \neq \emptyset$. Si $E_c = \mathbb{R}$, alors pour tout $\sigma \in \mathbb{R}$, la série $\sum_n a_n n^{-\sigma}$ converge et on a $\sigma_c = -\infty$. Il s'agit alors de montrer que pour tout $s \in \mathbb{C}$, la série $\sum_n a_n n^{-s}$ converge. C'est à nouveau une conséquence du théorème 7.1.1, puisque si $s \in \mathbb{C}$, alors $\Re(s) > \sigma_0$ avec $\sigma_0 \in E_c$.

On peut donc supposer maintenant que $E_c \neq \emptyset$ et $E_c \neq \mathbb{R}$. Dans ce cas, il est facile de voir que σ_c est fini. Soit $s \in \mathbb{C}$, $\Re(s) > \sigma_c$. Alors il existe $\sigma_0 \in E_c$ tel que $\Re(s) > \sigma_0 \geq \sigma_c$. Le théorème 7.1.1 implique une nouvelle fois que la série $\sum_n a_n n^{-s}$ converge. Finalement il reste à montrer que si $s \in \mathbb{C}$, $\Re(s) < \sigma_c$, la série $\sum_n a_n n^{-s}$ diverge. Par l'absurde, supposons qu'il existe $s \in \mathbb{C}$, $\Re(s) < \sigma_c$, telle que la série $\sum_n a_n n^{-s}$ converge. Alors, si $\Re(s) < \sigma_1 < \sigma_c$, le théorème 7.1.1 implique que $\sum_n a_n n^{-\sigma_1}$ converge, ce qui contredit la définition de σ_c.

□

Corollaire 7.1.4 *Soit $\sum_n a_n n^{-s}$ une série de Dirichlet. On note*

$$E_a = \left\{ \sigma \in \mathbb{R} : \sum_n a_n n^{-\sigma} \text{ converge absolument} \right\}$$

et

$$\sigma_a = \begin{cases} \inf E_a & \text{si } E_a \neq \emptyset \\ +\infty & \text{si } E_a = \emptyset. \end{cases}$$

Alors

- *si $\Re(s) > \sigma_a$, la série $\sum_n a_n n^{-s}$ converge absolument ;*
- *si $\Re(s) < \sigma_a$, la série $\sum_n a_n n^{-s}$ ne converge pas absolument.*

On appelle σ_a l'abscisse de convergence absolue de la série de Dirichlet et le demi-plan $\Re(s) > \sigma_a$ le demi-plan de convergence absolu.

Preuve : Remarquons que

$$\left| \frac{a_n}{n^s} \right| = \frac{|a_n|}{n^{\Re(s)}}$$

et donc la série $\sum_n a_n n^{-s}$ converge absolument si et seulement si la série $\sum_n |a_n| n^{-\sigma}$ converge, où $\sigma = \Re(s)$. De plus,

$$E_a = \left\{ \sigma \in \mathbb{R} : \sum_n |a_n| n^{-\sigma} \text{ converge} \right\}.$$

Il suffit donc d'appliquer le corollaire 7.1.3 à la série de Dirichlet $\sum_n a_n n^{-s}$.

□

Proposition 7.1.5 *Soit $\sum_n a_n n^{-s}$ une série de Dirichlet. Alors on a*

$$\sigma_a - 1 \leq \sigma_c \leq \sigma_a.$$

Preuve : Si la série $\sum_n a_n n^{-\sigma}$ converge absolument, alors elle converge et donc $\sigma_c \leq \sigma_a$. Pour prouver la deuxième inégalité, choisissons $\sigma > \sigma_c + 1$. Alors il existe σ_0 tel que $\sigma - 1 > \sigma_0 > \sigma_c$. Comme la série $\sum_n a_n n^{-\sigma_0}$ converge, la suite $(a_n n^{-\sigma_0})_n$ est bornée par une constante, disons M. Ecrivons donc

$$\frac{|a_n|}{n^\sigma} = \frac{|a_n|}{n^{\sigma_0}} \frac{1}{n^{\sigma - \sigma_0}} \leq \frac{M}{n^{\sigma - \sigma_0}}.$$

Or $\sigma - \sigma_0 > 1$, donc la série $\sum_n n^{-(\sigma-\sigma_0)}$ converge et donc la série $\sum_n a_n n^{-\sigma}$ est absolument convergente. Ainsi $\sigma_a \leq \sigma_c + 1$.

□

7.2 Holomorphie et unicité des coefficients

Le résultat suivant précise la régularité de la somme d'une série de Dirichlet sur son demi-plan de convergence.

Théorème 7.2.1 *Soit*

$$F(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}, \qquad \Re(s) > \sigma_c$$

une série de Dirichlet. Alors la fonction F est holomorphe sur le demi-plan $\Re(s) > \sigma_c$ et, pour tout $k \geq 0$, on a

$$F^{(k)}(s) = \sum_{n=1}^{+\infty} \frac{a_n(-\log n)^k}{n^s}, \qquad \Re(s) > \sigma_c.$$

Preuve : Rappelons le théorème de Weierstrass : si $(f_n)_n$ est une suite de fonctions holomorphes sur un ouvert Ω du plan complexe et si $(f_n)_n$ converge uniformément vers f sur tout compact $K \subset \Omega$, alors la fonction f est holomorphe sur Ω et pour tout $k \geq 0$, on a

$$f^{(k)}(z) = \lim_{n \to +\infty} f_n^{(k)}(z), \qquad z \in \Omega.$$

Fixons donc K un compact contenu dans le demi-plan $\Re(s) > \sigma_c$. Il est facile de voir qu'il existe $s_0 \in \mathbb{C}$ et $0 \leq \alpha < \pi/2$ tel que $\Re(s_0) > \sigma_c$ et $K \subset \Delta_{s_0,\alpha}$. D'après le théorème 7.1.1, la série $\sum_n a_n n^{-s}$ converge uniformément vers F sur $\Delta_{s_0,\alpha}$ donc sur K. Le théorème de Weierstrass permet alors d'en déduire que F est holomorphe sur $\Re(s) > \sigma_c$. De plus, on a $F^{(k)}(s) = \sum_{n=1}^{+\infty} a_n(-\log n)^k n^{-s}$.

□

Le résultat suivant est un résultat d'unicité.

Proposition 7.2.2 *Soit*

$$F(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s} \qquad (\Re(s) > \sigma_c)$$

une série de Dirichlet. Supposons que, pour tout entier $N \geq 0$, on a

$$\lim_{\sigma \to +\infty} N^\sigma F(\sigma) = 0.$$

Alors $a_n = 0$, pour tout $n \geq 1$.

Preuve : Montrons le résultat par récurrence. Soit $\sigma_1 > \sigma_c$. La série converge uniformément sur $[\sigma_1, +\infty[$ d'après le théorème 7.1.1. Donc on peut écrire que

$$\lim_{\sigma \to +\infty} F(\sigma) = \sum_{n=1}^{+\infty} \lim_{\sigma \to +\infty} (a_n n^{-\sigma}).$$

Remarquons que

$$\lim_{\sigma \to +\infty} (a_n n^{-\sigma}) = \begin{cases} a_1 & \text{si } n = 1 \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, en utilisant l'hypothèse, on obtient que $a_1 = 0$. Supposons maintenant que $a_1 = a_2 = \cdots = a_{N-1} = 0$. Alors

$$N^\sigma F(\sigma) = \sum_{n=N}^{+\infty} a_n N^\sigma n^{-\sigma}.$$

En faisant tendre $\sigma \to +\infty$, on obtient que $a_N = 0$.

□

En particulier, la proposition suivante implique immédiatement le résultat suivant.

Corollaire 7.2.3 *Soient $F(s) = \sum_{n=1}^{+\infty} a_n n^{-s}$ et $G(s) = \sum_{n=1}^{+\infty} b_n n^{-s}$ deux séries de Dirichlet et supposons qu'il existe un réel σ_0 tel que $F(\sigma) = G(\sigma)$, pour tout $\sigma > \sigma_0$. Alors $a_n = b_n$, pour tout $n \geq 1$.*

7.3 Produit Eulérien

Le résultat suivant montre qu'une série de Dirichlet associée à une fonction arithmétique multiplicative admet une représentation en produit infini sur son demi-plan de convergence absolue. Cette représentation qui fait intervenir un produit qui porte uniquement sur les nombres premiers est fondamentale en arithmétique.

Théorème 7.3.1 *Soient f une fonction arithmétique multiplicative et σ_a l'abscisse de convergence absolue de la série de Dirichlet $\sum_n f(n)n^{-s}$. Alors*

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(\sum_{n=0}^{+\infty} \frac{f(p^n)}{p^{ns}} \right), \qquad \Re(s) > \sigma_a.$$

De plus, le produit infini converge uniformément sur tout demi-plan $\Re(s) \geq \Re(s_0) > \sigma_a$.

Preuve : Pour $T \geq 0$, notons

$$\mathcal{N}(T) = \{n \in \mathbb{N} : v_p(n) > 0 \Longrightarrow p \leq T\}.$$

Autrement dit, $\mathcal{N}(T)$ est l'ensemble des entiers naturels dont tous les facteurs premiers sont inférieurs ou égaux à T. Si $p_1, \ldots, p_k$ est la liste des nombres premiers $\leq T$, on a en utilisant la multiplicativité de f

$$\begin{aligned}\prod_{2\leq p\leq T}\left(\sum_{n=0}^{+\infty}\frac{f(p^n)}{p^{ns}}\right) &= \sum_{n_1,n_2,\ldots,n_k\geq 0}\frac{f(p_1^{n_1})\ldots f(p_k^{n_k})}{(p_1^{n_1}\ldots p_k^{n_k})^s}\\ &= \sum_{n\in\mathcal{N}(T)}\frac{f(n)}{n^s}.\end{aligned}$$

Ainsi

$$\left|\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}-\prod_{2\leq p\leq T}\left(\sum_{n=0}^{+\infty}\frac{f(p^n)}{p^{ns}}\right)\right| = \left|\sum_{n\notin\mathcal{N}(T)}\frac{f(n)}{n^s}\right| \leq \sum_{n\notin\mathcal{N}(T)}\frac{|f(n)|}{n^{\Re(s)}}.$$

Remarquons que $\{n\in\mathbb{N} : n\notin\mathcal{N}(T)\}\subset\{n\in\mathbb{N} : n>T\}$. D'où

$$\left|\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}-\prod_{2\leq p\leq T}\left(\sum_{n=0}^{+\infty}\frac{f(p^n)}{p^{ns}}\right)\right| \leq \sum_{n>T}\frac{|f(n)|}{n^{\Re(s)}}.$$

Pour $\Re(s)\geq\Re(s_0)>\sigma_a$, on a

$$\left|\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}-\prod_{2\leq p\leq T}\left(\sum_{n=0}^{+\infty}\frac{f(p^n)}{p^{ns}}\right)\right| \leq \sum_{n>T}\frac{|f(n)|}{n^{\Re(s_0)}}$$

et comme la série $\sum_n f(n)n^{-s}$ converge absolument sur $\Re(s)>\sigma_a$, pour tout $\varepsilon>0$, il existe $T\geq 0$ tel que

$$\sum_{n>T}\frac{|f(n)|}{n^{\Re(s_0)}}\leq\varepsilon.$$

D'où

$$\left|\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}-\prod_{2\leq p\leq T}\left(\sum_{n=0}^{+\infty}\frac{f(p^n)}{p^{ns}}\right)\right|\leq\varepsilon,$$

ce qui prouve le résultat.

□

Dans le cas d'une fonction complètement multiplicative, le produit eulérien se simplifie grandement.

Corollaire 7.3.2 *Soient f une fonction arithmétique complètement multiplicative et σ_a l'abscisse de convergence absolue de la série de Dirichlet $\sum_n f(n)n^{-s}$. Alors*

$$\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\left(1-\frac{f(p)}{p^s}\right)^{-1},\qquad \Re(s)>\sigma_a.$$

Preuve : D'après le théorème 7.3.1, comme $f(p^n)=f(p)^n$, on a

$$\sum_{n=1}^{+\infty}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\left(\sum_{n=0}^{+\infty}\left(\frac{f(p)}{p^s}\right)^n\right).$$

Comme le membre de gauche est fini, le membre de droite l'est aussi. Ainsi, pour tout premier p, la série

$$\sum_n \left(\frac{f(p)}{p^s}\right)^n$$

converge. Donc nécessairement, on a $|f(p)| < |p^s|$ et on obtient que

$$\sum_{n=0}^{+\infty} \left(\frac{f(p)}{p^s}\right)^n = \left(1 - \frac{f(p)}{p^s}\right)^{-1},$$

ce qui donne le résultat.

□

7.4 Produit de deux séries de Dirichlet

Considérons deux sommes du type

$$\sum \frac{f(n)}{n^s} \qquad \text{et} \qquad \sum \frac{g(n)}{n^s},$$

où $f, g : \mathbb{N}^* \longrightarrow \mathbb{C}$ sont deux fonctions arithmétiques nulles sauf en un nombre fini de points. Ainsi les deux sommes sont finies et on a

$$\left(\sum_{n=1}^{+\infty} \frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{g(n)}{n^s}\right) = \sum_{n,m\geq 1} \frac{f(n)g(m)}{n^s m^s}.$$

On peut alors regrouper dans la somme double les termes de même dénominateur, ce qui conduit à écrire

$$\left(\sum_{n=1}^{+\infty} \frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{g(n)}{n^s}\right) = \sum_{n=1}^{+\infty} \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right)\right) n^{-s} = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s}.$$

On voit donc apparaitre naturellement le produit de convolution $f*g$, ce qui justifie à postériori son introduction.

Nous avons supposé ici que les fonctions f et g sont supportées sur un ensemble fini, ce qui évite les problèmes de convergence car toutes les sommes sont finies. On a cependant un résultat plus général.

Théorème 7.4.1 *Soient*

$$F(s) = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s} \qquad \text{et} \qquad G(s) = \sum_{n=1}^{+\infty} \frac{g(n)}{n^s}$$

deux séries de Dirichlet d'abscisse de convergence absolue respectivement σ_a^F et σ_a^G. Notons σ_a l'abscisse de convergence absolue de la série de Dirichlet $\sum_n (f*g)(n)n^{-s}$. Alors

(i) $\sigma_a \leq \max(\sigma_a^F, \sigma_a^G)$.

(ii) Pour tout $s \in \mathbb{C}$, $\Re(s) > \max(\sigma_a^F, \sigma_a^G)$, *on a*

$$\sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s} = F(s)G(s).$$

Preuve : On a pour $\sigma = \Re(s) > \max(\sigma_a^F, \sigma_a^G)$, on a

$$\begin{aligned}
\sum_{n\leq x} \left| \frac{(f*g)(n)}{n^s} \right| &= \sum_{n\leq x} \frac{|(f*g)(n)|}{n^\sigma} \\
&= \sum_{n\leq x} \left| \sum_{dd'=n} f(d)g(d') \right| n^{-\sigma} \\
&\leq \sum_{n\leq x} \sum_{dd'=n} \frac{|f(d)||g(d')|}{n^\sigma} \\
&\leq \left(\sum_{d\leq x} \frac{|f(d)|}{d^\sigma} \right) \left(\sum_{d'\leq x} \frac{|g(d')|}{d'^\sigma} \right).
\end{aligned}$$

Ceci prouve que la série de Dirichlet $\sum_n (f*g)(n)n^{-s}$ converge absolument pour tout $s \in \mathbb{C}$ tel que $\Re(s) > \max(\sigma_a^F, \sigma_a^G)$. Ainsi on a $\sigma_a \leq \max(\sigma_a^F, \sigma_a^G)$, ce qui prouve le point (i). Pour le point (ii), remarquons que la série double

$$\sum_{n,m} \frac{f(n)g(m)}{(mn)^s}$$

converge absolument vers le produit $F(s)G(s)$ sur le demi-plan $\Re(s) > \max(\sigma_a^F, \sigma_a^G)$. Comme la convergence est absolue, on peut regrouper les termes arbitrairement et on a

$$F(s)G(s) = \sum_{n=1}^{+\infty} \left(\sum_{d|n} f(d)g\left(\frac{n}{d}\right) \right) n^{-s} = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s}.$$

□

7.5 La fonction zeta de Riemann

Il est immédiat de vérifier que la série de Dirichlet $\sum_n n^{-s}$ converge absolument pour $\Re(s) > 1$. Ainsi, d'après le Théorème 7.2.1, la fonction

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \qquad (\Re(s) > 1)$$

est analytique sur $\Re(s) > 1$ et s'appelle la fonction *zeta de Riemann.*

Théorème 7.5.1 *Pour* $\Re(s) > 1$, *on a*

$$\zeta(s) = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Preuve : découle immédiatement du corollaire 7.3.2.

□

Théorème 7.5.2 *La fonction ζ se prolonge en une fonction méromorphe sur le demi-plan $\Re(s) > 0$, avec un unique pôle, d'ordre 1, en $s = 1$.*

Preuve : La formule d'Abel implique immédiatement

$$\sum_{n=1}^{N} \frac{1}{n^s} = \frac{1}{N^{s-1}} + s \int_1^N \frac{\lfloor t \rfloor}{t^{s+1}}\, dt.$$

En écrivant que $\lfloor t \rfloor = t - \{t\}$, on obtient

$$\begin{aligned} \sum_{n=1}^{N} \frac{1}{n^s} &= \frac{1}{N^{s-1}} + s \int_1^N \frac{dt}{t^s} - s \int_1^N \frac{\{t\}}{t^{s+1}}\, dt \\ &= \frac{1}{(1-s)N^{s-1}} - \frac{s}{1-s} - s \int_1^N \frac{\{t\}}{t^{s+1}}\, dt. \end{aligned}$$

Comme $N^{\sigma-1} \to +\infty$ lorsque $N \to +\infty$, pour $\sigma = \Re(s) > 1$, on en déduit que

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\, dt = \frac{1}{s-1} + 1 - s \int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\, dt.$$

Remarquons alors que

$$\left| \frac{\{t\}}{t^{s+1}} \right| \leq \frac{1}{t^{\sigma+1}}$$

et l'intégrale $\displaystyle\int_1^{+\infty} \frac{dt}{t^{1+\sigma}}$ converge si $\sigma > 0$. On en déduit que la fonction

$$s \longmapsto \int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\, dt$$

est holomorphe sur $\Re(s) > 0$ et la fonction $s \longmapsto \zeta(s) - \dfrac{1}{s-1}$ se prolonge en une fonction holomorphe sur $\Re(s) > 0$.

□

7.6 Exercices

Exercice 7.6.1 Déterminer les abscisses de convergence et de convergence absolue de

1. $\displaystyle\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$.
2. $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ avec $a_n = \begin{cases} 1 & \text{si } n \text{ est un carré} \\ 0 & \text{sinon.} \end{cases}$

Exercice 7.6.2 Soit $\sum_n a_n n^{-s}$ une série de Dirichlet. Supposons que la suite des coefficients $(a_n)_n$ soit bornée. Montrer alors que l'abscisse de convergence absolue σ_a vérifie $\sigma_a \leq 1$. Est-ce que cette borne est optimale ?

Exercice 7.6.3 Soit $\sum_n a_n n^{-s}$ une série de Dirichlet et supposons que la suite des sommes partielles $\sum_{k=1}^{N} a_k$ soit bornée. Montrer alors que $\sigma_c \leq 0$.

Exercice 7.6.4 Soit $\sum_n a_n n^{-s}$ une série de Dirichlet telle que $a_n \geq 0$, $n \geq 1$. Supposons que la série converge sur $\Re(s) > \sigma_0$ pour un certain $\sigma_0 \in \mathbb{R}$ et notons

$$F(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}, \qquad \Re(s) > \sigma_0.$$

Montrer que si F se prolonge analytiquement au voisinage de σ_0, alors $\sigma_c < \sigma_0$.

Exercice 7.6.5 Soit λ la fonction de Liouville défine dans la feuille précédente. Déterminer l'abscisse de convergence absolue de

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}.$$

Transformer la somme en un produit eulérien et montrer que pour $\Re(s) > 1$ on a

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}.$$

Exercice 7.6.6

1. Montrer que la fonction d est le produit de convolution d'une fonction très simple par elle même.
2. En utilisant le théorème relatif à la série de Dirichlet d'un produit de convolution démontrer que l'abscisse de convergence de la série de Dirichlet

   $$\sum_{n=1}^{\infty} \frac{d(n)}{n^s}$$

   est inférieure ou égale à 1 et que, pour $\Re(s) > 1$ la somme de cette série de Dirichlet est $\zeta(s)^2$.

Exercice 7.6.7 Démontrer que pour tout s, $\Re(s) > 2$, on a

$$\sum_{n \geq 1} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1)$$

Démontrer que l'abscisse de convergence de cette série de Dirichlet est exactement2.

Exercice 7.6.8

1. Démontrer que, pour $\Re(s) > 2$ la série génératrice de $\varphi(n)$ est absolument convergente et que

   $$\sum_{n \geq 1} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

2. Retrouver ce résultat plus rapidement, en partant de l'identité

$$n = \sum_{d|n} \varphi(d),$$

que vous exprimerez comme une identité de convolution.

3. En utilisant la minoration $\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}$ montrer que l'abscisse de convergence de cette série de Dirichlet est 2.

Exercice 7.6.9 On se propose dans cet exercice de calculer un équivalent du nombre $S(x)$ des entiers sans facteur carré, inférieurs ou égaux à x.

1. Montrer que $S(x) = \sum_{n \leq x} \mu^2(n)$, où μ est la fonction de Möbius.
2. Montrer que la série de Dirichlet

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s}$$

converge pour $\Re(s) > 1$, et que, alors

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

3. Montrer qu'il existe une unique fonction arithmétique multiplicative g telle que $\mu^2 = \mathbf{I} * g$, et expliciter $g(p^\alpha)$. En déduire que $g(n) = 0$ si n n'est pas un carré, et que $g(n^2) = \mu(n)$.
4. Montrer que la série de Dirichlet de g converge absolument pour $\Re(s) > 1/2$, et que, dans ce cas

$$\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \frac{1}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{2s}}.$$

5. Transformer la somme $\sum_{n \leq x} \mu^2(n)$ en utilisant l'égalité $\mu^2 = g * \mathbf{I}$, puis une permutation de l'ordre de sommation. En déduire que

$$S(x) = \frac{x}{\zeta(2)} + O(\sqrt{x}).$$

Exercice 7.6.10 Soit $S := \left\{ n \geq 1 \ : \ p|n \longrightarrow p^2|n \right\}$ et $S_x = \text{card}\,(S \cap [1, x])$.

1. Montrer que tout élément de S s'écrit de manière unique sous la forme m^3u^2 avec m sans facteur carré.
2. En déduire que

$$S_x = \sum_{m \leq \sqrt[3]{x}} \mu(m)^2 \left\lfloor \sqrt{\frac{x}{m^3}} \right\rfloor = \sqrt{x} \sum_{m=1}^{\infty} \frac{\mu(m)^2}{m^{3/2}} + O\left(x^{1/3}\right)$$

3. En transformant la somme ci-dessus en un produit eulérien, montrer que

$$S_x \sim \frac{\zeta(3/2)}{\zeta(3)} \sqrt{x}.$$

Exercice 7.6.11 On peut démontrer relativement simplement, en utilisant le théorème des nombres premiers, que la série

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n}$$

est convergente (et réciproquement, si l'on admet que cette série est convergente, il est assez facile de prouver le théorème des nombres premiers).

En considérant la série de Dirichlet

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$$

démontrer que

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = 0.$$

Exercice 7.6.12 Soit G la série de Dirichlet associée à la fonction de Möbius,

$$G(s) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}.$$

1. Montrer que la série G converge absolument sur $\Re(s) > 1$.
2. Montrer que $\zeta(s)G(s) = 1$, $\Re(s) > 1$.
3. En déduire que

$$\sum_{n \leq x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right).$$

Exercice 7.6.13

1. Montrer que, pour tout entier n, on a
$$\varphi(n) = \sum_{d'd=n} d'\mu(d).$$
2. Montrer que
$$\sum_{n\leq x} \varphi(n) = \frac{3x^2}{\pi^2} + O(x \log x).$$
3. En déduire que la probabilité que deux entiers naturels (positifs) soient premiers entre eux est de $\frac{6}{\pi^2}$.

Chapitre 5

Appendice : Quelques rappels d'arithmétique élémentaire

Dans tout le cours, on note $\mathbb{N} = \{0, 1, 2, \dots, \}$ l'ensemble des entiers naturels et $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ l'ensemble des entiers relatifs. Rappelons que le groupe $\mathbb{Z}$ est l'unique groupe (à isomorphisme près) qui est cyclique (i.e. engendré par un seul élément) et infini. L'ensemble $\mathbb{Z}$ est également muni d'une multiplication qui en fait un anneau commutatif. Dans cet anneau, on a la notion importante de division euclidienne.

5.1 Division euclidienne

Théorème 5.1.1 (division euclidienne) *Soient $b \in \mathbb{N}^*$ un entier strictement positif et $a \in \mathbb{Z}$. Alors il existe un unique couple (q, r) d'entiers naturels tel que*

$$a = bq + r \quad avec \quad 0 \leq r < b.$$

L'entier q s'appelle le **quotient** *et r le* **reste** *de la division de a par b.*

Preuve : Exercice !

□

Notation Dans la suite, pour $a \in \mathbb{Z}$ et b un entier ≥ 1, on notera souvent $a \div b$ le quotient et $a \bmod b$ le reste de la division de a par b.

5.2 Divisibilité, Pgcd et Ppcm

Définition 5.2.1 *Soient $a, b \in \mathbb{Z}$. On dit que b est un* **diviseur** *de a (ou a est un* **multiple** *de b) s'il existe un entier q tel que $a = bq$. On écrit alors $b|a$ dans $\mathbb{Z}$.*

Etant donnés $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \setminus \{(0, 0, \ldots, 0)\}$. Comme $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, il existe un unique élément $d \in \mathbb{N}^*$ tel que

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}.$$

L'entier d s'appelle le **Pgcd** de $a_1, a_2, \ldots, a_n$ et se note $d = (a_1, a_2, \ldots, a_n)$. La terminologie de Pgcd est alors justifiée par le fait que d est le plus grand commun diviseur de $a_1, a_2, \ldots, a_n$ (exercice !). Comme $d \in d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, il existe un n-uplet d'entiers $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n$ tel que

$$d = a_1u_1 + a_2u_2 + \ldots a_nu_n \tag{5.1}$$

Une telle relation est appelée une **relation de Bezout**. Il faut prendre garde au fait que d'une part, le n-uplet d'entiers relatifs vérifiant (5.1) n'est pas unique. En effet, si $(u_1, u_2, \ldots, u_n)$ vérifie (5.1), alors pour tout $\alpha \in \mathbb{Z}$, on a

$$d = a_1(u_1 + \alpha a_2) + a_2(u_2 - \alpha a_1) + a_3u_3 + \ldots a_nu_n$$

et donc $(u_1 + \alpha a_2, u_2 - \alpha a_1, u_3, \ldots, u_n)$ vérifie aussi l'équation de Bezout (5.1). D'autre part, une relation (5.1) ne caractérise bien sûr pas le Pgcd (sauf si $d = 1$, voir théorème 5.2.3). En effet, par exemple si $a = 5$ et $b = 7$, alors on peut écrire $3 = 9 \times 5 - 6 \times 7$ et pourtant $(5, 7) \neq 3$.

Définition 5.2.2 *On dit que les entiers $a_1, a_2, \ldots, a_n$ sont* **premiers entre eux** *si $(a_1, a_2, \ldots, a_n) = 1$.*

Le résultat suivant caractérise les entiers premiers entre eux.

Théorème 5.2.3 (de Bezout) *Les entiers $a_1, a_2, \ldots, a_n$ sont premiers entre eux si et seulement s'il existe $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n$ tel que*

$$a_1u_1 + a_2u_2 + \ldots a_nu_n = 1. \tag{5.2}$$

Preuve : Si $(a_1, a_2, \ldots, a_n) = 1$, il est clair qu'il existe un n-uplet d'entiers satisfaisant la relation (5.2). Réciproquement supposons l'existence d'un tel n-uplet. Cela implique que $1 \in a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = (a_1, a_2, \ldots, a_n)\mathbb{Z}$. Donc l'entier positif $(a_1, a_2, \ldots, a_n)$ est inversible dans $\mathbb{Z}$ et comme les seuls inversibles de $\mathbb{Z}$ sont ± 1, on en déduit que $(a_1, a_2, \ldots, a_n) = 1$.

□

On rappelle dans la section suivante les algorithmes d'Euclide et d'Euclide étendu qui permettent de calculer le pgcd de nombres et une solution d'une relation de Bezout. Soient $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$. Comme $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$ est un

idéal de $\mathbb{Z}$, il existe un unique $m \in \mathbb{N}$ tel que

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = m\mathbb{Z}.$$

L'entier m s'appelle le **Ppcm** de $a_1, a_2, \ldots, a_n$ et se note $m = [a_1, a_2, \ldots, a_n]$. La terminologie de Ppcm est justifiée par le fait que m est plus petit commun multiple (strictement positif) de $a_1, a_2, \ldots, a_n$.

5.3 Algorithme d'Euclide

Etant donné $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, le problème qui se pose est de trouver le Pgcd d de (a, b) et un couple (u, v) satisfaisant la relation de Bezout (5.1). Un algorithme efficace est celui d'Euclide que nous allons rappeler dans cette section et qui consiste à effectuer des divisions euclidiennes successives.

5.3.1 Lemme fondamental

L'algorithme d'Euclide est basé sur le résultat suivant dont la preuve est laissée en exercice :

Lemme 5.3.1 *Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $(c, d) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ satisfaisant la relation $a = bc + d$. Alors $(a, b) = (b, d)$.*

5.3.2 Description de l'algorithme d'Euclide

Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Nous allons décrire l'algorithme d'Euclide permettant de calculer $d = (a, b)$. Comme $(a, b) = (|a|, |b|) = (|b|, |a|)$, on peut supposer que $0 < b < a$.

On pose $r_0 = a$ et $r_1 = b$. On effectue alors la division euclidienne de r_0 par r_1 : il existe $(q_1, r_2) \in \mathbb{Z}^2$ tel que

$$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1.$$

D'après le Lemme 5.3.1, on a $d = (r_0, r_1) = (r_1, r_2)$.
Si $r_2 = 0$, alors

$$d = (a, b) = (r_1, 0) = r_1.$$

Si $r_2 > 0$, on recommence. On effectue la division euclidienne de r_1 par r_2 : il existe $(q_2, r_3) \in \mathbb{Z}^2$ tel que

$$r_1 = q_2 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

En utilisant une nouvelle fois le Lemme 5.3.1, on a $d = (r_0, r_1) = (r_1, r_2) = (r_2, r_3)$. Si $r_3 = 0$, alors $d = (a, b) = (r_2, 0) = r_2$, sinon on recommence. On obtient ainsi une suite strictement décroissante r_i de nombres entiers positifs satisfaisant

$$r_i = q_{i+1} r_{i+1} + r_{i+2}. \tag{5.3}$$

et $d = (r_i, r_{i+1}) = (r_{i+1}, r_{i+2})$. Nécessairement, il existe $n \geq 2$ tel que $r_n = 0$. On a alors

$$d = (r_{n-1}, r_n) = r_{n-1}.$$

Autrement dit, le *Pgcd* de a, b cherché est le dernier reste non nul dans le calcul des divisions euclidiennes successives (5.3).

5.3.3 Description de l'algorithme d'Euclide étendu

Rappelons que si $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $d = (a, b)$, alors il existe un couple $(u, v) \in \mathbb{Z}^2$ satisfaisant une relation de Bezout

$$d = au + bv.$$

L'algorithme d'Euclide étendu décrit comment trouver un couple (u, v) satisfaisant une telle relation. Parallèlement aux divisions successives (5.3), on calcule $w_0 = (1, 0)$, $w_1 = (0, 1)$ puis

$$w_{i+2} = w_i - q_{i+1} w_{i+1}, \qquad 0 \leq i \leq n - 3. \tag{5.4}$$

Montrons par récurrence que pour tout $0 \leq i \leq n - 1$, on a $r_i = w_i \begin{pmatrix} a \\ b \end{pmatrix}$. On a

$$r_0 = a = (1, 0) \begin{pmatrix} a \\ b \end{pmatrix} \quad \text{et} \quad r_1 = b = (0, 1) \begin{pmatrix} a \\ b \end{pmatrix}.$$

Supposons maintenant la relation vraie au rang i et $i+1$. En utilisant (5.3) et (5.4), on a

$$\begin{aligned} w_{i+2} \begin{pmatrix} a \\ b \end{pmatrix} &= w_i \begin{pmatrix} a \\ b \end{pmatrix} - q_{i+1} w_{i+1} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= r_i - q_{i+1} r_{i+1} = r_{i+2}. \end{aligned}$$

Par récurrence, on en déduit donc la relation souhaitée. On en déduit alors que $d = (a, b) = r_{n-1} = w_{n-1} \begin{pmatrix} a \\ b \end{pmatrix}$. Ainsi si $w_{n-1} = (u, v)$, on a $d = au + bv$ et le couple (u, v) est une solution de l'équation de Bezout.

Ainsi, pour obtenir une solution à l'équation de Bezout, il suffit parallèlement aux divisions successives (5.3) de calculer les w_i donnés par la relation (5.4). Une solution à l'équation de Bezout est alors donnée par w_{n-1} si r_{n-1} est le dernier reste non nul (et donc le Pgcd de a et b).

5.3.4 Calcul du Pgcd de n nombres

Pour calculer le Pgcd de n nombres $(a_1, a_2, \ldots, a_n)$, on utilise l'algorithme d'Euclide par récurrence. Pour cela, la propriété d'associativité suivante est essentielle : étant donnés $(a, b, c) \in \mathbb{Z}^3$. On a

$$(a, b, c) = (a, (b, c)) = ((a, b), c) = ((a, c), b)$$

et

$$[a, b, c] = [a, [b, c]] = [[a, b], c] = [[a, c], b].$$

Pour calculer un n-uplet solution de l'équation de Bezout (5.1), on applique par récurrence l'algorithme d'Euclide étendu. Par exemple, si (a, b, c) est un triplet d'entiers relatifs et si $d = (a, b, c)$. On commence par trouver un couple d'entiers (u, v) solution de

$$au + bv = \delta,$$

où $\delta = (a, b)$. Puis comme $d = (\delta, c)$, on trouve un couple (λ, μ) solution de

$$\lambda\delta + \mu c = d.$$

Ainsi

$$d = \lambda(au + bv) + \mu c = \lambda ua + \lambda vb + \mu c.$$

Le triplet $(\lambda u, \lambda v, \mu)$ donne donc une solution à une relation de Bezout entre (a, b, c).

5.3.5 Complexité de l'algorithme d'Euclide

La question qui se pose est la complexité de calcul de l'algorithme d'Euclide pour calculer le PGCD. Faut-il effectuer beaucoup de divisions ? Un mathématicien français Gabriel Lamé a répondu à cette question en 1844.

Théorème 5.3.2 (Lamé) *Le nombre de divisions à effectuer pour trouver le PGCD de deux entiers naturels à l'aide de l'algorithme d'Euclide ne dépasse pas cinq fois le nombre de chiffres de l'écriture décimale du plus petit des deux nombres.*

Preuve : Soient deux entiers naturels a, b avec $a > b > 0$ et supposons que le PGCD de a et b, r_{n-1}, a été trouvé en $n-1$ divisions euclidiennes successives :

$$\begin{aligned}
a &= q_1 b + r_2, & 0 < r_2 < b \\
b &= q_2 r_2 + r_3, & 0 < r_3 < b \\
&\vdots & \vdots \\
r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_{n-1} r_{n-1}.
\end{aligned}$$

Comme tous les nombres intervenant sont des entiers naturels non nuls, on a donc $q_j \geq 1$ et $q_{n-1} > 1$. En effet, si $q_{n-1} = 1$, alors $r_{n-2} = r_{n-1}$, ce qui contredit la condition $r_{n-1} < r_{n-2}$. On trouve alors en remontant la chaîne des divisions euclidiennes de bas en haut :

$$\begin{aligned} r_{n-1} &\geq 1 \\ r_{n-2} &= q_{n-1}r_{n-1} \geq 2 \times 1 = 2 \\ r_{n-3} &= q_{n-2}r_{n-2} + r_{n-1} \geq 1 \times 2 + 1 = 3 \\ r_{n-4} &= q_{n-3}r_{n-3} + r_{n-2} \geq 1 \times 3 + 2 = 5 \\ r_{n-5} &= q_{n-4}r_{n-4} + r_{n-3} \geq 1 \times 5 + 3 = 8 \\ &\vdots \qquad \vdots \end{aligned}$$

On reconnaît alors dans les membres de droite les premiers termes de la suite de Fibonacci. Rappelons que cette suite est définie par :

$$F_1 = F_2 = 1 \text{ puis } F_n = F_{n-1} + F_{n-2}, \quad n \geq 3.$$

Montrons que, pour tout $1 \leq j \leq n-1$, on a $r_j \geq F_{n+1-j}$. C'est vrai pour $j = n-1$. Supposons que ce soit vrai pour tout $k \geq j$. Alors on a

$$r_{j-1} = q_j r_j + r_{j+1} \geq r_j + r_{j+1} \geq F_{n+1-j} + F_{n-j} = F_{n+2-j},$$

ce qui prouve la propriété pour $k = j - 1$. Ainsi par récurrence, on en déduit que tout $1 \leq j \leq n-1$, on a $r_j \geq F_{n+1-j}$. En particulier, on a

$$b = r_1 \geq F_n.$$

Autrement dit, pour qu'il y ait eu $n-1$ divisions dans l'algorithme d'Euclide, il faut donc que $b \geq F_n$, où b est le plus petit des deux nombres dont on cherche le PGCD.

Lemme 5.3.3 *On a $F_n \geq \alpha^{n-2}$, où $\alpha = (1+\sqrt{5})/2$ est le nombre d'or.*

Ainsi on obtient que $b \geq \alpha^{n-2}$. D'où

$$\log_{10} b = \frac{\log b}{\log 10} \geq (n-2)\log_{10}\alpha.$$

Or[1] $\log_{10}\alpha > \frac{1}{5}$, d'où

$$\log_{10} b \geq \frac{n-2}{5}.$$

1. On peut remarquer que $\alpha^5 = \left(\frac{5+\sqrt{125}}{10}\right)^5 > \left(\frac{5+11}{10}\right)^5 = \frac{16^5}{10^5} = \frac{1024^2}{10^5} \geq \frac{1000^2}{10^5} = 10$.

Soit maintenant k le nombre de chiffres dans le développement décimal de b. On a $b < 10^k$ et donc

$$\log_{10} b < k,$$

ce qui donne $k > \frac{n-2}{5}$. On obtient donc $n - 2 < 5k$ et comme les nombres sont des entiers, cela implique que

$$n - 1 \leq 5k.$$

Il reste le Lemme 5.3.3 à prouver. Il suffit pour cela d'utiliser une récurrence jointe à la relation $\alpha^2 = \alpha + 1$.

□

5.4 L'équation diophantienne $a_1x_1 + \cdots + a_nx_n = b$

Le résultat suivant est un résultat utile qui donne un critère pour qu'une équation diophantienne possède des solutions.

Théorème 5.4.1 *Soient $a_1, \ldots, a_n \in \mathbb{Z}$ non tous nuls. Pour tout entier $b \in \mathbb{Z}$, il existe des entiers $x_1, \ldots, x_n \in \mathbb{Z}$ tels que*

$$a_1x_1 + \cdots + a_nx_n = b \tag{5.5}$$

si et seulement si b est un multiple de $(a_1, \ldots, a_n)$. En particulier, l'équation (5.5) *a des solutions pour tout b si et seulement si les entiers $a_1, \ldots, a_n$ sont premiers entre eux.*

Preuve : Soit $d = (a_1, \ldots, a_n)$. Si l'équation (5.5) admet des solutions entières, alors d divise b car d divise chacun des a_i. Réciproquement, si $d|b$, alors $b = dq$ pour un certain $q \in \mathbb{Z}$. D'autre part, par définition, il existe des entiers $y_1, \ldots, y_n$ satisfaisant une relation de Bezout

$$a_1y_1 + \cdots + a_ny_n = d.$$

D'où

$$a_1qy_1 + \cdots + a_nqy_n = qd = b.$$

Autrement dit $x_1 = qy_1, \ldots, x_n = qy_n$ fournit une solution de (5.5).

□

5.5 Lemme de Gauss

Lemme 5.5.1 (Gauss) *Soient a, b, c dans $\mathbb{Z}$. Si $a|bc$ et $(a, b) = 1$, alors $a|c$.*

Preuve : Comme $(a,b)=1$, il existe $(u,v)\in\mathbb{Z}^2$ tel que

$$au+bv=1,$$

ce qui donne $acu+bcv=c$. Or $a|acu$ et $a|bc$ donc $a|bcv$. Finalement, on en déduit que $a|c=acu+bcv$.

□

Théorème 5.5.2 *Soient $a_1,a_2,\ldots,a_n\in\mathbb{Z}$. Si $b\in\mathbb{Z}$ est premier avec chacun des nombres $a_1,a_2,\ldots,a_n$, alors il est premier avec le produit $a_1a_2\ldots a_n$.*

Preuve : Comme $(b,a_i)=1$, il existe $(u_i,v_i)\in\mathbb{Z}^2$ tel que $a_iu_i+bv_i=1$, pour tout $i\in[\![1,n]\!]$. En multipliant ces inégalités, on obtient que

$$1=\prod_{i=1}^{n}(a_iu_i+v_ib)=a_1a_2\ldots a_nu_1u_2\ldots u_n+bv,$$

où $v\in\mathbb{Z}$. Ainsi le théorème de Bezout implique que $(a_1a_2\ldots a_n,b)=1$.

□

Théorème 5.5.3 *Soient $a_1,a_2,\ldots,a_n$ des nombres entiers deux à deux premiers entre eux. Si chaque entier a_i divise b, alors le produit $a_1a_2\ldots a_n$ divise aussi b.*

Preuve : On effectue une récurrence sur l'entier n. Si $n=2$, supposons donc que $(a_1,a_2)=1$, $a_1|b$ et $a_2|b$. En particulier, il existe $c\in\mathbb{Z}$ tel que $b=a_1c$. Comme $a_2|b=a_1c$ et $(a_1,a_2)=1$, le lemme de Gauss implique que $a_2|c$. Ainsi il existe $d\in\mathbb{Z}$ tel que $c=a_2d$. D'où

$$b=a_1c=a_1a_2d,$$

ce qui prouve que a_1a_2 divise aussi b. Supposons le résultat vrai jusqu'au rang $n-1$. Soient $a_1,a_2,\ldots,a_n$ n nombres entiers deux à deux premiers entre eux et supposons que chaque entier a_i divise b. D'après l'hypothèse de récurrence, on peut en déduire que le produit $a_1a_2\ldots a_{n-1}$ divise b. De plus, comme $(a_n,a_i)=1$, $1\leq i\leq n-1$, le théorème 5.5.2 implique que $(a_n,a_1a_2\ldots a_{n-1})=1$. Le cas $n=2$ implique alors que le produit $a_1a_2\ldots a_n$ divise b.

□

Le résultat suivant montre qu'on peut déduire le calcul du Ppcm de celui du Pgcd.

Théorème 5.5.4 *Soient $(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$. On a*

$$(a,b)\times[a,b]=|ab|.$$

Preuve : Notons $d = (a, b)$. Alors par définition, il existe $(\alpha, \beta) \in \mathbb{Z}^2$ tel que $a = \alpha d$ et $b = \beta d$. Montrons que $[a, b] = d|\alpha||\beta|$. Tout d'abord, il est clair que $d|\alpha||\beta|$ est un multiple de a et b. D'autre part, si δ est un multiple (positif) de a et b, alors il existe $(c, e) \in \mathbb{Z}^2$ tel que $\delta = ac = be$. D'où

$$\frac{\delta}{d} = \alpha c = \beta e.$$

Donc $\alpha|\frac{\delta}{d}$ et $\beta|\frac{\delta}{d}$. Comme $(\alpha, \beta) = 1$, le théorème 5.5.3 implique alors que $\alpha\beta|\frac{\delta}{d}$. Autrement dit, on en déduit que $|\alpha||\beta|d$ divise δ. Ceci montre donc que $[a, b] = d|\alpha||\beta|$. D'où

$$(a, b) \times [a, b] = d^2|\alpha||\beta| = |ab|.$$

□

5.6 Les nombres premiers

5.6.1 Théorème d'Euclide

Un **nombre premier** est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs (qui sont alors 1 et lui-même). Cette définition exclut 1, qui n'a qu'un seul diviseur entier positif; elle exclut aussi 0, qui est divisible par tous les entiers positifs. Par opposition, un nombre non nul produit de deux nombres entiers différents de 1 est dit **composé**.

Théorème 5.6.1 *Tout nombre entier naturel $n \geq 2$ est divisible par un nombre premier. Tout nombre entier naturel $n \geq 2$ non premier admet un diviseur premier $p \leq \sqrt{n}$.*

Preuve : Comme n est divisible par lui-même, si n est premier, il vérifie la première assertion du théorème. Supposons donc maintenant que n n'est pas premier et montrons qu'on peut trouver un diviseur de n qui est premier et inférieur ou égal à $\sqrt{n}$. Comme n n'est pas premier, l'ensemble

$$D^\sharp(n) = \{d \in \mathbb{N} : 1 < d < n \,\&\, d|n\}$$

est non vide. Ainsi, il admet un élément minimal, disons p. Remarquons alors nécessairement que p est premier. En effet, sinon il aurait un diviseur q tel que $1 < q < p$. Comme $q|p$ et $p|n$, la relation de transitivité de la divisibilité impliquerait que $q|n$. D'où $q \in D^\sharp(n)$, ce qui est absurde par minimalité de p. Donc p est premier. Remarquons maintenant que $\frac{n}{p}$ divise n et $1 < \frac{n}{p} < n$ (car $1 < p < n$). Donc par minimalité de p, on a $\frac{n}{p} \geq p$, soit $p \leq \sqrt{n}$.

□

Application : Méthode des divisions successives.

Pour voir si n est premier, on le divise par $2, 3, 5, 7, \ldots, p \leq \sqrt{n}$. Si une division tombe juste, alors n n'est pas premier, sinon n est premier. Par exemple, si n est de l'ordre de 10^{30}, alors $\sqrt{n}$ est de l'ordre de 10^{15}. Or $\pi(10^{15})$ est de l'ordre de 10^{13}, donc il faut environ 10^{13} divisions pour savoir si un nombre de l'ordre de 10^{30} est premier ou non. Sachant qu'un ordinateur effectue 10^9 opérations par seconde, cela prend environ 3 heures ! On verra dans ce cours d'autres méthodes plus efficaces.

Un des grands problème de la théorie des nombres est de comprendre la répartition des nombres premiers. Ce sujet est encore loin d'être épuisé et de nombres questions dans cette direction de recherche restent ouvertes. Un des outils pour comprendre cette répartition est d'introduire la fonction sommatoire

$$\pi(x) = \sum_{\substack{p \leq x \\ p \text{ premier}}} 1$$

qui compte le nombre de nombre premiers $p \leq x$.

Le résultat suivant montre que $\pi(x) \to +\infty$ lorsque $x \to +\infty$.

Théorème 5.6.2 (Euclide) *Il existe une infinité de nombres premiers.*

Preuve : On raisonne par l'absurde, en supposant qu'il existe un nombre fini de nombres premiers, disons $p_1 = 2, p_2 = 3, \ldots, p_n$. Soit $N = p_1 p_2 \ldots p_n + 1$. Le théorème précédent implique qu'il existe un nombre premier p qui divise N. Donc nécessairement il existe un entier $1 \leq i \leq n$ tel que $p_i | N$. Comme $p_i | p_1 p_2 \ldots p_n$, on a $p_i | N - p_1 p_2 \ldots p_n = 1$, ce qui est absurde.

□

Lemme 5.6.3 (Euclide) *Si un nombre premier p divise un produit, il divise un des facteurs.*

Preuve : On raisonne par récurrence sur le nombre de facteurs n. Pour $n = 2$, supposons que p divise le produit $a_1 a_2$. Remarquons que p étant premier, on a soit $(p, a_1) = 1$ soit $(p, a_1) = p$. Si $(p, a_1) = 1$, alors le lemme de Gauss implique que p divise a_2. Si $(p, a_1) = p$, alors cela signifie que p divise a_1. Ceci achève la preuve du cas $n = 2$. Soit maintenant $n > 2$. Supposons que le résultat est vrai pour $n - 1$ facteurs et supposons que p divise le produit $a_1 a_2 \ldots a_n$. En utilisant le cas $n = 2$, on obtient que p divise $a_1 a_2 \ldots a_{n-1}$ ou p divise a_n. Si p divise $a_1 a_2 \ldots a_{n-1}$, on

applique l'hypothèse de récurrence et on obtient que p divise l'un des facteurs a_i, $1 \leq i \leq n-1$. Ceci prouve le résultat.

□

Application : si p est premier et $1 \leq k \leq p-1$, alors p divise le coefficient binomial $\binom{p}{k}$. Rappelons que

$$\binom{p}{k} = C_p^k = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k(k-1)\dots 2}.$$

Par conséquent,

$$p(p-1)\dots(p-k+1) = \binom{p}{k} \times k(k-1)\dots 2.$$

Comme p divise le membre de gauche, il divise le produit $\binom{p}{k} \times k(k-1)\dots 2$. Le lemme d'Euclide implique alors que p divise un des facteurs. Comme p ne peut pas diviser $k, k-1, \dots, 2$ (car $k \leq p-1$), nécessairement p divise $\binom{p}{k}$.

5.6.2 Décomposition en facteurs premiers

Le théorème suivant dit que $\mathbb{Z}$ est un anneau factoriel.

Théorème 5.6.4 *Soit $n \in \mathbb{Z}^*$. Alors n admet une écriture sous la forme*

$$n = \varepsilon p_1 p_2 \dots p_k, \tag{5.6}$$

où $\varepsilon = \pm 1$ et les nombres p_i sont des nombres premiers. De plus cette écriture est unique à l'ordre près.

Preuve : On peut bien sûr supposer que $n > 0$ (quitte à multiplier par -1). On raisonne par récurrence sur n. Pour $n = 1$, c'est bien sûr vrai. Supposons que le résultat soit vrai pour tout entier $k \leq n-1$. D'après le théorème 5.6.1, l'entier n est divisible par un nombre premier $p \geq 2$. En particulier, on a $\frac{n}{p} \leq n-1$. On peut donc appliquer l'hypothèse de récurrence. Donc $\frac{n}{p}$ s'écrit comme un produit de facteurs premiers et donc n aussi. Il reste l'unicité de la décomposition. Soit deux écritures de n en produit de facteurs premiers

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

et supposons par exemple que $k \leq \ell$. Le nombre p_1 divise le produit $q_1 q_2 \dots q_\ell$. D'après le lemme d'Euclide, p_1 divise l'un des facteurs, disons q_{i_1} pour un certain $1 \leq i_1 \leq \ell$. Comme q_{i_1} est premier et que $p_1 \neq 1$, nécessairement $p_1 = q_{i_1}$. On peut alors simplifier par p_1 et q_{i_1}. De proche en proche, on obtient ainsi que pour tout $1 \leq r \leq k$, il existe $1 \leq i_r \leq \ell$ tel que

$$p_r = q_{i_r}.$$

Si $k < \ell$, alors $J := [\![1, \ell]\!] \setminus \{i_r : 1 \leq r \leq k\} \neq \emptyset$ et en simplifiant, on obtient finalement que

$$1 = \prod_{j \in J} q_j.$$

Comme $q_j \geq 2$, on aboutit à une contradiction. Ainsi $k = \ell$ et on obtient le résultat.

□

Dans la décomposition (5.6), rien ne dit bien sûr que les facteurs premiers p_k sont différents. Il est souvent utile de regrouper les facteurs identiques entre eux. Ainsi, on obtient que tout entier $n \in \mathbb{Z}^*$ s'écrit de façon unique sous la forme

$$n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \tag{5.7}$$

où $\varepsilon = \pm 1$, $\alpha_i \geq 1$ et les p_i sont des nombres premiers rangés par ordre croissant $p_1 < p_2 < \cdots < p_k$. L'écriture (5.7) s'appelle la *décomposition canonique* de n en facteurs premiers.

5.7 Valuation p-adique

Soit $n \in \mathbb{Z}^*$ et p un nombre premier. On définit la *valuation p-adique* de n comme le plus grand entier $\alpha \in \mathbb{N}$ tel que n est divisible par p^α mais pas par $p^{\alpha+1}$. On la note $v_p(n)$. De façon plus concise,

$$v_p(n) = \max\{\alpha \geq 0 : p^\alpha | n \text{ et } p^{\alpha+1} \not| n\}.$$

De plus, par convention, on pose $v_p(0) = +\infty$.

Remarquons que si p ne divise pas n, alors $v_p(n) = 0$. En particulier, pour un entier $n \in \mathbb{N}^*$ donné, la valuation p-adique $v_p(n)$ est nulle sauf pour un nombre fini de nombre premier p.

Exemple : pour $n = 100$, on a $v_2(100) = 2$, $v_5(100) = 2$ et $v_p(100) = 0$ pour tout $p \neq 2, 5$.

Notons $\mathbb{P}$ l'ensemble des nombres premiers,

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}.$$

Alors d'après le théorème 5.6.4, pour tout entier $n \in \mathbb{Z}^*$, on a

$$n = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

Bien que l'ensemble $\mathbb{P}$ soit infini, le produit ci-dessus est en fait un produit fini car comme on l'a remarqué $v_p(n) = 0$ sauf au plus pour un nombre fini de p.

Proposition 5.7.1 *Soient $m, n \in \mathbb{Z}^*$ tels que*

$$m = \varepsilon_1 \prod_{p \in \mathbb{P}} p^{v_p(m)} \quad et \quad n = \varepsilon_2 \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

Alors

$$(m, n) = \prod_{p \in \mathbb{P}} p^{\min(v_p(m), v_p(n))}$$

et

$$[m, n] = \prod_{p \in \mathbb{P}} p^{\max(v_p(m), v_p(n))}.$$

Preuve : Exercice!

□

La décomposition en facteurs premiers est un problème difficile. La proposition précédente s'applique seulement si on connait les factorisations de m et n en facteurs premiers. Sinon, l'algorithme d'Euclide est bien meilleur pour calculer le pgcd de deux nombres.

La proposition précédente regroupe quelques propriétés de la valuation p-adique.

Proposition 5.7.2 *Soient $a, b \in \mathbb{Z}^*$ et p un nombre premier. On a*

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Preuve : Exercice!

□

Pour $r = \frac{a}{b}$, $a, b \in \mathbb{Z}^*$, on pose

$$v_p(r) = v_p(a) - v_p(b). \tag{5.8}$$

Remarquons que la définition est correcte et ne dépend pas du choix de a et b. En effet, si $r = \frac{a'}{b'} = \frac{a}{b}$, avec $a, a', b, b' \in \mathbb{Z}^*$, alors $ab' = a'b$ et donc en appliquant la proposition 5.7.2 (i), on obtient $v_p(a) + v_p(b') = v_p(a') + v_p(b)$, ce qui donne

$$v_p(a) - v_p(b) = v_p(a') - v_p(b').$$

De plus, comme $v_p(\pm 1) = 0$, pour tout premier p, on obtient que la formule (5.8) prolonge la valuation p-adique pour les entiers. On vérifie facilement que la proposition 5.7.2 reste vrai sur les rationnels.

Chapitre 9

Appendice : Quelques rappels sur la théorie des corps

Dans cet appendice, nous nous contentons de rappeler les principales définitions et résultats sur les corps qui nous serons utiles dans ce cours ; la plupart des démonstrations sont omises et le lecteur est invité à consulter le livre d'I. Gozard, *Théorie de Galois*, Mathématiques 2-ème cycle, Ellipse, pour plus de détails.

9.1 Sous-groupes finis

Le théorème suivant est fondamental et nous en donnons une preuve complète.

Théorème 9.1.1 *Soit k un corps. Tout sous-groupe fini du groupe k^* est cyclique.*

Preuve : Soit G un groupe fini de k^* et soit n l'ordre de G. Soit d un diviseur de n. Le polynôme X^d-1, de degré d à coefficients dans k, admet au plus d racines dans k. Donc l'équation $x^d = 1$, d'inconnue $x \in G$, admet au plus d solutions distinctes. Montrons que cela implique que G est un groupe cyclique. Notons Ω_d l'ensemble des éléments de G d'ordre d. Nous devons montrer que $\Omega_n \neq \emptyset$. Notons

$$\psi(d) = \text{card}(\Omega_d)$$

et $T_d = \{x \in G : x^d = 1\}$. On a clairement $\Omega_d \subset T_d$. Supposons $\psi(d) \geq 1$ et soit $x \in \Omega_d$. Alors $x \in T_d$ et donc $\langle x \rangle \subset T_d$. Comme $\text{card}(T_d) \leq d$ et $\text{card}(\langle x \rangle) = d$, il vient $T_d = \langle x \rangle$. Donc T_d est un groupe cyclique d'ordre d et il a donc exactement $\varphi(d)$ générateurs. Comme nous venons de montrer que tout élément de Ω_d est un générateur de T_d, on en déduit que $\psi(d) \leq \varphi(d)$. D'autre part, si x est un générateur de T_d, alors x est d'ordre d et donc appartient à Ω_d. Ainsi on obtient $\varphi(d) \leq \psi(d)$ et donc

$$\psi(d) = \varphi(d).$$

On a donc montré que si d est un diviseur de n, alors $\psi(d)$ est soit 0 soit $\varphi(d)$. D'autre part, en utilisant le théorème de Lagrange, on voit que l'ensemble $\{\Omega_d : d|n\}$ forme une partition de G. Donc

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

D'après le corollaire 1.6.3, on a aussi

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

Finalement on en tire que pour tout entier d divisant n, on a $\psi(d) = \varphi(d)$. En particulier,

$$\psi(n) = \varphi(n) \geq 1$$

et donc $\Omega_n \neq \emptyset$.

□

9.2 Extension et sous-extension d'une extension de corps

Soit k un corps. On appelle **extension** de k tout corps K tel qu'il existe un homomorphisme de corps j de k dans K. La notation K/k, utilisée dans la suite, signifiera "le corps K est une extension du corps k".

Remarquons que si k est un sous-corps de K, alors K est une extension de k (il suffit de considérer l'injection canonique $i : k \longrightarrow K$). Réciproquement, un homéomorphisme de corps $j : k \longrightarrow K$ est forcément injectif (en effet, $\ker j$ est un idéal de k et les seuls idéaux d'un corps k sont $\{0\}$ et k lui-même ; le cas $\ker j = k$ est exclu car $j(1_k) = 1_K$). Par conséquent, le sous-corps $k' = j(k)$ de K est isomorphe à k. En identifiant k et k', on peut donc dire que k est un sous-corps de k.

Considérons maintenant

$$\begin{array}{rccc} j : & \mathbb{Z} & \longrightarrow & k \\ & n & \longmapsto & n1_k. \end{array}$$

L'application j est un homéomorphisme d'anneaux. En particulier, $\ker j$ est un idéal de $\mathbb{Z}$ et donc de la forme

$$\ker j = c\mathbb{Z},$$

pour un certain $c \in \mathbb{N}$. On appelle l'entier c la **caractéristique** du corps k et on note $c = \mathrm{car}(k)$. Remarquons qu'un corps et un quelconque de ses sous-corps ont la même caractéristique.

Lemme 9.2.1 *Soit k un corps fini. Alors $car(k) \neq 0$ et $car(k)$ divise le cardinal de k.*

Preuve : Si la caractéristique de k était nulle, alors $\mathrm{Im}j$ serait isomorphe à $\mathbb{Z}$, donc infini, ce qui est contraire à l'hypothèse. Donc $c = \mathrm{car}(k) \neq 0$. Maintenant, l'homéomorphisme j induit un isomorphisme entre $\mathbb{Z}/c\mathbb{Z}$ et $\mathrm{Im}j$. En particulier, le cardinal de $\mathrm{Im}j$ est c. Le théorème de Lagrange implique que $c = \mathrm{card}(\mathrm{Im}j)$ divise le cardinal de k.

□

Lemme 9.2.2 *Soit k un corps. Alors $car(k)$ est ou bien nulle ou bien un nombre premier.*

Preuve : On a vu dans la preuve précédente que $\mathrm{Im}(f)$ est isomorphe à $\mathbb{Z}/\mathrm{car}(k)\mathbb{Z}$. Or $\mathrm{Im}f$ étant intègre, l'anneau $\mathbb{Z}/\mathrm{car}(k)\mathbb{Z}$ est aussi intègre. Cela implique alors que $\mathrm{car}(k) = 0$ ou $\mathrm{car}(k) = p$, p premier.

□

On déduit facilement du lemme 9.2.2 que si k est un corps, alors soit k est une extension de $\mathbb{Q}$ si $\mathrm{car}(k) = 0$, soit k est une extension de $\mathbf{F}_p$ si $\mathrm{car}(k) = p$, p premier. En particulier, tout corps fini de cardinal p est isomorphe à $\mathbf{F}_p$.

Définition 9.2.3 *Soient L un corps et k un sous-corps de L. On appelle* **sous-extension** *de L/k tout sous-corps H de L qui contient k, c'est-à-dire tout corps H tel que*

$$k \subset H \subset L.$$

Etant donné L/k et P une partie de L, il existe un plus petit sous-corps de L (au sens de l'inclusion) qui contient k et P. Ce sous-corps est noté $k(P)$ et est appelé la **sous-extension de L/k engendrée par P**. Lorsque $P = \{\alpha_1, \ldots, \alpha_n\}$ est une partie finie de L, on note $k(\alpha_1, \ldots, \alpha_n)$ au lieu de $k(\{\alpha_1, \ldots, \alpha_n\})$ la sous-extension de L/k engendrée par P. On peut décrire plus précisément $k(P)$.

Proposition 9.2.4 *Soient L un corps, k un sous-corps de L et P une partie de L. Le corps $k(P)$ est le corps des fractions de l'anneau $k[P]$ [1], c'est-à-dire*

$$k(P) = \{ab^{-1} : a \in k[P], b \in k[P] \setminus \{0\}\}.$$

Exemple 9.2.5 *Soient k un corps, L une extension de k et $\alpha \in L$. Alors*

$$k(\alpha) = \left\{f(\alpha)g(\alpha)^{-1} : f, g \in k[X],\, g(\alpha) \neq 0\right\}.$$

1. Ici $k[P]$ désigne la sous k-algèbre de L engendrée par P.

Soient k un corps et L une extension de k. On dit que L est une **extension de type fini** de k s'il existe un nombre fini d'éléments $\alpha_1, \ldots, \alpha_n$ de L tel que

$$L = k(\alpha_1, \ldots, \alpha_n).$$

L'extension est dite **monogène** ou **simple** si $L = L(\alpha)$, pour un certain $\alpha \in L$.

Donnons un lemme élémentaire qui nous sera utile dans ce cours.

Lemme 9.2.6 *Soit K une extension de $\mathbf{F}_p$ et $y \in K$. On a*

$$y \in \mathbf{F}_p \Longleftrightarrow y^p = y.$$

Preuve : Si $y \in \mathbf{F}_p$, le théorème de Fermat implique que $y^p = y$. Donc

$$\mathbf{F}_p \subset \{x \in K : x^p = x\}.$$

D'autre part, le polynôme $P(X) = X^p - X$ a au plus p racines dans K. Comme $\text{card}(\mathbf{F}_p) = p$, on obtient que $\mathbf{F}_p = \{x \in K : x^p = x\}$, ce qui conclut la preuve.

□

9.3 Element algébrique et transcendant

Soient k un corps, K une extension de k et $a \in K$. On dit que a est **algébrique** sur k s'il existe un polynôme $P \in k[x]$ tel que $P(a) = 0$. Dans le cas contraire, on dit que a est **transcendant**.

Supposons que a soit algébrique sur k. Cela implique que l'idéal

$$I(a) = \{P \in k[X] : P(a) = 0\}$$

est non réduit à $\{0\}$. Comme $k[X]$ est principal, il existe un unique polynôme unitaire M_a de $k[X]$ tel que

$$I(a) = M_a k[X] = \{M_a(X)P(X) : P \in k[X]\}.$$

Le polynôme M_a s'appelle le **polynôme minimal** de a. On vérifie facilement que si $P \in k[X]$, alors P est le polynôme minimal de a si et seulement si P est unitaire, $P(a) = 0$ et P est irréductible dans $k[X]$.

Lemme 9.3.1 *Soient k un corps, K une extension de k et $a \in K$. Supposons que a soit algébrique sur k, alors*

$$k(a) = k[a].$$

Preuve : L'inclusion $k[a] \subset k(a)$ est claire. Comme $k(a)$ est le plus petit sous-corps de K contenant a et k, il suffit pour montrer l'inclusion inverse de montrer que $k[a]$ est un sous-corps de K contenant k et a. Bien évidemment, $k[a]$ est un sous-anneau de K contenant k et a. Soit $b \in k[a]$, $b \neq 0$ et notons M_a le polynôme minimal de a. Par hypothèse, il existe $P \in k[X]$ tel que $b = P(a)$. Comme $b \neq 0$, M_a ne divise pas P et comme M_a est irréductible, les deux polynômes M_a et P sont premiers entre eux dans $k[X]$. D'après le théorème de Bezout (valable dans l'anneau euclidien $k[X]$), il existe $U, V \in k[X]$ tels que

$$U(X)M_a(X) + V(X)P(X) = 1.$$

D'où $U(a)M_a(a) + V(a)P(a) = 1$, c'est-à-dire $V(a)b = 1$. Donc $b^{-1} = V(a) \in k[a]$ et $k[a]$ est un corps.

□

Proposition 9.3.2 *Soient K un corps et k un sous-corps de K. L'ensemble*

$$A = \{\alpha \in K : \alpha \text{ est algébrique sur } k\}$$

est un sous-corps de K qui contient k. Ce sous-corps A s'appelle la **fermeture algébrique** *de k dans K et se note $\overline{k}$.*

Preuve : La preuve est laissée en exercice.

Soit K un corps et k un sous-corps de K. On dit que K est une **extension algébrique** si tous les éléments de K sont algébriques sur k, ce qui est équivalent à $\overline{k} = K$.

9.4 Corps de rupture d'un polynôme

Soit f un polynôme irréductible de degré ≥ 1 sur un corps k. On peut construire une extension monogène de k dans lequel f a au moins un zéro. Rappelons la construction : puisque f est irréductible sur k, l'idéal $(f) = fk[X]$ est maximal dans l'anneau $k[X]$. L'anneau quotient $k[X]/(f)$ est alors un corps. On considère la surjection canonique

$$\begin{array}{rccc} s: & k[X] & \longrightarrow & k[X]/(f) \\ & P(X) & \longmapsto & P(X) + (f), \end{array}$$

et notons $\alpha = j(X)$. Remarquons que la restriction de s à k est injective. En effet, si $a, b \in k$ et $j(a) = j(b)$, alors $a - b \in (f)$. Comme f est un polynôme de degré supérieur ou égal à 1 sur $k[X]$, on en déduit que nécessairement $a - b = 0$, soit $a = b$. Ainsi s induit un isomorphisme de k sur $s(k)$ et on peut donc "plonger" k

dans $k[X]/(f)$ et considérer ce dernier corps comme un surcorps de k. De plus, si $g \in k[X]$,

$$g(X) = \sum_{\ell=0}^{N} a_\ell x^\ell, \qquad a_\ell \in k,$$

alors comme s est un homéomorphisme d'anneaux, on a

$$\begin{aligned} s(g) &= \sum_{\ell=1}^{N} a_\ell s(X)^\ell \\ &= \sum_{\ell=1}^{N} a_\ell \alpha^\ell \\ &= g(\alpha). \end{aligned}$$

En particulier,

$$f(\alpha) = s(f) = 0.$$

Remarquons que

$$k[X]/(f) = k(\alpha). \tag{9.1}$$

En effet, d'après le calcul précédent, l'inclusion $k[X]/(f) \subset k(\alpha)$ est claire. L'inclusion réciproque découle du fait que $k[X]/(f)$ est un corps qui contient k et α et $k(\alpha)$ est le plus petit sous-corps avec cette propriété. Le corps $L = k(\alpha)$ s'appelle un **corps de rupture** de f.

En itérant le processus précédent, on peut montrer le théorème suivant :

Théorème 9.4.1 *Soient k un corps et $P \in k[X]$ un polynôme de degré $n \geq 1$. Alors, il existe une extension L de k, unique à isomorphisme près, et il existe $(a, \alpha_1, \ldots, \alpha_n) \in L^{n+1}$ tel que*

(i) $P(X) = a(X - \alpha_1)\ldots(X - \alpha_n)$;

(ii) $L = k(\alpha_1, \ldots, \alpha_n)$.

Preuve : La preuve est laissée en exercice, voir []. □

L'extension L de k, donnée par le théorème 9.4.1, s'appelle le **corps de décomposition** de P sur k. Par unicité de la décomposition en facteurs irréductibles, on montre facilement que c'est l'extension minimale de k telle que P ait $n = \deg(P)$ racines (comptées avec multiplicité) dans cette extension.

Définition 9.4.2 *Soient k un corps et L une extension de k. On dit que L est une* **clôture algébrique** *de k si*

(a) L est algébrique sur k.

(b) L est algébriquement close, i.e. que tout polynôme de degré ≥ 1 de $L[X]$ est scindé sur L.

Le théorème suivant est important.

Théorème 9.4.3 *Soit k un corps commutatif. Alors k admet une clôture algébrique, notée $\widetilde{k}$. De plus, si $\widetilde{k}_1$ et $\widetilde{k}_2$ sont deux clôtures algébriques de k, alors il existe un k-isomorphisme de $\widetilde{k}_1$ sur $\widetilde{k}_2$.*

Preuve : admis. Voir []. □

9.5 Corps des racines n-ièmes sur un corps k

Soit k un corps et n un entier ≥ 3. On suppose que

(i) soit $\mathrm{car}(k) = 0$;

(ii) soit $\mathrm{car}(k) = p$, où p est un nombre premier ne divisant pas n.

On considère le polynôme $X^n - 1 \in k[X]$. On appelle **corps des racines n-ièmes de l'unité** sur k, et on note $\Sigma_n(k)$, le corps de décomposition du polynôme du polynôme $X^n - 1$ sur k. Notons que $\Sigma_n(k)$ peut aussi être vue comme le sous-corps de la clôture algébrique $\widetilde{k}$ de k engendrée par les racines du polynôme $X^n - 1$. On notera

$$\mu_n(\Sigma_n(k)) = \{\alpha \in \Sigma_n(k) : \alpha^n = 1\}$$

l'ensemble des racines du polynôme $X^n - 1$ dans $\Sigma_n(k)$.

Un élément de $\mu_n(\Sigma_n(k))$ s'appelle une **racine n-ième** de l'unité sur k.

Théorème 9.5.1 *L'ensemble $\mu_n(\Sigma_n(k))$ est un groupe cyclique d'ordre n.*

Preuve : On vérifie facilement que $\mu_n(\Sigma_n(k))$ est un sous-groupe de $(\sigma_n(k))^*$. Comme le polynôme $X^n - 1$ a au plus n racines distinctes dans $\Sigma_n(k)$, le groupe $\mu_n(\Sigma_n(k))$ est fini, d'ordre $\leq n$. Le théorème 9.1.1 implique donc que $\mu_n(\Sigma_n(k))$ est cyclique. De plus, le polynôme dérivé de $P(X) = X^n - 1$ est $P'(X) = nX^{n-1}$ qui n'admet que 0 comme racine. Donc le polynôme P n'admet que des racines simples dans $\Sigma_n(k)$ et comme il est de degré n, on en déduit finalement qu'il admet n racines distinctes dans son corps de décomposition. Ainsi $\mu_n(\Sigma_n(k))$ est d'ordre n.

□

Définition 9.5.2 *On appelle* **racine primitive n-ième de l'unité sur k** *tout générateur du groupe $\mu_n(\Sigma_n(k))$.*

Autrement dit, un élément $\zeta \in \mu_n(\Sigma_n(k))$ est dite primitive si $\zeta^d \neq 1$ pour tout $1 \leq d < n$. On sait qu'il existe $\varphi(n)$ racines primitives n-ième de l'unité sur k. Plus précisément, si ζ est une racine primitive n-ième de l'unité sur k, alors les autres racines primitives n-ième de l'unité sur k sont les ζ^r avec $1 \leq r < n$ et $(r, n) = 1$.

Nous donnons maintenant un lemme élémentaire mais qui nous sera utile.

Lemme 9.5.3 *Soit ζ une racine primitive n-ième de l'unité sur un corps k. Alors*

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

Preuve : Remarquons que

$$(1 - \zeta)(1 + \zeta + \cdots + \zeta^{n-1}) = 1 - \zeta^n = 0.$$

Comme $\zeta \neq 1$, on en déduit le résultat.

□