Théorie des Nombres

Notes de Cours

Master M1 — 2025–2026

Yaë Ulrich Gaba

« Les mathématiques sont la reine des sciences et la théorie des nombres est la reine des mathématiques. »
— Carl Friedrich Gauss

25 mars 2026

Préface

La théorie des nombres, que Carl Friedrich Gauss qualifiait de *reine des mathématiques* (*die Königin der Mathematik*), est l'une des branches les plus anciennes et les plus profondes des mathématiques. Ses origines remontent à l'Antiquité, aux travaux d'Euclide dans ses *Éléments*, et ses questions fondamentales — la nature des nombres premiers, la résolution des équations diophantiennes, la distribution des entiers ayant des propriétés arithmétiques particulières — continuent de fasciner et de défier les mathématiciens de notre époque.

Ce qui rend la théorie des nombres si singulière, c'est le contraste saisissant entre la simplicité apparente de ses énoncés et la profondeur souvent abyssale de ses démonstrations. La conjecture de Goldbach, formulée en 1742, peut être comprise par un collégien : *tout entier pair supérieur à* 2 *est somme de deux nombres premiers*. Pourtant, près de trois siècles plus tard, elle résiste toujours aux efforts des plus brillants esprits.

L'histoire de la théorie des nombres est jalonnée de noms illustres : Euclide, Diophante, Fermat, Euler, Gauss, Riemann, Ramanujan, et plus récemment Andrew Wiles, dont la démonstration du dernier théorème de Fermat en 1995 a couronné trois siècles et demi de recherches. Chacun de ces mathématiciens a apporté des outils nouveaux — l'analyse complexe, la géométrie algébrique, la théorie des représentations — montrant que la théorie des nombres se nourrit de toutes les branches des mathématiques et les enrichit en retour.

De surcroît, la théorie des nombres a acquis au cours des dernières décennies une importance pratique considérable. La cryptographie à clé publique, en particulier le système RSA, repose de manière essentielle sur l'arithmétique des grands nombres premiers et sur la difficulté du problème de la factorisation. La théorie des codes correcteurs d'erreurs, les générateurs de nombres pseudo-aléatoires et de nombreux algorithmes en informatique théorique puisent directement dans l'arsenal de la théorie des nombres.

Organisation de ces notes. Ce cours est conçu pour des étudiants de niveau licence avancée ou master. Il suppose une bonne maîtrise de l'algèbre élémentaire (groupes, anneaux) et de l'analyse de base. Les chapitres sont organisés de manière progressive :

- Les **Chapitres 1–2** posent les fondations : divisibilité, algorithme d'Euclide, nombres premiers, théorème fondamental de l'arithmétique.
- Les **Chapitres 3–5** développent l'arithmétique modulaire, les résidus quadratiques et les fonctions arithmétiques.
- Les **Chapitres 6–8** abordent des sujets plus avancés : fractions continues, approximation diophantienne, formes quadratiques.
- Les **Chapitres 9–10** offrent une introduction à la théorie analytique des nombres et aux méthodes du crible.

Chaque chapitre contient des démonstrations complètes, des exemples détaillés et une série d'exercices classés par difficulté :

⋆ Exercices d'application directe.

$\star\star$ Exercices demandant une réflexion plus poussée.

$\star\star\star$ Problèmes de niveau olympiade ou concours.

Conventions. Sauf mention contraire, les lettres a, b, c, d, m, n désignent des entiers. Le mot « nombre » sans qualificatif signifie « entier ». Toutes les démonstrations sont rédigées de manière complète ; le symbole $\square$ marque la fin d'une preuve.

Notations

Le tableau ci-dessous rassemble les notations utilisées tout au long de ce cours.

Notation	**Signification**
$\mathbb{N}$	Ensemble des entiers naturels $\{0, 1, 2, \ldots\}$
$\mathbb{N}^*$	Ensemble des entiers naturels non nuls $\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Anneau des entiers relatifs
$\mathbb{Q}$	Corps des nombres rationnels
$\mathbb{R}$	Corps des nombres réels
$\mathbb{C}$	Corps des nombres complexes
$\mathbb{Z}/n\mathbb{Z}$	Anneau des entiers modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	Groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
$\mathbb{F}_p$	Corps fini à p éléments (p premier)
$a \mid b$	a divise b
$a \nmid b$	a ne divise pas b
$\text{pgcd}(a, b)$	Plus grand commun diviseur de a et b
$\text{ppcm}(a, b)$	Plus petit commun multiple de a et b
$a \equiv b \pmod{n}$	a est congru à b modulo n
$\lfloor x \rfloor$	Partie entière (plancher) de x
$\lceil x \rceil$	Partie entière supérieure (plafond) de x
$\{x\}$	Partie fractionnaire de x : $\{x\} = x - \lfloor x \rfloor$
$v_p(n)$	Valuation p-adique de n
$\varphi(n)$	Indicatrice d'Euler
$\mu(n)$	Fonction de Möbius
$\tau(n)$, $d(n)$	Nombre de diviseurs de n
$\sigma(n)$	Somme des diviseurs de n
$\sigma_k(n)$	Somme des puissances k-ièmes des diviseurs de n
$\Lambda(n)$	Fonction de von Mangoldt
$\pi(x)$	Nombre de premiers $\leq x$
$\left(\frac{a}{p}\right)$	Symbole de Legendre
$\left(\frac{a}{n}\right)$	Symbole de Jacobi
$\text{ord}_n(a)$	Ordre de a modulo n
$f * g$	Convolution de Dirichlet de f et g
$f = O(g)$	$\lvert f(x)\rvert \leq C \lvert g(x)\rvert$ pour x assez grand
$f \sim g$	$f(x)/g(x) \to 1$ quand $x \to +\infty$

Table des matières

Chapitre 1

Divisibilité et Algorithme d'Euclide

« Les mathématiques sont la reine des sciences, et la théorie des nombres est la reine des mathématiques. »

— *Carl Friedrich Gauss*

1.1 Introduction historique

L'étude de la divisibilité est aussi ancienne que les mathématiques elles-mêmes. Dans le Livre VII de ses *Éléments*, rédigés vers 300 av. J.-C., Euclide pose les fondations de l'arithmétique en définissant la notion de diviseur, de nombre premier, et en établissant un algorithme pour calculer la « plus grande commune mesure » de deux entiers — ce que nous appelons aujourd'hui le *plus grand commun diviseur*.

L'algorithme d'Euclide est remarquable à plus d'un titre : c'est l'un des plus anciens algorithmes connus, et il reste l'un des plus efficaces pour le calcul du pgcd, même à l'ère des ordinateurs. Sa variante *étendue*, qui fournit les coefficients de Bézout, est au cœur de la cryptographie moderne, notamment du système RSA.

Ce chapitre développe de manière rigoureuse les notions fondamentales de divisibilité dans $\mathbb{Z}$, l'algorithme d'Euclide et ses applications.

1.2 Divisibilité dans $\mathbb{Z}$

Définition 1.1 (Divisibilité)**.** Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b, et l'on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. On dit aussi que a est un *diviseur* de b, ou que b est un *multiple* de a.
Si a ne divise pas b, on note $a \nmid b$.

Exemple 1.2 (Exemples fondamentaux)**.**
(i) $3 \mid 12$ car $12 = 4 \times 3$.
(ii) $7 \mid (-21)$ car $-21 = (-3) \times 7$.
(iii) $1 \mid n$ pour tout $n \in \mathbb{Z}$ car $n = n \times 1$.
(iv) $n \mid 0$ pour tout $n \in \mathbb{Z}$ car $0 = 0 \times n$.
(v) $0 \mid n$ si et seulement si $n = 0$.
(vi) $5 \nmid 13$ car il n'existe aucun $k \in \mathbb{Z}$ tel que $13 = 5k$.

Proposition 1.3 (Propriétés élémentaires de la divisibilité)**.** *Soient $a, b, c \in \mathbb{Z}$. Les propriétés suivantes sont vérifiées :*

(i) ***Réflexivité*** *: $a \mid a$.*

(ii) ***Transitivité*** *: si $a \mid b$ et $b \mid c$, alors $a \mid c$.*

(iii) ***Combinaison linéaire*** *: si $a \mid b$ et $a \mid c$, alors $a \mid (ub + vc)$ pour tous $u, v \in \mathbb{Z}$.*

(iv) ***Antisymétrie (à signe près)*** *: si $a \mid b$ et $b \mid a$, alors $a = \pm b$.*

(v) ***Compatibilité avec le produit*** *: si $a \mid b$, alors $a \mid bc$ pour tout $c \in \mathbb{Z}$.*

(vi) ***Simplification*** *: si $c \neq 0$ et $ca \mid cb$, alors $a \mid b$.*

Démonstration. (i) On a $a = 1 \cdot a$, donc $a \mid a$.

(ii) Supposons $a \mid b$ et $b \mid c$. Il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 b$. Alors $c = k_2(k_1 a) = (k_1 k_2)a$, d'où $a \mid c$.

(iii) Si $a \mid b$ et $a \mid c$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 a$. Pour tous $u, v \in \mathbb{Z}$:

$$ub + vc = u(k_1 a) + v(k_2 a) = (uk_1 + vk_2)\, a,$$

donc $a \mid (ub + vc)$.

(iv) Si $a \mid b$ et $b \mid a$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $a = k_2 b$. Si $a = 0$, alors $b = 0$ et $a = b$. Sinon, $a = k_2 k_1 a$, d'où $k_1 k_2 = 1$. Comme $k_1, k_2 \in \mathbb{Z}$, on a $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$, c'est-à-dire $a = \pm b$.

(v) Si $b = ka$, alors $bc = (kc)a$, donc $a \mid bc$.

(vi) Si $ca \mid cb$, il existe $k \in \mathbb{Z}$ tel que $cb = k \cdot ca$. Comme $c \neq 0$, on simplifie par c pour obtenir $b = ka$, soit $a \mid b$. □

Remarque 1.4. La relation de divisibilité est une relation d'ordre partiel sur $\mathbb{N}^*$: elle est réflexive, antisymétrique et transitive. Elle n'est pas totale : par exemple, $3 \nmid 5$ et $5 \nmid 3$.

1.3 Division euclidienne

Théorème 1.5 (Division euclidienne)**.** *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|\,.$$

L'entier q est appelé le quotient *et r le* reste *de la division euclidienne de a par b.*

Démonstration. **Existence.** Considérons l'ensemble

$$S = \{a - bk : k \in \mathbb{Z}\} \cap \mathbb{N} = \{a - bk : k \in \mathbb{Z},\ a - bk \geq 0\}.$$

Montrons que S est non vide. Si $b > 0$, prenons $k = -|a|$: alors $a - bk = a + b|a| \geq a + |a| \geq 0$. Si $b < 0$, prenons $k = |a|$: alors $a - bk = a + |b|\,|a| \geq 0$. Dans les deux cas, $S \neq \emptyset$.

Comme $S \subseteq \mathbb{N}$, S admet un plus petit élément par le principe du bon ordre. Notons $r = \min S$ et q l'entier correspondant, de sorte que $r = a - bq \geq 0$.

Montrons que $r < |b|$. Par l'absurde, supposons $r \geq |b|$. Alors

$$a - b(q + \operatorname{sgn}(b)) = a - bq - |b| = r - |b| \geq 0,$$

où $\operatorname{sgn}(b) = b/|b|$. Donc $r - |b| \in S$ avec $r - |b| < r$, ce qui contredit la minimalité de r. Par conséquent $0 \leq r < |b|$.

Unicité. Supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) vérifiant les conditions. Alors

$$bq_1 + r_1 = bq_2 + r_2 \implies b(q_1 - q_2) = r_2 - r_1.$$

Or $0 \leq r_1, r_2 < |b|$, d'où $|r_2 - r_1| < |b|$. Comme $b(q_1 - q_2) = r_2 - r_1$ et $|b(q_1 - q_2)| = |b|\,|q_1 - q_2|$, on doit avoir $|b|\,|q_1 - q_2| < |b|$, ce qui impose $|q_1 - q_2| < 1$, soit $q_1 = q_2$. Il s'ensuit que $r_1 = r_2$. □

Exemple 1.6 (Calculs de division euclidienne)**.**
(i) Division de $a = 157$ par $b = 13$: $157 = 13 \times 12 + 1$, donc $q = 12$ et $r = 1$.
(ii) Division de $a = -157$ par $b = 13$: $-157 = 13 \times (-13) + 12$, donc $q = -13$ et $r = 12$.
(iii) Division de $a = 100$ par $b = -7$: $100 = (-7) \times (-14) + 2$, donc $q = -14$ et $r = 2$.

Remarque 1.7. Le reste r est nul si et seulement si $b \mid a$. La division euclidienne généralise donc la notion de divisibilité : $b \mid a$ si et seulement si le reste de la division de a par b est 0.

1.4 Plus grand commun diviseur

Définition 1.8 (Plus grand commun diviseur)**.** Soient $a, b \in \mathbb{Z}$, non tous les deux nuls. Le *plus grand commun diviseur* de a et b, noté $\operatorname{pgcd}(a, b)$, est le plus grand entier $d \in \mathbb{N}^*$ tel que $d \mid a$ et $d \mid b$.

Proposition 1.9 (Existence et caractérisation du pgcd)**.** *Soient $a, b \in \mathbb{Z}$, non tous les deux nuls. Le $\operatorname{pgcd}(a, b)$ existe et est l'unique entier $d \in \mathbb{N}^*$ vérifiant :*

(i) $d \mid a$ et $d \mid b$;

(ii) pour tout $c \in \mathbb{Z}$, si $c \mid a$ et $c \mid b$, alors $c \mid d$.

Démonstration. L'ensemble des diviseurs communs de a et b est non vide (il contient 1) et majoré par $\max(|a|, |b|)$ (tout diviseur de a est $\leq |a|$ en valeur absolue, et de même pour b, sauf si $a = 0$ ou $b = 0$, auquel cas le pgcd est $|b|$ ou $|a|$ respectivement). Il admet donc un plus grand élément d.

Pour la propriété (ii), nous la démontrerons comme conséquence de l'identité de Bézout (cf. efthm :bezout). □

Proposition 1.10 (Propriétés du pgcd). *Pour tous $a, b, c \in \mathbb{Z}$:*

(i) $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, a)$ (commutativité).

(ii) $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(|a|, |b|)$.

(iii) $\operatorname{pgcd}(a, 0) = |a|$ *pour* $a \neq 0$.

(iv) $\operatorname{pgcd}(a, 1) = 1$.

(v) $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, b - qa)$ *pour tout* $q \in \mathbb{Z}$.

(vi) $\operatorname{pgcd}(ca, cb) = |c| \operatorname{pgcd}(a, b)$ *pour* $c \neq 0$.

Démonstration. Les propriétés (i)–(iv) découlent immédiatement de la définition.

(v) Il suffit de montrer que a et b ont les mêmes diviseurs communs que a et $b - qa$. Si $d \mid a$ et $d \mid b$, alors $d \mid (b - qa)$ par linéarité. Réciproquement, si $d \mid a$ et $d \mid (b - qa)$, alors $d \mid ((b - qa) + qa) = b$.

(vi) Si $d = \operatorname{pgcd}(a, b)$, alors $d \mid a$ et $d \mid b$, donc $|c|\ d \mid ca$ et $|c|\ d \mid cb$. Réciproquement, tout diviseur commun de ca et cb est de la forme $|c|\ e$ où e est un diviseur commun de a et b, d'où le résultat. □

La propriété (v) est la clé de l'algorithme d'Euclide.

1.5 Algorithme d'Euclide

L'algorithme d'Euclide calcule le pgcd de deux entiers par une suite de divisions euclidiennes. Il repose sur la propriété fondamentale $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, a \bmod b)$.

Théorème 1.11 (Algorithme d'Euclide — Correction). *Soient $a, b \in \mathbb{N}$ avec $b > 0$. La suite de divisions euclidiennes :*

$$\begin{aligned}
a &= bq_1 + r_1, && 0 \leq r_1 < b,\\
b &= r_1 q_2 + r_2, && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, && 0 \leq r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, && 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1} + 0,
\end{aligned}$$

se termine en un nombre fini d'étapes, et le dernier reste non nul r_n est $\operatorname{pgcd}(a, b)$.

Démonstration. **Terminaison.** La suite $b > r_1 > r_2 > \cdots \geq 0$ est une suite strictement décroissante d'entiers naturels. Par le principe du bon ordre, elle atteint 0 en un nombre fini d'étapes.

Correction. Par la propriété (v) de la efprop :pgcd :props, $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r_1) = \operatorname{pgcd}(r_1, r_2) = \cdots = \operatorname{pgcd}(r_{n-1}, r_n) = \operatorname{pgcd}(r_n, 0) = r_n$. □

Exemple 1.12 (Calcul de $\text{pgcd}(252, 198)$)**.** Appliquons l'algorithme d'Euclide :

$$\begin{aligned} 252 &= 198 \times 1 + 54, \\ 198 &= 54 \times 3 + 36, \\ 54 &= 36 \times 1 + 18, \\ 36 &= 18 \times 2 + 0. \end{aligned}$$

Le dernier reste non nul est 18, donc $\text{pgcd}(252, 198) = 18$.

Exemple 1.13 (Calcul de $\text{pgcd}(1071, 462)$)**.**

$$\begin{aligned} 1071 &= 462 \times 2 + 147, \\ 462 &= 147 \times 3 + 21, \\ 147 &= 21 \times 7 + 0. \end{aligned}$$

Le dernier reste non nul est 21, donc $\text{pgcd}(1071, 462) = 21$.

Proposition 1.14 (Complexité de l'algorithme d'Euclide)**.** *L'algorithme d'Euclide appliqué à deux entiers $a \geq b > 0$ effectue au plus $\lfloor 2\log_2(\max(a, b)) \rfloor + 1$ divisions. Plus précisément, si l'algorithme effectue n divisions, alors $b \geq F_n$ et $a \geq F_{n+1}$, où (F_k) est la suite de Fibonacci.*

Démonstration. Montrons que les restes décroissent au moins d'un facteur 2 tous les deux pas. Si $r_{i+1} \leq r_i/2$, c'est immédiat. Si $r_{i+1} > r_i/2$, alors $q_{i+2} = 1$ et $r_{i+2} = r_i - r_{i+1} < r_i/2$. Donc en deux étapes, le reste est au moins divisé par 2, ce qui donne au plus $2\log_2(b)$ étapes.

Pour la borne de Fibonacci, on montre par récurrence descendante que $r_{n-k} \geq F_{k+2}$ pour $0 \leq k \leq n$, en utilisant $r_{n-k-2} \geq r_{n-k-1} + r_{n-k} \geq F_{k+2} + F_{k+3} = F_{k+4}$, ce qui est la récurrence de Fibonacci. En remontant, on obtient $b \geq F_n$ et $a \geq F_{n+1}$. □

Remarque 1.15. Ce résultat est essentiellement le **théorème de Lamé** (1844) : le nombre de divisions dans l'algorithme d'Euclide appliqué à deux entiers inférieurs à N est au plus $\lfloor \log_\phi(N\sqrt{5}) \rfloor$, où $\phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. Les pires cas sont atteints pour des nombres de Fibonacci consécutifs.

1.6 Identité de Bézout

Théorème 1.16 (Identité de Bézout)**.** *Soient $a, b \in \mathbb{Z}$, non tous les deux nuls. Il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = \text{pgcd}(a, b).$$

De plus, l'ensemble $\{au + bv : u, v \in \mathbb{Z}\}$ est exactement l'ensemble des multiples de $\text{pgcd}(a, b)$, c'est-à-dire $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\,\mathbb{Z}$.

Démonstration. Considérons l'ensemble

$$I = \{au + bv : u, v \in \mathbb{Z}\} \cap \mathbb{N}^*.$$

Cet ensemble est non vide car $|a| = a \cdot \operatorname{sgn}(a) + b \cdot 0 \in I$ (en supposant $a \neq 0$; sinon $|b| \in I$). Soit $d = \min I$ le plus petit élément de I (par le principe du bon ordre). Par construction, $d = au_0 + bv_0$ pour certains $u_0, v_0 \in \mathbb{Z}$.

Montrons que $d \mid a$. Effectuons la division euclidienne de a par d : $a = dq + r$ avec $0 \leq r < d$. Alors

$$r = a - dq = a - (au_0 + bv_0)q = a(1 - u_0 q) + b(-v_0 q).$$

Donc $r \in a\mathbb{Z} + b\mathbb{Z}$. Si $r > 0$, alors $r \in I$ et $r < d$, ce qui contredit la minimalité de d. Donc $r = 0$ et $d \mid a$.

Par le même argument, $d \mid b$. Donc d est un diviseur commun de a et b.

Montrons que $d = \operatorname{pgcd}(a, b)$. Si c est un diviseur commun quelconque de a et b, alors $c \mid (au_0 + bv_0) = d$. Donc $c \leq d$ (en valeur absolue), ce qui montre que d est bien le plus grand diviseur commun.

Caractérisation de $I \cup \{0\}$. Si $m \in a\mathbb{Z} + b\mathbb{Z}$, effectuons la division euclidienne de m par d : $m = dq + r$ avec $0 \leq r < d$. Le même argument montre $r = 0$, donc $d \mid m$, i.e. $m \in d\mathbb{Z}$. Réciproquement, $d = au_0 + bv_0$, donc $dk = a(ku_0) + b(kv_0) \in a\mathbb{Z} + b\mathbb{Z}$. Ainsi $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. □

Corollaire 1.17. *Le $\operatorname{pgcd}(a, b)$ est le plus petit élément strictement positif de l'ensemble $\{au + bv : u, v \in \mathbb{Z}\}$.*

1.6.1 Algorithme d'Euclide étendu

L'algorithme d'Euclide étendu permet de calculer simultanément le $\operatorname{pgcd}(a, b)$ et les coefficients de Bézout u, v tels que $au + bv = \operatorname{pgcd}(a, b)$. L'idée est de remonter les étapes de l'algorithme d'Euclide.

Exemple 1.18 (Coefficients de Bézout pour $\operatorname{pgcd}(252, 198)$)**.** Reprenons l'exemple 1.12. On a trouvé :

$$\begin{aligned} 252 &= 198 \times 1 + 54, \\ 198 &= 54 \times 3 + 36, \\ 54 &= 36 \times 1 + 18. \end{aligned}$$

Remontons les équations :

$$\begin{aligned} 18 &= 54 - 36 \times 1 \\ &= 54 - (198 - 54 \times 3) \times 1 \\ &= 54 \times 4 - 198 \times 1 \\ &= (252 - 198 \times 1) \times 4 - 198 \times 1 \\ &= 252 \times 4 - 198 \times 5. \end{aligned}$$

Donc $u = 4$, $v = -5$ et $252 \times 4 + 198 \times (-5) = 1008 - 990 = 18$.

Exemple 1.19 (Coefficients de Bézout pour $\text{pgcd}(1071, 462)$)**.** Reprenons l'exemple 1.13 :

$$\begin{aligned} 1071 &= 462 \times 2 + 147, \\ 462 &= 147 \times 3 + 21. \end{aligned}$$

Remontée :

$$\begin{aligned} 21 &= 462 - 147 \times 3 \\ &= 462 - (1071 - 462 \times 2) \times 3 \\ &= 462 \times 7 - 1071 \times 3. \end{aligned}$$

Donc $1071 \times (-3) + 462 \times 7 = -3213 + 3234 = 21$. On a $u = -3$, $v = 7$.

Remarque 1.20 (Implémentation tabulaire). En pratique, on peut calculer les coefficients de Bézout par un tableau. On maintient à chaque étape les triplets (r_i, u_i, v_i) tels que $r_i = au_i + bv_i$:

Étape	r_i	u_i	v_i
0	a	1	0
1	b	0	1
$i+1$	$r_{i-1} - q_i r_i$	$u_{i-1} - q_i u_i$	$v_{i-1} - q_i v_i$

Lorsque $r_{i+1} = 0$, on a $\text{pgcd}(a, b) = r_i$ et les coefficients de Bézout sont (u_i, v_i).

1.7 Plus petit commun multiple

Définition 1.21 (Plus petit commun multiple)**.** Soient $a, b \in \mathbb{Z} \setminus \{0\}$. Le *plus petit commun multiple* de a et b, noté $\text{ppcm}(a, b)$, est le plus petit entier $m \in \mathbb{N}^*$ tel que $a \mid m$ et $b \mid m$.

Théorème 1.22 (Relation pgcd–ppcm)**.** *Pour tous* $a, b \in \mathbb{Z} \setminus \{0\}$,

$$\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = |ab| \,.$$

Démonstration. Posons $d = \text{pgcd}(a, b)$ et écrivons $a = da'$, $b = db'$ avec $\text{pgcd}(a', b') = 1$. Montrons que $\text{ppcm}(a, b) = da'b' = |ab| / d$.

D'abord, $a \mid da'b'$ car $da'b' = ab'$, et $b \mid da'b'$ car $da'b' = a'b$. Donc $da'b'$ est un multiple commun.

Soit m un multiple commun quelconque : $m = ak = bl$ pour certains $k, l \in \mathbb{Z}$. Alors $da'k = db'l$, soit $a'k = b'l$. Comme $\text{pgcd}(a', b') = 1$ et $a' \mid b'l$, le lemme de Gauss (eflemme :gauss) donne $a' \mid l$. Donc $m = bl = db'l \geq db'a' = da'b'$ (en valeur absolue). Ainsi $da'b'$ est le plus petit multiple commun positif.

Enfin, $d \cdot da'b' = d^2 a'b' = (da')(db') = |a|\,|b| = |ab|$. □

Exemple 1.23. $\text{pgcd}(12, 18) = 6$ et $\text{ppcm}(12, 18) = 36$. Vérifions : $6 \times 36 = 216 = 12 \times 18 = |12 \times 18|$. ✓

1.8 Entiers premiers entre eux et lemme de Gauss

Définition 1.24 (Entiers premiers entre eux)**.** Deux entiers a et b sont dits *premiers entre eux* (ou *copremiers*) si $\text{pgcd}(a, b) = 1$.

Proposition 1.25 (Caractérisation par Bézout)**.** *Deux entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. Si $\text{pgcd}(a, b) = 1$, l'identité de Bézout fournit directement de tels u, v. Réciproquement, si $au + bv = 1$ et si $d \mid a$ et $d \mid b$, alors $d \mid (au + bv) = 1$, donc $d = \pm 1$, et $\text{pgcd}(a, b) = 1$. □

Lemme 1.26 (Lemme de Gauss)**.** *Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.*

Démonstration. Puisque $\text{pgcd}(a, b) = 1$, l'identité de Bézout fournit $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. En multipliant par c :

$$acu + bcv = c.$$

Or $a \mid acu$ (évidemment) et $a \mid bcv$ (car $a \mid bc$ par hypothèse). Donc $a \mid (acu + bcv) = c$. □

Corollaire 1.27. *Si $a \mid c$, $b \mid c$ et $\text{pgcd}(a, b) = 1$, alors $ab \mid c$.*

Démonstration. De $a \mid c$, on tire $c = ak$ pour un certain $k \in \mathbb{Z}$. Comme $b \mid c = ak$ et $\text{pgcd}(a, b) = 1$, le lemme de Gauss donne $b \mid k$, soit $k = bl$. Donc $c = abl$ et $ab \mid c$. □

Corollaire 1.28. *Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

Démonstration. Si $p \nmid a$, alors $\text{pgcd}(p, a) = 1$ (car les seuls diviseurs positifs de p sont 1 et p, et $p \nmid a$). Par le lemme de Gauss, $p \mid b$. □

Remarque 1.29. Le efcor :gauss :premier$_d$*ivise*$_p$*roduitsegnraliseparrcurrence* : *si*p*estpremieret*p $\mid a_1 a_2 \cdots a_n$, alors $p \mid a_i$ pour au moins un indice i. Cette propriété est cruciale pour la démonstration de l'unicité dans le théorème fondamental de l'arithmétique (efthm :fta).

1.9 Diagramme du treillis de divisibilité

Le diagramme ci-dessous illustre le treillis des diviseurs de 30 : deux nœuds sont reliés si l'un divise l'autre (avec le plus petit en bas).

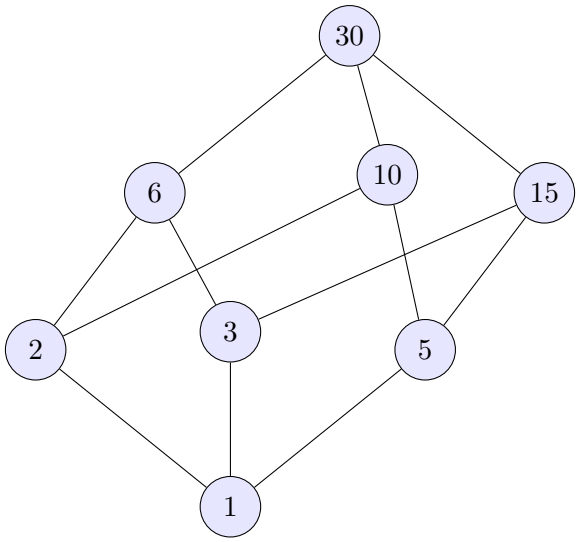


FIGURE 1.1 – Treillis des diviseurs de 30.

Dans ce treillis, le pgcd de deux éléments est leur borne inférieure et le ppcm est leur borne supérieure. Par exemple, $\text{pgcd}(6, 10) = 2$ (la borne inférieure de 6 et 10) et $\text{ppcm}(6, 10) = 30$ (la borne supérieure).

1.10 Connexion avec la cryptographie : le système RSA

Le calcul efficace du pgcd, via l'algorithme d'Euclide, est une brique fondamentale de la cryptographie à clé publique. Dans le système RSA, inventé par Rivest, Shamir et Adleman en 1977 :

1. On choisit deux grands nombres premiers p et q et on pose $n = pq$.
2. On choisit un exposant de chiffrement e tel que $\text{pgcd}(e, \varphi(n)) = 1$, où $\varphi(n) = (p-1)(q-1)$ est l'indicatrice d'Euler.
3. L'exposant de déchiffrement d est l'inverse de e modulo $\varphi(n)$, calculé par l'algorithme d'Euclide étendu : on trouve u, v tels que $eu + \varphi(n)v = 1$, et on prend $d = u \bmod \varphi(n)$.

L'algorithme d'Euclide étendu intervient donc de manière cruciale dans la génération des clés RSA. Sa rapidité (complexité en $O(\log^2 n)$ opérations sur les bits) est essentielle pour la praticabilité du système.

1.11 Exercices

Exercice 1.1 ($\star$)**.** Calculer, à l'aide de l'algorithme d'Euclide :

(a) $\text{pgcd}(420, 378)$,

(b) $\text{pgcd}(1001, 770)$,

(c) $\text{pgcd}(10403, 3731)$.

Pour chaque cas, trouver les coefficients de Bézout.

Exercice 1.2 ($\star$)**.** Calculer $\text{ppcm}(120, 252)$ de deux manières : directement et via la relation $\text{pgcd} \times \text{ppcm} = |ab|$.

Exercice 1.3 ($\star$)**.** Montrer que pour tout $n \in \mathbb{N}^*$, les entiers n et $n+1$ sont premiers entre eux.

Exercice 1.4 ($\star\star$)**.** Résoudre dans $\mathbb{Z}^2$ l'équation $252x + 198y = 36$.

Exercice 1.5 ($\star\star$)**.** Soient $a, b \in \mathbb{Z}$ tels que $\text{pgcd}(a,b) = 1$. Montrer que $\text{pgcd}(a+b, a-b) \in \{1, 2\}$.

Exercice 1.6 ($\star\star$)**.** Montrer que pour tout $n \geq 1$, $\text{pgcd}(F_n, F_{n+1}) = 1$, où (F_n) est la suite de Fibonacci définie par $F_1 = F_2 = 1$ et $F_{n+2} = F_{n+1} + F_n$.

Exercice 1.7 ($\star\star$)**.** Soient $a, b \in \mathbb{N}^*$. Montrer que $\text{pgcd}(a^n - 1, a^m - 1) = a^{\text{pgcd}(n,m)} - 1$.

Exercice 1.8 ($\star\star$)**.** Soient $a, b, c \in \mathbb{Z}$ avec $\text{pgcd}(a,b) = 1$. Montrer que si $a \mid c$ et $b \mid c$, alors $ab \mid c$.

Exercice 1.9 ($\star\star\star$)**.** Soient $a, b \in \mathbb{N}^*$ tels que $\text{pgcd}(a,b) = 1$. Montrer que tout entier $n \geq (a-1)(b-1)$ peut s'écrire sous la forme $n = xa + yb$ avec $x, y \in \mathbb{N}$. En déduire que le plus grand entier qui *ne peut pas* être représenté est $ab - a - b$.

Exercice 1.10 ($\star\star\star$)**.** Soit $n \geq 2$ un entier. Montrer que

$$\sum_{k=1}^{n} \text{pgcd}(k, n) = \sum_{d \mid n} d\, \varphi(n/d),$$

où φ désigne l'indicatrice d'Euler. *(On pourra regrouper les termes de la somme de gauche selon la valeur de* $\text{pgcd}(k,n)$*.)*

Exercice 1.11 ($\star\star\star$)**.** Montrer que $\text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m,n)}$ pour tous $m, n \geq 1$, où (F_n) est la suite de Fibonacci.

1.12 Résumé du chapitre

Chapitre 1 — Résumé

- **Divisibilité** : $a \mid b \iff \exists k \in \mathbb{Z},\ b = ka$. Relation d'ordre partiel sur $\mathbb{N}^*$.
- **Division euclidienne** : $a = bq + r$ avec $0 \leq r < |b|$; existence et unicité.
- **Pgcd** : plus grand diviseur commun ; calculé efficacement par l'algorithme d'Euclide en $O(\log(\min(a,b)))$ divisions.
- **Identité de Bézout** : $\text{pgcd}(a,b) = au + bv$ pour certains $u, v \in \mathbb{Z}$; les coefficients sont calculés par l'algorithme étendu.
- **Ppcm** : $\text{pgcd}(a,b) \cdot \text{ppcm}(a,b) = |ab|$.
- **Lemme de Gauss** : si $a \mid bc$ et $\text{pgcd}(a,b) = 1$, alors $a \mid c$.
- **Corollaire fondamental** : si p premier divise ab, alors $p \mid a$ ou $p \mid b$.

Chapitre 2

Nombres Premiers — Infinité, Distribution, Crible d'Ératosthène

« Les nombres premiers sont à la théorie des nombres ce que les atomes sont à la chimie : les constituants fondamentaux à partir desquels tout le reste est construit. »

2.1 Introduction historique

Les nombres premiers ont fasciné les mathématiciens depuis l'Antiquité. Euclide a démontré leur infinitude dans la Proposition 20 du Livre IX de ses *Éléments* — une démonstration dont l'élégance reste inégalée après plus de deux millénaires. Euler, au XVIII^{e} siècle, a donné une preuve analytique de l'infinitude des premiers en montrant que la série $\sum_p 1/p$, étendue aux nombres premiers, diverge. Cette approche a ouvert la voie à la théorie analytique des nombres.

Le XIX^{e} siècle a vu l'émergence de la question centrale : *comment les nombres premiers sont-ils distribués parmi les entiers ?* Les travaux de Legendre, Gauss, Chebyshev, Riemann, Hadamard et de la Vallée-Poussin ont culminé dans le *théorème des nombres premiers*, démontré indépendamment par Hadamard et de la Vallée-Poussin en 1896.

Au XX^{e} siècle, Paul Erdős et Atle Selberg ont donné en 1949 une preuve « élémentaire » (n'utilisant pas l'analyse complexe) du théorème des nombres premiers, un résultat qui a surpris la communauté mathématique.

2.2 Définitions fondamentales

Définition 2.1 (Nombre premier, nombre composé)**.** Un entier $p \geq 2$ est dit *premier* si ses seuls diviseurs positifs sont 1 et p. Un entier $n \geq 2$ qui n'est pas premier est dit *composé* : il possède un diviseur d vérifiant $1 < d < n$.
Par convention, 1 n'est ni premier ni composé.

Remarque 2.2. Le nombre 2 est le seul nombre premier pair. Tout nombre premier $p \geq 3$ est impair.

Proposition 2.3 (Existence d'un diviseur premier)**.** *Tout entier $n \geq 2$ possède un diviseur premier. De plus, le plus petit diviseur $d > 1$ de n est premier.*

Démonstration. Soit d le plus petit diviseur de n supérieur à 1. Un tel d existe car n se divise lui-même. Montrons que d est premier. Par l'absurde, si d est composé, il possède un diviseur d' avec $1 < d' < d$. Par transitivité de la divisibilité, $d' \mid n$, ce qui contredit la minimalité de d. □

Corollaire 2.4. *Si $n \geq 2$ est composé, alors n possède un diviseur premier $p \leq \sqrt{n}$.*

Démonstration. Si n est composé, $n = ab$ avec $1 < a \leq b < n$. Si $a > \sqrt{n}$, alors $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, contradiction. Donc $a \leq \sqrt{n}$, et a possède un diviseur premier $p \leq a \leq \sqrt{n}$. □

2.3 Le théorème fondamental de l'arithmétique

Théorème 2.5 (Théorème fondamental de l'arithmétique)**.** *Tout entier $n \geq 2$ s'écrit de manière unique (à l'ordre des facteurs près) comme produit de nombres premiers :*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

où $p_1 < p_2 < \cdots < p_k$ sont des nombres premiers et $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$.

Démonstration. **Existence** (par récurrence forte sur n).

Base : $n = 2$ est premier, donc $n = 2$ est un produit de premiers (un seul facteur).

Hérédité : soit $n \geq 3$. Supposons que tout entier m vérifiant $2 \leq m < n$ s'écrive comme produit de premiers.

- Si n est premier, alors n est un produit de premiers.
- Si n est composé, alors $n = ab$ avec $2 \leq a, b < n$. Par hypothèse de récurrence, a et b s'écrivent comme produits de premiers, donc $n = ab$ aussi.

Unicité (par récurrence forte sur n).

Supposons que n admette deux factorisations :

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

où les p_i et q_j sont premiers (non nécessairement distincts, non nécessairement ordonnés).

Comme $p_1 \mid n = q_1 q_2 \cdots q_s$, le

efcor :gauss :premier$_d ivise_p roduit(appliquparrcurrence) donne$p$_1$ $\mid q_j$ pour un certain j. Comme q_j est premier et $p_1 \geq 2$, on a $p_1 = q_j$.

En simplifiant par p_1 :

$$p_2 \cdots p_r = q_1 \cdots q_{j-1}\, q_{j+1} \cdots q_s.$$

Si $r = 1$, alors le membre gauche vaut 1, donc $s = 1$ et les deux factorisations sont identiques. Si $r \geq 2$, le produit $p_2 \cdots p_r < n$, et par hypothèse de récurrence, les deux factorisations du membre simplifié sont identiques (à l'ordre près). En réintroduisant $p_1 = q_j$, les deux factorisations de n sont identiques à l'ordre près. □

Notation 2.6 (Factorisation canonique). On écrira la factorisation canonique de n sous la forme

$$n = \prod_{p \mid n} p^{v_p(n)},$$

où $v_p(n)$ désigne la *valuation p-adique* de n, c'est-à-dire le plus grand exposant α tel que $p^\alpha \mid n$.

Proposition 2.7 (Pgcd et ppcm via les factorisations). *Si $a = \prod_p p^{\alpha_p}$ et $b = \prod_p p^{\beta_p}$, alors :*

$$\gcd(a,b) = \prod_p p^{\min(\alpha_p,\beta_p)}, \qquad \operatorname{ppcm}(a,b) = \prod_p p^{\max(\alpha_p,\beta_p)}.$$

Démonstration. Posons $d = \prod_p p^{\min(\alpha_p,\beta_p)}$. Pour tout premier p, on a $v_p(d) = \min(\alpha_p,\beta_p) \le \alpha_p = v_p(a)$, donc $d \mid a$. De même $d \mid b$. Si $c \mid a$ et $c \mid b$, alors $v_p(c) \le \min(\alpha_p,\beta_p) = v_p(d)$ pour tout p, donc $c \mid d$. Ainsi $d = \gcd(a,b)$.

La preuve pour le ppcm est analogue avec max au lieu de min. □

Exemple 2.8. $360 = 2^3 \cdot 3^2 \cdot 5$ et $756 = 2^2 \cdot 3^3 \cdot 7$. Donc :

$$\gcd(360,756) = 2^{\min(3,2)} \cdot 3^{\min(2,3)} \cdot 5^{\min(1,0)} \cdot 7^{\min(0,1)} = 2^2 \cdot 3^2 = 36,$$
$$\operatorname{ppcm}(360,756) = 2^{\max(3,2)} \cdot 3^{\max(2,3)} \cdot 5^{\max(1,0)} \cdot 7^{\max(0,1)} = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = 7560.$$

Vérifions : $36 \times 7560 = 272160 = 360 \times 756$. ✓

2.4 Infinitude des nombres premiers

Nous présentons trois démonstrations classiques de ce résultat fondamental.

Théorème 2.9 (Infinitude des nombres premiers — Euclide). *L'ensemble des nombres premiers est infini.*

2.4.1 Première preuve : par l'absurde (Euclide)

Preuve d'Euclide. Supposons par l'absurde que l'ensemble des nombres premiers soit fini : $\{p_1, p_2, \dots, p_n\}$. Considérons l'entier

$$N = p_1 p_2 \cdots p_n + 1.$$

Par la efprop :diviseur$_p$*remier*,N*possdeundiviseurpremier*p.*Orpourtout*i $\in \{1,\dots,n\}$, $p_i \mid p_1 p_2 \cdots p_n$, donc $p_i \mid (N - p_1 \cdots p_n) = 1$ si $p = p_i$, ce qui est impossible. Donc $p \neq p_i$ pour tout i, ce qui contredit l'hypothèse que $\{p_1,\dots,p_n\}$ est l'ensemble de *tous* les premiers. □

2.4.2 Deuxième preuve : par la divergence de $\sum 1/p$ (Euler)

Théorème 2.10 (Euler, 1737). *La série* $\displaystyle\sum_{p \text{ premier}} \frac{1}{p}$ *diverge. En particulier, l'ensemble des nombres premiers est infini.*

Démonstration. Pour $x \geq 2$, considérons le produit eulérien :

$$\prod_{p \leq x} \frac{1}{1 - 1/p} = \prod_{p \leq x} \sum_{k=0}^{\infty} \frac{1}{p^k} \geq \sum_{n=1}^{\lfloor x \rfloor} \frac{1}{n},$$

la dernière inégalité résultant du fait que le membre de droite est une sous-somme du développement du produit (par le théorème fondamental de l'arithmétique, chaque entier $n \leq x$ a tous ses facteurs premiers $\leq x$).

Or la série harmonique diverge : $\sum_{n=1}^{N} 1/n \geq \ln N$. Donc

$$\prod_{p \leq x} \frac{1}{1 - 1/p} \to +\infty \quad \text{quand } x \to +\infty.$$

En prenant le logarithme :

$$\sum_{p \leq x} -\ln\left(1 - \frac{1}{p}\right) \to +\infty.$$

Or $-\ln(1-t) = t + t^2/2 + t^3/3 + \cdots \leq t + t^2$ pour $0 < t \leq 1/2$, donc

$$\sum_{p \leq x} \frac{1}{p} \geq \sum_{p \leq x} \left(-\ln\left(1 - \frac{1}{p}\right)\right) - \sum_{p \leq x} \frac{1}{p^2}.$$

Comme $\sum_p 1/p^2 \leq \sum_{n=1}^{\infty} 1/n^2 = \pi^2/6 < \infty$, et le membre de gauche de l'inégalité tend vers $+\infty$, on conclut que $\sum_p 1/p = +\infty$. □

2.4.3 Troisième preuve : par les nombres de Fermat

Preuve par les nombres de Fermat. Considérons les nombres de Fermat $F_n = 2^{2^n} + 1$ pour $n \geq 0$:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad \ldots$$

Lemme. Pour $m \neq n$, $\operatorname{pgcd}(F_m, F_n) = 1$.

Preuve du lemme. Sans perte de généralité, supposons $m < n$. On montre par récurrence que

$$F_0 F_1 \cdots F_{n-1} = F_n - 2.$$

En effet, $F_0 = 3 = F_1 - 2$, et si la formule est vraie au rang $n-1$, alors $F_0 \cdots F_{n-1} = F_0 \cdots F_{n-2} \cdot F_{n-1} = (F_{n-1} - 2)F_{n-1} = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = 2^{2^n} - 1 = F_n - 2$.

Si $d \mid F_m$ et $d \mid F_n$, alors $d \mid (F_n - F_0 \cdots F_{n-1}) = 2$. Comme F_m est impair (car 2^{2^m} est pair), d est impair, donc $d = 1$.

Puisque les F_n sont deux à deux premiers entre eux et chacun ≥ 3, chacun possède au moins un diviseur premier, et ces diviseurs premiers sont distincts. Donc il y a au moins autant de premiers que de nombres de Fermat, soit une infinité. □

2.5 Le crible d'Ératosthène

Le crible d'Ératosthène est un algorithme ancien et élégant pour trouver tous les nombres premiers jusqu'à un entier N donné.

2.5.1 Description de l'algorithme

Étape 1. Écrire la liste des entiers de 2 à N.

Étape 2. Le plus petit nombre non barré ($p = 2$ au départ) est premier. Barrer tous ses multiples stricts $2p, 3p, 4p, \ldots$ qui sont $\leq N$.

Étape 3. Passer au prochain nombre non barré et répéter l'étape 2.

Étape 4. S'arrêter lorsque le prochain nombre non barré dépasse $\sqrt{N}$.

Étape 5. Les nombres non barrés restants sont premiers.

Proposition 2.11 (Correction du crible)**.** *Le crible d'Ératosthène identifie correctement tous les nombres premiers jusqu'à N.*

Démonstration. Un nombre $n \leq N$ est barré si et seulement s'il possède un diviseur premier $p \leq \sqrt{N}$, ce qui équivaut à être composé (par le efcor :diviseur$_p remier_s qrt$).$Lesnombresnonbarrssontdoncexactementlespremiers.$ □

Proposition 2.12 (Complexité du crible)**.** *Le crible d'Ératosthène a une complexité en $O(N \log \log N)$ opérations.*

Esquisse de preuve. Le nombre d'opérations de barrage est

$$\sum_{p \leq \sqrt{N}} \frac{N}{p} = N \sum_{p \leq \sqrt{N}} \frac{1}{p} \sim N \log \log \sqrt{N} \sim N \log \log N,$$

en utilisant le théorème de Mertens selon lequel $\sum_{p \leq x} 1/p \sim \log \log x$. □

2.5.2 Visualisation du crible

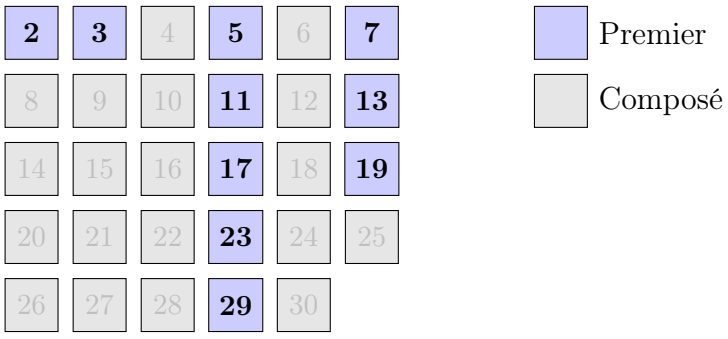


FIGURE 2.1 – Résultat du crible d'Ératosthène pour $N = 30$.

2.6 La fonction de comptage $\pi(x)$

Définition 2.13 (Fonction $\pi(x)$)**.** Pour $x \geq 0$ réel, on note $\pi(x)$ le nombre de nombres premiers p tels que $p \leq x$:

$$\pi(x) = \#\{p \leq x : p \text{ est premier}\}.$$

Exemple 2.14 (Valeurs de $\pi(x)$)**.**

x	10	20	50	100	200	500	1000	10^4	10^6	10^9
$\pi(x)$	4	8	15	25	46	95	168	1229	78498	50847534

Proposition 2.15 (Formule de Legendre)**.** *Pour tout entier $N \geq 2$, si $p_1, p_2, \ldots, p_k$ sont les nombres premiers inférieurs ou égaux à $\sqrt{N}$, alors*

$$\pi(N) - \pi(\sqrt{N}) + 1 = N - \sum_i \left\lfloor \frac{N}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{N}{p_i p_j} \right\rfloor - \cdots + (-1)^k \left\lfloor \frac{N}{p_1 p_2 \cdots p_k} \right\rfloor.$$

C'est une application directe du principe d'inclusion-exclusion.

Démonstration. Un entier n avec $1 \leq n \leq N$ est soit 1, soit premier $> \sqrt{N}$, soit admet un diviseur premier $\leq \sqrt{N}$. Les entiers de cette troisième catégorie sont exactement ceux divisibles par au moins un p_i. Le principe d'inclusion-exclusion compte les entiers $\leq N$ non divisibles par aucun des p_i, ce qui donne exactement 1 plus les premiers dans $(\sqrt{N}, N]$, soit $1 + \pi(N) - \pi(\sqrt{N})$. □

2.7 Le théorème des nombres premiers

Théorème 2.16 (Théorème des nombres premiers)**.** *Quand $x \to +\infty$,*

$$\pi(x) \sim \frac{x}{\ln x}.$$

Autrement dit, $\displaystyle\lim_{x \to +\infty} \frac{\pi(x)}{x/\ln x} = 1.$

Ce théorème, conjecturé par Legendre et Gauss vers 1800, a été démontré indépendamment par Hadamard et de la Vallée-Poussin en 1896, en utilisant les propriétés analytiques de la fonction zêta de Riemann $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. La preuve repose sur le fait que $\zeta(s)$ n'a pas de zéros sur la droite $\mathrm{Re}(s) = 1$.

Remarque 2.17 (Heuristique probabiliste). On peut interpréter le théorème des nombres premiers de la manière suivante : un entier n choisi « au hasard » est premier avec « probabilité » $\approx 1/\ln n$. Plus précisément, la « densité locale » des premiers autour

de n est $\sim 1/\ln n$. Ainsi :

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t} = \mathrm{Li}(x),$$

où $\mathrm{Li}(x)$ est l'intégrale logarithmique. En fait, $\mathrm{Li}(x)$ fournit une meilleure approximation de $\pi(x)$ que $x/\ln x$.

Théorème 2.18 (Encadrement de Chebyshev)**.** *Il existe des constantes $c_1, c_2 > 0$ telles que pour tout x assez grand :*

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}.$$

Plus précisément, Chebyshev a montré en 1852 que l'on peut prendre $c_1 = \ln 2/2 \approx 0{,}347$ et $c_2 = 6\ln 2/5 \approx 0{,}831$, et qu'en fait, si la limite $\lim_{x\to\infty} \pi(x)/(x/\ln x)$ existe, elle vaut 1.

Remarque 2.19. Chebyshev a également démontré le **postulat de Bertrand** : pour tout $n \geq 1$, il existe au moins un nombre premier p tel que $n < p \leq 2n$. Ce résultat, conjecturé par Bertrand en 1845, avait été vérifié numériquement par Bertrand jusqu'à $n = 6 \times 10^6$.

2.8 Nombres premiers remarquables

2.8.1 Nombres premiers de Mersenne

Définition 2.20 (Nombre de Mersenne)**.** Un *nombre de Mersenne* est un entier de la forme $M_n = 2^n - 1$, où $n \in \mathbb{N}^*$. Si M_n est premier, on parle de *premier de Mersenne*.

Proposition 2.21. *Si $M_n = 2^n - 1$ est premier, alors n est premier.*

Démonstration. Si $n = ab$ avec $1 < a, b < n$, alors

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)\big((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\big),$$

et $2^a - 1 > 1$, donc M_n est composé. □

Remarque 2.22. La réciproque est fausse : $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier. Les premiers de Mersenne connus en 2024 sont au nombre de 51, le plus grand étant $M_{82589933}$, un nombre à plus de 24 millions de chiffres. La recherche de nouveaux premiers de Mersenne est menée par le projet GIMPS (Great Internet Mersenne Prime Search).

2.8.2 Nombres premiers de Fermat

Définition 2.23 (Nombre de Fermat)**.** Le n-ième *nombre de Fermat* est $F_n = 2^{2^n} + 1$.

Proposition 2.24. *Si $2^m + 1$ est premier, alors m est une puissance de 2.*

Démonstration. Si m a un facteur impair $d > 1$, disons $m = de$, alors

$$2^m + 1 = (2^e)^d + 1 = (2^e + 1)\big((2^e)^{d-1} - (2^e)^{d-2} + \cdots + 1\big),$$

(car d est impair), et $2^e + 1 > 1$, donc $2^m + 1$ est composé. □

Remarque 2.25. Fermat conjecturait que tous les F_n sont premiers. Cela est vrai pour $n = 0, 1, 2, 3, 4$ ($F_4 = 65537$), mais Euler a montré en 1732 que $F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$ est composé. Aucun autre premier de Fermat n'a été trouvé depuis ; il est conjecturé que seuls $F_0, \ldots, F_4$ sont premiers.

2.8.3 Nombres premiers jumeaux et conjecture de Goldbach

Définition 2.26 (Nombres premiers jumeaux)**.** Deux nombres premiers p et $p + 2$ sont dits *jumeaux*. Exemples : $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$, $(41, 43)$, ...

Remarque 2.27 (Conjecture des premiers jumeaux). Il est conjecturé qu'il existe une infinité de paires de premiers jumeaux. En 2013, Yitang Zhang a démontré qu'il existe une infinité de paires de premiers $(p, p + k)$ avec $k \leq 70\,000\,000$. Depuis, le projet Polymath a réduit cette borne à 246 : il existe une infinité de paires de premiers distants d'au plus 246.

Remarque 2.28 (Conjecture de Goldbach). La *conjecture de Goldbach* (1742) affirme que tout entier pair $n \geq 4$ est somme de deux nombres premiers. Elle a été vérifiée numériquement jusqu'à 4×10^{18}, mais reste non démontrée.
Des résultats partiels importants existent :

- **Théorème de Vinogradov** (1937) : tout entier impair suffisamment grand est somme de trois nombres premiers.
- **Théorème de Chen** (1966) : tout entier pair suffisamment grand est somme d'un premier et d'un produit d'au plus deux premiers (un « P_2 »).
- **Théorème de Helfgott** (2013) : tout entier impair ≥ 7 est somme de trois nombres premiers (version effective du théorème de Vinogradov).

2.9 Visualisations

2.9.1 Spirale d'Ulam

La spirale d'Ulam, découverte par Stanislaw Ulam en 1963, est obtenue en écrivant les entiers en spirale à partir du centre et en marquant les nombres premiers. Des structures

diagonales étonnantes apparaissent.

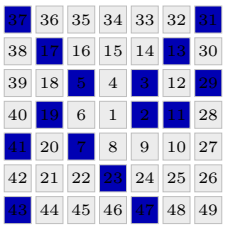


FIGURE 2.2 – Spirale d'Ulam (partielle) : les cases bleues sont les nombres premiers.

2.9.2 Graphe de la fonction $\pi(x)$

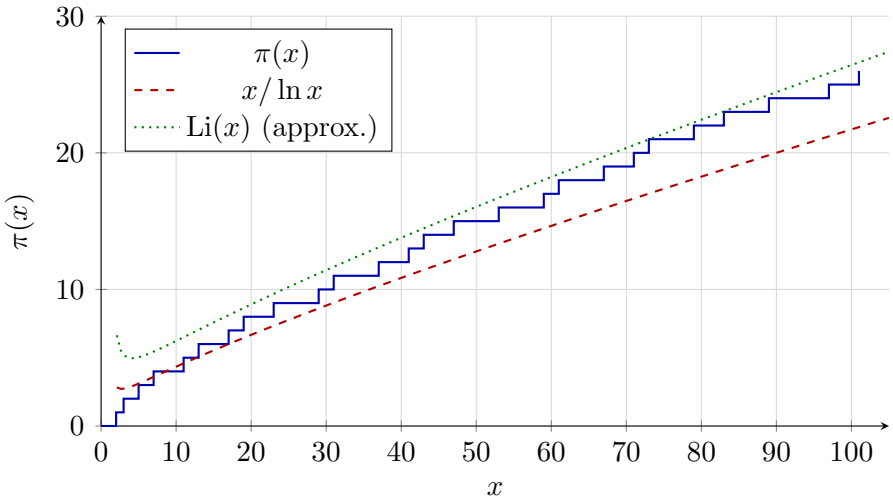


FIGURE 2.3 – La fonction $\pi(x)$ (escalier bleu) comparée à $x/\ln x$ (rouge pointillé) et une approximation de Li(x) (vert pointillé).

2.10 Connexions avec la cryptographie : le système RSA

La sécurité du système RSA repose sur la difficulté de factoriser de grands entiers. Le principe est le suivant :

1. **Génération des clés.** On choisit deux grands nombres premiers p et q (typiquement de 1024 bits chacun) et on calcule $n = pq$. Le nombre n est rendu public.
2. **Chiffrement.** Pour chiffrer un message $m < n$, on calcule $c = m^e \bmod n$, où e est l'exposant public.
3. **Déchiffrement.** Le destinataire, connaissant p et q, calcule $d = e^{-1} \bmod \varphi(n)$ et retrouve $m = c^d \bmod n$.

Un adversaire souhaitant casser le système devrait factoriser n pour retrouver p et q. Le meilleur algorithme connu (le crible du corps de nombres) a une complexité sous-exponentielle $L_n[1/3, c]$, ce qui le rend infaisable pour des n de 2048 bits ou plus.

C'est pourquoi la génération de grands nombres premiers est un enjeu crucial en cryptographie. Les tests de primalité (Miller–Rabin, AKS) permettent de vérifier efficacement qu'un nombre est premier, et le théorème des nombres premiers garantit que les premiers sont suffisamment denses : en moyenne, il faut tester environ $\ln n \approx 710$ candidats pour trouver un premier de 1024 bits.

2.11 Exercices

Exercice 2.1 ($\star$)**.** Trouver tous les nombres premiers inférieurs à 100 à l'aide du crible d'Ératosthène.

Exercice 2.2 ($\star$)**.** Factoriser en produit de facteurs premiers les entiers suivants :

(a) 2024,

(b) 10!,

(c) $\binom{20}{10}$.

Exercice 2.3 ($\star$)**.** Vérifier que $M_7 = 2^7 - 1 = 127$ est premier et que $M_{11} = 2^{11} - 1 = 2047$ est composé.

Exercice 2.4 ($\star\star$)**.** Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$. *(Indication : adapter la preuve d'Euclide en considérant $N = 4p_1p_2 \cdots p_n - 1$.)*

Exercice 2.5 ($\star\star$)**.** Montrer qu'il existe une infinité de nombres premiers de la forme $6k + 5$.

Exercice 2.6 ($\star\star$)**.** Montrer la formule de Legendre : pour tout premier p et tout $n \geq 1$,

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

En déduire que $v_p(n!) = \dfrac{n - s_p(n)}{p - 1}$, où $s_p(n)$ est la somme des chiffres de n en base p.

Exercice 2.7 ($\star\star$)**.** Montrer que le produit de n entiers consécutifs est divisible par $n!$. *(Indication : utiliser l'exercice précédent et les coefficients binomiaux.)*

Exercice 2.8 ($\star\star$)**.** En admettant le postulat de Bertrand, montrer que pour tout $n \geq 1$, il existe n nombres composés consécutifs. *(Indication : considérer $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$.)*

Exercice 2.9 ($\star\star\star$)**.** Montrer l'*inégalité de Bonse* : si $p_1 < p_2 < \cdots < p_n$ sont les n premiers nombres premiers et $n \geq 4$, alors $p_n^2 < p_1p_2 \cdots p_{n-1}$.

Exercice 2.10 ($\star\star\star$)**.** Soit p un nombre premier. Montrer que $\sqrt{p}$ est irrationnel.

Exercice 2.11 ($\star\star\star$)**.** Montrer que parmi n entiers consécutifs supérieurs à n, au moins l'un d'entre eux possède un facteur premier $> n$. *(C'est le théorème de Sylvester.)*

Exercice 2.12 ($\star\star\star$)**.** Montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod 4$. *(Indication : considérer $(2p_1p_2 \cdots p_n)^2 + 1$ et montrer que tout facteur premier de ce nombre est $\equiv 1 \pmod 4$.)*

2.12 Résumé du chapitre

Chapitre 2 — Résumé

- **Nombre premier** : $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p.
- **Théorème fondamental de l'arithmétique** : tout entier ≥ 2 s'écrit de manière unique comme produit de premiers (à l'ordre près).
- **Infinitude des premiers** : démontrée par Euclide (argument par l'absurde), Euler (divergence de $\sum 1/p$), et via les nombres de Fermat.
- **Crible d'Ératosthène** : algorithme en $O(N \log \log N)$ pour lister tous les premiers $\leq N$.
- **Théorème des nombres premiers** : $\pi(x) \sim x/\ln x$.
- **Encadrement de Chebyshev** : $c_1\, x/\ln x \leq \pi(x) \leq c_2\, x/\ln x$ pour x assez grand.
- **Premiers remarquables** : premiers de Mersenne $(2^p - 1)$, de Fermat $(2^{2^n} + 1)$, premiers jumeaux.
- **Conjectures ouvertes** : conjecture des premiers jumeaux, conjecture de Goldbach.
- **Applications** : la densité des premiers et la difficulté de la factorisation sont au cœur de la cryptographie RSA.

Chapitre 3

Congruences et Arithmétique Modulaire

« Les recherches dont les résultats sont exposés dans cet ouvrage ont pour objet la science des nombres entiers. »
— *Carl Friedrich Gauss,* Disquisitiones Arithmeticae *(1801)*

3.1 Introduction historique

La notion de congruence, telle que nous la connaissons aujourd'hui, a été formalisée par Carl Friedrich Gauss dans ses célèbres *Disquisitiones Arithmeticae*, publiées en 1801, alors qu'il n'avait que vingt-quatre ans. Gauss introduisit la notation $a \equiv b \pmod{n}$, qui révolutionna la manière de raisonner sur la divisibilité. Bien que des résultats isolés sur les restes fussent connus depuis l'Antiquité — les Chinois étudiaient déjà les systèmes de congruences simultanées — c'est Gauss qui érigea l'arithmétique modulaire en une théorie systématique et rigoureuse.

L'idée fondamentale est simple : deux nombres entiers sont considérés comme *équivalents* dès lors qu'ils laissent le même reste dans la division par un entier fixé n. Cette perspective transforme les questions de divisibilité en un calcul algébrique dans un ensemble fini, ce qui simplifie considérablement de nombreux problèmes.

3.2 Définition et propriétés élémentaires

Définition 3.1 (Congruence modulo n)**.** Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$ avec $n \geqslant 1$. On dit que a est **congru à** b **modulo** n, et l'on note

$$a \equiv b \pmod{n},$$

lorsque $n \mid (a - b)$, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a - b = kn$.

Remarque 3.2. De manière équivalente, $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Exemple 3.3.

(i) $17 \equiv 2 \pmod 5$ car $5 \mid (17-2) = 15$.

(ii) $-3 \equiv 8 \pmod{11}$ car $11 \mid (-3-8) = -11$.

(iii) $100 \equiv 0 \pmod 4$ car $4 \mid 100$.

(iv) Pour tout $a \in \mathbb{Z}$, on a $a \equiv a \pmod n$.

Proposition 3.4 (Relation d'équivalence)**.** *La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$:*

(i) ***Réflexivité :*** $a \equiv a \pmod n$ *pour tout* $a \in \mathbb{Z}$.

(ii) ***Symétrie :*** *si* $a \equiv b \pmod n$, *alors* $b \equiv a \pmod n$.

(iii) ***Transitivité :*** *si* $a \equiv b \pmod n$ *et* $b \equiv c \pmod n$, *alors* $a \equiv c \pmod n$.

Démonstration.

(i) On a $a - a = 0 = 0 \cdot n$, donc $n \mid (a-a)$.

(ii) Si $n \mid (a-b)$, alors $a - b = kn$ pour un certain $k \in \mathbb{Z}$, d'où $b - a = (-k)n$, et donc $n \mid (b-a)$.

(iii) Si $n \mid (a-b)$ et $n \mid (b-c)$, alors $a - c = (a-b) + (b-c)$ est la somme de deux multiples de n, donc $n \mid (a-c)$. □

Les classes d'équivalence pour cette relation sont appelées *classes de congruence* ou *classes de restes*. La classe de a modulo n est

$$\bar{a} = [a]_n = \{a + kn : k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Il y a exactement n classes distinctes : $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

3.3 Arithmétique des congruences

L'un des atouts majeurs de la congruence est sa *compatibilité* avec les opérations arithmétiques.

Théorème 3.5 (Compatibilité avec l'addition et la multiplication)**.** *Soient* $a, b, c, d \in \mathbb{Z}$ *et* $n \geqslant 1$. *Si* $a \equiv b \pmod n$ *et* $c \equiv d \pmod n$, *alors :*

(i) $a + c \equiv b + d \pmod n$,

(ii) $a - c \equiv b - d \pmod n$,

(iii) $ac \equiv bd \pmod n$.

Démonstration. Par hypothèse, $n \mid (a-b)$ et $n \mid (c-d)$.

(i) $(a+c) - (b+d) = (a-b) + (c-d)$, somme de deux multiples de n.

(ii) $(a-c) - (b-d) = (a-b) - (c-d)$, différence de deux multiples de n.

(iii) On écrit $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d)$. Or $n \mid c(a-b)$ et $n \mid b(c-d)$, donc $n \mid (ac - bd)$. □

Corollaire 3.6 (Puissances). *Si $a \equiv b \pmod{n}$, alors pour tout $k \in \mathbb{N}$,*

$$a^k \equiv b^k \pmod{n}.$$

Démonstration. Par récurrence sur k. Le cas $k = 0$ est trivial ($1 \equiv 1$). Si $a^k \equiv b^k \pmod{n}$, alors en multipliant par $a \equiv b \pmod{n}$ on obtient $a^{k+1} \equiv b^{k+1} \pmod{n}$ par le théorème 3.5(iii). □

Exemple 3.7. Calculons le reste de 3^{100} dans la division par 7.
On a $3^2 = 9 \equiv 2 \pmod{7}$, puis $3^3 \equiv 3 \cdot 2 = 6 \equiv -1 \pmod{7}$. Donc $3^6 \equiv (-1)^2 = 1 \pmod{7}$. Puisque $100 = 6 \times 16 + 4$, on obtient

$$3^{100} = (3^6)^{16} \cdot 3^4 \equiv 1^{16} \cdot 3^4 = 81 \equiv 81 - 11 \cdot 7 = 81 - 77 = 4 \pmod{7}.$$

Remarque 3.8 (Simplification prudente). Attention : on ne peut pas toujours simplifier une congruence. Si $ca \equiv cb \pmod{n}$, on ne peut conclure $a \equiv b \pmod{n}$ que si $\operatorname{pgcd}(c, n) = 1$. En effet, $ca \equiv cb \pmod{n}$ signifie $n \mid c(a - b)$. Si $\operatorname{pgcd}(c, n) = 1$, le lemme de Gauss donne $n \mid (a - b)$. En général, on a seulement

$$ca \equiv cb \pmod{n} \iff a \equiv b \pmod{*}\frac{n}{\operatorname{pgcd}(c, n)}.$$

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

Définition 3.9 (L'anneau $\mathbb{Z}/n\mathbb{Z}$). L'ensemble quotient

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

muni des opérations

$$\bar{a} + \bar{b} = \overline{a + b}, \qquad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

est un anneau commutatif unitaire. L'élément neutre pour l'addition est $\bar{0}$ et l'élément neutre pour la multiplication est $\bar{1}$.

Remarque 3.10. La bonne définition des opérations (c'est-à-dire leur indépendance par rapport au choix du représentant) est précisément le contenu du théorème 3.5.

Définition 3.11 (Éléments inversibles et diviseurs de zéro). Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

(i) $\bar{a}$ est **inversible** (ou est une **unité**) s'il existe $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a} \cdot \bar{b} = \bar{1}$.

(ii) $\bar{a}$ est un **diviseur de zéro** si $\bar{a} \neq \bar{0}$ et s'il existe $\bar{b} \neq \bar{0}$ tel que $\bar{a} \cdot \bar{b} = \bar{0}$.

Proposition 3.12 (Caractérisation des inversibles)**.** *L'élément $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si* $\text{pgcd}(a, n) = 1$*. De plus, lorsque $\bar{a}$ est inversible, son inverse peut être calculé à l'aide de l'identité de Bézout.*

Démonstration. $\bar{a}$ est inversible si et seulement s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$, c'est-à-dire $ab - 1 = kn$ pour un $k \in \mathbb{Z}$, soit $ab + n(-k) = 1$. Par le théorème de Bézout, une telle identité existe si et seulement si $\text{pgcd}(a, n) = 1$. □

Notation 3.13. Le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ se note $(\mathbb{Z}/n\mathbb{Z})^\times$. Son cardinal est la fonction indicatrice d'Euler $\varphi(n)$, que nous étudierons en détail au chapitre 4.

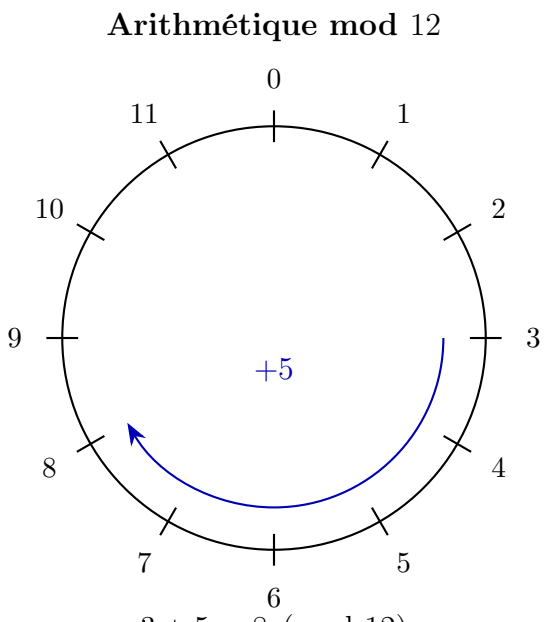
Corollaire 3.14 ($\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier)**.** *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Démonstration. Si $n = p$ est premier, alors pour tout a avec $1 \leqslant a \leqslant p - 1$, on a $\text{pgcd}(a, p) = 1$, donc $\bar{a}$ est inversible. Réciproquement, si n n'est pas premier, alors $n = ab$ avec $1 < a, b < n$, et $\bar{a} \cdot \bar{b} = \bar{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ avec $\bar{a} \neq \bar{0}$ et $\bar{b} \neq \bar{0}$: l'anneau possède des diviseurs de zéro et ne peut donc être un corps. □

Exemple 3.15. Dans $\mathbb{Z}/12\mathbb{Z}$, les inversibles sont les classes $\bar{a}$ avec $\text{pgcd}(a, 12) = 1$, soit $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$, de cardinal $\varphi(12) = 4$.
Les diviseurs de zéro sont $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$. Par exemple, $\bar{3} \cdot \bar{4} = \overline{12} = \bar{0}$.

3.5 Visualisation de l'arithmétique modulaire

L'arithmétique modulo n peut être visualisée comme une *arithmétique d'horloge* : les entiers sont disposés sur un cercle de n positions, et les opérations « bouclent » après n.



$3 + 5 \equiv 8 \pmod{12}$

Table de multiplication dans $\mathbb{Z}/7\mathbb{Z}$

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Remarque 3.16. Dans la table de multiplication modulo 7 (un nombre premier), chaque ligne et chaque colonne contient une permutation de $\{1, 2, 3, 4, 5, 6\}$. Cette propriété reflète le fait que tout élément non nul est inversible : $\mathbb{Z}/7\mathbb{Z}$ est un corps.

3.6 Congruences linéaires

Théorème 3.17 (Résolution de $ax \equiv b \pmod{n}$)**.** *Soient $a, b \in \mathbb{Z}$ et $n \geqslant 1$. Posons $d = \operatorname{pgcd}(a, n)$.*

(i) La congruence $ax \equiv b \pmod{n}$ admet une solution si et seulement si $d \mid b$.

(ii) Lorsque $d \mid b$, l'ensemble des solutions est une unique classe modulo n/d : si x_0 est une solution particulière, les solutions sont

$$x \equiv x_0 \pmod{*}\frac{n}{d}.$$

Modulo n, il y a donc exactement d solutions distinctes : $x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \ldots, x_0 + (d-1) \cdot \frac{n}{d}$.

Démonstration. L'équation $ax \equiv b \pmod{n}$ équivaut à l'existence de $y \in \mathbb{Z}$ tel que $ax + ny = b$. Par le théorème de Bézout, cette équation diophantienne admet une solution si et seulement si $d = \operatorname{pgcd}(a, n)$ divise b.

Supposons $d \mid b$. En divisant par d, on obtient

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{*}\frac{n}{d}.$$

Or $\operatorname{pgcd}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, donc $\frac{a}{d}$ est inversible modulo $\frac{n}{d}$, et il existe une unique solution $x_0 \equiv \left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d} \pmod{*}\frac{n}{d}$.

Modulo n, les valeurs $x_0, x_0 + \frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$ sont distinctes et forment l'ensemble complet des solutions. □

Exemple 3.18. Résolvons $6x \equiv 15 \pmod{21}$.
On a $d = \gcd(6, 21) = 3$ et $3 \mid 15$, donc il y a des solutions. On divise par 3 : $2x \equiv 5 \pmod 7$. L'inverse de 2 modulo 7 est 4 (car $2 \times 4 = 8 \equiv 1$). Donc $x \equiv 4 \times 5 = 20 \equiv 6 \pmod 7$.
Modulo 21, les trois solutions sont $x \equiv 6, 13, 20 \pmod{21}$.

Exemple 3.19. La congruence $4x \equiv 3 \pmod 6$ n'a pas de solution car $\gcd(4, 6) = 2$ et $2 \nmid 3$.

3.7 Systèmes de congruences

Il est fréquent de devoir résoudre simultanément plusieurs congruences. Par exemple :

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

La théorie complète de ces systèmes repose sur le *théorème des restes chinois* (CRT), que nous démontrerons au chapitre suivant. Pour l'instant, notons le résultat fondamental :

Théorème 3.20 (Théorème des restes chinois — énoncé préliminaire)**.** *Si $n_1, n_2, \ldots, n_k$ sont deux à deux premiers entre eux et si $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, alors le système*

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, \ldots, k,$$

admet une solution, unique modulo $N = n_1 n_2 \cdots n_k$.

Exemple 3.21. Le système ci-dessus donne $x \equiv 23 \pmod{105}$ (on vérifie : $23 = 7 \times 3 + 2$, $23 = 4 \times 5 + 3$, $23 = 3 \times 7 + 2$).

3.8 Critères de divisibilité par congruences

Les critères classiques de divisibilité s'expliquent élégamment par les congruences. Soit $N = a_k a_{k-1} \cdots a_1 a_0$ un entier écrit en base 10, c'est-à-dire $N = \sum_{i=0}^{k} a_i \cdot 10^i$.

Proposition 3.22 (Critère de divisibilité par 3 et par 9)**.** *Un entier N est divisible par 3 (resp. par 9) si et seulement si la somme de ses chiffres $a_0 + a_1 + \cdots + a_k$ est divisible par 3 (resp. par 9).*

Démonstration. Puisque $10 \equiv 1 \pmod 9$, on a $10^i \equiv 1 \pmod 9$ pour tout i, d'où

$$N = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1 = a_0 + a_1 + \cdots + a_k \pmod 9.$$

Comme $3 \mid 9$, le même raisonnement vaut modulo 3. □

Proposition 3.23 (Critère de divisibilité par 11)**.** *Un entier N est divisible par* 11 *si et seulement si la somme alternée de ses chiffres $a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$ est divisible par* 11*.*

Démonstration. On a $10 \equiv -1 \pmod{11}$, donc $10^i \equiv (-1)^i \pmod{11}$, d'où $N \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}$. □

Proposition 3.24 (Critère de divisibilité par 7)**.** *Les puissances de* 10 *modulo* 7 *suivent le cycle* $10^0 \equiv 1$, $10^1 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1 \pmod{7}$*, de période* 6*. Ainsi,*

$$N \equiv a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + \cdots \pmod{7}.$$

Exemple 3.25. Soit $N = 123\,456\,789$.

- Somme des chiffres : $1+2+3+4+5+6+7+8+9 = 45$. Or $9 \mid 45$, donc $9 \mid N$ (et a fortiori $3 \mid N$).
- Somme alternée : $9-8+7-6+5-4+3-2+1 = 5$. Or $11 \nmid 5$, donc $11 \nmid N$.

3.9 Exponentiation modulaire rapide

Le calcul de $a^k \bmod n$ est une opération fondamentale en théorie des nombres et en cryptographie. L'algorithme naïf (multiplier a par lui-même k fois) nécessite $k-1$ multiplications. L'algorithme d'**exponentiation rapide** (*binary exponentiation* ou *square-and-multiply*) réduit ce nombre à $O(\log k)$ multiplications.

Définition 3.26 (Algorithme d'exponentiation rapide)**.** Pour calculer $a^k \bmod n$:

1. Écrire k en binaire : $k = (b_s b_{s-1} \cdots b_1 b_0)_2$.
2. Initialiser $r \leftarrow 1$.
3. Pour $i = s, s-1, \ldots, 0$:
   - $r \leftarrow r^2 \bmod n$ (élever au carré),
   - si $b_i = 1$, alors $r \leftarrow r \cdot a \bmod n$ (multiplier).
4. Retourner r.

Exemple 3.27. Calculons $3^{45} \bmod 17$. On a $45 = (101101)_2$.

Étape	Bit b_i	Opération	Résultat $r \bmod 17$
Init	—	$r = 1$	1
$i = 5$	1	$1^2 = 1$, puis $1 \cdot 3 = 3$	3
$i = 4$	0	$3^2 = 9$	9
$i = 3$	1	$9^2 = 81 \equiv 13$, puis $13 \cdot 3 = 39 \equiv 5$	5
$i = 2$	1	$5^2 = 25 \equiv 8$, puis $8 \cdot 3 = 24 \equiv 7$	7
$i = 1$	0	$7^2 = 49 \equiv 15$	15
$i = 0$	1	$15^2 = 225 \equiv 4$, puis $4 \cdot 3 = 12$	12

Donc $3^{45} \equiv 12 \pmod{17}$, obtenu en seulement 9 multiplications modulaires au lieu de 44.

3.10 Connexion avec la cryptographie

L'arithmétique modulaire est la pierre angulaire de la cryptographie moderne. Le système RSA, inventé par Rivest, Shamir et Adleman en 1977, repose entièrement sur les propriétés des congruences et de l'exponentiation modulaire. L'idée centrale est que le calcul de $a^k \bmod n$ est efficace (grâce à l'exponentiation rapide), tandis que le problème inverse — trouver k connaissant a, $a^k \bmod n$ et n — est supposé calculatoirement difficile (c'est le problème du *logarithme discret*). Nous détaillerons le RSA au chapitre 4 après avoir établi les théorèmes de Fermat et d'Euler.

3.11 Exercices

Exercice 3.1 ($\star$)**.** Déterminer le reste de la division euclidienne de 2^{100} par 7.

Exercice 3.2 ($\star$)**.** Résoudre la congruence $5x \equiv 3 \pmod{13}$.

Exercice 3.3 ($\star$)**.** Montrer que $n^3 - n$ est divisible par 6 pour tout $n \in \mathbb{Z}$.

Exercice 3.4 ($\star$)**.** Calculer les quatre derniers chiffres de 7^{2024} (c'est-à-dire $7^{2024} \bmod 10000$).

Exercice 3.5 ($\star\star$)**.** Résoudre la congruence $12x \equiv 18 \pmod{30}$. Donner toutes les solutions modulo 30.

Exercice 3.6 ($\star\star$)**.** Dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$ et identifier les inversibles et les diviseurs de zéro.

Exercice 3.7 ($\star\star$)**.** Montrer que si p est un nombre premier impair, alors $1^2 + 2^2 + \cdots + (p-1)^2 \equiv 0 \pmod{p}$.

Indication : utiliser l'appariement $k \leftrightarrow p - k$.

Exercice 3.8 ($\star\star$)**.** Soit $n \geqslant 2$. Montrer que $\bar{a}$ est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\gcd(a, n) > 1$ et $a \not\equiv 0 \pmod{n}$.

Exercice 3.9 ($\star\star\star$)**.** Résoudre le système de congruences

$$\begin{cases} x \equiv 1 \pmod 2, \\ x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 7. \end{cases}$$

Exercice 3.10 ($\star\star\star$)**.** Montrer que pour tout $n \geqslant 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre si et seulement si n est premier.

Indication : un anneau intègre est un anneau commutatif unitaire sans diviseur de zéro non nul.

Exercice 3.11 ($\star\star\star$)**.** Soit p un nombre premier. Montrer que les seules solutions de $x^2 \equiv 1 \pmod p$ sont $x \equiv \pm 1 \pmod p$.

Résumé du chapitre

1. $a \equiv b \pmod n$ si et seulement si $n \mid (a - b)$. C'est une relation d'équivalence compatible avec l'addition et la multiplication.
2. L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire ; c'est un corps si et seulement si n est premier.
3. L'élément $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\operatorname{pgcd}(a, n) = 1$.
4. La congruence $ax \equiv b \pmod n$ a des solutions si et seulement si $\operatorname{pgcd}(a, n) \mid b$, auquel cas il y a exactement $\operatorname{pgcd}(a, n)$ solutions modulo n.
5. Les critères de divisibilité classiques découlent des congruences de 10 modulo $3, 7, 9, 11$.
6. L'exponentiation rapide permet de calculer $a^k \bmod n$ en $O(\log k)$ multiplications.
7. L'arithmétique modulaire est le fondement de la cryptographie moderne (RSA, échange de Diffie–Hellman).

Chapitre 4

Théorèmes de Fermat, Euler et Wilson

« J'ai trouvé un grand nombre de très belles propositions que je vous communiquerai une autre fois ... Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1 [...]. »

— Pierre de Fermat, lettre à Frénicle de Bessy (18 octobre 1640)

4.1 Introduction historique

En 1640, dans une lettre adressée à Bernard Frénicle de Bessy, Pierre de Fermat énonça sans démonstration ce qui allait devenir l'un des résultats les plus célèbres de la théorie des nombres : si p est premier et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$. La première démonstration publiée est due à Euler (1736), qui, trente ans plus tard, généralisa le résultat à tout module n en introduisant sa fameuse fonction φ.

Quant au théorème de Wilson, il fut conjecturé par Edward Waring en 1770 (l'attribuant à son élève John Wilson) et démontré pour la première fois par Lagrange la même année.

4.2 La fonction indicatrice d'Euler $\varphi(n)$

Définition 4.1 (Fonction indicatrice d'Euler)**.** Pour $n \geqslant 1$, on définit la **fonction indicatrice d'Euler**

$$\varphi(n) = \#\{a \in \{1, 2, \ldots, n\} : \operatorname{pgcd}(a, n) = 1\} = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|.$$

Exemple 4.2.

(i) $\varphi(1) = 1$.

(ii) Si p est premier, $\varphi(p) = p - 1$.

(iii) $\varphi(6) = \#\{1, 5\} = 2$.

(iv) $\varphi(12) = \#\{1, 5, 7, 11\} = 4$.

(v) $\varphi(8) = \#\{1, 3, 5, 7\} = 4$.

Proposition 4.3 (Calcul de φ pour les puissances de premiers)**.** *Si p est premier et $k \geqslant 1$, alors*

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

Démonstration. Parmi les entiers $1, 2, \ldots, p^k$, ceux qui ne sont *pas* premiers avec p^k sont exactement les multiples de p, à savoir $p, 2p, 3p, \ldots, p^{k-1} \cdot p = p^k$. Il y en a p^{k-1}. Donc $\varphi(p^k) = p^k - p^{k-1}$. □

Théorème 4.4 (Multiplicativité de φ)**.** *Si* $\operatorname{pgcd}(m,n) = 1$*, alors* $\varphi(mn) = \varphi(m)\,\varphi(n)$.

Démonstration. Par le théorème des restes chinois (théorème 3.20), l'application

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad \bar{a} \longmapsto (\bar{a}, \bar{a})$$

est un isomorphisme d'anneaux lorsque $\operatorname{pgcd}(m,n) = 1$. En passant aux groupes d'unités, on obtient un isomorphisme $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, d'où $\varphi(mn) = \varphi(m)\,\varphi(n)$. □

Corollaire 4.5 (Formule générale pour $\varphi(n)$)**.** *Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ est la décomposition en facteurs premiers, alors*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = n \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdots \frac{p_r - 1}{p_r}.$$

Démonstration. C'est la combinaison de la proposition 4.3 et du théorème 4.4 :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1) = \prod_{i=1}^{r} p_i^{k_i} \cdot \frac{p_i - 1}{p_i} = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \qquad \square$$

Exemple 4.6.

(i) $\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$

(ii) $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$

(iii) $\varphi(1001) = \varphi(7 \cdot 11 \cdot 13) = 6 \cdot 10 \cdot 12 = 720.$

Proposition 4.7 (Identité de Gauss pour φ)**.** *Pour tout $n \geqslant 1$,*

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

Démonstration. Considérons les fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. Pour chaque diviseur d de n, les fractions qui se simplifient en une fraction irréductible de dénominateur d sont exactement les $\frac{a}{d}$ avec $1 \leqslant a \leqslant d$ et $\operatorname{pgcd}(a,d) = 1$. Il y en a $\varphi(d)$. Puisque chacune des n fractions se simplifie en une unique fraction irréductible dont le dénominateur divise n, on a $\sum_{d \mid n} \varphi(d) = n$. □

4.3 Le théorème d'Euler

Théorème 4.8 (Euler). *Pour tout $n \geqslant 1$ et tout $a \in \mathbb{Z}$ avec* $\operatorname{pgcd}(a, n) = 1$,

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

Démonstration. Soit $(\mathbb{Z}/n\mathbb{Z})^\times = \{u_1, u_2, \ldots, u_{\varphi(n)}\}$ le groupe des unités de $\mathbb{Z}/n\mathbb{Z}$. Puisque $\operatorname{pgcd}(a, n) = 1$, l'élément $\bar{a}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$, et la multiplication par $\bar{a}$ est une bijection de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur lui-même. Donc l'ensemble $\{\bar{a}u_1, \bar{a}u_2, \ldots, \bar{a}u_{\varphi(n)}\}$ est une permutation de $\{u_1, u_2, \ldots, u_{\varphi(n)}\}$.

En prenant le produit de tous ces éléments :

$$(\bar{a}u_1)(\bar{a}u_2)\cdots(\bar{a}u_{\varphi(n)}) = u_1u_2\cdots u_{\varphi(n)}.$$

Le membre de gauche vaut $\bar{a}^{\varphi(n)} \cdot u_1u_2\cdots u_{\varphi(n)}$. En simplifiant par le produit $u_1u_2\cdots u_{\varphi(n)}$ (qui est inversible dans $(\mathbb{Z}/n\mathbb{Z})^\times$), on obtient

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

c'est-à-dire $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Remarque 4.9. Cette preuve est parfois appelée *preuve par permutation*, car elle repose sur le fait que la multiplication par un élément inversible permute les éléments du groupe. C'est essentiellement l'argument utilisé par Euler lui-même.

4.4 Le petit théorème de Fermat

Corollaire 4.10 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ avec $p \nmid a$,*

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

De manière équivalente, pour tout $a \in \mathbb{Z}$,

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

Démonstration. Si $p \nmid a$, alors $\operatorname{pgcd}(a, p) = 1$ et $\varphi(p) = p - 1$. Le théorème d'Euler donne $a^{p-1} \equiv 1 \pmod{p}$, d'où $a^p = a \cdot a^{p-1} \equiv a \pmod{p}$.

Si $p \mid a$, alors $a \equiv 0 \pmod{p}$, et $a^p \equiv 0 \equiv a \pmod{p}$. Ainsi, la seconde formulation vaut pour tout $a \in \mathbb{Z}$. □

Exemple 4.11.

(i) Calculons 2^{340} mod 341. Si 341 était premier, on aurait $2^{340} \equiv 1 \pmod{341}$. On vérifie que $2^{340} \equiv 1 \pmod{341}$ (en effet, cela est vrai). Pourtant, $341 = 11 \times 31$ n'est pas premier ! C'est un *pseudo-premier de Fermat* en base 2.

(ii) Calculons 7^{222} mod 11. Par Fermat, $7^{10} \equiv 1 \pmod{11}$. Or $222 = 10 \times 22 + 2$, donc $7^{222} = (7^{10})^{22} \cdot 7^2 \equiv 1 \cdot 49 \equiv 5 \pmod{11}$.

(iii) Quel est le dernier chiffre de 3^{1000} ? On travaille modulo 10 : $\varphi(10) = 4$, et

$\gcd(3, 10) = 1$, donc $3^4 \equiv 1 \pmod{10}$. Puisque $1000 = 4 \times 250$, on a $3^{1000} \equiv 1 \pmod{10}$. Le dernier chiffre est 1.

4.5 Applications du petit théorème de Fermat

4.5.1 Calcul de grandes puissances modulaires

Le théorème de Fermat (ou d'Euler) permet de réduire l'exposant avant d'appliquer l'exponentiation rapide.

Exemple 4.12. Calculons $3^{10^{100}} \bmod 17$.
Par Fermat, $3^{16} \equiv 1 \pmod{17}$. Il suffit donc de trouver $10^{100} \bmod 16$. On a $\varphi(16) = 8$, et $\gcd(10, 16) = 2 \neq 1$, donc on ne peut pas appliquer Euler directement. Calculons : $10^2 = 100 \equiv 4 \pmod{16}$, $10^3 \equiv 40 \equiv 8 \pmod{16}$, $10^4 \equiv 80 \equiv 0 \pmod{16}$. Donc pour $k \geqslant 4$, $10^k \equiv 0 \pmod{16}$.
Ainsi $10^{100} \equiv 0 \pmod{16}$, et $3^{10^{100}} \equiv 3^0 = 1 \pmod{17}$.

4.5.2 Test de primalité de Fermat

Définition 4.13 (Test de Fermat)**.** Soit $n > 1$ un entier impair. Si l'on trouve a avec $1 < a < n$ et $\gcd(a, n) = 1$ tel que $a^{n-1} \not\equiv 1 \pmod{n}$, alors n est *certainement* composé. On dit que a est un **témoin de Fermat** pour la non-primalité de n.

Remarque 4.14. Le test de Fermat est un test probabiliste : il peut déclarer un nombre composé comme « probablement premier ». Les nombres composés n tels que $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier avec n sont appelés *nombres de Carmichael* (par exemple, $561 = 3 \times 11 \times 17$). Des tests plus puissants, comme le test de Miller–Rabin, surmontent cette limitation.

4.6 Le théorème de Wilson

Théorème 4.15 (Wilson)**.** *Un entier $n \geqslant 2$ est premier si et seulement si*

$$(n-1)! \equiv -1 \pmod{n}.$$

Démonstration. **Sens direct.** Supposons p premier. Nous travaillons dans le corps $\mathbb{Z}/p\mathbb{Z}$. Pour $a \in \{1, 2, \ldots, p-1\}$, l'élément $\bar{a}$ est inversible dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Nous cherchons les éléments qui sont leur propre inverse, c'est-à-dire les solutions de $x^2 \equiv 1 \pmod{p}$, soit $p \mid (x-1)(x+1)$. Puisque p est premier, $p \mid (x-1)$ ou $p \mid (x+1)$, ce qui donne $x \equiv 1$ ou $x \equiv -1 \pmod{p}$.

Ainsi, dans le produit $(p-1)! = 1 \cdot 2 \cdots (p-1)$, les éléments $\bar{1}$ et $\overline{p-1} = \overline{-1}$ sont les seuls à être leur propre inverse. Les $p-3$ autres éléments de $\{2, 3, \ldots, p-2\}$ se regroupent

en $\frac{p-3}{2}$ paires (a, a^{-1}) avec $a \neq a^{-1}$. Le produit de chaque paire vaut 1, donc

$$(p-1)! \equiv 1 \cdot \underbrace{(2 \cdot 2^{-1})(3 \cdot 3^{-1}) \cdots}_{\text{produit}=1} \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

Réciproque. Supposons n composé. Si $n = ab$ avec $1 < a, b < n$ et $a \neq b$, alors a et b apparaissent tous deux comme facteurs dans $(n-1)!$, donc $n = ab \mid (n-1)!$, d'où $(n-1)! \equiv 0 \pmod{n}$, et en particulier $(n-1)! \not\equiv -1 \pmod{n}$.

Le cas $n = p^2$ avec p premier nécessite un argument séparé. Si $p \geqslant 3$, alors p et $2p$ sont deux facteurs distincts dans $\{1, \ldots, p^2 - 1\}$, donc $p^2 \mid (p^2-1)!$. Si $n = 4 = 2^2$, on vérifie directement : $3! = 6 \equiv 2 \not\equiv -1 \pmod{4}$. □

Exemple 4.16.

(i) $4! = 24 \equiv 4 \equiv -1 \pmod{5}$. Confirmé : 5 est premier.

(ii) $6! = 720 \equiv 720 - 102 \times 7 = 720 - 714 = 6 \equiv -1 \pmod{7}$. Confirmé.

(iii) $9! = 362880 \equiv 0 \pmod{10}$. Or $-1 \equiv 9 \pmod{10}$, donc $9! \not\equiv -1 \pmod{10}$. En effet, 10 n'est pas premier.

Remarque 4.17. Le théorème de Wilson est théoriquement élégant mais pratiquement inutilisable comme test de primalité, car le calcul de $(n-1)!$ est de complexité exponentielle en la taille de n.

4.7 Racines primitives

4.7.1 Ordre d'un élément

Définition 4.18 (Ordre multiplicatif)**.** Soit $n \geqslant 1$ et $a \in \mathbb{Z}$ avec $\gcd(a, n) = 1$. L'**ordre multiplicatif** de a modulo n, noté $\mathrm{ord}_n(a)$, est le plus petit entier $d \geqslant 1$ tel que $a^d \equiv 1 \pmod{n}$.

Proposition 4.19 (Propriétés de l'ordre)**.** *Soient $a \in \mathbb{Z}$ avec $\gcd(a, n) = 1$ et $d = \mathrm{ord}_n(a)$.*

(i) $a^k \equiv 1 \pmod{n}$ si et seulement si $d \mid k$.

(ii) En particulier, $d \mid \varphi(n)$.

(iii) Les éléments $a^0, a^1, \ldots, a^{d-1}$ sont distincts modulo n.

Démonstration.

(i) Si $d \mid k$, alors $k = dq$ et $a^k = (a^d)^q \equiv 1 \pmod{n}$. Réciproquement, écrivons $k = dq + r$ avec $0 \leqslant r < d$. Alors $a^r = a^k \cdot (a^d)^{-q} \equiv 1 \pmod{n}$. Par minimalité de d, on a $r = 0$, donc $d \mid k$.

(ii) Par Euler, $a^{\varphi(n)} \equiv 1 \pmod{n}$, donc $d \mid \varphi(n)$ par (i).

(iii) Si $a^i \equiv a^j \pmod{n}$ avec $0 \leqslant i < j < d$, alors $a^{j-i} \equiv 1 \pmod{n}$ avec $0 < j - i < d$, ce qui contredit la minimalité de d. □

4.7.2 Définition et existence des racines primitives

Définition 4.20 (Racine primitive)**.** Un entier g est une **racine primitive modulo** n si $\gcd(g, n) = 1$ et $\mathrm{ord}_n(g) = \varphi(n)$, c'est-à-dire si g engendre le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{g}^0, \bar{g}^1, \ldots, \bar{g}^{\varphi(n)-1}\}.$$

Théorème 4.21 (Existence des racines primitives pour les premiers)**.** *Pour tout nombre premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Autrement dit, il existe une racine primitive modulo p.*

Esquisse de la preuve. Pour chaque diviseur d de $p-1$, notons $\psi(d)$ le nombre d'éléments d'ordre exactement d dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Nous allons montrer que $\psi(d) = \varphi(d)$ pour tout $d \mid (p-1)$, ce qui en particulier donne $\psi(p-1) = \varphi(p-1) \geqslant 1$.

Étape 1. Si $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément a d'ordre d, alors $a, a^2, \ldots, a^d$ sont d racines distinctes du polynôme $X^d - 1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$. Puisqu'un polynôme de degré d sur un corps a au plus d racines, ce sont les *seules* racines. Tout élément d'ordre d est une puissance a^k avec $\gcd(k, d) = 1$, et il y en a $\varphi(d)$. Donc $\psi(d) \in \{0, \varphi(d)\}$.

Étape 2. Chaque élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ a un ordre qui divise $p-1$. Donc $\sum_{d \mid (p-1)} \psi(d) = p-1$. Or, par l'identité de Gauss (proposition 4.7), $\sum_{d \mid (p-1)} \varphi(d) = p-1$. Puisque $\psi(d) \leqslant \varphi(d)$ pour tout d et que les sommes sont égales, on conclut $\psi(d) = \varphi(d)$ pour tout $d \mid (p-1)$.

En particulier, $\psi(p-1) = \varphi(p-1) \geqslant 1$, ce qui prouve l'existence d'une racine primitive modulo p. □

Remarque 4.22 (Existence générale). Plus généralement, des racines primitives existent modulo n si et seulement si $n \in \{1, 2, 4, p^k, 2p^k\}$ où p est un premier impair et $k \geqslant 1$. Nous admettrons ce résultat.

4.7.3 Dénombrement des racines primitives

Corollaire 4.23 (Nombre de racines primitives)**.** *Si p est premier, le nombre de racines primitives modulo p est $\varphi(p-1)$.*

Démonstration. C'est exactement $\psi(p-1) = \varphi(p-1)$ établi dans la preuve ci-dessus. □

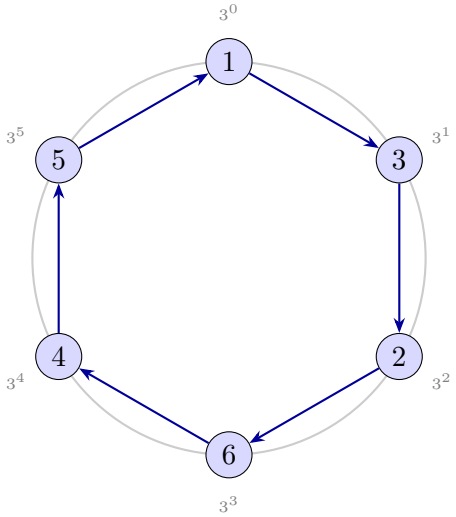
Exemple 4.24. Déterminons les racines primitives modulo 7. On a $\varphi(6) = 2$, donc il y a 2 racines primitives. Les ordres possibles divisent 6 : $\{1, 2, 3, 6\}$.

a	a^1	a^2	a^3	a^4	a^5	a^6
1	1					
2	2	4	1			
3	3	2	6	4	5	1
4	4	2	1			
5	5	4	6	2	3	1
6	6	1				

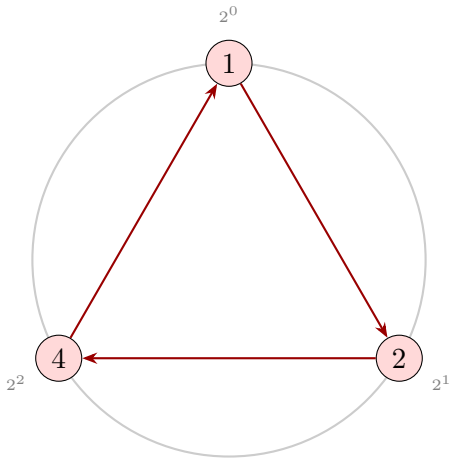
Les ordres sont : $\mathrm{ord}_7(1) = 1$, $\mathrm{ord}_7(2) = 3$, $\mathrm{ord}_7(3) = 6$, $\mathrm{ord}_7(4) = 3$, $\mathrm{ord}_7(5) = 6$, $\mathrm{ord}_7(6) = 2$. Les racines primitives sont 3 et 5.

4.7.4 Visualisation du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$

Puissances de $g = 3$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$



Puissances de $a = 2$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$ (ordre 3)



4.8 Le cryptosystème RSA

Le système RSA, inventé par Rivest, Shamir et Adleman en 1977, est l'un des cryptosystèmes à clé publique les plus utilisés au monde. Sa sécurité repose sur la difficulté de factoriser de grands entiers, et sa correction sur le théorème d'Euler.

4.8.1 Génération des clés

1. Choisir deux grands nombres premiers distincts p et q (typiquement de 1024 bits chacun).
2. Calculer $n = pq$ et $\varphi(n) = (p-1)(q-1)$.

3. Choisir e avec $1 < e < \varphi(n)$ et $\text{pgcd}(e, \varphi(n)) = 1$. Le choix classique est $e = 65537 = 2^{16} + 1$.
4. Calculer $d \equiv e^{-1} \pmod{\varphi(n)}$ (par l'algorithme d'Euclide étendu).
5. La **clé publique** est (n, e). La **clé privée** est (n, d).

4.8.2 Chiffrement et déchiffrement

Définition 4.25 (Chiffrement RSA)**.** Soit $m \in \{0, 1, \ldots, n-1\}$ le message en clair (représenté comme un entier).

— **Chiffrement :** $c \equiv m^e \pmod{n}$.

— **Déchiffrement :** $m \equiv c^d \pmod{n}$.

4.8.3 Preuve de correction

Théorème 4.26 (Correction du RSA)**.** *Avec les notations ci-dessus, pour tout* $m \in \{0, 1, \ldots, n-1\}$,

$$(m^e)^d \equiv m \pmod{n}.$$

Démonstration. Puisque $ed \equiv 1 \pmod{\varphi(n)}$, on a $ed = 1 + k\varphi(n)$ pour un certain $k \in \mathbb{N}$.

Cas 1 : $\text{pgcd}(m, n) = 1$. Par le théorème d'Euler, $m^{\varphi(n)} \equiv 1 \pmod{n}$, d'où

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1^k = m \pmod{n}.$$

Cas 2 : $\text{pgcd}(m, n) > 1$. Puisque $n = pq$ et $m < n$, on a soit $p \mid m$ (mais $q \nmid m$), soit $q \mid m$ (mais $p \nmid m$). Traitons le premier cas (l'autre est symétrique).

Si $p \mid m$, alors $m^{ed} \equiv 0 \equiv m \pmod{p}$. D'autre part, $\text{pgcd}(m, q) = 1$, et $\varphi(n) = (p-1)(q-1)$, donc $(q-1) \mid \varphi(n)$. Par Fermat, $m^{q-1} \equiv 1 \pmod{q}$, d'où

$$m^{ed} = m \cdot (m^{\varphi(n)})^k = m \cdot ((m^{q-1})^{(p-1)})^k \equiv m \cdot 1 = m \pmod{q}.$$

Puisque $p \mid (m^{ed} - m)$ et $q \mid (m^{ed} - m)$, et que $\text{pgcd}(p, q) = 1$, on conclut $pq = n \mid (m^{ed} - m)$. □

4.8.4 Exemple numérique complet

Exemple 4.27. Prenons $p = 61$ et $q = 53$.

1. $n = 61 \times 53 = 3233$ et $\varphi(n) = 60 \times 52 = 3120$.
2. Choisissons $e = 17$. Vérifions : $\text{pgcd}(17, 3120) = 1$. ✓
3. Calculons $d \equiv 17^{-1} \pmod{3120}$. Par l'algorithme d'Euclide étendu : $17 \times 2753 = 46801 = 15 \times 3120 + 1$, donc $d = 2753$.
4. Clé publique : $(3233, 17)$. Clé privée : $(3233, 2753)$.
5. Chiffrement de $m = 65$: $c = 65^{17} \bmod 3233$.

Par exponentiation rapide : $17 = (10001)_2$.

$65^1 \equiv 65 \pmod{3233}$
$65^2 \equiv 4225 \equiv 992 \pmod{3233}$
$65^4 \equiv 992^2 = 984064 \equiv 984064 - 304 \times 3233 = 1 + 2432 \equiv 2433 \pmod{3233}$
$65^8 \equiv 2433^2 = 5919489 \equiv 5919489 - 1831 \times 3233 = 5919489 - 5921723 \ldots$

En poursuivant le calcul (ou par ordinateur), on trouve $c = 2790$.

6. Déchiffrement : $m = 2790^{2753} \bmod 3233 = 65$. ✓

4.8.5 Considérations pratiques

Remarque 4.28. En pratique, le RSA nécessite :

— Des nombres premiers de grande taille (au moins 2048 bits pour n, soit environ 617 chiffres décimaux) pour résister aux algorithmes de factorisation connus.

— La génération de grands nombres premiers, réalisée en pratique par des tests de primalité probabilistes (Miller–Rabin).

— Un *padding* cryptographique (par exemple OAEP) pour éviter certaines attaques.

— La destruction sécurisée de p, q et $\varphi(n)$ après la génération des clés.

4.9 L'échange de clés de Diffie–Hellman

Le protocole de Diffie–Hellman (1976) permet à deux parties, Alice et Bob, d'établir un secret partagé sur un canal non sécurisé.

1. Alice et Bob choisissent publiquement un grand premier p et une racine primitive g modulo p.
2. Alice choisit un secret $a \in \{2, \ldots, p-2\}$ et envoie $A = g^a \bmod p$ à Bob.
3. Bob choisit un secret $b \in \{2, \ldots, p-2\}$ et envoie $B = g^b \bmod p$ à Alice.
4. Alice calcule $s = B^a \bmod p = g^{ab} \bmod p$.
5. Bob calcule $s = A^b \bmod p = g^{ab} \bmod p$.

Les deux parties partagent maintenant le secret $s = g^{ab} \bmod p$. Un espion qui observe g, p, $A = g^a \bmod p$ et $B = g^b \bmod p$ devrait résoudre le problème du logarithme discret pour retrouver a ou b, ce qui est supposé calculatoirement difficile.

Exemple 4.29. Avec $p = 23$ et $g = 5$ (racine primitive modulo 23) :

— Alice choisit $a = 6$, envoie $A = 5^6 \bmod 23 = 15625 \bmod 23 = 8$.

— Bob choisit $b = 15$, envoie $B = 5^{15} \bmod 23 = 19$.

— Alice calcule $s = 19^6 \bmod 23 = 2$.

— Bob calcule $s = 8^{15} \bmod 23 = 2$.

— Le secret partagé est $s = 2$.

4.10 Exercices

Exercice 4.1 ($\star$)**.** Calculer $\varphi(n)$ pour $n = 36, 72, 100, 250, 360$.

Exercice 4.2 ($\star$)**.** En utilisant le petit théorème de Fermat, calculer $2^{1000} \bmod 13$.

Exercice 4.3 ($\star$)**.** Déterminer le dernier chiffre de 7^{9999}.

Exercice 4.4 ($\star$)**.** Vérifier le théorème de Wilson pour $p = 11$ en calculant $10! \bmod 11$.

Exercice 4.5 ($\star\star$)**.** Trouver toutes les racines primitives modulo 11.

Exercice 4.6 ($\star\star$)**.** En utilisant le théorème d'Euler, calculer $3^{340} \bmod 341$. En déduire que 341 n'est pas nécessairement premier.

Exercice 4.7 ($\star\star$)**.** Soit p premier. Montrer que si g est une racine primitive modulo p, alors g^k est aussi une racine primitive si et seulement si $\gcd(k, p-1) = 1$.

Exercice 4.8 ($\star\star$)**.** Montrer que pour tout premier $p \geqslant 5$, on a $1^{p-2} + 2^{p-2} + \cdots + (p-1)^{p-2} \equiv 0 \pmod{p}$.

Indication : utiliser le petit théorème de Fermat et la somme des inverses dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 4.9 ($\star\star$)**.** Montrer que $\varphi(n)$ est pair pour tout $n \geqslant 3$.

Exercice 4.10 ($\star\star\star$)**.** Alice utilise RSA avec $n = 2537$, $e = 13$. Elle reçoit le message chiffré $c = 2081$. Factoriser n, calculer d et déchiffrer le message.

Indication : $2537 = 43 \times 59$.

Exercice 4.11 ($\star\star\star$)**.** En utilisant le théorème de Wilson, montrer que pour tout premier $p \equiv 1 \pmod 4$, l'entier $\left(\frac{p-1}{2}\right)!$ satisfait $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$.

Indication : dans le produit $(p-1)! = 1 \cdot 2 \cdots (p-1)$, apparier chaque $k > \frac{p-1}{2}$ avec $p - k$.

Exercice 4.12 ($\star\star\star$)**.** Soit p un premier impair et g une racine primitive modulo p. Montrer que $g^{(p-1)/2} \equiv -1 \pmod{p}$.

Exercice 4.13 ($\star\star\star$)**.** Montrer que $561 = 3 \times 11 \times 17$ est un nombre de Carmichael, c'est-à-dire que $a^{560} \equiv 1 \pmod{561}$ pour tout a avec $\gcd(a, 561) = 1$.

Indication : vérifier que 560 est divisible par $\varphi(3) = 2$, $\varphi(11) = 10$ et $\varphi(17) = 16$, puis appliquer Fermat modulo chaque facteur premier et conclure par le CRT.

Résumé du chapitre

1. La fonction indicatrice d'Euler $\varphi(n)$ compte les entiers de $\{1, \ldots, n\}$ premiers avec n. Elle est multiplicative et se calcule par $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$.
2. **Théorème d'Euler :** si $\gcd(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.
3. **Petit théorème de Fermat :** si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.
4. **Théorème de Wilson :** n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.
5. Une **racine primitive** modulo n est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique pour tout premier p, et possède $\varphi(p-1)$ racines primitives.
6. Le **cryptosystème RSA** repose sur le théorème d'Euler : on chiffre par $c = m^e \bmod n$ et on déchiffre par $m = c^d \bmod n$, où $ed \equiv 1 \pmod{\varphi(n)}$.
7. L'**échange de Diffie–Hellman** permet d'établir un secret partagé en exploitant la difficulté du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Chapitre 5

Restes Chinois et Applications

Perspective historique

Le *théorème des restes chinois* constitue l'un des résultats les plus anciens de la théorie des nombres. Sa première formulation connue remonte au traité *Sunzi Suanjing* (« Manuel de calcul du Maître Sun »), rédigé entre le III^{e} et le V^{e} siècle de notre ère. Le problème fondateur est le suivant :

> *« Un nombre donne un reste de* 2 *quand on le divise par* 3*, un reste de* 3 *quand on le divise par* 5*, et un reste de* 2 *quand on le divise par* 7*. Quel est ce nombre ? »*

Au XIII^{e} siècle, le mathématicien chinois **Qin Jiushao** (1202–1261) formula une méthode algorithmique générale dans son ouvrage *Shushu Jiuzhang* (1247), anticipant de plusieurs siècles les travaux européens. En Occident, le résultat fut redécouvert et généralisé par Euler, puis placé dans un cadre algébrique par Gauss dans ses *Disquisitiones Arithmeticae* (1801).

Dans ce chapitre, nous énonçons et démontrons le théorème des restes chinois sous sa forme classique et algébrique, puis nous en présentons de nombreuses applications, allant du calcul calendaire à la cryptographie RSA.

5.1 Systèmes de congruences simultanées

Définition 5.1 (Système de congruences)**.** Un *système de congruences simultanées* est un ensemble d'équations de la forme

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

où les $a_i \in \mathbb{Z}$ sont les *restes* prescrits et les $m_i \geq 2$ sont les *modules*.

Remarque 5.2. Sans hypothèse supplémentaire sur les modules, un tel système peut n'avoir aucune solution. Par exemple, le système $x \equiv 0 \pmod 2$, $x \equiv 1 \pmod 4$ est incompatible, car la première congruence impose que x est pair, tandis que la seconde impose $x \equiv 1 \pmod 4$, donc x impair.

5.2 Le théorème des restes chinois

Théorème 5.3 (Théorème des restes chinois — CRT)**.** *Soient $m_1, m_2, \ldots, m_k$ des entiers ≥ 2 deux à deux premiers entre eux, c'est-à-dire* $\gcd(m_i, m_j) = 1$ *pour tout $i \neq j$. Posons $M = m_1 m_2 \cdots m_k$. Alors, pour tout choix d'entiers $a_1, a_2, \ldots, a_k$, le système*

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

admet une solution, et cette solution est unique modulo M*. Autrement dit, l'ensemble des solutions est exactement une classe de congruence modulo M.*

Démonstration. La preuve procède en deux étapes : construction d'une solution, puis unicité.

Existence (construction explicite). Pour chaque $i \in \{1, \ldots, k\}$, posons

$$M_i = \frac{M}{m_i} = \prod_{j \neq i} m_j.$$

Par hypothèse, $\gcd(M_i, m_i) = 1$ puisque m_i est premier avec chacun des m_j ($j \neq i$), donc premier avec leur produit. Il existe donc, par le théorème de Bézout, un entier N_i tel que

$$M_i N_i \equiv 1 \pmod{m_i}.$$

L'entier N_i est l'inverse de M_i modulo m_i, calculable par l'algorithme d'Euclide étendu.

Posons alors

$$x_0 = \sum_{i=1}^{k} a_i M_i N_i. \tag{5.1}$$

Vérifions que x_0 résout le système. Fixons un indice j. Pour $i \neq j$, le terme $a_i M_i N_i$ est divisible par m_j (car M_i contient le facteur m_j). Ainsi

$$x_0 \equiv a_j M_j N_j \pmod{m_j}.$$

Or $M_j N_j \equiv 1 \pmod{m_j}$ par construction, donc $x_0 \equiv a_j \pmod{m_j}$.

Unicité. Supposons que x_0 et x_1 soient deux solutions. Pour tout i, on a $x_0 \equiv x_1 \pmod{m_i}$, donc $m_i \mid (x_0 - x_1)$. Comme les m_i sont deux à deux premiers entre eux, leur produit $M = m_1 \cdots m_k$ divise aussi $x_0 - x_1$. Ainsi $x_0 \equiv x_1 \pmod M$. □

Remarque 5.4. La formule (5.1) fournit un algorithme effectif :

(i) Calculer $M = m_1 \cdots m_k$ et les quotients partiels $M_i = M/m_i$.

(ii) Pour chaque i, déterminer $N_i \equiv M_i^{-1} \pmod{m_i}$ par l'algorithme d'Euclide étendu.

(iii) Former la somme $x_0 = \sum a_i M_i N_i$ et la réduire modulo M.

5.3 Exemples détaillés

Exemple 5.5 (Problème de Sun Tzu)**.** Résolvons le système

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7.$$

Les modules $3, 5, 7$ sont deux à deux premiers entre eux, et $M = 105$.

— $M_1 = 105/3 = 35$. On cherche N_1 tel que $35N_1 \equiv 1 \pmod 3$. Or $35 \equiv 2 \pmod 3$ et $2 \cdot 2 = 4 \equiv 1 \pmod 3$, donc $N_1 = 2$.

— $M_2 = 105/5 = 21$. On cherche N_2 tel que $21N_2 \equiv 1 \pmod 5$. Or $21 \equiv 1 \pmod 5$, donc $N_2 = 1$.

— $M_3 = 105/7 = 15$. On cherche N_3 tel que $15N_3 \equiv 1 \pmod 7$. Or $15 \equiv 1 \pmod 7$, donc $N_3 = 1$.

Ainsi,

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}.$$

Vérification : $23 = 7 \cdot 3 + 2$, $23 = 4 \cdot 5 + 3$, $23 = 3 \cdot 7 + 2$. ✓

Exemple 5.6 (Système à quatre modules)**.** Résolvons

$$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod 7.$$

Ici $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

— $M_1 = 105$, $105 \equiv 1 \pmod 2$, $N_1 = 1$. Contribution : $1 \cdot 105 \cdot 1 = 105$.

— $M_2 = 70$, $70 \equiv 1 \pmod 3$, $N_2 = 1$. Contribution : $2 \cdot 70 \cdot 1 = 140$.

— $M_3 = 42$, $42 \equiv 2 \pmod 5$, $2 \cdot 3 = 6 \equiv 1 \pmod 5$, $N_3 = 3$. Contribution : $3 \cdot 42 \cdot 3 = 378$.

— $M_4 = 30$, $30 \equiv 2 \pmod 7$, $2 \cdot 4 = 8 \equiv 1 \pmod 7$, $N_4 = 4$. Contribution : $4 \cdot 30 \cdot 4 = 480$.

Total : $x_0 = 105 + 140 + 378 + 480 = 1103 \equiv 53 \pmod{210}$.
Vérification : $53 = 26 \cdot 2 + 1$, $53 = 17 \cdot 3 + 2$, $53 = 10 \cdot 5 + 3$, $53 = 7 \cdot 7 + 4$. ✓

5.4 Interprétation algébrique

Le théorème des restes chinois admet une reformulation élégante en termes d'isomorphisme d'anneaux.

Théorème 5.7 (Forme algébrique du CRT). *Soient $m, n \geq 2$ des entiers tels que* $\operatorname{pgcd}(m,n) = 1$. *L'application*

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad \overline{x} \longmapsto (\overline{x}_m, \overline{x}_n)$$

(où $\overline{x}_m$ désigne la classe de x modulo m) est un isomorphisme d'anneaux.

Démonstration. L'application Φ est clairement un morphisme d'anneaux (elle préserve l'addition et la multiplication). Son noyau est

$$\ker \Phi = \{\overline{x} \in \mathbb{Z}/mn\mathbb{Z} : m \mid x \text{ et } n \mid x\} = \{\overline{x} \in \mathbb{Z}/mn\mathbb{Z} : mn \mid x\} = \{\overline{0}\},$$

la dernière égalité résultant de $\operatorname{pgcd}(m,n) = 1$. Ainsi Φ est injectif. Comme les deux ensembles ont le même cardinal mn, l'application Φ est bijective, donc un isomorphisme. □

Corollaire 5.8 (Forme générale). *Si $m_1, \ldots, m_k$ sont deux à deux premiers entre eux et $M = m_1 \cdots m_k$, alors*

$$\mathbb{Z}/M\mathbb{Z} \;\simeq\; \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

en tant qu'anneaux.

La figure 5.1 illustre l'isomorphisme du CRT pour $m = 3$, $n = 5$.

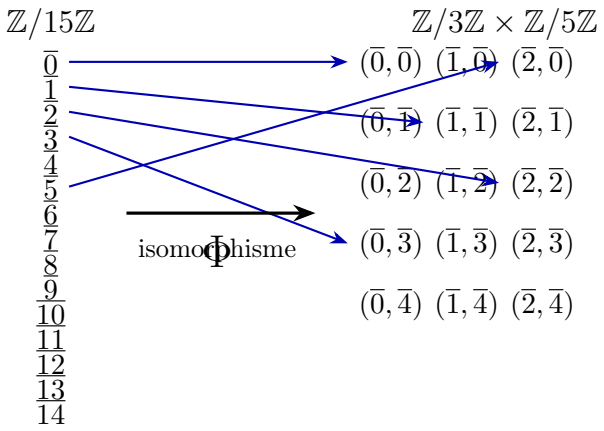


FIGURE 5.1 – Isomorphisme du CRT : $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Quelques correspondances sont indiquées.

5.5 Conséquences pour la fonction d'Euler

Corollaire 5.9 (Multiplicativité de φ). *Si* $\operatorname{pgcd}(m,n) = 1$, *alors* $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Démonstration. Par le théorème 5.7, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Cet isomorphisme envoie les éléments inversibles sur les éléments inversibles :

$$(\mathbb{Z}/mn\mathbb{Z})^\times \;\simeq\; (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

En effet, un couple (a, b) est inversible dans le produit si et seulement si a est inversible dans $\mathbb{Z}/m\mathbb{Z}$ et b est inversible dans $\mathbb{Z}/n\mathbb{Z}$. En prenant les cardinaux :

$$\varphi(mn) = \left|(\mathbb{Z}/mn\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| \cdot \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(m) \cdot \varphi(n). \qquad \square$$

Corollaire 5.10 (Formule d'Euler revisitée)**.** *Pour tout $n \geq 2$ ayant la décomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$,*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Démonstration. Par la multiplicativité (Corollaire 5.9), $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i})$. Or $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$ pour tout premier p et $k \geq 1$. Le résultat suit. $\square$

5.6 Applications

5.6.1 Calcul calendaire

Exemple 5.11 (Jour de la semaine)**.** Supposons que nous sachions qu'un événement a lieu un nombre de jours x après un lundi de référence, avec les contraintes :

$$x \equiv 3 \pmod 7 \quad \text{(c'est un jeudi)}, \qquad x \equiv 0 \pmod 4 \quad \text{(multiple de 4 jours)}.$$

Comme $\text{pgcd}(7, 4) = 1$, le CRT donne une solution unique modulo 28. On a $M_1 = 4$, $N_1 \equiv 4^{-1} \equiv 2 \pmod 7$ (car $4 \cdot 2 = 8 \equiv 1$), et $M_2 = 7$, $N_2 \equiv 7^{-1} \equiv 3 \pmod 4$ (car $7 \cdot 3 = 21 \equiv 1$). Donc $x_0 = 3 \cdot 4 \cdot 2 + 0 \cdot 7 \cdot 3 = 24 \equiv 24 \pmod{28}$. Le 24^{e} jour après le lundi tombe bien un jeudi, et c'est un multiple de 4.

5.6.2 Partage de secret

Exemple 5.12 (Partage de secret par le CRT)**.** Un secret $s = 47$ est encodé modulo des nombres premiers entre eux $m_1 = 11$ et $m_2 = 13$. On distribue :

— À la personne A : le reste $r_1 = 47 \bmod 11 = 3$.

— À la personne B : le reste $r_2 = 47 \bmod 13 = 8$.

Aucune des deux personnes ne peut reconstituer s seule, car il existe 13 (resp. 11) solutions possibles modulo 143. En revanche, la combinaison des deux parts permet de retrouver s par le CRT :

$$x \equiv 3 \pmod{11}, \quad x \equiv 8 \pmod{13} \implies x \equiv 47 \pmod{143}.$$

5.6.3 Codes détecteurs d'erreurs

Exemple 5.13 (Codage par résidus)**.** Un système de *codage par résidus* (Residue Number System, RNS) représente un entier $x \in \{0, 1, \ldots, M-1\}$ par le k-uplet $(x \bmod m_1, \ldots, x \bmod m_k)$ où les m_i sont deux à deux premiers entre eux et $M = m_1 \cdots m_k$. Pour détecter des erreurs, on ajoute un module redondant m_{k+1} premier

avec les précédents. Si le vecteur reçu ne correspond à aucun $x < M$ via le CRT, une erreur est détectée.

5.6.4 Accélération CRT de RSA

Proposition 5.14 (Déchiffrement RSA par le CRT)**.** *Soit (n, d) la clé privée RSA avec $n = pq$. Pour déchiffrer un message c, au lieu de calculer $c^d \bmod n$ directement, on peut :*

(i) Calculer $d_p = d \bmod (p-1)$ et $d_q = d \bmod (q-1)$.

(ii) Calculer $m_p = c^{d_p} \bmod p$ et $m_q = c^{d_q} \bmod q$.

(iii) Reconstituer $m = c^d \bmod n$ par le CRT à partir de m_p et m_q.

Cette méthode est environ quatre fois plus rapide *que l'exponentiation directe modulo n, car les exponentiations se font modulo des nombres de taille moitié.*

Démonstration. Par le petit théorème de Fermat, pour tout a non divisible par p : $a^{p-1} \equiv 1 \pmod p$. Écrivons $d = q_p(p-1) + d_p$. Alors

$$c^d = c^{q_p(p-1)+d_p} = (c^{p-1})^{q_p} \cdot c^{d_p} \equiv c^{d_p} \pmod p.$$

De même $c^d \equiv c^{d_q} \pmod q$. Le CRT reconstitue alors $c^d \bmod n$ à partir de ces deux résidus.

Pour le gain de vitesse, une exponentiation modulaire modulo un nombre de b bits coûte $O(b^3)$ opérations binaires (par élévation au carré itérée avec multiplications de nombres de b bits). Modulo p ou q de taille $b/2$, chaque exponentiation coûte $O((b/2)^3) = O(b^3/8)$. Deux telles exponentiations coûtent $O(b^3/4)$, soit un facteur 4 de gain. □

5.7 Exercices

Exercice 5.1 ($\star$)**.** Résoudre le système $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 3 \pmod{11}$.

Exercice 5.2 ($\star$)**.** Trouver le plus petit entier positif x tel que $x \equiv 3 \pmod 4$, $x \equiv 5 \pmod 9$, $x \equiv 7 \pmod{11}$.

Exercice 5.3 ($\star$)**.** Montrer que si $\gcd(m, n) = 1$, alors le système $x \equiv a \pmod m$, $x \equiv b \pmod n$ a exactement une solution modulo mn, directement à partir de Bézout (sans invoquer le CRT).

Exercice 5.4 ($\star\star$)**.** Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. En utilisant le CRT, montrer que $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$, et en déduire la formule $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$.

Exercice 5.5 ($\star\star$)**.** Soit $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ l'isomorphisme du CRT avec $\gcd(m, n) = 1$. Déterminer explicitement $f^{-1}(1, 0)$ et $f^{-1}(0, 1)$. Montrer que ces deux éléments sont des idempotents orthogonaux dans $\mathbb{Z}/mn\mathbb{Z}$.

Exercice 5.6 ($\star\star$)**.** Montrer que si $\gcd(m, n) = d > 1$, le système $x \equiv a \pmod m$, $x \equiv b \pmod n$ a une solution si et seulement si $a \equiv b \pmod d$, et que dans ce cas la solution est unique modulo $\operatorname{ppcm}(m, n)$.

Exercice 5.7 ($\star\star\star$)**.** On dit que n est un *nombre de Carmichael* si n est composé et $a^{n-1} \equiv 1 \pmod{n}$ pour tout a avec $\text{pgcd}(a, n) = 1$. En utilisant le CRT, montrer le *critère de Korselt* : n est un nombre de Carmichael si et seulement si n est sans facteur carré et, pour tout premier p divisant n, on a $(p-1) \mid (n-1)$.

Exercice 5.8 ($\star\star\star$)**.** Soit p un nombre premier impair et a un entier non divisible par p. En utilisant le CRT avec les modules p et $p-1$, montrer qu'il existe un entier x tel que $x^x \equiv a \pmod{p}$. *Indication : chercher x tel que $x \equiv g^k \pmod{p}$ et $x \equiv k \pmod{p-1}$ pour un choix convenable de k.*

Résumé du chapitre

- Le **théorème des restes chinois** affirme que si les modules $m_1, \ldots, m_k$ sont deux à deux premiers entre eux, un système de congruences simultanées admet une unique solution modulo $M = m_1 \cdots m_k$.
- La solution se construit explicitement via la formule $x_0 = \sum a_i M_i N_i$ où $M_i = M/m_i$ et $N_i \equiv M_i^{-1} \pmod{m_i}$.
- **Forme algébrique** : $\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$.
- La **multiplicativité** de la fonction d'Euler φ est une conséquence directe du CRT.
- Les **applications** incluent le calcul calendaire, le partage de secret, les codes par résidus et l'accélération RSA.

Chapitre 6

Résidus Quadratiques et Réciprocité Quadratique

Perspective historique

La question de savoir quand une congruence $x^2 \equiv a \pmod{p}$ admet une solution est l'un des problèmes centraux de la théorie des nombres. **Leonhard Euler** (1707–1783) étudia le premier cette question de manière systématique et découvrit le critère qui porte son nom. **Adrien-Marie Legendre** (1752–1833) introduisit le symbole $\left(\frac{a}{p}\right)$ et formula la loi de réciprocité quadratique, mais sa « preuve » comportait une lacune.

C'est **Carl Friedrich Gauss** (1777–1855) qui donna la première démonstration complète en 1796, à l'âge de dix-huit ans. Gauss qualifia ce résultat de *theorema aureum* (« théorème d'or ») et en donna pas moins de *huit démonstrations différentes* au cours de sa vie, témoignant de la richesse du sujet. La preuve que nous présenterons utilise le lemme de Gauss et le comptage de points du réseau, dans l'esprit de la démonstration d'Eisenstein.

6.1 Résidus quadratiques modulo un premier

Dans tout ce chapitre, p désigne un nombre premier *impair* (sauf mention contraire).

Définition 6.1 (Résidu quadratique)**.** Soit $a \in \mathbb{Z}$ avec $p \nmid a$. On dit que a est un *résidu quadratique* modulo p (noté QR) s'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod{p}$. Sinon, on dit que a est un *non-résidu quadratique* (noté QNR).

Proposition 6.2 (Dénombrement des QR)**.** *Parmi les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$, il y a exactement $\frac{p-1}{2}$ résidus quadratiques et $\frac{p-1}{2}$ non-résidus quadratiques.*

Démonstration. Considérons l'application $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ définie par $\sigma(\overline{x}) = \overline{x}^2$. Son image est exactement l'ensemble des QR. Montrons que σ est deux-pour-un : si $x^2 \equiv y^2 \pmod{p}$, alors $p \mid (x-y)(x+y)$, donc $x \equiv y$ ou $x \equiv -y \pmod{p}$. Comme p est impair, $x \not\equiv -x \pmod{p}$ pour $x \not\equiv 0$, donc chaque QR a exactement deux antécédents. Il y a donc $\frac{p-1}{2}$ résidus quadratiques et $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ non-résidus. $\square$

Exemple 6.3. Pour $p = 13$, les carrés modulo 13 sont :

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 3, \quad 5^2 \equiv 12, \quad 6^2 \equiv 10.$$

Les QR modulo 13 sont donc $\{1, 3, 4, 9, 10, 12\}$, et les QNR sont $\{2, 5, 6, 7, 8, 11\}$. On a bien 6 éléments dans chaque catégorie.

6.2 Critère d'Euler

Théorème 6.4 (Critère d'Euler)**.** *Soit p un premier impair et $a \in \mathbb{Z}$ avec $p \nmid a$. Alors*

$$a^{(p-1)/2} \equiv \begin{cases} +1 \pmod p & \text{si } a \text{ est un QR modulo } p, \\ -1 \pmod p & \text{si } a \text{ est un QNR modulo } p. \end{cases}$$

Démonstration. Par le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod p$, c'est-à-dire $p \mid (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$. Comme p est premier, $a^{(p-1)/2} \equiv 1$ ou $a^{(p-1)/2} \equiv -1 \pmod p$.

Cas QR. Supposons $a \equiv x^2 \pmod p$. Alors

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

par le petit théorème de Fermat.

Cas QNR. Le polynôme $X^{(p-1)/2} - 1$ a au plus $(p-1)/2$ racines dans $\mathbb{Z}/p\mathbb{Z}$ (corps). Or les $(p-1)/2$ résidus quadratiques sont des racines (par le cas précédent). Donc les $(p-1)/2$ non-résidus ne sont *pas* racines de ce polynôme, et vérifient nécessairement $a^{(p-1)/2} \equiv -1 \pmod p$. □

Exemple 6.5. Vérifions que 5 est un QNR modulo 13 : $5^6 = 15625$. Or $15625 = 1201 \cdot 13 + 12$, donc $5^6 \equiv 12 \equiv -1 \pmod{13}$. ✓
En pratique, on calcule par élévation au carré : $5^2 = 25 \equiv 12$, $5^4 \equiv 12^2 = 144 \equiv 1$, $5^6 \equiv 5^4 \cdot 5^2 \equiv 1 \cdot 12 \equiv -1$. ✓

6.3 Le symbole de Legendre

Définition 6.6 (Symbole de Legendre)**.** Pour p premier impair et $a \in \mathbb{Z}$, le *symbole de Legendre* est

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ +1 & \text{si } a \text{ est un QR modulo } p, \\ -1 & \text{si } a \text{ est un QNR modulo } p. \end{cases}$$

Le critère d'Euler se réécrit alors de manière concise.

Corollaire 6.7. *Pour tout $a \in \mathbb{Z}$ et tout premier impair p avec $p \nmid a$:*

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

Proposition 6.8 (Propriétés du symbole de Legendre)**.** *Soient p un premier impair et $a, b \in \mathbb{Z}$.*

(i) ***Périodicité*** *: $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$.*

(ii) ***Multiplicativité*** *: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.*

(iii) ***Carrés*** *: $\left(\frac{a^2}{p}\right) = 1$ si $p \nmid a$.*

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

Démonstration. (i) Immédiat car le symbole ne dépend que de la classe de a modulo p.

(ii) Par le critère d'Euler, $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}$. Comme les deux membres sont dans $\{-1, 0, 1\}$ et $p \geq 3$, la congruence est une égalité.

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

(iv) $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$, et comme $(-1)^{(p-1)/2} \in \{-1, 1\}$ et $p \geq 3$, c'est une égalité. Concrètement : -1 est QR modulo p si et seulement si $p \equiv 1 \pmod{4}$. □

Exemple 6.9. Calculons $\left(\frac{-3}{13}\right)$. Par multiplicativité : $\left(\frac{-3}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{3}{13}\right)$.
$\left(\frac{-1}{13}\right) = (-1)^6 = 1$ car $13 \equiv 1 \pmod{4}$.
Pour $\left(\frac{3}{13}\right)$: $3^6 = 729$, $729 = 56 \cdot 13 + 1$, donc $\left(\frac{3}{13}\right) = 1$.
Ainsi $\left(\frac{-3}{13}\right) = 1 \cdot 1 = 1$, et $-3 \equiv 10$ est bien un QR modulo 13 (on vérifie : $6^2 = 36 \equiv 10 \pmod{13}$). ✓

6.4 Le lemme de Gauss

Notation 6.10. Pour p premier impair, on note $S = \{1, 2, \ldots, (p-1)/2\}$ l'ensemble des *représentants positifs* des classes non nulles modulo p.

Lemme 6.11 (Lemme de Gauss)**.** *Soient p un premier impair et $a \in \mathbb{Z}$ avec $p \nmid a$. Pour chaque $s \in S$, réduisons $as \bmod p$ dans l'intervalle $\{1, \ldots, p-1\}$ et écrivons le résultat sous la forme $\varepsilon_s \cdot r_s$ avec $r_s \in S$ et $\varepsilon_s \in \{+1, -1\}$ (c'est-à-dire $r_s = as \bmod p$ si $as \bmod p \leq (p-1)/2$, et $r_s = p - (as \bmod p)$ sinon). Alors :*

(a) Les r_s pour $s \in S$ forment une permutation de S.

(b) $\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s = (-1)^\nu$, où ν est le nombre d'éléments $s \in S$ tels que le résidu $as \bmod p$ tombe dans $\{(p+1)/2, \ldots, p-1\}$.

Démonstration. **(a)** Montrons que les r_s sont deux à deux distincts. Supposons $r_s = r_t$ avec $s \neq t$. Cela signifie que $as \equiv \pm at \pmod p$. Si $as \equiv at$, alors $s \equiv t$ (car $\gcd(a,p)=1$), contradiction. Si $as \equiv -at$, alors $a(s+t) \equiv 0$, donc $p \mid (s+t)$. Mais $2 \leq s+t \leq p-1$, contradiction. Ainsi les $(p-1)/2$ valeurs r_s sont distinctes et appartiennent à S (qui a $(p-1)/2$ éléments), donc elles forment une permutation de S.

(b) Par construction, $as \equiv \varepsilon_s \cdot r_s \pmod p$ pour chaque $s \in S$. En prenant le produit sur tous les $s \in S$:

$$\prod_{s\in S}(as) \equiv \prod_{s\in S}(\varepsilon_s \cdot r_s) \pmod p.$$

Le membre de gauche vaut $a^{(p-1)/2}\prod_{s\in S} s$. Le membre de droite vaut $(\prod \varepsilon_s)\cdot\prod_{s\in S} r_s$. Par (a), $\prod r_s = \prod s$, et ce produit est non nul modulo p. En simplifiant :

$$a^{(p-1)/2} \equiv \prod_{s\in S}\varepsilon_s = (-1)^{\nu} \pmod p.$$

Par le critère d'Euler, $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$, d'où le résultat. □

Exemple 6.12 (Application du lemme de Gauss)**.** Calculons $\left(\frac{5}{11}\right)$. Ici $p=11$, $S=\{1,2,3,4,5\}$.

s	1	2	3	4	5
$5s \bmod 11$	5	10	4	9	3
r_s	5	1	4	2	3
ε_s	$+1$	-1	$+1$	-1	$+1$

Le nombre ν de signes négatifs est $\nu = 2$, donc $\left(\frac{5}{11}\right) = (-1)^2 = +1$. Ainsi 5 est un QR modulo 11.
Vérification : $4^2 = 16 \equiv 5 \pmod{11}$. ✓

6.5 Premier supplément : $\left(\frac{-1}{p}\right)$

Théorème 6.13 (Premier supplément)**.** *Pour tout premier impair p :*

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

Démonstration. C'est la propriété (iv) de la Proposition 6.8, conséquence immédiate du critère d'Euler. □

Corollaire 6.14. *Un premier impair p est somme de deux carrés ($p = a^2 + b^2$) seulement si $p \equiv 1 \pmod 4$.*

Démonstration. Si $p = a^2 + b^2$ avec p impair, alors $a^2 + b^2 \equiv 0 \pmod p$, et $b \not\equiv 0$, donc $a^2 \equiv -b^2$, d'où $(ab^{-1})^2 \equiv -1 \pmod p$. Ainsi -1 est un QR, ce qui impose $p \equiv 1 \pmod 4$. □

6.6 Second supplément : $\left(\frac{2}{p}\right)$

Théorème 6.15 (Second supplément). *Pour tout premier impair p :*

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

Démonstration. Appliquons le lemme de Gauss avec $a = 2$. Pour $s \in S = \{1, \dots, (p-1)/2\}$, le produit $2s$ modulo p est simplement $2s$ si $2s \leq p-1$ (c'est-à-dire $s \leq (p-1)/2$, toujours vrai), mais il faut déterminer si $2s$ tombe dans $\{1, \dots, (p-1)/2\}$ ou dans $\{(p+1)/2, \dots, p-1\}$. On a $\varepsilon_s = -1$ si et seulement si $2s > (p-1)/2$, c'est-à-dire $s > (p-1)/4$. Donc

$$\nu = \left|\left\{s \in \{1, \dots, \tfrac{p-1}{2}\} : s > \tfrac{p-1}{4}\right\}\right| = \tfrac{p-1}{2} - \left\lfloor \tfrac{p-1}{4} \right\rfloor.$$

Un calcul par cas selon $p \bmod 8$ montre que $\nu \equiv (p^2-1)/8 \pmod 2$:

- $p = 8k+1$: $\nu = 4k - 2k = 2k$, $(p^2-1)/8 = 8k^2 + 2k$, parité identique.
- $p = 8k+3$: $\nu = 4k + 1 - (2k) = 2k+1$, $(p^2-1)/8 = 8k^2 + 6k + 1$, parité identique.
- $p = 8k+5$: $\nu = 4k + 2 - (2k+1) = 2k+1$, $(p^2-1)/8 = 8k^2 + 10k + 3$, parité identique.
- $p = 8k+7$: $\nu = 4k + 3 - (2k+1) = 2k+2$, $(p^2-1)/8 = 8k^2 + 14k + 6$, parité identique.

Donc $\left(\frac{2}{p}\right) = (-1)^\nu = (-1)^{(p^2-1)/8}$. □

6.7 La loi de réciprocité quadratique

Nous arrivons au résultat central de ce chapitre, qualifié de « théorème d'or » par Gauss.

Théorème 6.16 (Loi de réciprocité quadratique). *Soient p et q deux premiers impairs distincts. Alors*

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

De manière équivalente :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{sauf si } p \equiv q \equiv 3 \pmod 4, \text{ auquel cas } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Avant de démontrer ce théorème, établissons un lemme combinatoire clé.

Lemme 6.17 (Lemme d'Eisenstein). *Avec les notations du lemme de Gauss*

(Lemme 6.11), le nombre ν de changements de signe est

$$\nu = \sum_{s=1}^{(p-1)/2} \left\lfloor \frac{as}{p} \right\rfloor.$$

Démonstration. Pour chaque $s \in \{1, \dots, (p-1)/2\}$, effectuons la division euclidienne de as par p :

$$as = \left\lfloor \frac{as}{p} \right\rfloor \cdot p + (as \bmod p).$$

Le reste $as \bmod p$ appartient à $\{1, \dots, p-1\}$ (car $p \nmid as$). Si $as \bmod p \leq (p-1)/2$, alors $\varepsilon_s = +1$ et $r_s = as \bmod p$. Si $as \bmod p > (p-1)/2$, alors $\varepsilon_s = -1$ et $r_s = p - (as \bmod p)$. Dans le second cas :

$$as = \left\lfloor \frac{as}{p} \right\rfloor \cdot p + (p - r_s) = \left(\left\lfloor \frac{as}{p} \right\rfloor + 1 \right) p - r_s.$$

Sommons sur tout $s \in S$:

$$a \sum_{s=1}^{(p-1)/2} s = p \sum_{s=1}^{(p-1)/2} \left\lfloor \frac{as}{p} \right\rfloor + \sum_{\varepsilon_s = +1} r_s + \sum_{\varepsilon_s = -1} (p - r_s).$$

La dernière somme se réécrit : $\sum_{\varepsilon_s=-1} p - \sum_{\varepsilon_s=-1} r_s = \nu p - \sum_{\varepsilon_s=-1} r_s$. Donc :

$$a \sum s = p \left(\sum \left\lfloor \frac{as}{p} \right\rfloor + \nu \right) + \sum_{\varepsilon_s=+1} r_s - \sum_{\varepsilon_s=-1} r_s.$$

Or, comme les r_s forment une permutation de S : $\sum r_s = \sum s$ et $\sum_{\varepsilon_s=+1} r_s - \sum_{\varepsilon_s=-1} r_s$ plus $2\sum_{\varepsilon_s=-1} r_s = \sum s$. On obtient, en travaillant modulo 2 :

$$a \sum s \equiv \sum s + 2\,(\text{termes}) + \nu \cdot p \pmod 2.$$

Comme $\sum s$ et p sont impairs (on peut les simplifier dans le calcul de parité), une analyse modulo 2 donne $\nu \equiv \sum \lfloor as/p \rfloor \pmod 2$. Puisque seule la parité de ν intervient dans $\left(\frac{a}{p}\right) = (-1)^\nu$, le résultat est établi. □

Nous pouvons maintenant démontrer la loi de réciprocité quadratique.

Preuve de la loi de réciprocité quadratique (méthode d'Eisenstein). Par le lemme de Gauss et le Lemme 6.17, on a

$$\left(\frac{q}{p}\right) = (-1)^A, \quad \text{où} \quad A = \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{iq}{p} \right\rfloor,$$

et de même

$$\left(\frac{p}{q}\right) = (-1)^B, \quad \text{où} \quad B = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor.$$

Il suffit donc de montrer que

$$A + B = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{6.1}$$

Comptage de points du réseau. Considérons le rectangle $R = \{(i,j) \in \mathbb{Z}^2 : 1 \le i \le (p-1)/2,\ 1 \le j \le (q-1)/2\}$. Ce rectangle contient $\frac{p-1}{2} \cdot \frac{q-1}{2}$ points entiers.

Considérons la droite $D : j = \frac{q}{p}\, i$ (qui passe par l'origine et le point (p,q)). Comme $p \nmid q$ et les deux sont premiers, aucun point entier (i,j) de R ne se trouve exactement sur D. En effet, $j = qi/p$ entier impliquerait $p \mid i$, impossible pour $1 \le i \le (p-1)/2$.

Comptons les points de R situés *en dessous* de D (c'est-à-dire $j < qi/p$) :

$$|\{(i,j) \in R : j < qi/p\}| = \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor = A.$$

Par symétrie, les points situés *au-dessus* de D (c'est-à-dire $j > qi/p$, soit $i < pj/q$) sont comptés par :

$$|\{(i,j) \in R : i < pj/q\}| = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor = B.$$

Puisque aucun point n'est sur D, chaque point de R est soit au-dessus, soit en dessous. Donc $A + B = \frac{p-1}{2} \cdot \frac{q-1}{2}$, ce qui établit (6.1) et achève la preuve. □

La figure 6.1 illustre ce comptage pour $p = 5$, $q = 7$.

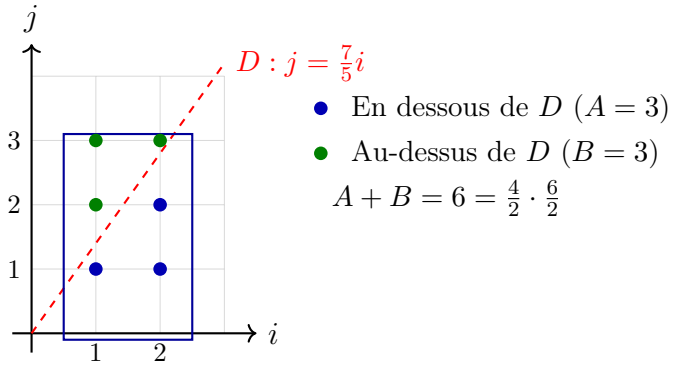


FIGURE 6.1 – Comptage de points du réseau pour la preuve d'Eisenstein avec $p = 5$ et $q = 7$. Le rectangle R contient $2 \times 3 = 6$ points entiers, répartis en $A = 3$ sous la diagonale et $B = 3$ au-dessus.

6.8 Exemples de calcul du symbole de Legendre

Exemple 6.18 (Calcul de $\left(\frac{23}{59}\right)$)**.** Par réciprocité quadratique (puisque $59 \equiv 3 \pmod 4$

et $23 \equiv 3 \pmod 4$, on est dans le cas exceptionnel) :

$$\left(\frac{23}{59}\right) = -\left(\frac{59}{23}\right) = -\left(\frac{59 \bmod 23}{23}\right) = -\left(\frac{13}{23}\right).$$

Maintenant $23 \equiv 3 \pmod 4$ et $13 \equiv 1 \pmod 4$, donc :

$$\left(\frac{13}{23}\right) = \left(\frac{23}{13}\right) = \left(\frac{23 \bmod 13}{13}\right) = \left(\frac{10}{13}\right).$$

Décomposons : $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right)$.
$\left(\frac{2}{13}\right)$: $13 \equiv 5 \pmod 8$, donc $\left(\frac{2}{13}\right) = (-1)^{(169-1)/8} = (-1)^{21} = -1$.
$\left(\frac{5}{13}\right)$: $13 \equiv 1 \pmod 4$, donc $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$. Or $5 \equiv 1 \pmod 4$, donc $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$. Et $3 \equiv 3 \pmod 8$, donc $\left(\frac{2}{3}\right) = -1$.
Rassemblons : $\left(\frac{10}{13}\right) = (-1)(-1) = 1$, puis $\left(\frac{13}{23}\right) = 1$, et enfin $\left(\frac{23}{59}\right) = -1$.
Donc 23 est un QNR modulo 59.

Exemple 6.19 (Calcul de $\left(\frac{-6}{31}\right)$)**.** $\left(\frac{-6}{31}\right) = \left(\frac{-1}{31}\right) \cdot \left(\frac{2}{31}\right) \cdot \left(\frac{3}{31}\right)$.
$\left(\frac{-1}{31}\right) = (-1)^{15} = -1$ car $31 \equiv 3 \pmod 4$.
$\left(\frac{2}{31}\right)$: $31 \equiv 7 \pmod 8$, donc $\left(\frac{2}{31}\right) = +1$.
$\left(\frac{3}{31}\right)$: $31 \equiv 3 \pmod 4$ et $3 \equiv 3 \pmod 4$, cas exceptionnel : $\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
Bilan : $\left(\frac{-6}{31}\right) = (-1)(+1)(-1) = +1$.
Vérification : $-6 \equiv 25 \pmod{31}$, et $5^2 = 25$. ✓

6.9 Le symbole de Jacobi

Définition 6.20 (Symbole de Jacobi)**.** Soit n un entier impair ≥ 3 avec la factorisation $n = p_1^{e_1} \cdots p_r^{e_r}$. Pour $a \in \mathbb{Z}$ avec $\operatorname{pgcd}(a, n) = 1$, le *symbole de Jacobi* est

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

Remarque 6.21. **Attention** : $\left(\frac{a}{n}\right) = 1$ n'implique *pas* que a soit un QR modulo n. Par exemple, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1$, mais $x^2 \equiv 2 \pmod{15}$ n'a aucune solution (car $x^2 \equiv 2 \pmod 3$ n'en a pas). En revanche, $\left(\frac{a}{n}\right) = -1$ garantit que a est un QNR modulo n.

Proposition 6.22 (Propriétés du symbole de Jacobi)**.** *Soient m, n des entiers impairs ≥ 3 et $a, b \in \mathbb{Z}$ premiers avec m et n.*

(i) ***Multiplicativité en haut*** *:* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$.

(ii) ***Multiplicativité en bas*** *:* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$.

(iii) ***Périodicité*** *:* $\left(\frac{a}{n}\right) = \left(\frac{a+n}{n}\right)$.

(iv) ***Premier supplément*** *:* $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(v) ***Second supplément*** *:* $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Démonstration. Les points (i), (ii) et (iii) découlent directement de la définition et des propriétés correspondantes du symbole de Legendre. Pour (iv), on utilise le fait que $(n-1)/2 \equiv \sum e_i(p_i-1)/2 \pmod 2$ et de même pour (v) avec $(n^2-1)/8$. □

Théorème 6.23 (Réciprocité quadratique pour le symbole de Jacobi)**.** *Soient m, n des entiers impairs ≥ 3 avec* $\gcd(m,n) = 1$. *Alors*

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

Démonstration. Écrivons $m = p_1 \cdots p_s$ et $n = q_1 \cdots q_t$ (avec répétitions). Alors

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = \prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{p_i}{q_j}\right)\cdot\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

L'exposant total est

$$\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \left(\sum_i \frac{p_i-1}{2}\right)\left(\sum_j \frac{q_j-1}{2}\right) \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2,$$

la dernière congruence résultant du fait que $\sum_i (p_i-1)/2 \equiv (m-1)/2 \pmod 2$. □

6.9.1 Calcul efficace du symbole de Jacobi

Grâce aux propriétés ci-dessus, le symbole de Jacobi $\left(\frac{a}{n}\right)$ se calcule en temps $O(\log^2 n)$ sans connaître la factorisation de n, par un algorithme analogue à celui d'Euclide :

Étape 1. Réduire a modulo n pour que $0 \leq a < n$.

Étape 2. Si $a = 0$, retourner 0. Si $a = 1$, retourner 1.

Étape 3. Écrire $a = 2^e \cdot a'$ avec a' impair. Calculer $\left(\frac{2}{n}\right)^e = (-1)^{e(n^2-1)/8}$.

Étape 4. Appliquer la réciprocité : $\left(\frac{a'}{n}\right) = (-1)^{(a'-1)(n-1)/4} \cdot \left(\frac{n}{a'}\right)$.

Étape 5. Réduire n modulo a' et recommencer.

Exemple 6.24 (Calcul de $\left(\frac{1001}{9907}\right)$)**.** Ici $1001 = 7 \times 11 \times 13$ et 9907 est premier, mais nous n'utilisons pas ces factorisations.
$\left(\frac{1001}{9907}\right)$: 1001 et 9907 sont impairs, $1001 \equiv 1 \pmod 4$, donc $\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right)$.
$9907 \bmod 1001 = 9907 - 9\cdot 1001 = 9907 - 9009 = 898$. $\left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\cdot\left(\frac{449}{1001}\right)$.
$\left(\frac{2}{1001}\right)$: $1001 \equiv 1 \pmod 8$, donc $\left(\frac{2}{1001}\right) = 1$.
$\left(\frac{449}{1001}\right)$: $449 \equiv 1 \pmod 4$, donc $\left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right)$. $1001 \bmod 449 = 1001 - 2\cdot 449 = 103$.
$\left(\frac{103}{449}\right)$: $103 \equiv 3 \pmod 4$, $449 \equiv 1 \pmod 4$, donc $\left(\frac{103}{449}\right) = \left(\frac{449}{103}\right)$. $449 \bmod 103 = 449 - 4\cdot 103 = 37$. $\left(\frac{37}{103}\right)$: $37 \equiv 1 \pmod 4$, donc $\left(\frac{37}{103}\right) = \left(\frac{103}{37}\right)$. $103 \bmod 37 = 103 - 2\cdot 37 = 29$.
$\left(\frac{29}{37}\right)$: $29 \equiv 1 \pmod 4$, donc $\left(\frac{29}{37}\right) = \left(\frac{37}{29}\right)$. $37 \bmod 29 = 8 = 2^3$. $\left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3$. Or

$29 \equiv 5 \pmod 8$, donc $\left(\frac{2}{29}\right) = -1$, et $\left(\frac{2}{29}\right)^3 = -1$.
Conclusion : $\left(\frac{1001}{9907}\right) = 1 \cdot (-1) = -1$.
Donc 1001 est un QNR modulo 9907.

6.10 Visualisation des résidus quadratiques

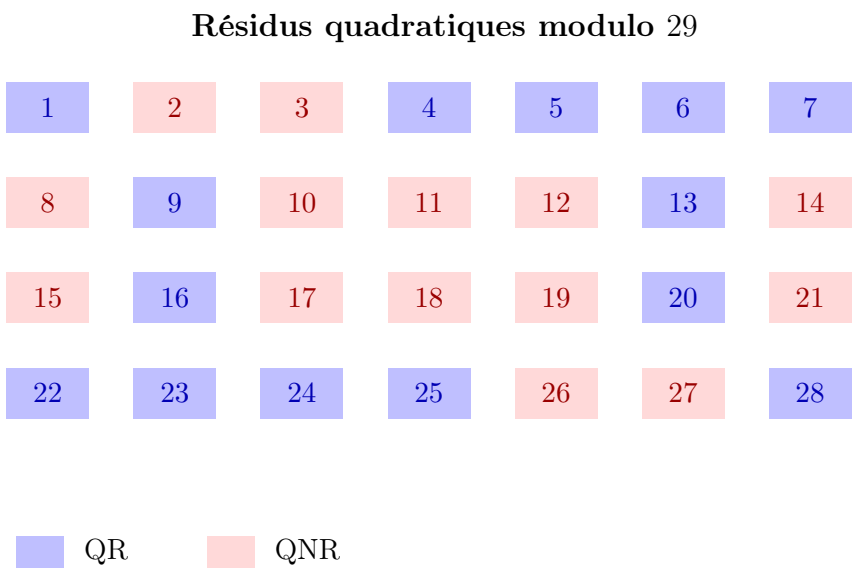


FIGURE 6.2 – Résidus quadratiques et non-résidus modulo 29. Les 14 cases bleues correspondent aux QR, les 14 rouges aux QNR.

6.11 Connexion avec les formes quadratiques

Proposition 6.25 (QR et représentation par des formes quadratiques)**.** *Soit p un premier impair et $d \in \mathbb{Z}$ avec $p \nmid d$. L'équation $x^2 + dy^2 \equiv 0 \pmod p$ admet une solution non triviale (c'est-à-dire $p \nmid x$ ou $p \nmid y$) si et seulement si $\left(\frac{-d}{p}\right) = 1$.*

Démonstration. Si $p \nmid y$, l'équation se réécrit $(xy^{-1})^2 \equiv -d \pmod p$, ce qui équivaut à $\left(\frac{-d}{p}\right) = 1$. Si $p \mid y$ et $p \nmid x$, alors $x^2 \equiv 0$, contradiction. L'existence d'une solution non triviale est donc équivalente à ce que $-d$ soit un QR modulo p. □

Remarque 6.26. En prenant $d = 1$, on retrouve le fait que $x^2 + y^2 \equiv 0 \pmod p$ admet une solution non triviale si et seulement si $\left(\frac{-1}{p}\right) = 1$, soit $p \equiv 1 \pmod 4$. C'est la première étape de la preuve du théorème de Fermat sur les sommes de deux carrés.

6.12 Exercices

Exercice 6.1 ($\star$)**.** Dresser la liste des résidus quadratiques modulo 17.

Exercice 6.2 ($\star$)**.** Calculer $\left(\frac{7}{29}\right)$ par le critère d'Euler, puis vérifier par la réciprocité quadratique.

Exercice 6.3 ($\star$)**.** Calculer les symboles de Legendre suivants en utilisant la réciprocité :

$$\left(\frac{3}{43}\right), \quad \left(\frac{-5}{37}\right), \quad \left(\frac{11}{71}\right), \quad \left(\frac{15}{97}\right).$$

Exercice 6.4 ($\star$)**.** Montrer que -1 est un QR modulo tout premier de la forme $4k+1$ en exhibant explicitement une racine carrée (indication : considérer $((2k)!)^2$, ou plus directement $((p-1)/2)!$, modulo p).

Exercice 6.5 ($\star\star$)**.** Soit p un premier impair. Montrer que la somme des résidus quadratiques modulo p dans $\{1, \dots, p-1\}$ est $p(p-1)/4$.

Exercice 6.6 ($\star\star$)**.** Montrer que le produit de deux QNR modulo p est un QR, et que le produit d'un QR et d'un QNR est un QNR. En déduire que les QR modulo p forment un sous-groupe d'indice 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 6.7 ($\star\star$)**.** Soit p un premier ≥ 5. Montrer qu'il existe deux résidus quadratiques consécutifs modulo p (c'est-à-dire a et $a+1$ tous deux QR). *Indication : utiliser le fait que* $\sum_{a=1}^{p-2}(1+\left(\frac{a}{p}\right))(1+\left(\frac{a+1}{p}\right)) > 0$.

Exercice 6.8 ($\star\star$)**.** Calculer $\left(\frac{713}{1009}\right)$ par l'algorithme du symbole de Jacobi, en détaillant chaque étape.

Exercice 6.9 ($\star\star\star$)**.** Soit p un premier impair. La *somme de Gauss* est $g = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e^{2\pi i a/p}$. Montrer que $g^2 = (-1)^{(p-1)/2} p = \left(\frac{-1}{p}\right) p$. *Indication : calculer* $|g|^2 = g\overline{g}$ *en échangeant les sommes.*

Exercice 6.10 ($\star\star\star$)**.** En utilisant le premier supplément, montrer qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod 4$. *Indication : considérer* $(2n!)^2 + 1$ *pour un entier* n *convenable et examiner ses facteurs premiers.*

Exercice 6.11 ($\star\star\star$)**.** Donner une preuve de la loi de réciprocité quadratique en utilisant les sommes de Gauss. *Indication : montrer que* $g^p \equiv \left(\frac{p}{q}\right) \cdot g \pmod p$ *et utiliser le fait que* $g^2 = (-1)^{(q-1)/2} q$.

Résumé du chapitre

— Un entier a non divisible par p est un **résidu quadratique** (QR) modulo p s'il existe x tel que $x^2 \equiv a \pmod p$. Il y a exactement $(p-1)/2$ QR et $(p-1)/2$ QNR modulo p.

— Le **critère d'Euler** affirme que $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$.

— Le **symbole de Legendre** $\left(\frac{a}{p}\right)$ vaut 0, $+1$ ou -1 selon que $p \mid a$, a est QR, ou a est QNR.

— Le **lemme de Gauss** relie $\left(\frac{a}{p}\right)$ au nombre de « dépassements » dans la multiplication par a des éléments de $\{1, \dots, (p-1)/2\}$.

— Les **suppléments** donnent : $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ et $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

— La **loi de réciprocité quadratique** : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ pour p, q premiers impairs distincts.

— Le **symbole de Jacobi** $\left(\frac{a}{n}\right)$ généralise le symbole de Legendre aux modules composés impairs et satisfait la même loi de réciprocité. Il se calcule efficacement sans factorisation.

Chapitre 7

Représentations par des Formes Quadratiques

Introduction historique

L'étude des représentations d'entiers par des formes quadratiques constitue l'un des chapitres les plus anciens et les plus riches de la théorie des nombres. Dès le III^{e} siècle, **Diophante d'Alexandrie** s'interrogeait sur les entiers pouvant s'écrire comme sommes de deux carrés. La question resta largement ouverte jusqu'au XVII^{e} siècle, lorsque **Pierre de Fermat** annonça, sans démonstration complète, que tout nombre premier $p \equiv 1 \pmod 4$ est somme de deux carrés. C'est **Leonhard Euler** qui, après des décennies d'efforts, fournit en 1749 la première preuve rigoureuse de ce résultat fondamental.

Joseph-Louis Lagrange étendit considérablement la théorie : il démontra en 1770 que tout entier naturel est somme de quatre carrés, et développa une théorie systématique des formes quadratiques binaires. Cette théorie fut ensuite portée à un haut degré de perfection par **Carl Friedrich Gauss** dans ses *Disquisitiones Arithmeticae* (1801), où il introduisit les notions de classe d'équivalence de formes et de composition.

7.1 Formes quadratiques binaires

Définition 7.1 (Forme quadratique binaire)**.** Une *forme quadratique binaire* est un polynôme de la forme

$$f(x, y) = ax^2 + bxy + cy^2$$

où $a, b, c \in \mathbb{Z}$. On note cette forme (a, b, c). Le *discriminant* de f est

$$\Delta = b^2 - 4ac.$$

On dit que f *représente* un entier n s'il existe $x_0, y_0 \in \mathbb{Z}$ tels que $f(x_0, y_0) = n$. Si $\gcd(x_0, y_0) = 1$, la représentation est dite *propre*.

Exemple 7.2 (Formes quadratiques classiques)**.** (a) La forme $f(x, y) = x^2 + y^2$ a pour discriminant $\Delta = -4$. Elle représente n si et seulement si n est somme de deux carrés.

(b) La forme $f(x,y) = x^2 + xy + y^2$ a pour discriminant $\Delta = -3$. Elle représente les entiers de la forme $x^2 + xy + y^2$, liés aux nombres premiers $p \equiv 1 \pmod 3$.

(c) La forme $f(x,y) = x^2 - y^2 = (x+y)(x-y)$ a pour discriminant $\Delta = 4$. Elle représente toute différence de deux carrés.

Définition 7.3 (Forme définie positive)**.** Une forme quadratique binaire (a,b,c) est dite *définie positive* si $a > 0$ et $\Delta = b^2 - 4ac < 0$. Dans ce cas, $f(x,y) \geq 0$ pour tout $(x,y) \in \mathbb{Z}^2$, avec égalité si et seulement si $(x,y) = (0,0)$.

Remarque 7.4. Pour une forme définie positive (a,b,c) avec $\Delta < 0$, on a nécessairement $c > 0$ puisque $4ac = b^2 - \Delta > 0$ et $a > 0$.

7.2 Sommes de deux carrés

7.2.1 Identité de Brahmagupta

L'étude des sommes de deux carrés repose sur une identité multiplicative fondamentale.

Lemme 7.5 (Identité de Brahmagupta–Fibonacci)**.** *Pour tous $a,b,c,d \in \mathbb{Z}$,*

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 = (ac+bd)^2 + (ad-bc)^2.$$

Démonstration. Par développement direct :

$$\begin{aligned}(ac-bd)^2 + (ad+bc)^2 &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2).\end{aligned}$$

□

Corollaire 7.6. *Le produit de deux sommes de deux carrés est une somme de deux carrés.*

Remarque 7.7. L'identité de Brahmagupta s'interprète naturellement dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$: si $\alpha = a + bi$ et $\beta = c + di$, alors $|\alpha|^2 |\beta|^2 = |\alpha\beta|^2$, ce qui n'est autre que la multiplicativité de la norme.

7.2.2 Entiers de Gauss

Pour la preuve du théorème de Fermat sur les sommes de deux carrés, nous utiliserons l'anneau des entiers de Gauss.

Définition 7.8 (Anneau des entiers de Gauss)**.** L'*anneau des entiers de Gauss* est

$$\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z}\} \subset \mathbb{C}.$$

La *norme* d'un élément $\alpha = a + bi$ est $N(\alpha) = a^2 + b^2 = \alpha\bar{\alpha} \in \mathbb{N}$.

Proposition 7.9 (Propriétés de $\mathbb{Z}[i]$). *(i) La norme est multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$.*

(ii) Les inversibles de $\mathbb{Z}[i]$ sont $\{1, -1, i, -i\}$, c'est-à-dire les éléments de norme 1.

(iii) L'anneau $\mathbb{Z}[i]$ est un anneau euclidien pour la norme N, et donc un anneau principal et factoriel.

Démonstration. (i) $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\bar{\alpha} \cdot \beta\bar{\beta} = N(\alpha)N(\beta)$.

(ii) Si α est inversible, $N(\alpha)N(\alpha^{-1}) = N(1) = 1$, donc $N(\alpha) = 1$, d'où $a^2 + b^2 = 1$, ce qui donne $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$.

(iii) Soient $\alpha, \beta \in \mathbb{Z}[i]$ avec $\beta \neq 0$. On écrit $\alpha/\beta = u + vi$ avec $u, v \in \mathbb{Q}$. Soient $m, n \in \mathbb{Z}$ les entiers les plus proches de u et v. Posons $\gamma = m + ni$ et $\rho = \alpha - \beta\gamma$. Alors $N(\rho) = N(\beta)N(\alpha/\beta - \gamma) = N(\beta)\big((u-m)^2 + (v-n)^2\big) \leq N(\beta)(1/4 + 1/4) = N(\beta)/2 < N(\beta)$. □

Lemme 7.10 (Factorisation des premiers dans $\mathbb{Z}[i]$). *Soit p un nombre premier (de $\mathbb{Z}$).*

(i) Si $p = 2$, alors $p = -i(1+i)^2$, et $1 + i$ est irréductible dans $\mathbb{Z}[i]$.

(ii) Si $p \equiv 1 \pmod 4$, alors $p = \pi\bar{\pi}$ où π est irréductible dans $\mathbb{Z}[i]$ et $\pi \neq \bar{\pi}$ (à association près).

(iii) Si $p \equiv 3 \pmod 4$, alors p reste irréductible dans $\mathbb{Z}[i]$.

Démonstration. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p = \alpha\beta$ avec $1 < N(\alpha), N(\beta) < p^2$, donc $N(\alpha) = N(\beta) = p$, ce qui signifie que p est somme de deux carrés.

Pour $p = 2$: $2 = 1^2 + 1^2$, et $2 = -i(1+i)^2$.

Pour $p \equiv 3 \pmod 4$: si $p = a^2 + b^2$, alors $a^2 + b^2 \equiv 3 \pmod 4$. Or $a^2 \equiv 0$ ou 1 modulo 4, de même pour b^2, donc $a^2 + b^2 \equiv 0, 1$ ou 2 modulo 4. Contradiction.

Pour $p \equiv 1 \pmod 4$: par le théorème de Wilson, $(p-1)! \equiv -1 \pmod p$. Posons $m = (p-1)/2$. Alors

$$(p-1)! = 1 \cdot 2 \cdots m \cdot (m+1) \cdots (p-1).$$

Or $p - k \equiv -k \pmod p$, donc $(p-1)! \equiv (-1)^m (m!)^2 \pmod p$. Puisque $p \equiv 1 \pmod 4$, m est pair, et $(-1)^m = 1$, d'où $(m!)^2 \equiv -1 \pmod p$. Posons $r = m!$. Alors $p \mid r^2 + 1 = (r+i)(r-i)$ dans $\mathbb{Z}[i]$. Si p était irréductible dans $\mathbb{Z}[i]$, il diviserait $r + i$ ou $r - i$, ce qui est impossible car $r/p \notin \mathbb{Z}$. Donc p n'est pas irréductible dans $\mathbb{Z}[i]$, et l'argument initial montre $p = \pi\bar{\pi}$ avec $N(\pi) = p$. □

7.2.3 Théorème de Fermat sur les sommes de deux carrés

Théorème 7.11 (Fermat, 1640 – Euler, 1749). *Un nombre premier p est somme de deux carrés d'entiers si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.*

Démonstration. La preuve découle directement du lemme 7.10. Si $p = 2$, alors $2 = 1^2 + 1^2$. Si $p \equiv 1 \pmod 4$, alors $p = \pi\bar{\pi}$ dans $\mathbb{Z}[i]$ avec $\pi = a + bi$, d'où $p = N(\pi) = a^2 + b^2$. Si $p \equiv 3 \pmod 4$, alors p est irréductible dans $\mathbb{Z}[i]$, donc p ne peut s'écrire $a^2 + b^2$ avec $a, b \in \mathbb{Z}$. □

Théorème 7.12 (Caractérisation des sommes de deux carrés)**.** *Un entier $n \geq 1$ est somme de deux carrés si et seulement si, dans la factorisation $n = \prod p_i^{e_i}$, tout facteur premier $p_i \equiv 3 \pmod 4$ apparaît avec un exposant e_i pair.*

Démonstration. Condition suffisante. Si tout premier $p \equiv 3 \pmod 4$ divisant n apparaît à une puissance paire, alors $n = m^2 \cdot n'$ où n' n'a que des facteurs premiers $p = 2$ ou $p \equiv 1 \pmod 4$. Chacun de ces facteurs est somme de deux carrés, et par l'identité de Brahmagupta (lemme 7.5), n' l'est aussi. Donc $n = m^2 n' = m^2(a^2 + b^2) = (ma)^2 + (mb)^2$.

Condition nécessaire. Soit $p \equiv 3 \pmod 4$ et supposons $p^{2k+1} \| n$ avec $n = a^2 + b^2$. Dans $\mathbb{Z}[i]$, on a $n = (a + bi)(a - bi)$. Puisque p est irréductible dans $\mathbb{Z}[i]$ (lemme 7.10), p divise $a + bi$ et $a - bi$ le même nombre de fois. Si $p^r \mid (a + bi)$ et $p^s \mid (a - bi)$ dans $\mathbb{Z}[i]$, alors $p^{r+s} \mid n$ dans $\mathbb{Z}$, et $r = s$ car $\overline{a + bi} = a - bi$. Donc p divise n à une puissance paire. □

Exemple 7.13 (Application du critère)**.**
(a) $n = 50 = 2 \cdot 5^2$. Les facteurs premiers 2 et 5 vérifient $2 = 1^2 + 1^2$ et $5 \equiv 1 \pmod 4$. Pas de facteur $\equiv 3 \pmod 4$, donc 50 est somme de deux carrés : $50 = 1^2 + 7^2 = 5^2 + 5^2$.

(b) $n = 21 = 3 \cdot 7$. Les deux facteurs premiers sont $\equiv 3 \pmod 4$ et apparaissent à la puissance 1 (impaire). Donc 21 n'est pas somme de deux carrés.

(c) $n = 45 = 3^2 \cdot 5$. Le seul facteur $\equiv 3 \pmod 4$ est 3, qui apparaît au carré. Donc 45 est somme de deux carrés : $45 = 3^2 + 6^2$.

7.2.4 Dénombrement des représentations

Définition 7.14 (Fonction $r_2(n)$)**.** Pour $n \geq 0$, on note $r_2(n)$ le nombre de couples $(a, b) \in \mathbb{Z}^2$ tels que $a^2 + b^2 = n$. On compte les représentations *ordonnées* et avec signes.

Théorème 7.15 (Jacobi)**.** *Pour tout $n \geq 1$,*

$$r_2(n) = 4 \sum_{d \mid n} \chi(d) = 4\big(d_1(n) - d_3(n)\big),$$

où χ est le caractère de Dirichlet non principal modulo 4 (défini par $\chi(d) = 0$ si d est pair, $\chi(d) = 1$ si $d \equiv 1 \pmod 4$, $\chi(d) = -1$ si $d \equiv 3 \pmod 4$), et $d_k(n)$ désigne le nombre de diviseurs de n congrus à k modulo 4.

Exemple 7.16.
(a) $r_2(5) = 4(d_1(5) - d_3(5)) = 4(2 - 0) = 8$. En effet, $5 = 1^2 + 2^2$ donne les huit couples $(\pm 1, \pm 2)$ et $(\pm 2, \pm 1)$.

(b) $r_2(25) = 4(d_1(25) - d_3(25)) = 4(3 - 0) = 12$. Les diviseurs de 25 congrus à 1 (mod 4) sont $1, 5, 25$.

7.2.5 Visualisation : points entiers sur des cercles

La figure suivante illustre les points $(a, b) \in \mathbb{Z}^2$ tels que $a^2 + b^2 = n$ pour différentes valeurs de n.

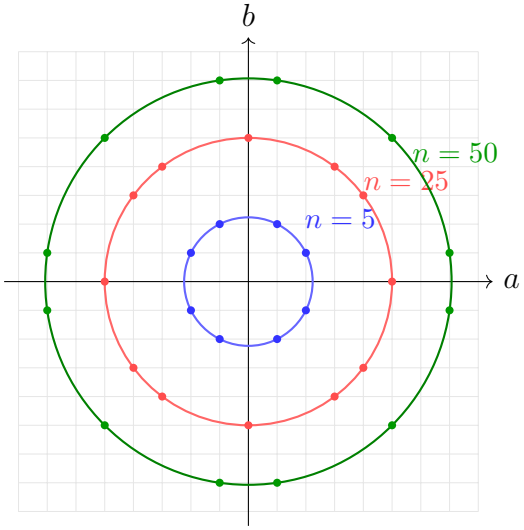


FIGURE 7.1 – Points entiers sur les cercles $a^2 + b^2 = n$ pour $n \in \{5, 25, 50\}$.

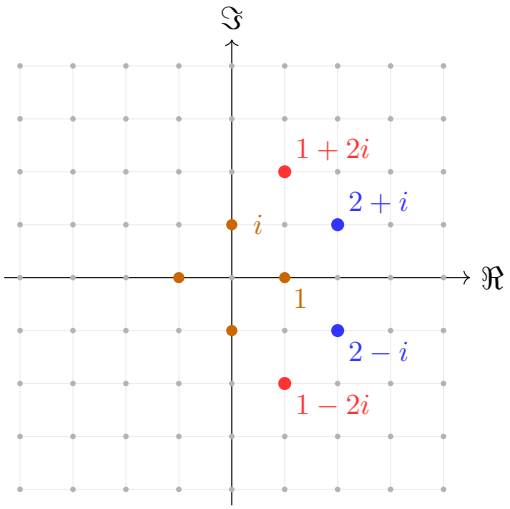


FIGURE 7.2 – L'anneau des entiers de Gauss $\mathbb{Z}[i]$: inversibles (orange), premiers associés à $5 = (2 + i)(2 - i)$ (bleu et rouge).

7.3 Sommes de quatre carrés

Théorème 7.17 (Lagrange, 1770)**.** *Tout entier naturel est somme de quatre carrés d'entiers :*

$$\forall n \in \mathbb{N}, \quad \exists\, a, b, c, d \in \mathbb{Z} : \quad n = a^2 + b^2 + c^2 + d^2.$$

La preuve repose sur deux ingrédients : une identité multiplicative et un argument arithmétique.

Lemme 7.18 (Identité d'Euler pour les quaternions)**.** *Pour tous* $a_1, \dots, a_4, b_1, \dots, b_4 \in \mathbb{Z}$,

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

où

$$c_1 = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4, \qquad c_2 = a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3,$$
$$c_3 = a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2, \qquad c_4 = a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1.$$

Démonstration. On identifie (a_1, a_2, a_3, a_4) au quaternion $\alpha = a_1 + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}$, et de même pour β. Alors $N(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2$, et la multiplicativité de la norme des quaternions donne $N(\alpha\beta) = N(\alpha)N(\beta)$. Le produit $\alpha\beta$ a pour composantes exactement c_1, c_2, c_3, c_4. □

Preuve du théorème 7.17 (schéma). Grâce au lemme 7.18, il suffit de montrer que tout nombre premier p est somme de quatre carrés.

Étape 1. On montre qu'il existe m avec $1 \le m < p$ tel que mp est somme de quatre carrés. En effet, l'équation $x^2 + y^2 + 1 \equiv 0 \pmod p$ admet une solution car l'ensemble $\{x^2 \bmod p : x = 0, 1, \dots, (p-1)/2\}$ a $(p+1)/2$ éléments, et $\{-1 - y^2 \bmod p : y = 0, 1, \dots, (p-1)/2\}$ en a autant. Par le principe des tiroirs, ces ensembles ont une intersection non vide : il existe x_0, y_0 tels que $x_0^2 + y_0^2 + 1 \equiv 0 \pmod p$, soit $mp = x_0^2 + y_0^2 + 1^2 + 0^2$ avec $m < p$.

Étape 2. On montre par descente infinie que si $mp = a_1^2 + a_2^2 + a_3^2 + a_4^2$ avec $m > 1$, on peut trouver m' avec $1 \le m' < m$ tel que $m'p$ est aussi somme de quatre carrés. On choisit $b_i \equiv a_i \pmod m$ avec $|b_i| \le m/2$, et on utilise l'identité d'Euler pour réduire le multiplicateur.

Par descente, on atteint $m = 1$, c'est-à-dire $p = a_1^2 + a_2^2 + a_3^2 + a_4^2$. □

Exemple 7.19. (a) $7 = 4 + 1 + 1 + 1 = 2^2 + 1^2 + 1^2 + 1^2$.
(b) $15 = 9 + 4 + 1 + 1 = 3^2 + 2^2 + 1^2 + 1^2$.
(c) $23 = 9 + 9 + 4 + 1 = 3^2 + 3^2 + 2^2 + 1^2$.

7.4 Le problème de Waring

Théorème 7.20 (Hilbert, 1909)**.** *Pour tout entier $k \ge 2$, il existe un entier $g(k)$ tel que tout entier naturel est somme de $g(k)$ puissances k-ièmes d'entiers naturels.*

Remarque 7.21. Les premières valeurs connues de $g(k)$ sont :

k	2	3	4	5	6	7
$g(k)$	4	9	19	37	73	143

Le théorème de Lagrange donne $g(2) = 4$. La valeur $g(3) = 9$ fut établie par Wieferich

et Kempner. On conjecture (et c'est démontré pour k assez grand) que

$$g(k) = 2^k + \lfloor * \rfloor \left(\frac{3}{2}\right)^k - 2.$$

7.5 Formes ternaires et théorème de Legendre

Théorème 7.22 (Legendre, 1785). *L'équation $ax^2 + by^2 + cz^2 = 0$ avec $a, b, c \in \mathbb{Z}$ non tous de même signe et sans facteur carré commun admet une solution non triviale $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ si et seulement si :*

(i) *$-bc$ est un résidu quadratique modulo $|a|$,*

(ii) *$-ac$ est un résidu quadratique modulo $|b|$,*

(iii) *$-ab$ est un résidu quadratique modulo $|c|$.*

Corollaire 7.23 (Théorème des trois carrés – Gauss–Legendre). *Un entier $n \geq 0$ est somme de trois carrés si et seulement si n n'est pas de la forme $4^a(8b + 7)$ avec $a, b \in \mathbb{N}$.*

7.6 Équivalence et réduction de formes

Définition 7.24 (Équivalence de formes). Deux formes quadratiques binaires f et g sont dites *proprement équivalentes* s'il existe une matrice $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ telle que

$$g(x, y) = f(\alpha x + \beta y,\ \gamma x + \delta y).$$

Des formes équivalentes ont le même discriminant et représentent les mêmes entiers.

Définition 7.25 (Forme réduite au sens de Gauss). Une forme définie positive (a, b, c) de discriminant $\Delta < 0$ est *réduite* si

$$|b| \leq a \leq c,$$

et de plus $b \geq 0$ lorsque $|b| = a$ ou $a = c$.

Théorème 7.26. *Toute forme définie positive de discriminant $\Delta < 0$ est proprement équivalente à une unique forme réduite.*

Exemple 7.27. Pour $\Delta = -4$, la seule forme réduite est $(1, 0, 1)$, c'est-à-dire $x^2 + y^2$. Pour $\Delta = -20$, les formes réduites sont $(1, 0, 5)$ et $(2, 2, 3)$. Le nombre de classes est $h(-20) = 2$.

7.7 Exercices

Exercice 7.1 ($\star$)**.** Déterminer lesquels des entiers suivants sont sommes de deux carrés, et trouver une représentation le cas échéant : $n = 65$, $n = 99$, $n = 130$, $n = 225$, $n = 1000$.

Exercice 7.2 ($\star$)**.** Calculer $r_2(n)$ pour $n = 1, 2, 4, 5, 10, 13, 25$.

Exercice 7.3 ($\star$)**.** Écrire chacun des entiers 30, 47, 100, 200 comme somme de quatre carrés.

Exercice 7.4 ($\star\star$)**.** Montrer directement (sans utiliser les entiers de Gauss) que si p est un premier avec $p \equiv 1 \pmod 4$, alors il existe m avec $1 \leq m < p$ tel que $mp = a^2 + b^2$ pour certains $a, b \in \mathbb{Z}$.

Exercice 7.5 ($\star\star$)**.** Montrer qu'il existe une infinité de nombres premiers p tels que $p = a^2 + b^2$ avec $a, b \in \mathbb{N}^*$. *Indication : utiliser le théorème de Dirichlet sur les progressions arithmétiques.*

Exercice 7.6 ($\star\star$)**.** Montrer qu'un entier de la forme $4^a(8b + 7)$ ne peut pas être somme de trois carrés. *Indication : raisonner modulo* 8.

Exercice 7.7 ($\star\star$)**.** Trouver la forme réduite équivalente à $f(x, y) = 3x^2 + 10xy + 9y^2$.

Exercice 7.8 ($\star\star\star$)**.** Montrer que le nombre de classes $h(\Delta)$ est fini pour tout discriminant $\Delta < 0$. *Indication : montrer que pour une forme réduite (a, b, c), on a $a \leq \sqrt{|\Delta|/3}$.*

Exercice 7.9 ($\star\star\star$)**.** Soient $r_4(n)$ le nombre de représentations de n comme somme de quatre carrés. Montrer que $r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d$. En déduire que $r_4(n) \geq 1$ pour tout $n \geq 1$.

Résumé du chapitre

1. Une **forme quadratique binaire** $f(x, y) = ax^2 + bxy + cy^2$ a pour discriminant $\Delta = b^2 - 4ac$.
2. L'**identité de Brahmagupta** montre que le produit de deux sommes de deux carrés est une somme de deux carrés.
3. L'anneau des **entiers de Gauss** $\mathbb{Z}[i]$ est un anneau euclidien, et la factorisation des premiers dans cet anneau détermine quels entiers sont sommes de deux carrés.
4. **Théorème de Fermat** : p premier est somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \pmod 4$.
5. Un entier n est somme de deux carrés ssi tout facteur premier $p \equiv 3 \pmod 4$ apparaît avec un exposant pair.
6. **Théorème de Lagrange** : tout entier est somme de quatre carrés.
7. Le **problème de Waring** : tout entier est somme de $g(k)$ puissances k-ièmes.
8. Deux formes de même discriminant sont proprement équivalentes si et seulement si elles ont la même forme réduite.

Chapitre 8

Fonctions Arithmétiques

Introduction

Les fonctions arithmétiques — fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ — sont omniprésentes en théorie des nombres. Elles codent des propriétés fondamentales des entiers : nombre de diviseurs, somme des diviseurs, structure multiplicative. Ce chapitre développe la théorie algébrique de ces fonctions, centrée sur le *produit de Dirichlet*, et culmine avec la *formule d'inversion de Möbius*, l'un des outils les plus puissants et les plus élégants de la théorie des nombres élémentaire.

8.1 Définitions et exemples fondamentaux

Définition 8.1 (Fonction arithmétique)**.** Une *fonction arithmétique* est une application $f : \mathbb{N}^* \to \mathbb{C}$.

Définition 8.2 (Multiplicativité)**.** Une fonction arithmétique f est :

(i) *multiplicative* si $f(1) = 1$ et $f(mn) = f(m)f(n)$ pour tout $m, n \in \mathbb{N}^*$ avec $\text{pgcd}(m, n) = 1$;

(ii) *complètement multiplicative* si $f(1) = 1$ et $f(mn) = f(m)f(n)$ pour tout $m, n \in \mathbb{N}^*$.

Remarque 8.3. Une fonction multiplicative est entièrement déterminée par ses valeurs sur les puissances de nombres premiers $f(p^k)$. Une fonction complètement multiplicative est déterminée par ses valeurs sur les nombres premiers $f(p)$.

8.2 L'indicatrice d'Euler $\varphi(n)$

Définition 8.4 (Indicatrice d'Euler)**.** Pour $n \geq 1$, l'*indicatrice d'Euler* est

$$\varphi(n) = \#\{k \in \{1, 2, \ldots, n\} : \text{pgcd}(k, n) = 1\}.$$

Théorème 8.5 (Formule produit pour φ)**.** *Pour tout $n \geq 1$,*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

En particulier, si $n = p_1^{a_1} \cdots p_r^{a_r}$, alors

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

Démonstration. On montre d'abord que φ est multiplicative. Soient m, n avec $\gcd(m, n) = 1$. Par le théorème chinois des restes, l'application

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

est un isomorphisme d'anneaux, qui induit un isomorphisme sur les groupes d'inversibles : $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Donc $\varphi(mn) = \varphi(m)\varphi(n)$.

Il reste à calculer $\varphi(p^a)$ pour p premier. Les entiers de $\{1, \ldots, p^a\}$ non premiers à p^a sont exactement les multiples de p, au nombre de p^{a-1}. Donc $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1 - 1/p)$.

La formule générale s'obtient par multiplicativité. □

Théorème 8.6 (Identité de Gauss)**.** *Pour tout $n \geq 1$,*

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

Démonstration. Considérons les fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. Chaque fraction $\frac{k}{n}$, réduite sous forme irréductible, s'écrit $\frac{a}{d}$ où $d \mid n$ et $\gcd(a, d) = 1$. Pour un diviseur d fixé de n, le nombre de fractions $\frac{a}{d}$ avec $1 \leq a \leq d$ et $\gcd(a, d) = 1$ est exactement $\varphi(d)$. Les n fractions se répartissent donc en classes indexées par les diviseurs de n, ce qui donne

$$n = \sum_{d \mid n} \varphi(d).$$ □

Exemple 8.7. (a) $\varphi(12) = 12(1 - 1/2)(1 - 1/3) = 12 \cdot 1/2 \cdot 2/3 = 4$. En effet, les entiers premiers à 12 dans $\{1, \ldots, 12\}$ sont $1, 5, 7, 11$.

(b) $\varphi(100) = 100(1 - 1/2)(1 - 1/5) = 100 \cdot 1/2 \cdot 4/5 = 40$.

(c) Vérification de $\sum_{d \mid 12} \varphi(d)$: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$. ✓

8.3 Fonctions de diviseurs

Définition 8.8 (Fonctions τ, σ et σ_k)**.** Pour $n \geq 1$ et $k \in \mathbb{N}$, on pose :

$$\tau(n) = \sum_{d|n} 1 \qquad \text{(nombre de diviseurs de } n\text{)},$$

$$\sigma_k(n) = \sum_{d|n} d^k \qquad \text{(somme des puissances } k\text{-ièmes des diviseurs)},$$

$$\sigma(n) = \sigma_1(n) = \sum_{d|n} d \qquad \text{(somme des diviseurs)}.$$

On a $\tau(n) = \sigma_0(n)$. On note aussi $d(n) = \tau(n)$.

Proposition 8.9 (Formules explicites)**.** *Soit $n = p_1^{a_1} \cdots p_r^{a_r}$ la factorisation de n. Alors :*

(i) $\tau(n) = \prod_{i=1}^{r} (a_i + 1)$.

(ii) $\sigma_k(n) = \prod_{i=1}^{r} \dfrac{p_i^{k(a_i+1)} - 1}{p_i^k - 1}$ *pour* $k \geq 1$.

(iii) $\sigma(n) = \prod_{i=1}^{r} \dfrac{p_i^{a_i+1} - 1}{p_i - 1}$.

Démonstration. Les trois fonctions sont multiplicatives (ce qui se vérifie directement). Il suffit donc de les calculer sur les puissances de premiers.

(i) $\tau(p^a) = \#\{1, p, p^2, \ldots, p^a\} = a + 1$.

(ii) $\sigma_k(p^a) = 1 + p^k + p^{2k} + \cdots + p^{ak} = \frac{p^{k(a+1)}-1}{p^k-1}$.

(iii) Cas particulier de (ii) avec $k = 1$. □

Définition 8.10 (Nombre parfait)**.** Un entier $n \geq 2$ est *parfait* si $\sigma(n) = 2n$, c'est-à-dire si la somme de ses diviseurs propres (distincts de n) est égale à n.

Théorème 8.11 (Euler–Euclide)**.** *Un entier pair n est parfait si et seulement si $n = 2^{p-1}(2^p - 1)$ où $2^p - 1$ est un nombre premier (de Mersenne).*

Démonstration. Suffisance. Si $q = 2^p - 1$ est premier, alors $\sigma(2^{p-1}q) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)(q + 1) = q \cdot 2^p = 2 \cdot 2^{p-1}q$.

Nécessité. Soit $n = 2^a m$ avec m impair et $a \geq 1$. Alors $\sigma(n) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m) = 2n = 2^{a+1}m$. Donc $(2^{a+1} - 1) \mid 2^{a+1}m$, et comme $\operatorname{pgcd}(2^{a+1} - 1, 2^{a+1}) = 1$, on a $(2^{a+1} - 1) \mid m$. Posons $m = (2^{a+1} - 1)k$. Alors $(2^{a+1} - 1)\sigma(m) = 2^{a+1}(2^{a+1} - 1)k$, d'où $\sigma(m) = 2^{a+1}k = m + k$. Si $k > 1$, alors m a au moins les trois diviseurs $1, k, m$, donc $\sigma(m) \geq 1 + k + m > m + k$, contradiction. Donc $k = 1$, $m = 2^{a+1} - 1$ est premier, et $n = 2^a(2^{a+1} - 1)$. □

Exemple 8.12. Les premiers nombres parfaits pairs sont : $6 = 2^1(2^2-1)$, $28 = 2^2(2^3-1)$, $496 = 2^4(2^5-1)$, $8128 = 2^6(2^7-1)$. L'existence de nombres parfaits impairs reste un problème ouvert célèbre.

8.4 La fonction de Möbius $\mu(n)$

Définition 8.13 (Fonction de Möbius)**.** La *fonction de Möbius* est définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n = p_1 p_2 \cdots p_k \text{ avec } p_1, \ldots, p_k \text{ premiers distincts}, \\ 0 & \text{si } p^2 \mid n \text{ pour un nombre premier } p. \end{cases}$$

Proposition 8.14. *La fonction μ est multiplicative.*

Démonstration. Il est clair que $\mu(1) = 1$. Soient m, n avec $\gcd(m,n) = 1$. Si m ou n a un facteur carré, mn en a un aussi, et les deux côtés valent 0. Sinon, $m = p_1 \cdots p_r$ et $n = q_1 \cdots q_s$ sont des produits de premiers distincts. Comme $\gcd(m,n) = 1$, tous les p_i, q_j sont distincts, et mn est un produit de $r+s$ premiers distincts. Donc $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. □

Théorème 8.15 (Propriété fondamentale de μ)**.** *Pour tout $n \geq 1$,*

$$\sum_{d \mid n} \mu(d) = [n = 1] = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

Démonstration. Pour $n = 1$, la somme vaut $\mu(1) = 1$. Pour $n > 1$, écrivons $n = p_1^{a_1} \cdots p_r^{a_r}$ avec $r \geq 1$. Un diviseur d de n contribue $\mu(d) \neq 0$ uniquement si d est sans facteur carré, c'est-à-dire si d est un produit de premiers distincts choisis parmi $p_1, \ldots, p_r$. Donc

$$\sum_{d \mid n} \mu(d) = \sum_{S \subseteq \{p_1, \ldots, p_r\}} (-1)^{|S|} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0.$$

On a utilisé le binôme de Newton. Ceci achève la preuve. □

Exemple 8.16. (a) $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$.

(b) $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$.

(c) $\mu(12) = \mu(2^2 \cdot 3) = 0$ car $4 \mid 12$.

(d) $\sum_{d \mid 6} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(6) = 1 + (-1) + (-1) + 1 = 0$. ✓

8.5 La fonction de Liouville $\lambda(n)$

Définition 8.17 (Fonction de Liouville)**.** La *fonction de Liouville* est définie par $\lambda(n) = (-1)^{\Omega(n)}$, où $\Omega(n)$ est le nombre total de facteurs premiers de n comptés avec multiplicité.

Proposition 8.18. *(i) La fonction λ est complètement multiplicative.*

(ii) Pour tout $n \geq 1$, $\displaystyle\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n \text{ est un carré parfait,} \\ 0 & \text{sinon.} \end{cases}$

Démonstration. (i) $\Omega(mn) = \Omega(m) + \Omega(n)$, donc $\lambda(mn) = (-1)^{\Omega(m)+\Omega(n)} = \lambda(m)\lambda(n)$.

(ii) La somme est multiplicative en n. Pour $n = p^a$: $\sum_{k=0}^{a} \lambda(p^k) = \sum_{k=0}^{a} (-1)^k = \frac{1-(-1)^{a+1}}{2}$, qui vaut 1 si a est pair et 0 si a est impair. Le résultat suit par multiplicativité. □

8.6 La fonction de von Mangoldt $\Lambda(n)$

Définition 8.19 (Fonction de von Mangoldt)**.** La *fonction de von Mangoldt* est définie par

$$\Lambda(n) = \begin{cases} \ln p & \text{si } n = p^k \text{ pour un premier } p \text{ et un entier } k \geq 1, \\ 0 & \text{sinon.} \end{cases}$$

Proposition 8.20. *Pour tout $n \geq 1$, on a*

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

Démonstration. Soit $n = p_1^{a_1} \cdots p_r^{a_r}$. Les diviseurs d de n pour lesquels $\Lambda(d) \neq 0$ sont de la forme p_i^j avec $1 \leq j \leq a_i$. Donc

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{j=1}^{a_i} \ln p_i = \sum_{i=1}^{r} a_i \ln p_i = \ln\left(\prod_{i=1}^{r} p_i^{a_i}\right) = \ln n. \qquad \square$$

Remarque 8.21. La fonction de von Mangoldt joue un rôle central en théorie analytique des nombres. La *fonction de Tchébychev* $\psi(x) = \sum_{n \leq x} \Lambda(n)$ est liée à la distribution des nombres premiers : le théorème des nombres premiers est équivalent à $\psi(x) \sim x$ quand $x \to +\infty$.

8.7 Le produit de Dirichlet

Définition 8.22 (Produit de Dirichlet)**.** Le *produit de Dirichlet* (ou *convolution de Dirichlet*) de deux fonctions arithmétiques f et g est la fonction arithmétique $f * g$ définie par

$$(f * g)(n) = \sum_{d|n} f(d)\, g\Big(\frac{n}{d}\Big) = \sum_{\substack{ab=n \\ a,b\geq 1}} f(a)\, g(b).$$

Notation 8.23. On introduit les fonctions arithmétiques suivantes :

$$\begin{aligned}
\varepsilon(n) = [n=1] &= \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{sinon,} \end{cases} && \text{(identité de Dirichlet),} \\
\mathbf{1}(n) &= 1 \quad \text{pour tout } n, && \text{(fonction constante 1),} \\
\mathrm{id}(n) &= n, && \text{(fonction identité),} \\
\mathrm{id}_k(n) &= n^k. &&
\end{aligned}$$

Théorème 8.24 (Structure d'anneau)**.** *L'ensemble des fonctions arithmétiques, muni de l'addition ponctuelle et du produit de Dirichlet $*$, forme un anneau commutatif unitaire dont :*

(i) le zéro est la fonction nulle,

(ii) l'unité est ε,

(iii) le produit $*$ est associatif et commutatif.

Démonstration. La commutativité est immédiate par le changement $d \mapsto n/d$. Pour l'associativité :

$$\begin{aligned}
((f*g)*h)(n) &= \sum_{d|n} (f*g)(d)\, h\Big(\frac{n}{d}\Big) = \sum_{d|n} \sum_{e|d} f(e)\, g\Big(\frac{d}{e}\Big)\, h\Big(\frac{n}{d}\Big) \\
&= \sum_{abc=n} f(a)\, g(b)\, h(c) = (f*(g*h))(n).
\end{aligned}$$

La propriété $f * \varepsilon = f$ est claire : $(f*\varepsilon)(n) = \sum_{d|n} f(d)\,\varepsilon(n/d) = f(n)$ car $\varepsilon(n/d) = 0$ sauf pour $d = n$. □

Les résultats des sections précédentes se réexpriment élégamment :

Proposition 8.25 (Identités de convolution)**.** *(i)* $\mathbf{1} * \mathbf{1} = \tau$ *(car* $\sum_{d|n} 1 = \tau(n)$*).*

(ii) $\mathrm{id} * \mathbf{1} = \sigma$ *(car* $\sum_{d|n} d = \sigma(n)$*).*

(iii) $\varphi * \mathbf{1} = \mathrm{id}$ *(identité de Gauss, théorème 8.6).*

(iv) $\mu * \mathbf{1} = \varepsilon$ *(propriété fondamentale de μ, théorème 8.15).*

(v) $\Lambda * \mathbf{1} = \ln$ *(proposition 8.20).*

Théorème 8.26 (Inversibilité). *Une fonction arithmétique f admet un inverse pour le produit de Dirichlet si et seulement si $f(1) \neq 0$. L'inverse f^{-1} est défini récursivement par*

$$f^{-1}(1) = \frac{1}{f(1)}, \qquad f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d \mid n \\ d<n}} f\Big(\frac{n}{d}\Big)\, f^{-1}(d) \quad \text{pour } n > 1.$$

Démonstration. La condition $f * f^{-1} = \varepsilon$ donne, pour $n = 1$: $f(1)f^{-1}(1) = 1$, d'où la nécessité de $f(1) \neq 0$ et la valeur de $f^{-1}(1)$. Pour $n > 1$: $(f * f^{-1})(n) = 0$ donne $\sum_{d \mid n} f(n/d)\, f^{-1}(d) = 0$, soit $f(1)f^{-1}(n) + \sum_{\substack{d \mid n \\ d<n}} f(n/d)\, f^{-1}(d) = 0$, d'où la formule récursive. □

Corollaire 8.27. *La fonction de Möbius μ est l'inverse de Dirichlet de $\mathbf{1}$: $\mu * \mathbf{1} = \varepsilon$, c'est-à-dire $\mu = \mathbf{1}^{-1}$.*

Proposition 8.28 (Produit de fonctions multiplicatives). *Si f et g sont multiplicatives, alors $f * g$ est multiplicative.*

Démonstration. Soient m, n avec $\gcd(m, n) = 1$. Tout diviseur d de mn s'écrit de manière unique $d = d_1 d_2$ avec $d_1 \mid m$ et $d_2 \mid n$ (et $\gcd(d_1, d_2) = 1$). Donc

$$\begin{aligned}
(f * g)(mn) &= \sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2)\, g\Big(\frac{m}{d_1} \cdot \frac{n}{d_2}\Big) \\
&= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) f(d_2)\, g\Big(\frac{m}{d_1}\Big)\, g\Big(\frac{n}{d_2}\Big) \\
&= \Big(\sum_{d_1 \mid m} f(d_1)\, g\Big(\frac{m}{d_1}\Big)\Big) \Big(\sum_{d_2 \mid n} f(d_2)\, g\Big(\frac{n}{d_2}\Big)\Big) \\
&= (f * g)(m)\,(f * g)(n).
\end{aligned}$$

□

8.7.1 Visualisation : treillis des diviseurs

8.8 La formule d'inversion de Möbius

Théorème 8.29 (Inversion de Möbius). *Soient f et g deux fonctions arithmétiques. On a l'équivalence :*

$$g(n) = \sum_{d \mid n} f(d) \quad \text{pour tout } n \geq 1 \qquad \Longleftrightarrow \qquad f(n) = \sum_{d \mid n} \mu(d)\, g\Big(\frac{n}{d}\Big) \quad \text{pour tout } n \geq 1.$$

Autrement dit : $g = f * \mathbf{1} \;\Leftrightarrow\; f = g * \mu = \mu * g$.

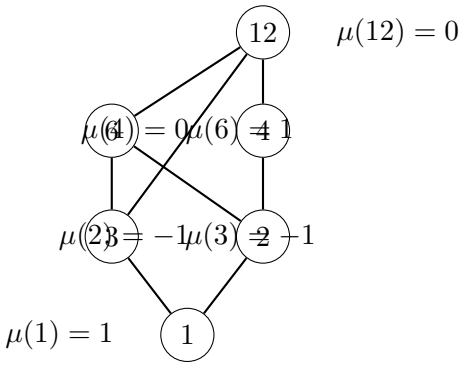


FIGURE 8.1 – Treillis des diviseurs de 12 avec les valeurs de μ. On vérifie $\sum_{d|12} \mu(d) = 1 + (-1) + (-1) + 0 + 1 + 0 = 0$.

Produit de Dirichlet $(f * g)(12)$

$f(1)$	$\times$	$g(12)$	$=$	$f(1)\,g(12)$	$\Big\}$
$f(2)$	$\times$	$g(6)$	$=$	$f(2)\,g(6)$	
$f(3)$	$\times$	$g(4)$	$=$	$f(3)\,g(4)$	
$f(4)$	$\times$	$g(3)$	$=$	$f(4)\,g(3)$	
$f(6)$	$\times$	$g(2)$	$=$	$f(6)\,g(2)$	
$f(12)$	$\times$	$g(1)$	$=$	$f(12)\,g(1)$	$\Big\}$

$\sum$

FIGURE 8.2 – Schéma du calcul de $(f * g)(12) = \sum_{d|12} f(d)\, g(12/d)$.

Démonstration. Sens direct ($\Rightarrow$). Supposons $g = f * \mathbf{1}$. Alors

$$\begin{aligned}(\mu * g)(n) &= \sum_{d|n} \mu(d)\, g\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{e|(n/d)} f(e) \\ &= \sum_{e|n} f(e) \sum_{\substack{d|n \\ e|(n/d)}} \mu(d) = \sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d).\end{aligned}$$

Par le théorème 8.15, $\sum_{d|(n/e)} \mu(d) = [n/e = 1] = [e = n]$. Donc $(\mu * g)(n) = f(n)$.

Sens réciproque ($\Leftarrow$). Supposons $f = \mu * g$. Alors

$$\begin{aligned}(f * \mathbf{1})(n) &= \sum_{d|n} f(d) = \sum_{d|n} (\mu * g)(d) = \sum_{d|n} \sum_{e|d} \mu(e)\, g\Big(\frac{d}{e}\Big) \\ &= \sum_{e|n} \mu(e) \sum_{\substack{d|n \\ e|d}} g\Big(\frac{d}{e}\Big) = \sum_{e|n} \mu(e) \sum_{k|(n/e)} g(k).\end{aligned}$$

Posant $h(m) = \sum_{k|m} g(k) = (g * \mathbf{1})(m)$, cela vaut $\sum_{e|n} \mu(e)\, h(n/e) = (\mu * h)(n) = (\mu * g * \mathbf{1})(n)$. Or $\mu * \mathbf{1} = \varepsilon$, donc par associativité, $\mu * g * \mathbf{1} = g * (\mu * \mathbf{1}) = g * \varepsilon = g$. Donc $(f * \mathbf{1})(n) = g(n)$. □

8.8.1 Applications de l'inversion de Möbius

Corollaire 8.30 (Formule de φ par inversion)**.** *On a $\varphi = \mu * \mathrm{id}$, c'est-à-dire*

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

Démonstration. L'identité de Gauss (théorème 8.6) s'écrit $\mathrm{id} = \varphi * \mathbf{1}$. Par inversion de Möbius, $\varphi = \mu * \mathrm{id}$. □

Exemple 8.31. Calculons $\varphi(12)$ par la formule d'inversion :

$$\begin{aligned}\varphi(12) &= \sum_{d|12} \mu(d) \cdot \frac{12}{d} \\ &= \mu(1)\cdot 12 + \mu(2)\cdot 6 + \mu(3)\cdot 4 + \mu(4)\cdot 3 + \mu(6)\cdot 2 + \mu(12)\cdot 1 \\ &= 1\cdot 12 + (-1)\cdot 6 + (-1)\cdot 4 + 0\cdot 3 + 1\cdot 2 + 0\cdot 1 = 12 - 6 - 4 + 2 = 4.\end{aligned}$$

Corollaire 8.32 (Formule de Λ par inversion)**.** *On a $\Lambda = \mu * (-\ln)$, c'est-à-dire, en écrivant $L(n) = \ln n$: $L = \Lambda * \mathbf{1}$ implique $\Lambda = \mu * L$, soit*

$$\Lambda(n) = -\sum_{d|n} \mu(d) \ln d = \sum_{d|n} \mu(d) \ln \frac{n}{d}.$$

8.8.2 Forme sommatoire de l'inversion de Möbius

Théorème 8.33 (Inversion de Möbius – forme sommatoire)**.** *Soient $f, g : \mathbb{N}^* \to \mathbb{C}$. On a l'équivalence :*

$$g(x) = \sum_{n \le x} f\left(\lfloor * \rfloor \frac{x}{n}\right) \qquad \Longleftrightarrow \qquad f(x) = \sum_{n \le x} \mu(n)\, g\left(\lfloor * \rfloor \frac{x}{n}\right).$$

Plus généralement, si $G(x) = \sum_{n\le x} f(n)$ et $H(x) = \sum_{n \le x} g(n)$ avec $g = f * \mathbf{1}$, alors

$$F(x) = \sum_{n \le x} f(n) = \sum_{n \le x} \mu(n)\, H\left(\frac{x}{n}\right).$$

8.9 Introduction aux séries de Dirichlet

Définition 8.34 (Série de Dirichlet)**.** À toute fonction arithmétique f, on associe la *série de Dirichlet*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad s \in \mathbb{C}.$$

Théorème 8.35 (Produit d'Euler)**.** *Si f est multiplicative et la série $F(s)$ converge absolument, alors*

$$F(s) = \prod_{p \text{ premier}} \left(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right).$$

Si f est complètement multiplicative, cela se simplifie en

$$F(s) = \prod_{p \text{ premier}} \frac{1}{1 - f(p)\, p^{-s}}.$$

Exemple 8.36 (Séries de Dirichlet classiques)**.** (a) La *fonction zêta de Riemann* :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}} \text{ pour } \Re(s) > 1.$$

(b) $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$ pour $\Re(s) > 1$.

(c) $\displaystyle\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$ pour $\Re(s) > 2$.

(d) $\displaystyle\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2$ pour $\Re(s) > 1$.

(e) $\displaystyle\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s)\,\zeta(s-1)$ pour $\Re(s) > 2$.

Remarque 8.37. Le produit de Dirichlet $f * g$ correspond au *produit* des séries de Dirichlet : si $F(s) = \sum f(n)/n^s$ et $G(s) = \sum g(n)/n^s$, alors $F(s) \cdot G(s) = \sum (f * g)(n)/n^s$, dans la zone de convergence absolue commune. Cela justifie par exemple $\mu * \mathbf{1} = \varepsilon \Leftrightarrow 1/\zeta(s) \cdot \zeta(s) = 1$.

8.10 Tableau récapitulatif

Fonction	**Définition**	**Mult.**	**Série de Dirichlet**
$\varepsilon(n) = [n = 1]$	identité de $*$	oui	1
$\mathbf{1}(n) = 1$	constante	comp. mult.	$\zeta(s)$
$\mathrm{id}(n) = n$	identité	comp. mult.	$\zeta(s-1)$
$\mu(n)$	Möbius	mult.	$1/\zeta(s)$
$\varphi(n)$	Euler	mult.	$\zeta(s-1)/\zeta(s)$
$\tau(n) = \sigma_0(n)$	nb. de diviseurs	mult.	$\zeta(s)^2$
$\sigma(n) = \sigma_1(n)$	somme des diviseurs	mult.	$\zeta(s)\zeta(s-1)$
$\lambda(n)$	Liouville	comp. mult.	$\zeta(2s)/\zeta(s)$
$\Lambda(n)$	von Mangoldt	non	$-\zeta'(s)/\zeta(s)$

8.11 Exemples de calcul

Exemple 8.38 (Calcul complet pour $n = 60$)**.** Soit $n = 60 = 2^2 \cdot 3 \cdot 5$.

(a) $\varphi(60) = 60(1-1/2)(1-1/3)(1-1/5) = 60 \cdot 1/2 \cdot 2/3 \cdot 4/5 = 16$.

(b) $\tau(60) = (2+1)(1+1)(1+1) = 12$.

(c) $\sigma(60) = \frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 4 \cdot 6 = 168$.

(d) $\mu(60) = 0$ car $4 \mid 60$.

(e) $\lambda(60) = (-1)^{2+1+1} = (-1)^4 = 1$.

(f) $\Lambda(60) = 0$ car 60 n'est pas une puissance de premier.

Vérification : $\sum_{d \mid 60} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(12) + \varphi(15) + \varphi(20) + \varphi(30) + \varphi(60) = 1 + 1 + 2 + 2 + 4 + 2 + 4 + 4 + 8 + 8 + 8 + 16 = 60$. ✓

Exemple 8.39 (Identités via convolution)**.** (a) De $\varphi * \mathbf{1} = \mathrm{id}$ et $\mu * \mathbf{1} = \varepsilon$, on déduit : $\varphi = \mathrm{id} * \mu$, puis $\sigma = \mathrm{id} * \mathbf{1}$, d'où $\sigma * \mu = \mathrm{id} * \mathbf{1} * \mu = \mathrm{id} * \varepsilon = \mathrm{id}$. Conclusion : $\sum_{d \mid n} \mu(d)\, \sigma(n/d) = n$.

(b) De $\tau = \mathbf{1} * \mathbf{1}$, on obtient $\tau * \mu = \mathbf{1} * \mathbf{1} * \mu = \mathbf{1}$, soit $\sum_{d \mid n} \mu(d)\, \tau(n/d) = 1$ pour tout $n \geq 1$.

Exemple 8.40 (Application : polynômes cyclotomiques)**.** Le n-ième polynôme cyclotomique s'exprime par inversion de Möbius :

$$\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}.$$

En effet, $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$, et l'inversion de Möbius multiplicative donne la formule ci-dessus.

8.12 Exercices

Exercice 8.1 ($\star$)**.** Calculer $\varphi(n), \tau(n), \sigma(n), \mu(n)$ et $\lambda(n)$ pour $n \in \{36, 72, 100, 105, 210, 360\}$.

Exercice 8.2 ($\star$)**.** Vérifier l'identité $\sum_{d\mid n} \varphi(d) = n$ pour $n = 24$ et $n = 30$.

Exercice 8.3 ($\star$)**.** Calculer le produit de Dirichlet $(\mu * \mathrm{id})(n)$ pour $n = 1, 2, \ldots, 10$ et vérifier que l'on obtient $\varphi(n)$.

Exercice 8.4 ($\star\star$)**.** Montrer que $\varphi(n)$ est pair pour tout $n \geq 3$.

Exercice 8.5 ($\star\star$)**.** Démontrer directement (sans utiliser les séries de Dirichlet) que σ est multiplicative.

Exercice 8.6 ($\star\star$)**.** Montrer que $\sum_{d\mid n} \mu(d)^2 = 2^{\omega(n)}$ où $\omega(n)$ est le nombre de facteurs premiers distincts de n.

Exercice 8.7 ($\star\star$)**.** Montrer que $\sum_{d\mid n} |\mu(d)| \cdot \varphi(n/d) = n \prod_{p\mid n} \frac{2}{p+1} \cdot \frac{p+1}{1} \cdot \frac{1}{1}$. Plus précisément, montrer que $\mu^2 * \varphi = \mathrm{id} \cdot$ (une fonction multiplicative), et identifier cette fonction. *Indication : évaluer les deux côtés sur les puissances de premiers.*

Exercice 8.8 ($\star\star$)**.** En utilisant l'identité $\ln n = \sum_{d\mid n} \Lambda(d)$, exprimer la fonction de von Mangoldt $\Lambda(n)$ comme somme impliquant μ et $\ln$.

Exercice 8.9 ($\star\star$)**.** Soit $Q(x) = \#\{n \leq x : n \text{ est sans facteur carré}\}$. Montrer que $Q(x) = \sum_{d \leq \sqrt{x}} \mu(d) \lfloor x/d^2 \rfloor$. *Indication : utiliser* $\mu^2(n) = \sum_{d^2\mid n} \mu(d)$.

Exercice 8.10 ($\star\star\star$)**.** Soit $M(x) = \sum_{n\leq x} \mu(n)$ la fonction de Mertens.

(a) Montrer que $\sum_{n\leq x} M(\lfloor x/n \rfloor) = 1$ pour tout $x \geq 1$.

(b) En admettant le théorème des nombres premiers sous la forme $\psi(x) \sim x$, montrer que $M(x) = o(x)$.

Exercice 8.11 ($\star\star\star$)**.** (a) Montrer que pour $\Re(s) > 1$, le produit d'Euler $\prod_p (1 - p^{-s})^{-1}$ converge et vaut $\zeta(s)$.

(b) En déduire que $\sum_{n=1}^{\infty} \mu(n)/n^s = 1/\zeta(s)$ pour $\Re(s) > 1$.

(c) Montrer que $\zeta(s)$ a un pôle simple en $s = 1$ avec résidu 1, et interpréter en termes de densité des nombres premiers.

Exercice 8.12 ($\star\star\star$)**.** La *somme de Ramanujan* est $c_q(n) = \sum_{\substack{a=1 \\ \mathrm{pgcd}(a,q)=1}}^{q} e^{2\pi i a n/q}$. Montrer que $c_q(n) = \sum_{d\mid \mathrm{pgcd}(q,n)} d\,\mu(q/d)$.

Résumé du chapitre

1. Une **fonction arithmétique** est une application $f : \mathbb{N}^* \to \mathbb{C}$. Elle est **multiplicative** si $f(mn) = f(m)f(n)$ pour $\mathrm{pgcd}(m, n) = 1$.
2. L'**indicatrice d'Euler** satisfait $\varphi(n) = n \prod_{p\mid n}(1 - 1/p)$ et $\sum_{d\mid n} \varphi(d) = n$.
3. La **fonction de Möbius** satisfait $\sum_{d\mid n} \mu(d) = [n = 1]$ et est l'inverse de Dirichlet de $\mathbf{1}$.
4. Le **produit de Dirichlet** $(f * g)(n) = \sum_{d\mid n} f(d)\, g(n/d)$ munit les fonctions arithmétiques d'une structure d'anneau commutatif unitaire, d'identité ε.

5. La **formule d'inversion de Möbius** stipule que $g = f * \mathbf{1} \Leftrightarrow f = g * \mu$.
6. Les **séries de Dirichlet** $F(s) = \sum f(n)/n^s$ transforment la convolution de Dirichlet en produit ordinaire, et admettent un **produit d'Euler** lorsque f est multiplicative.
7. La fonction ζ de Riemann, les fonctions τ, σ, φ, μ, λ, Λ forment un réseau d'identités reliées par le produit de Dirichlet.

Chapitre 9

Introduction aux Nombres p-adiques

« Les nombres p-adiques ne sont pas un simple artifice technique ;
ils révèlent une géométrie arithmétique invisible dans $\mathbb{Q}$. »
— Kurt Hensel (1861–1941)

9.1 Introduction historique

En 1897, Kurt Hensel introduisit les nombres p-adiques dans le but d'appliquer les méthodes de la théorie des séries de puissances à la théorie des nombres. L'idée fondamentale est la suivante : de même que les nombres réels $\mathbb{R}$ s'obtiennent en complétant $\mathbb{Q}$ par rapport à la valeur absolue usuelle $|\cdot|$, on peut compléter $\mathbb{Q}$ par rapport à d'autres distances, indexées par les nombres premiers p. Chaque complétion produit un corps $\mathbb{Q}_p$ radicalement différent de $\mathbb{R}$, mais tout aussi fondamental pour la compréhension de l'arithmétique.

Cette construction offre un point de vue *local* sur les propriétés des nombres : résoudre une équation dans $\mathbb{Q}_p$ revient à analyser sa solubilité « modulo les puissances de p ». Le *principe local-global* affirme que, pour certaines classes d'équations, la solubilité dans $\mathbb{Q}$ équivaut à la solubilité simultanée dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$.

9.2 Valuation p-adique

Définition 9.1 (Valuation p-adique sur $\mathbb{Z}$)**.** Soit p un nombre premier. Pour tout entier $n \in \mathbb{Z} \setminus \{0\}$, la *valuation p-adique* de n, notée $v_p(n)$, est le plus grand entier $k \geq 0$ tel que $p^k \mid n$. Autrement dit,

$$v_p(n) = \max\bigl\{k \in \mathbb{N} : p^k \mid n\bigr\}.$$

Par convention, on pose $v_p(0) = +\infty$.

Exemple 9.2 (Calculs de valuations)**.** (i) $v_2(12) = v_2(2^2 \cdot 3) = 2$, $v_3(12) = 1$, $v_5(12) = 0$.

(ii) $v_3(81) = v_3(3^4) = 4$.

(iii) $v_7(2401) = v_7(7^4) = 4$.

(iv) $v_2(1000) = v_2(2^3 \cdot 125) = 3, \quad v_5(1000) = 3.$

Définition 9.3 (Valuation p-adique sur $\mathbb{Q}$)**.** On étend v_p à $\mathbb{Q}^*$ en posant, pour $r = a/b$ avec $a, b \in \mathbb{Z}$, $b \neq 0$:

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Cette définition ne dépend pas du représentant choisi pour la fraction.

Proposition 9.4 (Propriétés de la valuation p-adique)**.** *Pour tout $x, y \in \mathbb{Q}^*$, on a :*

(i) $v_p(xy) = v_p(x) + v_p(y)$ *(morphisme multiplicatif) ;*

(ii) $v_p(x+y) \geq \min\big(v_p(x), v_p(y)\big)$*, avec égalité si* $v_p(x) \neq v_p(y)$.

Démonstration. (i) Soient $x = p^a \cdot u$ et $y = p^b \cdot w$ avec $\gcd(u,p) = \gcd(w,p) = 1$. Alors $xy = p^{a+b} \cdot uw$, et $\gcd(uw,p) = 1$, d'où $v_p(xy) = a + b = v_p(x) + v_p(y)$.

(ii) Écrivons $x = p^a \cdot u/v$ et $y = p^b \cdot r/s$ sous forme réduite, avec $a = v_p(x)$, $b = v_p(y)$. Supposons $a \leq b$. Alors

$$x + y = p^a \left(\frac{u}{v} + p^{b-a} \cdot \frac{r}{s}\right),$$

d'où $v_p(x+y) \geq a = \min(v_p(x), v_p(y))$. Si $a < b$, le terme entre parenthèses a valuation 0, d'où l'égalité. □

Remarque 9.5. La décomposition en facteurs premiers de tout $n \in \mathbb{Z} \setminus \{0\}$ se lit directement sur les valuations :

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

où le produit est fini car $v_p(n) = 0$ pour presque tout p.

9.3 Valeur absolue p-adique

Définition 9.6 (Valeur absolue p-adique)**.** Pour $x \in \mathbb{Q}$, on définit la *valeur absolue p-adique* par

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases}$$

Exemple 9.7. (i) $|12|_3 = 3^{-v_3(12)} = 3^{-1} = 1/3$.

(ii) $|75|_5 = 5^{-v_5(75)} = 5^{-2} = 1/25$.

(iii) $|1/7|_7 = 7^{-v_7(1/7)} = 7^{-(-1)} = 7$.

(iv) Pour $\gcd(n,p) = 1$: $|n|_p = 1$.

Théorème 9.8 (Propriétés de $|\cdot|_p$). *L'application* $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ *vérifie :*

(i) ***Positivité :*** $|x|_p = 0 \iff x = 0$;

(ii) ***Multiplicativité :*** $|xy|_p = |x|_p \cdot |y|_p$;

(iii) ***Inégalité ultramétrique :*** $|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$.

Démonstration. Les points (i) et (ii) découlent directement des propriétés de v_p.

Pour (iii), si $x = 0$ ou $y = 0$, c'est immédiat. Sinon :

$$\begin{aligned} |x+y|_p &= p^{-v_p(x+y)} \\ &\leq p^{-\min(v_p(x),\, v_p(y))} \quad \text{(par la Proposition 9.4)} \\ &= \max\big(p^{-v_p(x)},\, p^{-v_p(y)}\big) \\ &= \max\big(|x|_p,\, |y|_p\big). \end{aligned}$$

□

Remarque 9.9 (Conséquence de l'ultramétricité). L'inégalité ultramétrique est *plus forte* que l'inégalité triangulaire usuelle :

$$|x+y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p .$$

Cela entraîne des propriétés géométriques surprenantes : dans un espace ultramétrique, tout triangle est isocèle, et toute boule ouverte est aussi fermée.

Proposition 9.10 (Formule du produit). *Pour tout* $x \in \mathbb{Q}^*$,

$$|x|_\infty \cdot \prod_{p \text{ premier}} |x|_p = 1,$$

où $|\cdot|_\infty$ *désigne la valeur absolue usuelle sur* $\mathbb{Q}$.

Démonstration. Il suffit de vérifier pour $x = \pm p_1^{a_1} \cdots p_k^{a_k}$. On a $|x|_\infty = p_1^{a_1} \cdots p_k^{a_k}$ et $|x|_{p_i} = p_i^{-a_i}$ pour chaque i, tandis que $|x|_q = 1$ pour tout premier $q \notin \{p_1, \ldots, p_k\}$. Le produit vaut donc $p_1^{a_1} \cdots p_k^{a_k} \cdot p_1^{-a_1} \cdots p_k^{-a_k} = 1$. □

9.4 Métrique p-adique et convergence

Définition 9.11 (Distance p-adique). La *distance p-adique* sur $\mathbb{Q}$ est définie par

$$d_p(x, y) = |x - y|_p \quad \text{pour tout } x, y \in \mathbb{Q}.$$

Le couple $(\mathbb{Q}, d_p)$ est un espace métrique (ultramétrique).

Exemple 9.12 (Convergence p-adique). Dans $(\mathbb{Q}, d_5)$, la suite (a_n) définie par $a_n =$

$\sum_{k=0}^{n} 5^k$ converge, car $|a_{n+1} - a_n|_5 = |5^{n+1}|_5 = 5^{-(n+1)} \to 0$. En fait,

$$\sum_{k=0}^{\infty} 5^k = \frac{1}{1-5} = -\frac{1}{4}$$

dans $\mathbb{Q}_5$. La série géométrique converge pour $|5|_5 = 1/5 < 1$.

Remarque 9.13. Dans un espace ultramétrique, si $|x|_p \neq |y|_p$, alors $|x+y|_p = \max(|x|_p, |y|_p)$. Géométriquement : dans tout triangle p-adique, les deux plus grands côtés sont égaux.

9.5 Entiers p-adiques et corps $\mathbb{Q}_p$

Définition 9.14 (Corps $\mathbb{Q}_p$ des nombres p-adiques)**.** Le corps $\mathbb{Q}_p$ est le complété de $\mathbb{Q}$ par rapport à la distance d_p. C'est un corps valué complet contenant $\mathbb{Q}$ comme sous-corps dense.

Définition 9.15 (Anneau $\mathbb{Z}_p$ des entiers p-adiques)**.** L'anneau des *entiers p-adiques* est

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

C'est un anneau local d'idéal maximal $p\mathbb{Z}_p$.

Proposition 9.16 (Représentation en série)**.** *Tout élément $x \in \mathbb{Z}_p$ s'écrit de manière unique sous la forme*

$$x = \sum_{i=0}^{\infty} a_i\, p^i, \quad a_i \in \{0, 1, \ldots, p-1\}.$$

Plus généralement, tout $x \in \mathbb{Q}_p^*$ s'écrit

$$x = \sum_{i=v_p(x)}^{\infty} a_i\, p^i, \quad a_i \in \{0, 1, \ldots, p-1\}, \quad a_{v_p(x)} \neq 0.$$

Exemple 9.17 (Calculs dans $\mathbb{Z}_5$)**.** Représentons -1 dans $\mathbb{Z}_5$. On cherche $x = \sum a_i \cdot 5^i$ tel que $x + 1 = 0$. On a $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$, soit

$$-1 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots = \sum_{i=0}^{\infty} 4 \cdot 5^i.$$

Vérification : $1 + (4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots) = 5 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots = 5(1 + 4 + 4 \cdot 5 + \cdots)$. En itérant, tous les chiffres s'annulent, donnant 0.

Exemple 9.18 (Représentation de $1/3$ dans $\mathbb{Z}_5$)**.** On cherche $x \in \mathbb{Z}_5$ tel que $3x = 1$. On résout par développement successif : $3a_0 \equiv 1 \pmod 5$ donne $a_0 = 2$. Puis $3(2 + a_1 \cdot 5 + \cdots) = 1$, soit $6 + 3a_1 \cdot 5 + \cdots = 1$, d'où $(6-1)/5 = 1$ et $3a_1 \equiv -1 \pmod 5$, soit $a_1 = 3$. En continuant :

$$\frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots$$

Les chiffres alternent périodiquement entre 3 et 1 (après le premier terme).

Proposition 9.19 (Structure de $\mathbb{Z}_p$)**.** *(i)* $\mathbb{Z}_p$ *est un anneau intègre, local, principal.*

(ii) Les idéaux de $\mathbb{Z}_p$ *sont exactement les* $p^n\mathbb{Z}_p$ *pour* $n \geq 0$*, et l'idéal nul.*

(iii) $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ *pour tout* $n \geq 1$*.*

(iv) $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p$*.*

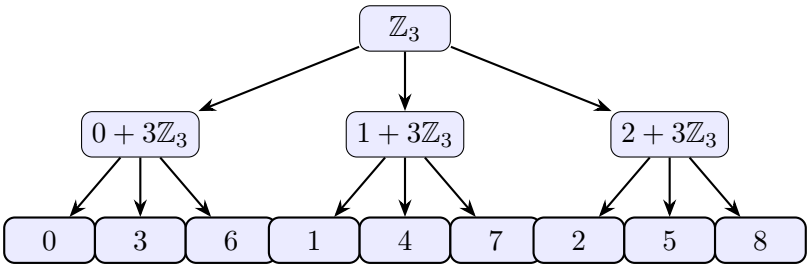


FIGURE 9.1 – Arbre des classes de $\mathbb{Z}_3$ modulo 3 et 9 : chaque élément de $\mathbb{Z}_3$ est déterminé par ses chiffres successifs en base 3.

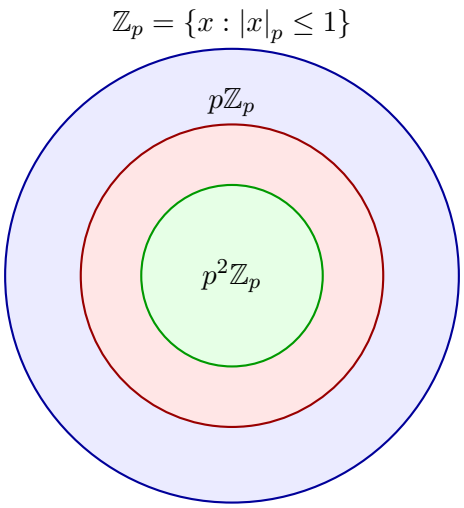


FIGURE 9.2 – Structure emboîtée des disques p-adiques : $\cdots \subset p^2\mathbb{Z}_p \subset p\mathbb{Z}_p \subset \mathbb{Z}_p$.

9.6 Lemme de Hensel

Le lemme de Hensel est l'analogue p-adique du théorème des fonctions implicites : il permet de « relever » une solution approchée en une solution exacte.

Théorème 9.20 (Lemme de Hensel). *Soit $f(x) \in \mathbb{Z}_p[x]$ un polynôme à coefficients dans $\mathbb{Z}_p$. Supposons qu'il existe $a_0 \in \mathbb{Z}_p$ tel que*

$$v_p\big(f(a_0)\big) > 2\, v_p\big(f'(a_0)\big).$$

Alors il existe un unique $a \in \mathbb{Z}_p$ tel que $f(a) = 0$ et $|a - a_0|_p \leq |f(a_0)/f'(a_0)^2|_p^{1/2}$.

Preuve (cas simple : $f'(a_0) \not\equiv 0 \pmod p$). On suppose $v_p(f'(a_0)) = 0$ (c'est-à-dire $f'(a_0) \in \mathbb{Z}_p^\times$) et $v_p(f(a_0)) \geq 1$. On construit une suite (a_n) par la méthode de Newton p-adique :

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

Étape 1 : Bonne définition. Puisque $f'(a_0) \in \mathbb{Z}_p^\times$, la division est bien définie dans $\mathbb{Q}_p$.

Étape 2 : Convergence quadratique. Par le développement de Taylor dans $\mathbb{Z}_p[x]$:

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + c(a_{n+1} - a_n)^2$$

pour un certain $c \in \mathbb{Z}_p$. Or $a_{n+1} - a_n = -f(a_n)/f'(a_n)$, d'où

$$f(a_{n+1}) = f(a_n) - f(a_n) + c \cdot \frac{f(a_n)^2}{f'(a_n)^2} = c \cdot \frac{f(a_n)^2}{f'(a_n)^2}.$$

Ainsi $v_p(f(a_{n+1})) \geq 2\, v_p(f(a_n))$, ce qui donne la convergence quadratique $v_p(f(a_n)) \geq 2^n$.

Étape 3 : $f'(a_n) \in \mathbb{Z}_p^\times$ pour tout n. On montre par récurrence que $a_{n+1} \equiv a_n \pmod p$, d'où $f'(a_{n+1}) \equiv f'(a_n) \pmod p$ et $v_p(f'(a_n)) = 0$ pour tout n.

Étape 4 : Convergence et unicité. La suite (a_n) est de Cauchy dans $\mathbb{Z}_p$ (car $|a_{n+1} - a_n|_p \to 0$), donc elle converge vers un $a \in \mathbb{Z}_p$ vérifiant $f(a) = 0$. L'unicité dans le disque considéré découle de l'estimation. □

Corollaire 9.21 (Version modulo p). *Si $f(x) \in \mathbb{Z}[x]$ et $a_0 \in \mathbb{Z}$ vérifient $f(a_0) \equiv 0 \pmod p$ et $f'(a_0) \not\equiv 0 \pmod p$, alors il existe $a \in \mathbb{Z}_p$ tel que $f(a) = 0$ et $a \equiv a_0 \pmod p$.*

9.7 Applications du lemme de Hensel

9.7.1 Résolution de $x^2 = -1$ dans $\mathbb{Q}_5$

Exemple 9.22 ($x^2 + 1 = 0$ dans $\mathbb{Q}_5$)**.** Cherchons $x \in \mathbb{Z}_5$ tel que $x^2 = -1$.
Étape 1 : Solution modulo 5. On vérifie $2^2 = 4 \equiv -1 \pmod 5$. Prenons $a_0 = 2$.
Étape 2 : Vérification des hypothèses de Hensel. Soit $f(x) = x^2+1$. On a $f(2) = 5 \equiv 0 \pmod 5$ et $f'(2) = 4 \not\equiv 0 \pmod 5$.
Étape 3 : Application du lemme de Hensel (Corollaire 9.21). Il existe $a \in \mathbb{Z}_5$ tel que $a^2 = -1$ et $a \equiv 2 \pmod 5$.
Relèvement explicite : On cherche a_1 tel que $a_1 \equiv 2 \pmod 5$ et $a_1^2 \equiv -1 \pmod{25}$. La méthode de Newton donne

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = 2 - \frac{5}{4}.$$

Or $4^{-1} \equiv 4 \pmod 5$, donc $5/4 \equiv 5 \cdot 4 = 20 \pmod{25}$, et $a_1 = 2 - 20 = -18 \equiv 7 \pmod{25}$. Vérifions : $7^2 = 49 \equiv -1 \pmod{25}$.
On obtient les premiers chiffres : $i = 2 + 1 \cdot 5 + \cdots$ dans $\mathbb{Z}_5$, où $i^2 = -1$.

Remarque 9.23. En revanche, $x^2 = -1$ n'a pas de solution dans $\mathbb{Q}_3$, car -1 n'est pas un carré modulo 3 (les carrés modulo 3 sont $\{0, 1\}$).

9.7.2 Principe local-global

Théorème 9.24 (Hasse–Minkowski)**.** *Soit $Q(x_1, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$ une forme quadratique à coefficients dans $\mathbb{Q}$. Alors Q représente 0 dans $\mathbb{Q}$ (c'est-à-dire il existe $(x_1, \ldots, x_n) \in \mathbb{Q}^n \setminus \{0\}$ tel que $Q(x_1, \ldots, x_n) = 0$) si et seulement si Q représente 0 dans $\mathbb{R}$ et dans $\mathbb{Q}_p$ pour tout premier p.*

Remarque 9.25. Le théorème de Hasse–Minkowski ne se généralise pas aux formes de degré supérieur. Par exemple, Selmer a montré que l'équation $3x^3 + 4y^3 + 5z^3 = 0$ a des solutions non triviales dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$, mais pas dans $\mathbb{Q}$.

9.8 Théorème d'Ostrowski

Théorème 9.26 (Ostrowski)**.** *Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à la valeur absolue usuelle $|\cdot|_\infty$, soit à une valeur absolue p-adique $|\cdot|_p$ pour un certain nombre premier p.*

Remarque 9.27. Ce théorème signifie que les « places » de $\mathbb{Q}$ — c'est-à-dire les classes d'équivalence de valeurs absolues non triviales — sont naturellement indexées par $\{2, 3, 5, 7, 11, \ldots\} \cup \{\infty\}$. Chaque complétion correspondante donne soit $\mathbb{R}$ (pour ∞),

soit $\mathbb{Q}_p$ (pour le premier p).

9.9 Exemples détaillés

Exemple 9.28 (Calculs dans $\mathbb{Z}_7$)**.** Représentons $1/2$ dans $\mathbb{Z}_7$. On cherche $x = \sum a_i \cdot 7^i$ tel que $2x = 1$.

- $2a_0 \equiv 1 \pmod 7$: $a_0 = 4$ (car $2 \cdot 4 = 8 \equiv 1$).
- $2(4 + a_1 \cdot 7) \equiv 1 \pmod{49}$: $8 + 14a_1 \equiv 1 \pmod{49}$, soit $14a_1 \equiv -7 \pmod{49}$, $2a_1 \equiv -1 \equiv 6 \pmod 7$, $a_1 = 3$.
- En continuant : $a_2 = 3$, $a_3 = 3$, ...

On obtient $1/2 = 4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + \cdots = 4 + 3 \cdot \frac{7}{1-7}$ dans $\mathbb{Z}_7$, ce qui est cohérent car $4 + 3 \cdot 7/(1-7) = 4 - 7/2 = 1/2$.

Exemple 9.29 (Résolution de $x^2 = 2$ dans $\mathbb{Q}_7$)**.** On a $3^2 = 9 \equiv 2 \pmod 7$. De plus, $f(x) = x^2 - 2$, $f'(3) = 6 \not\equiv 0 \pmod 7$. Par le lemme de Hensel, $\sqrt{2} \in \mathbb{Z}_7$ et $\sqrt{2} \equiv 3 \pmod 7$.
Relèvement : $a_1 = 3 - (9-2)/(2 \cdot 3) = 3 - 7/6$. Or $6^{-1} \equiv 6 \pmod 7$, donc $7/6 \equiv 7 \cdot 6 = 42 \equiv 0 \pmod 7$, soit $a_1 = 3 + 1 \cdot 7 = 10$. Vérifions : $10^2 = 100 = 2 + 2 \cdot 49$, donc $v_7(10^2 - 2) = v_7(98) = 2 \geq 2$.

9.10 Résumé du chapitre

Concept	Description
Valuation $v_p(n)$	Plus grande puissance de p divisant n
$\lvert x\rvert_p = p^{-v_p(x)}$	Valeur absolue p-adique
Inégalité ultramétrique	$\lvert x+y\rvert_p \leq \max(\lvert x\rvert_p, \lvert y\rvert_p)$
$\mathbb{Z}_p$	Entiers p-adiques : séries $\sum a_i p^i$, $a_i \in \{0, \ldots, p-1\}$
$\mathbb{Q}_p$	Corps des nombres p-adiques, complétion de $(\mathbb{Q}, d_p)$
Lemme de Hensel	Relèvement de racines modulo p en racines p-adiques
Ostrowski	Classification de toutes les valeurs absolues sur $\mathbb{Q}$

9.11 Exercices

Exercice 9.1 ($\star$ — Calculs de valuations)**.** Calculer les valuations suivantes :

(a) $v_2(360)$, $v_3(360)$, $v_5(360)$.

(b) $v_7(50!/7)$.

(c) $v_p(n!)$ en fonction de n et p (formule de Legendre).

Exercice 9.2 ($\star$ — Valeur absolue p-adique)**.** (a) Calculer $\lvert 63\rvert_3$, $\lvert 140\rvert_7$, $\lvert -250\rvert_5$.

(b) Montrer que $\lvert n\rvert_p = 1$ pour tout $n \in \mathbb{Z}$ avec $\text{pgcd}(n, p) = 1$.

(c) Montrer que pour tout $n \in \mathbb{Z} \setminus \{0\}$, il n'existe qu'un nombre fini de premiers p tels que $|n|_p \neq 1$.

Exercice 9.3 ($\star\star$ — Propriétés ultramétriques)**.** Soit $(K, |\cdot|)$ un corps muni d'une valeur absolue ultramétrique.

(a) Montrer que si $|x| \neq |y|$, alors $|x+y| = \max(|x|, |y|)$.

(b) En déduire que dans un espace ultramétrique, tout point d'une boule ouverte en est le centre.

(c) Montrer que toute boule ouverte est aussi un ensemble fermé.

Exercice 9.4 ($\star\star$ — Développements p-adiques)**.** (a) Trouver le développement 3-adique de -1, $1/2$ et $2/5$.

(b) Montrer que $x \in \mathbb{Z}_p$ est rationnel si et seulement si son développement p-adique est ultimement périodique.

Exercice 9.5 ($\star\star\star$ — Applications de Hensel)**.** (a) Montrer que $\sqrt{-1} \in \mathbb{Q}_p$ si et seulement si $p \equiv 1 \pmod 4$ ou $p = 2$. *Indication :* pour $p = 2$, vérifier qu'il n'y a pas de racine modulo 8.

(b) Soit p un premier impair et $a \in \mathbb{Z}$ avec $\operatorname{pgcd}(a, p) = 1$. Montrer que a est un carré dans $\mathbb{Z}_p$ si et seulement si $\left(\frac{a}{p}\right) = 1$.

(c) Montrer que $\sqrt{6} \in \mathbb{Q}_5$ mais $\sqrt{6} \notin \mathbb{Q}_7$.

Exercice 9.6 ($\star\star\star$ — Formule de Legendre)**.** Démontrer la formule de Legendre : pour tout premier p et tout entier $n \geq 1$,

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

où $s_p(n)$ désigne la somme des chiffres de n en base p.

Chapitre 10

Aperçu sur la Théorie Analytique des Nombres

« Les nombres premiers sont les atomes de l'arithmétique,
et la fonction zêta est le spectre qui révèle leur structure. »
— Bernhard Riemann (1826–1866)

10.1 Introduction historique

La théorie analytique des nombres est née de l'idée audacieuse d'utiliser les outils de l'analyse — séries, intégrales, fonctions de variable complexe — pour étudier les propriétés des nombres entiers et, en particulier, la distribution des nombres premiers.

— **Euler (1737)** établit le produit eulérien $\sum n^{-s} = \prod_p (1 - p^{-s})^{-1}$ et en déduit une nouvelle preuve de l'infinité des premiers.

— **Dirichlet (1837)** introduit les L-fonctions et démontre que toute progression arithmétique $a, a+q, a+2q, \ldots$ avec $\gcd(a, q) = 1$ contient une infinité de premiers.

— **Riemann (1859)** publie son mémoire fondateur « Über die Anzahl der Primzahlen unter einer gegebenen Grösse », introduisant la prolongation analytique de ζ et formulant sa célèbre hypothèse.

— **Hadamard** et **de la Vallée-Poussin** (1896) démontrent indépendamment le théorème des nombres premiers.

10.2 La fonction zêta de Riemann

Définition 10.1 (Fonction zêta de Riemann)**.** La *fonction zêta de Riemann* est définie pour $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$ par la série de Dirichlet

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Proposition 10.2 (Convergence). *La série $\sum_{n=1}^{\infty} n^{-s}$ converge absolument pour $\mathrm{Re}(s) > 1$ et y définit une fonction holomorphe.*

Démonstration. Pour $s = \sigma + it$ avec $\sigma > 1$, on a $|n^{-s}| = n^{-\sigma}$. La série $\sum n^{-\sigma}$ est une série de Riemann convergente pour $\sigma > 1$. La convergence est uniforme sur tout demi-plan $\{\mathrm{Re}(s) \geq \sigma_0\}$ avec $\sigma_0 > 1$, ce qui assure l'holomorphie par le théorème de Weierstrass. □

10.2.1 Produit eulérien

Théorème 10.3 (Produit eulérien d'Euler). *Pour tout $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$,*

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}}.$$

Démonstration. Fixons s avec $\sigma = \mathrm{Re}(s) > 1$. Pour tout $N \geq 1$, notons $P_N = \{p_1, \ldots, p_k\}$ l'ensemble des premiers $\leq N$. Développons le produit fini :

$$\prod_{j=1}^{k} \frac{1}{1 - p_j^{-s}} = \prod_{j=1}^{k} \sum_{e_j=0}^{\infty} p_j^{-e_j s} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq N}} \frac{1}{n^s},$$

où la dernière égalité résulte du théorème fondamental de l'arithmétique : chaque entier dont tous les facteurs premiers sont $\leq N$ apparaît exactement une fois dans le développement.

Or, la somme du membre droit contient au moins tous les termes $1/n^s$ pour $n \leq N$ (car si $n \leq N$, tous ses facteurs premiers sont $\leq N$). Ainsi :

$$\left| \zeta(s) - \prod_{j=1}^{k} \frac{1}{1 - p_j^{-s}} \right| \leq \sum_{n > N} \frac{1}{n^{\sigma}}.$$

Quand $N \to \infty$, le reste de la série convergente $\sum n^{-\sigma}$ tend vers 0, d'où la convergence du produit infini vers $\zeta(s)$. □

Corollaire 10.4 (Infinité des nombres premiers). *Il existe une infinité de nombres premiers.*

Démonstration. Si l'ensemble des premiers était fini, le produit eulérien serait un produit fini, donc fini pour $s = 1$. Or $\zeta(1) = \sum 1/n = +\infty$, contradiction. □

Remarque 10.5. Plus quantitativement, Euler a montré que $\sum_p 1/p = +\infty$, ce qui donne une mesure de la « densité » des premiers : ils sont non seulement infinis, mais suffisamment nombreux pour que la somme de leurs inverses diverge.

10.2.2 Valeurs spéciales de ζ

Théorème 10.6 ($\zeta(2) = \pi^2/6$ (Euler, 1735))**.** *On a*

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Esquisse de preuve (méthode d'Euler). On considère la fonction $\sin(\pi x)/(\pi x) = \prod_{n=1}^{\infty}(1 - x^2/n^2)$. En développant le produit et en identifiant le coefficient de x^2, on obtient

$$-\frac{\pi^2}{6} \cdot \frac{1}{\pi^2} = -\sum_{n=1}^{\infty} \frac{1}{n^2},$$

en comparant avec le développement en série $\sin(\pi x)/(\pi x) = 1 - \pi^2 x^2/6 + \cdots$, d'où le résultat. La justification rigoureuse du produit infini utilise le théorème de factorisation de Weierstrass. □

Remarque 10.7. Plus généralement, Euler a calculé $\zeta(2k)$ pour tout $k \geq 1$ en termes des nombres de Bernoulli :

$$\zeta(2k) = \frac{(-1)^{k+1}(2\pi)^{2k} B_{2k}}{2 \cdot (2k)!}.$$

En revanche, les valeurs $\zeta(2k+1)$ (et en particulier $\zeta(3)$, la *constante d'Apéry*) restent mystérieuses : $\zeta(3)$ est irrationnel (Apéry, 1978), mais on ignore si $\zeta(5)$ l'est.

10.3 L-fonctions de Dirichlet

Définition 10.8 (Caractère de Dirichlet)**.** Un *caractère de Dirichlet* modulo q est un morphisme de groupes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$, étendu à $\mathbb{Z}$ par périodicité et en posant $\chi(n) = 0$ si $\gcd(n, q) > 1$.

Définition 10.9 (L-fonction de Dirichlet)**.** Pour un caractère χ modulo q, la *L-fonction de Dirichlet* associée est

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

Elle admet un produit eulérien :

$$L(s, \chi) = \prod_{p \text{ premier}} \frac{1}{1 - \chi(p)\, p^{-s}}.$$

Remarque 10.10. Pour le caractère trivial χ_0 modulo 1 (c'est-à-dire $\chi_0(n) = 1$ pour tout n), on retrouve $L(s, \chi_0) = \zeta(s)$.

10.4 Théorème de Dirichlet sur les progressions arithmétiques

Théorème 10.11 (Dirichlet, 1837)**.** *Soient $a, q \in \mathbb{Z}$ avec $q \geq 1$ et* $\operatorname{pgcd}(a, q) = 1$. *Alors la progression arithmétique*

$$a,\ a+q,\ a+2q,\ a+3q,\ \ldots$$

contient une infinité de nombres premiers. Plus précisément,

$$\sum_{\substack{p \text{ premier} \\ p \equiv a \pmod q}} \frac{1}{p} = +\infty.$$

Remarque 10.12. La preuve de Dirichlet repose sur deux ingrédients principaux :

(i) L'utilisation des caractères de Dirichlet pour « isoler » la progression arithmétique via la relation d'orthogonalité :

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(n)\overline{\chi(a)} = \begin{cases} 1 & \text{si } n \equiv a \pmod q, \\ 0 & \text{sinon.} \end{cases}$$

(ii) La non-annulation $L(1, \chi) \neq 0$ pour tout caractère $\chi \neq \chi_0$ modulo q, qui est le cœur technique de la preuve.

10.5 Le théorème des nombres premiers

Notation 10.13. On note $\pi(x) = \#\{p \leq x : p \text{ premier}\}$ la fonction de comptage des nombres premiers.

Théorème 10.14 (Théorème des nombres premiers (Hadamard, de la Vallée-Poussin, 1896))**.**

$$\pi(x) \sim \frac{x}{\ln x} \quad \textit{quand } x \to \infty,$$

c'est-à-dire $\displaystyle\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1.$

Remarque 10.15. Ce théorème, conjecturé indépendamment par Legendre (vers 1798) et Gauss (vers 1793), fut démontré indépendamment en 1896 par Hadamard et de la Vallée-Poussin. Les deux preuves utilisent de manière essentielle la non-annulation de $\zeta(s)$ sur la droite $\operatorname{Re}(s) = 1$.

Définition 10.16 (Logarithme intégral)**.** Le *logarithme intégral* est défini par

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}.$$

C'est une meilleure approximation de $\pi(x)$ que $x/\ln x$: $\pi(x) \sim \mathrm{Li}(x)$.

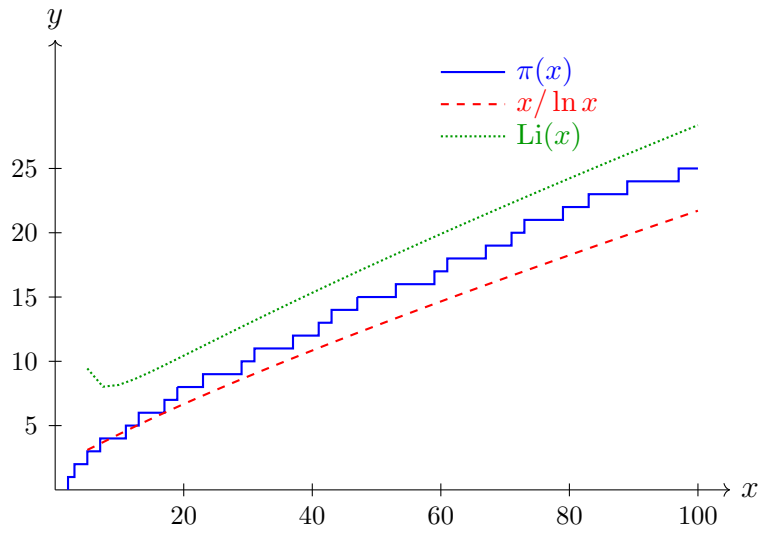


FIGURE 10.1 – Comparaison de $\pi(x)$ avec ses approximations $x/\ln x$ et $\mathrm{Li}(x)$ pour $x \leq 100$.

10.6 Fonctions de Tchebychev

Définition 10.17 (Fonctions θ et ψ de Tchebychev)**.** On définit :

$$\theta(x) = \sum_{\substack{p \leq x \\ p \text{ premier}}} \ln p, \qquad \psi(x) = \sum_{\substack{p^k \leq x \\ p \text{ premier}, k \geq 1}} \ln p = \sum_{n \leq x} \Lambda(n),$$

où Λ est la *fonction de von Mangoldt* :

$$\Lambda(n) = \begin{cases} \ln p & \text{si } n = p^k \text{ pour un premier } p \text{ et } k \geq 1, \\ 0 & \text{sinon.} \end{cases}$$

Proposition 10.18 (Relation avec le TNP)**.** *Les assertions suivantes sont équivalentes :*

(i) $\pi(x) \sim x/\ln x$ *(théorème des nombres premiers) ;*

(ii) $\theta(x) \sim x$ *;*

(iii) $\psi(x) \sim x$.

Esquisse. L'équivalence (ii) $\iff$ (iii) résulte de l'estimation $\psi(x) = \theta(x) + O(\sqrt{x})$, car les

termes avec $k \geq 2$ dans ψ contribuent au plus $\sum_{p \leq \sqrt{x}} \ln p \leq \sqrt{x} \ln x$.

Pour (i) $\iff$ (ii), on utilise la sommation d'Abel : $\theta(x) = \pi(x) \ln x - \int_2^x \pi(t)/t \, dt$, et on montre que si l'un des deux équivalents vaut, l'autre aussi. □

Remarque 10.19. Avant la preuve du TNP, Tchebychev (1852) avait établi l'encadrement

$$0{,}921 \cdot \frac{x}{\ln x} < \pi(x) < 1{,}106 \cdot \frac{x}{\ln x}$$

pour x assez grand, prouvant ainsi que *si* $\pi(x)/(x/\ln x)$ admet une limite, celle-ci vaut nécessairement 1.

10.7 L'hypothèse de Riemann

Théorème 10.20 (Prolongement analytique de ζ)**.** *La fonction $\zeta(s)$ admet un prolongement méromorphe à tout le plan complexe $\mathbb{C}$, avec un unique pôle simple en $s = 1$ de résidu 1. Elle satisfait l'équation fonctionnelle*

$$\pi^{-s/2} \, \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-(1-s)/2} \, \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s).$$

Définition 10.21 (Bande critique et zéros)**.**

— Les *zéros triviaux* de ζ sont les entiers négatifs pairs : $s = -2, -4, -6, \ldots$

— Les *zéros non triviaux* se trouvent tous dans la *bande critique* $0 < \mathrm{Re}(s) < 1$.

— La *droite critique* est $\mathrm{Re}(s) = 1/2$.

Théorème 10.22 (Hypothèse de Riemann (1859, non démontrée))**.** *Tous les zéros non triviaux de la fonction ζ de Riemann se trouvent sur la droite critique* $\mathrm{Re}(s) = 1/2$.

Remarque 10.23 (Importance et statut). L'hypothèse de Riemann est considérée comme l'un des problèmes ouverts les plus importants des mathématiques. Elle fait partie des sept problèmes du millénaire du *Clay Mathematics Institute*, assortis d'un prix d'un million de dollars.

Parmi ses conséquences :

— Un terme d'erreur optimal dans le TNP : $\pi(x) = \mathrm{Li}(x) + O(\sqrt{x} \ln x)$.

— Des estimations fines sur les écarts entre nombres premiers consécutifs.

— Des résultats sur la distribution des nombres premiers dans les progressions arithmétiques.

À ce jour (2026), l'hypothèse de Riemann reste non démontrée, bien que des vérifications numériques aient confirmé qu'elle est vraie pour les premiers 10^{13} zéros non triviaux.

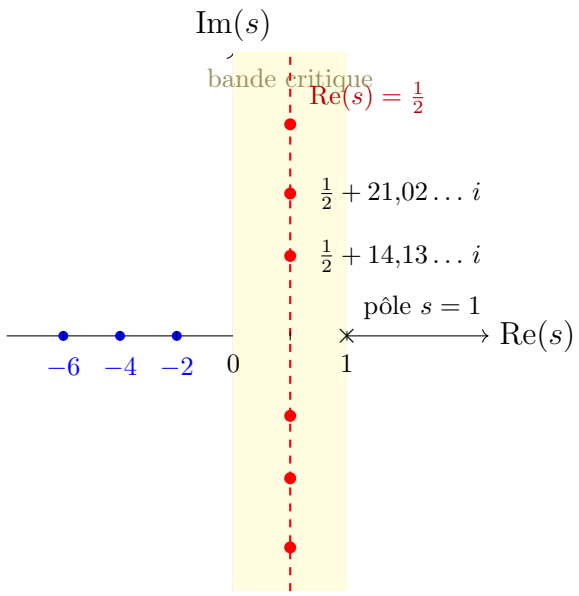


FIGURE 10.2 – La bande critique $0 < \mathrm{Re}(s) < 1$, la droite critique $\mathrm{Re}(s) = 1/2$ (tirets rouges), les zéros triviaux (points bleus) et les premiers zéros non triviaux (points rouges).

10.8 Problèmes ouverts célèbres

Nous terminons ce cours par un bref panorama de quelques-unes des conjectures les plus célèbres de la théorie des nombres, toujours non résolues.

10.8.1 Conjecture de Goldbach

Théorème 10.24 (Conjecture de Goldbach (1742, non démontrée))**.** *Tout entier pair $n \geq 4$ est somme de deux nombres premiers.*

Remarque 10.25. Parmi les résultats partiels :

- Vinogradov (1937) a montré que tout entier *impair* suffisamment grand est somme de trois premiers (« conjecture faible de Goldbach »).
- Helfgott (2013) a rendu le résultat de Vinogradov effectif pour tout entier impair > 5.
- Chen (1966) a montré que tout entier pair assez grand s'écrit $p + q$ où p est premier et q est premier ou semi-premier.
- La conjecture a été vérifiée numériquement jusqu'à 4×10^{18}.

10.8.2 Conjecture des nombres premiers jumeaux

Théorème 10.26 (Conjecture des premiers jumeaux (non démontrée))**.** *Il existe une infinité de nombres premiers p tels que $p + 2$ soit aussi premier.*

Remarque 10.27. — Brun (1919) a montré que $\sum_{p,\,p+2 \text{ premiers}} 1/p$ converge (la *constante de Brun* $\approx 1{,}902$), même si la conjecture est vraie.

— Zhang (2013) a prouvé un résultat spectaculaire : il existe une infinité de paires de premiers dont l'écart est $\leq 70\,000\,000$.

— Le projet Polymath a réduit cette borne à 246 (2014). La conjecture des premiers jumeaux correspond à la borne 2.

10.9 Résumé du chapitre

Concept	**Description**
$\zeta(s) = \sum n^{-s}$	Fonction zêta de Riemann, convergente pour $\mathrm{Re}(s) > 1$
Produit eulérien	$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$: lien zêta–premiers
$L(s, \chi)$	L-fonctions de Dirichlet, généralisations de ζ
Dirichlet	Infinité de premiers dans toute progression $a + nq$, $\gcd(a, q) = 1$
TNP	$\pi(x) \sim x/\ln x$ (Hadamard, de la Vallée-Poussin, 1896)
$\theta(x)$, $\psi(x)$	Fonctions de Tchebychev, TNP $\iff \psi(x) \sim x$
Hypothèse de Riemann	Zéros non triviaux sur $\mathrm{Re}(s) = 1/2$ (ouverte)

10.10 Exercices

Exercice 10.1 ($\star$ — Produit eulérien)**.** (a) En utilisant le produit eulérien, montrer que $\zeta(s) \neq 0$ pour $\mathrm{Re}(s) > 1$.

(b) Calculer $\prod_p (1 - p^{-2})^{-1}$ et retrouver ainsi $\zeta(2) = \pi^2/6$.

(c) En déduire que $\sum_{n=1}^{\infty} \mu(n)/n^2 = 6/\pi^2$, où μ est la fonction de Möbius.

Exercice 10.2 ($\star$ — Fonction de comptage)**.** (a) Calculer $\pi(100)$, $\pi(200)$ et $\pi(1000)$.

(b) Comparer avec $x/\ln x$ et $\mathrm{Li}(x)$ pour ces valeurs.

(c) Pour quels $x \leq 1000$ l'écart $|\pi(x) - x/\ln x|$ est-il maximal ?

Exercice 10.3 ($\star\star$ — Identités de la fonction zêta)**.** (a) Montrer que $\zeta(s)^2 = \sum_{n=1}^{\infty} d(n)/n^s$ pour $\mathrm{Re}(s) > 1$, où $d(n)$ est le nombre de diviseurs de n.

(b) Montrer que $\zeta(s)/\zeta(2s) = \sum_{n=1}^{\infty} |\mu(n)|/n^s$.

(c) En déduire que la densité des entiers sans facteur carré est $6/\pi^2$.

Exercice 10.4 ($\star\star$ — Fonctions de Tchebychev)**.** (a) Calculer $\theta(30)$ et $\psi(30)$.

(b) Montrer que $\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots$

(c) En déduire que $\psi(x) - \theta(x) = O(\sqrt{x}\ln x)$.

Exercice 10.5 ($\star\star\star$ — Divergence de $\sum 1/p$)**.** En utilisant le produit eulérien et le fait que $\zeta(s) \to +\infty$ quand $s \to 1^+$, montrer que

$$\sum_{p \text{ premier}} \frac{1}{p} = +\infty.$$

Indication : prendre le logarithme du produit eulérien et estimer $-\ln(1-p^{-s})$.

Exercice 10.6 ($\star\star\star$ — Formule de Mertens)**.** Démontrer que

$$\sum_{\substack{p\le x\\ p \text{ premier}}} \frac{1}{p} = \ln\ln x + M + O\left(\frac{1}{\ln x}\right),$$

où $M \approx 0{,}2615$ est la constante de Meissel–Mertens.

Exercice 10.7 ($\star\star\star$ — Hypothèse de Riemann et terme d'erreur)**.** Admettre l'hypothèse de Riemann.

(a) Montrer que $\psi(x) = x + O(\sqrt{x}\,(\ln x)^2)$.

(b) En déduire que $\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\ln x)$.

(c) Comparer avec le meilleur terme d'erreur connu sans l'HR : $\pi(x) = \mathrm{Li}(x) + O(x\exp(-c\sqrt{\ln x}))$.

Bibliographie

[1] Hardy, G.H. et Wright, E.M., *An Introduction to the Theory of Numbers*, 6e édition, Oxford University Press, 2008.

[2] Serre, J.-P., *Cours d'arithmétique*, 3e édition, Presses Universitaires de France, 1988.

[3] Ireland, K. et Rosen, M., *A Classical Introduction to Modern Number Theory*, 2e édition, Graduate Texts in Mathematics 84, Springer, 1990.

[4] Apostol, T.M., *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer, 1976.

[5] Niven, I., Zuckerman, H.S. et Montgomery, H.L., *An Introduction to the Theory of Numbers*, 5e édition, Wiley, 1991.

[6] Nathanson, M.B., *Elementary Methods in Number Theory*, Graduate Texts in Mathematics 195, Springer, 2000.

[7] Koblitz, N., *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2e édition, Graduate Texts in Mathematics 58, Springer, 1984.

[8] Davenport, H., *Multiplicative Number Theory*, 3e édition, révisée par H.L. Montgomery, Graduate Texts in Mathematics 74, Springer, 2000.

Index