Arithmétique dans $\mathbb{Z}$

Geoffrey Deperle

Table des matières

Chapitre 1

Bases de l'arithmétique

1.1 Divisibilité et division euclidienne

1.1.1 Propriétés fondamentales de $\mathbb{N}$ et $\mathbb{Z}$

Sans rentrer dans les détails de la construction, la propriété caractérisant $\mathbb{N}$ est la propriété de récurrence qui peut s'écrire de deux manières.

Théorème 1 (de récurrence)**.** *Soit $P(n)$ une propriété logique dépendant de $n \in \mathbb{N}$ vérifiant*

(i) Il existe n_0 tel que $P(n_0)$ est vraie.

(ii) pour tout $n \geq n_0, [P(n) \implies P(n+1)]$ est vraie.

alors pour tout $n \geq n_0$, $P(n)$ est vraie.

Ce théorème utile pour toute démonstration sur $\mathbb{N}$ peut se ré-écrire differemment :

Théorème 2. *Toute sous-ensemble non-vide de $\mathbb{N}$ admet un plus petit élément.*

Proposition 3. *Le théorème 1.1 et le théorème 1.2 sont équivalents.*

Preuve : ($\implies$) Supposons que le théorème 1.1 est vraie. Montrons le théorème 1.2. Par contraposé, supposons qu'il existe un ensemble A n'admettant pas de plus petit élément. Montrons que A est vide. Soit $P(n)$: pour tout $k \leq n, k \notin A$. Montrons que $P(n)$ est vraie pour tout $n \in \mathbb{N}$ par récurrence.

— $0 \notin A$ car 0 minore $\mathbb{N}$. Donc $P(0)$ est vraie.

— Soit $n \in \mathbb{N}$ tel que pour tout $k \leq n$, $k \notin A$. $n+1 \notin A$ car $n+1$ serait alors le minorant de A. D'où pour tout $k \leq n+1, k \notin A$.

($\Longleftarrow$) Supposons le théorème 1.2. Montrons le principe de récurrence. Soit P une propriété vérifiant (i) et (ii). Montrons que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.
Soit $A = \{n \in A \,|\, P(n) \text{ est faux}\} \cap \{n \in \mathbb{N}, |n \geq n_0\}$. Pour montrer que $A = \emptyset$, il suffit de montrer que A n'admet pas de plus petit élément. Soit $n \in A$, si $n = n_0$, alors comme $P(n_0)$ est vraie, le plus petit élément de A est de la forme $k+1$ avec $k \in \mathbb{N}$. Or, si $k+1 \in A$, alors $P(k+1)$ est faux et par contraposé $P(k)$ est faux. Donc il existe $k \in A < n$ donc A n'admet pas de plus petit élément. Donc A est vide, d'où pour tout $n \geq n_0, P(n)$ est vraie. □

On dit alors que la relation d'ordre $\leq$ est un bon ordre et que l'ensemble $\mathbb{N}$ est bien ordonné.

L'ensemble $\mathbb{Z}$ possède aussi une propriété fondamentale :

Théorème 4. — *Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.*
— *Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.*

Preuve :
— Soit A une partie de $\mathbb{Z}$ minorée par un entier $k \in \mathbb{Z}$. Alors la partie $A' = n - k | n \in A$ est une partie de $\mathbb{N}$ non vide par hypothèse donc admet un plus petit élément n_0. L'entier $n_0 + k$ est le plus petit élément de A.
— Soit A une partie de $\mathbb{Z}$ non vide et majorée de $\mathbb{Z}$. L'ensemble $-A = \{-k \,|\, k \in A\}$ est une partie non vide et minorée de $\mathbb{Z}$ donc admet un plus petit élément n_0. L'entier $-n_0$ est le plus grand élément de A.

□

Ainsi, dans $\mathbb{N}$ et $\mathbb{Z}$ les notions de sup et max coïncident.

1.1.2 Relation de divisibilité

Définition 5. Soit $a, b \in \mathbb{Z}$. On dit que a divise b et on note $a|b$ lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Exemple 6. $5|10$ car $10 = 2 \times 2$.

Remarque 7. Les entiers 1 et -1 divisent tout élément de $\mathbb{Z}$ et 0 est divisible par tout entier.

La relation de divisibilité est compatible avec les opérations arithmétiques :

Proposition 8. *Soit $a, b, b' \in \mathbb{Z}$ tel que $a|b$ et $a|b'$, a divise toute combinaison arithmétique de b et b' : $\forall k, k' \in \mathbb{Z}, a|kb + k'b'$*

Preuve : $a|b$ donc il existe $l \in \mathbb{Z}$ tel que $b = la$ et $a|b'$ donc il existe $l' \in \mathbb{Z}$ tel que $b' = l'a$ d'où $kb + k'b' = (kl + k'l')a$. □

Proposition 9. *La relation de divisibilité définit un pré-ordre sur $\mathbb{Z}$, c'est-à-dire :*
(i) Pour tout $a \in \mathbb{Z}, a|a$.
(ii) Pour tout $a, b, c \in \mathbb{Z}$, si $a|b$ et $b|c$ alors $a|c$.

Preuve :
(i) Il suffit de prendre $k = 1$.
(ii) Soit $a, b, c \in \mathbb{Z}$ tel que $a|b$ et $b|c$. Il existe $k \in \mathbb{Z}$ tel que $b = ka$ et $k' \in \mathbb{Z}$ tel que $c = k'b$. D'où $c = kk'a$ donc $a|c$.

□

Pour que la relation de divisibilité soit une relation d'ordre sur $\mathbb{Z}$ il faudrait que si a divise b et b divise a, alors $a = b$. Or, ce n'est pas le cas comme le montre l'exemple de $a = 1$ et $b = -1$. Cependant, cette propriété est vraie sur $\mathbb{N}$.

Lemme 10. *Les inversibles de $\mathbb{Z}$ sont $\{-1, 1\}$.*

Preuve : 1 et -1 sont inversibles dans $\mathbb{Z}$, montrons que ce sont les seuls. Soit a un élément inversible dans $\mathbb{Z}$, c'est-à-dire il existe b tel que $ab = 1$. On a donc $|ab| = 1$ d'où $|a||b| = 1$. En particulier a et b sont non nuls et vérifient $|a| \leq 1$ (car $|b| \geq 1$). D'où $|a| \in \{-1, 1\}$. □

On remarque en particulier que si $a|b$, alors $|a| \leq |b|$.

Proposition 11. *Soit $a, b \in \mathbb{Z}$ tel que $a|b$ et $b|a$. Alors $a = \pm b$.*

Preuve : $a|b$ donc il existe $k \in \mathbb{Z}$ tel que $b = ka$ et $b|a$ tel que $a = k'a$. D'où $a = kk'a$. Comme $a \neq 0$ (sinon on ne pourrait avoir $a|b$), on a $kk' = 1$ d'où k est inversible dans $\mathbb{Z}$. Or, l'ensemble des inversibles de $\mathbb{Z}$ est $\{-1, 1\}$. □

1.1.3 Division euclidienne

Passons maintenant au théorème fondamental de la division euclidienne :

Théorème 12. *Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. Il existe un unique couple (q, r) vérifiant les propriétés suivantes tel que $a = bq + r$ et $r \in [\![0, b-1]\!]$. Les entiers q et r s'appellent respectivement quotient et reste de la division euclidienne de a par b.*

Preuve : Montrons ce résultat par analyse-synthèse :
Analyse :
Supposons qu'il existe un couple (q, r) vérifiant $a = bq + r$ et $r \in [\![0, b-1]\!]$. On a alors

$$\begin{aligned} & 0 \leq r < b \\ \iff & 0 \leq a - bq < b \\ \iff & bq \leq a < b(q+1) \\ \iff & \frac{a}{b} \leq q < \frac{a}{b} + 1 \end{aligned}$$

Ainsi q est un entier vérifiant $\frac{a}{b} \leq q < \frac{a}{b} + 1$. Un tel entier est unique et est définie par $q = \left\lfloor \frac{a}{b} \right\rfloor$.

Synthèse :
Il s'agit de vérifier l'existence d'un tel entier.
L'ensemble $\{k \in \mathbb{Z} \,|\, k \leq \frac{a}{b}\}$ est sous-ensemble de $\mathbb{Z}$ non vide et majoré donc admet un maximum q. Posons $r = a - bq$. Montrons que ces entiers vérifient la propriété voulue. $q + 1$ majore $\{k \in \mathbb{Z} \,|\, k \leq \frac{a}{b}\}$ donc comme $k + 1 \in \mathbb{Z}$ on a $q \leq \frac{a}{b} < q + 1$. d'où $bq \leq a < b(q+1)$ d'où $0 \leq r < b - 1$ □

Exemple 13. La division euclidienne de 19 par 7 est $19 = 2 \times 7 + 5$.

On peut lier la division euclidienne à la divisibilité avec la proposition suivante :

Proposition 14. *Soit $a, b \in \mathbb{Z}$. $a|b \iff$ le reste de la division euclidienne de b par a est 0.*

Preuve : Le sens réciproque est trivial vu que si le reste de la division euclidienne de b par a est 0 alors $b = qa + 0$ d'où $a|b$.
Supposons que $a|b$ donc il existe $k \in \mathbb{Z}$ tel que $b = ka$. Par théorème de division euclidienne il existe (q, r) tel que $b = qa + r$ et $0 \leq r < a$.
D'où $ka = qa + r$ d'où $r = (k - q)a$. En particulier $r|a$ d'où $r = 0$ car $|r| < a$. □

1.1.4 Congruences

Définition 15. Soit $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$, on dit que a congrue en b modulo n et on note $a \equiv b\,[n]$ lorsque $n|b - a$.

La caractérisation suivante de $a \equiv b\,[n]$ est souvent prise comme définition :

Proposition 16. *Soit $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $a \equiv b\,[n]$ si et seulement si a et b ont le même reste par la divison euclidienne par n.*

Preuve : ($\Longrightarrow$) Écrivons la division euclidienne de a et b par n : il existe q, q', r, r' avec $0 \leq r < n$ et $0 \leq r' < n$ tel que $a = qn + r$ et $b = q'n + r'$. D'où $b - a = (q' - q)n + r' - r$ avec $r' - r < n$. Il s'agit donc de l'écriture de la division euclidienne de $b - a$ par n. Comme $n|b - a$, il vient que $r' - r = 0$ d'où $r = r'$.
($\Longleftarrow$) En reprenant les notations suivantes, supposons que $r = r'$, on a donc $b - a = (q' - q)n$ d'où $n \,|\, b - a$. □

Ainsi, on a $a|b \iff a \equiv 0\,[b]$. En particulier le reste de la division euclidienne de a par b est le plus petit entier positif r tel que $a \equiv r\,[b]$.

Proposition 17. *La relation de congruence modulo $n \in \mathbb{N}^*$ est une relation d'équivalence sur $\mathbb{Z}$, c'est à dire :*

(i) Pour tout $a \in \mathbb{Z}, a \equiv a\,[n]$

(ii) Pour tout $a, b, c \in \mathbb{Z}$ tel que $a \equiv b\,[n]$ et $b \equiv c\,[n])$ alors $a \equiv c\,[n]$

(iii) Si $a, b \in \mathbb{Z}$ tel que $a \equiv b\,[n]$ alors $b \equiv a\,[n]$.

Preuve :

(i) Tout entier divise 0.

(ii) Soit $a, b, c \in \mathbb{Z}$ tel que $a \equiv b\,[n]$ et $b \equiv c\,[n])$. En écrivant $c - a = c - b + b - a$, comme $n|c - b$ et $n|b - a$, $n|c - a$.

(iii) Supposons que $n|b - a$, alors $n|a - b$.

□

La relation de congruence est compatible avec les opérations arithmétiques :

Proposition 18. *Soit $a, b, c, d \in \mathbb{Z}$ tel que $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors*

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

(ii) $ac \equiv bd\,[n]$

Preuve : Soit $a, b, c, d \in \mathbb{Z}$ tel que $a \equiv b\,[n]$ et $c \equiv d\,[n]$

1. On a $n|b - a$ et $n|d - c$ d'où $n|b + d - (a + b)$.
2. $bd - ac = d(b - a) + a(d - c)$ d'où comme $n|b - a$ et $n|d - c$, on a $n|bd - ac$.

□

Remarque 19. En itérant le point (ii), si $a \equiv b\,[n]$ alors $\forall k \in \mathbb{N}$, $a^k \equiv b^k\,[n]$.

Exercice 20. Trouver le chiffre des unités de 3^{2021}.
Le chiffre des unités d'un nombre est le reste de ce nombre par la division euclidienne par 10. Il s'agit donc de trouver le plus entier positif r tel que $3^{2021} \equiv r\,[10]$.
On a $3^4 = 81$ donc $3^4 \equiv 1\,[10]$.
Or, $3^{2021} = 4 \times 505 + 1$ d'où $3^{2021} = 3 \times (3^4)^{505}$ et comme $3^4 \equiv 1\,[10]$, on a $(3^4)^{505} \equiv \underbrace{1^{505}}_{=1}\,[10]$ d'où par compatibilité avec les opérations arithmétiques, $3^{2021} \equiv 3\,[10]$. Le chiffre des unités de 3^{2021} est 3.

1.1.5 Application de la congruence : Critère de divisibilité

Proposition 21. *Soit $a \in \mathbb{N}$, on note $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ l'écriture décimale de a avec a_0 le chiffre des unités, a_1 le chiffre des dizaines, c'est-à-dire les uniques nombres dans $[\![0, 9]\!]$ tel que $a = \sum_{k=0}^{n} a_k 10^k$*

(i) $2|a \iff 2|a_0$.

(ii) $3|a \iff 3|a_0 + \dots a_n$.

(iii) $5|a \iff 5|a_0$.

(iv) $9|a \iff 9|a_0 + \dots a_n$.

(v) $11|a_0 - a_1 + \dots + (-1)^{n-1} a_{n-1} + (-1)^n a_n$

Preuve :

(i) Comme $2|10$, on a $10 \equiv 0\,[2]$ d'où $\sum_{k=0}^{n} a_k 10^k \equiv a_0\,[2]$ d'où $2|a \iff 2|a_0$.

(ii) $10 \equiv 1\,[3]$ d'où $\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k\,[3]$ d'où $3|a \iff 3|\sum_{k=0}^{n} a_k$.

(iii) De même que (i).

(iv) De même que (ii).

(v) $10 \equiv -1\,[11]$ d'où $\sum_{k=0}^{n} (-1)^k a_k \equiv \sum_{k=0}^{n} (-1)^k a_k\,[11]$ d'où $11|a \iff 11|\sum_{k=0}^{n} (-1)^k a_k$.

□

Exemple 22. 5928 est divisible par 3 car $5 + 9 + 2 + 8 = 24$ est divisible par 3.

1.2 PGCD et PPCM

1.2.1 PGCD

Définition 23. Soit $a, b \in \mathbb{Z}$, l'ensemble des diviseurs commun positif de a et de b est une partie non-vide et majoré (par $\max(a, b)$) donc admet un plus grand élément appelé **PGCD** de a et b, noté $a \wedge b$.

Exemple 24. Les diviseurs de 16 sont $1, 2, 4, 8$ et 16 et les diviseurs de 24 sont $1, 2, 3, 4, 6, 8, 12, 24$ donc le plus grand diviseur commun de 16 et 24 est 8.

Remarque 25. On a pour tout $a \in \mathbb{Z}$, $a \wedge 0 = a$.

Pour calculer le pgcd de deux entiers a et b, on peut utiliser l'algorithme d'Euclide :

Algorithme d'Euclide

Présentons un lemme :

Lemme 26. *Soit $a, b \in \mathbb{Z}$, le PGCD de a et b est égal au PGCD de b avec le reste de la division euclidienne de a par b.*

Preuve : Écrivons la division euclidienne de a par b : $a = bq+r$. Montrons que les diviseurs communs de a et b sont les mêmes que les diviseurs communs de b et r.
Soit k un diviseur commun de a et b, alors k divise $a - bq$ d'où k divise r.
Soit k un diviseur commun de b et r, alors k divise $bq + r$ donc divise a. □

Présentons l'algorithme : Soit a et $b \in \mathbb{Z}$,
Posons $a_0 = a$ et $b_0 = b$ et pour $n \in \mathbb{N}$, posons $a_{n+1} = b_n$ et $b_{n+1} = r_n$ avec r_n le reste de la division euclidienne de a_n par b_n (pour $b_n \neq 0$).
On a pour tout $n \in \mathbb{N}$, $a_{n+1} \wedge b_{n+1} = b_n \wedge r_n = a_n \wedge b_n$ d'après le lemme. Ainsi, la suite $(a_n \wedge b_n)$ est constante.
De plus, pour tout $n \in \mathbb{N}, b_{n+1} = r_n < b_n$ donc la suite (b_n) est strictement décroissante, comme c'est une suite d'entier, elle stationne à 0.
Ainsi, il existe un rang n_0 à partir du quel on a $b_{n_0} = 0$ d'où pour tout $n \in \mathbb{N}, a_n \wedge b_n = a_{n_0} \wedge b_{n_0} = a_{n_0} \wedge 0 = a_{n_0}$.

Exemple 27. Appliquons l'algorithme d'Euclide pour calculer le PGCD de 72 et 30.
On a $72 = 2 \times 30 + 12$
$30 = 2 \times 12 + 6$
$12 = 2 \times 6 + 0$ donc le PGCD de 72 et 30 est 6.

L'algorithme d'Euclide permet d'écrire le PGCD comme une combinaison arithmétique des deux entiers.

Proposition 28 (Relation de Bézout)**.** *Soit $a, b \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $a \wedge b = au + bv$. Une telle relation est appelée* ***relation de Bézout****.*

Preuve : En reprenant les notations précédentes. On va montrer par récurrence double la proposition suivante : P_n : il existe deux entiers u_n et v_n tel que $a_n = au_n + bv_n$.
Initialisation : On a $a_0 = a$ donc en posant $u_0 = 1$ et $v_0 = 0$ on a $a_0 = au_0 + bv_0$.
On a $a_1 = b_0$ donc en posant $u_1 = 0$ et $v_1 = 1$ on a $a_1 = au_1 + bv_1$.
Hérédité : Soit $n \in \mathbb{N}$ tel que P_n et P_{n+1} est vraie. Montrons P_{n+2}.
$a_{n+2} = b_{n+1} = r_n = a_n - q_n b_n = a_n - q_n a_{n+1}$ avec q_n le quotient de la division euclidienne de a_n par b_n. Par hypothèse de récurrence, il existe u_n, u_{n+1}, v_n et v_{n+1} tel que $a_n = au_n + bv_n$ et $a_{n+1} = au_{n+1} + bv_{n+1}$. D'où

$$a_{n+2} = au_n + bv_n - q(au_{n+1} + bv_{n+1}) = a(u_n - qu_{n+1}) + b(v_n - qv_{n+1})$$

En posant $u_{n+2} = u_n - qu_{n+1}$ et $v_{n+1} = v_n - qv_{n+1}$. On a P_{n+2}.
On a donc au rang $n_0, a \wedge b = a_{n_0} = au_{n_0} + bv_{n_0}$. □

Ainsi, la proposition dit que le pgcd de deux entiers s'exprime comme une combinaison arithmétique de ces deux entiers.

Proposition 29. *Soit $a, b, c \in \mathbb{Z}$, $c|a$ et $c|b$ si et seulement si $c|a \wedge b$.*

Preuve :
($\Longrightarrow$) On utilise la relation de Bézout de a et b : il existe $u, v \in \mathbb{Z}$ tel que $a \wedge b = au + bv$. Donc si $c|a$ et $c|b$. c divise toute combinaison arithmétique de a et de b donc en particulier $au + bv$.
($\Longleftarrow$) Si $c|a \wedge b$, alors comme $a \wedge b|a$ et $a \wedge b|b$, par transitivité $c|a$ et $c|b$. □

Ainsi, le pgcd de a et b est le plus grand au sens diviseur non plus seulement pour en terme de l'inégalité classique sur $\mathbb{N}$ mais également au sens de la relation de la divisibilité.

Quelques propriétés du PGCD

Proposition 30 (homogénéité du PGCD)**.** *Soit $k \in \mathbb{N}$, $a, b \in \mathbb{Z}$*

$$k(a \wedge b) = ka \wedge kb$$

Preuve : Il existe $u, v \in \mathbb{Z}$ tel que $a \wedge b = au + bv$ d'où $k(a \wedge b) = kau + kbv$.
Il suffit de montrer que le plus grand diviseur commun à ka et à kb est $k(a \wedge b)$.
On a déjà que $a \wedge b$ divise a donc $k(a \wedge b)$ divise ka, de même $k(a \wedge b)$ divise kb donc $k(a \wedge b)$ est un diviseur de ka et kb.
Soit l un diviseur commun à ka et kb, alors l divise $kau + kbv$ donc divise $k(a \wedge b)$. □

Proposition 31 (Associativité du PGCD)**.** *Soit $a, b, c \in \mathbb{Z}$, on a*

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

Preuve : Il suffit de montrer que l'ensemble des diviseurs communs de a et $b \wedge c$ est égal à l'ensemble des diviseurs communs de $a \wedge b$ et c.
Soit $l \in \mathbb{Z}$:

$$\begin{aligned} l|a \text{ et } l|b \wedge c &\iff l|a \text{ et } [l|b \text{ et } l|c] \\ &\iff l|a \text{ et } l|b \text{ et } l|c \\ &\iff [l|a \text{ et } l|b] \text{ et } l|c \\ &\iff l|a \wedge b \text{ et } l|c \end{aligned}$$

□

1.2.2 Entiers premiers entre eux

Définition 32. Soit $a, b \in \mathbb{Z}$, on dit que a et b sont **premiers entre eux** lorsque $a \wedge b = 1$.

Exemple 33. Les entiers 12 et 21 sont premiers entre eux.

Remarque 34. Soit $a, b \in \mathbb{Z}$, les entiers $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux par homogénéité du PGCD.

La notion de premiers entre eux est mise en avant avec le théorème suivant, fondamental en arithmétique.

Théorème 35. *Soit $a, b \in \mathbb{Z}$,*

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z} \,|\, au + bv = 1$$

Preuve : Le sens direct est immédiat avec la proposition 10. Pour le sens réciproque, supposons qu'il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$. Soit $k \in \mathbb{Z}$ un diviseur de a et b, alors k divise toute combinaison arithmétique de a et b donc divise 1. Ainsi $k = 1$. D'où $a \wedge b = 1$. □
Le théorème de Bézout admet deux corollaires très importants :

Théorème 36 (Lemme de Gauss)**.** *Soit $a, b, c \in \mathbb{Z}$, si $a|bc$ et $a \wedge b = 1$ alors $a|c$.*

Preuve : $a \wedge b$ donc d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$. En multipliant par c, on a $auc + bvc = c$. Or, comme $a|bc$, il existe $k \in \mathbb{Z}$ tel que $bc = ka$ d'où $c = auc + kav = a(uc + kv)$ d'où $a|c$. □

Proposition 37. *Soit $a, b, c \in \mathbb{Z}$ tel que $a|c$, $b|c$ et $a \wedge b = 1$ alors $ab|c$.*

Preuve : $a \wedge b$ donc d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$. De même en multipliant par c, on a $auc + bvc = c$. Comme $a|c$ et $b|c$ il existe $k, l \in \mathbb{Z}$ tel que $c = ka$ et $c = lb$. D'où $c = aulb + bvka = ab(ul + vk)$ d'où $ab|c$. □

Exemple 38. Un exemple application est le suivant :
Soit $P \in \mathbb{Z}[X]$ unitaire que l'on notera $P = X^n + \sum_{k=0}^{n-1} a_k X^k$, si α est une racine rationnelle de P alors $\alpha \in \mathbb{Z}$.
En effet, notons $\alpha = \frac{p}{q}$ avec $p \wedge q = 1$.
On a

$$P(\alpha) = \alpha^n + \sum_{k=0}^{n-1} a_k \alpha^k = \frac{p^n}{q^n} + \sum_{k=0}^{n-1} a_k \frac{p^k}{q^k} = 0$$

D'où en multipliant par q^n, on a

$$p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k}$$

Pour tout $k \in [\![0, n-1]\!]$, $q|a_k p^k q^{n-k}$ d'où $q|p^n$. Comme $q \wedge p = 1$ d'après le lemme de Gauss, on a $q|p$ d'où $\alpha \in \mathbb{Z}$.

1.2.3 Équations diophantiennes linéaires

Une autre application du lemme de Gauss et la résolution d'équations diophantiennes linéaires. On s'intéresse pour $a, b, c \in \mathbb{Z}$ à la résolution de l'équation

$$ax + by = c \quad (E)$$

avec $x, y \in \mathbb{Z}$.

Les relations de Bézout permettent de donner l'existence ou non de solutions :

Proposition 39. *L'équation (E) admet une solution si et seulement si $a \wedge b|c$.*

Preuve : Si (E) admet un couple de solution (x, y) alors comme $a \wedge b$ divise a et b, $a \wedge b$ divise $ax + by$ donc $a \wedge b$ divise c.
Réciproquement, en écrivant la relation de Bézout de a et b, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = a \wedge b$. Si $a \wedge b|c$, il existe $k \in \mathbb{Z}$ tel que $c = k(a \wedge b)$ d'où en multipliant la relation de Bézout par k, on a $auk + bvk = c$. Le couple (uk, vk) est solution de (E). □

Le théorème suivant permet de décrire dans le cas de l'existence d'une solution, l'ensemble des solutions :

Théorème 40. *Soit (x_0, y_0) une solution particulière de (E). L'équation (E) admet une infinité de solutions qui sont de la forme $(x_0 + kb, y_0 - ka), k \in \mathbb{Z}$.*

Preuve : (E) admet une solution donc quitte à diviser l'équation par $a \wedge b$, considérons que a et b sont premiers entre eux.
Analyse :

Soit (x, y) un couple de solution, comme (x_0, y_0) est solution de (E), on a $(E) \iff ax + by = ax_0 + by_0 \iff a(x - x_0) = b(y_0 - y)$.
Comme $b|a(x - x_0)$ et $a \wedge b = 1$, d'après le lemme de Gauss $b|x - x_0$, donc il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kb \iff x = x_0 + kb$.
De plus, $a(x_0 + kb) + by = ax_0 + by_0$ donc comme $b \neq 0$, on a $ka + y = y_0$ d'où $y = y_0 - ka$.
Ainsi on a $x = x_0 + kb$ et $y = y_0 - ka$.

Synthèse :
Montrons que les couples $(x_0 + kb, y_0 - ka)$ sont solutions :

$$a(x_0 + kb) + b(y_0 - ka) = ax_0 + by_0 = c$$

. □

Exemple 41. Résolvons l'équation diophantienne $2x + 3y = 1$.
$2 \wedge 3 = 1$ donc il existe au moins une solution que l'on peut trouver à l'oeil : $(-1, 1)$.
Soit (x, y) une solution de $2x + 3y = 1$, on a $2x + 3y = 2 \times -1 + 3 \times 1$ d'où $2(x + 1) = 3(1 - y)$.
Comme $3|2(x + 1)$ et $2 \wedge 3 = 1$, d'après le lemme de Gauss, $3|x + 1$ donc il existe $k \in \mathbb{Z}$ tel que $x + 1 = 3k$ d'où $x = -1 + 3k$.
De plus, comme $2(-1 + 3k) + 3y = 2 \times -1 + 3 \times 1$, on a $2k + y = 1$ d'où $y = 1 - 2k$.
On peut vérifier que les $(-1 + 3k, 1 - 2k)$ sont bien solutions.
D'où l'ensemble des solutions est $\{(-1 + 3k, 1 - 2k), k \in \mathbb{Z}\}$.

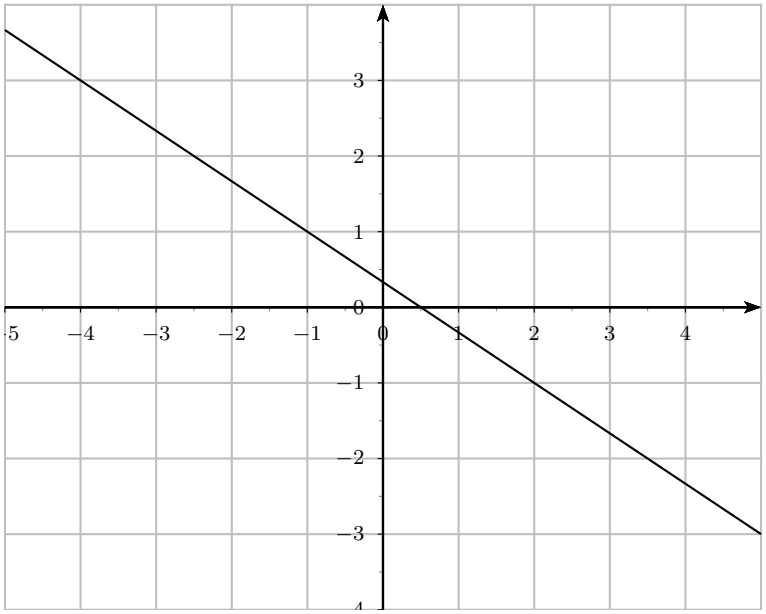


FIGURE 1.1 – La droite d'équation $2x + 3y = 1$ coupe le réseau $\mathbb{Z}^2$ aux solutions de l'équation diophantienne ci-dessus

1.2.4 PPCM

Définition 42. Soit $a, b \in \mathbb{Z}$, l'ensemble des multiples non nuls de a et de b est une partie de $\mathbb{Z}$ minorée par $\max(a, b)$, donc admet un plus petit élément appelé **PPCM** de a et de b, noté $a \vee b$.

Exemple 43. Les multiples de 16 sont $16, 32, 48, 64, \ldots$ et les multiples de 24 sont $24, 48, 72, \ldots$ dont le plus petit multiple commun est 48.

Proposition 44. *Soit $a, b \in \mathbb{Z}$, le PPCM de a et de b est le plus petit multiple de a et de b en terme de divisibilité : soit m un multiple de a et de b alors m est un multiple de $a \vee b$:*

$$\forall m \in \mathbb{Z}, [a|m \text{ et } b|m] \iff a \vee b|m$$

Preuve : ($\Longleftarrow$) Comme $a|a \vee b$ et $b|a \vee b$ et $a \vee b|m$ alors $a|m$ et $b|m$.
($\Longrightarrow$) Supposons que $a|m$ et $b|m$. Montrons que $a \vee b|m$.
Pour cela, écrivons la division euclidienne de m par $a \vee b$: il existe $q \in \mathbb{Z}$ et $0 \leq r < a \vee b$ tel que $m = q(a \vee b) + r$. D'où $r = m - q(a \vee b)$.
Comme $a|m$ et $a|a \vee b$, on a $a|r$ et de même $b|r$. Ainsi r est un multiple commun à a et b et est strictement plus petit que $a \vee b$ d'où $r = 0$. D'où $a \vee b|m$. □

Il y a une relation liant le PGCD et le PPCM :

Proposition 45. *Soit $a, b \in \mathbb{Z}$,*

$$|ab| = (a \wedge b) \times (a \vee b)$$

Preuve : Il suffit de prouver cette relation pour a et b positifs.
On peut écrire $a = da'$ et $b = db'$ avec $d = a \wedge b$ et $a' \wedge b' = 1$.
Il suffit de prouver que l'entier $da'b'$ est égal au PPCM de a et de b. Utilisons pour cela la caractérisation du PPCM précédente.
$da'b'$ est un multiple commun de a et de b. Soit m un multiple commun à a et b. Montrons que m est un multiple de $da'b'$.
Il existe $k \in \mathbb{Z}$ tel que $m = ka = kda'$ et il existe $l \in \mathbb{Z}$ tel que $m = lb = ldb'$ d'où $kda' = ldb'$ d'où $ka' = lb'$ car $d \neq 0$.
Or, $a' \wedge b' = 1$ donc d'après le lemme de Gauss, $a'|l$ donc il existe $n \in \mathbb{Z}$ tel que $l = na'$ d'où $m = nda'b'$ donc m est un multiple de $da'b'$. □

1.2.5 Généralisation à $n \geq 2$ entiers

Définition 46. Soit $a_1, \ldots, a_n$ n entiers. Comme le PGCD et le PPCM est associatif, on peut définir par récurrence le PGCD (resp. le PPCM) de $a_1, \ldots, a_n$ noté $\bigwedge_{k=1}^{n} a_k$ (resp. $\bigvee_{k=1}^{n} a_k$) comme étant $a_1 \wedge a_2$ si $n = 2$ et $(\bigwedge_{k=1}^{n-1} a_k) \wedge a_n$ si $n \geq 3$ (resp. $a_1 \vee a_2$ si $n = 2$ et $(\bigvee_{k=1}^{n-1} a_k) \vee a_n$ si $n \geq 3$.

Toutes les propriétés établit à présent se généralisent sans difficulté pour $n \geq 3$ entiers.

Définition 47. Soit $a_1, \ldots, a_n$ n entiers. On dit que $a_1, \ldots, a_n$ sont **premiers entre eux dans leurs ensemble** si $\bigwedge_{k=1}^{n} a_k = 1$.

Remarque 48. Il convient de distinguer la notion de premiers entre eux dans leurs ensemble et la notion de premiers entre eux deux à deux. Si $a_1, \ldots, a_n$ sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leurs ensemble mais la réciproque est fausse. Les entiers $6, 10$ et 15 ne sont pas premiers entre eux deux à deux mais sont premiers entre eux dans leurs ensemble.

Le théorème de Bézout se généralise par récurrence :

Proposition 49. *Soit $a_1, \dots, a_n \in \mathbb{Z}$.*

(i) Il existe $u_1, \dots, u_n \in \mathbb{Z}$ tel que $\bigwedge_{k=1}^{n} a_k = \sum_{k=1}^{n} u_k a_k$

(ii) $a_1, \dots, a_n$ sont premiers entre eux dans leurs ensemble si et seulement si il existe $u_1, \dots, u_n \in \mathbb{Z}$ tel que $\sum_{k=1}^{n} u_k a_k = 1$.

1.3 Nombres premiers

1.3.1 Définition et premières propriétés

Définition 50. Soit $n \in \mathbb{N}^*$, on dit que n est premier si n admet exactement deux diviseurs (lui-même et 1).

Un nombre non premier est appelé un nombre composé.

Remarque 51. 1 n'est pas un nombre premier

Exemple 52. Les nombres $2, 3, 5, 7, 11, 13$ sont premiers.

Remarque 53. Tous les nombres premiers sont impairs sauf 2.

Les nombres premiers constituent des "brique élémentaires" de l'arithmétique : en effet, tout nombre composé admet des diviseurs premiers. Nous préciserons ce fait dans la prochaine section.

Proposition 54. *Tout nombre entier ≥ 2 admet au moins un diviseur premier*

Preuve : Par récurrence forte, si $n = 2$, comme 2 est premier, il admet 2 comme diviseur premier.
Soit $n \in \mathbb{N}$ tel que pour tout $k \leq n$, k admet un diviseur premier. Montrons que $n+1$ admet un diviseur premier :
Si $n+1$ est premier alors il admet $n+1$ comme diviseur premier.
Si $n+1$ est composé, il existe $1 < a, b \leq n$ tel que $n+1 = ab$. Par hypothèse de récurrence, a admet un diviseur premier donc $n+1$ admet un diviseur premier. □

Un corollaire de cette proposition est le théorème d'Euclide qui affirme qu'il y a une infinité de nombres premiers :

Théorème 55 (d'Euclide)**.** *Il existe une infinité de nombres premiers.*

Preuve : Par l'absurde supposons qu'il existe un nombre fini N de nombre premier. Notons les $p_1, \dots, p_N$. Considérons l'entier $M = p_1 \times \cdots \times p_N + 1$.
Or, $\forall i \in [\![1, N]\!], M \equiv 1 \,[p_i]$ donc M n'admet pas de diviseur premier. Absurde. □

Pour déterminer si un nombre $n$est premier, on peut effectuer un test de primalité qui consiste à vérifier si il est divisible par k pour tout $1 < k < n$. La proposition suivante indique qu'il suffit de le verifier pour $k \leq \sqrt{n}$.

Proposition 56. *Soit n un nombre composé, n admet un diviseur $\leq \sqrt{n}$.*

Preuve : n est composé donc admet un diviseur dans $[\![2, n-1]\!]$. Considérons le plus petit diviseur dans $[\![2, n-1]\!]$ notons le a. Il existe donc $b \geq a$ tel que $ab = n$.
D'où $n = ab \geq b^2$ donc $b \leq \sqrt{n}$. □

Ainsi, par contraposition si n n'admet pas de diviseur $> \sqrt{n}$, alors n est premier.

Pour trouver tous les nombres premiers inférieurs à un entier donné, on utilise le test de primalité précédent sur chaque entier $k \leq n$. Cet algorithme est appelé **le crible d'Eratosthène** :

— On coche 1.
— Pour le prochain nombre premier p non criblé, on crible tous les kp $k \in [\![1, \frac{N}{p}]\!]$
— On arrête lorsque $p \geq \sqrt{N}$.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

FIGURE 1.2 – Crible d'Eratosthène pour $N = 100$

Calculons la complexité en nombre de fois où on crible un nombre :
On effectue pour chaque nombre premier $p \leq \sqrt{N}$, on crible $\frac{N}{p}$ fois d'où la complexité est dominé par

$$\sum_{\substack{p \leq \sqrt{N} \\ p \text{ premier}}} \left\lfloor \frac{N}{p} \right\rfloor \leq N \sum_{\substack{p \leq \sqrt{N} \\ p \text{ premier}}} \frac{1}{p}$$

.

1.3.2 Théorème fondamental de l'arithmétique

La vision des nombres premiers comme étant des "briques élémentaires de l'arithmétique" est justifiée par le théorème suivant dit "fondamental de l'arithmétique". Tout d'abord, montrons un lemme qui généralise le lemme de Gauss pour les nombres premiers.

Lemme 57. *Soit $a_1, \ldots, a_k \in \mathbb{Z}$, p un nombre premier. Si $p | a_1 \times \cdots \times a_k$ alors il existe $i \in [\![1, k]\!]$ tel que $p | a_i$*

Preuve : Montrons le lemme par récurrence sur k.
Si $k = 2$, alors comme $p | a_1 a_2$. Si $a_1 = p$ alors le résultat est vrai. Sinon comme p est premier, on a $p \wedge a_1 = 1$ donc d'après le lemme de Gauss $p | a_2$.

Supposons le résultat vrai pour un $k \in \mathbb{N}$ fixé. Montrons qu'il est vrai pour $k+1$. Soit $a_1, \ldots, a_{k+1}$ tel que $p | a_1 \times \cdots \times a_k \times a_{k+1}$. Si $p | a_1 \times \cdots \times a_k$ alors par hypothèse récurrence, il divise l'un des a_i. Sinon, comme p est premier, $p \wedge a_1 \times \cdots \times a_k$ donc d'après le lemme de Gauss, $p | a_{k+1}$. □

Passons maintenant au théorème :

Théorème 58 (fondamental de l'arithmétique)**.** *Soit $n \geq 2$, il existe une unique suite de nombre premier distincts $p_1, \ldots, p_k$ et d'entiers $\alpha_1, \ldots, \alpha_k$ tel que*

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$$

. Cette décomposition est appelée décomposition en facteurs premiers.

Preuve :

Existence :

Montrons l'existence d'une telle décomposition par récurrence forte.

Pour $n = 2$ la décomposition est déjà donnée.

Soit $n \in \mathbb{N}$ tel que tout $k \leq n$ admet une décomposition en facteurs premiers. Montrons que $n+1$ admet une décomposition en facteurs premiers.

- Si $n+1$ alors $n+1$ est sa propre décomposition en facteurs premiers.
- Si $n+1$ est composée, il existe $1 < a, b \leq n$ tel que $n+1 = ab$. Par hypothèse de récurrence il existe $p_1, \ldots, p_k, q_1, \ldots q_l$ des nombres premiers et des entiers $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$ tel que $a = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ et $b = q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$.
  La décomposition
  $$n+1 = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \times q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$$
  est une décomposition en facteurs premiers.

Unicité :

Supposons que $n \geq 2$ admet deux décomposition en facteurs premiers :

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$$

.

$p_1 | p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ donc $p_1 | q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$ donc d'après le lemme de Gauss, il existe $i \in [\![1, l]\!]$ tel que $p_1 | q_i$. Or, comme p_i et q_i sont premiers, on a $p_1 = q_i$. De même tout facteur premier de la décomposition de gauche est inclus dans la décomposition de droite et par symétrie, les facteurs de la décomposition sont égaux.

Montrons maintenant que les exposants sont égaux.

On a $p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k}$. Par l'absurde supposons qu'il existe $i \in [\![1, k]\!]$ tel que $\alpha_i \neq \beta_i$. Supposons que $\alpha_i > \beta_i$, alors en divisant par β_i, on a

$$p_1^{\alpha_1} \times \cdots \times p_i^{\alpha_i - \beta_i} \times \cdots \times p_k^{\alpha_k} = p_1^{\beta_1} \times \cdots \times p_{i-1}^{\beta_{i-1}} \times p_{i+1}^{\beta_{i+1}} \times \cdots \times p_k^{\alpha_k}$$

Donc $p_i | p_1^{\alpha_1} \times \cdots \times p_i^{\alpha_i - \beta_i} \times \cdots \times p_k^{\alpha_k}$ donc $p_i | p_1^{\beta_1} \times \cdots \times p_{i-1}^{\beta_{i-1}} \times p_{i+1}^{\beta_{i+1}} \times \cdots \times p_k^{\alpha_k}$ donc par lemme de Gauss divise un des p_r $r \neq i$ d'où comme p_r et p_i sont premiers, on a $p_i = p_r$. Absurde car les facteurs premiers sont distincts. D'où l'unicité. □

Exemple 59. La décomposition en facteurs premiers de 60 est $2^2 \times 3^1 \times 5^1$.

1.3.3 Valuation p-adique

Le théorème fondamental de l'arithmétique permet donc d'identifier un entier aux exposants des nombres premiers qui apparaissent dans la décomposition. Cela nous permet de poser la définition suivante :

Définition 60. Soit $n \in \mathbb{N}^*$, et p un nombre premier. On appelle **valuation p-adique** de n noté $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. On a donc :

$$v_p(n) = \max\{k \in \mathbb{N}\,,\, p^k | n\}$$

Exemple 61. Comme $60 = 2^2 \times 3^1 \times 5^1$, on a $v_2(60) = 2, v_3(60) = 1$ et $v_5(60) = 1$ et pour tout autre nombre premier p, on a $v_p(n) = 0$.

Remarque 62. On a pour tout p premier, $v_p(1) = 0$.

Ainsi, la décomposition en facteurs premiers peut s'écrire :

$$\forall n \in \mathbb{N}^*, n = \prod_{p \text{ premier}} p^{v_p(n)}$$

Ce produit contient un nombre fini de terme non égaux à 1 ce qui en justifie la convergence.

La valuation p-adique a une propriété de morphisme de monoïde :

Proposition 63. *Soit $a, b \in \mathbb{N}^*, v_p(ab) = v_p(a) + v_p(b)$.*

Preuve : Direct avec les propriétés sur les puissances et la décomposition en facteur premier. □ La valuation p-adique permet de calculer le PGCD et le PPCM de deux entiers :

Proposition 64. *Soit $a, b \in \mathbb{N}$,*

(i) $a|b \iff \forall p$ *premier* $v_p(a) \leq v_p(b)$

(ii) $a \wedge b = \prod_{p \text{ premier}} p^{\min(v_p(a), v_p(b))}$

(iii) $a \vee b = \prod_{p \text{ premier}} p^{\max(v_p(a), v_p(b))}$

Preuve :

(i) Supposons que $a|b$, il existe $k \in \mathbb{N}$ tel que $b = ka$. On a pour tout p premier, $v_p(b) = v_p(ka) = v_p(a) + v_p(k) \geq v_p(a)$.
Réciproquement, si pour tout p premier, $v_p(a) \leq v_p(b)$, alors

$$b = \prod_{p \text{ premier}} p^{v_p(b)} = \underbrace{\prod_{p \text{ premier}} p^{v_p(a)}}_{=a} \prod_{p \text{ premier}} p^{v_p(b) - v_p(a)}$$

d'où $a|b$.

(ii) D'après (i), $\prod_{p \text{ premier}} p^{\min(v_p(a), v_p(b))}$ est un diviseur commun à a et à b.
Soit k un diviseur de a et b, on a pour tout p premier , $v_p(k) \leq v_p(a)$ et $v_p(k) \leq v_p(b)$ d'où $v_p(k) \leq \min(v_p(a), v_p(b))$ d'où $v_p(k) | v_p(\prod_{p \text{ premier}} p^{\min(v_p(a), v_p(b))})$.
Donc $k | v_p(\prod_{p \text{ premier}} p^{\min(v_p(a), v_p(b))})$. Ainsi, par caractérisation $a \wedge b = \prod_{p \text{ premier}} p^{\min(v_p(a), v_p(b))}$.

(iii) Idem que (ii).

□

Enfin, parlons de la formule de Legendre qui permet de calculer la valuation p-adique de $n!$.

Théorème 65. *Soit $n \in \mathbb{N}^*$ et p un nombre premier.*

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

Remarque 66. Cette somme est en réalité finie car la suite $(p^k)_{k\in\mathbb{N}}$ est strictement croissante donc il existe $k \in \mathbb{N}$ tel que pour tout $l \geq k, p^l > n$ d'où $\left\lfloor \frac{n}{p^l} \right\rfloor = 0$.

Preuve :

$$v_p(n!) = v_p(\prod_{k=1}^{n} k) = \sum_{k=1}^{n} v_p(k)$$

Pour calculer l'exposant de p dans la décomposition en facteur premier de k, on note $\delta_i^k = 1$ si $p^i | k$ et 0 sinon. La valuation p-adique de k est égal à $\sum_{i=1}^{+\infty} \delta_i^k$.
D'où

$$v_p(n!) = \sum_{k=1}^{n} \sum_{i=1}^{+\infty} \delta_i^k = \sum_{i=1}^{+\infty} \sum_{k=1}^{n} \delta_i^k$$

Et $\sum_{k=1}^{n} \delta_i^k$ est le nombre d'entiers $1 \leq k \leq n$ tel que $p^i | k$ c'est donc $\left\lfloor \frac{n}{p^i} \right\rfloor$.
D'où $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$. □

Exemple 67. Calculons le nombre de zero dans l'ecriture décimale de 2021!.
Il s'agit de trouver le plus grand entier $k \in \mathbb{N}$ tel que $10^k | 2021!$. Or, $10^k = 2^k 5^k$ d'où comme $2^k \wedge 5^k = 1$, on a $10^k | 2021! \iff 2^k | 2021!$ et $5^k | 2021!$.
Calculons $v_2(2021!)$ et $v_5(2021!)$.
D'après la formule de Legendre :

$$v_2(2021!) = v_2(2021!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{2021}{2^k} \right\rfloor = 1010 + 505 + 252 + 126 + 63 + 31 + 15 + 7 + 3 + 1 = 2013$$

$$v_5(2021!) = v_5(2021!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{2021}{5^k} \right\rfloor = 404 + 80 + 16 + 3 = 503$$

. D'où il y a 503 zéros dans l'écriture décimale de 2021!.

Corollaire 68. *Soit $1 \leq k \leq n \in \mathbb{N}$, p un nombre premier, on a*

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

Exercice 69. Montrer que $4 | \binom{2n}{n}$ si et seulement si n n'est pas une puissance de 2.

On a d'après la formule de Legendre

$$v_2(\binom{2n}{n}) = \sum_{k=1}^{+\infty} \left\lfloor \frac{2n}{2^k} \right\rfloor - 2 \left\lfloor \frac{n}{2^k} \right\rfloor$$

$4 | \binom{2n}{n}$ si et seulement si $v_2(\binom{2n}{n}) \geq 2$.
Écrivons $n = 2^r q$ avec $q \wedge 1 = 1$:

$$\begin{aligned} v_2(\binom{2n}{n}) &= \sum_{k=1}^{r} \left\lfloor 2^{r+1-k} q \right\rfloor - 2 \left\lfloor 2^{r-k} q \right\rfloor + \sum_{k=0}^{+\infty} \left\lfloor \frac{q}{2^k} \right\rfloor - 2 \left\lfloor \frac{q}{2^{k+1}} \right\rfloor \\ &= \sum_{k=0}^{+\infty} \left\lfloor \frac{q}{2^k} \right\rfloor - 2 \left\lfloor \frac{q}{2^{k+1}} \right\rfloor \end{aligned}$$

Si $q = 1$, alors $v_2(\binom{2n}{n}) = 1$. Sinon il existe $k \in \mathbb{N}^*$ tel que $2^k \leq 2^{k+1}$ et on a donc en considérant le k-ème terme de la somme $v_2(\binom{2n}{n}) \geq 1 + \left\lfloor \frac{q}{2^k} \right\rfloor - 2\left\lfloor \frac{q}{2^{k+1}} \right\rfloor \geq 2$ d'où $4|\binom{2n}{n}$.

1.3.4 Petit théorème de Fermat

Concluons ce chapitre par ce théorème, très utile pour établir des congruences :

Théorème 70 (Petit théorème de Fermat)**.** *Soit $a \in \mathbb{Z}$, p un nombre premier. On a*

$$a^p \equiv a\,[p]$$

.
Si de plus $a \wedge p$, alors $a^{p-1} \equiv 1\,[p]$.

Preuve : Il suffit de montrer le résultat pour $a \in \mathbb{N}^*$.
Montrons le théorème par récurrence.
Si $a = 1$, alors le résultat est vrai.
Soit $a \in \mathbb{N}$ tel que $a^p \equiv a\,[p]$, montrons que $(a+1)^p \equiv a+1\,[p]$.
D'après la formule du binôme de Newton, $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k$.
Or, par hypothèse de récurrence, on a $a^p \equiv a\,[p]$. Il suffit donc de montrer que $p|\sum_{k=1}^{p-1} \binom{p}{k} a^k$.
Or, pour $k \in [\![1, p-1]\!]$, $k\binom{p}{k} = p\binom{p-1}{k-1}$, donc comme $p|k\binom{p}{k}$ et $p \wedge k = 1$ car p est premier et $k \in [\![1, p-1]\!]$, d'après le lemme de Gauss, $p|\binom{p}{k}$ d'où $p|\sum_{k=1}^{p-1} \binom{p}{k} a^k$ d'où le résultat.

De plus si $a \wedge p = 1$, alors comme $\underbrace{a^p - a}_{=a(a^{p-1}-1)} \equiv 0\,[p]$, on a $p|a(a^{p-1}-1)$ avec $a \wedge p = 1$ donc d'après le lemme de Gauss $p|a^{p-1} - 1$ d'où le résultat. □

Chapitre 2

Arithmétique modulaire : Étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Dans ce chapitre nous n'étudierons que l'aspect arithmétique de $\mathbb{Z}/n\mathbb{Z}$ pour pouvoir l'appliquer à l'arithmétique dans $\mathbb{Z}$. Nous n'étudierons pas l'aspect théorie des groupes de $\mathbb{Z}/n\mathbb{Z}$.

2.1 Définition et propriétés

2.1.1 Définition de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition 71. Soit $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence. Pour $k \in \mathbb{Z}$, on note $\overline{k}$ la classe d'équivalence de k pour cette relation c'est-à-dire l'ensemble des entiers qui sont congrus à k modulo n.

Exemple 72. Pour $n = 5$, on a :
$\overline{8} = \{\ldots, -2, 3, 8, 13, 18, 23, \ldots\}$.
$\overline{1} = \{\ldots, -4, 1, 6, 11, 16, 21, \ldots\}$.

Dans toute la suite, on fixe un entier $n \in \mathbb{N}^*$.

Proposition 73. *Soit $a, b \in \mathbb{Z}$,*

$$\overline{a} = \overline{b} \iff a \equiv b\,[n]$$

Preuve : Si $a \equiv b\,[n]$ alors si $k \in \overline{a}$, on a $k \equiv a\,[n]$, donc par transitivité $k \equiv b\,[n]$ d'où $k \in \overline{b}$ d'où $\overline{a} \subset \overline{b}$. Par symétrie, on a également $\overline{b} \subset \overline{a}$ d'où $\overline{a} = \overline{b}$.
Réciproquement si $a \equiv b\,[n]$, comme $a \in \overline{a}$, on a $a \in \overline{b}$ d'où $a \equiv b\,[n]$. □

Définition 74. Soit $n \in \mathbb{N}^*$, on appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{k}, k \in \mathbb{Z}\}$$

Avec cette définition, on peut penser que $\mathbb{Z}/n\mathbb{Z}$ est un ensemble infini mais il n'en est rien :

Proposition 75. *Soit $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n.*

Preuve : Montrons que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$. Soit $a \in \mathbb{Z}$, montrons que $\overline{a} \in \{\overline{0}, \dots, \overline{n-1}\}$. En effectuant la division euclidienne de a par n : il existe $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$ tel que $a = qn + r$ donc en passant à la congruence modulo n, on a $a \equiv r\,[n]$ d'où $\overline{a} = \overline{r}$. D'où $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \dots, \overline{n-1}\}$ d'où comme l'autre inclusion est immédiate, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$. Montrons à présent que $|\{\overline{0}, \dots, \overline{n-1}\}| = n$. Pour cela, il suffit de prouver que les $\overline{k}$ avec $k \in [\![0, n-1]\!]$ sont différents. Par l'absurde si il existe $k, l \in [\![0, n-1]\!]$ tel que $\overline{k} = \overline{l}$, on a $k \equiv l\,[n]$. D'où $k - l \equiv 0\,[n]$ d'où $n|k-l$ avec $k - l < n$. D'où $k - l = 0$ et $k = l$. Absurde. □

L'intérêt de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est que l'on peut le munir d'opérations :

Proposition-Définition 76. Soit $a, b \in \mathbb{Z}/n\mathbb{Z}$, soit k un représentant de a et l un représentant de b. La classe $\overline{k+l}$ ne dépend pas du choix du représentant k et l et est noté $a + b$.

Preuve : Soit k, k' deux représentants de a et l, l' deux représentants de b. Montrons que $\overline{k+l} = \overline{k'+l'}$ c'est-à-dire $k + l \equiv k' + l'\,[n]$.
Comme $\overline{k} = \overline{k'}$, on a $k \equiv k'\,[n]$ et de même $l \equiv l'\,[n]$ d'où par somme $k + l \equiv k' + l'\,[n]$. □

Proposition 77. *L'opération $+$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, commutatif, admet pour élément neutre $\overline{0}$ et pour tout $a \in \mathbb{Z}$ il existe un élément que l'on notera $-a$ vérifiant $a + (-a) = 0$.*

Preuve : L'associativité et la commutativité découle directement de l'associativité et la commutativité de l'addition classique. De même, on vérifie aisément que $\overline{0}$ est élément neutre et que pour tout $a \in \mathbb{Z}$, $\overline{a} + (\overline{-a}) = \overline{0}$. □

La proposition précédente dit que l'ensemble $(\mathbb{Z}/n\mathbb{Z}, +)$ a une structure de groupe abélien.

Proposition-Définition 78. Soit $a, b \in \mathbb{Z}/n\mathbb{Z}$, soit k un représentant de a et l un représentant de b. La classe $\overline{k \times l}$ ne dépend pas du choix du représentant k et l et est noté $a \times b$.

Preuve : Soit k, k' deux représentants de a et l, l' deux représentants de b. Montrons que $\overline{k \times l} = \overline{k' \times l'}$ c'est-à-dire $k \times l \equiv k' \times l'\,[n]$.
Comme $\overline{k} = \overline{k'}$, on a $k \equiv k'\,[n]$ et de même $l \equiv l'\,[n]$ d'où par somme $k \times l \equiv k' \times l'\,[n]$. □

Proposition 79. *L'opération $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, commutatif, admet pour élément neutre $\overline{1}$.*

Preuve : Idem que pour l'addition, les propriétés se découlent des propriétés de la multiplication classique. □

Ces opérations permettent de dire que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

2.1.2 Inverse modulo n

On s'intéresse maintenant à l'inversibilité dans $\mathbb{Z}/n\mathbb{Z}$: quels sont les éléments $a \in \mathbb{Z}/n\mathbb{Z}$ tel qu'il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 1$?

Soit $a \in \mathbb{Z}/n\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $\overline{k} = a$. Supposons que a admet un inverse b dans $\mathbb{Z}/n\mathbb{Z}$, il existe $l \in \mathbb{Z}$ tel que $\overline{l} = b$.
La condition $ab = 1$ se traduit par $\overline{kl} = \overline{1}$ ce qui est équivalent à $kl \equiv 1\,[n]$. D'où il existe $r \in \mathbb{N}$ tel que $kl = 1 + nr$ d'où $kl - nr = 1$. Le théorème de Bézout assure que cette condition est rempli si et seulement si $k \wedge n = 1$.
Reciproquement, on vérifie que si $k \wedge n = 1$ en écrivant la relation de Bézout, on trouve un inverse de k modulo n.

Définition 80. Soit $k \in \mathbb{Z}$, on dit que $l \in \mathbb{Z}$ est un inverse de k modulo n si $kl \equiv 1\,[n]$.

Le raisonnement précédent permet de prouver la proposition suivante :

Proposition 81. *Soit $a \in \mathbb{Z}/n\mathbb{Z}$ et k un représentant de a. a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.*

Dans ce cas, on trouve l'inverse de a en écrivant la relation de Bézout entre k et n.

Exemple 82. Dans $\mathbb{Z}/10\mathbb{Z}$, on a $3 \wedge 10$ donc $\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$. Pour calculer son inverse, on cherche la relation de Bézout entre 3 et 10 en appliquant l'algorithme d'Euclide : on a $10 + (-3) \times 3 = 1$ d'où l'inverse de $\overline{3}$ est $\overline{-3} = \overline{7}$.

Pour résoudre l'équation

$$ax \equiv b\,[n]$$

avec $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ d'inconnu $x \in \mathbb{Z}$.
Si $a \wedge n = 1$, alors a admet un inverse modulo n, notons le a^{-1} donc en multipliant par a^{-1}, on a $x \equiv a^{-1}b\,[n]$.
Si $a \wedge n \neq 1$, $ax \equiv b\,[n] \iff$ il existe $k \in \mathbb{Z}$ tel que $ax - kn = b$ donc la proposition 15 permet de dire que cette équation a une solution si et seulement si $a \wedge n | b$.

Le cas particulier si n est premier fournit le théorème suivant :

Théorème 83. *$\mathbb{Z}/n\mathbb{Z}$ est un corps (ie. tout élément non nul est inversible) si et seulement si n est premier.*

Preuve : Si n est premier, alors pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ non nul, il existe $k \in \mathbb{Z}$ tel que $a = \overline{k}$ tel que $k \not| n$ d'où $k \wedge n = 1$ donc a est inversible.
Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors de même tout élément non nul est inversible donc premier avec n. Donc n est premier. □

Ainsi, dans le cas où n est premier, les règles de calcul sont les mêmes que dans $\mathbb{R}$ car possèdent tous les deux une structure de corps.

Proposition 84 (Générateur de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $x \in \mathbb{Z}/n\mathbb{Z}$ et k tel que $x = \overline{k}$. Si $k \wedge n = 1$ alors x génère $\mathbb{Z}/n\mathbb{Z}$ c'est-à-dire pour tout $y \in \mathbb{Z}/n\mathbb{Z}$, il existe $l \in \mathbb{Z}$ tel que $lx = y$.*

Preuve : Soit m un représentant de y.
Comme $k \wedge n = 1$, en écrivant la relation de Bézout entre k et n : il existe $u, v \in \mathbb{Z}$ tel que $uk + nv = 1$, en multipliant par m, on a $muk + nvm = m$ d'où modulo n, on a $muk \equiv m\,[n]$ d'où en posant $l = mu$ on a $lk \equiv m\,[n]$ d'où $lx = y$. □

2.2 Théorème des restes chinois

Proposition-Définition 85. Soit $n_1, \ldots, n_k$ k entiers non nuls. On définit sur l'ensemble $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ une structure d'anneau en le munissant de l'addition + en sommant terme à terme les composantes et d'une multiplication en multipliant terme à terme les composantes.

On notera dans la suite pour $n \in \mathbb{Z}, \overline{n}^k$ sa classe d'équivalence pour la relation d'équivalence modulo k. C'est un élément de $\mathbb{Z}/k\mathbb{Z}$.

Exemple 86. Dans l'anneau $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, on a

$$(\overline{3}^4, \overline{5}^7) + (\overline{2}^4, \overline{1}^7) = (\overline{1}^4, \overline{6}^7)$$

$$(\overline{3}^4, \overline{5}^7) \times (\overline{2}^4, \overline{1}^7) = (\overline{2}^4, \overline{5}^7)$$

2.2.1 Le théorème

Théorème 87 (des restes chinois)**.** *Soit $n, m \in \mathbb{N}^*$, si $n \wedge m = 1$ alors l'application*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & \overline{k}^{nm} & \mapsto & (\overline{k}^n, \overline{k}^m) \end{array}$$

est un isomorphisme d'anneaux, c'est-à-dire c'est une application bijective vérifiant pour tout $x, y \in \mathbb{Z}/nm\mathbb{Z}$:

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

(ii) $\varphi(x + y) = \varphi(x) + \varphi(y)$

(iii) $\varphi(xy) = \varphi(x)\varphi(y)$

Preuve : Commençons par montrer que cette application est bien définie, c'est-à-dire qu'elle ne dépend pas du représentant k choisi.
Soit l, k deux représentants de $x \in \mathbb{Z}/nm\mathbb{Z}$. Montrons que $\varphi(\bar{l}) = \varphi(\bar{k})$. On a $\varphi(\bar{l}) = (\bar{l}^n, \bar{l}^m)$. Il suffit de montrer que $l \equiv k\,[n]$ et $l \equiv k\,[m]$. On a $l \equiv k\,[mn]$ donc $mn|l - k$. Comme $m \wedge n = 1$, alors $m|l - k$ et $n|l - k$ d'où $(\bar{l}^n, \bar{l}^m) = (\overline{k}^n, \overline{k}^m)$.

Les conditions (i),(ii) et (iii) sont immédiatement vérifiées.

Montrons que φ est bijective.
Montrons l'injectivité : Soit $x, y \in \mathbb{Z}/nm\mathbb{Z}$ tel que $\varphi(x) = \varphi(y)$. On a $\varphi(x - y) = 0$ donc en prenant un représentant k de x et l de y, on a $k - l \equiv 0\,[n]$ et $k - l \equiv 0\,[m]$ d'où $n|k - l$ et $m|k - l$. Comme $n \wedge m = 1$, alors $nm|k - l$ d'où $x - y = 0$. L'application est injective.
Comme on a égalité des cardinaux des ensembles de départ et d'arrivé, l'application est bijective.
□

Proposition 88. *Soit $n_1, \ldots, n_k \in \mathbb{N}^*$ tel que $n_1, \ldots, n_k$ sont premiers deux à deux, alors l'application*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}/n_1 \times \cdots \times n_k\mathbb{Z} & \to & \mathbb{Z}n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ & & \overline{k}^{n_1 \times \cdots \times n_k} & \mapsto & (\overline{k}^{n_1}, \ldots, \overline{k}^{n_k}) \end{array}$$

est un isomorphisme d'anneaux.

Preuve : Récurrence. □

Ainsi, pour $n \in \mathbb{N}^*$ de décomposition en facteurs premiers $p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$. L'étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$ revient à étudier l'anneau $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ donc à étudier les anneaux $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}, \ldots, \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$.

2.2.2 Application aux systèmes de congruences

Le théorème des restes chinois peut-être réecrit dans le cadre d'un système congruence :

Théorème 89 (des restes chinois)**.** *Soit $n_1, \dots, n_k$ des entiers premiers entre eux deux à deux. Pour tout entiers $a_1, \dots, a_k$, il existe un entier x unique modulo $n_1 \times \cdots \times$ tel que*

$$\begin{cases} x & \equiv a_1 \, [n_1] \\ & \vdots \\ x & \equiv a_k \, [n_k] \end{cases}$$

Preuve : Il suffit d'écrire le système d'équations comme une équation dans $\mathbb{Z}/n_1 \times \cdots \times n_k\mathbb{Z}$. Le système est équivalent à

$$\begin{aligned} (\overline{x}^{n_1}, \dots, \overline{x}^{n_k}) &= (\overline{a_1}^{n_1}, \dots, \overline{a_k}^{n_k}) \\ \varphi(\overline{x}^{n_1 \dots n_k}) &= (\overline{a_1}^{n_1}, \dots, \overline{a_k}^{n_k}) \end{aligned}$$

avec φ l'application du théorème chinois. Cette application est bien définis par les $n_1, \dots, n_k$ sont premiers entre eux deux à deux.
La bijectivité de φ nous garantit l'existence et l'unicité (modulo $n_1, \dots, n_k$) d'une telle solution. □

Exemple 90. Voici le problème original apparaissant dans le livre de Sun Zi au III-ème siècle et donnant naissance au théorème : Soient des objets en nombre inconnu, si on les range par 3, il en reste 2. Si on les range par 5, il en reste 3. Si on les range par 7, il en reste 2. Combien a-t'on d'objets ?
Soit x le nombre d'objets, x vérifie le système de congruence suivant :

$$\begin{cases} x & \equiv 2 \, [3] \\ x & \equiv 3 \, [5] \\ x & \equiv 2 \, [7] \end{cases}$$

Comme $3, 5$ et 7 sont premiers entre eux deux à deux, le théorème des restes chinois nous garantit l'existence et l'unicité (modulo 105) de la solution.

Pour trouver explicitement une solution on applique la méthode suivante :
Pour $i \in [\![1, k]\!]$, posons n_i' l'entier $n_1 \times n_{i-1} n_{i+1} \dots n_k$, on a $n_i \wedge n_i' = 1$ car les entiers sont premiers entre eux deux à deux. Ainsi n_i est inversible modulo n_i' donc il existe $n_i'^{-1}$ tel que $n_i'^{-1} n_i' \equiv 1 \, [n_i]$ et comme pour tout $j \neq i, n_j | n_i'$, on a $n_i'^{-1} n_i' \equiv 0 \, [n_j]$.
Ainsi l'entier $\sum_{k=1}^{i} a_i n_i'^{-1} n_i'$ vérifie le système de congruence.

Exemple 91. Dans notre exemple précédent, On a $n_1 = 3$ et $n_1' = 35$. En écrivant la relation de Bézout $-35 + 12 \times 3 = 1$, on a que -1 est un inverse de 35 modulo 3 donc $n_1'^{-1} n_1' = -35$.
On a $n_2 = 5$ et $n_1' = 21$. En écrivant la relation de Bézout $-4 \times 5 + 1 \times 21 = 1$, on a que 1 est un inverse de 21 modulo 5 donc $n_1'^{-1} n_1' = 21$.
On a $n_3 = 7$ et $n_1' = 15$. En écrivant la relation de Bézout $1 \times 15 - 2 \times 7 = 1$, on a que 1 est un inverse de 15 modulo 7 donc $n_1'^{-1} n_1' = 15$.
L'entier $2 \times -35 + 3 \times 21 + 2 \times 15 = 23$ est une solution du système et c'est l'unique solution dans $[\![1, 105]\!]$.

2.3 Groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z}, \times)$

2.3.1 Fonction indicatrice d'Euler

Définition 92. On appelle **fonction indicatrice d'Euler** noté φ la fonction qui à un entier n associe le nombre d'entiers inférieurs n qui sont premiers avec n :

$$\varphi(n) = |\{k \in [\![1, n]\!] \mid k \wedge n = 1\}|.$$

Comme un élément $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$, on a $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$.

La fonction indicatrice d'Euler sa calcule facilement pour les nombres premiers et pour les puissances de nombre premier :

Proposition 93. *Soit p un nombre premier et $\alpha \in \mathbb{N}$, on a*

(i) $\varphi(p) = p - 1$

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

Preuve :

(i) Si p est premier, alors il n'y a que p dans $[\![1, p]\!]$ qui n'est pas premier avec p d'où $\varphi(p) = p - 1$.

(ii) Soit $k \in \mathbb{N}^*$, k n'est pas premier avec p^α si et seulement si $p|k$ car tous les diviseurs de p^α sont des multiples de p. Ainsi les entiers non premiers avec p et inférieurs à p^α sont de la forme $kp, k \in [\![1, p^{\alpha-1}]\!]$. Ainsi, il y a $p^\alpha - p^{\alpha-1}$ entiers inférieurs à p^α qui sont premiers avec p^α.

□

Pour calculer $\varphi(n)$ lorsque n est composé, on utilise la proposition suivante :

Proposition 94. *Soit $a, b \in \mathbb{N}^*$ tel que $a \wedge b = 1$, alors*

$$\varphi(ab) = \varphi(a)\varphi(b)$$

On dit que φ est une fonction multiplicative.

Preuve : $\varphi(ab)$ est le cardinal de $\mathbb{Z}/ab\mathbb{Z}$ qui est d'après le théorème chinois isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Ainsi, les inversibles de $\mathbb{Z}/ab\mathbb{Z}$ sont exactement les inversibles de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Un tel inversible est formée en prenant un inversible de $\mathbb{Z}/a\mathbb{Z}$ et un inversible de $\mathbb{Z}/b\mathbb{Z}$: il y en a donc $\varphi(a)\varphi(b)$. □

Ainsi, en écrivant $n = p_1^{\alpha_1} \times p_k^{\alpha_k}$ la décomposition de n en facteurs premiers on a

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1} \times p_k^{\alpha_k}) \\
&= \varphi(p_1^{\alpha_1}) \times \varphi(p_k^{\alpha_k}) \qquad \text{car les } p_i \text{ sont premiers entre eux deux à deux} \\
&= p_1^{\alpha-1}(p_1 - 1) \times \cdots \times p_k^{\alpha_k - 1}(p_k - 1) \\
&= p_1^{\alpha} \times \cdots \times p_k^{\alpha_k} \times \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

Ainsi, pour $n = p_1^{\alpha_1} \times p_k^{\alpha_k}$ sa décomposition en facteurs premiers, on a :

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

La fonction indicatrice d'Euler se retrouve dans le théorème d'Euler, qui généralise le petit théorème de Fermat :

Théorème 95 (d'Euler)**.** *Soit $a \in \mathbb{Z}, n \in \mathbb{N}^*$, on a*

$$a^{\varphi(n)} \equiv 1\,[n]$$

Preuve : Il s'agit en fait de l'application du théorème de Lagrange au groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^\times$.
Montrons le directement dans ce cas. Notons r la classe d'équivalence de a dans $\mathbb{Z}/n\mathbb{Z}$ Notons $x_1, \ldots, x_{\varphi(n)}$ les différents éléments de $\mathbb{Z}/n\mathbb{Z}^\times$. L'application

$$\begin{array}{rccc} \psi & : & \mathbb{Z}/n\mathbb{Z}^\times & \to & \mathbb{Z}/n\mathbb{Z}^\times \\ & & x & \mapsto & rx \end{array}$$

est une bijection de $\mathbb{Z}/n\mathbb{Z}^\times$ d'inverse $\psi' : x \mapsto r^{-1}x$. Ainsi, les rx_i sont différents deux à deux par injectivité et tout élément x_i peut s'écrire sous la forme rx_j. Ainsi le produit$rx_1 \times \cdots \times rx_{\varphi(n)}$ est égal au produit $x_1 \times \ldots x_{\varphi(n)}$. D'où $r^{\varphi(n)}x_1 \times \ldots x_{\varphi(n)} = x_1 \times \ldots x_{\varphi(n)}$ d'où comme $x_1 \times \ldots x_{\varphi(n)}$ est inversible, on a $r^{\varphi(n)} = 1$ d'où $a^{\varphi(n)} \equiv 1\,[n]$. □

En particulier, si n est un nombre premier, on a $\varphi(n) = n - 1$, on a donc $a^{n-1} \equiv 1\,[n]$ ce qui est le petit théorème de Fermat.

2.3.2 Théorème de Wilson

Le théorème de Wilson constitue un critère de primalité :

Théorème 96. *Soit $p \in \mathbb{N}^*$.*

$$p \text{ est premier } \iff (p-1)! \equiv -1[p]$$

Preuve :
($\Longleftarrow$) Si $(p-1)! \equiv -1[p]$ alors soit $1 \leq k \leq p-1$, on a $k|(p-1)!$ donc si par l'absurde $k|p$ alors $(p-1)! \equiv 0\,[p]$. Absurde. D'où p est premier. ($\Longrightarrow$) Si p est premier alors en notant x_1 la classe de 1 modulo p,x_{p-1} la classe de $p-1$ modulo p. Calculons $x_1 \ldots x_{p-1}$. Comme chaque x_i est inversible, on peut regrouper dans le produit tous les termes avec leurs inverses. Ainsi :

$$\prod_{i=1}^{p-1} x_i = \underbrace{\prod_{\substack{i=1 \\ x_i^{-1} \neq x_i}}^{p-1} x_i}_{=1} \prod_{\substack{i=1 \\ x_i^{-1} = x_i}}^{p-1} x_i$$

Il s'agit de calculer le produit de tous les termes égaux à leurs propres inverses : or pour $x \in \mathbb{Z}/p\mathbb{Z}$ $x = x^{-1} \iff x^2 = \overline{1} \iff (x-\overline{1})(x+\overline{1}) = 0$ D'où les termes égaux à leurs inverses sont $\overline{1}$ soit $\overline{-1}$. Leur produit fait donc $\overline{-1}$. D'où $x_1 \ldots x_{p-1} = \overline{-1}$ d'où $(p-1)! \equiv -1\,[p]$. □

Le théorème de Wilson n'a que des intérêts théoriques car en pratique calculer algorithmiquement si un nombre est premier avec le théorème de Wilson devient vite long et d'autres algorithmes sont préférables.

Chapitre 3

Loi de réciprocité quadratique

Dans ce chapitre, nous allons établir la loi de réciprocité quadratique et parler de quelques applications.

Dans toute la suite p désignera un nombre premier impair.

3.1 Symbole de Legendre

3.1.1 Résidu quadratique et dénombrement

Définition 97. Soit $x \in \mathbb{Z}/p\mathbb{Z}$, on dit que x est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si il existe $y \in \mathbb{Z}/p\mathbb{Z}$ tel que $x = y^2$.

Définition 98. Soit $n \in \mathbb{Z}$, on dit que n est un **résidu quadratique** modulo p s il existe $k \in \mathbb{Z}$ tel que $n \equiv k^2\,[p]$

Ainsi, les classes d'équivalence des résidus quadratiques modulo p sont les carrés dans $\mathbb{Z}/p\mathbb{Z}$
Dénombrons le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$:

Proposition 99. *Il existe $\frac{p-1}{2}$ carrés inversibles dans $\mathbb{Z}/p\mathbb{Z}$.*

Preuve : La preuve repose sur un résultat de théorie des groupes, adaptons la démonstration dans notre cas :
Posons

$$\begin{array}{ccccc} \psi & : & (\mathbb{Z}/p\mathbb{Z})^\times & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ & & x & \mapsto & x^2 \end{array}$$

Il s'agit de dénombrer $\operatorname{Im}\psi$.
Pour $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$, on introduit la relation $x \sim y \iff \psi(x) = \psi(y)$. Il y a autant de classes d'équivalence que de carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
Calculons le cardinal de chaque classe d'équivalence : pour $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $x \sim y \iff \psi(x) = \psi(y) \iff x^2 = y^2 \iff (xy^{-1})^2 = 1 \iff xy^{-1} = \pm 1 \iff x = y$ ou $x = -y$. Comme x est non nul, x et $-x$ sont différents donc chaque classe d'équivalence comporte deux éléments distincts. Ainsi, en dénombrons $(\mathbb{Z}/p\mathbb{Z})^\times$ en partionnant avec les classes d'équivalence, on a $p - 1 = 2|\operatorname{Im}\psi|$ d'où $|\operatorname{Im}\psi| = \frac{p-1}{2}$. □

Le cas particulier de -1 est intéressant :

Proposition 100. *$\overline{-1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1\,[4]$*

Preuve : ($\Longrightarrow$) Supposons qu'il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $x^2 = \overline{-1}$. On a d'après le théorème d'Euler $x^{p-1} = \overline{1}$ donc comme p est impaire, on peut écrire $x^{p-1} = x^{2\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = 1$ d'où $\frac{p-1}{2}$ est paire : il existe $k \in \mathbb{Z}$ tel que $\frac{p-1}{2} = 2k$ d'où $p = 4k+1$.

($\Longleftarrow$) Supposons que $p \equiv 1\,[4]$, présentons deux méthodes :

Méthode 1 : Pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, on a d'après le théorème d'Euler $x^{p-1} = \overline{1}$. Si on a $x^2 = \overline{-1}$ alors on a $(x^2)^{\frac{p-1}{2}} = \overline{1}$, on a va donc chercher x comme étant racine d'une telle équation.
L'équation $x^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ solutions donc comme $(\mathbb{Z}/p\mathbb{Z})^\times$ a $p-1 > \frac{p-1}{2}$ éléments, il existe x tel que $x^{p-1}2 \neq 1$. Or, un tel élément verifie $x^2 = 1$ qui admet deux solutions 1 et -1 d'où $x^{p-1}2 = -1$. Comme $p \equiv 1\,[4]$ il existe $k \in \mathbb{Z}$ tel que $p = 4k+1$ d'où $\frac{p-1}{2} = 2k$ et $x^{p-1}2 = -1 \iff (x^k)^2 = -1$ d'où l'élément $y = x^k$ est une racine carré de -1 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
Méthode 2 : Comme p est premier, la formule de Wilson donne

$$\begin{aligned}(p-1)! &\equiv -1\,[p]\\ 1 \times \cdots \times (2k) \times (2k+1) \times \cdots \times (4k) &\equiv -1\,[4k+1]\\ 1 \times \cdots \times (2k) \times (-2k) \times \cdots \times (-1) &\equiv -1\,[4k+1]\\ (-1)^{2k}(1 \times \cdots \times (2k))^2 &\equiv -1\,[4k+1]\\ (1 \times \cdots \times (2k))^2 &\equiv -1\,[4k+1]\end{aligned}$$

En prenant $x = \overline{(1 \times \cdots \times (2k))}$, on a $x^2 = \overline{-1}$. □

Pour vérifier si un nombre est un carré dans $(\mathbb{Z}p\mathbb{Z})^\times$, on utilise la notation suivante :

3.1.2 Symbole de Legendre et critère d'Euler

Définition 101. Soit $x \in \mathbb{Z}$, on note :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } p|x \\ 1 & \text{si } p\not|x \text{ et } x \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } p\not|x \text{ et } x \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Exemple 102. On a $\left(\frac{-1}{p}\right) = 1$ si et seulement si $p \equiv 1\,[4]$.

Pour généraliser cette formule, on a besoin du critère d'Euler :

Théorème 103 (Critère d'Euler)**.** *Soit $x \in \mathbb{Z}$ tel que $p \wedge x = 1$, alors*

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}}\,[p]$$

Preuve : Il s'agit de généraliser la preuve pour $x = -1$.
L'équation $x^{\frac{p-1}{2}} = \overline{1}$ admet au plus $\frac{p-1}{2}$ solutions. Or, tous les carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ sont solutions car s'écrivent de la forme $x = y^2$ d'où $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Ainsi, l'ensemble des solutions de $x^{\frac{p-1}{2}} = \overline{1}$ sont exactement les carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
Pour $x \in \mathbb{Z}$, $\overline{x^{\frac{p-1}{2}}}$ vérifie l'équation $x^2 = 1$ donc est égal à 1 ou -1. Or, nd'après ce qui précède il est égal à 1 si et seulement si x est un carré dans $(\mathbb{Z}/pZ)^\times$. Ainsi, x n'est pas un carré dans $(\mathbb{Z}/pZ)^\times$ si et seulement si $\overline{x^{\frac{p-1}{2}}} = \overline{-1}$ d'où le résultat. □

Corollaire 104. *Soit $x, y \in \mathbb{Z}$, alors*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$

Preuve : Si p divise x ou y alors il divise xy donc la formule est vraie.
Si p ne divise ni x ni y, alors d'après la formule précédente, on a

$$\left(\frac{xy}{p}\right) \equiv (xy)^{\frac{p-1}{2}} \equiv x^{\frac{p-1}{2}} y^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \ [p]$$

Comme $p > 2$, et que le symbole de Legendre est à valeurs dans $\{1, -1\}$, on a égalité. □

3.1.3 Un autre calcul du symbole de Legendre

Soit $a \in \mathbb{Z}$ tel que $p \not| a$, notons $S = \{\overline{1}, \ldots, \overline{\frac{p-1}{2}}\}$, on a $\overline{a}\,\overline{s} \in (\mathbb{Z}/p\mathbb{Z})^\times$, écrivons $\overline{a}\,\overline{s}$ sous la forme $\overline{a}\,\overline{s} = \varepsilon_s(a)\overline{s_a}$ avec $\varepsilon_s(a) \in \{-1, 1\}$ et $s_a \in S$.
L'application

$$\begin{array}{rccc} \varphi & : & S & \to & S \\ & & \overline{s} & \mapsto & \overline{s_a} \end{array}$$

est bijective : en effet, pour $\overline{s}, \overline{t} \in S$, si $\overline{s_a} = \overline{t_a}$ alors $\varepsilon_s(a)\overline{as} = \varepsilon_t(a)\overline{at}$ d'où $\varepsilon_s(a)\overline{s} = \varepsilon_t(a)\overline{t}$ et $\overline{s} = \varepsilon_s(a)\varepsilon_t(a)\overline{t}$. Or, comme $1 \leq s, t \leq \frac{p-1}{2}$, on a forcément $\varepsilon_s(a)\varepsilon_t(a) = 1$ d'où φ est injective. D'après le principe des tiroirs, φ est bijective.
Cette application permet de donner une méthode de calcul de $\left(\frac{x}{p}\right)$

Proposition 105. *Soit $a \in \mathbb{Z}$ tel que $p \not| a$,*

$$\left(\frac{a}{p}\right) = (-1)^{\mu_a}$$

avec $\mu_a = |\{s \in S \,|\, \varepsilon_s(a) = -1\}|$

Preuve :

$$\prod_s^{\frac{p-1}{2}} \overline{s} \times \left(\frac{a}{p}\right) = \prod_s^{\frac{p-1}{2}} \overline{s} \times a^{\frac{p-1}{2}} = \prod_s^{\frac{p-1}{2}} \overline{as} = \prod_s^{\frac{p-1}{2}} \varepsilon_s(a) \prod_s^{\frac{p-1}{2}} \overline{s_a} = (-1)^{\mu_a} \prod_s^{\frac{p-1}{2}} \overline{s_a}$$

Or, comme φ est bijective, $\prod_s^{\frac{p-1}{2}} \overline{s_a} = \prod_s^{\frac{p-1}{2}} \overline{s}$ d'où comme le produit est non nul, en simplifiant on a la formule. □

Exemple 106. Pour $p = 11$, calculons $\left(\frac{5}{11}\right)$. On a :
$5 \times 1 = 5$ donc $\varepsilon_1(5) = 1$
$5 \times 2 = 10$ donc $\varepsilon_1(5) = -1$
$5 \times 3 = 15 \equiv 4\,[11]$ donc $\varepsilon_1(5) = 1$
$5 \times 4 = 20 \equiv 9\,[11]$ donc $\varepsilon_1(5) = -1$
$5 \times 5 = 25 \equiv 4\,[11]$ donc $\varepsilon_1(5) = 1$
D'où $\left(\frac{5}{11}\right) = (-1)^2 = 1$ donc 5 est résidu quadratique modulo 11.
On peut également calculer $5^5 = 3125 \equiv 1\,[11]$ donc d'après le critère d'Euler, 5 est un résidu quadratique modulo 11.

3.2 Loi de réciprocité quadratique

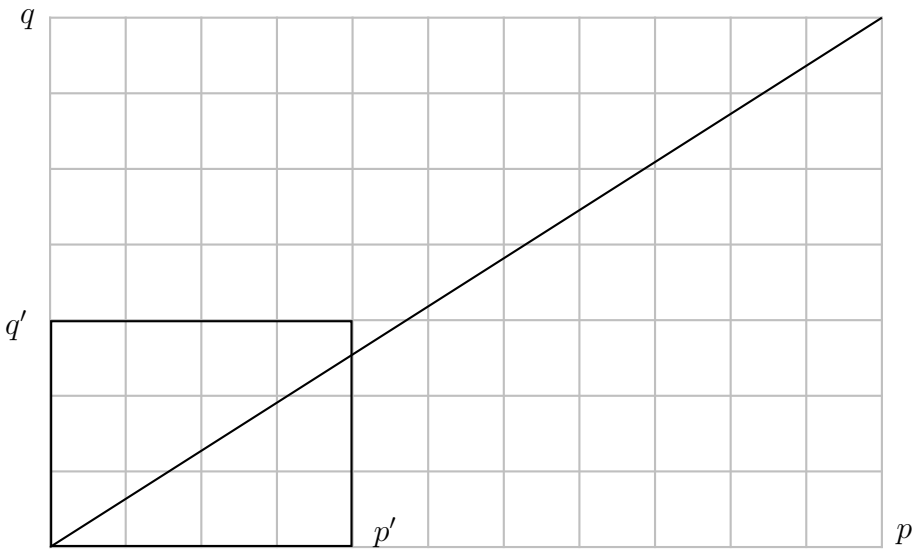
Dans la suite, pour un nombre premier impaire p, on pose $p' = \frac{p-1}{2}$. Passons au théorème principal du chapitre : tout d'abord, nous devons présenter un lemme :

Lemme 107. *Soit p, q deux nombres premiers impairs tel que $p \neq q$. Posons*

$$S_{pq} = \sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor \text{ et } S_{qp} = \sum_{s=1}^{q'} \left\lfloor \frac{sp}{q} \right\rfloor$$

On a la relation $S_{pq} + S_{qp} = p'q'$.

Preuve : Présentons une preuve graphique :



La somme S_{pq} représente le nombre de point dans le carré situé au dessus de la diagonale et la somme S_{qp} représente le nombre de point dans le carré situé en dessous de la diagonale.
Comme $p \wedge q = 1$, la somme ne coupe aucun point de coordonnées entières. Ainsi, en dénombrant les points situé dans le carré, on a la relation $S_{pq} + S_{qp} = p'q'$. □

Passons à présent à la formule :

Théorème 108 (Loi de réciprocité quadratique)**.** *Soit p, q deux nombres premiers impairs distincts et $x, y \in \mathbb{Z}$, on a :*

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

Preuve : Soit $1 \leq s \leq p'$, on effectue la division euclidienne de sq par p, on a $sq = \lfloor \frac{sq}{p} \rfloor p + u_s$ avec $0 \leq u_s \leq p-1$.
Si $u_s \leq p'$, alors $u_s = s_q$ et $\varepsilon_s(q) = 1$.
So $u_s > p'$, alors $u_s = p - s_q$ et $\varepsilon_s(q) = -1$. En sommant :

$$\begin{aligned}\sum_{s=1}^{p'} sq &= pS_{pq} + \sum_{\substack{s=1 \\ \varepsilon_s(q)=1}}^{p'} s_q + \sum_{\substack{s=1 \\ \varepsilon_s(q)=-1}}^{p'} (p - s_q) \\ &= pS_{pq} + \sum_{\substack{s=1 \\ \varepsilon_s(q)=1}}^{p'} s_q + p\mu_q - \sum_{\substack{s=1 \\ \varepsilon_s(q)=-1}}^{p'} s_q\end{aligned}$$

Donc modulo 2, on a comme p et q sont impairs

$$\sum_{s=1}^{p'} sq \equiv S_{pq} + \sum_{s=1}^{p'} s_q + p\mu_q \,[2]$$
$$q\frac{p'(p'+1)}{2} \equiv S_{pq} + \sum_{s=1}^{p'} s + \mu_q \,[2]$$
$$\frac{p'(p'+1)}{2} \equiv S_{pq} + \frac{p'(p'+1)}{2} + \mu_q \,[2]$$

D'où S_{pq} et μ_q sont de même parité.
De même S_{qp} et μ_p sont de même parité. D'où, d'après la proposition 34 :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu_p}(-1)^{\mu_q} = (-1)^{S_{pq}+S_{qp}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

Exemple 109. Supposons $p > 5$, On cherche sous quel condition $\overline{5}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$:
D'après la loi de réciprocité quadratique :

$$\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)$$

Modulo 5 les carrés sont 1 et 4 donc $\left(\frac{5}{p}\right) = 1$ si et seulement si $p \equiv 1\,[5]$ ou $p \equiv 4\,[5]$. Comme $(-1)^{\frac{p-1}{2}} = 1$ si et seulement si $p \equiv 1\,[4]$, le seul cas où les termes sont de même signe est le cas où $p \equiv 1\,[10]$. Ainsi, 5 est un résidu quadratique modulo p si et seulement si $p \equiv 1\,[10]$.

3.2.1 Équation du second degré

Il s'agit de résoudre l'équation

$$ax^2 + bx + c \equiv 0\,[p]$$

d'inconnue $x \in \mathbb{Z}$

Supposons $p \nmid a$ (dans le cas $p|a$, on peut se référer à la section 2.1.2).
Projetons cette équation dans $\mathbb{Z}/p\mathbb{Z}$. En factorisant comme dans $\mathbb{R}$, on a

$$\overline{ax^2 + bx + c} = \overline{a}[(\overline{x} + \overline{b}(2\overline{a})^{-1})^2 - \Delta(4\overline{a}^2)^{-1}]$$

Avec $\Delta = \overline{b^2 - 4ac}$

Théorème 110. *En posant $\Delta = b^2 - 4ac$:*
- *Si Δ n'est pas un résidu quadratique modulo p alors l'équation n'a pas de solution.*
- *Si $p|\Delta$, alors l'équation admet comme solution :*

$$\{-b(2a)^{-1} + kp,\ k \in \mathbb{Z}\}$$

  avec $(2a)^{-1}$ un inverse de $2a$ modulo p.
- *Si $p \nmid \Delta$ et Δ est un résidu quadratique modulo p, en posant δ tel que $\delta^2 = \Delta$, l'équation admet comme solution :*

$$\{(-b-\delta)(2a)^{-1} + kp, k \in \mathbb{Z}\} \cup \{(-b+\delta)(2a)^{-1} + kp, k \in \mathbb{Z}\}$$

Preuve : La preuve est similaire à la preuve sur $\mathbb{R}$ ou $\mathbb{C}$: on part de la factorisation

$$\overline{ax^2+bx+c} = \overline{a}[(\overline{x}+\overline{b}(2\overline{a})^{-1})^2 - \Delta(2\overline{a})^{-2}]$$

. Comme on souhaite résoudre $\overline{ax^2+bx+c} = 0$, et que $p \nmid a$, par lemme de Gauss, on a $(\overline{x} + \overline{b}(2\overline{a})^{-1})^2 - \overline{\Delta}(2\overline{a})^{-2} = 0$

- Supposons que Δ n'est pas un résidu quadratique modulo p, alors comme $\overline{\Delta} = [(\overline{x} + \overline{b}(2\overline{a})^{-1})(2\overline{a})]^2$, Δ est un résidu quadratique modulo p. Absurde. Donc l'équation n'a pas de solution.
- Si $p|\Delta$, alors $\overline{\Delta} = 0$, d'où $(\overline{x} + \overline{b}(2\overline{a})^{-1})^2 = 0$ donc d'après le lemme de Gauss on a $\overline{x} + \overline{b}(2\overline{a})^{-1} = 0$ d'où $\overline{x} = \overline{b}(2\overline{a})^{-1}$. Ainsi $x \equiv -b(2a)^{-1}\,[p]$.
- Si Δ est un résidu quadratique modulo p, alors il existe $\Delta = \delta^2$. On a alors $(\overline{x} + \overline{b}(2\overline{a})^{-1})^2 - \overline{\delta^2}(2\overline{a})^{-2} = (\overline{x}+\overline{b}(2\overline{a})^{-1})^2 - (\overline{\delta^2}(2\overline{a})^{-1})^2$ d'où en factorisant on a $(\overline{x}+\overline{b}(2\overline{a})^{-1})^2 - (\overline{\delta}(2\overline{a})^{-1})^2 = (\overline{x} + \overline{b}(2\overline{a})^{-1} - (\overline{\delta}(2\overline{a})^{-1}))(\overline{x} + \overline{b}(2\overline{a})^{-1} + (\overline{\delta}(2\overline{a})^{-1})) = 0$ d'où le résultat en utilisant le lemme de Gauss.

□

Exemple 111. Résolvons l'équation $x^2 - 31x + 18 \equiv 0\,[37]$.

Posons $\Delta = 31^2 - 4 \times 18 = 889 \equiv 1\,[37]$.
1 est un résidu quadratique modulo 37. Cherchons un inverse de 2 modulo 37 : $37 - 2 \times 18 = 1$ donc $-18 \equiv 19\,[37]$ est un inverse de 2 modulo 37. Posons $x_1 = (31-1) \times 19 = 570 \equiv 15\,[37]$ et $x_2 = (31+1) \times 19 = 608 \equiv 16\,[37]$. Les solutions sont donc :

$$\{15 + kp, k \in \mathbb{Z}\} \cup \{16 + kp, k \in \mathbb{Z}\}$$

3.3 Symbole de Jacobi

Le but du symbole de Jacobi est de généraliser le symbole de Legendre pour des nombres non premiers.

3.3.1 Définitions et propriétés

Définition 112. Soit $a, b \in \mathbb{Z}$, en posant $b = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On pose le symbole de Jacobi $\left(\frac{a}{b}\right)$ par

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \times \cdots \times \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Remarque 113. Le symbole de Jacobi n'a pas les mêmes propriétés que le symbole de Legendre. On peut avoir $\left(\frac{a}{b}\right) = 1$ même si a n'est pas un carré modulo p comme le montre l'exemple : pour $a = 2$ et $b = 9$, on a $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = (-1)^2 = 1$. Or 2 n'est pas un carré modulo 9.

Cependant, il existe un critère (un peu lourd) pour que a soit un résidu quadratique modulo b avec b impair :

Proposition 114. *Soit $a \in \mathbb{Z}$ et b un entier positif impair. a est un résidu quadratique modulo b si et seulement si a est un résidu quadratique modulo tous les facteurs premiers de b.*

Preuve : Notons $b = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ la décomposition en facteurs premiers de b.
($\Longrightarrow$) Supposons que a est un résidu quadratique modulo p, il existe $m \in \mathbb{Z}$ tel que $a \equiv m^2\,[b]$ Comme tout facteur premier p_i divise b alors pour tout $i \in [\![1, k]\!]$, $a \equiv m^2\,[p_i]$.
($\Longleftarrow$) Supposons que pour tout $i \in [\![1, k]\!]$, il existe $m_i \in \mathbb{Z}$ tel que $a \equiv m_i^2\,[p_i]$ Posons $m = m_1^{\alpha_1} \times \cdots \times m_k^{\alpha_k}$. Montrons que $a \equiv m^2\,[b]$. D'après le théorème chinois, il suffit que pour tout $i \in [\![1, k]\!], a \equiv m^2\,[p_i^{\alpha_i}]$ □

Proposition 115. *Soit $a, a', b, b' \in \mathbb{Z}$*

(i) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$

(ii) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

(iii) Si b est impaire, $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$

Preuve : En posant $b = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ et $b' = q_1^{\alpha_1} \times \cdots \times q_k^{\alpha_k}$

(i) On a

$$\left(\frac{aa'}{b}\right) = \left(\frac{aa'}{p_1}\right)^{\alpha_1} \times \cdots \times \left(\frac{aa'}{p_k}\right)^{\alpha_k}$$

puis on utilise la multiplicité du symbole de Legendre.

(ii) De même, en écrivant la décomposition en facteur premier de b et b' et en regroupant les termes, on trouve le résultat.

(iii)

$$\begin{aligned}\left(\frac{-1}{b}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1} \times \cdots \times \left(\frac{-1}{p_k}\right)^{\alpha_k} \\ &= ((-1)^{\frac{p_1-1}{2}})^{\alpha_1} \times \cdots \times ((-1)^{\frac{p_k-1}{2}})^{\alpha_k} \\ &= (-1)^{\frac{\alpha_1 p_1 + \cdots + \alpha_k p_k - (\alpha_1 + \cdots + \alpha_k)}{2}}\end{aligned}$$

Pour conclure, il suffit de conclure que $b - 1 \equiv \alpha_1 p_1 + \cdots + \alpha_k p_k - (\alpha_1 + \cdots + \alpha_k)2\,[2]$. Comme b est impaires, tous ses facteurs premiers sont impaires d'où

$$\alpha_1 p_1 + \cdots + \alpha_k p_k - (\alpha_1 + \cdots + \alpha_k) \equiv \alpha_1 + \cdots + \alpha_k - (\alpha_1 + \cdots + \alpha_k) \equiv 0\,[2]$$

D'où le résultat.

□

Proposition 116 (Généralisation de la loi de réciprocité quadratique)**.** *Soit a, b impairs tel que $a \wedge b = 1$, alors*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

Preuve : a et b sont premiers entre eux donc l'ensemble de leurs facteurs premiers sont disjoints. Notons $a = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ et $b = q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$.
On a

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{l}\left(\frac{a}{q_i}\right)^{\beta_i} = \prod_{i=1}^{l}\prod_{j=1}^{k}\left(\frac{p_j}{q_i}\right)^{\alpha_j\beta_i} = \prod_{i=1}^{l}\prod_{j=1}^{k}\left[(-1)^{\frac{(p_j-1)(q_i-1)}{4}}\left(\frac{q_i}{p_j}\right)\right]^{\alpha_j\beta_i}$$

D'après la loi de réciprocité quadratique pour les nombres premiers. D'où

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)\prod_{i=1}^{l}\prod_{j=1}^{k}(-1)^{\frac{\alpha_j(p_j-1)\beta_i(q_i-1)}{4}} = (-1)^{\frac{\sum_{j=1}^{k}\alpha_j(p_j-1)\sum_{i=1}^{l}\beta_i(q_i-1)}{4}}$$

Il suffit de montrer que $\frac{a-1}{2} \times \frac{b-1}{2}$ et $\frac{\sum_{j=1}^{k} \alpha_j (p_j - 1) \sum_{i=1}^{l} \beta_i (q_i - 1)}{4}$ ont la même parité. Comme a et b sont impairs, le résultat est vrai avec le même argument que la démonstration précédente. □

Chapitre 4

Fonction arithmétiques

On appelle fonction arithmétique une fonction définie sur $\mathbb{N}^*$ à valeurs dans $\mathbb{C}$. Nous allons étudier quelques aspects des fonctions arithmétiques et notamment des fonctions multiplicatives.

4.1 Convolution de Dirichlet

4.1.1 Fonction multiplicative

Définition 117. Soit f une fonction arithmétique, on dit que f est **multiplicative** si

(i) $f(1) = 1$

(ii) Pour tout $a, b \in \mathbb{N}^*$ tel que $a \wedge b = 1$, $f(ab) = f(a)f(b)$.

Exemple 118. La fonction constante égal à 1, la fonction identité et l'indicatrice d'Euler sont des fonctions arithmétiques.

Remarque 119. Si une fonction arithmétique f vérifie $f(1) = 1$ et pour tout $a, b \in \mathbb{N}^*$, $f(ab) = f(a)f(b)$, alors on dit que f est **complètement multiplicative**.

Soit $n \in \mathbb{N}^*$, en notant $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On a pour toute fonction multiplicative f :

$$f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$$

Ainsi, une fonction multiplicative est uniquement déterminée par ses valeurs sur les puissances des nombres premiers.

4.1.2 Convolution de Dirichlet

Dans toute la suite, pour $n \in \mathbb{N}^*$ on note $\mathcal{D}_n$ l'ensemble des diviseurs de n.

Définition 120. Soit f, g deux fonctions arithmétiques, on pose le produit de convolution $f \star g$ de f et g par

$$\forall n \in \mathbb{N}^*, (f \star g)(n) = \sum_{d \in \mathcal{D}_n} f(d) g\left(\frac{n}{d}\right)$$

Proposition 121. *Le produit de convolution est associatif, commutatif et admet pour élément neutre la fonction*

$$\begin{array}{rccl} \delta_1 & : & \mathbb{N}^* & \to & \mathbb{R} \\ & & n & \mapsto & \begin{cases} 1 & si\ n = 1 \\ 0 & sinon \end{cases} \end{array}$$

Preuve :
Montrons l'associativité du produit de convolution.
Soit f, g et h trois fonctions arithmétiques. Montrons que $(f \star g) \star h = f \star (g \star h)$.

$$\begin{aligned} ((f \star g) \star h)(n) &= \sum_{d \in \mathcal{D}_n} (f \star g)(d) h\left(\frac{n}{d}\right) \\ &= \sum_{d \in \mathcal{D}_n} \sum_{d' \in \mathcal{D}_d} f(d') g\left(\frac{d'}{d}\right) h\left(\frac{n}{d}\right) \end{aligned}$$

Or, en posant $\mathcal{C}_n = \{(d_1, d_2, d_3) | d_1 d_2 d_3 = n\}$, on a $\mathcal{C}_n = \{(d', \frac{d'}{d}, \frac{n}{d}) | d \in \mathcal{D}_n \text{ et } d' \in \mathcal{D}_d\}$. D'où

$$((f \star g) \star h)(n) = \sum_{(d_1, d_2, d_3) \in \mathcal{C}_n} f(d_1) g(d_2) h(d_3)$$

Par symétries des rôles joués par d_1, d_2 et d_3, on a également

$$(f \star (g \star h))(n) = \sum_{(d_1, d_2, d_3) \in \mathcal{C}_n} f(d_1) g(d_2) h(d_3)$$

d'où l'égalité.
Montrons la commutativité du produit de convolution.
On a $(f \star g)(n) = \sum_{d \in \mathcal{D}_n} f(d) g\left(\frac{n}{d}\right)$, donc en effectuant le changement d'indice $d' = \frac{n}{d}$, on a $(f \star g)(n) = \sum_{d' \in \mathcal{D}_n} g(d') f\left(\frac{n}{d'}\right) = (g \star f)(n)$.
Montrons que δ_1 est élément neutre pour le produit de convolution.
Soit $n \in \mathbb{N}^*, (f \star \delta_1)(n) = \sum_{d \in \mathcal{D}_n} f(d) g\left(\frac{n}{d}\right) = f(n)$ d'où $f \star \delta_1 = f$ et par commutativité on a également $\delta_1 \star f = f$. □

Les fonctions multiplicatives sont stables pour le produit de convolution :

Proposition 122. *Soit f, g deux fonctions multiplicatives, alors $f \star g$ est multiplicative.*

Preuve : On vérifie aisément que si $f(1) = 1$ et $g(1) = 1$, alors $(f \star g)(1) = 1$.
Soit $a, b \in \mathbb{N}^*$ tel que $a \wedge b = 1$. Montrons que $(f \star g)(ab) = (f \star g)(a)(f \star g)(b)$.

$$(f \star g)(ab) = \sum_{d \in \mathcal{D}_{ab}} f(d) g\left(\frac{ab}{d}\right)$$

Or, comme $a \wedge b = 1$, on dispose d'une bijection :

Lemme 123. *Soit $a, b \in \mathbb{N}^*$ tel que $a \wedge b = 1$, alors*

$$\begin{array}{rccl} \varphi & : & \mathcal{D}_a \times \mathcal{D}_b & \to & \mathcal{D}_{ab} \\ & & (d, d') & \mapsto & dd' \end{array}$$

est une bijection de $\mathcal{D}_a \times \mathcal{D}_b$ vers $\mathcal{D}_{ab}$.

Preuve : [du lemme]
La fonction est bien définie car si d est un diviseur de a et d' un diviseur de b, comme $a \wedge b = 1$, dd' est un diviseur de ab.
Posons $a = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ et $b = q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$ la décomposition en facteurs premiers de a et b. Commençons par l'injectivité, soit $(d_1, d_2), (d_1', d_2') \in \mathcal{D}_a \times \mathcal{D}_b$ tel que $d_1 d_2 = d_1' d_2'$. Montrons que $d_1 = d_1'$ et $d_2 = d_2'$.
Comme d_1 et d_1' sont des diviseurs de a, leurs facteurs premiers ne contiennent que des facteurs premiers de a. De même les facteurs premiers de d_2 et d_2' contiennent que des facteurs premiers de b. Ainsi, en écrivant l'écriture en facteurs de premiers de $d_1 d_2$ et de $d_1' d_2'$ et en utilisant l'unicité de la décomposition en facteurs premiers, on a nécessairement $d_1 = d_1'$ et $d_2 = d_2'$.
Montrons la surjectivité, soit m un diviseur de ab. Il existe $k \in \mathbb{Z}$ tel que $ab = rm = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \times q_1^{\beta_1} \times \cdots \times q_l^{\beta_l}$. Comme $r | ab$ alors il existe $I \subset [\![1, k]\!]$ et $J \subset [\![1, l]\!]$ tel que $k = \prod_{\substack{i \in I \\ j \in J}} p_i^{\alpha_i'} q_j^{\beta_j'}$ avec $\alpha_i' \leq \alpha_i$ et $\beta_j' \leq \beta_j$. Posons $m_A = \prod_{i \in [\![1,k]\!] \setminus I} p_i^{\alpha_i - \alpha_i'}$ et $m_B == \prod_{j \in [\![1,l]\!] \setminus L} q_i^{\beta_i - \beta_i'}$. On a $m = m_A m_B$ et $m_A | a$ et $m_B | b$ d'où la surjectivité. □
Ainsi, comme d'après le lemme D_{ab} et $D_a \times D_b$ sont en bijection, en ré-ecrivant la somme, on a

$$(f \star g)(ab) = \sum_{d_1 \in \mathcal{D}_a} \sum_{d_2 \in \mathcal{D}_b} f(d_1 d_2) g\left(\frac{a}{d_1}\frac{b}{d_2}\right) = \sum_{d_1 \in \mathcal{D}_a} \sum_{d_2 \in \mathcal{D}_b} f(d_1) f(d_2) g\left(\frac{a}{d_1}\right) g\left(\frac{b}{d_2}\right)$$

car comme $a \wedge b = 1$, pour tout diviseur d_1 de a et d_2 de b, on a $d_1 \wedge d_2 = 1$ et f et g sont multiplicatives.

$$(f \star g)(ab) = \sum_{d_1 \in \mathcal{D}_a} f(d_1) g\left(\frac{a}{d_1}\right) \sum_{d_2 \in \mathcal{D}_b} f(d_2) g\left(\frac{a}{d_2}\right) = (f \star g)(a)(f \star g)(b)$$

□

Comme $\star$ est associative, commutative et possède un élément neutre. On peut s'interroger sur l'inversibilité des fonctions multiplicatives pour $\star$, ce qui donnerait à l'ensemble des fonctions multiplicatives une structure de groupe abélien :

Pour f multiplicative, posons $g(1) = 1$ et pour tout nombre premier p et entier naturel k, posons par récurrence

$$g(p^k) = -\sum_{i=1}^{k} f(p^i) g(p^{k-i})$$

On définit ainsi une fonction multiplicative. Pour montrer que g est l'inverse de f pour $\star$. Il suffit pour cela de le montrer sur les p^k avec p premier et $k \in \mathbb{N}^*$. Montrons par récurrence ce résultat. Le résultat est vraie pour $k = 0$, supposons que pour $k \in \mathbb{N}^*$ on a $(f \star g)(p^k) = \delta_1(p^k) = 0$. Montrons que $(f \star g)(p^{k+1}) = \delta_1(p^{k+1}) = 0$.
On a $(f \star g)(p^k) = \sum_{i=0}^{k} f(p^{k-i}) g(p^i) = 0$.

$$\begin{aligned}(f \star g)(p^{k+1}) &= \sum_{i=0}^{k+1} f(p^{k+1-i}) g(p^i) \\ &= \sum_{i=0}^{k} f(p^{k-i}) g(p^i) + g(p^{k+1}) = 0\end{aligned}$$

D'où g est l'inverse de f pour $\star$.

4.1.3 Formule d'inversion de Möbius

Définition 124. On appelle **fonction de Möbius** la fonction définie sur $\mathbb{N}^*$ par :

$$\begin{array}{rccl} \mu & : & \mathbb{N}^* & \to & \mathbb{R} \\ & & n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

Exemple 125.
On a $\mu(6) = 1$ car $6 = 2 \times 3$, c'est le produit de deux nombres premiers distincts.
On a $\mu(50) = 0$ car $50 = 2 \times 5^2$, ce n'est pas le produit de deux nombres premiers distincts.
On a $\mu(30) = -1$ car $30 = 2 \times 3 \times 5$, c'est le produit de trois nombres premiers distincts.

La fonction de Möbius est fondamentale pour le théorème suivant :

Théorème 126 (Inversion de Möbius)**.** *Soit f une fonction multiplicative. Posons $F(n) = \sum_{d|n} f(d)$ la somme des diviseurs de f. On dispose de la formule suivante :*

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Preuve : La formule peut se ré-écrire $f = \mu \star F$. Or $F = f \star 1$. Il s'agit donc de montrer que $\mu \star (f \star 1) = f$ ce qui, par commutativité et associativité revient à montrer $\mu \star 1 = \delta_1$. Les fonctions coïncident en $n = 1$, montrons que les deux fonctions coïncident pour $n \geq 2$,

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)$$

Posons $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ la décomposition de n en facteurs premiers. La somme est non nulle si et seulement si d est de la forme $\prod_{i \in I} p_i$ avec I une partie de $[\![1, k]\!]$. Dans ce cas, on a

$$\sum_{d|n} \mu(d) = \sum_{I \subset [\![1,k]\!]} (-1)^{|I|} = \sum_{i=0}^{k} \sum_{\substack{I \subset [\![1,k]\!] \\ |I|=i}} (-1)^i = \binom{k}{i} (-1)^i = 0$$

□

En particulier, la preuve montre que l'inverse de la fonction constante égale à 1 est la fonction de Möbius.

Un exemple important est celui de l'indicatrice d'Euler :

Proposition 127. *Soit $n \in \mathbb{N}^*$,*

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

Autrement dit, $\mathrm{id} = \varphi \star 1$.

Preuve : Pour d un diviseur de n, posons $A_d = \{k \in [\![1, n]\!] \mid k \wedge n = d\}$.
Les $(A_d)_{d|n}$ forment une partition de $[\![1, n]\!]$ (car pour tout entier $k \in [\![1, n]\!]$, $k \wedge n$ est un diviseur

de n et donc appartient à l'un des A_d et les A_d sont deux à deux disjoints).
Pour d un diviseur de n, calculons $|A_d|$.
Soit $k \in [\![1,n]\!]$, $k \in A_d \iff k \wedge n = d \iff k \wedge \frac{n}{d} = 1$. Il y a donc autant d'élément dans A_d que dans $\{k \in [\![1,n]\!] \mid k \wedge \frac{n}{d} = 1\}$ donc $|A_d| = \varphi\left(\frac{n}{d}\right)$.
Ainsi, $n = |[\![1,n]\!]| = \sum_{d|n} |A_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$. En effectuant le changement d'indice dans la somme $d' = \frac{n}{d}$ (qui parcourt les diviseurs de n lorsque $\frac{n}{d}$ parcourt les diviseurs de n). On obtient :

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

□

Exercice 128. Soit A la matrice de $\mathcal{M}_n(\mathbb{C})$, définie par pour $i,j \in [\![1,n]\!]$, $M_{ij} = i \wedge j$. Calculer $\det(M)$.

On a $M_{ij} = i \wedge j = \sum_{d|i\wedge j} \varphi(d) = \sum_{d|i}\sum_{d|j} \varphi(d) = \sum_{d=1}^{n} \varphi(d) b_{di} b_{dj}$ avec $b_{dk} = 1$ si $d|k$ et 0 sinon.
On dit que la matrice $B = (b_{ij})$ est la matrice d'incidence de la divisibilité. C'est une matrice triangulaire supérieure avec des 1 sur la diagonale.
La relation s'écrit $M = B^T \mathrm{diag}(\varphi(1), \ldots, \varphi(n)) B$ d'où en passant au déterminant, on a

$$\det(M) = \prod_{d=1}^{n} \varphi(d).$$

Ce déterminant est appelé le **déterminant de Smith**.

4.1.4 Application : Probabilité que deux entiers soient premiers entre eux

Considérons le problème suivant : on choisit au hasard deux entiers dans $[\![1,n]\!]$. Quel est la probabilité que ces deux entiers soient premiers entre eux ?

Notons $A_n = \{(a,b) \in [\![1,n]\!] | a \wedge b = 1\}$. La probabilité p_n recherchée est donc $p_n = \dfrac{|A_n|}{n^2}$.
Pour calculer $|A_n|$, posons $p_1, \ldots, p_k$ les nombres premiers appartenant à $[\![1,n]\!]$ et posons $U_i = \{(a,b) \in [\![1,n]\!] \,|\, p_i|a \text{ et } p_i|b\}$.
A_n est alors le complémentaire de l'union des U_i donc $|A_n| = n^2 - |\bigcup_{i=1}^{k} U_i|$. Pour calculer le cardinal de cette union, nous avons besoin de la formule du crible de Poincaré : on a

$$\left|\bigcup_{i=1}^{k} U_i\right| = \sum_{\substack{I \subset [\![1,k]\!] \\ I \neq \emptyset}} (-1)^{|I|+1} \left|\bigcap_{i\in I} U_i\right|$$

Et $n \in \bigcap_{i\in I} U_i \iff \prod_{i\in I} p_i | n$ d'où $\left|\bigcap_{i\in I} U_i\right| = \left\lfloor \dfrac{n}{\prod_{i\in I} p_i} \right\rfloor^2$. On a ainsi

$$|A_n| = n^2 - \sum_{\substack{I \subset [\![1,k]\!] \\ I \neq \emptyset}} (-1)^{|I|+1} \left\lfloor \frac{n}{\prod_{i\in I} p_i} \right\rfloor^2 = \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$$

car cette somme ne contient qu'en réalité que les produit de nombre premiers distincts. D'où la formule suivante :

$$p_n = \frac{1}{n^2}\sum_{d=1}^{n}\mu(d)\left\lfloor\frac{n}{d}\right\rfloor^2$$

Ainsi, $n \mapsto n^2 p_n$ se présente comme l'inverse de Möbius de la partie entière au carré.

Nous pouvons calculer la limite de p_n avec quelques outils d'analyse :

Commençons par montrer que $p_n \xrightarrow[n\to+\infty]{} \sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}$.

On a pour $n \in \mathbb{N}^*$n

$$\begin{aligned}|p_n - \sum_{d=1}^{n}\frac{\mu(d)}{d^2}| &= |\sum_{d=1}^{n}\mu(d)\left[\left\lfloor\frac{n}{d}\right\rfloor^2 - \frac{1}{d^2}\right]| \\ &\leq \sum_{d=1}^{n}\left|\frac{1}{n^2}\left\lfloor\frac{n}{d}\right\rfloor^2 - \frac{1}{d^2}\right|\end{aligned}$$

Et $\frac{n}{d} - 1 \leq \left\lfloor\frac{n}{d}\right\rfloor \leq \frac{n}{d}$ d'où comme les termes sont positifs $(\frac{n}{d})^2 - \frac{2n}{d} + 1 \leq \left\lfloor\frac{n}{d}\right\rfloor^2 \leq \frac{n}{d}^2$ d'où $\frac{1}{n^2} - \frac{2}{nd} \leq \frac{1}{n^2}\left\lfloor\frac{n}{d}\right\rfloor^2 \leq 0$ d'où la majoration

$$|p_n - \sum_{d=1}^{n}\frac{\mu(d)}{d^2}| \leq \sum_{d=1}^{n}\mu(d)\frac{1}{n^2} - \frac{2}{nd} = \frac{1}{n} - \frac{2}{n}\sum_{d=1}^{n}\frac{1}{d} \xrightarrow[n\to+\infty]{} 0$$

On peut calculer explicitement la somme $\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}$. En effet, comme la famille $(\frac{\mu(d)}{d^2})$ est sommable, on a :

$$\begin{aligned}\left(\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}\right)\left(\sum_{n=1}^{+\infty}\frac{1}{n^2}\right) &= \sum_{d,n=1}^{+\infty}\frac{\mu(d)}{(dn)^2} \\ &= \sum_{\substack{d=1\\ n|p}}^{+\infty}\frac{\mu(d)}{p^2} \\ &= \sum_{p=1}^{+\infty}\sum_{d|p}\frac{\mu(d)}{p^2} \\ &= \sum_{p=1}^{+\infty}\frac{1}{p^2}\sum_{d|p}\mu(d) \\ &= 1 \quad \text{d'après la formule d'inversion de Möbius}\end{aligned}$$

Ainsi comme on a la formule $\sum_{n=1}^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$, on a la formule suivante :

$$p_n \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}$$

4.2 Séries de Dirichlet

4.2.1 Définition et abscisse de convergence

Définition 129. Soit f une fonction arithmétique, on définit la **série de Dirichlet** de f par la fonction (lorsqu'elle est définie)

$$L_f(s) = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s}$$

Définition 130. L'ensemble des $\{s > 0 | \sum_n \frac{f(n)}{n^s}$ converge$\}$ est une partie non-vide minorée de $\mathbb{R}$ donc admet une borne inférieure. On appelle **abscisse de convergence** noté $A_c(f)$:

$$A_c(f) = \inf(\{s > 0 | \sum_n \frac{f(n)}{n^s} \text{ converge}\})$$

Proposition 131. *Soit f une fonction arithmétique, pour tout $s > A_c(f)$, la série de Dirichlet en s de f converge absolument.*

Preuve : Comme $s > A_c(f)$, il existe $A_c(f) < t < s$ tel que $\sum_n \frac{|f(n)|}{n^t}$ converge d'où

$$\frac{\frac{|f(n)|}{n^s}}{\frac{|f(n)|}{n^t}} = \frac{1}{n^{s-t}} \xrightarrow[n\to+\infty]{} 0$$

D'où par comparaison pour les séries à termes positifs, la série $\sum_n \frac{f(n)}{n^s}$ converge absolument. □

Proposition 132 (Injectivité des séries de Dirichlet)**.** *Soit f, g des fonctions arithmétiques, tel que pour tout $s > \max(A_c(f), A_c(g))L_f(s) = L_g(s)$, alors $f = g$.*

Preuve : Supposons par l'absurde que $f \neq g$, posons k_0 le premier entier tel que $f(k_0) \neq g(k_0)$. On a :

$$\begin{aligned} 0 = L_f(s) - L_g(s) &= \left| \sum_{k=k_0}^{+\infty} \frac{f(k) - g(k)}{k^s} \right| \\ &= \frac{f(k_0) - g(k_0)}{k_0^s} + \sum_{k=k_0+1}^{+\infty} \frac{f(k) - g(k)}{k^s} \end{aligned}$$

En multipliant par k_0^s, on a

$$0 = f(k_0) - g(k_0) + \sum_{k=k_0+1}^{+\infty} (f(k) - g(k)) \left(\frac{k_0}{k}\right)^s$$

Avec

$$\left| \sum_{k=k_0+1}^{+\infty} (f(k) - g(k)) \left(\frac{k_0}{k}\right)^s \right| \leq \sum_{k=k_0+1}^{+\infty} |f(k) - g(k)| \left(\frac{k_0}{k}\right)^s$$

Soit s_0 tel que $s > s_0 > \max(A_c(f), A_c(g))L_f(s)$. On a :

$$\begin{aligned}\left|\sum_{k=k_0+1}^{+\infty}(f(k)-g(k))\left(\frac{k_0}{k}\right)^s\right| &\leq \sum_{k=k_0+1}^{+\infty}|f(k)-g(k)|\left(\frac{k_0}{k}\right)^{s_0}\left(\frac{k_0}{k}\right)^{s-s_0}\\ &\leq \sum_{k=k_0+1}^{+\infty}|f(k)-g(k)|\left(\frac{k_0}{k}\right)^{s_0}\left(\frac{k_0}{k_0+1}\right)^{s-s_0}\\ &\leq \left(\frac{k_0}{k_0+1}\right)^{s-s_0}\left(\sum_{k=k_0+1}^{+\infty}|f(k)-g(k)|\left(\frac{k_0}{k}\right)^{s_0}\right)\end{aligned}$$

La somme converge car $s_0 > \max(A_c(f), A_c(g))$ et comme $k_0 + 1 > k_0$, on a

$$\left(\frac{k_0}{k_0+1}\right)^{s-s_0} \xrightarrow[s\to+\infty]{} 0$$

D'où $|f(k_0) - g(k_0)| = 0$ ce qui est absurde. D'où $f = g$. □

Les séries de Dirichlet ont une compatibilité avec la convolution :

Proposition 133. *Soit f, g deux fonctions arithmétiques, pour $s \geq \max(A_c(f), A_c(g))$, on a*

$$L_{f\star g}(s) = L_f(s) \times L_g(s)$$

Preuve : Soit $s \geq \max(A_c(f), A_c(g))$, comme les séries $\sum_n \frac{f(n)}{n^s}$ et $\sum_n \frac{g(n)}{n^s}$ convergent absolument. Les familles sont sommables, d'après le théorème de sommation par paquet on a

$$\begin{aligned}\left(\sum_{a=1}^{+\infty}\frac{f(a)}{a^s}\right)\left(\sum_{b=1}^{+\infty}\frac{g(b)}{b^s}\right) &= \sum_{a,b=1}^{+\infty}\frac{f(a)g(b)}{(ab)^s}\\ &= \sum_{p=1}^{+\infty}\sum_{d|p}\frac{f(d)g\left(\frac{n}{d}\right)}{p^s}\\ &= \sum_{p=1}^{+\infty}\frac{(f\star g)(p)}{p^s}\end{aligned}$$

□

4.2.2 Fonction Zêta de Riemann

Définition 134. Pour $s > 1$, la série $\sum_{n\geq 1}\frac{1}{n^s}$ converge. Sa somme est noté $\zeta(s)$.

$$\zeta(s) = \sum_{n=1}^{+\infty}\frac{1}{n^s}$$

Exemple 135. En particulier, on a $\zeta(2) = \sum_{n=1}^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$.

Proposition 136. *La fonction ζ vérifie les propriétés suivantes :*

(i) *ζ est strictement décroissante sur $]1, +\infty[$*

(ii) $\lim_{x\to 1}\zeta(x) = +\infty$ *et* $\lim_{x\to+\infty}\zeta(x) = 0$

(iii) $\zeta(x) \sim_{x\to+\infty} \frac{1}{x-1}$

Preuve : Ces propriétés découlent d'une étude de fonction. La fonction ζ est dérivable grâce à la convergence uniforme sur tout compact de la série de fonction. □

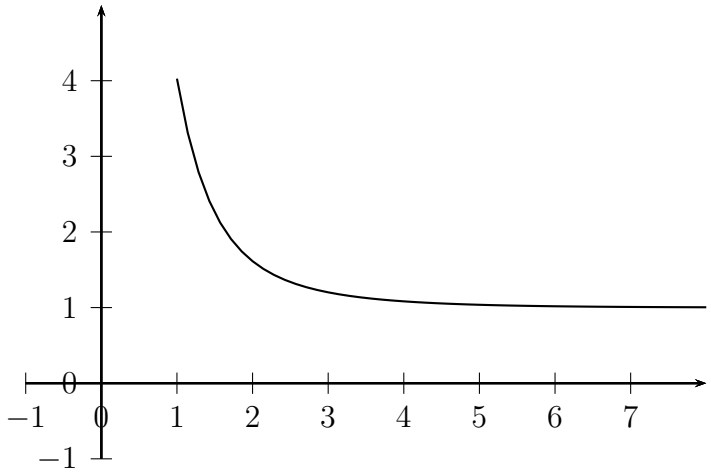


FIGURE 4.1 – Représentation graphiquement de la fonction Zêta

Remarque 137. La fonction Zêta est la série de Dirichlet associée à la fonction constante égale à 1. Son abscisse de convergence est 1.

La compatibilité du produit de Dirichlet permet de prouver des convergences de séries de Dirichlet.

Comme $\mu \star 1 = \delta_1$, on a pour $s > 1$

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$$

Comme $\varphi \star 1 = \mathrm{id}$, on a pour $s > 2$ $\zeta(s) \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s} = \zeta(s-1)$ d'où

$$\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

La fonction *zeta* permet d'établir un lien entre l'analyse et l'arithmétique. En effet, on peut exprimer la fonction *zeta* à l'aide d'un produit portant sur tous les nombres premiers.

Théorème 138 (Produit Eulérien)**.** *Soit f une fonction bornée par 1 et complètement multiplicative. Alors pour tout $s > 1$:*

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} = \prod_{p \text{ premier}} \left(1 - \frac{f(p)}{p^s}\right)^{-1}$$

Avec la fonction $f = 1$, on dispose de l'identité suivante :

$$\forall s > 1, \zeta(s) = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

.

Preuve : Commençons par remarquer que la somme infini ainsi que le produit infini convergent car f est bornée.
Soit $T > 0$, Pour p un nombre premier fixé, comme $|\frac{f(p)}{p^s}| < 1$ car $s > 1$, d'après la formule de la somme géométrique, on a $\left(1 - \frac{f(p)}{p^s}\right)^{-1} = \sum_{m=0}^{+\infty} \left(\frac{f(p)}{p^s}\right)^m = \sum_{m=0}^{+\infty} \frac{f(p)^m}{p^{ms}}$ car f est complètement multiplicative.
D'où

$$\prod_{\substack{p \text{ premier} \\ p \leq M}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{\substack{p \text{ premier} \\ p \leq M}} \sum_{m=0}^{+\infty} \frac{f(p)^m}{p^{ms}}$$

En posant $p_1, \ldots, p_k$ les nombres premiers inférieurs à M, on a donc en développant le produit, comme les séries convergent absolument, le théorème de Fubini permet d'écrire :

$$\prod_{\substack{p \text{ premier} \\ p \leq M}} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{(m_1,\ldots,m_k) \in \mathbb{N}^k} \frac{f(p_1)^{m_1} \times \cdots \times f(p_k)^{m_k}}{(p_1^{m_1} \times \cdots \times p_k^{m_k})^s} = \sum_{n \in \mathcal{N}(T)} \frac{f(n)}{n^s}$$

Avec $\mathcal{N}(M)$ l'ensemble des entiers dont tous les diviseurs premiers sont inférieurs à M.
Ainsi,

$$\left|\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} - \prod_{\substack{p \text{ premier} \\ p \leq M}} \left(1 - \frac{1}{p^s}\right)^{-1}\right| = \left|\sum_{n \notin \mathcal{N}(T)} \frac{f(n)}{n^s}\right| \leq \sum_{n \notin \mathcal{N}(T)} \frac{|f(n)|}{n^s} \leq \sum_{n > T} \frac{|f(n)|}{n^s}$$

Il s'agit du reste d'une série convergente, donc tend vers 0 lorsque $T \to +\infty$. D'où le résultat.
□

Corollaire 139. *La série* $\sum_{p \text{ premier}} \frac{1}{p}$ *diverge.*

Preuve : Notons $(p_i)_{i \in \mathbb{N}}$ la suite croissante des nombres premiers. Comme pour tout $x \in [0, \frac{1}{2}]$, on a $\ln(1 - x) \geq -2x$ (par inégalité de convexité), on a

$$\sum_{i=0}^{+\infty} \frac{1}{p_i^s} \geq \frac{1}{2} \ln \zeta(s)$$

Or, comme $\zeta(s) \xrightarrow[s \to 1]{} +\infty$, on a $\ln \zeta(s) \xrightarrow[s \to 1]{} +\infty$ d'où par décroissance de $s \mapsto \sum_{i=0}^{+\infty} \frac{1}{p_i^s}$, on a la divergence de $\sum_{p \text{ premier}} \frac{1}{p}$. □

Ainsi, par critère de Riemann, pour tout $\alpha > 1$, la suite des inverses des nombres premiers n'est pas dominée devant $(\frac{1}{n^\alpha})$, ce qui peut s'interpréter que les nombres premiers sont plus rares que n'importe suite de nombre n^α.