Leçon 121 : Nombres premiers et applications

astrid.thollet

October 2025

1 Nombres premiers et arithmétiques dans $\mathbb{Z}$

1.1 Définitions et propriétés

Définition 1. *Soit $p \in \mathbb{Z}$, on dit que p est premier s'il admet exactement deux diviseurs positifs distincts (1 et $|p|$).*
On note $\mathcal{P}$ l'ensemble des nombres premiers positifs.

Exemple 2. *Les nombres premiers compris entre 1 et 20 sont* $2, 3, 5, 7, 11, 13, 17, 19$.

Définition 3. *Soient $a, b \in \mathbb{Z}$. On note $pgcd(a, b)$ le plus grand diviseur commun positif de a et de b, et $ppcm(a, b)$ le plus petit multiple commun positif de a et b.*

Définition 4. *Deux entiers a et b sont premiers entre eux si $pgcd(a, b) = 1$.*

Définition-Proposition 5. *Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. On appelle cette égalité une relation de Bézout.*

Exemple 6. *6 et 35 ne sont pas premiers, mais ils sont premiers entre eux et on a* $6 \times 6 + (-1) \times 35 = 1$.

Théorème 7 (Algorithme d'Euclide Etendu)**.** *Soient $a, b \in \mathbb{N}$, on pose $(r_0, r_1) = (a, b)$, $(u_0, u_1) = (1, 0)$ et $(v_0, v1) = (0, 1)$. Puis on définit la suite (r_i, q_i) par les divisions euclidiennes $r_{i-1} = q_i r_i + r_{i+1}$.*
On déininit ensuite les suites u et v par $u_{i+1} = u_{i+1} - u_i q_i$ et $v_{i+1} = v_{i+1} - v_i v_i$.

1. *La suite (r_i) est strictement décroissante tant qu'elle est non nullle, et on peut définir un rang n à partir duquel $r_{n+1} = 0$ et on arrête l'algorithme.*
2. *On a alors $r_n = pgcd(a, b)$ et $au_n + bv_n = r_n$.*

Remarque 8 (culturel)**.** *L'algorithme marche pour tout anneau euclidien, et permet de trouver une relation de Bézout en temps logarithmique.*

Proposition 9 (Lemme de Gauss)**.** *Soient $a, b \in \mathbb{Z}$ premiers entre eux et $c \in \mathbb{Z}$ tels que $a|bc$ alors $a|c$.*

Théorème 10 (Théorème fondamental de l'arithmétique)**.** *Soit $n \in \mathbb{N}^*$, il existe une unique décomposition en facteurs premiers, i.e. il existe de manière unique un $r \in \mathbb{N}^*$, un r-uplet $(p_1, \dots, p_r)$ d'éléments de $\mathcal{P}$, et $(a_1, \dots, a_r) \in (\mathbb{N}^*)^r$ tels que $n = \prod_{i=1}^{r} p_i^{a_i}$.*

Exemple 11. *On a la décomposition suivante :* $825 = 3 \times 5^2 \times 11$

1.2 Recherche des nombres premiers

Proposition 12. *Il existe une infinité de nombres premiers.*

Théorème 13. *Pour n on pose $\pi(n) = |\mathcal{P} \cap [\![1, n]\!]|$ et on a alors $\pi(n) \underset{n\to\infty}{\sim} \frac{n}{ln(n)}$*

Théorème 14 (Théorème de Fermat)**.** *Soit $p \in \mathcal{P}$ et a premier avec p, alors $a^{p-1} \equiv 1[p]$.*

Définition 15 (nombre de Carmichaël)**.** *On appelle nombre de Carmichaël tout entier $n \geq 3$ non premier qui vérifie la propriété suivante : pour tout a premier avec n on a $a^{n-1} \equiv 1[n]$.*

Exemple 16. $561 = 5 \times 11 \times 17$ *est un nombre de Carmichaël.*

Proposition 17. *Soit $n \in \mathbb{N}$, $n \notin \mathcal{P}$. Il existe un diviseur de n inférieur à $\sqrt{n}$.*

Remarque 18 (Crible d'ératosthène)**.** *Un premier algorithme pour trouver les nombres premiers compris entre 1 et a consiste à rayer les multiples de n sur cet intervalle, en partant de 2 et en ignorant ceux déjà rayés.*

La proposition précédente nous permet donc de vérifier si p est premier en testant s'il est divisble par tous les premiers entre 1 et $\sqrt{p}$, dont on peut obtenir une liste.

2 Anneaux et corps finis, $\mathbb{Z}/n\mathbb{Z}$

On garde un contexte où les anneaux sont commutatifs.

2.1 Indicatrice d'Euler

Définition 19 (Indicatrice d'Euler)**.** *Soit $n \in \mathbb{N}^*$,*
on pose $\varphi(n) = |\{k \in [\![1, n]\!], pgcd(k, n) = 1\}|$.

Proposition 20. *Soit $n \in \mathbb{N}^*$ de décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{a_i}$.*
On a alors $\varphi(n) = \prod_{i=1}^{r} (p_i - 1)p_i^{a_i - 1}$.

Exemple 21. $\varphi(561) = 2 \times 6 \times 10 = 120$

Proposition 22. *Soit $n \in \mathbb{N}*$, on a $n = \sum_{d|n} \varphi(d)$*

Proposition 23. *Soit $n \in \mathbb{N}^*$ alors on a :*

1. *$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$*
2. *$\varphi(n)$ est égal au nombre de générateurs de l'anneau $\mathbb{Z}/n\mathbb{Z}$*
3. *Au nombre de racines n-ième primitives sur $\mathbb{C}$.*

Proposition 24 (Euler)**.** *Soit $n \in \mathbb{N}^*$, pour tout entier a premier avec n on a $a^{\varphi(n)} \equiv 1 (mod\ n)$*

Théorème 25 (des Restes Chinois)**.** *Si les $n_1, \ldots, n_r$ sont des entiers premiers entre eux et $n = n_1 \times \cdots \times n_r$ alors on a un isomorphismes d'anneaux*

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$
$$k \mapsto (k\ mod\ n_1, \ldots, k\ mod\ n_r)$$

Proposition 26. *Pour $p \in \mathcal{P}$, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Théorème 27 (Condition de cyclicité)**.** *Soit $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 1, 2, 4, p^\alpha$ ou $2p^\alpha$ où $p \in \mathcal{P}, \alpha \in \mathbb{N}^*$*

2.2 Corps finis

Proposition 28. *Les assertions suivantes sont équivalentes :*

1. *p est un nombre premier*
2. *$\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre.*
3. *$\mathbb{Z}/p\mathbb{Z}$ est un corps, qu'on note alors $\mathbb{F}_p$.*

Définition-Proposition 29. *Pour A un anneau, on définit $f_A : \mathbb{N} \longrightarrow A$ telle que $f_A(n) = 1 + \cdots + 1$ (n fois).*
On note $car(A)$ et on appelle caractéristique de A, l'unique $n \in \mathbb{N}$ qui engendre $\ker(f_A)$.

Proposition 30. *1. Si A intègre alors $car(A) = 0$ ou $p \in \mathcal{P}$.*

2. Si A fini, $car(A) \neq 0$ et $car(A)$ divise $|A|$.
En particulier si $\mathbb{K}$ est un corps fini, il existe $p \in \mathcal{P}, n \in \mathbb{N}^*$ tel que $|\mathbb{K}| = p^n$

Proposition 31. *Réciproquement, pour $p \in \mathcal{P}, n \in \mathbb{N}^*$, il existe un unique corps de cardinal $q = p^n$ à isomorphisme près. On le note alors $\mathbb{F}_q$.*

2.3 Carrés

Soit $q = p^n$ avec $p \in \mathcal{P}$, $n \in \mathbb{N}^*$

Définition-Proposition 32. *On note $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^* \cap \mathbb{F}_q^2$. Alors $\mathbb{F}_q^{*2}$ est un sous groupe de $\mathbb{F}_q^*$.*

Définition 33 (Symbole de Legendre)**.** *Soit $p \in \mathcal{P}, n \in \mathbb{N}$ on définit*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p|n \\ 1 & \text{sinon, si } n \in \mathbb{F}_p^2 \\ -1 & \text{sinon} \end{cases}$$

Dans le second cas, n est un résidu quadratique.

Proposition 34. *$\mathbb{F}_p^{*2}$ est d'ordre $(p-1)/2$.*

Proposition 35 (Euler)**.** *On a la congruence*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} (mod\ p)$$

On a en particulier pour $n, m \in \mathbb{N}$

$$\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$$

Proposition 36 (Extraction de racines carrées)**.** *Soit $p \in \mathcal{P}$ congure à 3 modulo 4 et x un résidu quadratique dans F_p^*. Alors*

$$y = x^{\frac{p+1}{4}}$$

est une racine carrée de x.

Proposition 37. *Soit $n = pq$ avec $p, q \in \mathcal{P}$ distincts.*
Un résidu quadratique de $(\mathbb{Z}/n\mathbb{Z})^*$ possède 4 racines carrées.
$x \in (\mathbb{Z}/n\mathbb{Z})^*$ est un carré si et seulement si $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1$.

3 Cryptologie

3.1 Le cryptosystème RSA - DEV 2

On a comme corollaire du petit théorème de Fermat :

Proposition 38. *Soient $p, q \in \mathcal{P}$ distincts et $n = pq$.*
Pour tout $t \equiv 1(mod\ \varphi(n))$ et $x \in \mathbb{Z}/n\mathbb{Z}$ on a $x^t = x$.

On peut donc utiliser le protocole suivant :
L'utilisateur A procède ainsi:

- Il choisit $p, q \in \mathcal{P}$ puis calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
- Il choisit e inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$ et détermine son inverse d
- Il publique la clef publique (e, n) et conserve la clef privée d.

L'algorithme de chiffrement est $f_A : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définit par $f_A(x) = x^e$ (cryptogramme), bijectif grâce à la proposition précédente.
L'algorithme de déchiffrement est $f_A^{-1}(x) = x^d$.

Proposition 39. *Les algorithmes de chiffrement et déchiffrement sont en temps logarithmique.*
Connaissant n et $\varphi(n)$, on peut déterminer p et q en temps logarithmique.

Proposition 40. *Si le message x à envoyer n'est pas premier avec n, on peut factoriser n en temps logarithmique à l'aide du cryptogramme reçu.*

Remarque 41. *Cependant, la probabilité de tomber sur x n'étant pas premier à n est faible car on a $\frac{\varphi(n)}{n} = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{n} > 1 - \frac{2}{p}$ pour $p < q$.*

Enfin, la connaissance de $\varphi(n)$ n'est pas nécessaire, il suffit de posséder **une** clef de déchiffrement r qui vérifie $\forall x \in \mathbb{Z}/n\mathbb{Z}, x^{er} = x$.

Proposition 42. *On pose $m = ppcm(p-1, q-1)$. Les conditions suivantes sont équivalentes :*

1. $\forall x \in \mathbb{Z}/n\mathbb{Z}, x^u = x$
2. $u \equiv 1(mod\ m)$

On a alors $pgcd(p-1, q-1)$ clefs de déchiffrements dans $[\![1, \varphi(n)[\![$

3.2 Le cryptosystème de Rabin

L'utilisateur choisit $n = pq$, avec $p, q \in \mathcal{P}$ congrus à 3 modulo 4.
La clef publique est n et la clef secrète est (p, q).
Si le message est $u \in \mathbb{Z}/n\mathbb{Z}$, le cryptogramme est u^2.

La partie 2.3 montre qu'extraire une racine carré est de complexité logarithmique si on connaît la factorisation de n.

3.3 Protocole de Goldwasser-Micali

L'utilisateur choisir une clef privée (p, q) un couple de nombres premiers, et publie une clef publique (n, x) où $n = pq$ et x est un non-résidu quadratique dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$.
Si un message est une suite de bits $(a_1, \dots a_r)$ le cryptogramme est $(y_1, \dots, y_r)$ où pour tout i, on choisit $x_i \in (\mathbb{Z}/n\mathbb{Z})^*$ au hasard et $y_i = x_i^2 x^{a_i}$.

La partie 2.3 montre que déterminer si un entier est un résidu quadratique est de complexité logarithmique si on connaît la factorisation de n.

Remarque 43. *La connaissance de trois racines carrées permet uen factorisation de n en temps logarithmique.*