121 Nombres premiers. Applications.

Motivation : les nombres premiers sont les « briques » des nombres entiers.

I Arithmétique dans $\mathbb{Z}$

1) Nombres premiers

Définition 2. On dit que $p\in\mathbb{N}_{\geq 2}$ est *premier* si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

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

Contre-exemple 5. 1, $24=4\times 6$, $203=7\times 29$ ne sont pas premiers

Propriété 7. Si $a\in\mathbb{Z}$ est tel que $p\nmid a$ alors $\mathrm{pgcd}(p,a)=1$.

2) Résultats fondamentaux

Lemme 11 (Euclide). Soient $p\in\mathcal{P}$ et $a,b\in\mathbb{Z}$ tels que $p|ab$. Alors $p|a$ ou $p|b$.

Application 13. Si $p\in\mathcal{P}$ et $k\in\{1..p-1\}$ alors $p\mid\binom{p}{k}$.

Proposition 17. Tout entier ≥ 2 est divisible par un nombre premier.

→ **Corollaire 19.** Il existe une infinité de nombres premiers.

→ **Corollaire 23 (Théorème fondamental de l'arithmétique).** Tout entier $n\geq 2$ se décompose de manière unique, à l'ordre des facteurs près, sous la forme $\boxed{n=\prod_{i=1}^{r} p_i^{\alpha_i}}$ où $r\in\mathbb{N}^*$, $p_i\in\mathcal{P}$ deux à deux distincts et $\alpha_i\in\mathbb{N}^*$.

Exemple 29. $24=2^3\cdot 3$, $90=2\cdot 3^2\cdot 5$.

Remarque 31. Ce qui précède mène à la définition d'*anneau factoriel*.

→ **Application 37.** Si $n\in\mathbb{N}$ n'est pas un carré parfait alors $\sqrt{n}$ est irrationnel.

→ **Application 41.** Soient $a,b\in\mathbb{N}_{\geq 2}$ que l'on écrit $a=\prod_{i=1}^{r} p_i^{\alpha_i}$ et $b=\prod_{i=1}^{r} p_i^{\beta_i}$ avec $r\in\mathbb{N}^*$, $p_i\in\mathcal{P}$ deux à deux distincts et $\alpha_i,\beta_i\in\mathbb{N}$, $\alpha_i+\beta_i\geq 1$.

Alors $[a|b$ ssi $\forall i, \alpha_i\leq\beta_i]$ et $\mathrm{pgcd}(a,b)=\prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$, $\mathrm{ppcm}(a,b)=\prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$

→ **Corollaire 43 (produit eulérien).** Pour $s\in\mathbb{R}_{>1}$, on pose $\zeta(s):=\sum_{n=1}^{+\infty}\frac{1}{n^s}$.

Alors $\zeta(s)=\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p^s}\right)^{-1}$

3) Deux fonctions arithmétiques

Définition 47. On définit l'*indicatrice d'Euler* $\varphi:\mathbb{N}^*\to\mathbb{N}^*$ par :

$$\varphi(n):=\#\{i\in\{1..n\} \,/\, \mathrm{pgcd}(i,n)=1\}.$$

Proposition 53. Si $p\in\mathcal{P}$ et $\alpha\in\mathbb{N}^*$ alors $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$.

Proposition 59. Si $m,n\in\mathbb{N}^*$ sont premiers entre eux alors $\varphi(mn)=\varphi(m)\varphi(n)$.

Corollaire 61. Si $n\in\mathbb{N}_{\geq 2}$ alors $\varphi(n)=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$ où les p_i sont les facteurs premiers distincts de n.

Définition 67. On définit la *fonction de Möbius* $\mu:\mathbb{N}^*\to\{-1,0,1\}$ par $\mu(1)=1$ et

si $n=p_1\cdots p_r\in\mathbb{N}_{\geq 2}$, $r\in\mathbb{N}^*$, $p_i\in\mathcal{P}$, $\mu(n):=\begin{cases}0 & \text{si } \exists i\neq j,\ p_i=p_j\\ (-1)^r & \text{sinon.}\end{cases}$

Proposition 71 (formule d'inversion de Möbius). Soit G un groupe abélien et soient $f,g:\mathbb{N}^*\to G$ telles que $\forall n\in\mathbb{N}^*$, $f(n)=\sum_{\substack{d|n\\(d>0)}} g(d)$.

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

Application 73. Si $\Phi_n\in\mathbb{C}[X]$ est le n^e polynôme cyclotomique alors $\Phi_n=\prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})}$.

4) Répartition des nombres premiers

Propriété 79. Pour tout $n\in\mathbb{N}^*$, il existe n entiers naturels consécutifs non premiers.

Propriété 83. Il n'existe pas de polynôme $P\in\mathbb{Z}[X]$ non constant tel que $P(n)$ soit premier pour n assez grand.

Théorème 89 (Dirichlet) [ADMIS]. Si $a,b\in\mathbb{N}^*$ sont premiers entre eux, il existe une infinité de nombres premiers de la forme $ka+b$, $k\in\mathbb{N}$. **DEV 1** $(b=1)$

Définition 97. Pour $n\in\mathbb{N}^*$, on pose $\pi(n):=\#(\mathcal{P}\cap\{1..n\})$.

Théorème 101 (Théorème des nombres premiers) [ADMIS]. $\pi(n)\sim\frac{n}{\log n}$.

Corollaire 103. Si $(p_n)_{n\geq 1}$ désigne la suite croissante des nombres premiers alors $\pi(p_n)=n$, $\boxed{p_n\sim n\log n}$ et $\frac{p_{n+1}}{p_n}\sim 1$.

II Corps finis (commutatifs)

1) Anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 107. Soit $n \in \mathbb{N}_{\geq 2}$. Alors $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $n \in \mathcal{P}$.

Remarque 109. Si c'est le cas, alors $n = p \in \mathcal{P}$ et on note $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$. L'inverse d'un élément $\bar{x} \in \mathbb{F}_p^*$ se calcule grâce à l'algorithme d'Euclide étendu appliqué à (p, x).

Exemple 113. $5 \in \mathcal{P}$ donc $\mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$ est un corps. On a $-5 + 2 \times 3 = 1$ donc $\bar{2} \cdot \bar{3} = \bar{1}$.

Corollaire 127 (petit théorème de Fermat). Si $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ alors $a^p \equiv a \, [p]$.
De plus, si $p \nmid a$ alors $\boxed{a^{p-1} \equiv 1 \, [p]}$

Corollaire 131 (Théorème de Wilson). $p \in \mathbb{N}_{\geq 2}$ est premier ssi $(p-1)! \equiv -1 \, [p]$.

Proposition 137. Si $n \in \mathbb{N}_{\geq 2}$ alors $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$.

Corollaire 139 (Euler). Si $n \in \mathbb{N}_{\geq 2}$ et $a \in \mathbb{Z}$ premier avec n alors $a^{\varphi(n)} \equiv 1 \, [n]$.

Application 149 (cryptosystème RSA). Arielle et Bertrand désirent s'envoyer un message crypté. Arielle choisit secrètement $p, q \in \mathcal{P}$ très grands ($p \neq q$) et calcule $n := pq$. Elle choisit un entier e premier avec $\varphi(n)$ et rend publics n et e. Finalement, elle calcule secrètement $d := e^{-1} \, [\varphi(n)]$. Si Bertrand veut envoyer un message $m \in \mathbb{Z}$ (premier avec n) à Arielle, Bertrand envoie le message crypté $m^e \, [n]$; il est alors très difficile de retrouver m, sauf pour Arielle car $(m^e)^d \equiv m \, [n]$.

2) Théorie élémentaire des corps finis

Proposition / Définition 151. Soit k un corps fini. Il existe un unique $p \in \mathbb{N}^*$ tel que $\mathbb{Z}/p\mathbb{Z}$ s'injecte dans k; l'entier p est la caractéristique de k et on a $p \in \mathcal{P}$. De plus, k est muni d'une structure de $\mathbb{F}_p$-espace vectoriel d'où $\boxed{\# k = p^d}$ pour un $d \in \mathbb{N}^*$.

Dans la suite, on fixe $p \in \mathcal{P}$ et $d \in \mathbb{N}^*$, et on note $q := p^d$.

Théorème 157. Il existe un corps fini à q éléments, unique à isomorphisme de corps près : on le note $\mathbb{F}_q$.

Définition 163. L'endomorphisme de Frobenius sur $\mathbb{F}_q$ est $\Phi_q : \begin{vmatrix} \mathbb{F}_q \longrightarrow \mathbb{F}_q \\ x \longmapsto x^p \end{vmatrix}$.

Théorème 167. Φ_q est un automorphisme de corps (donc en particulier un endomorphisme).

Théorème 173. $\mathbb{F}_q^*$ est cyclique, et donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Application 179 (Théorème de Chevalley-Warning). Soit $n \in \mathbb{N}^*$ et soit $(f_\alpha)_{\alpha \in A}$ une famille d'éléments de $\mathbb{F}_q[X_1, \dots, X_n]$ telle que $\sum_{\alpha \in A} \mathrm{tdeg}(f_\alpha) < n$. Avec $V := \{x \in \mathbb{F}_q^n \mid \forall \alpha \in A, f_\alpha(x) = 0\}$ on a $\# V \equiv 0 \, [p]$.

Application 181 (Théorème d'Erdős–Ginzburg–Ziv). Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_{2n-1} \in \mathbb{Z}$. Il existe $I \subseteq \{1, \dots, 2n-1\}$ de cardinal n telle que $\sum_{i \in I} a_i \equiv 0 \, [n]$. (**DEV2**)

3) Carrés dans $\mathbb{F}_q$ $\quad (q = p^d, p \in \mathcal{P}, d \geq 1)$

Proposition 191. Tout entier naturel est un carré modulo une infinité de nombres premiers.

Remarque 193. Φ_2 étant bijectif, tous les éléments de $\mathbb{F}_{2^d}$ sont des carrés ; on suppose donc $p \geq 3$.

Proposition 197. Il y a exactement $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$. Plus précisément, $\forall x \in \mathbb{F}_q^*$, $x^{\frac{q-1}{2}} \in \{-1, 1\}$ et $\left[x^{\frac{q-1}{2}} = 1 \text{ ssi } x \text{ est un carré dans } \mathbb{F}_q^* \right]$.

→ **Corollaire 199.** -1 est un carré dans $\mathbb{F}_q$ ssi $q \equiv 1 \, [4]$.

Application 211 (Théorème des deux carrés). $\exists (x,y) \in \mathbb{Z}^2, p = x^2 + y^2$ ssi $p \equiv 1 \, [4]$ (**DEV3**)

→ **Corollaire / Définition 223.** Pour $x \in \mathbb{F}_p^*$ on a $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ où $\left(\frac{x}{p}\right) := \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$ est le symbole de Legendre de x.

Corollaire 227. $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$ est un morphisme.

Illustration 229 (Théorème de Frobenius–Zolotarev). $\forall u \in \mathrm{GL}(\mathbb{F}^n)$, $\varepsilon(u) = \left(\frac{\det u}{p}\right)$.

Théorème 233 (réciprocité quadratique). Si $p' \in \mathcal{P}_{\geq 3}$ alors $\boxed{\left(\frac{p'}{p}\right)\left(\frac{p}{p'}\right) = (-1)^{\frac{p'-1}{2} \frac{p-1}{2}}}$

Application 239. $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^1 = -1$ donc 3 n'est pas un carré modulo 17.

III Théorie des groupes

1) p-groupes $\quad (p \in \mathcal{P})$

Définition 241. Un p-groupe est un groupe (fini) de cardinal une puissance de p.

Exemple 251. $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/8\mathbb{Z}$, Q_8 sont des 2-groupes.

Proposition 257. Tout groupe d'ordre p est cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 263. Le centre d'un p-groupe non trivial est non trivial.

↳ Corollaire 269. Tout groupe d'ordre p^2 sont abéliens.

Application 271. Les groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$ (à isomorphisme près).

↳ Corollaire 277. Tout p-groupe est résoluble.

2) Théorèmes de Sylow

But: établir une réciproque au théorème de Lagrange.

Soit G un groupe de cardinal $n\in\mathbb{N}_{\geq 2}$ et $p\in\mathcal{P}$ avec $n=p^\alpha m$, $\alpha\in\mathbb{N}^*$ et $p\nmid m$.

Théorème 281 (Cauchy). G possède un élément d'ordre p.

Définition 283. On appelle p-Sylow de G un sous-groupe de G d'ordre p^α.

Exemple 293. Pour $N\in\mathbb{N}_{\geq 2}$, $\left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}\right\}\subseteq GL_N(p)$ est un p-Sylow.

Théorème 307 (Sylow). G admet au moins un p-Sylow.

Théorème 311 (Sylow).

(i) Tout p-sous-groupe de G est inclus dans un p-Sylow.

(ii) Les p-Sylow de G sont conjugués deux à deux.

(iii) Si n_p désigne le nombre de p-Sylow de G alors $\boxed{n_p\equiv 1 [p]}$ et $\boxed{n_p \mid m}$.

Corollaire 313. Si S est un p-Sylow de G, alors $S\lhd G$ ssi $n_p=1$.

↳ Application 317. Les groupes d'ordre 24, 63, 255 ne sont pas simples.

↳ Application 331. Si $q\in\mathcal{P}$ est tel que $\begin{cases} q>p \\ p\nmid q-1\end{cases}$ alors tout groupe d'ordre pq est cyclique.

IV Primalité en pratique

1) Premiers algorithmes (élémentaires)

Algorithme 337. Pour prouver que $n\in\mathbb{N}_{\geq 2}$ est premier, on peut utiliser la définition en testant $i\mid n$ pour les $i=2..n-1$. On peut faire une première amélioration en s'arrêtant dès que $i^2>n$, et une deuxième en ne testant que pour les i impairs (si $n>2$).

Algorithme 347 (crible d'Ératosthène). On désire trouver tous les nombres premiers inférieurs à une borne $N\in\mathbb{N}_{\geq 2}$ donnée. On pose $P_1:=\{2..N\}$, $P_2:=\emptyset$ et on fait:

tant que $P_1\neq\emptyset$ faire

$P_2\leftarrow P_2\cup\{\min P_1\}$;

$P_1\leftarrow P_1\setminus(\min P_1)\mathbb{N}^*$;

L'ensemble P_2 est à la fin de la procédure égal à $\mathcal{P}\cap\{2..N\}$.

Remarque 349. Ce dernier algorithme est utile si l'on doit tester plusieurs fois que des nombres de $\{2..N\}$ sont premiers.

2) Test de non primalité de Fermat

Idée: on veut utiliser le petit théorème de Fermat (corollaire 127).

Théorème 353 (Alford, Granville, Pomerance, 1992) [ADMIS]. Il existe une infinité d'entiers non premiers $n\geq 2$ tels que $\forall a\in\mathbb{Z}$, $a^n\equiv a [n]$.

Définition 359. De tels entiers n sont appelés nombres de Carmichael.

Remarque 367. Les premiers nombres de Carmichael sont 561, 1105, 1729...

Théorème 373 (Korselt). $n\in\mathbb{N}_{\geq 2}$ est un nombre de Carmichael ssi $n=p_1\cdots p_r$ avec $r\in\mathbb{N}_{\geq 2}$, $p_i\in\mathcal{P}$ deux à deux distincts et $p_i-1\mid n-1$ $\forall i$.

3) Test probabiliste de primalité de Solovay-Strassen

Idée: on veut utiliser le corollaire 223.

Définition 379. Soit $n\in\mathbb{N}_{\geq 2}$ impair, que l'on écrit $n=\prod_{i=1}^{r} p_i$ avec $r\in\mathbb{N}^*$ et $p_i\in\mathcal{P}$.

Pour $a\in\mathbb{Z}$ premier avec n, on définit le symbole de Jacobi $\left(\frac{a}{n}\right):=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)$.

Remarque 383. Si $p\in\mathcal{P}_{\geq 3}$, les symboles de Legendre $\left(\frac{\cdot}{p}\right)$ et de Jacobi $\left(\frac{\cdot}{p}\right)$ coïncident.

Théorème 389 (Solovay-Strassen). Soit $n\in\mathbb{N}_{\geq 2}$ impair. Alors on a

$$n\in\mathcal{P} \text{ ssi } \forall a\in(\mathbb{Z}/n\mathbb{Z})^\times,\ \left(\frac{a}{n}\right)=a^{\frac{n-1}{2}}.$$

Corollaire 397. Soit $n\in\mathbb{N}_{\geq 2}$ non premier. Alors $\#\left\{a\in(\mathbb{Z}/n\mathbb{Z})^\times \,/\, \left(\frac{a}{n}\right)=a^{\frac{n-1}{2}}\right\}\leq\frac{\varphi(n)}{2}$.

Application 401. On dispose d'une procédure qui, répétée N fois, détermine si $n\in\mathbb{N}_{\geq 2}$ impair est premier avec une probabilité d'erreur nulle si le test renvoie «n non premier» et $\leq 2^{-N}$ si le test renvoie «n est premier».

Références :

- Gourdon
- Perrin
- Demazure