121 — Nombres premiers — Applications

I - Propriétés arithmétiques et de répartition

1 - Arithmétique dans $\mathbb{Z}$

Déf 1 : Un nombre de $\mathbb{Z}\setminus\{\pm 1\}$ est dit premier ssi il admet exactement deux diviseurs positifs : 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Ex 2 : 1 n'est pas premier, 2 est premier, 4 n'est pas premier.

Lemme (Lemme de Gauss) Soient $k, m, n \in \mathbb{Z}$ avec $k \mid mn$ et $k \wedge m = 1$ alors $k \mid n$.

Lemme 3 : (Lemme d'Euclide) Soit $p \in \mathcal{P}$ et $m, n \in \mathbb{Z}$ tels que $p \mid mn$. Alors $p \mid m$ ou $p \mid n$.

Ex 4 : $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$

Th 5 : L'anneau $\mathbb{Z}$ est euclidien donc factoriel. $\forall m \in \mathbb{Z}$, $\exists (p_1, \dots, p_r) \in \mathcal{P}^r$, $\exists (\alpha_1, \dots, \alpha_r) \in \mathbb{N}^{*r}$ tq $m = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i}$, $\varepsilon \in \{-1, 1\}$.
Cette décomposition est unique à l'ordre près des facteurs.
On a $\alpha_i = v_{p_i}(m)$ = valuation p_i-adique de m.

Ex 6 : $350 = 2 \times 5^2 \times 7$, $v_5(350) = 2$

Prop 7 : Soient $m, n \in \mathbb{Z}\setminus\{0, 1, -1\}$. $n \mid m$ si, et seulement si, pour tout $p \in \mathcal{P}$ divisant n, $v_p(n) \leq v_p(m)$.

Prop 8 (PGCD, PPCM)
Si $n = \prod_{i=1}^{r} p_i^{v_{p_i}(n)}$ et $m = \prod_{i=1}^{r} p_i^{v_{p_i}(m)}$, où $v_{p_i}(n,m) \neq 0$ [illegible]

alors $n \wedge m = \prod_{i=1}^{r} p_i^{\min\{v_{p_i}(n), v_{p_i}(m)\}}$
$n \vee m = \prod_{i=1}^{r} p_i^{\max\{v_{p_i}(n), v_{p_i}(m)\}}$

Ex 9 : $280 = 2^3 \times 5 \times 7$, donc $280 \wedge 350 = 2 \times 5 \times 7 = 70$

2 - Répartition des nombres premiers

Prop 9 (Crible d'Ératosthène) On peut trouver les nombres premiers compris entre 1 et n en éliminant tous les multiples de tout $p \in \mathcal{P} \cap [\![2, \sqrt{n}]\!]$ [illegible]

[illegible]

Prop : $\mathcal{P}$ est infini

Prop 12 (Fonction ζ de Riemann) Soit $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$. On pose $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$

Prop 13 : (Produit eulérien) Soit $s \in \{\mathrm{Re}(s) > 1\}$. On a alors
$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}}$$

Application : La série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge.

Th 15 (Théorème des nombres premiers, admis)
Soit $x > 0$. Soit $\pi(x) = \mathrm{Card}(\mathcal{P} \cap [\![1, x]\!])$. Alors $\pi(x) \sim \frac{x}{\ln x}$

II - Application aux corps finis

Prop 16 : Soit $\mathbb{K}$ un corps fini. Il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{K}$, donné par $\varphi(k) = k 1_{\mathbb{K}}$. De plus, il existe $p_0 \in \mathcal{P}$ tel que $p_0\mathbb{Z} = \mathrm{Ker}(\varphi)$.

Def 17 : Ce $p_0 \in \mathcal{P}$ est appelé caractéristique de $\mathbb{K}$, on la note $\mathrm{Car}(\mathbb{K})$.

Th 18 : Soit $\mathbb{K}$ un corps fini, il existe $n \in \mathbb{N}^*$ tel que $\mathrm{Card}(\mathbb{K}) = \mathrm{Car}(\mathbb{K})^n$

1 - Le corps $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$

Th 19 (Théorème de Bézout) Soient $(m, n) \in \mathbb{Z}^2$, $m \wedge n = 1$ ssi il existe [illegible] $\exists (a, b) \in \mathbb{Z}^2 : am + bn = 1$ (a et b sont appelés coefficients de Bézout)

Prop 20 : $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, on peut trouver un inverse explicite grâce à l'algorithme d'Euclide.

Th 21 (Petit théorème de Fermat) Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$.
Alors $\bar{a}^p = \bar{a}$ dans $\mathbb{F}_p$ i.e. $a^p \equiv a \; [p]$

Prop 22 : (Théorème de Wilson) $p \in \mathcal{P} \iff (p-1)! \equiv -1 \; [p]$

Prop 23 $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est un groupe cyclique

2 - Polynômes irréductibles

Prop 24 Soit P un polynôme irréductible de degré n, $P \in \mathbb{F}_p[X]$. Alors $\frac{\mathbb{F}_p[X]}{(P)}$ est un corps fini à p^n éléments.

Ex 25 $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(X^2 + X + 1)}$

Prop 26 Soit $P \in \mathbb{Z}[X]$ non constant, $p \in \mathcal{P}$ tel que p ne divise pas le coefficient dominant de P. Alors si P est irréductible dans $\mathbb{F}_p[X]$, il l'est dans $\mathbb{Q}[X]$

Rq 27 La réciproque est fausse.

Contre-ex 28 : $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{F}_p[X]$.

Théo : (Critère d'Eisenstein) Soit $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{Z}[X]$ tel que

(i) $p \nmid a_N$ (ii) $\forall i \in [\![0, N-1]\!]$, $p \mid a_i$ (iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$

Ex : $3X^2 + 2X + 6$ est irréductible dans $\mathbb{Q}[X]$

Prop : Un seul $p \in \mathbb{P}$ est intéressant

Ex : Si $P = X^2 - 2$, le critère marche seulement pour $p = 2$ mais pour aucun autre $p \in \mathbb{P} \setminus \{2\}$, mais P est irréductible dans $\mathbb{Q}[X]$

3 - Carrés dans $\mathbb{F}_p$

Prop : Pour $p \in \mathbb{P} \setminus \{2\}$, l'application $\varphi : \mathbb{F}_p^* \to \{-1, 1\}$, $x \mapsto x^{\frac{p-1}{2}}$ est un morphisme de groupes

Prop : Pour $p \in \mathbb{P} \setminus \{2\}$, l'ensemble $\mathbb{F}_p^2$ des carrés de $\mathbb{F}_p$ est de cardinal $\frac{p+1}{2}$

Déf : (Symbole de Legendre) Soit $p \in \mathbb{P}$ et $a \in \mathbb{Z}$. On définit le symbole de Legendre par :

$$\left(\frac{a}{p}\right) = \bar{a}^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \neq 0 \text{ et si } a \text{ est un carré modulo } p \\ -1 & \text{si } a \text{ n'est pas un carré modulo } p \\ 0 & \text{si } a = 0 \end{cases}$$

ou $\bar{a}$ = classe de a modulo p

Th : Soit $a \in \mathbb{Z}$, soient $p, q \in \mathbb{P} \setminus \{2\}$ tels que $p \wedge q = 1$:

(i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(iii) [Loi de réciprocité quadratique] $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{1}{4}(p-1)(q-1)}$] DVPT 4

(iv) Si $m, n \in \mathbb{Z}$, alors $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

(v) Si $m, n \in \mathbb{Z}$ tels que $m \equiv n \ [p]$, alors $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$

Ex : $\left(\frac{43}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \underbrace{(-1)^{\frac{7^2-1}{8}}}_{=-1}\left(\frac{7}{3}\right)(-1)^{\frac{1}{4}(7-1)(3-1)}$

$= \left(\frac{1}{3}\right) = 1$ donc 43 est un carré modulo 7

Appli : Etude d'équations quadratiques dans $\mathbb{F}_p$ (existence de solutions)

Th : (Théorème des deux carrés)

Soit $\Sigma = \{n \in \mathbb{N} : \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$

Soit $p \in \mathbb{P}$ alors $p \in \Sigma \iff p = 2$ ou $p \equiv 1 \ [4]$] DVPT 2

III - Autres applications

1 - Théorie des groupes

Déf : Un p-groupe est un groupe fini d'ordre p^α où $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$

Th : Le centre d'un p-groupe est non trivial

Prop : Tout groupe d'ordre p^2, $p \in \mathbb{P}$, est abélien

Th : (Théorème de Cauchy) Soit G un groupe fini d'ordre $p \in \mathbb{P}$ tel que $p \mid |G|$. Alors G admet un élément d'ordre p

Prop : Soit G un groupe abélien d'ordre $p_1^{\alpha_1} \times \dots \times p_n^{\alpha_n}$, $n \in \mathbb{N}^*$, $p_1, \dots, p_n \in \mathbb{P}$ distincts, $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$. Alors G est cyclique

Théo : Si G est un groupe d'ordre $2p$, où $p \in \mathbb{P}$, alors $G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$ ou $G \simeq \mathbb{D}_p$ (Groupe diédral de p-gone régulier)

Rappel : Cardinal des groupes d'ordre inférieur à 11

2 - Conséquences du théorème de Fermat

Th : Soit $n \in \mathbb{N}$, $n \geq 2$: $\exists a \in \mathbb{Z}, a^n \not\equiv a \ [n]$ alors n n'est pas premier. C'est un témoin de Fermat

Ex : $2^{12} = 8^4 \equiv (-4)^4 = 16^2 \equiv 4^2 = 16 \equiv 4 \not\equiv 2 \ [12]$

12 n'est pas premier

Déf : Un nombre de Carmichael est un entier $n \geq 2$ tel que $\forall a \in \mathbb{Z}, a^n \equiv a \ [n]$, non premier

Ex : 561 est un nombre de Carmichael

Th : Soit $n \in \mathbb{N}$, $n-1 \leq 2^k b$ avec b impair. Si $\exists a \in \mathbb{N}$, $a^b \not\equiv 1 \ [n]$ et $\forall i \in [\![0, k-1]\!]$, $a^{2^i b} \not\equiv -1 \ [n]$, alors n n'est pas premier. Un tel a premier avec n est appelé témoin de Miller pour n

Ex : 2 est un témoin de Miller pour 561, donc 561 n'est pas premier

Prop : Si n n'est pas premier, au moins $\frac{3}{4}$ parmi des entiers de 2 à $n-1$ sont des témoins de Miller

Appli : (Test de Miller-Rabin)

Pour déterminer si n est premier, on choisit aléatoirement un entier a entre 2 et $n-1$. Si a est témoin de Miller, soit on recommence, après k tentatives de ce type, le nombre n est premier avec probabilité $1 - \left(\frac{1}{4}\right)^k$

3- Famille de nombres premiers

Déf: Un nombre de Fermat est un entier de la forme $F_n = 2^{2^n} + 1$

Ex: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$

Th: (Théorème de Gauss-Wantzel)

Un polygône régulier à n côtés est constructible à la règle et au compas si $n = 2^k F_1 \ldots$ où F_i est un nombre de Fermat premier.

Figure

	1	2	3	4	5	6	7	8	9
[illegible]	11	[illegible]	13	[illegible]	[illegible]	[illegible]	17	[illegible]	19
[illegible]	[illegible]	[illegible]	23	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	29
[illegible]	31	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	37	[illegible]	[illegible]
[illegible]	41	[illegible]	43	[illegible]	[illegible]	[illegible]	47	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	53	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	59
[illegible]	61	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	67	[illegible]	[illegible]
[illegible]	71	[illegible]	73	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	79
[illegible]	[illegible]	[illegible]	83	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	89
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	97	[illegible]	[illegible]

Références:

1. P. Samuel, Cours d'Arithmétique [illegible]

2. [illegible], Cours d'algèbre