Nombres premiers. Applications.

121

I) Généralités sur les nombres premiers [1]

A] Définitions et propriétés

Def 1 : Un entier naturel p est dit premier s'il admet exactement deux diviseurs : 1 et p.

Ex 2 : 2, 3, 5 sont premiers, 1, 4, 9 ne le sont pas.

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Thm 3 : $\forall n \in \mathbb{Z}, n \notin \{1; 0; -1\} \Rightarrow \exists p \in \mathcal{P}, p \mid n$.

Def 4 : $n \in \mathbb{N}$ est dit composé si $\exists p \in \mathcal{P}, p \mid n$ et $p \neq n$

Def 5 : Deux entiers sont dits premiers entre eux si leur seul diviseur commun positif est 1.

Thm 6 : (de Gauss) Soient $a, b, c \in \mathbb{Z}$. On suppose que $a \mid bc$ et a et b sont premiers entre eux. Alors $a \mid c$.

Lem 7 : $\forall a, b \in \mathbb{Z}, \forall p \in \mathcal{P}, p \mid ab \Leftrightarrow p \mid a$ ou $p \mid b$.

Thm 8 : (d'Euclide) $\mathcal{P}$ est un ensemble infini.

Thm 9 : Soit $n \in \mathbb{N}^*$. Alors $\exists k \in \mathbb{N}^*, \exists p_1, \dots, p_k \in \mathcal{P}$, $\exists \alpha_1, \dots, \alpha_k \in \mathbb{N}^*, n = \prod_{i=1}^{k} p_i^{\alpha_i}$. De plus, cette décomposition est unique.

B] Tests de primalité et caractérisations

Prop 10 : Soit $n \in \mathbb{N}$ un nombre composé. Alors : $\exists p \in \mathcal{P}, p \leq \sqrt{n}$

Rem 11 : $n \in \mathbb{N}$ est donc premier si et seulement si il n'admet aucun diviseur premier inférieur à $\sqrt{n}$.

Algo 12 : Soit $n \in \mathbb{N}$. On souhaite trouver tous les nombres premiers inférieurs à n. Soit $\mathcal{P}_n = [\![2; n]\!]$. Tant que $\mathcal{P}_n \neq \mathcal{P}$, on vérifie si $\min \mathcal{P}_n$ est premier ou non. Si oui, on réitère à $\min(\mathcal{P}_n) + 1$. Sinon, on retire de $\mathcal{P}_n$ tous les multiples de $\min(\mathcal{P}_n)$. C'est le crible d'Ératosthène.

Thm 13 : (de Wilson). Soit $n \in \mathbb{N}$, $n \in \mathcal{P} \Leftrightarrow (n-1)! \equiv -1 [n]$

Thm 14 : (de Fermat). Si $p \in \mathcal{P}$, alors pour tout $a \in \mathbb{N}^*$ premier avec p, $a^{p-1} \equiv 1 [p]$.

Rem 15 : Ceci donne une condition nécessaire pour la primalité. Cependant, la réciproque est fausse.

Def 16 : On appelle nombre de Carmichaël tout entier $n \geq 3$ tel que pour tout $a \in \mathbb{N}$ premier avec n, $a^{n-1} \equiv 1 [n]$ et qui soit non premier.

Ex 17 : $561 = 3 \times 11 \times 17$ est un nombre de Carmichaël.

C] Répartition des nombres premiers

Def 18 : Soit $n \in \mathbb{N}^*$. On définit $\pi(n)$ par : $\pi(n) = \{p \in \mathcal{P} \mid 0 < p \leq n\}$.

Thm 19 : (admis) $\pi(n) \sim \frac{n}{\ln(n)}$

Cor 20 : (version faible de Legendre) $\lim_{n \to +\infty} \frac{\pi(n)}{n} = 0$

Rem 21 : La connaissance des zéros de la fonction ζ de Riemann a permis des informations sur π.

Thm 22 : (de progression arithmétique faible de Dirichlet) Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers p tels que $p \equiv 1 [n]$

DEV 1

Rem 23: On peut affiner ce résultat : pour tout $a, b \in \mathbb{N}^*$ premiers entre eux, il existe une infinité de nombres premiers p tels que $p \equiv a[b]$.

II) Conséquences en arithmétique

A] Dans les relations de divisibilité [1]

Def 24 : Soit $n \in \mathbb{N}^*$ et soit $p \in \mathcal{P}$. On appelle valuation p-adique de n : $v_p(n) = \max\{k \in \mathbb{N} \mid p^k \mid n\}$.

Ex 25 : $v_3(18) = 2$, $v_2(18) = 1$, $\forall p \in \mathcal{P} \setminus \{2;3\}$, $v_p(18) = 0$

Prop 26 : Soient $n, m \in \mathbb{N}^*$. Soit $p \in \mathcal{P}$. Alors
$v_p(nm) = v_p(n+m)$ et $v_p(n+m) \geq \min(v_p(n), v_p(m))$.

Prop 27 : Soient $n, m \in \mathbb{N}^*$. $n \mid m \Leftrightarrow \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$

Def 28 : Soient $n, m \in \mathbb{N}^*$. On appelle PGCD de n et m
$\mathrm{PGCD}(n,m) = \max\{k \in \mathbb{N}^* \mid k \mid n$ et $k \mid m\}$ et PPCM de n et m $\mathrm{PPCM}(n,m) = \min\{k \in \mathbb{N}^* \mid n \mid k$ et $m \mid k\}$.

Cor 29 : Soient n et m dans $\mathbb{N}^*$. Alors : $\forall p \in \mathcal{P}$,
$v_p(\mathrm{PGCD}(n,m)) = \min(v_p(n), v_p(m))$, $v_p(\mathrm{PPCM}(n,m)) = \max(v_p(n), v_p(m))$

B] Dans l'étude des fonctions arithmétiques [1]

Def 29 : On appelle fonction arithmétique toute fonction $f : \mathbb{N}^* \to \mathbb{C}$ telle que : $\forall n, m \in \mathbb{N}^*$, $\mathrm{PGCD}(n,m) = 1 \Rightarrow f(nm) = f(n) f(m)$.

Ex 30 : L'indicatrice d'Euler φ définie par $\varphi(n) = \#\{k \in [\![1;n]\!] \mid \mathrm{PGCD}(k,n) = 1\}$ est arithmétique.

Rem 31 : Par la décomposition en facteurs premiers, la connaissance des valeurs d'une fonction arithmétique sur les puissances des nombres premiers détermine la fonction.

Ex 32 : $\forall \alpha \in \mathbb{N}^*$, $\forall p \in \mathcal{P}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Def 33 : On définit la fonction de Möbius μ par :
$\forall n \in \mathbb{N}^*$, $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n \text{ est produit de } r \text{ premiers distincts} \\ 0 \text{ sinon} \end{cases}$

Prop 34 : μ est une fonction arithmétique.

Prop 35 : Soit $n \in \mathbb{N}^*$. On note D_n l'ensemble des diviseurs positifs de n. Alors $\forall n \in \mathbb{N}^*$, $\sum_{d \in D_n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$

Thm 36 : (Formule d'inversion de Möbius) Soit $f : \mathbb{N}^* \to \mathbb{C}$ une fonction arithmétique. Soit $g : \mathbb{N}^* \to \mathbb{C}$ définie par : $\forall n \in \mathbb{N}^*$, $g(n) = \sum_{d \in D_n} f(d)$. Alors $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d \in D_n} \mu(d) g\left(\frac{n}{d}\right)$

App 37 : $\forall n \in \mathbb{N}^*$, $\varphi(n) = \sum_{d \in D_n} \mu\left(\frac{n}{d}\right) d$

III) Etude des corps finis [2]

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

A] Description des corps finis

Def 38 : Soit $\mathbb{K}$ un corps. On appelle sous-corps premier de $\mathbb{K}$ son plus petit sous-corps contenant 1.

Prop-def 39 : Soit $\varphi : \mathbb{Z} \to \mathbb{K}$ ($n \mapsto n.1$). On appelle caractéristique de $\mathbb{K}$ le nombre $p \in \mathbb{N}$ tel que $\ker \varphi = p\mathbb{Z}$. Alors $\mathrm{im}\,\varphi$ est le sous corps premier de $\mathbb{K}$.

Cor 40 : Soit $\mathbb{K}$ un corps. Si $\mathrm{car}\,\mathbb{K} = 0$, alors $\mathbb{Q} \hookrightarrow \mathbb{K}$. Si $p = \mathrm{car}\,\mathbb{K} \in \mathcal{P}$, alors $\mathbb{F}_p \hookrightarrow \mathbb{K}$.

Cor 41 : Soit $\mathbb{K}$ un corps fini de caractéristique p. Alors $\exists n \in \mathbb{N}$, $\#\mathbb{K} = p^n$.

Prop-def 42 : Soit $\mathbb{K}$ un corps de caractéristique p. $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Thm 43 : Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. On pose $q = p^n$. Alors il existe un unique corps à q éléments à isomorphisme près.

B] Etude des carrés dans $\mathbb{F}_q$.

On pose $\mathbb{F}_q^{*2} = \{x^2 \mid x \in \mathbb{F}_q^*\}$ pour $q = p^n$, $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.

Prop 44 : Si $p=2$, $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$. Si $p>2$, $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Prop 45 : $\forall x \in \mathbb{F}_q$, $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

Cor 46 : $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 [4]$

App 47 : Il existe une infinité de nombres premiers de la forme $4m+1$.

Def 48 : Soit $x \in \mathbb{F}_p$. On appelle symbole de Legendre de l'entier : $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ -1 \text{ si } x \notin \mathbb{F}_p^{*2} \\ 0 \text{ si } x = 0 \end{cases}$. Cette définition s'étend sur $\mathbb{Z}$ en considérant le reste modulo p.

Thm 49 : (loi de réciprocité quadratique) $\forall p, q \in \mathcal{P}$, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$] DEV 2 [3]

IV] En théorie des groupes [2]

Soit $p \in \mathcal{P}$.

A] Etude des p-groupes

Def 50 : On appelle p-groupe tout groupe d'ordre une puissance de p.

Lem 51 : Soient G un p-groupe opérant sur un ensemble fini X. Soit $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$. Alors $|X| \equiv |X^G| [p]$

Cor 52 : Le centre d'un p-groupe est non trivial.

Ex 53 : $\mathbb{Z}/p\mathbb{Z}$ est un p-groupe de centre lui-même.

B] Les théorèmes de Sylow.

Soient G un groupe d'ordre $|G| = p^\alpha m$ avec $p \nmid m$.

Def 54 : On appelle p-Sylow de G tout sous-groupe de G d'ordre p^α.

Rem 55 : $H < G$ est un p-Sylow si et seulement si $p \nmid [G:H]$

Ex 56 : L'ensemble des matrices triangulaires supérieures à diagonale unité dans $GL_n(\mathbb{F}_p)$ est un p-Sylow.

Thm 57 : (premier théorème de Sylow) G admet un p-Sylow.

Cor 58 : G contient des sous-groupes d'ordre p^i pour $i \leq \alpha$.

Thm 59 : (deuxième théorème de Sylow) Soit k le nombre de p-Sylow de G. Alors
- Si $H < G$, il existe un p-Sylow S de G tel que $H < S$.
- Les p-Sylow sont conjugués. En particulier, $k \mid |G|$.
- $k \equiv 1 [p]$.

Cor 60 : Un p-Sylow est conjugué dans G si et seulement si il est le seul.

App 61 : Tout groupe d'ordre 63 n'est pas simple.

Références :
- Mathématiques pour l'agrégation (Rombaldi) [1]
- Cours d'algèbre (Perrin) [2]
- Histoires hédonistes de groupes et de géométries (Caldero, Germoni) [3]