121

Nombres premiers - Applications

I Généralités

1) Définitions et premières propriétés

Déf : Un entier naturel p est dit premier si $p \geq 2$ et si ses seuls diviseurs sont 1 et lui-même.

Notation : On note $\mathbb{P}$ l'ensemble des nombres premiers

Ex : 2, 7, 13 sont premiers alors que $15 = 3 \times 5$ n'est pas premier : il est dit composé.

Th : Tout entier $n \in \mathbb{N}^*$ peut se décomposer de manière unique (à l'ordre près) en produit de facteurs premiers.
Autrement dit, il existe $r \in \mathbb{N}$, $p_1, \dots, p_r$ r éléments distincts de $\mathbb{P}$ et $\alpha_1, \dots, \alpha_r$ r entiers non nul tq :
$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

Rq : On peut écrire tout entier n ainsi : $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ où un nombre fini de $v_p(n)$ sont non nuls.
$v_p(n)$ est la valuation p-ième de n.

Prop : $\mathbb{P}$ est un ensemble infini

Rq : Le raisonnement de la démonstration, à savoir, à partir de $p_1, \dots, p_k$ premiers, construire $p_{k+1} = p_1 \dots p_k + 1$ peut se réutiliser pour démontrer la non finitude de premiers vérifiant une certaine condition.

Ex : Il y a un nombre infini de premiers p tel que $p \equiv 3 [4]$

2) Nombres premiers et arithmétique

Prop : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et ssi $p \in \mathbb{P}$

Th de Fermat : Soit $p \in \mathbb{P}$. Alors $\forall a \in \mathbb{Z}$, $a^p \equiv a [p]$
et si $a \wedge p = 1$, $a^{p-1} \equiv 1 [p]$

Déf : On appelle indicatrice d'Euler la fonction φ de $\mathbb{N}$ ds $\mathbb{N}$ qui à n associe $|\{k \in \mathbb{N} \mid k < n$ et $k \wedge n = 1\}|$ et $\varphi(1) = 1$

Prop : Si $p \in \mathbb{P}$, $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, pour $\alpha \in \mathbb{N}^*$
Pour $(p,q) \in \mathbb{N}^2$ tel que $p \wedge q$, $\varphi(p)\varphi(q) = \varphi(pq)$

Prop : Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$
pour $p_i \in \mathbb{P}$

On peut alors affiner le théorème de Fermat.

Prop : $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe de cardinal $\varphi(n)$

Th d'Euler : Pour $n \in \mathbb{N} \setminus \{0,1\}$ et k tel que $k \wedge n = 1$, $k^{\varphi(n)} \equiv 1 [n]$

Th de Wilson : Pour $n \in \mathbb{N} \setminus \{0,1\}$, $n \in \mathbb{P}$ ssi $(n-1)! \equiv -1 [n]$

Crible d'Eratosthène : Soit $n \in \mathbb{N}$ dont on teste la primalité de $k \leq n$
On écrit tous les nombres de $[\![2, n]\!]$
On enlève successivement les multiples de 2 puis on itère le procédé avec le plus petit nombre > 2 non enlevé.
Lorsqu'on atteint $\sqrt{n}$, on arrête le processus et les nombres restant sont premiers.

Rq : Marche car si $n \notin \mathbb{P}$, $\exists p \in \mathbb{P}$ tq $p \mid n$ et $p \leq \sqrt{n}$

II Applications

1) En théorie des groupes

Déf : Pour $p \in \mathbb{P}$, un p-groupe est un groupe fini d'ordre une puissance de p.

Prop : Le centre d'un p-groupe n'est pas réduit à $\{e\}$
Si $|G| = p^l$, $\exists H < G$ d'ordre p^k, pour $k \leq l$

Lemme de Cauchy : Si $p \mid |G|$ avec $p \in \mathbb{P}$, alors $\exists a \in G$ tq ord$(a) = p$

Th : Un groupe d'ordre $p \in \mathbb{P}$ est toujours abélien et cyclique
Un groupe d'ordre p^2 où $p \in \mathbb{P}$ est toujours abélien.

Rq : Conséquence du lemme de Cauchy et de $|Z(G)| > 1$.

Déf : Soit G un groupe fini d'ordre $p^l q$ où $p \wedge q$, $p \in \mathbb{P}$, $l \in \mathbb{N}^*$
Un p-sous-groupe de Sylow de G est un sous-groupe d'ordre p^l

Th de Sylow : Avec les mêmes notations :
- G admet au moins un p-Sylow
- Les p-Sylow sont conjugués
- Si n_p est le nombre de p-Sylow, $n_p \mid q$ et $n_p \equiv 1 [p]$

Appli : Si $n_p = 1$, le p-Sylow est distingué dans G
Ce théorème fournit alors un critère de non-simplicité

2) En théorie des anneaux et des corps

→ On peut étudier les résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}\setminus\{2\}$

Déf : Soit $p \in \mathbb{P}\setminus\{2\}$ et $n \in \mathbb{N}$.
On définit le symbole de Legendre de n sur p par $\left(\frac{n}{p}\right) = \begin{cases} 1 & n \text{ est carré de } \mathbb{Z}/p\mathbb{Z} \\ 0 & p \mid n \\ -1 & \text{sinon} \end{cases}$

Ex : $\left(\frac{3}{7}\right) = -1$ car 3 n'est pas un carré de $\mathbb{Z}/7\mathbb{Z}$

Propriété : Pour $p \in \mathbb{P}\setminus\{2\}$ et $n \in \mathbb{N}$: $\left(\frac{n}{p}\right) \equiv x^{\frac{p-1}{2}} [p]$

$\boxed{\text{DEV 1}}$ — Loi de réciprocité quadratique

Soient $(p,q) \in (\mathbb{P}\setminus\{2\})^2$, $p \neq q$ et $G = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^*$, $U = \{(1,1),(-1,-1)\}$
G/U est un groupe quotient qui admet comme système de représentants $E_1 = \{(i,j) \in G \,/\, 1 \le i \le \frac{p-1}{2}$ et $1 \le j \le \frac{q-1}{2}\}$
et $E_2 = \{(k,l) \in G \,/\, 1 \le l \le \frac{pq-1}{2}$ et $l \wedge pq = 1\}$
Alors on en déduit $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Ex : $\left(\frac{7}{15}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right) = -1$

→ Critères d'irréductibilité pour les polynômes à coefficients entiers.

Rappel : $p\mathbb{Z}$ est un idéal irréductible de l'anneau factoriel $\mathbb{Z}$

Prop (Réduction modulo p) : Soit $P \in \mathbb{Z}[X]$ unitaire et $p \in \mathbb{P}$
Alors : P irréductible sur $\mathbb{Z}/p\mathbb{Z}[X] \Rightarrow$ P irréductible sur $\mathbb{Z}[X]$

Ex : $X^3 - 2014X^2 + 1991X + 1$ est irréductible sur $\mathbb{Z}$

Prop (Critère d'Eisenstein) : Soit $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$
Soit $p \in \mathbb{P}$ tel que $p \mid a_k$, $\forall k \in [\![0, n-1]\!]$ et $p^2 \nmid a_0$
Alors P est irréductible sur $\mathbb{Z}[X]$

Ex : Pour $p \in \mathbb{P}$, $X^{p-1} + \dots + 1$ irréductible sur $\mathbb{Z}[X]$

Prop : La caractéristique d'un corps est 0 ou $p \in \mathbb{P}$
Un corps fini a pour cardinal une puissance de p.

Rappel : $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ où $p \in \mathbb{P}$

Dev

3) Cryptographie

Lemme : Soit $n \in \mathbb{N}^*$ sans facteur multiple et r tel que $r \equiv 0 [\varphi(n)]$
Alors $\forall a \in \mathbb{Z}$ tel que $a \wedge n = 1$, $a^r \equiv 1 [n]$ et $a^{r+1} \equiv a [n]$

Méthode RSA : Soit n sans facteurs carrés et r tel que $r \wedge \varphi(n) = 1$
- Un entier définit un message qu'on cherche à crypter
- On publie n et r et l'application de chiffrement C telle que $C \left(\begin{array}{l} \mathbb{N} \to \mathbb{Z}/n\mathbb{Z} \\ m \mapsto m^r \end{array} \right)$
- On garde en privé $\varphi(n)$ et l'entier s tel que $m^{rs} \equiv m [n]$ $\forall m \in \mathbb{N}$, i.e. tq $rs \equiv 1 [\varphi(n)]$ (via le lemme)

et l'application de déchiffrement $D \left(\begin{array}{l} \mathbb{N} \to \mathbb{Z}/n\mathbb{Z} \\ m \mapsto m^s \end{array} \right)$

Alors une personne peut crypter un message via C que le destinataire, connaissant s, peut décoder via D.

Rq : En pratique, n est produit de deux très grands premiers p et q. La publication de n ne permet pas de connaître $\varphi(n)$ et de calculer s. La décomposition de n étant difficile, s reste bien privé tandis que le destinataire peut le calculer via l'algorithme d'Euclide sachant que $\varphi(n) = (p-1)(q-1)$

(2)

III À la recherche des nombres premiers

1) Les exemples historiques

Ool
Rem

Dev

Déf : Le nombre $F_n = 2^{2^n} + 1$ est appelé n-ième nombre de Fermat

Culture : Fermat a montré que $F_0, F_1, F_2, F_3 = 257$ et $F_4 = 65537$ sont premiers et a affirmé que $F_n \in \mathbb{P}$, $\forall n \in \mathbb{N}$.
Hélas c'est faux et pire, aucun autre F_n, $n \geq 5$ est assuré d'être premier.

Euler a prouvé que $F_5 \notin \mathbb{P}$ et à ce jour, on a prouvé que F_k est composé pour $k \in [\![5, 30]\!]$ (le reste étant globalement inconnu)

Déf : Le nombre $M_n = 2^n - 1$ est appelé n-ième nombre de Mersenne

Prop : Si $M_n = 2^n - 1$ est premier, alors n est premier.

Culture : Mersenne a prouvé que $M_n \in \mathbb{P}$ pour $n \in \{2, 3, 5, 13, 17, 19, 31, 67, 127, 257\} =: X$ et $M_n \notin \mathbb{P}$ pour $n \notin X$ et $n \leq 257$. Depuis, on connaît 46 autres nombres de Mersenne premiers mais on ne sait toujours pas s'il y en a d'autres voire une infinité.

2) Tests de primalité

Critère de non-primalité de Fermat : Soit $n \in \mathbb{N}$

Si il existe $a \in \mathbb{N}$ tel que $a^{n-1} \not\equiv 1 [n]$, $a < n$, alors $n \notin \mathbb{P}$.

Rq : Condition suffisante mais pas nécessaire !
Les nombres de Carmichael sont les nombres non premiers non détectés par ce test.

Critère de non-primalité de Miller-Rabin : Soit $n \in \mathbb{N}$ et posons $n - 1 = 2^s t$ où $2 \nmid t$. Si $\exists a \in [\![2, n-1]\!]$ tel que :

- $a^t \not\equiv 1 [n]$
- $a^{2^i t} \not\equiv -1 [n]$ pour tout $i \in [\![0, s-1]\!]$

alors $n \notin \mathbb{P}$

Rq : Prendre $a = 2, 3$ ou 5 suffit à faire marcher le critère d'où une certaine praticité.

Critère de primalité de Lucas-Lehmer : Soit $n \in \mathbb{N}$ tel que la décomposition en nombres premiers de $n-1$ est connue.
S'il existe $a \in \mathbb{N}$ tel que

- $a^{n-1} \equiv 1 [n]$
- $\forall q \in \mathbb{N}$ tel que $q \mid n-1$, $a^{\frac{n-1}{q}} \not\equiv 1 [n]$

alors $n \in \mathbb{P}$

Rq : Test hasardeux, à faire quand on suspecte n premier.
Il faut connaître la décomposition de $n-1$, c'est pas évident.
Marche bien sur les nombres de Mersenne ou de Fermat.

3) Répartition des nombres premiers

DEV 2 — Théorème des deux carrés

Soit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2 \text{ pour } (a,b) \in \mathbb{N}^2\}$. Alors :

- pour $p \in \mathbb{P}$, $p \in \Sigma \iff p = 2$ ou $p \equiv 1 [4]$
- $n \in \Sigma \iff \forall p \in \mathbb{P}$, $v_p(n) \equiv 0 [2]$ pour $p \equiv 3 [4]$

Lemme : L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) = a^2 + b^2$ et $N(zz') = N(z)N(z')$ pour $(z, z') \in \mathbb{Z}[i]^2$

Théorème de Dirichlet (version faible) : Soit $n \in \mathbb{N}$

Il y a une infinité de nombres premiers p tel que $p \equiv 1 [n]$

Rq : Dans la suite arithmétique $(kn+1)$, il y a une infinité de $\mathbb{P}$

Traitons de la raréfaction des nombres premiers

Prop : $\sum_{p \in \mathbb{P}} \frac{1}{p} = +\infty$

Rq : Les nombres premiers ne se raréfient pas très vite.
Utiliser l'analyse complexe et la fonction ζ de Riemann : pour $s \in \mathbb{C}$ tq $\mathrm{Re}(s) > 1$, $\zeta(s) = \sum_{n \in \mathbb{N}^*} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$

Th des nombres premiers : Soit $\pi(n) = |\{k \in \mathbb{N} \mid k \leq n, k \in \mathbb{P}\}|$

Alors $\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln(n)}$

Rq : La démonstration nécessite la fonction ζ de Riemann.
Résultat démontré par Hadamard et de la Vallée Poussin.
À l'infini, les nombres premiers apparaissent donc ainsi.
Résultat historique et très difficile.

Th de la progression arithmétique de Dirichlet :
Soient a et b deux entiers premiers entre eux.
Alors il y a une infinité de nombres premiers de la forme $p \equiv a [b]$

Rq : Résultat aussi difficile.

De nombreuses questions restent ouvertes.
Par exemple, les nombres premiers jumeaux ((p,q) tel que $p - q = 2$ et $(p,q) \in \mathbb{P}^2$) sont-ils en nombre fini ou infini ?

Rq : Pour $p \in \mathbb{P}$, on ne peut pas faire un carré avec p boules.

) Marche via la propriété : si $p \in \mathbb{P}$
$d \mid p \Rightarrow d = 1$ ou $d = p$

) Dès lors, il est crucial de chercher des nombres premiers.

) $F_5 \notin \mathbb{P}$

Soit $n = 641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$

Alors $-2^{32} \equiv -2^{28}(2^4)$

$\equiv 2^{28} 5^4$

$\equiv (5 \cdot 2^7)^4$

$\equiv (-1)^4 \equiv 1 \, [n]$

Donc $641 \mid 2^{32} + 1 = F_5$

$\Rightarrow F_5 \notin \mathbb{P}$

) Rappelez qu'il y a une infinité de $p \in \mathbb{P}$

) se démontre via l'irréductibilité de Φ_n

Références

[Dem] : DEMAZURE

[Del] : J.-P. DELAHAYE
Merveilleux nombres premiers

[Per] : PERRIN

[Gou] : GOURDON Algèbre

Rev1 : $\emptyset$

Rev2 : PERRIN