121

120

Nombres premiers. Applications

I) Des nombres particuliers

1) Premières définitions

Déf 1: $n \in \mathbb{N}$ est dit premier s'il admet exactement deux diviseurs: 1 et n.
On note $\mathcal{P}$ l'ensemble de ces nombres.

Déf 2: Des entiers sont premiers entre eux si leur pgcd est 1.

Théorème fondamental de l'arithmétique:
Soit $n \geq 2$. n s'écrit de manière unique de la forme
$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, avec $p_1, \dots, p_k \in \mathcal{P}$, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$
à l'ordre près

Application 3: Calcul rapide de pgcd et ppcm de nombres dont on connait la décomposition

Application 4: si $1 \leq k \leq p-1$, alors $p \mid \binom{p}{k}$

2) Familles particulières de nombres premiers

Nombres de Fermat: [MAD]

Déf 5: $n \in \mathbb{N}$. $F_n = 2^{2^n} + 1$

Ex: $F_3 = 257$, $F_4 = 65537$ sont premiers
F_5 n'est pas premier

Prop 6: $m \neq n \Rightarrow F_m \wedge F_n = 1$

Conjecture: $\{F_n \mid n \in \mathbb{N}\} \cap \mathcal{P}$ est fini

Application géométrique (CULTURE): Un polygone régulier à n côtés est constructible à la règle et au compas si n est le produit d'une puissance de 2 et de nombres de Fermat premiers distincts.

Nombres de Mersenne:

Thm 7: $a, n \geq 2$. $a^n - 1$ premier $\Rightarrow a = 2$ et n premier

Déf 8: Un tel nombre est dit de Mersenne, noté M_n

Ex: $M_3 = 7$ est premier
$M_{11} = 2047$ n'est pas premier (23×89)

Prop 9: M_p premier $\Leftrightarrow 2^{p-1}(2^p - 1)$ parfait

Prop 10: On pose $\begin{cases} x_0 = 2 \\ x_{n+1} = 2x_n^2 - 1 \end{cases}$
Pour $n \geq 3$, M_n premier $\Leftrightarrow M_n \mid x_{n-2}$

Application 11: A permis de déterminer de très grands nombres premiers. ($\sim 10^7$ chiffres)

3) Des fonctions particulières liés à ces nombres

Indicatrice d'Euler:

Déf 12: $n \geq 1$. $\varphi(n)$ est le cardinal de $\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$

Prop 13: $n \geq 2$ se décompose en $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$
Alors $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$

Thm 14: Si $n \geq 1$, $n^{\varphi(n)} \equiv 1 [n]$

Prop 15: $\forall n \geq 1$, $\varphi(n) = \sum_{d \mid n} \varphi(d)$

Fonction de Möbius: $[x] = \max\{n \in \mathbb{N} \mid n \leq x\}$.

Déf 16: $\mu : \mathbb{N}^* \to \mathbb{Z}$
$1 \mapsto 1$
$n \mapsto 0$ si n a un facteur carré
$p_1 \dots p_k \mapsto (-1)^k$ si les p_i premiers distincts

Prop 17: $\sum_{d \mid n} \mu(d) = \begin{cases} 0 \text{ si } n \geq 2 \\ 1 \text{ si } n = 1 \end{cases}$

DEV 1

Application:
On pose p_n la probabilité que deux entiers de $[\![1,n]\!]$ soient premiers entre eux.
Alors $p_n \xrightarrow[n\to\infty]{} \frac{6}{\pi^2}$

[DLM]
[FGN]

I) Conséquences sur les structures algébriques

1) Groupes

Prop 1.2: Un groupe d'ordre p premier est cyclique engendré par tous ses éléments non-neutres.

Théorème de Cauchy: Si G fini est d'ordre divisible par p, il contient au moins un élément d'ordre p

Prop 1.3: p premier. Le centre d'un p-groupe n'est jamais réduit à $\{e\}$.

Cor 1.4: Un groupe d'ordre p^2 est abélien

Def 1.1: Si $|G|=n$, $p|n$, un p-Sylow de G est un p-sous groupe d'indice premier avec p

Théorèmes de Sylow: Si $p|n=|G|$, alors :
- G contient k p-Sylow, avec $k \geq 1$
- Tous les p-Sylow sont conjugués
- $k \mid n$
- $k \equiv 1 [p]$
- si S p-Sylow, on a : $S \lhd G \iff k=1$.

Exemples Un groupe d'ordre 63 n'est pas simple.

2) Corps finis

Prop 2.2: $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n premier

Def 2.3: K corps. Le sous-corps premier $\mathbb{K}$ de K est le plus petit sous-corps de K contenant 1.
Il est de cardinal premier (si K fini), que l'on appelle caractéristique de K.

Théorème 2.4: $p \in \mathcal{P}$, $n \in \mathbb{N}^*$, $q = p^n$. Alors
- Il existe un corps K à q éléments
- K est unique à isomorphisme près, noté $\mathbb{F}_q$

Résidus quadratiques :

Def 2.5: $p \in \mathcal{P}\setminus\{2\}$, $x \in \mathbb{Z}$. symbole de Legendre :
$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } p \mid x \\ 1 & \text{si } p \in (\mathbb{F}_p^*)^2 \\ -1 & \text{sinon} \end{cases}$$

Identité d'Euler : $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} [p]$ si $p \in \mathcal{P}$

Prop 2.6: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $\qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Loi de réciprocité quadratique :
$p, q \in \mathcal{P}\setminus\{2\}$, $p \neq q$. Alors $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

II) Une répartition intéressante

1) En quantité

Théorème 2.7: $\mathcal{P}$ est infini

On note $\pi(n) = \#(\mathcal{P} \cap [\![1, n]\!])$.

Théorème des nombres premiers :
$\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln n}$

Écrit autrement, en oubliant la rapidité :

$$\frac{\pi(x)}{x} \xrightarrow[+\infty]{} 0$$

cependant, il y a assez de premiers pour que :

Prop 2.?: $\sum_{p\in\mathcal{P}} \frac{1}{p}$ diverge.

2) et son emplacement

Thème très pointu, beaucoup de questions difficiles/ouvertes

Théorème de Dirichlet faible : Si $a \in \mathbb{N}$, ≥ 2 [X-ENS 1]

$\mathcal{P} \cap \{an+1\}$ est infini.

Théorème de la progression arithmétique [CULTURE] :

$a, b \in \mathbb{N}$. $a \wedge b = 1 \Rightarrow \mathcal{P} \cap \{an+b\}$ est infini

Postulat de Bertrand [CULTURE] :

$\forall n \in \mathbb{N}\ \exists p \in \mathcal{P},\ n < p < 2n$

IV) En pratique

1) Savoir si un nombre est premier [HIN]

* Force brute : tester tous les diviseurs possibles jusqu'à $\sqrt{n}$ → peu efficace

* Test de Wilson

p premier $\Leftrightarrow (p-1)! \equiv -1 [p]$

→ Calcul de $(p-1)!$ très cher

* Test de Fermat. basé sur $a^{n-1} \not\equiv 1 [n] \Rightarrow n$ composé.

Le test se base sur la recherche de a tels que $a^{n-1} \not\equiv 1 [n]$.

Si on en trouve : n est composé

Sinon : n est "probablement" premier   C-ex : 561

* Test de Solovay-Strassen : On essaie de vérifier l'identité d'Euler pour des x au hasard : on sait alors si n est composé ou probablement premier

2) Complexité

Algorithme AKS : (2004)

repose sur : $\forall n \geq 2, \forall a, a \wedge n = 1$.

$n \in \mathcal{P} \Leftrightarrow (X+a)^n \equiv X+a [n]$.

complexité en $O(\log^{12} n)$

Conséquences :

PRIMES est dans P

FACTOR(N,M) est dans NP ∩ co-NP

3) Application en cryptographie [DEV]

— Bob choisit p, q premiers, e premier avec $(p-1)(q-1)$, d tel que $e.d = 1 [(p-1)(q-1)]$

- Bob publie $n = pq$ et e

- Alice veut communiquer A. Elle envoie $B = A^e [n]$

- Bob calcule $B^d [n]$.

Thm du RSA : $B^d = A [n]$

Robustesse basée sur la difficulté de factoriser n

[DEL] Delahaye - Merveilleux nombres premiers.

[HIN] Hindry - Arithmétique.

[X-ENS I] Cours X-ENS Algèbre 1.

[PER] Perrin - Cours d'algèbre.

[WAS] Washington - Théorie des corps.

[NOB] Nobre - Leçons d'algèbre.