Nombres premiers. Applications.

121

I - NOMBRES PREMIERS, RÉPARTITION

a) Définition, décomposition en facteurs premiers

Def 1 : Un entier naturel p est premier s'il possède exactement deux diviseurs positifs, nommément 1 et p.

Ex 2 : 2, 3 sont des nombres premiers ; 1 ne l'est pas.

Thm 3 : Tout entier naturel n supérieur à 2 admet au moins un diviseur premier p, tel que $2 \leq p \leq \sqrt{n}$.

Thm 4 : Tout entier naturel n non nul se décompose de manière unique sous la forme $n = q_1^{v_{q_1}(n)} \dots q_r^{v_{q_r}(n)}$, à permutation près des q_i, où $q_1, \dots, q_r$ sont des nombres premiers et $v_{q_1}(n), \dots, v_{q_r}(n)$ sont des entiers naturels non nuls.

Def 5 : Dans le théorème précédent, $v_q(n)$ est appelé la valuation q-adique de n.

Thm 6 : Soient $n \geq 2$, $m \geq 2$ deux entiers, et $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, $m = \prod_{k=1}^{r} q_k^{\beta_k}$, leurs décompositions en facteurs premiers où les α_k, β_k peuvent être nuls.

Alors $\cdot \ pgcd(n,m) = \prod_{k=1}^{r} q_k^{\min(\alpha_k, \beta_k)}$;

$\cdot \ ppcm(n,m) = \prod_{k=1}^{r} q_k^{\max(\alpha_k, \beta_k)}$.

b) Répartition des nombres premiers.

Lemme 7 : [Euclide]
L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Théorème 8 : [Bertrand, admis]
Pour tout $n \in \mathbb{N}^*$, il existe des nombres premiers compris entre n et $2n$.

Théorème 9 : [Hadamard, admis]
Soit $\pi(n) = \#\{\mathcal{P} \cap [\![1, n]\!]\}$.
Alors $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$.

II - RÉDUCTION MODULO P

a) L'anneau $\mathbb{Z}/p\mathbb{Z}$.

Def 10 : La relation de congruence modulo n $a \sim b \Leftrightarrow n \mid a-b$ est une relation d'équivalence sur $\mathbb{Z}$, dont l'ensemble des classes d'équivalences modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

Thm 11 : Pour $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure d'anneau commutatif unitaire, telle que la surjection canonique $\begin{cases} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ k \mapsto k \bmod n \end{cases}$ soit un morphisme d'anneaux.

Thm 12 : Soit $a \in \mathbb{Z}$. $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow pgcd(a,n) = 1$.

Def 13 : On définit la fonction indicatrice d'Euler φ sur $\mathbb{N}^*$, comme : $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Prop 14 : $\cdot \ \varphi(p) = p-1$, pour p premier $\quad \cdot \ \varphi(p^\alpha) = (p-1)p^{\alpha-1}$, pour $\alpha \geq 1$

Thm 15 : [Euler] Pour tout $a \in \mathbb{Z}$, $pgcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$.

b) Le théorème des restes chinois, et une application à la cryptographie

Thm 16 : Soient n et m deux entiers naturels non nuls premiers entre eux, ie. tels que $pgcd(n,m) = 1$.
Alors il existe un isomorphisme d'anneaux entre $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Corollaire 17 : Soient $n, m \in \mathbb{N}_{\geq 1}$.
$\varphi(nm) = \varphi(n)\varphi(m)$. $\varphi(N) = \prod_{p^\alpha \| N} \varphi(p^\alpha)$ ... !

Application 18 : [protocole RSA]

Alice souhaite coder un message x, afin de l'envoyer à Bob et qu'il puisse le décoder. Pour cela, Bob choisit deux grands nombres premiers p et q, et transmet la clé publique $n = pq$.
Bob choisit également une clé de codage e, c'est-à-dire un entier e premier avec $\varphi(n) = (p-1)(q-1)$, qu'il transmet à Alice.

à faire

retirer si pas $\mathbb{Z}/p\mathbb{Z}$ corps.

Bob calcule enfin la clé de déchiffrement d, l'inverse de e modulo $\varphi(n)$, par exemple grâce à l'algorithme d'Euclide étendu.

Ainsi, Alice pourra envoyer le message codé $x^e \bmod n$, que Bob saura déchiffrer.

III - APPLICATIONS

a) Théorie des groupes finis

Thm 18 : [Cauchy]
Soit G un groupe fini d'ordre $n \geq 2$. Soit p un diviseur premier de n.
Alors il existe dans G un élément d'ordre p.

Def 19 : Soit p un nombre premier.
On appelle p-groupe tout groupe de cardinal p^α, où $\alpha \in \mathbb{N}^*$.

Prop 20 : Si G agit sur un ensemble fini E, on a
$$\#E^G \equiv \#E \bmod p.$$

Thm 21 : Le centre d'un p-groupe n'est pas réduit à $\{1\}$.

Thm 22 : Tout groupe d'ordre p^2, avec p premier, est commutatif.

Corollaire 23 : À isomorphisme près, il existe deux groupes d'ordre p^2 :
- $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

b) Théorie des corps finis

On considère K un corps dont le cardinal est fini.

Def 24 : On appelle caractéristique du corps K, le nombre p, générateur de $\ker \varphi$, où φ est le morphisme d'anneaux $\mathbb{Z} \to K$, $n \mapsto n.1$.

Rem 25 : Pour K fini, p est un nombre premier. Son sous-corps premier le plus petit corps de K contenant 1, est $\mathbb{Z}/p\mathbb{Z}$.
Par le théorème de la base téléscopique, K est alors de cardinal une puissance de p.

Prop 26 : L'application $F : K \to K$ définie par $x \mapsto x^p$ est un morphisme de corps, appelé morphisme de Frobenius.

Thm 27 : Pour tout entier n, pour tout nombre premier p, il existe un unique corps fini K de cardinal p^n, à isomorphisme près, noté $\mathbb{F}_{p^n}$.

Prop 28 : Soit $\mathbb{F}_q$ un corps de caractéristique $p > 2$.
Notons $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q,\ x = y^2\}$.
Alors $x \in \mathbb{F}_q^2 \iff x^{\frac{q-1}{2}} = 1$.

Corollaire 29 : Soit p premier $p > 2$, $q = p^n$, $n \in \mathbb{N}$.
-1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \bmod 4$.

Thm 30 : [Berlekamp]
Soient p premier, $n \in \mathbb{N}$, $q = p^n$, et $P \in \mathbb{F}_q[X]$ sans facteur carré.
On pose $P = \prod_{r=1}^{s} P_r$ la décomposition de P en produit d'irréductibles.
Si $r \neq 1$, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tels que $\operatorname{pgcd}(P, V - a)$ soit un facteur non trivial de P.

c) Résolution de problèmes arithmétiques

On pose $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2\}$. On cherche à caractériser Σ.

Lemme 31 : Σ est stable par multiplication.

Thm 32 : Soit p un nombre premier.
$p \in \Sigma \iff p = 2$ ou $p \equiv 1 \bmod 4$.

Thm 33 : Soit $n \geq 2$, $n = \prod_{p \geq 3} p^{v_p(n)}$ sa décomposition en facteurs premiers.
Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 \bmod 4$.

DEV 1

IV _ RECHERCHE DES NOMBRES PREMIERS

a) Des caractérisations, peu efficaces.

Thm 34 : [Wilson]
Soit $p \geq 2$.
p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

Rem 35 : Un algorithme utilisant cette caractérisation utiliserait $(p-1)$ multiplications, ce qui est absurde.

Thm 36 : [Fermat]
Soit $p \geq 2$ un nombre premier.
Alors pour tout a dans $\mathbb{Z}$ premier avec p, $a^{p-1} \equiv 1 \mod p$.

Rem 37 : Un algorithme voulant vérifier la non-primalité de p consiste en chercher un entier a premier avec p, telle que $a^{p-1} \not\equiv 1 \mod p$

Rem 38 : Cet algorithme ne permet pas de prouver la primalité de p.

Def 39 : On appelle nombre de Carmichael un entier $n \geq 2$, composé, tel que pour tout $a \in \mathbb{Z}$, $a^n \equiv a \mod n$.
Ainsi les nombres de Carmichael sont des entiers composés n'échouant pas au test de Fermat.

Thm 40 : [Korselt]
Soit $n \geq 2$.
n est un nombre de Carmichael si et seulement si n est sans facteur carré et pour tout diviseur premier p, $p-1 \mid n-1$.

Cor 41 : Tout nombre de Carmichael est impair et admet au moins trois diviseurs premiers distincts.

Lemme 39.5 : Soit p premier. $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique.

2 136

b) Le critère de Rabin-Miller.

Prop 42 : Soit $p > 2$ un nombre premier.
Écrivons $p - 1 = 2^s t$, avec t impair.
Soit a un entier non divisible par p. Alors :
- soit $a^t \equiv 1 \mod p$;
- soit il existe i, avec $0 \leq i < s$, tel que $a^{2^i t} \equiv -1 \mod n$.

Corollaire 43 : Soit $n > 1$ un entier impair. Écrivons $n-1 = 2^s t$, avec t impair.
Supposons qu'il existe un entier a, avec $1 < a < n$,
tel que $a^t \not\equiv 1 \mod n$ et $a^{2^i t} \equiv -1 \mod n$ $\forall i \leq s-1$.
Alors n est composé.

Thm 44 : [Rabin]
Si n est un entier impair composé, au moins les trois quarts des entiers de $[\![1, n[\![$ sont des témoins vérifiant le test ci-dessus.