NOMBRES PREMIERS. APPLICATIONS.

121

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

I - Généralités sur les nombres premiers

1 - Définitions et exemples [GOU] p.7-9

Déf 1 : Soit $p \in \mathbb{N}$ tq $p \geq 2$. p est dit premier ssi ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Ex 2 : 2, 3, 5, 7, 11, 13, ...

Thm 3 : (BEZOUT) Soient $a, b \in \mathbb{Z}$. Alors $\text{pgcd}(a,b) = 1$ ssi $\exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = 1$.

Rq : On trouve un tel couple à l'aide de l'algorithme d'Euclide.

Thm 4 : (GAUSS) Soient $a, b, c \in \mathbb{N}^*$. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Cor 5 : (Lemme d'Euclide) Soit p premier. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$

Application 6 : Soit $p \in \mathbb{P}$ et $1 \leq k \leq p-1$. Alors $p \mid \binom{p}{k}$.

2 - Décomposition en facteurs premiers [GOU]

Prop 7 : Tout entier $n, |n| \geq 2$ est divisible par un nombre premier. p.8

Prop 8 : L'ensemble $\mathbb{P}$ des nombres premiers est infini. p.9

Thm 9 : (Théorème fondamental de l'arithmétique)
Soit $n \geq 2$ s'écrit de manière unique à l'ordre près :

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad (*) \qquad \text{p.8}$$

où $p_i \in \mathbb{P}$ (distincts) et $\alpha_i \in \mathbb{N}^*$. $(*)$ est la décomposition en facteurs premiers de n.

Ex 10 : $300 = 2^2 \times 3 \times 5^2$

Rq : Cela mène à la définition d'anneau factoriel.

Application 11 : (produit Eulérien) $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$ [R-W] p.279

3 - Deux fonctions arithmétiques

Déf 12 : Soit $n > 1$. On appelle indicatrice d'Euler : [GOU] p.31
$\varphi(n) = \#\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$ ou $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

Prop 13 : Si $\text{pgcd}(m,n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$. p.32

Prop 14 : Soit $p \in \mathbb{P}$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. p.31

Prop 15 : Soit $n \geq 2$, on a $n = \sum_{d \mid n} \varphi(d)$ p.32

Déf 16 : On appelle fonction de Möbius $\mu : \mathbb{N}^* \to \{0, 1, -1\}$ tq $\mu(1) = 1$, $\mu(m) = 0$ si $\exists p \in \mathbb{P}$ tq $p^2 \mid m$ [PER] et $\mu(p_1 \dots p_r) = (-1)^r$ si les p_i sont distincts. p.99

Prop 17 : Si $\text{pgcd}(m,n) = 1$ alors $\mu(mn) = \mu(m)\mu(n)$. p.89

Prop 18 : $\forall n \in \mathbb{N}^*, n \neq 1$, on a $\sum_{d \mid n} \mu(d) = 0$.

Prop 19 : (Formule d'inversion) Soit $n \geq 1$, on a $\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$ p.89

Application 20 : Soit Φ_n le n-ième polynôme cyclotomique.

$$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)} \qquad \text{p.92}$$

4 - Répartition des nombres premiers. [R-W] p. 275, 276

Thm 21 : (Dirichlet) [ADMIS] Soit $a, b \in \mathbb{N}$ tq $\text{pgcd}(a,b) = 1$.
Alors $\{an + b \mid n \in \mathbb{N}\}$ contient une infinité de nombres premiers.

Déf 22 : On note $\pi(n) = \text{card}\{p \in \mathbb{P} \mid p \leq n\}$.

Thm 23 : (Théorème des nombres premiers)

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

II - Corps finis

1 - Anneau $\mathbb{Z}/n\mathbb{Z}$ [GOU] p.9 et p.31

Prop 24 : Soit $n \geq 2$. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $n \in \mathbb{P}$.
On note $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Méthode : Soit $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*$. Par Bezout $ap + bx = 1 \Rightarrow \bar{x}^{-1} = \bar{b}$

Ex 25 : $\bar{36}^{-1} = \bar{17}$ dans $(\mathbb{Z}/47\mathbb{Z})^*$.

Thm 26 : (FERMAT) Soit $p \geq 2$ premier. Alors :

$$\forall a \in \mathbb{Z},\ a^p \equiv a \ [p]$$
$$\forall a \in \mathbb{Z},\ p \nmid a,\ a^{p-1} \equiv 1 \ [p].$$

DVPT 1

Application 27 : (Thm de Sophie Germain) Soit $p \in \mathbb{P}$ impair tq $q = 2p + 1 \in \mathbb{P}$. Alors $\exists (x, y, z) \in \mathbb{Z}^3$ tq $xyz \not\equiv 0 [p]$ et $x^p + y^p + z^p = 0$. [FGN] p.167

Application 28 : (Chiffrement RSA). Soient $p, q \in \mathbb{P}$ distincts et $n = pq$.
Soient $c, d \in \mathbb{Z}$ tq $cd \equiv 1 [\varphi(n)]$. $\forall t \in \mathbb{Z}$, on a $t^{cd} \equiv t [\varphi(n)]$
• fonction de chiffrement : $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \mapsto \bar{t}^c$

• fonction de déchiffrement: $g: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \mapsto \bar{t}^d$ [GOU] p.34-35

On a $f \circ g(\bar{t}) = \bar{t}$.
(n,c) est la clé publique et d est la clé secrète.
Sans la connaissance de d, il est quasiment impossible de déchiffrer le message $\bar{t}$.

2- Théorie élémentaire des corps finis [PER] p.72

Déf 29: Soit k un corps et $\Psi: \mathbb{Z} \to k$, $n \mapsto n.1_k$. Le nombre p générateur de $\ker\Psi$ est la caractéristique de k, $p=0$ ou $p \in \mathcal{P}$.

Rq: Ici k est fini donc $\mathrm{car}(k) = p > 0$.

Prop 30: Soit k un corps fini tq $\mathrm{car}(k) = p$.
Alors $q = |k| = p^n$. $(n \in \mathbb{N}^*)$.

Prop 31: Soit k un corps fini, $\mathrm{car}(k) = p > 0$.
$F: k \to k$, $x \mapsto x^p$ est un automorphisme (appelé morphisme de Frobenius).

Thm 32: Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, $q = p^n$.
1) $\exists$ un corps k à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
2) k est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Thm 33: Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique (isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$)

3- Carrés dans $\mathbb{F}_q$ $(q = p^n)$ [R-W] p.129-130, [PER] p.74

$\mathbb{F}_q^2 = \{ x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \text{ tq } x = y^2 \}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$

Rq: Pour $p=2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$.

Prop 34: Pour $p \geq 3$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Déf 35: Soit $p \in \mathcal{P}$, $p \geq 3$. Soit $x \in \mathbb{F}_p^*$. Symbole de Legendre:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon} \end{cases}$$

Si $p \nmid a$, $\left(\frac{a}{p}\right) = \left(\frac{x}{p}\right)$ où x est la classe de a modulo p.

Prop 36: (Formule d'Euler) Soit $x \in \mathbb{F}_p^*$. Alors $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ DVPT 2 [FGN] p.158 ou [PER] p.57

Application 37 (Théorème des 2 carrés)
p est somme de 2 carrés $\iff p \equiv 1 [4]$ ou $p=2$.

Thm 38: (Loi de réciprocité quadratique)
Soit $q \in \mathcal{P}$, $q \neq p$. Alors $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \times (q-1)/2}$

Ex 39: $\left(\frac{3}{17}\right) = -1$.

4- Application à la réduction des polynômes mod p

Prop 40: (Critère d'Eisenstein) $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$. [GOU] p.58
On suppose que $\exists p \in \mathcal{P}$ tq:
(i) $p \mid a_k$ $\forall k \in [\![0, n-1]\!]$ et $p \nmid a_n$
(ii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 41: Soit $p \in \mathcal{P}$ et $\Phi(X) = X^{p-1} + \dots + X + 1$.

Thm 42: $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $\bar{P}$ sa réduction mod p.
On suppose $\bar{a}_n \neq 0$ dans $\mathbb{F}_p$. Alors, si $\bar{P}$ est irréductible sur $\mathbb{F}_p[X]$, P est irréductible sur $\mathbb{Q}[X]$. [PER] p.77

Ex 43: $p=2$, $P = X^3 + 462X^2 + 2433X - 67691$
$\bar{P} = X^3 + X + 1$ irréductible sur $\mathbb{F}_2$.

Rq: La réciproque est fausse: X^4+1 irréductible sur $\mathbb{Q}[X]$ mais réductible sur $\mathbb{F}_p$ $\forall p \in \mathcal{P}$. [PER] p.78.

III - Théorie des groupes

1- p-groupes $(p \in \mathcal{P})$ [GOU] p.27

Déf 44: Un p-groupe est un groupe d'ordre p^α $(\alpha \in \mathbb{N}^*)$.

Ex 45: $(\mathbb{Z}/2\mathbb{Z})^2$, Q_8 sont des 2-groupes.

Prop 46: Tout groupe d'ordre p est cyclique.

Prop 47: Le centre d'un p-groupe non trivial est non trivial.

Cor 48: Tout p-groupe d'ordre p^2 est abélien.

Cor 49: Tout p-groupe est résoluble.

2 - Théorèmes de Sylow [PER] p. 18-20

Déf 50 : Soit G un groupe tq $|G| = n = p^\alpha m$ avec $p \in \mathcal{P}$ et $p \nmid m$.
On appelle p-sous-groupe de Sylow de G, un sous-groupe de cardinal p^α.

Ex 51 : $G = GL_n(\mathbb{F}_p)$, $P = \{ A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1 \}$ est un p-Sylow de G.

Thm 52 (Sylow) Soit G un groupe tq $|G| = p^\alpha m$ avec $p \nmid m$.
1) G contient au moins un p-sous groupe de Sylow.
2) Si $H < G$ est un p-groupe, alors $\exists$ un p-Sylow S tq $H \subset S$.
3) Les p-Sylows sont conjugués.
4) $n_p \equiv 1 \ [p]$ (n_p = nombre de p-Sylow)

Cor 53 : S un p-Sylow de G.
$S \trianglelefteq G \iff S$ est l'unique p-Sylow de G.

Application 54 : Un groupe d'ordre 63 n'est pas simple.

IV - Primalité en pratique

1 - Algorithmes élémentaires

Algorithme 55 : Soit $n \in \mathbb{N}$, $n \geq 2$. On teste si $i \mid n$ pour $i \in [2, n-1]$

Algorithme 56 : (Critère d'Ératosthène)
On veut trouver $\mathcal{P} \cap \{2, \dots, N\}$ pour un certain N.
On pose $P_1 := \{2, \dots, N\}$, $P_2 := \emptyset$ et on fait :
Tant que $P_1 \neq \emptyset$ | $P_2 \leftarrow P_2 \cup \{\min P_1\}$
$P_1 \leftarrow P_1 \setminus (\min P_1)\mathbb{N}^*$
Alors $P_2 = \mathcal{P} \cap \{2, \dots, N\}$.

Rq : Cet algorithme a l'avantage de nous donner tous les nombres premiers $\leq N$ contrairement au premier.

2 - Un test de primalité [DEM] p. 72

Prop 57 : (Critère de Lehmer) Soit $n > 1$ impair.
n premier $\iff$ ($\exists a \in \mathbb{N}$ tq $a^{n-1} \equiv 1 \ [n]$ et $a^{(n-1)/q} \not\equiv 1 \ [n]$ pour tout facteur premier q de $(n-1)$.)

Ex 58 : $n = 7$ et $a = 3$.

3 - Deux classes de nombres remarquables

- **Nombres de Fermat :** [DEM] p. 75

Conjecture de Fermat : tous les nombres de la forme $Fer_m = 2^{2^n} + 1$ sont premiers.
En réalité, $Fer_1, Fer_2, Fer_3, Fer_4$ sont premiers mais pas Fer_5 !

Lemme 55 (Critère de Pépin)
Fer_n premier $\iff (3^{2^{2^n}-1} \equiv -1 \ [Fer_n])$

Rq : Ce critère est encore valable avec 5 ou 7 au lieu de 3.

- **Nombres de Mersenne :** [DEM] p. 77

Ce sont les entiers de la forme $2^s - 1$.
Comme $2^a - 1 \mid 2^{ab} - 1$, $2^s - 1$ est premier $\Rightarrow s$ premier.
$2^s - 1$ est premier pour $s = 2, 3, 5, 7$ mais pas pour $s = 11$!
En effet, $2^{11} - 1 = 2047 = 23 \times 89$

Références :
[GOU] : Gourdon, Algèbre.
[PER] : Daniel Perrin, Cours d'algèbre.
[R-W] : Ramis - Warusfel, Algèbre.
[DEM] : Demazure, Cours d'algèbre, Primalité, divisibilité, codes.
[FGN] : Francinou, Gianella, Nicolas, Oraux X-ENS Algèbre 1.