Cadre : p désigne un nombre premier. $n \in \mathbb{N}$

I. Nombres premiers. Anneaux $\mathbb{Z}/n\mathbb{Z}$

1) Définition, premières propriétés

Déf. (1) : $n \geq 2$ est dit composé s'il existe $a, b \in \mathbb{N}$ et ≥ 2 tels que $n = ab$. Si $n \geq 2$ n'est pas composé on dit que c'est un nombre premier.

Ex. (2) : 2, 3 sont premiers. 6, 15 sont composés

Th. (3) : Soit $n \geq 2$. Il existe alors $p_1 \dots p_r$ des nombres premiers et $\alpha_1 \dots \alpha_r \in \mathbb{N}^*$ tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. De plus cette décomposition est unique à permutation des facteurs premiers près.

Th. (4) : L'ensemble $\mathcal{P}$ des nombres premiers est infini

Coro. (5) : On peut écrire pour $n \in \mathbb{N}^*$, $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ où les $v_p(n) \in \mathbb{N}$ sont presque tous nuls.

Rq (6) : Le corollaire s'étend à $n \in \mathbb{Z}$ (en ajoutant son signe). $\mathbb{Z}$ est alors un anneau factoriel et $\mathcal{P}$ une famille de représentants des irréductibles modulo la relation d'association.

2) Arithmétique dans $\mathbb{Z}$.

Prop. (7) : Soient $a, b \in \mathbb{Z}^*$. Alors : 1) $a | b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$

2) $\mathrm{pgcd}(a,b) = a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ 3) $\mathrm{ppcm}(a,b) : a \vee b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$

4) $p | ab \Rightarrow p | a$ ou $p | b$ (lemme d'Euclide)

Déf. (8) : $a, b \in \mathbb{Z}$ sont dits premiers entre eux si $a \wedge b = 1$

Lemme (9) : (Gauss) $a, b, c \in \mathbb{Z}$. Si $a | bc$ et $a \wedge b = 1$, alors $a | c$

Th. (10) : (Bezout) $a, b \in \mathbb{Z}$. $a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} / ua + vb = 1$

Rq (11) : L'algorithme d'Euclide étendu prouve l'implication de Th. (10)

3) Anneaux $\mathbb{Z}/n\mathbb{Z}$ $n \in \mathbb{N}^*$

Prop. (12) : Soit $k \in \mathbb{N}$. Sont équivalentes :
1) $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ 2) $k \wedge n = 1$
3) $\bar{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$

Déf. (13) : On définit pour $n > 1$: $\varphi(n) = |\{0 \leq k \leq n-1 \ / \ k \wedge n = 1\}|$. φ est appelée indicatrice d'Euler.

Rq (14) : Il y a $\varphi(n)$ générateurs de $\mathbb{Z}/n\mathbb{Z}$ $/ n \geq 2$

Prop. (15) : $\forall \alpha \geq 1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Prop. (16) : Soit $n \geq 2$. Alors
$\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier

Rq (17) : si $n = 0$, $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ est également intègre

Th. (18) : (petit théorème de Fermat)
Soit $a \in \mathbb{Z}$. Alors $a^p \equiv a \, [p]$ et si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \, [p]$.

II. Groupes

Cadre : $(G, \cdot)$ désigne un groupe fini [Ber]

1) p-groupes

Déf. (19) : On dit que G est un p-groupe si $|G| = p^\alpha$ où $\alpha \in \mathbb{N}$. 180

Lemme (20) : Si G est un p-groupe qui agit sur un ensemble fini X, et $X^G = \{x \in X \ / \ \forall g \in G, g \cdot x = x\}$, alors $|X| \equiv |X^G| \, [p]$. 181

Coro (21) : Le centre d'un p-groupe est non trivial

Appli (22) : Si $|G| = p^2$, alors G est abélien. ♡

2) Théorèmes de Sylow [Ber]

Cadre : On suppose que $|G| = p^\alpha m$ où $\alpha \in \mathbb{N}$, $m \in \mathbb{N}^*$ et $p \nmid m$

Déf. (23) : Un p-Sylow de G est un sous-groupe de G de cardinal p^α 311

Rq (24) : Un p-Sylow de G est un p-sous-groupe de G

Th. (25) : (*Sylow*)

1) Il existe (au moins) un p-Sylow de G.

313 2) Les p-Sylow sont conjugués (dans G)

3) Si $H \leq G$, et S est un p-Sylow de G, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

4) Soit n_p le nombre de p-Sylow de G. Alors $n_p \equiv 1\,[p]$ et $n_p \mid m$

[Per] 29 **Appli. (26) :** Soit $H \triangleleft \mathfrak{A}_5$. Si H contient un 5-cycle, alors il les contient tous.

III. Corps finis

1) Propriétés fondamentales

[Per] **Déf./Prop (27) :** Soit K un corps commutatif et $\varphi : (\mathbb{Z},+) \longrightarrow (K,+)$, $n \longmapsto n.1_K = 1_K + \dots + 1_K$.

72 φ est alors un morphisme de groupes. et $\ker \varphi = \{0\}$ ou $\ker \varphi = \mathbb{Z}/p\mathbb{Z}$. La caractéristique de K est alors 0 ou p.

Coro. (28) : Si K est un corps fini de cardinal q, alors il existe $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$ tels que $q = p^\alpha$. On note alors $K = \mathbb{F}_q$.

Ex. (29) : Il n'existe pas de corps de cardinal 12.

Notation (30) : On considèrera que $q = p^\alpha$, $\alpha \geq 1$.

Prop. (30 bis) : Soit K un corps de caractéristique $p > 0$. L'application $F : K \to K$ définie par $F(x) = x^p$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, $F = id_K$. 73

74 **Prop. (31) :** $(\mathbb{F}_q^*, \cdot)$ est cyclique. On a donc $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$

2) Construction de corps finis

Prop. (32) : Soit $P \in \mathbb{F}_p[X]$ irréductible et $n = \deg P$. Alors $\mathbb{F}_q[X]/(P)$ est un corps isomorphe à $\mathbb{F}_{p^n}$.

[Dem3] 220 **Th. (33) :** Pour tout $n \geq 1$, il existe des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$. De plus, si on note m_n leur nombre, alors $\dfrac{p^n - p^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n \leq \dfrac{p^n}{n}$. En particulier $m_n \sim \dfrac{p^n}{n}$

Rq. (34) : Si $P \in \mathbb{F}_q[X]$, l'algorithme de Berlekamp permet de le décomposer en produit de facteurs irréductibles. [BMP] 244

Ex. (35) : $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$ ▽

3) Carrés dans les corps finis

Notion (36) : On pose $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \{x^2, x \in \mathbb{F}_q^*\}$ [Per] 74

Prop. (37) : On rappelle que $q = p^\alpha$, $\alpha \geq 1$.

1) si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

2) si $p > 2$, $|\mathbb{F}_q^2| = \dfrac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \dfrac{q-1}{2}$

Prop. (38) : Si $p > 2$, alors : $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$ 75

Déf. (39) : Si $p > 2$ et $a \in \mathbb{F}_p$, le symbole de Legendre de a est 302

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*2} \\ -1 & \text{si } a \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2} \\ 0 & \text{si } a = 0 \end{cases}$$

Th. (40) : si $p > 2$, alors $M, N \in \mathcal{S}_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ sont congruentes SSI elles ont même déterminant modulo $\mathbb{F}_q^{*2}$ [Per] 129

Th. (41) : (*loi de réciprocité quadratique*) [NH2G2] 304

Soient p, q deux nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$ DVP

Appli. (42) : Calculer $\left(\frac{19}{43}\right)$

IV. Polynômes

1) Critères d'irréductibilité

[Per] **Th. 43 :** (critère d'Eisenstein)

Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$, $n \geq 2$ et $p \in \mathcal{P}$. On suppose que

76 1) $p \nmid a_n$ 2) $\forall 0 \leq i \leq n-1, p \mid a_i$ 3) $p^2 \nmid a_0$.

Alors P est irréductible sur $\mathbb{Q}$.

77 **Appli. 44 :** $\Phi_p = X^{p-1} + \dots + 1$ est irréductible sur $\mathbb{Z}$

Th. 45 : Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$. On suppose $\overline{a_n} = a_n[p] \neq \overline{0}$.
Alors si $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$, P est irréductible sur $\mathbb{Q}$.

Rq 46 : ⚠ P pas nécessairement irréductible sur $\mathbb{Z}$ ($P = 2X$, $p = 3$)

Ex. 47 : $X^3 + 28X^2 + 161X - 23$ est irréductible sur $\mathbb{Z}$.

2) Polynômes cyclotomiques

Notation 48 : $\mu_n = \{\zeta \in \mathbb{C} / \zeta^n = 1\}$ et $\mu_n^* = \{\zeta \in \mu_n / \zeta^d \neq 1 \ \forall 1 \leq d \leq n-1\}$

Déf. 49 : Pour $n \geq 1$, le n-ième polynôme cyclotomique est $\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$

[Per] 80 **Prop. 50 :** $X^n - 1 = \prod_{d \mid n} \Phi_d$

81 **Prop. 51 :** $\forall n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$

82 **Th. 52 :** $\forall n \geq 1$, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

Appli. 53 : (théorème de Dirichlet faible)

DVP2 [FGN1] 31 Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers congrus à 1 modulo n.

V. Test de primalité. Chiffrement RSA

1) Test de primalité de Fermat

Méthode 54 : On part d'un théorème du type :
si p est premier, alors la propriété (P) est vérifiée.

Test de Fermat : Entrée : $n \geq 3$ impair, $a \in \{2 \dots n-1\}$

- calculer $\mathrm{pgcd}(a,n)$ (Euclide)
- si $d \neq 1$, renvoyer "d divise n", sinon calculer $b = a^{n-1} [n]$
- si $b \neq 1$, renvoyer "non premier", sinon renvoyer "probablement premier".

Rq 55 : Le test de Fermat se passe mal pour les nombres de Carmichael, i.e. les entiers n tels que $a^n = a [n]$ pour tout n (ex. 561)

Rq 56 : on sait convenablement tester la primalité d'entiers de ~ 1000 chiffres

2) Chiffrement RSA [Dem]

Principe 57 : Alice souhaite envoyer à Bob un message crypté :

1) elle choisit un couple (p,q) de grands entiers premiers. On pose $n = pq$. 64
2) elle choisit $2 \leq \pi \leq \varphi(n) - 2$ tel que $\pi \wedge \varphi(n) = 1$ ($\varphi(n) = (p-1)(q-1)$).
La clef publique est alors (n, π)
3) elle détermine par l'algorithme d'Euclide s tel que $\pi s = 1 [\varphi(n)]$
La clef privée que seul Bob a est (n, s).
4) Alice envoie à Bob $m' = m^{\pi}$ où $m \in \mathbb{Z}/n\mathbb{Z}$ est son message

Prop. 58 : $m^{\pi s} = m [n]$

5) Bob fait m'^{s} et décrypte le message

Rq 59 : La robustesse du chiffrement RSA repose sur la difficulté à décomposer un grand entier en produit de facteurs premiers, la complexité des meilleurs étant en $\exp(O((\ln n)^{1/3}))$.

Références :

- [Ber] Berhuy, *Algèbre : le grand combat* (2ᵉ éd.)
- [Per] Perrin, *Cours d'algèbre*
- [DMJ] Demazure, *Cours d'algèbre*
- [NH2G2] Caldero, *Nouvelles...* Tome 1
- [FGN1] Francinou, *Oraux X-ENS Algèbre 1*
- [BMP] Beck, *Objectif agrégation* (2ᵉ éd.)