109 - Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications.

1 Généralités

On se donne $m, n \in \mathbf{N}^*$. On note $m \wedge n = pgcd(m,n)$.

Proposition 1. *Soit G un groupe fini monogène de cardinal n. Alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.*

Proposition 2. *$\mathbf{Z}/n\mathbf{Z}$ est un anneau.*

Exemple. Tests de divisibilité par 3, 9, 11.

Proposition 3. *Soit $d \in \mathbf{N}^*$ tel que $d \leq n$. Alors il existe un sous-groupe d'ordre d de $\mathbf{Z}/n\mathbf{Z}$ ssi $d|n$, auquel cas un tel sous groupe est unique et cyclique.*

Proposition 4. *$\mathbf{Z}/n\mathbf{Z}$ est intègre ssi n est premier, auquel cas c'est un corps.*

Théorème 1 (Bézout). *Soient a et b deux entiers relatifs. Alors ils sont premiers entre eux ssi il existe deux entiers relatifs u et v tels que $au+bv=1$.*

Théorème 2 (lemme chinois). *Si $m \wedge n = 1$, alors on a un isomorphisme d'anneaux : $\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$.*

Proposition 5. *Soit $(a,b,c) \in \mathbf{Z}^3$. L'équation $ax+by=c$, avec x et y cherchés dans $\mathbf{Z}$:*
- *n'a pas de solution si $a \wedge b$ ne divise pas c*
- *a pour solutions les $(x_0 + \frac{bk}{a\wedge b}, y_0 - \frac{ak}{a \wedge b})$, avec $k \in \mathbf{Z}$ et (x_0, y_0) une solution particulière sinon.*

2 Indicatrice d'Euler et groupe des inversibles

Théorème 3. *Soit $s \in \mathbf{Z}$. Lpsse :*

(i) $s \wedge n = 1$

(ii) *s est un générateur du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$*

(iii) $s \in (\mathbf{Z}/n\mathbf{Z})^*$

Proposition 6. *On a l'isomorphisme :*

$$\begin{aligned}\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) &\to (\mathbf{Z}/n\mathbf{Z})^* \\ \phi &\mapsto \phi(1)\end{aligned}$$

Définition 1. On appelle *indicatrice d'Euler* la fonction notée φ qui $n \in \mathbf{N}$ associe associe le nombre d'éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$. Par supra, on a $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^*| = |\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})|$

Proposition 7. *L'indicatrice d'Euler est multiplicative : si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$. De plus, pour tout nombre premier p et tout entier α, on a $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.*

Théorème 4 (Structure de $(\mathbf{Z}/n\mathbf{Z})^*$)**.** *On décompose n en facteurs premiers : $n = \prod_i p_i^{\alpha_i}$. Alors, par le lemme chinois, $(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_i (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*$. De plus pour tout nombre premier impair p et tout entier α on a : $(\mathbf{Z}/p^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z})^* \simeq \{1\}$, $(\mathbf{Z}/4Z)^* \simeq \mathbf{Z}/2Z$ et pour tout entier $\alpha > 2$, $(\mathbf{Z}/2^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$*

Exemple. $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique ssi $n = 4$ ou $n = p^\alpha$ ou $n = 2p^\alpha$, avec p nombre premier impair.

Application. Classification des groupes d'ordre pq.

3 Dual et classification des groupes abéliens finis

Proposition 8. *Dual de $\mathbf{Z}/n\mathbf{Z}$.*

Lemme 1. *Dual du produit, prolongement des caractères.*

Théorème 5. *Classification des groupes abéliens finis.*

Proposition 9. *Si G/Z est cyclique, alors G est abélien.*

Application. Classification des groupes d'ordre p^2.

4 Carrés de $\mathbf{Z}/p\mathbf{Z}$ et de $\mathbf{N}$

Définition 2. Soit p un nombre premier impair. Le *symble de Legendre* de n modulo p, noté $\left(\frac{n}{p}\right)$, est défini par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0\ [p] \\ 1 \text{ si } a \text{ est un carré non nul modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}$$

Remarque. Cela revient à résoudre l'équation dans $\mathbf{Z}$: $x^2 - p \cdot y + n = 0$.

Proposition 10. *Le nombre de carrés dans* $\mathbf{Z}/p\mathbf{Z}$ *est* $(p+1)/2$.

Proposition 11. $\forall a \in \mathbf{Z},\ \left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2}\ [p]$

Définition 3. Soit N un entier impair, $N = \prod_i p_i^{\alpha_i}$, et a un entier. Le *symbole de Jacobi* est donné par :

$$\left(\frac{a}{N}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$$

Remarque. Le symbole de Jacobi sert surtout comme un intermédiaire de calcul au symbole de Legendre.

Proposition 12. *(i) si* $a \equiv b\ [N]$, *alors* $\left(\dfrac{a}{N}\right) = \left(\dfrac{b}{N}\right)$, *et* $\left(\dfrac{a}{N}\right) = 0$ *ssi* $a \wedge N > 1$

(ii) $\forall a, b \in \mathbf{Z},\ \left(\dfrac{ab}{N}\right) = \left(\dfrac{a}{N}\right)\left(\dfrac{b}{N}\right)$

(iii) $\left(\dfrac{-1}{N}\right) = (-1)^{(p-1)/2}$ *et* $\left(\dfrac{2}{N}\right) = (-1)^{(p^2-1)/8}$

Application (Dirichlet faible)*.* Cf Perrin !

Théorème 6 (Loi de réciprocité quadratique)**.** *Soient* N, M *des nombres impairs distincts. Alors on a :*

$$\left(\frac{N}{M}\right)\left(\frac{M}{N}\right) = (-1)^{\frac{N-1}{2}\frac{M-1}{2}}$$

Ce théorème associé aux propositions précédentes fournit un algorithme rapide de calcul du symbole de Legendre : on est ramené à un algorithme d'Euclide.

Exemple (Hindry p.10)*.* Soit p un nombre premier s'écrivant $p = x^2 - 6y^2$, avec $x, y \in \mathbf{Z}$. Alors p ne divise pas y, car sinon p diviserait aussi x et donc p^2 diviserait p. Donc $6 \equiv (xy^{-1})^2\ [p]$, donc $\left(\dfrac{6}{p}\right) = 1$ i.e. $(-1)^{(p^2-1)/8}(-1)^{(p-1)/2}\left(\dfrac{p}{3}\right) = 1$, on en déduit des congruences de p modulo 24.

Théorème 7 (Frobénuis-Zolotarev)**.** *Soit* p *un nombre premier impair et* V *un* $\mathbb{F}_p$*-e.v. de dimension finie. Alors pour tout* $u \in Gl(V)$, *on peut considérer* u *comme un élément de* $\mathfrak{S}(V)$, *si bien qu'on peut lui associer sa signature. On a alors* $\varepsilon(u) = \left(\frac{det(u)}{p}\right)$.

Théorème 8 (Deux carrés)**.** *Un entier* $n \geq 2$ *, dont la décomposition en facteurs premiers s'écrit* $\prod_{p \in \mathcal{P}} p^{v_p(n)}$, *est la somme de deux carrés entiers ssi pour tout* $p \equiv 3\ [4]$, $v_p(n)$ *est pair.*

5 Algorithme RSA et tests de primalité

On se donne deux grands nombres premiers p et q tels que $n = pq$, et un entier d inversible modulo $\varphi(n)$, appelé *clef publique*. Le chiffrement d'un message $a \in \mathbf{Z}/n\mathbf{Z}$ est donné par la fonction $f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z},\ a \mapsto a^d$, et le déchiffrement par l'inverse de f : $g : a \mapsto a^e$, avec e un inverse de d dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$, appelé *clef privée*. La robustesse de cet algorithme réside dans le fait que le calcul de g, i.e. celui de e, nécessite la connaissance de $\varphi(n)$, et donc de p et de q. Or la factorisation de nombres tels que n est en pratique extrèmement longue : le calcul de l'inverse est impossible en temps raisonnable. Reste à savoir comment fabriquer de tels grands nombres premiers p et q.

Théorème 9 (Wilson)**.** *n est premier ssi $(n-1)! \equiv -1\ [n]$.*

Théorème 10 (Fermat-Euler)**.** *Soit $a \in \mathbf{Z}$, $a \wedge n = 1$. Alors $a^{\varphi(n)} \equiv 1\ [n]$.*

Remarque. Si n est premier, alors $a^{n-1} \equiv n\ [n]$.

Définition 4. n est dit de *Carmichael* si $\forall a \in \mathbf{Z} : a \wedge n = 1,\ a^{n-1} \equiv a\ [n]$.

Exemple. 561 est un nombre de Carmichael

Proposition 13. *n est de Carmichael ssi $\forall a \in \mathbf{Z}, a^n \equiv a\ [n]$ ssi n est sans facteur carré et pour tout diviseur premier p de n, $p - 1 | n - 1$.*

Lemme 2. *Soit $H = \{a \in (\mathbf{Z}/n\mathbf{Z})^* / a^{(n-1)/2} \equiv \left(\frac{a}{n}\right)\ [n]\}$. Alors n est premier ssi $H = (\mathbf{Z}/n\mathbf{Z})^*$.*

Le test de Solovay-Stassen consiste alors à tester l'égalité du lemme pour des nombres aléatoires. Si n passe successivement k tests, on peut dire qu'il est premier avec une probabilité supérieure à $1 - 2^{-k}$.

Algorithme ρ de Pollard

C'est un algorithme probabiliste déteminant une décomposition en facteurs premiers d'un entier N. On se donne une fonction $f : \mathbf{Z}/N\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$ "aléatoire" (on choisit souvent $f(x) = x^2 + 1 \bmod n$) et un élément $x_0 \in \mathbf{Z}/N\mathbf{Z}$. On considère alos la suite récurrente définie par $x_{n+1} = f(x_n)$. Un raisonnement semblable à celui du paradoxe des anniversaires montre alors qu'on a de grandes chances pour qu'il existe n assez petit (de l'ordre de $\sqrt[4]{N}$) tel que $x_n - x_{2n} \wedge N$ soit non trivial. On a alors trouvé un facteur premier de N.

Vaseux ?

Développements

- Réciprocité quadratique (Hindry) + ? ?
- Tests de primalité
- Carmichael (Demazure)