Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

I Definitions. Generalités

Definition : congruence

pour $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$, $a \equiv b[n] \Leftrightarrow (b-a) \in n\mathbb{Z}$

Puisque $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ définit un anneau commutatif, avec $a \to \bar{a}$ la surjection canonique

on a $a \equiv b[n]$ ssi $\bar{a} = \bar{b}$ dans $\mathbb{Z}/n\mathbb{Z}$

Definition : PGCD, PPCM

on note $n \wedge m$ le générateur >0 de $n\mathbb{Z} + m\mathbb{Z}$

$n \vee m$ le générateur >0 de $n\mathbb{Z} \cap m\mathbb{Z}$

on a $(n \wedge m)(n \vee m) = nm$

$n \wedge m = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} / nu + mv = 1$ (BEZOUT)

Premières propriétés

1) $\mathrm{Car}(\mathbb{Z}/n\mathbb{Z}) = \#\,\mathbb{Z}/n\mathbb{Z} = n$
2) $\bar{p}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow p \wedge n = 1$
3) $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ premier

Prop

$(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique

Réciproquement, un groupe cyclique d'ordre n est $\simeq \mathbb{Z}/n\mathbb{Z}$

Exemple : $\mathbb{U}_n = \{z \in \mathbb{C} / z^n = 1\}$ les racines n-ièmes de l'unité

on a $\mathbb{U}_n = \mathbb{Z}/n\mathbb{Z}$

Definition : Indicatrice d'Euler

$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

remarque : on a aussi $\varphi(n) = \#\{\text{générateurs de } (\mathbb{Z}/n\mathbb{Z}, +)\}$

Théorème Chinois

si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où (p_i) premiers distincts

alors $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$

Application ① résolution de systèmes de congruence

ex : $\begin{cases} a \equiv 3[4] \\ a \equiv 5[9] \end{cases}$ a pour solutions $\{23 + 36k, k \in \mathbb{Z}\}$

Application ② Calcul de φ

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Théorème de Fermat

$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{\varphi(n)} = 1$ dans $\mathbb{Z}/n\mathbb{Z}$

Théorème de Wilson

$n \geq 2$. n est premier $\Leftrightarrow (n-1)! \equiv -1[n]$

II Théorèmes de structure

1) les automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Prop

on a un isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

en particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien, d'ordre $\varphi(n)$

Théo

Tout sous groupe fini du groupe multiplicatif d'un corps est cyclique

Conséquence

si n est premier, $(\mathbb{Z}/n\mathbb{Z})^* \simeq \mathbb{Z}/(n-1)\mathbb{Z}$

On sait en fait classifier $(\mathbb{Z}/n\mathbb{Z})^*$ $\forall n \in \mathbb{Z}$:

Prop

si $\alpha \geq 2$ • $\forall p$ premier ≥ 3, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$

• $p = 2$ $\quad (\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

et par le théorème chinois, on a

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

le groupe diédral

Soit D_n le groupe des isométries du plan préservant un polygône régulier à n côtés.

Alors : $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

III Cyclotomie

Définition : polynômes cyclotomiques

- $\xi \in \mathbb{C}$ est racine primitive n-ième de l'unité si ξ engendre U_n
- $\Phi_n(X) = \prod_{\substack{\xi \in U_n \\ \xi \text{ primitive}}} (X - \xi)$ pour $n \geq 1$

Propriétés

i) $\deg \Phi_n = \varphi(n)$

ii) $\prod_{d|n} \Phi_d(X) = X^n - 1$

iii) $\Phi_n \in \mathbb{Z}[X]$.

Corollaire

$$\sum_{d|n} \varphi(d) = n$$

Théorème : WEDDERBURN

Tout anneau à division fini est un corps

Théorème :

Φ_n est irréductible dans $\mathbb{Z}[X]$

Corollaire :

Φ_n est le polynôme minimal de ξ, $\forall \xi$ racine primitive n-ème et $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n) = [\mathbb{Q}(\xi) : \mathbb{Q}]$

IV Arithmétique

1) fonction de Möbius

Définition

$n \in \mathbb{N}^*$. $\mu(n) = \begin{cases} 0 \text{ si } n \text{ a un facteur carré} \\ (-1)^k \text{ si } n = p_1 \dots p_k, \ p_i \text{ premiers distincts} \end{cases}$

Prop

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

μ est multiplicative

Théo : Formule d'inversion de Möbius

$h, H : \mathbb{N}^* \to G$ groupe abélien. Alors

$\forall n \in \mathbb{N}, \ H(n) = \sum_{d|n} h(d) \iff \forall n \in \mathbb{N}, \ h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d)$

Application

- Compter les polynômes irréductibles unitaires de degré n dans $(\mathbb{Z}/p\mathbb{Z})[X]$
- $\varphi(n) = \sum_{d|n} d\,\mu\left(\frac{n}{d}\right)$

2) Résidus quadratiques

Définition : symbole de Legendre

Si p premier, $n \in \mathbb{Z}$, on note

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } \bar{n} = 0 \\ 1 & \text{si } \bar{n} \neq 0 \text{ et } \bar{n} \text{ est un carré de } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{si } \bar{n} \neq 0 \text{ et } \bar{n} \text{ n'est pas un carré de } \mathbb{Z}/p\mathbb{Z} \end{cases}$$

Prop : Formule d'Euler

p premier impair. Alors la moitié des $(p-1)$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont des carrés, et

$$\forall n, \ \left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \ [p]$$

Corollaire

(-1) carré dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p \equiv 1[4]$

(Application: théorème des 2 carrés)

Corollaire 2

$n \to \left(\frac{n}{p}\right)$ est multiplicative: $\forall n,m \in \mathbb{Z}\ \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right) = \left(\frac{nn'}{p}\right)$

Loi de réciprocité quadratique

si p et q sont premiers, $p \neq q$, on a

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) \text{ si } p \text{ ou } q \equiv 1[4] \\ -\left(\frac{p}{q}\right) \text{ sinon} \end{cases}$$

V Applications

1) Cryptographie

Codage RSA

A et B désirent communiquer secrètement

B choisit p et q premiers distincts. Il calcule $N = pq$ et $\varphi(N) = (p-1)(q-1)$

e tel que $e \wedge \varphi(N)$, d tel que $ed + \varphi(N)u = 1$

On définit la fonction de codage

$$C : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$M \to M^e$$

Alors $C^{-1} = (M \to M^d)$

B donne N, e à A mais garde la clef de décodage "d"

Personne ne sait factoriser N, qui est pris très grand!

exemple: $n = 11 \times 211 = 2321$, $\varphi(n) = 2100$

On choisit $e = 143$. (En effet $143 \times (-793) + 54 \times 2100 = 1$)

$C(x) = x^{143}[2321]$

$C^{-1}(x) = x^{-793}[2321]$

exemple: $301^{143} = 1472[2321]$, $1472^{-793} = 301[231]$

2) Structure des groupes abéliens de type fini G

Théo: $\forall G$, $\exists p \in \mathbb{N}$, $(a_1, \dots a_r) \in \mathbb{N}^r$ / $a_i \geq 2$ et $a_i | a_{i+1}$ tq $G \simeq \mathbb{Z}^p \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/a_i\mathbb{Z}$. les a_i sont uniques

3) Irréductibilité des polynômes dans $\mathbb{Z}[X]$

- Critère d'Eisenstein

Q unitaire de $\mathbb{Z}[X]$, $Q = X^n + a_{n-1}X^{n-1} + \dots + a_0$, p premier

si • $p | a_i$ $\forall i \leq n-1$

• $p^2 \nmid a_0$

Alors: Q est irréductible dans $\mathbb{Q}[X]$ (donc dans $\mathbb{Z}[X]$)

- Théorème de réduction

Q polynôme de $\mathbb{Z}[X]$, $Q = a_n X^n + \dots + a_0$, p premier

si • $p \nmid a_n$

• $\overline{P} = \overline{a_n} X^n + \dots + \overline{a_0}$ irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$

Alors: P est irréductible dans $\mathbb{Z}[X]$

⚠ La condition n'est pas nécessaire

$P = X^4 + 1$ est réductible dans $\mathbb{Z}/p\mathbb{Z}$ $\forall p$ premier ($P = \Phi_8$)

irréductible dans $\mathbb{Z}$

REFERENCES

Perrin, Demazure, Tauvel

Saux-Picart (juste pour RSA)