Leçon 109 : Anneaux $\mathbb{Z}/n\mathbb{Z}$ - Applications

I Structure

1) L'anneau $\mathbb{Z}/n\mathbb{Z}$

[GOU p.7] **Déf 1** (Congruence modulo n) On note $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Pour $x, y \in \mathbb{Z}$, on dit que x et y sont congrus modulo n et on note $x \equiv y \pmod n$ si $x - y \in n\mathbb{Z}$.

[GOU p.18] **Déf 2** : • $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ et $n\mathbb{Z} \triangleleft \mathbb{Z}$ donc on peut définir le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$.

[GOU p.7] • $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$ donc on peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

Prop 3 :
1) [GOU p.7] $|\mathbb{Z}/n\mathbb{Z}| = n$
2) [GOU p.31] $\bar{k}$ inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ ssi $k \wedge n = 1$
3) [GOU p.20] $\bar{k}$ générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ ssi $k \wedge n = 1$
4) [GOU p. 9] $\mathbb{Z}/n\mathbb{Z}$ intègre ssi $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n premier

[GOU p.19] **Prop 4** : • $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique
• Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

[GOU p.31] **Déf 5** : (Indicatrice d'Euler) $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

[GOU p.31] **Rem 6** : $\varphi(n)$ est le nombre d'entiers $k \leq n$ tq. $k \wedge n = 1$

[GOU p.31] **Thm 7** : (Théorème chinois) Soient $n, m \in \mathbb{Z}$. Alors $n \wedge m = 1 \iff \mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Application 8 : Résolution d'un système de congruence [GOU p.31]
$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod 9 \end{cases}$ a pour solutions $\{23 + 36k, k \in \mathbb{Z}\}$

Application 9 : Calcul de $\varphi(n)$: si $n \geq 2$, [GOU p.31]
$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Longrightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.

Application 10 : Calcul des idempotents de $\mathbb{Z}/n\mathbb{Z}$ [Réf ?]
Si p est premier, les seuls idempotents de l'anneau $\mathbb{Z}/p^\alpha\mathbb{Z}$, avec $\alpha \in \mathbb{N}^*$, sont $\bar{0}$ et $\bar{1}$.

2) Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ [PER p.24-27]

Prop 11 : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Lemme 12 : Si p est un nombre premier, on a un isomorphisme $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Rem 13 : On peut voir le lemme 12 comme un cas particulier du fait que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Prop 14 : • Si p premier ≥ 3 et α entier ≥ 2 on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$
• Si $\alpha \geq 3$, alors on a : $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

Application 15 : Détermination des groupes d'ordre pq pour p, q premiers et $p < q$.

3) Structure des groupes abéliens finis

Thm 16 : Soit G un groupe abélien fini d'ordre $n \geq 2$ [COM p. 66]

12

Il existe des entiers $q_i \geq 2$, uniques, tels que $q_1 | \cdots | q_k$ et vérifiant :
$$G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}.$$

II Polynômes dans $\mathbb{Z}[X]$

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

[GOU p.58] **Thm 17** : (Critère d'Eisenstein)
Soit $P = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$.
On suppose qu'il existe un nombre premier p tel que :
i) $p | a_k \ \forall\, 0 \leq k \leq n-1$
ii) $p \nmid a_n$
iii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$ (et dans $\mathbb{Z}[X]$ pourvu que $\mathrm{pgcd}(a_i) = 1$).

[PER p.77] **Application 18** : Soit p premier. Alors le polynôme $X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Z}[X]$.

[PER p.77] **Thm 19** : (Réduction) Soit $P = a_nX^n + \cdots + a_0$ dans $\mathbb{Z}[X]$ et $\overline{P}$ sa réduction dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier. On suppose que $\overline{a_n} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$ (i.e. $p \nmid a_n$). Alors si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, le polynôme P est irréductible dans $\mathbb{Q}[X]$ (et dans $\mathbb{Z}[X]$ pourvu que $\mathrm{pgcd}(a_i) = 1$)

[PER p.77] **Application 20** : $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ (réduction modulo 2)

2) Polynômes cyclotomiques

[GOU p.91] **Rem 21** : $U_n = \{$racines n-ièmes de l'unité$\}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Def 22 : $P_n = \{$racines primitives n-ièmes de $1\}$
On définit le polynôme cyclotomique d'indice n par $\Phi_n(X) = \prod_{\xi \in P_n} (X - \xi)$.

Prop 23 : 1) $\deg(\Phi_n) = \varphi(n)$
2) $X^n - 1 = \prod_{d|n} \Phi_d(X)$
3) $\Phi_n \in \mathbb{Z}[X]$.

$\boxed{\textbf{Thm 24} : \Phi_n \text{ est irréductible dans } \mathbb{Z}[X].}$ DEV 1

III Arithmétique

1) Nombres premiers

Thm 25 : (Fermat) Soit p premier : pour tout $x \in \mathbb{Z}$, on a $x^p \equiv x \pmod p$. [COM p.265]

Application 26 : Test de primalité : sur un ordinateur, vérifier que $x^{p-1} - 1$ est divisible par p n'est pas difficile, même pour p grand. [COM p.265]

Thm 27 (Wilson) : $p \geq 2$ est un nombre premier ssi $(p-1)! \equiv -1 \pmod p$. [COM p.265]

Thm 28 (Euler) : Soit $n \geq 2$ entier. $\forall k \in \mathbb{Z}$ tq. $k \wedge n = 1$, on a $k^{\varphi(n)} \equiv 1 \pmod n$ [COM p.265]

[XENS1 p.135]

DEV 2

Thm 29 (Dirichlet Faible) Soit $n \geq 1$ entier. Il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod n$.

2) Résidus quadratiques

[RB p.138]

Déf 30 (Symbole de Legendre) Soit p premier impair et $x \in \mathbb{Z}$ non divisible par p. On pose $\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{si } x \text{ n'est pas un carré dans } \mathbb{Z}/p\mathbb{Z} \end{cases}$

[TAU p.328]

Prop 31 : Soit p premier impair et $x \in \mathbb{Z}$. Alors $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

[PER p.75]

Cor 32 : Soit p premier ≥ 3. Alors (-1) est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p \equiv 1 \pmod 4$.

[PER p.57]

Application 33 : (Théorème des deux carrés) Soit p premier : p est la somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \pmod 4$

[RB p.138]

Prop 34 : L'application $x \mapsto \left(\frac{x}{p}\right)$ est multiplicative : $\forall x, x' \in \mathbb{Z}$, $\left(\frac{x}{p}\right)\left(\frac{x'}{p}\right) = \left(\frac{xx'}{p}\right)$.

[RB p.139]

Thm 35 : (Loi de réciprocité quadratique) Si p, q premiers impairs, $p \neq q$, on a :
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

Ex 36 : 15 est un carré modulo 17.

3) Equations diophantiennes

[COM p.273-275]

Déf 37 : On appelle équation diophantienne, une équation $P(X,Y,Z) = 0$ où les inconnues X, Y, Z sont des entiers et où P est un polynôme à plusieurs variables à coefficients entiers.

Prop 38 : $(x, y, z) \in \mathbb{N}^3$ est solution de l'équation de Diophante $x^2 + y^2 = z^2$ ssi $\exists d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2 - v^2), 2duv, d(u^2+v^2))$

Application 39 : L'équation $x^4 + y^4 = z^2$ (Fermat) n'a pas de solution non triviale.

[XENS1 p.167]

DEV 3

Thm 40 (Sophie Germain) Soit p premier impair tel que $q = 2p+1$ est premier. Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ t.q $\begin{cases} xyz \not\equiv 0 \pmod p \\ x^p + y^p + z^p = 0 \end{cases}$

4) Cryptographie

[GOU p.34] ou [DEM p.63-6]

Système RSA.

Références :

- [GOU] : Gourdon, Algèbre
- [PER] : Perrin, Cours d'algèbre
- [COM] : Combes, Algèbre et géométrie
- [RB] : Risler-Boyer, Algèbre pour la licence 3 } pour les résidus quadratiques
- [TAU] : Tauvel, Algèbre } ([RB] utilise des notations + familières)
- [XENS1] : Oraux X-ENS Algèbre 1 (pour DEV 2 et DEV 3)
- ([DEM] : Demazure, Cours d'algèbre) ← pour une vision plus algorithmique

Autres développements possibles

- Groupes d'ordre pq
- Théorème des deux carrés
- Loi de réciprocité quadratique
- Frobenius-Zolotarev
- Automorphismes de $(\mathbb{Z}/p^\alpha\mathbb{Z})$