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

Cadre : Sauf indication contraire, $m, n \in \mathbb{N}^*$, $p, q \in \mathcal{P}$, où $\mathcal{P}$ est l'ensemble des nombres premiers.

I – Structure de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$

1 – Le groupe $\frac{\mathbb{Z}}{m\mathbb{Z}}$

Déf 1 : Le groupe $\frac{\mathbb{Z}}{m\mathbb{Z}}$ (également noté $\mathbb{Z}/m\mathbb{Z}$) est défini par le quotient du groupe additif $\mathbb{Z}$ par le sous-groupe $m\mathbb{Z}$.
La loi de groupe est donc donnée par :

$$(k + m\mathbb{Z}) + (k' + m\mathbb{Z}) = (k+k') + m\mathbb{Z}$$

Déf 2 : On note $\overline{k} = k + m\mathbb{Z}$, ou encore $[k]^m = k + m\mathbb{Z}$, c'est la classe de k modulo m, on a en pratique $k \in [\![0, m-1]\!]$, mais $k \in \mathbb{Z}$.

Ex 3 : Dans $\frac{\mathbb{Z}}{4\mathbb{Z}}$, $1 + 4\mathbb{Z} + 3 + 4\mathbb{Z} = 4 + 4\mathbb{Z} = 4\mathbb{Z} = [0]^4$

Prop 4 : $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est de cardinal m.

Prop 5 : Soit G un groupe cyclique de cardinal m. $G = \langle g \rangle$, $o(g) = m$.
On a alors cet isomorphisme de groupe :

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \xrightarrow{\sim} G$$
$$\overline{k} \longmapsto g^k$$

Ex 6 : Soit $\mathbb{U}_m$ l'ensemble des racines m-ièmes de l'unité.
Alors $\frac{\mathbb{Z}}{m\mathbb{Z}} \xrightarrow{\sim} \mathbb{U}_m$, $\overline{k} \longmapsto e^{\frac{2ik\pi}{m}}$ est un isomorphisme de groupes.

Prop 7 : $k \in [\![0, m]\!]$ est un générateur du groupe $\frac{\mathbb{Z}}{m\mathbb{Z}} \iff k \wedge m = 1$

Cor 8 : $\frac{\mathbb{Z}}{m\mathbb{Z}}$ possède $\varphi(m)$ générateurs, où φ est l'indicatrice d'Euler.

Prop 9 : Les sous-groupes de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $\frac{d\mathbb{Z}}{m\mathbb{Z}}$, où $d \mid m$.

Prop 10 : $\frac{d\mathbb{Z}}{m\mathbb{Z}} \simeq \frac{\mathbb{Z}}{\left(\frac{m}{d}\right)\mathbb{Z}}$

Ex 11 : Les sous-groupes de $\frac{\mathbb{Z}}{4\mathbb{Z}}$ sont $\{\overline{0}\}$, $\frac{\mathbb{Z}}{2\mathbb{Z}}$ et $\frac{\mathbb{Z}}{4\mathbb{Z}}$

Lemme 12 (Lemme chinois)
Si $m \wedge n = 1$, on a cet isomorphisme de groupe

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$
$$[x]^{mn} \longmapsto ([x]^m, [x]^n)$$

Th 13 : (Théorème de structure)
Soit G un groupe abélien fini.
Alors $\exists!\, d_1 \mid \dots \mid d_n \in \mathbb{N}$, $G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_n\mathbb{Z}}$

Ex 14 : Si G est abélien d'ordre 36, alors $G \simeq \frac{\mathbb{Z}}{36\mathbb{Z}}$, $G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{18\mathbb{Z}}$
ou $G \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{12\mathbb{Z}}$ ou $G \simeq \left(\frac{\mathbb{Z}}{6\mathbb{Z}}\right)^2$

2 – Anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$, congruences.

Déf 15 : L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est défini comme étant le quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$. On dit que $a \equiv b\ [n]$ si $\overline{a} = \overline{b}$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Prop 16 : $\overline{k} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \iff k \wedge n = 1$, $k \in [\![0, n-1]\!]$

Rq 17 : $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est le groupe des inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Cor 18 : $\left|\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times\right| = \varphi(n)$

Th 19 : Pour $k \in \mathbb{Z}$, $\overline{k} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times \iff \left(\frac{\mathbb{Z}}{m\mathbb{Z}}, +\right) = \langle \overline{k} \rangle$
$\iff k \wedge m = 1$

Ex 20 : $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^\times = \{\overline{1}, \overline{3}\}$

Prop 21 : Les assertions suivantes sont équivalentes
(i) $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est intègre
(ii) m est un entier premier
(iii) $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est un corps

Déf 22 : Le corps à p éléments, noté $\mathbb{F}_p$, est défini par : $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$

Prop 23 : $\varphi(p) = p-1$, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ et $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times = \frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{\overline{0}\}$.

Prop 24 : Les idéaux maximaux de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $\frac{p\mathbb{Z}}{m\mathbb{Z}}$, où $p \mid m$ est premier.

Ex 25 : Le seul idéal maximal de $\frac{\mathbb{Z}}{4\mathbb{Z}}$ est $\frac{2\mathbb{Z}}{4\mathbb{Z}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$

Déf 26 : (Congruence)
Soient $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo m et on note $a \equiv b\ [m]$ si on a $[a]^m = [b]^m$ dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$ ou $\exists k \in \mathbb{Z}$, $a = b + mk$

Ex 27 : $7 \equiv 5\ [2]$

Prop 28 : Soient $a, a', b, b' \in \mathbb{Z}$, $k \in \mathbb{N}$ tels que $a \equiv b\ [n]$, $a' \equiv b'\ [n]$
Alors on a ces propriétés :
(i) $a + a' \equiv b + b'\ [n]$ (ii) $a^k \equiv b^k\ [n]$
(iii) $aa' \equiv bb'\ [n]$

Prop 29 : $ab \equiv 0\ [p] \implies a \equiv 0\ [p]$ ou $b \equiv 0\ [p]$

Rq 30 : $m \mid a \iff a \equiv 0\ [m]$

Appli 31 : $\forall n \in \mathbb{N}$, $15 \mid 16^n - 1$

3 - Théorème Chinois

Th 32 (Théorème chinois)

Si $m \wedge n = 1$, on a cet isomorphisme d'anneaux

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \leftarrow \text{produit direct d'anneaux}$$

$$[x]^{mn} \longmapsto ([x]^m, [x]^n)$$

Th 33 : (Théorème chinois, version plus générale)

Soient $n_1, \dots, n_r \in \mathbb{N}^*$ deux à deux premiers entre eux et soit $n = \prod_{j=1}^{r} n_j$. On a alors l'isomorphisme d'anneaux

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{n_r\mathbb{Z}}$$

$$[x]^n \longmapsto ([x]^{n_1}, \dots, [x]^{n_r})$$

Appli 34 : Résolution de systèmes de congruences

Ex 35 : L'ensemble des solutions de ce système de congruences

$$\begin{cases} x \equiv 1 \ [2] \\ x \equiv 2 \ [3] \\ x \equiv 3 \ [5] \end{cases}$$ est donné par $\{-7 + 30k, k \in \mathbb{Z}\}$

II - Résultats arithmétiques

1 - Premiers théorèmes

Th 36 (Petit théorème de Fermat)

Si $a \in \mathbb{Z}$ et $a \wedge p = 1$, i.e. $p \nmid a$, alors $a^p \equiv a \ [p]$

Cor 37 : Ce théorème fournit un test de primalité sur p :

$\exists a < p \quad a^p \not\equiv a \ [p] \implies p$ est non premier.

Rq 38 : Les entiers p ne vérifiant pas l'assertion réciproque sont appelés nombres de Carmichael

Th 39 : (Théorème d'Euler)

On peut généraliser le petit théorème de Fermat avec

$a^{\varphi(n)} \equiv 1 \ [n]$

Ex 40 : $\left(\frac{\mathbb{Z}}{10\mathbb{Z}}\right)^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ donc $\varphi(10) = 4$. Ainsi $7^4 \equiv 1 \ [10]$

Th 41 : (Théorème de Wilson)

p est premier si et seulement si $(p-1)! \equiv -1 \ [p]$

Rq 42 : Ce théorème fournit à priori un test de primalité, mais est coûteux en temps (donc en pratique inutilisable)

Th 43 : (Théorème des deux carrés de Fermat)

Si p est impair, alors p est somme de deux carrés si, et seulement si $p \equiv 1 \ [4]$

2 - Résidus quadratiques

Def 44 : (Symbole de Legendre)

Pour $a \in \mathbb{Z}$, on appelle symbole de Legendre le nombre entier, noté $\left(\frac{a}{p}\right)$, défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \ [p] \\ 1 & \text{si } \exists k \in \mathbb{Z} \quad a \equiv k^2 \ [p] \ (a \text{ est un carré modulo } p) \\ -1 & \text{sinon} \end{cases}$$

Ex 45 : $1116 \equiv 1 \ [5]$ donc $\left(\frac{1116}{5}\right) = 1$

$1115 \equiv 0 \ [5]$ donc $\left(\frac{1115}{5}\right) = 0$

Th 46 : (Critère d'Euler)

Si $a \in \mathbb{Z}$: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ [p]$, pour $p \geq 3$

Prop 47 : (i) Pour $a, b \in \mathbb{Z}$, si $a \equiv b \ [p]$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$(p \geq 3)$ (ii) Pour $a, b \in \mathbb{Z}$: $a \wedge b = 1$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Ex 48 : $\left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \equiv 2^5 \, 3^5 \ [11] \equiv -1 \ [11]$

Prop 49 : (i) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

$(p \geq 3)$ (ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Ex 50 : $\left(\frac{2}{11}\right) = (-1)^{\frac{120}{8}} = -1$: 2 n'est pas un carré modulo 11 (dans $\mathbb{F}_{11}$)

Th 51 : (Loi de réciprocité quadratique)

Si $p, q \geq 3$ sont premiers distincts, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

DVPT 1

Ex 52 : 20 n'est pas un carré modulo 13 ; en effet, on a :

$$\left(\frac{20}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right)(-1)^{\frac{13-1}{2}\frac{7-1}{2}} = \left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{8}}\left(\frac{3}{7}\right)$$

$$\left(\frac{20}{13}\right) = \left(\frac{3}{7}\right) = \left(\frac{7}{3}\right)(-1)^{\frac{3-1}{2}\frac{7-1}{2}} = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

2

2 – Réduction modulo pour résoudre des équations diophantiennes

Méthode : Soit $P \in \mathbb{Z}[X_1, \dots, X_d]$ et soit l'équation diophantienne $P(x_1, \dots, x_d) = 0$ d'inconnue $(x_1, \dots, x_d) \in \mathbb{Z}^d$. Si $\exists n \in \mathbb{N}$, $\overline{P}(\overline{x_1}, \dots, \overline{x_d}) = \overline{0}$ n'admet pas de solution, alors l'équation n'admet pas de solution dans $\mathbb{Z}$.

Rq : Cette méthode sert à démontrer que certaines équations diophantiennes n'admettent pas de solution.

Ex : (i) L'équation $x^2 + 3y = 2$ n'admet pas de solution.
En effet, modulo 3, $\overline{x}^2 = \overline{2}$ et 2 n'est pas un carré modulo 3. Donc l'équation réduite n'a pas de solution et $x^2 + 3y = 2$ n'a pas de solution.

(ii) L'équation $x^2 + y^2 = 4z + 3$ n'a pas de solution $(x, y, z) \in \mathbb{Z}^3$.
En effet, modulo 4, l'équation réduite est $x^2 + y^2 \equiv 3\ [4]$, et $3 \not\equiv 1\ [4]$ donc par le théorème des deux carrés de Fermat, l'équation réduite n'a pas de solution, ce qui conclut.

III – D'autres applications

1 – Irréductibilité

Th 50 (Réduction modulo un entier)
Soit $P \in \mathbb{Z}[X]$ unitaire et soit $p \in \mathcal{P}$ un entier premier.
Soit $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme de réduction modulo p.
Si $\varphi(P)$ est irréductible alors P l'est aussi dans $\mathbb{Z}[X]$.

Ex 51 : Soit $P = X^3 + 2X + 1$.
Réduisons modulo 3 : $\varphi(P) = X^3 - X + 1$. Si $\varphi(P)$ est réductible sur $\mathbb{F}_3[X]$, c'est qu'il admet une racine car est de degré 3, or ce n'est pas le cas. Donc $X^3 + 2X + 1$ est irréductible dans $\mathbb{Z}[X]$.

Prop 52 (Fractions irréductibles)
(i) $\forall n \in \mathbb{N}^*$, $\dfrac{3^{n+1} + 5^{n+1}}{3^n + 5^n}$ est réductible

(ii) $\forall n \in \mathbb{N}^*$, $\dfrac{7^{n+1} - 10^{n+1}}{7^n - 10^n}$ est irréductible

(iii) Soient $(\lambda, \mu, \alpha, \beta) \in \mathbb{N}^4$, $n \in \mathbb{N}^*$ et $F_n = \dfrac{\lambda \alpha^{n+1} + \mu \beta^{n+1}}{\lambda \alpha^n + \mu \beta^n}$.
F_n est irréductible ssi [illegible]

DVPT 2

2 – Cryptographie

Prop 59 (Protocole d'échange des clefs de Diffie-Hellman)
Voici le protocole permettant d'échanger les clefs :
(i) Alice et Bob ont choisi $\mathbb{F}_p$, p premier, et ont un générateur g de $\mathbb{F}_p^*$
(ii) Alice choisit a au hasard et transmet g^a à Bob
(iii) Bob choisit b au hasard et transmet g^b à Alice
(iv) Alice et Bob connaissent respectivement a et b et peuvent calculer g^{ab}, ce sera la clef secrète.
$(\mathbb{F}_p, g, g^a, g^b)$ sont connus, c'est la clef publique.

Prop 60 (Envoi d'un message crypté)
(i) Alice veut envoyer un message $m \in \mathbb{F}_p^*$ à Bob. Elle calcule $m' = m g^{ab}$ et l'envoie à Bob.
(ii) Bob connaît g^{ab} et peut calculer m grâce à $m = m'(g^{ab})^{-1}$

ab est très difficile à déterminer à partir de g, g^a, g^b de manière efficace (problème du logarithme discret), ce qui rend le décodage du message impossible.

Rq 61 : p doit être choisi assez grand pour éviter toute attaque par force brute.

M

Références :

J.-P. Serre, Cours d'Arithmétique

FGN, Oraux X-ENS, Algèbre 1

D. Perrin, Cours d'algèbre