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

Dans toute la leçon, $n \in \mathbb{N}\setminus\{0,1\}$ et p est un nombre premier.

I - L'anneau $\mathbb{Z}/n\mathbb{Z}$

A - Rappels d'arithmétique des entiers

[R] 279 **Thm 1** (division euclidienne) :

$$\forall (a,b) \in \mathbb{Z}^2,\ \exists!\, (q,r) \in \mathbb{Z}^2 : \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

[R] 279 **Def 2** : Soit $(a,b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n, et on note $a \equiv b\,[n]$, si n divise $b-a$.

[R] 280 **Prop 3** : Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $a \equiv b\,[n]$ et $c \equiv d\,[n]$.

Alors $a + c \equiv b + d\,[n]$ et $ac \equiv bd\,[n]$.

B - Construction

Lemme 4 : Tout idéal de $\mathbb{Z}$ est principal, et admet un unique générateur positif.

[R] 280 **Def 5** : Le quotient de l'anneau $(\mathbb{Z}, +, \times)$ par son idéal $n\mathbb{Z}$ est l'anneau noté $\mathbb{Z}/n\mathbb{Z}$. On note $\bar{a}$ l'image de $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Rq 6 : $\bar{a} = \bar{b} \iff a \equiv b\,[n]$

[R] 280 **Prop 7** : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, et les lois sont données par Prop 3 et Rq 6.

Ex 8 : $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{9}, \overline{64}, \overline{-7}\}$

$\bar{1} + \bar{2} = \overline{1+2} = \bar{3} = \bar{0}$, $\bar{1} \times \bar{2} = \overline{1 \times 2} = \bar{2}$

C - Structure d'anneau

Prop 9 : L'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est : [R] 283

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\}$$

L'ensemble des diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$ est :

$$D_0(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \setminus \left[(\mathbb{Z}/n\mathbb{Z})^\times \cup \{0\}\right]$$

Ex 10 : $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, $D_0(\mathbb{Z}/8\mathbb{Z}) = \{\bar{2}, \bar{4}, \bar{6}\}$

Prop 11 : Les idéaux propres de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$, $d \notin \{1, n\}$. De plus, $(d\mathbb{Z}/n\mathbb{Z}, +) \simeq (\mathbb{Z}/\frac{n}{d}\mathbb{Z}, +)$. [R] 211 281

Cor 12 : $\mathbb{Z}/n\mathbb{Z}$ est principal.

Cor 13 : L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $(\mathbb{Z}/n\mathbb{Z})^\times$

Ex 14 : Les idéaux propres de $\mathbb{Z}/6\mathbb{Z}$ sont $2\mathbb{Z}/6\mathbb{Z}$ et $3\mathbb{Z}/6\mathbb{Z}$ respectivement isomorphes à $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

Prop 15 : $\forall n, m \geq 2$, $\mathrm{Hom}_{gr}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/(n \wedge m)\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, [R] 295 282

$\mathrm{Hom}_{Ann}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \{[k \bmod n \mapsto k \bmod m]\}$ si $m \mid n$, $\emptyset$ sinon.

D - Le corps $\mathbb{Z}/p\mathbb{Z}$

Thm 16 : Les assertions suivantes sont équivalentes :

1. $\mathbb{Z}/n\mathbb{Z}$ est un corps
2. $\mathbb{Z}/n\mathbb{Z}$ est intègre
3. n est premier

Cor 17 : $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ [R] 292

Cex 18 : C'est très faux pour n non premier !

$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ n'a même pas 7 éléments !

II - Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

A - Préambule : le théorème des restes chinois

[R] 285 **Thm 19** (des restes chinois) : Soit $(a_1, \dots, a_d) \in (\mathbb{N}\setminus\{0,1\})^d$.
Les entiers $a_1, \dots, a_d$ sont deux à deux premiers si, et seulement si les anneaux $\mathbb{Z}/a_1\cdots a_d\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_d\mathbb{Z}$ sont isomorphes.

Le cas échéant, il existe $(u_1, \dots, u_d) \in \mathbb{Z}^d$ tel que $\sum_{i=1}^d u_i b_i = 1$, où $b_i = \frac{a_1 \cdots a_d}{a_i}$. L'application :

$$\bar{\varphi} : \mathbb{Z}/a_1\cdots a_d\mathbb{Z} \longrightarrow \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_d\mathbb{Z}$$

$$x \bmod a_1\cdots a_d \longmapsto (x \bmod a_1, \dots, x \bmod a_d)$$

DEV 1

est un isomorphisme d'anneaux, de réciproque :

$$\bar{\varphi}^{-1} : (x_1 \bmod a_1, \dots, x_d \bmod a_d) \longmapsto \sum_{i=1}^d x_i u_i b_i \bmod a_1 \cdots a_d$$

B - Fonction indicatrice d'Euler

[R] 283 **Def 20** : L'indicatrice d'EULER est :

$$\varphi : n \longmapsto \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{k \in [\![1,n]\!] \mid k \wedge n = 1\}$$

Ex 21 : $\varphi(8) = 4$ d'après Ex 10.

[R] 288 **Prop 22** : Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.
Pour tout $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Cor 23 : Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, alors : [R] 288

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

Ex 24 : $\varphi(90) = \varphi(3^2)\varphi(2)\varphi(5) = 3(3-1)(2-1)(5-1) = 24$

Thm 25 (d'EULER) : Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ [n]$ [R] 283

Thm 26 (de FERMAT) : Si $a \wedge p = 1$, alors $a^{p-1} \equiv 1\ [p]$. [R] 284
De manière générale, $a^p \equiv a\ [p]$.

Prop 27 : $n = \sum_{d \mid n} \varphi(d)$ [R] 284

DEV 2

Thm 28 : Si $p \geq 3$, alors $\forall \alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. [R] 292

Thm 29 [admis] : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si $n \in \{2, 4, p^\alpha, 2p^\alpha\}$ avec $p \geq 3$ (premier) et $\alpha \geq 1$. [R] 294

III - Applications

A - Résolution de systèmes de congruence

Thm 30 : L'équation $ax \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$ admet des solutions si, et seulement si $a \wedge n \mid b$. Le cas échéant, [R] 290

$$S(ax \equiv b\ [n]) = \frac{b}{a \wedge n} x_0 + \frac{n}{a \wedge n}\mathbb{Z},$$ où x_0 est une solution particulière de l'équation.

Rq 31 : Le théorème des restes chinois permet de résoudre des systèmes de congruences.

[R] 291 **Ex 32 :** $S\left(\begin{cases} x \equiv 2 & [4] \\ x \equiv 3 & [5] \\ x \equiv 1 & [9] \end{cases}\right) = 118 + 180\mathbb{Z}$ **DEV 1**

[R] 291 **Rq 33 :** $S\left(\begin{cases} x \equiv x_1 & [a_1] \\ x \equiv x_2 & [a_2] \end{cases}\right) = \begin{cases} \emptyset \text{ si } a_1 \wedge a_2 \nmid x_1 - x_2 \\ x_0 + (a_1 \vee a_2)\mathbb{Z} \text{ sinon} \end{cases}$ (x_0 solution particulière)

B - Carrés de $\mathbb{Z}/p\mathbb{Z}$

Soit $c : \bar{x} \in \mathbb{Z}/p\mathbb{Z} \longmapsto \bar{x}^2$. On s'intéresse à $\mathrm{Im}(c)$.

Prop 34 : Tous les éléments de $\mathbb{Z}/2\mathbb{Z}$ sont des carrés

On supposera désormais $p \geq 3$.

[R] 426 **Prop 35 :** Soit $\ell : \bar{x} \in \mathbb{Z}/p\mathbb{Z} \longmapsto \bar{x}^{\frac{p-1}{2}}$.

- $\forall \bar{x} \in \mathbb{Z}/p\mathbb{Z}$, $c \circ \ell(\bar{x}) = \ell \circ c(\bar{x}) = \bar{1}$
- $\mathrm{Ker}(c) = \mathrm{Im}(\ell) = \{\pm\bar{1}\}$ et $\mathrm{Im}(c) = \mathrm{Ker}(\ell)$

Cor 36 : Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

[R] 325 **Thm 37** (de Wilson) : n est premier $\Leftrightarrow (n-1)! \equiv -1 \ [n]$

[P] 75 **Prop 38 :** -1 est un carré modulo p si, et seulement si $p \equiv 1 \ [4]$. Le cas échéant $-1 \equiv \left(2 \times 3 \times \cdots \times \frac{p-1}{2}\right)^2 \ [p]$.

[P] 56 **Thm 39** (des deux carrés de Fermat) : p s'écrit comme somme de deux carrés d'entiers si, et seulement si $p = 2$ ou $p \equiv 1 \ [4]$.

C - Algorithme de chiffrement RSA [G] 37

Alice veut envoyer à Bob un message représenté par un nombre entier m, en toute sécurité.

- Bob choisit en secret deux nombres premiers distincts p et q et calcule leur produit $n = pq$.
- Il choisit ensuite un entier $c < \varphi(n) = (p-1)(q-1)$ premier à $\varphi(n)$.
- Il trouve ensuite un entier d tel que $cd \equiv 1 \ [\varphi(n)]$
- La clé publique de Bob est (n, c), qu'il donne à Alice, et sa clé privée est (n, d), qu'il garde secrète.
- Alice envoie à Bob le message $m^c \bmod n$
- Pour décoder le message, Bob calcule $(m^c)^d \equiv m \ [n]$.

RÉFÉRENCES

[R] : Mathématiques pour l'agrégation – Algèbre et géométrie (Jean-Étienne Rombaldi) [2e édition]

[P] : Cours d'algèbre (Daniel Perrin)

[G] : Les maths en tête – Algèbre et probabilités (Xavier Gourdon) [3e édition]