120

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

I – Le groupe additif $\mathbb{Z}/n\mathbb{Z}$

1) Définition et résultats algébriques

Prop 1: La relation de congruence modulo $n \in \mathbb{N}^*$ est une relation d'équivalence dans $\mathbb{Z}$. On peut alors partitionner $\mathbb{Z}$ en classes d'équivalence : $\forall k \in [\![0;n-1]\!]$, $\overline{k}^{[n]} = \{x \in \mathbb{Z} / x \equiv k[n]\}$.

Déf 2: $\mathbb{Z}/n\mathbb{Z} = \{\overline{k}^{[n]} / k \in [\![0;n-1]\!]\}$

Prop 3: L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la loi $+$: $\forall (k,l) \in [\![0;n-1]\!]^2$, $\overline{k}+\overline{l} = \overline{k+l}$ est un groupe.

Rq 4: Cette opération est toujours définie modulo n. Par exemple, $\overline{6}^{[4]} = \overline{2}^{[4]}$. Donc dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{3}+\overline{3} = \overline{2}$.

Prop 5: Si $n \in \mathbb{N}^*$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique et abélien.

Lemme 6: Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z} = \langle \overline{k}^{[n]} \rangle) \iff (k \wedge n = 1)$.

Ex 7: $\overline{2}$ engendre $\mathbb{Z}/15\mathbb{Z}$, mais pas $\overline{5}$.

Prop 8: Soient $n \in \mathbb{N}^*$ et $d \in [\![0;n-1]\!]$ tel que $d|n$. Alors il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Ce groupe est engendré par $\overline{n/d}$.

2) Groupes isomorphes et classification

Lemme 9: Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$. $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Théorème 10: Soit G un groupe abélien fini. Alors il existe une famille $(d_i)_{1 \leq i \leq r}$ de $\mathbb{N}^*$ telle que $\forall i \in [\![1;r-1]\!]$, $d_i | d_{i+1}$ et $G \simeq \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$.

Théorème 11: Soit G un groupe abélien de type fini (ie : engendré par une famille finie). Alors $\exists l \in \mathbb{N}^*$ et (d_i) comme celle du résultat précédent, tels que : $G \simeq \mathbb{Z}^l \times \left(\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}\right)$.

II – L'anneau $\mathbb{Z}/n\mathbb{Z}$

1) Notions algébriques

Prop 12: Muni de la multiplication : $\overline{k} \times \overline{l} = \overline{kl}$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau.

Prop 13: $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \iff k \wedge n = 1$.

Rq 14: Cela découle du théorème de Bézout : $a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2$, $au+bv = 1$.

Théorème 15: Soit $n \geq 2$, il y a équivalence entre : (i) $\mathbb{Z}/n\mathbb{Z}$ est un corps (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre (iii) $n \in \mathbb{P}$.
Dans ce cas, si $p \in \mathbb{P}$, $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$.

Prop 16: Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, où $d|n$. Avec : $d\mathbb{Z}/n\mathbb{Z} = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} / d|k\}$. (et $\{0\}$).

Ex 17: $2\mathbb{Z}/6\mathbb{Z} = \{\overline{0};\overline{2};\overline{4}\}$ est un idéal de $\mathbb{Z}/6\mathbb{Z}$.

Prop 18: Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $p\mathbb{Z}/n\mathbb{Z}$ où $p \in \mathbb{P}$ et $p|n$.

2) Théorème chinois et isomorphismes

Déf 19: On définit l'indicatrice d'Euler φ par : $\forall n \in \mathbb{N}^*$, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \#\{k \in [\![1;n-1]\!] / k \wedge n = 1\}$.

Théorème 20: Soit $n \in \mathbb{N}^*$. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, donc $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien de cardinal $\varphi(n)$.

Théorème 21 (chinois): Soit $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \wedge n = 1$.

Alors : $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (morphisme d'anneau).

App 22 : Résolution de systèmes de congruences (S) $\begin{cases} x \equiv a[n_1] \\ x \equiv b[n_2] \end{cases}$, où $n_1 \wedge n_2 = 1$.

Par Bézout, $\exists (u,v) \in \mathbb{Z}^2$, $n_1 u + n_2 v = 1$. Alors $\begin{cases} n_1 u \equiv 0[n_1] \\ n_1 u \equiv 1[n_2] \end{cases}$ et : $\begin{cases} n_2 v \equiv 1[n_1] \\ n_2 v \equiv 0[n_2] \end{cases}$ Donc $x \equiv bn_1 u + an_2 v [n_1 n_2]$ vérifie le système.

Mieux, par le théorème chinois : (S) $\Leftrightarrow x \equiv bn_1 u + an_2 v [n_1 n_2]$.

Ex 23 : $\begin{cases} x \equiv 3[7] \\ x \equiv 2[11] \end{cases} \Leftrightarrow x \equiv 24[77]$.

Théorème 24 (généralisation du théorème chinois) : Soit $n \geq 2$ et $n = \prod_{i=1}^r p_i^{\alpha_i}$ sa DPFP. Alors (i) $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ (anneaux)

(ii) $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ (groupes).

Lemme 25 : (1) Soient $p \in \mathbb{P}\setminus\{2\}$ et $\alpha \in \mathbb{N}^*$: $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}$

(2) Cas $p=2$: $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$; $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$;
$\forall k \geq 3$, $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.

Théorème 26 : Soit $p \in \mathbb{P}$. $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Théorème 27 : Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique $\Leftrightarrow$ $n = 1, 2, 4$ ou $n = p^\alpha, 2p^\alpha$ avec $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$. DEV1

3) Calculs avec l'indicatrice d'Euler

Prop 28 : Si $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha(1-\frac{1}{p})$.

Prop 29 : Si $(m,n) \in (\mathbb{N}^*)^2$ avec $m \wedge n = 1$, alors : $\varphi(mn) = \varphi(m)\varphi(n)$.

Corollaire 30 : Si $n \geq 2$ avec $n = \prod_{i=1}^r p_i^{\alpha_i}$ sa DPFP. Alors :
$\varphi(n) = n \prod_{i=1}^r (1 - \frac{1}{p_i})$.

Prop 31 : Si $n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.

Prop 32 : Si $n \in \mathbb{N}^*$, $\varphi(n) = \sum_{d|n} \mu(\frac{n}{d}) d$, où μ est la fonction de Möbius $\mu : n \mapsto \begin{cases} 1 \text{ si } n=1 \\ 0 \text{ si } n \text{ admet un facteur carré} \\ (-1)^r \text{ si } n = \prod_{i=1}^r p_i. \end{cases}$

III - Nombres premiers et arithmétique

1) Théorème de Fermat et nombres de Carmichael

Théorème 33 (Fermat) : Soient $p \in \mathbb{P}$ et $a \in \mathbb{N}$. Alors $a^p \equiv a[p]$.
Et si $p \nmid a$, $a^{p-1} \equiv 1[p]$.

Prop 34 (test de primalité de Fermat) : (1) S'il existe $a \in \mathbb{N}$ tel que $a^n \not\equiv a[n]$, alors $n \notin \mathbb{P}$.

(2) Si $\forall a \in \mathbb{N}$, $a^n \equiv a[n]$, il y a "de grandes chances" pour que n soit premier.

Déf 35 : Un nombre $n \geq 2$ est dit de Carmichael si $n \notin \mathbb{P}$ et $\forall a \in \mathbb{N}$, $a^n \equiv a[n]$.

Ex 36 : 561 est le plus petit nombre de Carmichael.

Théorème 37 (Korselt) : Soit $n \geq 2$. Il y a équivalence entre :
(i) n est de Carmichael (ii) n est sans facteur carré et si $p | n$ avec $p \in \mathbb{P}$, alors $p-1 | n-1$.

Prop 38 : Si $n \in \mathbb{N}^*$ est de Carmichael, il est impair et composé d'au moins trois facteurs premiers.

Ex 39 : $561 = 3 \times 11 \times 17$. Et on a bien : $16 | 560$, $2 | 560$ et $10 | 560$.

2) Equations diophantiennes

Théorème 40 : Soit $n \in \mathbb{N}^*$. Alors il existe $q \in \mathbb{P}$ tel que pour tout entier $p \in \mathbb{P}$ avec $p \geq q$, l'équation $x^n + y^n \equiv z^n [p]$ admet une solution non triviale (ie : $xyz \not\equiv 0[p]$).

Théorème 41 (Sophie Germain) : Soit $p \in \mathbb{P}$ un nombre impair, tel que $q = 2p+1$ est premier. Alors il n'existe pas de triplet $(x;y;z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0\,[p]$. $\boxed{\text{DEV2}}$

Rq 42 : Les deux résultats précédents sont des cas particuliers du grand théorème de Fermat (ou Fermat-Wiles).

Prop 43 (Nagell-Ramanujan) : L'équation (E) : $x^2+3 = 2^n$, d'inconnues $x \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ admet seulement 2 solutions, à savoir $(-1;2)$ et $(1;2)$.

Déf 44 : Une équation de Mordell est une équation de la forme $x^3 = y^2 + k$, où $k \in \mathbb{Z}$ est un paramètre, et les inconnues sont x et $y \in \mathbb{Z}$.

Théorème 45 : L'équation (E) : $y^2 = x^3 + 16$ admet 2 solutions, à savoir $(0;4)$ et $(0;-4)$ pour le couple $(x;y)$.

Théorème 46 : L'équation (E) : $y^2 = x^3 - 5$ n'admet pas de solution sur $\mathbb{Z}^2$.

3) Carrés modulo p et réciprocité quadratique

Prop/déf 47 : Soit $q = p^n$ où $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. L'application
$$F_p : \begin{array}{ccc} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & x^p \end{array}$$
est un morphisme d'anneaux, appelé morphisme de Frobenius.

Prop 48 : (i) Si $p = 2$, tous les éléments de $\mathbb{F}_q$ sont des carrés.
(ii) Si $p \in \mathbb{P}\setminus\{2\}$, il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.

Prop 49 : Si $\mathrm{car}(\mathbb{F}_q) = p \in \mathbb{P}\setminus\{2\}$, $x \in \mathbb{F}_q^\times$ est un carré $\Leftrightarrow x^{\frac{q-1}{2}} = 1$.

Corollaire 50 : Avec les mêmes hypothèses sur $\mathbb{F}_q$, on a :
-1 est un carré dans $\mathbb{F}_q^\times \Leftrightarrow q \equiv 1\,[4]$.

Déf 51 : On dit que $x \in \mathbb{Z}$ est un résidu quadratique modulo $p \in \mathbb{P}\setminus\{2\}$ si x est un carré dans $\mathbb{F}_p$, c'est-à-dire : $x \equiv y^2\,[p]$.

Déf 52 : Si $x \in \mathbb{Z}$ et $p \in \mathbb{P}\setminus\{2\}$, le symbole de Legendre $\left(\frac{x}{p}\right)$ est défini par :
$$\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } p \mid x \\ 1 \text{ si } x \text{ est un résidu quadratique modulo } p. \\ -1 \text{ sinon} \end{cases}$$

Prop 53 : Si $p \in \mathbb{P}\setminus\{2\}$: ① $\forall (a,b) \in \mathbb{Z}^2$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$.

② $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ soit : $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1\,[4] \\ -1 \text{ si } p \equiv 3\,[4] \end{cases}$

③ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ soit : $\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1\,[8] \\ -1 \text{ si } p \equiv \pm 3\,[8] \end{cases}$

Théorème 54 (réciprocité quadratique) : Si $p, q \in \mathbb{P}\setminus\{2\}$, alors :
$\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$, soit : $\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1\,[4] \text{ \underline{ou} } q \equiv 1\,[4] \\ -1 \text{ si } p \equiv 3\,[4] \text{ \underline{et} } q \equiv -1\,[4]. \end{cases}$

Exc 55 : $\left(\frac{192}{101}\right) = \left(\frac{91}{101}\right) = \left(\frac{7}{101}\right) \times \left(\frac{13}{101}\right) = \left(\frac{101}{7}\right) \times \left(\frac{101}{13}\right) = \left(\frac{3}{7}\right) \times \left(\frac{10}{13}\right)$
$= \left(\frac{3}{7}\right) \times \left(\frac{2}{13}\right) \times \left(\frac{5}{13}\right) = \left(\frac{7}{3}\right) \times \left(\frac{13}{5}\right) = \left(\frac{1}{3}\right) \times \left(\frac{3}{5}\right) = \left(\frac{-1}{3}\right) = -1.$

Lemme 56 (Zolotarev) : Soit $p \in \mathbb{P}\setminus\{2\}$. $m_a : \begin{array}{ccc} \mathbb{F}_p & \to & \mathbb{F}_p \\ x & \mapsto & ax \end{array}$ est une permutation, et $\varepsilon(m_a) = \left(\frac{a}{p}\right)$.

Théorème 57 (Frobenius-Zolotarev) : Si $p \in \mathbb{P}\setminus\{2\}$ et $u \in GL_n(\mathbb{F}_p)$, alors u est une permutation de $\mathbb{F}_p^n$, de signature $\left(\frac{\det(u)}{p}\right)$.

Rq 58 : Il existe une méthode algorithmique pour déterminer la racine carrée d'un résidu quadratique modulo p, c'est l'algorithme de Tonelli-Shanks.

Prop 59 : $2^n - 1$ est un carré dans $\mathbb{N} \Leftrightarrow n = 0$ ou 1.