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

Soit $n \in \mathbb{N}$

I) Construction et propriétés de $\mathbb{Z}/n\mathbb{Z}$:

1) Congruences.

[Rom] 279 **Définition 1** : Soient $a, b \in \mathbb{Z}$, on dit que a est congru à b modulo n si n divise $b-a$. On note alors $a \equiv b\ [n]$.

[Esc] 217 **Proposition 2** : La relation de congruence est une relation d'équivalence. Pour $a \in \mathbb{Z}$, on note $\bar{a} = a + n\mathbb{Z}$ sa classe d'équivalence modulo n.
L'ensemble quotient associé est noté $\mathbb{Z}/n\mathbb{Z}$.
On notera $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique associée

[Rom] 280 **Théorème 3** : Si $n \neq 0$, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\}$, et $|\mathbb{Z}/n\mathbb{Z}| = n$

Exemples 4 : • $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}; \bar{1}\}$. $\pi(3) = \bar{1}$, $\pi(6) = \bar{0} = \overline{12}$

• Dans $\mathbb{Z}/17\mathbb{Z}$, $\overline{67} = \overline{16}$.

2) Structure d'anneau :

Proposition 5 : L'addition et la multiplication sur $\mathbb{Z}$ sont compatibles avec la relation de congruence
[Rom] 280 $\forall (a;b;c;d) \in \mathbb{Z}$, $(a \equiv b\ [n],\ c \equiv d\ [n]) \Rightarrow (a+c \equiv b+d\ [n]$ et $ac \equiv bd\ [n])$.

Théorème 6 : Pour $n \geq 2$, il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que π_n soit un morphisme d'anneaux

[Rom] 283 **Proposition 7** : $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ sont donc des groupes et, si $a \in \mathbb{Z}$, on a équivalence entre :
i) $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
ii) a est premier avec n
iii) $\bar{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

[Esc] 232 **Exercice 8** : 583 est-il inversible dans $\mathbb{Z}/679\mathbb{Z}$?

Remarque 9 : Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont les éléments non-premiers avec n.

Proposition 10 : Pour $n \geq 2$, les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques d'ordre qui divise n.
[Rom] 291 Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, le groupe $\langle \bar{q} \rangle$ où $qd = n$. Ce sous-groupe est aussi l'ensemble des éléments de G dont l'ordre divise d et ses générateurs sont tous les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

Exemple 11 : $(\mathbb{Z}/4\mathbb{Z}, +)$ les sous-groupes sont $\{\bar{0}\}$, $\{\bar{0}; \bar{2}\}$, $\{\bar{0}; \bar{1}; \bar{2}; \bar{3}\} = \mathbb{Z}/4\mathbb{Z}$

• Les seuls sous-groupes de $(\mathbb{Z}/7\mathbb{Z}, +)$ sont $\{\bar{0}\}$ et $\mathbb{Z}/7\mathbb{Z}$

3) Cas $n = p$ premier :

Proposition 12 : $\mathbb{Z}/p\mathbb{Z}$ est intègre.

Contre-exemple 13 : Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2} \times \bar{3} = \bar{6} = \bar{0}$. $\bar{2}$ et $\bar{3}$ sont des diviseurs de 0.

[Esc] 231 **Proposition 14** : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier

II) Étude de $(\mathbb{Z}/n\mathbb{Z})^\times$ et $\mathbb{Z}/p\mathbb{Z}$:

1) $(\mathbb{Z}/n\mathbb{Z})^\times$:

Exemple 15 : $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}; \bar{3}; \bar{5}; \bar{7}\}$

et $(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1};\bar{2};\bar{4};\bar{5};\bar{7};\bar{8}\}$

Théorème 16 : si p est premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique

Théorème 17 : si p est premier et impair et $\alpha \in \mathbb{N}$, $\alpha \geq 2$, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

2) Théorème des restes chinois

Lemme 18 : Soient $(n_i)_{1\leq i\leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1.

1) Si les entiers $n_1, \dots, n_r$ sont deux-à-deux premiers entre eux, leur ppcm est $\prod_{i=1}^{r} n_i$.

2) Si les $n_1, \dots, n_r$ ne sont pas deux-à-deux premier entre eux, $\text{ppcm}(n_1, \dots, n_r) < \prod_{i=1}^{r} n_i$

Contre-exemple 19 : $\text{ppcm}(2;3;4) = 12 < 2\times 3\times 4 = 24$

Théorème 20 : Soient $(n_j)_{1\leq j\leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = \prod_{j=1}^{r} n_j$. Les entiers $n_1, \dots, n_r$ sont deux-à-deux premiers entre eux si et seulement si $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ où $n = n_1 \dots n_r$. Dans ce cas, l'application :

$$\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z} \quad \Pi_n(k) = \Pi_{n_1}(k), \dots \Pi_{n_r}(k)$$

est un isomorphisme d'anneaux inverse

$$\psi^{-1} : \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$(\Pi_{n_1}(a_1), \dots, \Pi_{n_r}(a_r)) \longmapsto \Pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right)$$

où $(u_i)_{1\leq i\leq r}$ est une suite d'entiers tq $\sum_{i=1}^{r} u_i \frac{n}{n_i} = 1$

3) Fonction indicatrice d'Euler

Définition 21 : on appelle fonction indicatrice d'Euler la fonction qui associe à tout entier naturel non-nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n.

Exemple 22 : $\varphi(15) = 8$ $(1,2,4,7,8,11,13,14)$

Proposition 23 : $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}|$. $\varphi(n)$ est également égal au nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Corollaire 24 : $\varphi(p) = p - 1$ pour p premier.

Corollaire 25 : $\varphi(p^r) = p^r - p^{r-1}$ pour $r \in \mathbb{N}^*$

Proposition 26 : Si $a, b \in \mathbb{Z}$ sont premiers entre eux, $\varphi(ab) = \varphi(a)\varphi(b)$

Proposition 27 : $\forall n \geq 3$ $\varphi(n)$ est pair

Théorème 28 : Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha}$ avec $2 \leq p_i < \dots < p_r$ premiers et les α_i entiers naturels non-nuls, on a alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$

En particulier, si $d \mid n$, $\varphi(d) \mid \varphi(n)$.

Théorème 29 : pour tout $n \geq 2$, $\sqrt{n} - 1 < \varphi(n) < n - 1$

III) Applications

1) Système de congruences

Proposition / définition 30 : soit $n \geq 2$ un entier naturel, $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$. L'équation diophantienne $ax \equiv b[n]$ a des solutions entières ssi $\delta = \text{pgcd}(a; n)$ divise b.

Dans ce cas, l'ensemble des solutions est $S = \{ b'x_0' + kn' ; k \in \mathbb{Z} \}$ où x_0' est une solution particulière de $a'x \equiv 1 [n']$ ($a'\delta = a$ et $n'\delta = n$)

Proposition 31 : Si $(n_1, \dots, n_r)$ sont premiers entre eux deux-à-deux, alors le système de congruences $\begin{cases} x \equiv a_1 [n_1] \\ x \equiv a_2 [n_2] \\ \vdots \\ x \equiv a_r [n_r] \end{cases}$ admet des solutions

Application 32 : Résoudre le système $\begin{cases} k \equiv 2 [4] \\ k \equiv 3 [5] \\ k \equiv 1 [9] \end{cases}$

2) Arithmétique :

Théorème 33 : [Euler] pour tout $a \in \mathbb{Z}$ premier avec n, $a^{\varphi(n)} \equiv 1 [n]$

Théorème 34 : [Fermat] Si $p \in \mathbb{N}$ est premier, $a \in \mathbb{Z}$ est premier avec p alors $a^{p-1} \equiv 1 [p]$ et pour tout $a \in \mathbb{Z}$, $a^p \equiv a [p]$.

Proposition 35 : Si d divise n, il existe $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. On a alors $n = \sum_{d \mid n} \varphi(d)$