Leçon N° 120 : Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.

I) Construction de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Lemme 1 : Les sous-groupes de $(\mathbb{Z}, +)$ (respectivement les idéaux de $(\mathbb{Z}, +, \times)$) sont exactement les $n\mathbb{Z}$, $n \in \mathbb{N}$.

Définition 2 : Soient $n \in \mathbb{N}$, $(a,b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n lorsque $n \mid (b-a)$. On note alors $a \equiv b\ [n]$.

Proposition 3 : $\forall n \in \mathbb{N}$, cette relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. $\forall a \in \mathbb{Z}$, on note $\bar{a} = a + n\mathbb{Z}$ sa classe d'équivalence.

Définition 4 : $\forall n \in \mathbb{N}$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n. On note $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$ la surjection canonique.

Proposition 5 : $\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ de cardinal n.

Proposition 6 : $\forall n \in \mathbb{N}^*$, la congruence modulo n est compatible avec $+$ et $\times$.

Théorème 7 : Pour $n \geq 2$, $\exists$ une unique structure d'anneau commutatif sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique π_n soit un morphisme d'anneaux.

Proposition 8 : Pour $n > 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre qui divise n. Réciproquement pour tout diviseur d de n, $\exists!$ sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, c'est le groupe cyclique $\langle \bar{q} \rangle = \{\bar{0}, \bar{q}, \dots, (d-1)\bar{q}\}$ où $q = \frac{n}{d}$.

Lemme 9 : On introduit $\Sigma = \{n \in \mathbb{N},\ n = a^2 + b^2,\ (a,b) \in \mathbb{N}^2\}$

$\mathbb{Z}[i] = \{a + ib \mid (a,b) \in \mathbb{Z}^2\}$ sous-anneau de $\mathbb{C}$.

$N : \mathbb{Z}[i] \to \mathbb{N}$, $z = (a+ib) \mapsto z\bar{z} = a^2 + b^2$.

1) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

2) Σ est stable par $\times$

3) $\mathbb{Z}[i]$ est euclidien, donc principal

4) $(p \in \Sigma)$ ssi (p pas irréductible dans $\mathbb{Z}[i]$) pour p premier

Théorème 10 : (des deux carrés) Soit p premier, $(p \in \Sigma)$ ssi $(p = 2$ ou $p \equiv 1\ [4])$.

II) Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ et la fonction indicatrice d'Euler.

Définition 11 : Pour $n \geq 2$, on note $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Proposition 12 : (A partir de maintenant $n \geq 2$.) Soit $a \in \mathbb{Z}$. Il y a équivalence entre :

1) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

2) $a \wedge n = 1$

3) $\bar{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 13 : On appelle fonction indicatrice d'Euler la fonction qui associe à tout entier naturel n non nul, le nombre $\varphi(n)$ d'entiers $\in [\![1, n]\!]$ premiers avec n.

Remarque 14 : $\varphi(n)$ est le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 15 : Si p est premier, $\varphi(p) = p - 1$.

Théorème 16 : (d'Euler) $\forall a \in \mathbb{Z}$ tq $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1\ [n]$.

Théorème 17 : (de Fermat) Soit $p \in \mathbb{N}$ premier. $\forall a \in \mathbb{Z}$ tq $a \wedge p = 1$ on a $a^{p-1} \equiv 1\ [p]$ et $\forall a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.

Proposition 18 : $n = \sum_{d \mid n} \varphi(d)$.

leo possible

III) Théorème chinois et système d'équation diophantiennes

Théorème 19 : Soient $(n_j)_{1\leq j\leq r}$ une famille de $r\geq 2$ entiers naturels ≥ 2 et $n := \prod_{j=1}^{r} n_j$.
Les entiers $n_1, \dots, n_r$ sont deux-à-deux premiers entre eux ssi les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes.

Dans ce cas, l'application

$$\begin{aligned} \psi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} \\ \pi_n(q) &\longmapsto (\pi_{n_1}(q), \dots, \pi_{n_r}(q)) \end{aligned}$$

est un isomorphisme d'anneaux d'inverse :

$$\begin{aligned} \psi^{-1} : \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\pi_{n_1}(a_1), \dots, \pi_{n_r}(a_r)) &\longmapsto \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right) \end{aligned}$$

où $(u_j)_{1\leq j\leq r}$ est une famille d'entiers relatifs telle que $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$.

Lemme 20 : $\forall p \in \mathbb{N}$ premier et $\forall \alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$

Proposition 21 : Soit $n \geq 2$ tel que sa décomposition en produit de facteurs premiers soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
On a alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$
$= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

Proposition 22 : $\forall n \geq 2$, $\sqrt{n} - 1 \leqslant \varphi(n) \leq n - 1$.

Théorème 23 : Soient $n \geq 2$, $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$.
On considère l'équation diophantienne dans $\mathbb{Z}$: $ax \equiv b\ [n]$ (E).
On note $\delta = \gcd(a, n)$, $a = \delta a'$ et $n = \delta n'$ avec $n' \wedge a' = 1$.
L'équation (E) a des solutions ssi $\delta \mid b$.
Dans ce cas, $S = \{ b'x_0 + kn',\ k \in \mathbb{Z} \}$ où x_0 est une solution particulière de $a'x \equiv 1\ [n']$.

Exemple 24 : Considérons le système d'équation diophantiennes :

$$\begin{cases} q \equiv 2\ [4] \\ q \equiv 3\ [5] \\ q \equiv 1\ [9] \end{cases}$$

Les solutions sont $S = \{ 118 + 180k,\ k \in \mathbb{Z} \}$.

IV) Cyclicité de $\mathbb{Z}/p^\alpha\mathbb{Z}$.

Notation 25 : Soit p un nombre premier. $\forall d \mid p-1$, on note $\varphi(d)$ le nombre d'éléments d'ordre d dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$

Lemme 26 : Dans les mêmes conditions, $\psi(d) = \varphi(d)$.

Lemme 27 : Si $(G, \cdot)$ est un groupe commutatif, $r \geq 2$ un entier et $g_1, \dots, g_r$ des éléments deux-à-deux distincts de G d'ordres respectifs $m_1, \dots, m_r$, $\exists g \in G$ d'ordre égal au ppcm de ces ordres.

Théorème 28 : Tout sous groupe fini de groupe multiplicatif $\mathbb{K}^*$ ($\mathbb{K}$ étant un corps commutatif) est cyclique.

Théorème 29 : Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Théorème 30 : Si p est premier impair et $\alpha \in \mathbb{N}^*$, ≥ 2, alors le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique.

Théorème 31 : Soit $n \in \mathbb{N}^*$, ≥ 2. Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec $\alpha \in \mathbb{N}^*$ et p

premier impair.

V) Application: loi de réciprocité quadratique.

p est un nombre premier et on note $\mathbb{F}_p$ l'anneau $\mathbb{Z}/p\mathbb{Z}$.

On suppose p impair.

Lemme 32: $\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$ est un groupe d'ordre 2.

Corollaire 33: $|\mathbb{F}_p^{\times 2}| = \frac{p-1}{2}$

Lemme 34: $\forall \bar{x} \in \mathbb{F}_p^\times$, on a $\bar{x}^{\frac{p-1}{2}} = \pm 1$

De plus $\bar{x}^{\frac{p-1}{2}} = 1$ ssi $\bar{x} \in \mathbb{F}_p^{\times 2}$.

Notation 35: On définit le symbole de Legendre par $\forall a \in \mathbb{F}_p$:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \in \mathbb{F}_p^{\times 2} \\ -1 \text{ si } a \notin \mathbb{F}_p^{\times 2} \\ 0 \text{ si } a = 0 \end{cases}$$

Lemme 36: Soit $a \in \mathbb{F}_p^\times$. On a

$$|\{x \in \mathbb{F}_p \text{ tq } ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Théorème 37: (Loi de la réciprocité quadratique) Soit q un nombre premier impair $\neq p$.

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

On peut peut être parler de la fonction de Möbius après φ