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

Références : Rombaldi, Perrin, Gourdon (pour RSA)

I - Structure de $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

2) L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

II - Application à l'arithmétique dans $\mathbb{Z}$

1) Tests de primalité

2) Equations arithmétiques

3) Les carrés dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p premier

III - Application aux polynômes et à la théorie des corps

1) Irréductibilité de certains polynômes

2) Caractéristique d'un corps - corps finis

DEV 1 : Théorème de Korselt

DEV 2 : Loi de réciprocité quadratique

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

I - Structure de $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ [ROM] [PER]

DEF 1 : Soient $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$. On dit que a est congru modulo n et on note $a \equiv b \pmod n$ lorsque n divise $b-a$.

PROP 2 : La relation de congruence est une relation d'équivalence sur $\mathbb{Z}$. On note $\bar{x}$ la classe modulo cette relation. $\bar{x} = \{x + qn \mid q \in \mathbb{Z}\}$

DEF 3 : On note $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ et on désigne par $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \bar{k}$ la surjection canonique.

PROP 4 : On définit sur $\mathbb{Z}/n\mathbb{Z}$ une loi $+$ telle que $\bar{a} + \bar{b} = \overline{a+b}$. Elle munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe abélien de cardinal n.

THM 5 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique engendré par $\bar{1}$.

THM 6 : Tout groupe cyclique à n éléments est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Deux groupes cycliques sont isomorphes si et seulement s'ils ont même cardinal.

COR 7 : Si p est premier et $\#G = p$, alors $G \simeq \mathbb{Z}/p\mathbb{Z}$.

THM 8 : Tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre divisant n. Réciproquement, pour tout diviseur d de n il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. C'est le sous-groupe engendré par $\frac{n}{d}$.

PROP 9 : $\bar{a}$ engendre $\mathbb{Z}/n\mathbb{Z} \iff a \wedge n = 1$.

EX 10 : $\mathbb{Z}/8\mathbb{Z}$ est engendré par $1; 3; 5; 7$.

DEF 11 : On définit la fonction indicatrice d'Euler par $\varphi : n \in \mathbb{N}^* \mapsto \{k \in [\![1; n-1]\!] \mid k \wedge n = 1\}$

EX 12 : Pour tout p premier, $\varphi(p) = p-1$.

PROP 13 : Si $d \mid n$, il y a $\varphi(d)$ éléments d'ordre d

COR 14 : $\sum_{d \mid n} \varphi(d) = n$

THM 15 : (Structure des groupes abéliens finis, ADMIS) : Soit G un groupe abélien fini. Il existe des entiers $d_1, \dots, d_s \geq 2$ tels que $d_1 \mid d_2 \mid \dots \mid d_s$ tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$. La suite $(d_1, \dots, d_s)$ est unique et s'appelle la suite des invariants de G.

2) L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ [ROM]

PROP 16 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

PROP 17 : On munit $(\mathbb{Z}/n\mathbb{Z}, +)$ d'une multiplication $\times$ définie par $\bar{a} \times \bar{b} = \overline{ab}$. Cela munit $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ d'une structure d'anneau commutatif unitaire

REM 18 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes additifs.

THM 19 : Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{a}$ tels que $a \wedge n = 1$. Il y en a donc $\varphi(n)$. $(\mathbb{Z}/n\mathbb{Z})^\times$ est le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. Ainsi $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est premier.

THM 20 : $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$

THM 21 : (Chinois) Soit $(n_j)_{1 \leq j \leq r}$ est 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 $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$.

COR 22 : Soit $n \in \mathbb{N}^*$, $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On a alors :
1) $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$; $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ et $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

LEMME 23 : $\forall k \in \mathbb{N}^*$, p premier, $p \geq 3$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda \in \mathbb{N}^*$, $\lambda \wedge p = 1$.

PROP 24 : Si p est premier, $p \geq 3$, et $\alpha \in \mathbb{N}$, $\alpha \geq 1$, on a :
$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$ donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique

COR 25 : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \in \{2; 4; p^\alpha; 2p^\alpha;$ p premier, $p \geq 3\}$

II - Application à l'arithmétique dans $\mathbb{Z}$

1) Tests de primalité [Rom]

THM 26: Pour tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 \pmod n$

THM 27: (Fermat) Soit $p \in \mathbb{N}$ premier. Pour tout $a \in \mathbb{Z}$ tel que $a \wedge p = 1$, on a $a^{p-1} \equiv 1 \pmod p$ et pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \pmod p$.

THM 28: (Wilson) n est premier si et seulement si $(n-1)! \equiv -1 \pmod n$

DEF 29: On appelle nombre de Carmichael tout entier $n \geq 3$ non premier tel que pour tout a premier avec n, on a $a^{n-1} \equiv 1 \pmod n$

EX 30: 561 est un nombre de Carmichael.

DEV 1

LEMME 31: Un nombre de Carmichael est impair

LEMME 32: Un nombre de Carmichael est sans facteur carré.

THM 33: (Korselt) Soit $n \in \mathbb{N}$, $n \geq 3$: LASSE

(1) $\exists r \geq 3$, $\exists\, 3 \leq p_1 < \dots < p_r$ premiers tels que $n = \prod_{j=1}^{r} p_j$ et pour tout $j \in [\![1;r]\!]$, $p_j - 1 \mid n-1$

(2) n est non premier et pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, on a $x^n = x$

(3) n est un nombre de Carmichael

APPLI 34: (Cryptage RSA) [Gou]

Alice veut envoyer un message privé à Bob.

- Bob choisit deux nombres premiers distincts p, q et pose $n = pq$ puis il choisit $c, d \in \mathbb{N}$ tels que $cd \equiv 1 \pmod{\varphi(n)}$
- Bob diffuse la clé publique (n, c) et conserve la clé secrète (n, d)
- Pour envoyer son message m mod n, Alice envoie le message chiffré $M \equiv m^c \pmod n$
- Bob déchiffre le message $m = M^d \pmod n$ (par Euler)

Le succès de cet algorithme réside dans la difficulté de factoriser un entier.

2) Equations arithmétiques [Rom]

Pour $n \geq 2$, $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$, on veut résoudre dans $\mathbb{Z}$ l'équation diophantienne $ax \equiv b \pmod n$ $(*)$

PROP 35: Si $b = 1$, cette équation a des solutions si et seulement si $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $a \wedge n = 1$. Dans ce cas, on trouve une solution $x_0 \in \mathbb{Z}$ avec l'algorithme d'Euclide étendu et l'ensemble des solutions est : $S = \{x_0 + kn \mid k \in \mathbb{Z}\}$.

COR 36: Dans le cas où $a \wedge n = 1$, et $b \in \mathbb{Z}$, l'ensemble des solutions de $(*)$ est $S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$.

THM 37: (Cas général) Soit $\delta = a \wedge n$, $a = \delta a'$, $n = \delta n'$ avec $a' \wedge n' = 1$. L'équation $(*)$ a des solutions dans $\mathbb{Z}$ si et seulement si δ divise b. Dans ce cas, l'ensemble des solutions de $(*)$ est $S = \{b' x_0' + kn' \mid k \in \mathbb{Z}\}$ où x_0' est une solution de $a'x \equiv 1 \pmod{n'}$.

REM 38: Le théorème chinois peut être utilisé pour résoudre un système de congruences.

Ex 39: Les solutions de $\begin{cases} k \equiv 2 \pmod 4 \\ k \equiv 1 \pmod 9 \\ k \equiv 3 \pmod 5 \end{cases}$ sont les $118 + 180q'$ où $q' \in \mathbb{Z}$.

3) Les carrés dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p premier) [PER] [Rom]

On s'intéresse à $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $(\mathbb{F}_p^*)^2 = \{x^2 \mid x \in \mathbb{F}_p^*\}$

PROP 40: - Pour $p = 2$, on a $\mathbb{F}_p^2 = \mathbb{F}_p$.
- Pour $p \geq 3$, $\#\mathbb{F}_p^2 = \frac{p+1}{2}$ et $\#(\mathbb{F}_p^*)^2 = \frac{p-1}{2}$.

APPLI 41: Pour $a, b \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p$, l'équation $ax^2 + by^2$ admet des solutions dans $\mathbb{F}_p$.

PROP 42: Soit $p \geq 3$. Alors $x \in (\mathbb{F}_p^*)^2 \iff x^{\frac{p-1}{2}} = 1$

DEF 43: Pour p premier impair et $a \in \mathbb{F}_p$, on définit le symbole de Legendre de a par :

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } a = 0 \end{cases}$$

LEMME 44 : Soit p premier impair et $a \in \mathbb{F}_p^*$. On a :
$$\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = 1 + \left(\frac{a}{p}\right).$$

THM 45 : (Loi de réciprocité quadratique) Soient p, q deux nombres premiers impairs distincts. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

EX 46 : 2 est un carré dans $\mathbb{Z}/7\mathbb{Z}$ mais pas 3.

III - Application aux polynômes et à la théorie des corps

1) Irréductibilité de certains polynômes [PER]

PROP 47 : Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :
1) les constantes irréductibles dans $\mathbb{Z}$ (i.e premiers)
2) les polynômes $P \in \mathbb{Q}[X]$ primitifs et irréductibles.

THM 48 : (Critère d'Eisenstein) Soit $P(X) = a_nX^n + \dots + a_0 \in \mathbb{Z}[X]$. Soit $p \in \mathbb{Z}$ premier. On suppose que :
- $p \nmid a_n$ • $\forall i \in [\![0; n-1]\!]$, $p \mid a_i$ et $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$.

EX 49 : Soit $a \in \mathbb{Z}$, $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On suppose qu'il existe $i \in [\![1; r]\!]$, $\alpha_i = 1$. Alors $X^n - a$ est irréductible dans $\mathbb{Z}[X]$.

THM 50 : (Réduction modulo p) Soit $P \in \mathbb{Z}[X]$. On suppose qu'il existe $p \in \mathbb{Z}$ premier tel que $\bar{P}$ soit irréductible dans $\mathbb{F}_p[X]$. Alors, P est irréductible dans $\mathbb{Q}[X]$.

EX 51 : Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

DEF 52 : Soient K un corps et $n \in \mathbb{N}^*$ tel que $n \wedge car(K) = 1$. L'ensemble des racines n-ièmes de l'unité est $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$. C'est un sous-groupe de K^* donc cyclique.

DEF 53 : Une racine n-primitive de 1 est un élément ζ de $\mu_n(K)$ d'ordre n. Il y a $\varphi(n)$ racines primitives de 1. On note $\mu_n^*(K)$ leur ensemble.

DEF 54 : On définit le n-ième polynôme irréductible
$$\phi_{n,K}(X) = \prod_{\zeta \in \mu_n^*(K)} (X - \zeta)$$

PROP 55 : ϕ_n est unitaire de degré $\varphi(n)$ et $\phi_n \in \mathbb{Z}[X]$.

THM 56 : $\forall n \in \mathbb{N}^*$, $\phi_{n,\mathbb{Q}}$ est irréductible sur $\mathbb{Q}$.

2) Caractéristique d'un corps - corps finis [PER]

DEF 57 : Soit K un corps. On appelle sous-corps premier de K le plus petit sous-corps de K.
Soit $\varphi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1$. $\ker(\varphi)$ est idéal de $\mathbb{Z}$ donc $\ker(\varphi) = p\mathbb{Z}$ et comme $\mathbb{Z}/p\mathbb{Z} \simeq Im(\varphi) \subset K$ donc intègre, $p\mathbb{Z}$ est premier donc $p = 0$ ou p est premier.
Le nombre p est appelé la caractéristique du corps K on la note $car(K)$.

PROP 58 : • Si $car(K) = 0$, $\varphi(\mathbb{Z}) \simeq \mathbb{Z} \subset K$ donc K est infini. De plus, $K \supset Frac(\mathbb{Z}) = \mathbb{Q}$ et $\mathbb{Q}$ est le sous-corps premier de K.
• Si K est fini, on a $car(K) = p > 0$, le sous-corps premier de K est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

COR 59 : Si K est fini, on a $car(K) = p > 0$ donc $q = \#K = p^n$ où $n = [K : \mathbb{F}_p]$.

THM 60 : Soit p premier et $n \in \mathbb{N}^*$, $q = p^n$.
• Il existe un corps à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
• En particulier, K est unique à isomorphisme près.