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

Dans toute la leçon n désignera un nombre entier et p un nombre premier.

1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

1.1 Congruence dans $\mathbb{Z}$

Définition 1 (BER 30, ROM 279)**.** Soient $a, b \in \mathbb{Z}$.
On dit que a est congru à b modulo n si $a - b$ est multiple de n, i.e. s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.
On note $a \equiv b\ [n]$.

Remarque 2 (ROM 280)**.** Si $n = 0$, la congruence est une relation d'égalité.

Exemple 3 (No ref)**.**

n pair $\iff n \equiv 0\ [2]$

Remarque 4 (ROM 279)**.** $a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Proposition 5 (BER 30)**.** Soient $a, b, c, d \in \mathbb{Z}$. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ on a alors : $-a \equiv -b\ [n]$, $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$.

1.2 Construction de $\mathbb{Z}/n\mathbb{Z}$

Proposition 6 (ROM 279, BER 31)**.** La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Notation 7 (ROM 279, BER 31)**.** Pour tout $a \in \mathbb{Z}$, on note $\overline{a} = \{a + qn | q \in \mathbb{Z}\}$ la classe d'équivalence de a.
L'ensemble de toutes les classes d'équivalence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

Exemple 8 (BER 32)**.** $\forall a \in \mathbb{Z}, \overline{a} = \overline{0} \iff n | a$

Proposition 9 (BER 32)**.** Les lois $(\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} = \overline{a + b}$ et $(\overline{a}, \overline{b}) \mapsto \overline{a}.\overline{b} = \overline{ab}$ munissent $\mathbb{Z}/n\mathbb{Z}$ sont des loi de compositions interne dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 10 (TL1 131, ROM 280, BER 32, mixte)**.** Pour tout $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n. Ses éléments sont $\overline{0}, \overline{1}, ..., \overline{n-1}$.

Contre exemple 11 (BER 33)**.** Si $n = 0$, $a \equiv b\ [0] \iff a = b$. Donc $\overline{a} = \{a\}$ et $\mathbb{Z}/n\mathbb{Z}$ possède une infinité d'éléments.

Théorème 12 (ROM 281)**.** Pour $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire. De plus le morphisme canonique $\pi_n : k \mapsto \overline{k}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux.

Proposition 13 (ROM 281)**.** Pour $n \geq 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre d avec $d|n$. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d qui est $H =< \overline{q} >$ où $q = \frac{n}{d}$

Proposition 14 (ROM 281)**.** Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes donc ils sont principaux.

2 Etude de $(\mathbb{Z}/n\mathbb{Z})^{\times}$

Dans la suite, on considère $n \geq 2$.

2.1 Inversibles

Notation 15 (ROM 282)**.** On note $(\frac{\mathbb{Z}}{n\mathbb{Z}})^{\times}$ le groupe multiplicatif des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Remarque 16 (ROM 282)**.** Pour $n = 0$, $(\frac{\mathbb{Z}}{0\mathbb{Z}})^{\times} = \mathbb{Z}^{\times}$ et pour $n = 1$, $(\frac{\mathbb{Z}}{\mathbb{Z}})$ n'est pas un anneau.

Proposition 17 (ROM 283)**.** Soit $a \in \mathbb{Z}$. LASSE :

1. $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
2. a est premier avec n
3. $\overline{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

Théorème 18 (BER 33)**.** Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Notation 19 (BER 33)**.** Si p est premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Exemple 20. Si n n'est pas premier, il y a plusieur façon de voir que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps. Par exemple en montrant qu'il n'est pas intègre. Pour illustrer cela avec $\mathbb{Z}/4\mathbb{Z}$, on écrit que $\overline{2} \times \overline{2} = \overline{4} = \overline{0}$, pourtant $\overline{2} \neq \overline{0}$.

2.2 Indicatrice d'Euler

Définition 21 (TL1 146)**.** Pour $n \leq 1$, notons $\varphi(n)$ le nombre d'entiers $k \in [\![1, n]\!]$ premiers avec n. La fonction $\varphi : \mathbb{N} \to \mathbb{N}$ ainsi définie est appelée fonction indicatrice d'Euler.

Exemple 22 (TL1 147)**.** Si p est premier, $\varphi(p) = p-1$ car tout $k \in [\![1, p-1]\!]$ est premier avec p.

Proposition 23 (BER 488)**.** L'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\varphi(n)$.

Théorème 24 (ROM 283, TL1 147)**.** [Euler] Pour tout $a \in \mathbb{Z}$ premier avec n, on a : $a^{\varphi(n)} \equiv 1\ [n]$

Théorème 25 (ROM 284, TL1 147)**.** [petit théorème de Fermat] Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ premier avec p, on a $a^{p-1} \equiv 1\ [p]$ et pour tout entier relatif a, on a $a^p \equiv a\ [p]$.

Proposition 26 (ROM 284)**.** ["identité arithmétique" je crois] Pour tout $n \geq 2$, on a $n = \sum\limits_{d \in \mathcal{D}_n} \varphi(d)$ où $\mathcal{D}_n$ est l'ensemble des diviseurs positifs de n.

3 Applications à l'arithmétique

3.1 Équations diophantiennes

On considère toujours n un entiers supérieur ou égal à 2.

Définition 27 (ROM 289)**.** Une équation diophantienne est une équation à solutions dans $\mathbb{Z}$ de la forme $ax \equiv b\ [n]$ où $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Exemple 28. Si $b = 1$, cette équation a des solutions si et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème 29 (ROM 290)**.** Soit $\delta = pgcd(a, n)$. L'équation diophantienne $ax \equiv b\ [n]$ a des solutions entières si et seulement si δ 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 $a'x \equiv 1\ [n]$.

Exemple 30 (No ref)**.** $9x \equiv 15\ [23]$ admet une unique solution modulo 23

Théorème 31 (thm chinois)**.** [TL1 149, DEV 1] Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. Étant donné des entiers $a_1, .., a_r$, considérons le système de congruences :
$(S) : x \equiv a_i\ [m_i]\ (i = 1, ..., r)$
Ce système possède une solution $x \in \mathbb{Z}$ qui est unique modulo M.

Corollaire 32 (TL1 150)**.** Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. On a alors :

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_i\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$$

Application 33 (un peu ROM 290, 291)**.** Ce théorème permet de résoudre des système d'équations diophantienne. Le système

$$\begin{cases} k \equiv a_1\ [n_1] \\ \quad ... \\ k \equiv a_r\ [n_r] \end{cases}$$

a toujours une infinité de solutions si la famile $(a_i)_{1 \leq i \leq r}$ est une famille d'éléments 2 à 2 premiers entre eux. Cette solution est unique modulo $n = n_1..n_r$.

Exemple 34 (BER 469)**.** Considérons le système d'équations diophantiennes :

$$\begin{cases} k \equiv 1\ [3] \\ k \equiv 2\ [4] \\ k \equiv -1\ [7] \end{cases}$$

3, 4 et 7 sont deux à deux premiers entre eux donc ce système a des solutions. La 1ère équation donne $x = 1 + 3y, y \in \mathbb{Z}$. En reportant dans la $2-$ème, on obtient $3y \equiv 1[4]$. On a alors $y \equiv -1\ [4]$, soit $y = -1 + 4z, z \in \mathbb{Z}$ donc $x = 1 + 3(-1 + 4z) = -2 + 12z$ avec $z \in \mathbb{Z}$. En reportant dans la dernière égalité on a $12z \equiv 1\ [7]$ soit $5z \equiv 1[7]$ puis $z \equiv 3[7]$ car 3 est l'inverse de 5 modulo 7. Ainsi $z = 3 + 7t, t \in \mathbb{Z}$ et finalement $x =_2 + 12(3 + 7t) = 34 + 84t, t \in \mathbb{Z}$.

Application 35 (ROM 291)**.**

$$\begin{cases} k \equiv a_1\ [n_1] \\ k \equiv a_2\ [n_2] \end{cases}$$

a des solutions si et seulement si $\delta = n_1 \wedge n_2$ divise $a_2 - a_1$

Une autre app du thm chinois : Si $n \geq 2$ avec $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$, on a $\varphi(n) = \prod\limits_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$.

3.2 Théorème de Fermat

Théorème 36 (TL1 138)**.** [dernier théorème de Fermat, admis] Pour des entiers $n \leq 3$ et $xyz \neq 0$, l'égalité $x^n + y^n = z^n$ est impossible.

Exemple 37 (No ref)**.** Pour $n = 2$, $(x, y, z) = (3, 4, 5)$ est une solution de cette équation.

Théorème 38 (ORAUX XENS Al1)**.** [Théorème de Sophie Germain][DEV 2] Soit p un nombre premier de Sophie Germain, i.e. tel que p est impair et $q = 2p + 1$ est premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tels que $xyz \not\equiv 0$ $[p]$ et $x^p + y^p + z^p = 0$

3.3 Irréductibilité des polynômes dans $\mathbb{Q}[X]$

Définition 39 (ROM 382)**.** Le contenu d'un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ est l'entier $c(P) = pgcd(a_0, .., a_n)$.
Si $c(P) = 1$, on dit que P est primitif

Lemme 40 (GOU 62)**.** Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. Si p divise tous les coefficients de PQ, alors p divise tous les coefficients de P ou tous ceux de Q.

Lemme 41 (GOU 62)**.** [Gauss] Si $P, Q \in \mathbb{Z}[X]$ alors $c(PQ) = c(P)c(Q)$.

Lemme 42 (GOU 62)**.** Si $\phi \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.

Théorème 43 (GOU 62)**.** [critère d'Eisenstein] Soit $P = a_n X^n + .. + a_1 X + a_n \in \mathbb{Z}[X]$ et p un nombre premier. Si on a :

1. p ne divise pas a_n
2. p divide a_i, pour tout $1 \leq i \leq n - 1$
3. p^2 ne divise pas a_0

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

Application 44 (GOU 62)**.** Si p est premier, $\phi(X) = X^{p-1} + ... + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

Avoir en tête idée du cryptage RSA