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

Mathieu Alix

–

1 Rapport du Jury

« Il est attendu de construire rapidement $\mathbb{Z}/n\mathbb{Z}$, puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution des systèmes de congruences.

Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème RSA. Si des applications en sont proposées, l'étude des morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ ou le morphisme de Frobenius peuvent figurer dans la leçon.

Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$, au logarithme discret, ou à la transformée de Fourier rapide. »

2 Questions classiques

1. Résoudre dans $\mathbb{Z}$ la congruence suivante : $3x = 4 \mod [7]$.

   Solution: 3 étant premier avec 7, il est inversible dans $\mathbb{Z}/7\mathbb{Z}$, on vérifie rapidement que 5 est l'inverse de 3 dans $\mathbb{Z}/7\mathbb{Z}$, de sorte que l'équation se réécrit $x = 20 \mod [7] = -1 \mod [7]$,

2. Résoudre dans $\mathbb{Z}$ la congruence $9x = 12 \mod [21]$.

   Solution: En observant que $21 = 7 \times 3$, alors par le théorème chinois, il suffit de vérifier l'équation modulo 3 et modulo 7. Or, mod 3, l'équation se réécrit $0x = 0 \mod [3]$, et est donc toujours vérifiées. mod 7, on obtient $2x = -2 \mod [7]$, or 2 et 7 sont premiers entre eux, donc 2 est inversible dans $\mathbb{Z}/7\mathbb{Z}$, et son inverse est -3, on obtient ainsi que $x = -1 \mod [7]$, c'est donc le résultat final.

3. Montrer que $n^7 = n \mod [42]$.

Solution: On a $42 = 2\times3\times7$, alors par le théorème des restes chinois, il suffit de vérifier la congruence modulo $2, 3$ et 7. Pour 2 et 3, on a clairement que $n^7 = n$, et pour 7 le résultat découle du petit théorème de Fermat.

4. Calculer $\varphi(150)$

Solution: On commence par remarque que $150 = 2\times3\times5^2$, donc en utilisant les propriétés sur l'indicatrice d'Euler :

$$\begin{aligned}\varphi(150) &= \varphi(2)\times\varphi(3)\times\varphi(5^2) \text{ (multiplicativité premiers entre eux)}\\ &= 1\times(3-1)\times(5^2-5) \ (\varphi(p^k) = p^k - p^{k-1} \text{ pour } k \geq 1)\\ &= 2\times20 = 40\end{aligned}$$

5. Donner les morphismes de groupe de $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ puis ceux de $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$. Trouver une CNS sur m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ soit nul.

Solution: À rédiger, $pgcd(n, m) = 1$. Voir [ROM] page 282/295

6. $\mathbb{Z}/n\mathbb{Z}$ est-il principal ? Déterminer ses idéaux ? lesquels sont premiers ? maximaux ?

Solution: La principalité nécessite d'office l'intégrité, qui n'a lieu ssi $n \in \mathcal{P}$. Dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ est un corps et n'a que deux idéaux qui sont lui même et $\{0\}$. pour les autres n non premiers, $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal, et ses idéaux sont de la forme $d\mathbb{Z}/n\mathbb{Z}$, ils sont donc principaux. pour le caractère premier, on utilise la bijection des ideaux quotients, ce qui nous assure que les $p\mathbb{Z}/n\mathbb{Z}$ pour $p|n$ premiers sont les idéaux premiers. Pour les maximaux, il faut regarder si le quotient formé est un corps ?

7. Donner une construction de $\mathbb{F}_4$.

Solution: On vérifie que dans $\mathbb{F}_2[X]$ le polynôme X^2+X+1 est irréductible donc on peut construire $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$. (c'est un corps fini de cardinal 2).

8. Est-il possible de construire un corps fini à 6 éléments ?

Solution: Non ce n'est pas une puissance d'un premier.

9. On considère l'équation $(E) : x^2 + 2x - 3 = 0$.
   (a) Résoudre l'équation dans $\mathbb{Z}/7\mathbb{Z}$.
   (b) Résoudre l"équation dans $\mathbb{Z}/21\mathbb{Z}$.

Solution:

a) Dans $\mathbb{Z}/7\mathbb{Z}$, on a

$$x^2+2x-3 = x^2+2x+1-4 = (x+1)^2-2^2 = ((x+1)-2)(x+1)+2) = (x-1)(x+3)$$

Comme 7 est premier, alors $\mathbb{Z}/7\mathbb{Z}$ est un corps et donc intègre (n'a pas de diviseur de 0). Par conséquent les solutions sont $x = 1$ où $x = -3$.

b) Comme $21 = 3 \times 7$, les multiples de 3 et les multiples de 7 sont des diviseurs de 0. Les diviseurs de zéros dans $\mathbb{Z}/21\mathbb{Z}$ sont donc $3, 6, 7, 9, 12 = -9, 14 = -7, 15 = -6; 18 = -3$. Ainsi $x^2 + 2x - 3 = (x-1)(x+1) = 0$ dans $\mathbb{Z}/21\mathbb{Z}$ si et seulement si $x = 1$ ou $x = -3$ ou

$$(x-1, x+3) \in \{(\pm 3, \pm 7), (\pm 6, \pm 7), (\pm 7, \pm 3), (\pm 7, \pm 6), (\pm 7, \pm 9), (\pm 9, \pm 7)\}$$

3 Question plus exotique ?

1. Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un entier pair. Quid de $\varphi(2)$?

Solution: Pour $n \geq 3$, on a $\overline{(-1)} \neq \overline{1}$ et $\overline{(-1)}^2 = \overline{(-1)^2} = \overline{1}$, donc $\overline{(-1)}$ est d'ordre 2 qui va diviser l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ c'est à dire $\varphi(n)$.

Pour $n = 2, \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, et donc $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$ et donc $\varphi(2) = 1$.

2. Soient $n \geq 2$ et $m \geq 2$ deux entiers. Montrer que l'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/pgcd(n,m)\mathbb{Z} \times \mathbb{Z}/ppcm(n,m)\mathbb{Z}$.

Solution:

* Si $pgcd(n,m) = 1$ alors $ppcm(n,m) = nm$, et le théorème des restes chinois permet de conclure.
* Pour $\delta = pgcd(n,m) \geq 2$, on écrit les décompositions en facteurs premiers de n et m sous la forme, $n = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{k} p_i^{\beta_i}$ où les premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i et β_i étant positifs ou nuls. On a donc :

$$\delta = pgcd(n,m) = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{k} p_i^{\alpha_i} \text{ et } \mu = ppcm(n,m) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{k} p_i^{\beta_i}$$

et le théorème chinois donne les isomorphismes d'anneaux

$$\begin{aligned}\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z} &\simeq \prod_{i=1}^{k} \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \times \prod_{i=k+1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_{i=k+1}^{k} \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \\ &\simeq \prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_{i=k+1}^{t} \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \times \prod_{i=1}^{k} \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \times \prod_{i=k+1}^{k} \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \\ &\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\end{aligned}$$

3. Soit A un anneau commutatif. On dit que A est local si l'ensemble de ses éléments non inversibles $V(A)$ est un idéal.
   (a) Soit $m = p^n$ avec $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Démontrer que $\mathbb{Z}/m\mathbb{Z}$ est local.
   (b) Soit $m \geq 2$. Démontrer que $\mathbb{Z}/m\mathbb{Z}$ est local si et seulement s'il existe $p \in \mathcal{P}, n \in \mathbb{N}^*$ tel que $m = p^n$.

Solution:

a) On sait que $\overline{k}$ est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$ si et seulement si $pgcd(k, p^n) = 1$, c'est à dire si et seulement si $pgcd(k, p) = 1$. Ainsi $V(\mathbb{Z}/p^n\mathbb{Z}) = \{\overline{pk}, k \in \mathbb{Z}\}$. On vérifie alors aisément que c'est un idéal..

b) La réciproque a été vérifiée dans la question précédente, il suffit donc de regarder l'implication directe qu'on effectue par contraposée. Supposons que m admette deux diviseurs premiers distincts p et q. Alors par ce qui précède $\overline{p}, \overline{q} \in V(\mathbb{Z}/m\mathbb{Z})$. De plus, puisqu'ils sont deux premiers distincts, ils sont premiers entre eux, et donc par le théorème de Bezout :

$$\exists (u, v) \in \mathbb{Z}^2, pu + qv = 1 \text{ et donc dans } \mathbb{Z}/m\mathbb{Z}, \overline{pu} + \overline{qv} = \overline{1}.$$

Ainsi si $V(\mathbb{Z}/m\mathbb{Z}$ était un un idéal de $\mathbb{Z}/m\mathbb{Z}$, alors $\overline{1}$ serait un élément de $V(\mathbb{Z}/m\mathbb{Z})$ et donc on aurait $\mathbb{Z}/m\mathbb{Z} = V(\mathbb{Z}/m\mathbb{Z})$, ce qui est impossible. D'où la contraposée.

4. Application au calcul de carré dans les corps finis -> symbole de legendre etc..
5. Réduction modulo p pour trouver de bonnes propriétés (irreductiblité des Φ_n ou encore entier de Gauss)