Agrégation interne · DM

DM n°05 — Anneaux Z/nZ, éléments inversibles et théorème des restes chinois

CHAPITRES

Congruences et PGCD · Anneaux Z/nZ et éléments inversibles · Diviseurs de zéro et idéaux · Théorème des restes chinois · Indicatrice d'Euler, idempotents et équations polynomiales

> *Pour $N \geqslant 2$, deux entiers x et y sont congrus modulo N lorsque N divise $x - y$. On écrit alors $x \equiv y \pmod N$. Multiplier un entier puis ne conserver que son reste modulo N peut préserver tous les restes possibles ou, au contraire, en confondre plusieurs. Nous allons déterminer exactement quand chacun de ces phénomènes se produit, puis introduire les objets algébriques qui permettent de les décrire. Nous étudierons enfin ce qui se passe lorsqu'une même classe est observée simultanément modulo deux entiers.*

I Multiplier modulo N

1 Pour $a \in \mathbb{Z}$, on note T_a l'application qui, à $x \in \{0, \dots, 11\}$, associe le reste de ax dans la division euclidienne par 12.

(a) Déterminer les valeurs prises par T_5. Combien chaque élément de $\{0, \dots, 11\}$ possède-t-il d'antécédents ?

(b) Déterminer les valeurs prises par T_8. Combien chacun des éléments effectivement atteints possède-t-il d'antécédents ?

(c) Résoudre, parmi les entiers $x \in \{0, \dots, 11\}$,

$$5x \equiv 7 \pmod{12}, \qquad 8x \equiv 4 \pmod{12}, \qquad 8x \equiv 2 \pmod{12}.$$

Quelle différence arithmétique entre 5 et 8, relativement à 12, distingue les deux comportements observés ?

2 Soient $N \geqslant 2$ et $a \in \mathbb{Z}$. On pose $d = \mathrm{PGCD}(a, N)$.

(a) Soient $u, v, w \in \mathbb{Z}$. Montrer que

$$\mathrm{PGCD}(u, v) = 1 \quad \text{et} \quad v \mid uw \quad \Longrightarrow \quad v \mid w.$$

(b) Montrer que, pour tous $x, y \in \mathbb{Z}$,

$$ax \equiv ay \pmod N \quad \Longleftrightarrow \quad x \equiv y \pmod{N/d}.$$

(c) On définit maintenant T_a sur $\{0, \dots, N-1\}$ comme à la question 1. Montrer que tout élément de l'image de T_a possède exactement d antécédents. En déduire que T_a est bijective si et seulement si $\mathrm{PGCD}(a, N) = 1$.

3 Soient $a, b \in \mathbb{Z}$, $N \geqslant 2$ et $d = \mathrm{PGCD}(a, N)$. Montrer que la congruence

$$ax \equiv b \pmod N$$

admet une solution si et seulement si $d \mid b$. Lorsqu'elle en possède une, montrer qu'elle possède exactement d solutions modulo N. Si x_0 est l'une d'elles, les décrire toutes.

4 On dira qu'un entier b est un **inverse de a modulo N** lorsque $ab \equiv 1 \pmod{N}$. Montrer que a possède un inverse modulo N si et seulement si $\mathrm{PGCD}(a, N) = 1$, et que cet inverse est alors unique modulo N.

Déterminer l'inverse de 37 modulo 101, puis résoudre

$$37x \equiv 23 \pmod{101}.$$

II Les classes modulo N

Dans toute cette partie, $N \geqslant 2$ est fixé.

5 On définit sur $\mathbb{Z}$ la relation

$$a \sim b \iff a \equiv b \pmod{N}.$$

(a) Montrer que $\sim$ est une relation d'équivalence. Pour $a \in \mathbb{Z}$, on appelle **classe de a modulo N** l'ensemble

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{N}\}.$$

(b) Montrer que toute classe est égale à l'une des classes $\overline{0}, \overline{1}, \ldots, \overline{N-1}$, et que celles-ci sont deux à deux distinctes. On note désormais

$$\mathbb{Z}/N\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{N-1}\}.$$

6 Soient $\overline{a}, \overline{b} \in \mathbb{Z}/N\mathbb{Z}$. Choisissons des représentants $a, b \in \mathbb{Z}$.

(a) Montrer que les classes $\overline{a+b}$ et $\overline{ab}$ ne dépendent pas du choix des représentants. On définit alors

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a}\,\overline{b} = \overline{ab}.$$

On appelle **anneau commutatif unitaire** un ensemble muni d'une addition et d'une multiplication telles que : l'addition est associative et commutative, possède un élément neutre 0, et tout élément possède un opposé ; la multiplication est associative et commutative et possède un élément neutre 1 ; la multiplication est distributive par rapport à l'addition.

(b) Justifier que les opérations précédentes font de $\mathbb{Z}/N\mathbb{Z}$ un anneau commutatif unitaire. Identifier son 0, son 1 et l'opposé de $\overline{a}$.

7 Dans un anneau commutatif unitaire, un élément u est dit **inversible** s'il existe un élément v tel que $uv = 1$.

(a) Si $a' \equiv a \pmod{N}$, montrer que $\mathrm{PGCD}(a', N) = \mathrm{PGCD}(a, N)$.

(b) Montrer que

$$\boxed{\overline{a} \text{ est inversible dans } \mathbb{Z}/N\mathbb{Z} \iff \mathrm{PGCD}(a, N) = 1.}$$

(c) On note $(\mathbb{Z}/N\mathbb{Z})^\times$ l'ensemble des éléments inversibles. Un **groupe** est un ensemble muni d'une loi associative, possédant un élément neutre, dans lequel tout élément possède un inverse. Montrer que $(\mathbb{Z}/N\mathbb{Z})^\times$, muni de la multiplication, est un groupe.

8 Un élément non nul z d'un anneau commutatif est appelé **diviseur de zéro** s'il existe un élément non nul w tel que $zw = 0$.

(a) Soit $\overline{a} \neq \overline{0}$ dans $\mathbb{Z}/N\mathbb{Z}$. Montrer que

$$\boxed{\overline{a} \text{ est un diviseur de zéro } \iff \text{PGCD}(a, N) > 1.}$$

(b) Un **corps commutatif** est un anneau commutatif unitaire, avec $0 \neq 1$, dans lequel tout élément non nul est inversible. Montrer que les trois propriétés suivantes sont équivalentes :

N est premier;
tout élément non nul de $\mathbb{Z}/N\mathbb{Z}$ est inversible;
$\mathbb{Z}/N\mathbb{Z}$ ne possède aucun diviseur de zéro.

En déduire que $\mathbb{Z}/N\mathbb{Z}$ est un corps si et seulement si N est premier.

III Réductions naturelles et idéaux

Lorsque plusieurs modules interviennent, on note $[x]_q$ la classe de l'entier x modulo q.

9 Soient $r, s \geqslant 2$. Considérons la formule

$$\rho_{r,s}([x]_r) = [x]_s.$$

(a) Déterminer une condition nécessaire et suffisante sur r et s pour que cette formule définisse une application de $\mathbb{Z}/r\mathbb{Z}$ dans $\mathbb{Z}/s\mathbb{Z}$.

Une application $f : A \to B$ entre deux anneaux commutatifs unitaires est appelée **morphisme d'anneaux** lorsqu'elle préserve 0, 1, l'addition et la multiplication. Son **noyau** est

$$\ker f = \{x \in A \mid f(x) = 0\}.$$

(b) Lorsque la condition précédente est satisfaite, montrer que $\rho_{r,s}$ est un morphisme d'anneaux surjectif.

(c) Déterminer explicitement $\ker \rho_{r,s}$, puis calculer $|\ker \rho_{r,s}|$.

10 Soit $N \geqslant 2$. Une partie I d'un anneau commutatif A est appelée **idéal** lorsque $0 \in I$, et lorsque, pour tous $x, y \in I$ et $a \in A$,

$$x - y \in I \qquad \text{et} \qquad ax \in I.$$

(a) Montrer que le noyau d'un morphisme d'anneaux est un idéal.

(b) Pour tout diviseur positif d de N, on pose

$$I_d = \{[kd]_N \mid k \in \mathbb{Z}\} \subset \mathbb{Z}/N\mathbb{Z}.$$

Montrer que $I_d = \ker \rho_{N,d}$.

(c) Montrer réciproquement que tout idéal de $\mathbb{Z}/N\mathbb{Z}$ est égal à I_d pour un unique diviseur positif d de N.

IV Deux congruences à la fois

Soient désormais $m, n \geqslant 2$. On munit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ de l'addition et de la multiplication composante par composante. On obtient ainsi un anneau commutatif unitaire.

11 On définit

$$\Phi_{m,n} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad \Phi_{m,n}([x]_{mn}) = ([x]_m, [x]_n).$$

(a) Montrer que $\Phi_{m,n}$ est bien définie et qu'il s'agit d'un morphisme d'anneaux.

(b) En posant $\ell = \text{PPCM}(m, n)$, montrer que le noyau de $\Phi_{m,n}$ est constitué exactement des classes $[k\ell]_{mn}$, où $k \in \mathbb{Z}$. Calculer $|\ker \Phi_{m,n}|$.

(c) En déduire que $\Phi_{m,n}$ est injective si et seulement si m et n sont premiers entre eux.

12 On suppose dans cette question que $\text{PGCD}(m, n) = 1$.

(a) Justifier qu'il existe $u, v \in \mathbb{Z}$ tels que

$$um + vn = 1.$$

Fixer un tel couple (u, v) et poser dans $\mathbb{Z}/mn\mathbb{Z}$

$$e_m = [vn]_{mn}, \qquad e_n = [um]_{mn}.$$

(b) Calculer $\Phi_{m,n}(e_m)$ et $\Phi_{m,n}(e_n)$.

(c) Soient $a, b \in \mathbb{Z}$. Montrer que la classe $[avn + bum]_{mn}$ a pour image $([a]_m, [b]_n)$.

(d) En déduire que $\Phi_{m,n}$ est un isomorphisme d'anneaux, c'est-à-dire un morphisme bijectif, et établir

$$\boxed{\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.}$$

(e) Montrer que

$$e_m + e_n = 1, \qquad e_m e_n = 0, \qquad e_m^2 = e_m, \qquad e_n^2 = e_n.$$

Un élément e vérifiant $e^2 = e$ est appelé **idempotent**. Pour $x \in \mathbb{Z}/mn\mathbb{Z}$, déterminer les images par $\Phi_{m,n}$ de xe_m et xe_n.

13 On ne suppose plus m et n premiers entre eux. On pose $d = \text{PGCD}(m, n)$ et $\ell = \text{PPCM}(m, n)$.

(a) Montrer qu'un couple $([a]_m, [b]_n)$ appartient à l'image de $\Phi_{m,n}$ si et seulement si $a \equiv b \pmod{d}$. Vérifier en particulier que cette condition ne dépend pas du choix des représentants a et b.

(b) Lorsque cette condition est satisfaite, montrer que les solutions du système

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

forment une unique classe modulo ℓ. Déterminer le nombre de classes distinctes modulo mn contenant des solutions de ce système.

(c) En déduire que $\Phi_{m,n}$ est un isomorphisme si et seulement si $\text{PGCD}(m, n) = 1$.

(d) Pour $m = 4$ et $n = 6$, expliquer pourquoi

$$x \equiv 0 \pmod{4}, \qquad x \equiv 1 \pmod{6}$$

n'a pas de solution, puis déterminer toutes les classes modulo 24 satisfaisant

$$x \equiv 1 \pmod{4}, \qquad x \equiv 3 \pmod{6}.$$

V Lire des propriétés dans la décomposition

14 Pour tout entier $N \geqslant 2$, on définit l'indicatrice d'Euler par

$$\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times.$$

(a) Soient A et B deux anneaux commutatifs unitaires. Montrer qu'un élément (a, b) de $A \times B$ est inversible si et seulement si a est inversible dans A et b inversible dans B.

(b) Lorsque $\mathrm{PGCD}(m, n) = 1$, en déduire une bijection compatible avec la multiplication

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,$$

puis $\varphi(mn) = \varphi(m)\varphi(n)$.

(c) Si p est premier et $\alpha \geqslant 1$, montrer que

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

(d) Si $N = \prod_{i=1}^r p_i^{\alpha_i}$ est la décomposition de N en facteurs premiers, en déduire que

$$\boxed{\varphi(N) = N \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).}$$

15 **(a)** Montrer que si $n_1, \ldots, n_r \geqslant 2$ sont deux à deux premiers entre eux, alors

$$\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}.$$

(b) Soient p premier et $\alpha \geqslant 1$. Montrer que les seuls idempotents de $\mathbb{Z}/p^\alpha\mathbb{Z}$ sont 0 et 1.

(c) Si $N = \prod_{i=1}^r p_i^{\alpha_i}$ est la décomposition de N en facteurs premiers, en déduire que $\mathbb{Z}/N\mathbb{Z}$ possède exactement 2^r idempotents.

(d) Déterminer tous les idempotents de $\mathbb{Z}/60\mathbb{Z}$, sans tester successivement les 60 classes.

16 Soit

$$P(X) = a_0 + a_1 X + \cdots + a_r X^r \in \mathbb{Z}[X].$$

Pour tout entier $q \geqslant 2$ et tout $x \in \mathbb{Z}/q\mathbb{Z}$, on note

$$P(x) = [a_0]_q + [a_1]_q x + \cdots + [a_r]_q x^r.$$

(a) Lorsque $\mathrm{PGCD}(m, n) = 1$, montrer que

$$\Phi_{m,n}(P(x)) = \big(P(x_m), P(x_n)\big),$$

où $\Phi_{m,n}(x) = (x_m, x_n)$. En déduire que les racines de P dans $\mathbb{Z}/mn\mathbb{Z}$ correspondent bijectivement aux couples formés d'une racine modulo m et d'une racine modulo n.

(b) Soit $N = n_1 \cdots n_r$, où les $n_i \geqslant 2$ sont deux à deux premiers entre eux. Montrer que les racines de P modulo N correspondent bijectivement aux r-uplets formés d'une racine de P modulo chacun des n_i.

(c) Déterminer toutes les solutions modulo 105 de

$$x^2 \equiv 1 \pmod{105}.$$