27

Algèbre modulaire

I Congruences

Définition 1 : Rappel : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b \ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Propriété 1 : Rappel : Relation d'équivalence

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété 2 : Rappel : Nombre d'entiers modulo n

$\forall a \in \mathbb{Z}, \ \exists! r \in [\![0, n-1]\!], \ a \equiv r \ [n]$. r est le reste de la division euclidienne de k par n.
Ainsi, la relation d'équivalence $\cdot \equiv \cdot \ [n]$ possède exactement n classes d'équivalences.

Propriété 3 : Rappel : Compatibilité de $+$ et $\times$

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \ [n]$ et $c \equiv d \ [n]$. Alors $a + c \equiv b + d \ [n]$ et $a \times c \equiv b \times d \ [n]$.
Plus généralement, si $m \in \mathbb{N}$, $a^m \equiv b^m \ [n]$.

II Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$ fixé.

Définition 2 : $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble (quotient) des n classes d'équivalences de $\cdot \equiv \cdot \ [n]$, notées $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Ainsi

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

Remarque

R 1 – $\overline{k}$ est l'ensemble des entiers congrus à k modulo n, donc l'ensemble des $k + n\ell$ pour $\ell \in \mathbb{Z}$.
On peut toujours se ramener à un entier r entre 0 et $n-1$ en prenant le reste de la division euclidienne de k par n : $k \equiv r \ [n]$ donc $\overline{k} = \overline{r} = \overline{r + pn}$ pour tout $p \in \mathbb{Z}$.

Définition 3 : Surjection canonique

L'application surjective $\left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array} \right.$ est appelée **surjection canonique**.

Lemme 1 : Compatibilité avec $+$

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors

$$\overline{a+b} = \overline{c+d}$$

Ce lemme rend licite la définition suivante, car la somme de deux entiers modulo n ne dépend pas du choix de leurs représentants.

Définition 4 : Loi +

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$, ce qui définit une loi de composition interne + sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 4 : Structure de groupe additif

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif isomorphe à $(\mathbb{U}_n, \times)$.

Remarque

R 2 – On a alors facilement, pour $k \in \mathbb{Z}$, $k \cdot \overline{a} = \overline{ka}$.

Exemple

E 1 – Table d'addition dans $\mathbb{Z}/4\mathbb{Z}$.

III Groupes monogènes

1 Sous-groupe engendré par une partie

Définition 5 : Rappel : Groupe engendré par une partie, groupe monogène, groupe cyclique

Soit $(G, *)$ un groupe, A partie non vide de G.

- On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A \rangle$.
  On dit alors que A est une **partie génératrice** de $\langle A \rangle$.
- Les éléments de $\langle A \rangle$ sont exactement les produits (pour $*$) d'éléments de A ou de A^{-1}.
  Autrement dit, $x \in \langle A \rangle$ si et seulement s'il existe $k \in \mathbb{N}$, $(a_1, \dots, a_k) \in A^k$ et $(\varepsilon_1, \dots, \varepsilon_k) \in \{-1, 1\}^k$ tel que
$$x = a_1^{\varepsilon_1} * \cdots * a_k^{\varepsilon_k}.$$

Version additive : $x = \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k$

- Soit $a \in G$. Le sous-groupe **engendré par** a noté $\langle a \rangle$ plutôt que $\langle \{a\} \rangle$ est
$$\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$$
  On dit que a en est un **générateur**.
- Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \langle a \rangle$.
- Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

Version additive : $\langle a \rangle = \{ka,\ k \in \mathbb{Z}\}$

Propriété 5 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, dont les générateurs sont exactement les $\overline{k}$ où $k \wedge n = 1$

Remarque

R 3 – De même, les générateurs de $\mathbb{U}_n$ sont les $e^{\frac{2ik\pi}{n}}$ avec $k \wedge n = 1$, appelées **racines primitives n^e de l'unité.**

Exemple : À observer sur un dessin

E 2 – Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n = 5$ par exemple.

Propriété 6 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$

Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

IV ANNEAU $\mathbb{Z}/n\mathbb{Z}$

1 Structure

Lemme 2 : Compatibilité avec $\times$

Soient $a,b,c,d \in \mathbb{Z}$ tels que $\overline{a}=\overline{c}$ et $\overline{b}=\overline{d}$. Alors

$$\overline{a \times b} = \overline{c d}$$

Ce lemme rend licite la définition suivante, car le produit de deux entiers modulo n ne dépend pas du choix de leurs représentants.

Définition 6 : Loi $\times$

Si $a,b \in \mathbb{Z}$, on pose $\overline{a} \times \overline{b} = \overline{ab}$, ce qui définit une loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 7 : Structure d'anneau

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Propriété 8 : Groupe des inversible

Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des $\overline{k}$ pour $k \in \mathbb{Z}$ tel que $k \wedge n = 1$

Méthode 1 : Calcul de l'inverse d'un élément inversible

Si $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (donc si $k \wedge n = 1$), on trouve l'inverse de $\overline{k}$ soit « de tête », soit en utilisant l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre k et n.

Exemple

E 3 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E 4 – Inverse de $\overline{23}$ dans $\mathbb{Z}/120\mathbb{Z}$.

Corollaire 1 : CNS pour avoir un corps

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si et seulement si p est premier.

On le note parfois $\mathbb{F}_p$. (« corps fini à p éléments »)

2 Théorème Chinois

Théorème 1 : chinois

Soient $n,m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

1re formulation *Si $a,b \in \mathbb{Z}$, alors*

$$\begin{cases} k \equiv a \ [n] \\ k \equiv b \ [m] \end{cases} \iff k \equiv c \ [nm]$$

où c est une solution particulière, qui existe bien.

2e formulation *Pour tout $k \in \mathbb{Z}$, note $(k \bmod n)$, $(k \bmod m)$ et $(k \bmod nm)$ les classes de k dans $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ respectivement. On a alors*

(i) Si $k,\ell \in \mathbb{Z}$, et si

$$(k \bmod nm) = (\ell \bmod nm),$$

alors

$$(k \bmod n) = (\ell \bmod n)$$

et

$$(k \bmod m) = (\ell \bmod m).$$

(ii) L'application bien définie

$$f : \left| \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array} \right.$$

est un isomorphisme d'anneaux.

Le résultat s'étend à un nombre fini d'entiers premiers entre eux deux à deux.

Méthode 2 : Résolution de système de congruences

Trouver une solution particulière au système de congruence se fait soit en testant les valeurs, soit en trouvant des entiers de Bézout : on a $u, v \in \mathbb{Z}$ tels que $n \cdot u + m \cdot v = 1$. Alors

$$c = nub + mva$$

est une solution particulière car $nu \equiv 1 \ [m]$ et $mv \equiv 1 \ [n]$.

On peut aussi résoudre directement le système en remarquant qu'il est équivalent à $k = a + n \cdot u = b + m \cdot v$ avec $u, v \in \mathbb{Z}$ et en résolvant l'équation diophantienne $n \cdot u - m \cdot v = b - a$ par la méthode habituelle.

Démonstration

1re formulation La méthode ci-dessus donne l'existence d'une solution particulière c.

Puis

$$\begin{cases} k \equiv a \ [n] \\ k \equiv b \ [m] \end{cases} \iff \begin{cases} k \equiv c \ [n] \\ k \equiv c \ [m] \end{cases}$$
$$\iff k - c \text{ est divisible par } n \text{ et } m$$
$$\underset{n \wedge m = 1}{\iff} nm \mid (k - c)$$
$$\iff k \equiv c \ [nm].$$

2e formulation

(i) $k \equiv \ell \ [nm]$ donc $nm \mid (k - \ell)$ donc $n \mid (k - \ell)$ et $m \mid (k - \ell)$ donc $k \equiv \ell \ [n]$ et $k \equiv \ell \ [m]$.

(ii) f est bien définie d'après (i).

Puis, pour $k, \ell \in \mathbb{Z}$, par définition des additions sur $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

$$\begin{aligned} f\Big((k \bmod nm) + (\ell \bmod nm)\Big) &= f\Big((k+\ell) \bmod nm\Big) \\ &= \Big((k+\ell) \bmod n, (k+\ell) \bmod m\Big) \\ &= (k \bmod n, k \bmod m) + (\ell \bmod n, \ell \bmod m) \\ &= f\Big(k \bmod nm\Big) + f\Big(\ell \bmod nm\Big) \end{aligned}$$

On montre exactement de la même manière que

$$f\Big((k \bmod nm) \times (\ell \bmod nm)\Big) = f\Big(k \bmod nm\Big) \times f\Big(\ell \bmod nm\Big)$$

On a enfin que

$$f(1 \bmod nm) = (1 \bmod n, 1 \bmod m) = 1_{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}.$$

Donc f est un morphisme d'anneaux.

La bijectivité correspond à la 1re méthode. Mais elle peut se retrouver plus facilement : comme le cardinal est le même au départ et à l'arrivée, on se contente de montrer l'injectivité (qui équivaut alors à la bijectivité) : si $f(k \bmod nm) = 0_{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}$, alors $\begin{cases} k \equiv 0 \ [n] \\ k \equiv 0 \ [m] \end{cases}$ donc $k \equiv 0 \ [nm]$ soit en utilisant la première formulation, soit en remarquant que $n \mid k$, $m \mid k$ et $n \wedge m = 1$ donc $nm \mid k$.

Finalement, $\operatorname{Ker} f = \{0_{\mathbb{Z}/n\mathbb{Z}}\}$ et f est un isomorphisme.

Exercice 1 : CCINP 94

3 Indicatrice d'Euler

Définition 7 : Indicatrice d'Euler

L'**indicatrice d'Euler** est l'application définie sur $\mathbb{N}^*$ par $\varphi(n) = \left|\{k \in [\![1, n]\!] \mid k \wedge n = 1\}\right|$ ou $[\![0, n-1]\!]$

Remarque

R4 – $\varphi(1) = 1$.

R5 – Si $n \geqslant 2$, $\varphi(n)$ est la cardinal du groupe $U_{\mathbb{Z}/n\mathbb{Z}}$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$ (donc le nombre d'éléments inversibles). $(\mathbb{Z}/n\mathbb{Z})^\times$, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

R6 – Il s'agit aussi du nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Propriété 9 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

$$\varphi(p) = p - 1$$

Et si, plus généralement, $k \in \mathbb{N}^*$,

$$\varphi\left(p^k\right) = p^k - p^{k-1}$$

Propriété 10 : Théorème chinois avec les inversibles

Soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

(i) Si $k \in \mathbb{Z}$, et si $(k \bmod nm) \in (\mathbb{Z}/nm\mathbb{Z})^\times$ alors $(k \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $(k \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^\times$.

(ii) L'application bien définie

$$g : \left| \begin{array}{ccc} (\mathbb{Z}/nm\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array} \right.$$

est un isomorphisme de groupes (multiplicatifs).

Démonstration

(i) Si $(k \bmod nm) \in (\mathbb{Z}/nm\mathbb{Z})^\times$ alors $k \wedge (nm) = 1$ donc

$$k \wedge n = k \wedge m = 1$$

(pas de diviseur commun non trivial) donc $(k \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $(k \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^\times$.

(ii) Par (i), (et le (i) du théorème chinois), g est bien définie et comme f (du théorème chinois) était un morphisme d'anneaux, g est bien un morphisme de groupes multiplicatifs.

Comme restriction de f, g est injectif, reste à montrer la surjectivité (pas d'égalité des cardinaux cette fois : elle va servir au corollaire suivant) : soit $a, b \in \mathbb{Z}$ tel que $(a \bmod n, b \bmod m) \in (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.

Par surjectivité de f, on a $c \in \mathbb{Z}$ tel que

$$(a \bmod n, b \bmod m) = f(c \bmod nm).$$

Reste à voir si $(c \bmod nm) \in (\mathbb{Z}/nm\mathbb{Z})^\times$. Or

$$(a \bmod n) = (c \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^\times$$

et

$$(b \bmod m) = (c \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^\times$$

donc $c \wedge n = c \wedge m = 1$, donc $c \wedge (mn) = 1$ d'où $(c \bmod nm) \in (\mathbb{Z}/nm\mathbb{Z})^\times$ puis

$$(a \bmod n, b \bmod m) = g(c \bmod nm) \text{ :}$$

g est surjective. ■

Corollaire 2 : Multiplicativité de φ

φ est multiplicative, *c'est-à-dire que si $n \wedge m = 1$, alors* $\varphi(nm) = \varphi(n)\varphi(m)$

Démonstration

En effet, avec l'isomorphisme de la question précédente,

$$\left|(\mathbb{Z}/nm\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \times \left|(\mathbb{Z}/m\mathbb{Z})^\times\right|.$$

■

Corollaire 3 : Produit de plus de deux termes

Plus généralement, si $n_1, \ldots, n_r$ sont deux à deux premiers entre eux,

$$\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r).$$

Corollaire 4 : Expression à l'aide des diviseurs premiers

Si $p_1, \ldots, p_r$ sont les diviseurs premiers distincts de n,

$$\varphi(n) = n \times \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Exercice 2 : La même formule, avec des probabilités

Soit $\Omega = [\![1, n]\!]$ où n est un entier non premier supérieur ou égal à 2, muni de la probabilité uniforme. Si $d|n$, on note $A_d = \{kd \mid k \in \Omega \text{ et } kd \in \Omega\}$.

1. **Quelle est la probabilité de A_d ?**
2. **Soit P l'ensemble des diviseurs premiers de n.**
   (a) **Démontrer que $(A_p)_{p \in P}$ est une famille d'événements indépendants.**
   (b) **En déduire que $\varphi(n) = n \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.**

Exercice 3 : Une identité remarquable (et classique)

1. **Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ un diviseur de n. Parmi tous les nombres rationnels de la forme $\frac{q}{n}$ où $1 \leqslant q \leqslant n$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?**
2. **Montrer que, si $n \in \mathbb{N}^*$, $n = \sum_{k|n} \varphi(k)$.**

Théorème 2 : d'Euler

Si $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ tel que $a \wedge n = 1$, alors

$$a^{\varphi(n)} \equiv 1 \ [n]$$

Corollaire 5 : Petit théorème de Fermat

Si p est premier et $a \in \mathbb{Z}^*$ non divisible par p, alors

$$a^{p-1} \equiv 1 \ (p)$$

Dans tous les cas (que a soit divisible ou non par p),

$$a^p \equiv a \ (p)$$

Exercice 4 : CCINP 86 preuve directe de