

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 lorsque'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

$\forall a \in \mathbb{Z}, \exists ! r \in \llbracket 0, n-1 \rrbracket, a \equiv r [n]$. r est le reste de la division euclidienne de a par n .

Ainsi, la relation d'équivalence $\equiv \cdot [n]$ 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 $m \in \mathbb{N}$, $a^m \equiv b^m [n]$.

Propriété 4 : Rappel : critères de divisibilité

Si a_0, \dots, a_k sont les chiffres de n en base 10,

$$n = a_0 + a_1 \times 10 + \dots + a_k \times 10^k, \quad \text{avec } \forall i \in \llbracket 0, k \rrbracket, a_i \in \llbracket 0, 9 \rrbracket.$$

Divisibilité par 2 : $2|n \iff 2|a_0 \iff a_0 \in \{0, 2, 4, 6, 8\}$

Divisibilité par 3 : $3|n \iff 3 \left| \sum_{i=0}^k a_i \right.$

Divisibilité par 4 : $4|n \iff 4|\overline{a_1 a_0}^{10}$

Divisibilité par 5 : $5|n \iff 5|a_0 \iff a_0 \in \{0, 5\}$

Divisibilité par 8 : $8|n \iff 8|\overline{a_2 a_1 a_0}^{10}$

Divisibilité par 9 : $9|n \iff 9 \left| \sum_{i=0}^k a_i \right.$

Divisibilité par 11 : $11|n \iff 11|(a_0 - a_1 + a_2 - a_3 + \dots)$

II LE GROUPE $\mathbb{Z}/n\mathbb{Z}$

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

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

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

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

Définition 3 : Surjection canonique

L'application surjective $\begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k \longmapsto \overline{k} \end{array}$ 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 $\overline{a+b} = \overline{c+d}$.

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 5 : Structure de groupe additif

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

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

$$x = a_1^{\varepsilon_1} * \dots * a_k^{\varepsilon_k}.$$

Dans le cas d'un groupe additif $(G, +)$ cela devient

$$x = \varepsilon_1 \cdot a_1 + \dots + \varepsilon_k \cdot a_k.$$

- Soit $a \in G$. Le sous-groupe **engendré par a** noté $\langle a \rangle$ plutôt que $\langle \{a\} \rangle$ est

$$\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$$

dans le cas multiplicatif et

$$\langle a \rangle = \{k \cdot a, k \in \mathbb{Z}\}$$

dans le cas additif.

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.

**Propriété 6 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$**

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

Propriété 7 : 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 $(\mathbb{Z}/n\mathbb{Z}, +)$

**ANNEAU $\mathbb{Z}/n\mathbb{Z}$** **1 Structure****Lemme 2 : Compatibilité avec \times**

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

Définition 6 : Loi \times

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

Propriété 8 : Structure d'anneau

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

Propriété 9 : Groupe des inversible

Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ noté $U_{\mathbb{Z}/n\mathbb{Z}}$ ou $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des \bar{k} pour $k \in \mathbb{Z}$ tel que $k \wedge n = 1$.

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

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

Corollaire 1 : CNS pour avoir un corps

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

On note alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

2 Théorème Chinois**Théorème 1 : chinois (ou des restes chinois)**

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

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

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

où c est une solution particulière, qui existe bien.

2^e formulation Pour tout $k \in \mathbb{Z}$, note $(k \pmod{n})$, $(k \pmod{m})$ et $(k \pmod{nm})$ 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

$$(k \pmod{nm}) = (\ell \pmod{nm}),$$

alors

$$(k \pmod{n}) = (\ell \pmod{n})$$

et

$$(k \pmod{m}) = (\ell \pmod{m}).$$

(ii) L'application bien définie

$$f : \begin{cases} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ (k \pmod{nm}) & \longmapsto & (k \pmod{n}, k \pmod{m}) \end{cases}$$

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 $nu \equiv 1 \pmod{m}$ et $mv \equiv 1 \pmod{n}$.

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.

3 Indicatrice d'Euler**Définition 7 : Indicatrice d'Euler**

L'indicateur d'Euler est l'application définie sur \mathbb{N}^* par

$$\varphi(n) = |\{k \in \llbracket 1, n \rrbracket, n \wedge k = 1\}|.$$

Propriété 10 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

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

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

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

Théorème 3 : de Fermat-Wiles, ou grand théorème de Fermat

Si $n \in \mathbb{N}$ tel que $n \geq 3$, alors l'équation

$$x^n + y^n = z^n$$

n'admet aucune solution dans $(\mathbb{N}^*)^3$.

Propriété 11 : 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

$$g : \begin{cases} (\mathbb{Z}/nm\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{cases}$$

est un isomorphisme de groupes (multiplicatifs).

Corollaire 2 : Multiplicativité de φ

φ est multiplicative, c'est-à-dire que si $n \wedge m = 1$, alors

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Corollaire 3 : Produit de plus de deux termes

Plus généralement, si n_1, \dots, 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, \dots, p_r sont les diviseurs premiers distincts de n ,

$$\varphi(n) = n \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right).$$

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),

$$a^p \equiv a [p].$$