

Groupes cycliques et Algèbre modulaire

RÉVISIONS DE MP2I : ARITHMÉTIQUE SUR \mathbb{Z}

1 PGCD

Définition 1 : PGCD

Soient $a, b \in \mathbb{Z}$.
 $I = (a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv, u, v \in \mathbb{Z}\}$ est un idéal non réduit de $(\mathbb{Z}, +, \times)$ qui est un anneau principal.
 Son unique générateur positif est appelé **pgcd de a et b** , noté $a \wedge b$.
 On a donc, par définition, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Propriété 1 : Relation de Bézout

Si $a, b \in \mathbb{Z}$, on peut trouver $a, b \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

Propriété 2 : Propriété d'Euclide

Si $a, b, q \in \mathbb{Z}$, $a \wedge b = (a - bq) \wedge b$ (pas nécessairement une division euclidienne).

Propriété 3 : Caractérisation

Soit $(a, b) \in \mathbb{Z}^2$.

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall c \in \mathbb{Z}, (c|a \text{ et } c|b) \implies c|d \end{cases}$$

Il s'agit donc du plus grand diviseur positif au sens de la division.

Par conséquent, les diviseurs de $a \wedge b$ sont exactement les diviseurs communs de a et de b .

Définition 2 : Nombre entiers premiers entre eux

$a, b \in \mathbb{Z}$ sont dits **premiers entre eux** lorsque $a \wedge b = 1$, c'est-à-dire lorsque les seuls diviseurs communs ± 1 .

Théorème 1 : de Bézout

Soit $a, b \in \mathbb{Z}$.

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1$$

Corollaire 1

Soient $a, b, c \in \mathbb{Z}$.

- (i) $a \wedge bc = 1 \iff a \wedge b = a \wedge c = 1$
 (ii) Si $d = a \wedge b$, on a $a', b' \in \mathbb{Z}$ tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Théorème 2 : Lemme de Gauß

Soient $a, b, c \in \mathbb{Z}$. Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.



Méthode 1 : résolution des équations diophantiennes $ax + by = c$

où $a, b, c \in \mathbb{Z}^*$ sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si $d = a \wedge b | c$.

Lorsque c'est le cas, on peut trouver une solution particulière (x_0, y_0) avec l'algorithme d'Euclide par exemple.

Alors, si (x, y) solution, $ax + by = ax_0 + by_0$ puis $a(x - x_0) = b(y_0 - y)$ donc $a'(x - x_0) = b'(y_0 - y)$ avec $a' \wedge b' = 1$ en divisant par d .

Par lemme de Gauß, on a $k \in \mathbb{Z}$ tel que $x = x_0 + b'k$ puis en réinjectant $y = y_0 - a'k$.

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k), k \in \mathbb{Z}\}.$$

2 PPCM

Définition 3 : PPCM

Le PPCM de deux entiers a, b est l'unique générateur positif $a \vee b$ de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et à b .

On a donc $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Propriété 4 : du PPCM

- (i) Il s'agit du plus petit multiple positif commun à a et à b au sens de la division.
 (ii) On a toujours que $|ab| = (a \wedge b)(a \vee b)$.

3 Nombres premiers

Définition 4 : Nombre premier

Un **nombre premier** est un entier naturel $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p .

On notera \mathcal{P} l'ensemble des nombres premiers.

**Propriété 5 : d'Euclide**

L'ensemble des nombres premiers est infini.

Propriété 6 : Diviseur premier ou non

Si $p \in \mathcal{P}$ et $n \in \mathbb{Z}$, alors $p|n$ ou (exclusif) $p \wedge n = 1$.

Propriété 7 : Nombre premier divisant un produit

Soient $p \in \mathcal{P}$ et $a_1, \dots, a_n \in \mathbb{Z}$.

$p|(a_1 \times \dots \times a_n)$ si et seulement si p divise l'un des a_k .

Théorème 3 : fondamental de l'arithmétique – Décomposition primaire

Soit $n \in \mathbb{Z}^*$. On peut trouver $k \in \mathbb{N}$, p_1, \dots, p_k premiers deux à deux distincts, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

appelée décomposition primaire de n .

De plus, cette écriture est unique à l'ordre des facteurs près.

p_1, \dots, p_k sont les diviseurs premiers de n .

Définition 5 : Valuation p -adique

Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}^*$. On appelle **valuation p -adique** de n l'entier

$$v_p(n) = \max \{i \in \mathbb{N} \mid p^i \text{ divise } n\}.$$

Propriété 8 : des valuations p -adiques

Soient $n, m \in \mathbb{Z}^*$, $p \in \mathcal{P}$.

- (i) $v_p(n) \neq 0 \iff p|n$
- (ii) $v_p(n \times m) = v_p(n) + v_p(m)$
- (iii) $n|m \iff \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$
- (iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$
 $v_p(n \vee m) = \max(v_p(n), v_p(m))$

4 **Congruences****Définition 6 : 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 9 : Relation d'équivalence

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

Propriété 10 : 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 k par n .

Ainsi, la relation d'équivalence $\cdot \equiv \cdot [n]$ possède exactement n classes d'équivalences.

Propriété 11 : 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 $m \in \mathbb{N}$, $a^m \equiv b^m [n]$.

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

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

Définition 7 : $\mathbb{Z}/n\mathbb{Z}$

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

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

Définition 8 : Surjection canonique

L'application surjective $\begin{array}{l} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \\ k \mapsto \bar{k} \end{array}$ est appelée **surjection canonique**.

Lemme 1 : Compatibilité avec +

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

Définition 9 : Loi +

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

Propriété 12 : Structure de groupe additif

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

**GROUPES MONOGÈNES****1** **Sous-groupe engendré par une partie****Définition 10 : Groupe engendré par une partie**

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 $\langle A \rangle$.

Propriété 13 : Éléments 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

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

2 Groupes monogènes et cycliques

Propriété 14 : Sous-groupe engendré par un élément

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**.

Définition 11 : Groupe monogène

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 15 : 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 $k \wedge n = 1$.

3 Ordre d'un élément dans un groupe

$(G, *)$ est un groupe d'élément neutre e .

Définition 12 : Ordre d'un élément

On dit que $a \in G$ est d'**ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.

Dans ce cas, on appelle **ordre de a** le plus petit $k \in \mathbb{N}^*$ tel que $a^k = e$.

Propriété 16 : de l'ordre d'un élément

Soit a un élément de G d'ordre fini m .

- Si $k \in \mathbb{Z}$, $a^k = e$ si et seulement si $k \in m\mathbb{Z}$ ie m divise k .
- $\langle a \rangle = \{a^k, k \in \llbracket 0, m-1 \rrbracket\}$ et $|\langle a \rangle| = m$.

Propriété 17 : 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 $(\mathbb{Z}/n\mathbb{Z}, +)$

Théorème 4 : de Lagrange (HP mais très classique)

Soit $(G, *)$ un groupe fini, H un sous-groupe de G . Alors $|H|$ divise $|G|$.

Propriété 18 : de l'ordre

Soit $(G, *)$ un groupe fini de neutre e .

- (i) Tout élément de G est d'ordre fini.
- (ii) L'ordre de tout élément de G divise le cardinal de G .
- (iii) Pour tout $a \in G$, $a^{|G|} = e$.

IV 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 13 : 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 19 : Structure d'anneau

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

Propriété 20 : Groupe des inversible

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



Méthode 2 : 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 tête », soit en utilisant l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre k et n .

Corollaire 2 : CNS pour avoir un corps

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



2 Théorème Chinois

Théorème 5 : 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 $(k \bmod n)$, $(k \bmod m)$ 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

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

est un isomorphisme d'anneaux.



Méthode 3 : 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 14 : Indicatrice d'Euler

L'indicatrice d'Euler est l'application définie sur \mathbb{N}^* par $\varphi(n) = |\{k \in \llbracket 1, n \rrbracket, n \wedge k = 1\}|$.

Propriété 21 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

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

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

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

Propriété 22 : 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 $(k \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$ alors $(k \bmod n) \in U_{\mathbb{Z}/n\mathbb{Z}}$ et $(k \bmod m) \in U_{\mathbb{Z}/m\mathbb{Z}}$.

(ii) L'application bien définie

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

est un isomorphisme de groupes (multiplicatifs).

Démonstration

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

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

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

(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 $(a \bmod n, b \bmod m) \in U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}}$.

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 $(c \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$. Or

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

et

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

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

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

g est surjective. ■

Corollaire 3 : Multiplicativité de φ

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

Corollaire 4 : 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 5 : 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 6 : 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 6 : 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),

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

Théorème 7 : 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 .