Groupes cycliques et Algèbre modulaire

I Révisions de MP2I : Arithmétique sur $\mathbb{Z}$

1 PGCD

Les démonstrations sont similaires à celles vues pour les polynômes en début d'année, en remplaçant « unitaire » par « positif » et/ou ont été vues en MP2I.

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

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

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 $\boxed{d = a \wedge b | c.}$

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 :

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

Exercice 1 : Résoudre $199x + 54y = 4$ dans $\mathbb{Z}^2$.

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 $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

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

Remarque

R1 – 1 n'est pas premier.

R2 – 2 est le seul nombre premier pair.

R3 – Un nombre premier possède exactement 4 diviseurs : ± 1 et $\pm p$.

R4 – Pour qu'un nombre entier n soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et $\sqrt{n}$.

Propriété 5 : d'Euclide

L'ensemble des nombres premiers est infini.

Propriété 6 : Diviseur premier ou non

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

Propriété 7 : Nombre premier divisant un produit

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

$p|(a_1 \times \cdots \times a_n)$ 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

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

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

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

Remarque

R5 – La décomposition primaire se réécrit $n = \pm \prod_{p \in \mathscr{P},\ p|n} p^{v_p(n)} = \pm \prod_{p \in \mathscr{P}} p^{v_p(n)}$.

Propriété 8 : des valuations p-adiques

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

(i) $v_p(n) \neq 0 \iff p|n$

(ii) $v_p(n \times m) = v_p(n) + v_p(m)$

(iii) $n|m \iff \forall\, p \in \mathscr{P},\ \ v_p(n) \leqslant v_p(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$

$v_p(n \vee m) = \max(v_p(n), v_p(m))$

Remarque

R6 – Si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$$

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

Exercice 2 : Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est un carré parfait.

Exercice 3 : Exprimer le nombre de diviseurs positifs de n à l'aide de ses valuations p-adiques.

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

$\forall a \in \mathbb{Z}$, $\exists! r \in [\![0, n-1]\!]$, $a \equiv r\ [n]$. 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 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 $m \in \mathbb{N}$, $a^m \equiv b^m\ [n]$.

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

Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$ 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 $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Ainsi

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

Remarque

R 7 – $\overline{k}$ 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 8 : 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

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

Définition 9 : 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 12 : Structure de groupe additif

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

Remarque

R 8 – 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 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 $\langle A \rangle$.

Remarque

R 9 – À mettre en parallèle avec la définition de Vect en algèbre linéaire.

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 $k \in \mathbb{N}$, $(a_1, \ldots, a_k) \in A^k$ et $(\varepsilon_1, \ldots, \varepsilon_k) \in \{-1, 1\}^k$ tel que

Remarque

R 10 – On a aussi que $\langle A\rangle$ est l'intersection de tous les sous-groupes contenant A (car c'est un sous-groupe, contenant A, plus petit que tous les autres.)

Exemple

E 2 – $\mathfrak{S}_n$ est engendré par les cycles.
(*Toute permutation se décompose en produit de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.*)

E 3 – $\mathfrak{S}_n$ est engendré par les transpositions.
(*Les cycles eux-mêmes se décomposent en produit de transpositions. Cette fois, il n'y a plus unicité de la décomposition, mais seulement de la parité du nombre de termes.*)

E 4 – Soit $\mathbb{K}$ un corps. $\mathcal{GL}_n(\mathbb{K})$ est engendré par les matrices de transvection $T_{i,j}(\lambda)$ (avec $i \neq j$), de dilatation $D_i(a)$ (avec $a \neq 0$) et de permutation $P_{i,j}$.
(*C'est une conséquence du pivot de Gauß : par opérations élémentaires, on peut transformer une matrice inversible en I_n.*)

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*

*On dit que a en est un **générateur**.*

Remarque

R 11 – En notation additive, on a $\langle a\rangle = \{ka,\ k \in \mathbb{Z}\}$.

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.

Exemple

E 5 – Tout sous-groupe de $(\mathbb{Z},+)$ est

E 6 – $(\mathbb{U}_n,\times)$ est cyclique engendré par

Propriété 15 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique, dont les générateurs sont exactement les

Remarque

R 12 – 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 7 – Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n = 5$ par exemple.

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 $a^k = e$.

Remarque

R 13 – $f : \left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array}\right.$ est un morphisme de groupe donc son noyau est de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}$.
En distinguant les cas $m = 0$ et $m \neq 0$, on obtient des information sur l'ordre de a.

Exemple : À observer sur un dessin

E 8 – Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{5}$ est d'ordre 6 et $\overline{2}$ est d'ordre 3.

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*
- $\langle a\rangle =$
- $|\langle a\rangle| =$

Propriété 17 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à

Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à

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 $\overline{a}=\overline{c}$ et $\overline{b}=\overline{d}$. Alors

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

Définition 13 : 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 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 $\overline{k}$ pour $k \in \mathbb{Z}$ tel que

Méthode 2 : 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 9 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E 10 – Inverse de $\overline{23}$ dans $\mathbb{Z}/120\mathbb{Z}$.

Corollaire 2 : CNS pour avoir un corps

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

2 Théorème Chinois

Théorème 5 : 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.

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 $nu \equiv 1 \ [m]$ 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

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

$\iff k - c$ est divisible par n 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 $n \mid (k - \ell)$ 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 4 : CCINP 94

3 Indicatrice d'Euler

Définition 14 : Indicatrice d'Euler

L'**indicatrice d'Euler** est l'application définie sur $\mathbb{N}^*$ par $\varphi(n) =$

Remarque

R 14 – $\varphi(1) = 1$.

R 15 – 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).

R 16 – Il s'agit aussi du nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Propriété 21 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

$$\varphi(p) =$$

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

$$\varphi\left(p^k\right) =$$

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

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

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

Démonstration

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

$$\left|U_{\mathbb{Z}/nm\mathbb{Z}}\right| = \left|U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}}\right| = \left|U_{\mathbb{Z}/n\mathbb{Z}}\right| \times \left|U_{\mathbb{Z}/m\mathbb{Z}}\right|. \quad ■$$

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,

Exercice 5 : 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 6 : 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 6 : d'Euler

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

Corollaire 6 : Petit théorème de Fermat

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

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

Théorème 7 : de Fermat-Wiles, ou grand théorème de Fermat

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

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

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

Démonstration : Non exigible[1]

■

1. J'ai découvert une démonstration véritablement merveilleuse que ce cadre est trop étroit pour contenir...