

Groupes cycliques et Algèbre modulaire

Extrait du programme officiel :

CONTENUS

CAPACITÉS & COMMENTAIRES

Compléments sur les groupes

Sous-groupe engendré par une partie. Partie génératrice d'un groupe.

Sous-groupes du groupe $(\mathbb{Z}, +)$.

Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Groupe monogène, groupe cyclique.

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

Ordre d'un élément d'un groupe.

Si x est d'ordre fini d et si e désigne le neutre de G , alors, pour tout $n \in \mathbb{Z}$, $x^n = e \iff d|n$.

L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

Groupe des racines n -ièmes de l'unité.

L'ordre de x est le cardinal du sous-groupe de G engendré par x .

La démonstration n'est exigible que pour G commutatif.

Anneaux $\mathbb{Z}/n\mathbb{Z}$

Anneau $\mathbb{Z}/n\mathbb{Z}$.

Inversibles de $\mathbb{Z}/n\mathbb{Z}$. Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps.

Théorème chinois : isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si $m \wedge n = 1$; extension à plus de deux facteurs.

Indicatrice d'Euler φ . Calcul à l'aide de la décomposition en produits de facteurs premiers.

Théorème d'Euler.

Notation \mathbb{F}_p lorsque p est premier.

Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.

Relation $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux; expression de $\varphi(p^k)$ pour p premier.

Lien avec le petit théorème de Fermat.



Plan du cours

27 Groupes cycliques et Algèbre modulaire	1
I Révisions de MP2I : Arithmétique sur \mathbb{Z}	1
1 PGCD	1
2 PPCM	3
3 Nombres premiers	3
4 Congruences	5
II Le groupe $\mathbb{Z}/n\mathbb{Z}$	5
III Groupes monogènes	6
1 Sous-groupe engendré par une partie	6
2 Groupes monogènes et cycliques	7
3 Ordre d'un élément dans un groupe	8
IV Anneau $\mathbb{Z}/n\mathbb{Z}$	10
1 Structure	10
2 Théorème Chinois	11
3 Indicatrice d'Euler	14

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

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

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 sont ± 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 :

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

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

Ici, par l'algorithme d'Euclide, on a

$$(1) 199 = 54 \times 3 + 37 \quad (2) 54 = 37 \times 1 + 17 \quad (3) 37 = 17 \times 2 + 3 \quad (4) 17 = 3 \times 5 + 2 \quad (5) 3 = 2 \times 1 + 1$$

Donc $199 \wedge 54 = 1$ et $(5) - (4) + 6(3) - 13(2) + 19(1)$ donne $199 \times 19 - 54 \times 70 = 1$.

On a donc comme solution particulière $x_0 = 76$ et $y_0 = -280$.

Comme ci-dessus, on a ensuite (x, y) est solution de (E) si et seulement si $199(x - x_0) + 54(y - y_0) = 0$ si et seulement si $199(x - x_0) = 54(y_0 - y)$. Comme $199 \wedge 54 = 1$ et $199|54(y_0 - y)$, le théorème de Gauß donne alors $k \in \mathbb{Z}$ tel que $y_0 - y = 199k$ soit $y = -280 - 199k$. Puis, en remplaçant dans l'équation, $x = x_0 + 54k = 76 + 54k$. On vérifie aisément que la réciproque est vraie.

L'ensemble des solutions est donc $\{(76 + 54k, -280 - 199k) \mid k \in \mathbb{Z}\}$.



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.

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 $p \in \mathcal{P}$ 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

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

Remarque

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

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

Remarque

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

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

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

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

Si $\sqrt{n} = \frac{a}{b}$, alors $a^2 = n \times b^2$, $\forall p \in \mathcal{P}, 2v_p(a) = v_p(n) + 2v_p(b)$ donc $\forall p \in \mathcal{P}, v_p(n) \in 2\mathbb{N}$, donc n est un carré parfait.

Ou encore : si $\sqrt{n} = \frac{a}{b}$ sous forme irréductible, alors $a^2 = n \times b^2$ donc $b^2 | a^2$. Or $a \wedge b = 1$ donc $b^2 = a^2 \wedge b^2 = 1$ donc $n = a^2$.

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

Il s'agit de $\prod_{p \in \mathcal{P}, p|n} (v_p(n) + 1)$ vu la propriété (iii).

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 $\equiv \cdot [n]$ 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 $\equiv \cdot [n]$, notées $\bar{0}, \bar{1}, \dots, \overline{n-1}$. Ainsi

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

Remarque

R7 – \bar{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 $\bar{k} = \bar{r} = \overline{r + pn}$ pour tout $p \in \mathbb{Z}$.

Définition 8 : Surjection canonique

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

Démonstration

En effet $a \equiv c [n]$ et $b \equiv d [n]$ implique $a + b \equiv c + d [n]$. ■

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 $\bar{a} + \bar{b} = \overline{a+b}$, 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) .

Démonstration

En effet,

- + est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$,
- commutative car si $a, b \in \mathbb{Z}$, $\overline{a+b} = \overline{a+b} = \overline{b+a} = \overline{a+b}$,
- d'élément neutre $\overline{0}$ car pour tout $a \in \mathbb{Z}$, $\overline{a+0} = \overline{a+0} = \overline{a}$,
- associative car si $a, b, c \in \mathbb{Z}$,

$$(\overline{a+b}) + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + (\overline{b+c}),$$

- si $a \in \mathbb{Z}$, $\overline{a} + \overline{-a} = \overline{0}$ donc $\overline{-a} = -\overline{a}$ est l'opposé de \overline{a} .

De plus, on remarque que si $k \equiv \ell \pmod{n}$, alors $e^{\frac{2ik\pi}{n}} = e^{\frac{2i\ell\pi}{n}}$ ne dépend pas du choix du représentant de \overline{k} .

Donc $f : \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}_n, \times) \\ \overline{k} & \longmapsto & e^{\frac{2ik\pi}{n}} \end{cases}$ est

- bien définie,
- un morphisme car pour tout $k, \ell \in \mathbb{Z}$, $f(\overline{k+\ell}) = f(\overline{k})f(\overline{\ell})$,
- injectif car $\text{Ker } f = \{\overline{k}, e^{\frac{2ik\pi}{n}} = 1\} = \{\overline{k}, n|k\} = \{\overline{0}\}$
- bijectif car de plus $|\mathbb{Z}/n\mathbb{Z}| = n = |\mathbb{U}_n|$.

Remarque

R8 – On a alors facilement, pour $k \in \mathbb{Z}$, $k \cdot \overline{a} = \overline{ka}$.

Exemple

E1 – Table d'addition dans $\mathbb{Z}/4\mathbb{Z}$.



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

R9 – 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 $k \in \mathbb{N}$, $(a_1, \dots, a_k) \in A^k$ et $(\varepsilon_1, \dots, \varepsilon_k) \in \{-1, 1\}^k$ tel que

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



Démonstration

On note H l'ensemble de tels éléments.

On vérifie que H est un sous-groupe de $(G, *)$ par caractérisation (partie non vide de G stable par $*$ et par inverse).

Puis tout sous-groupe de G contenant A contient nécessairement H par stabilité.

Donc H est bien le plus petit sous-groupe de G contenant A : $H = \langle A \rangle$. ■

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

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

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 monogène.

E 6 – (\mathbb{U}_n, \times) est cyclique engendré par $e^{\frac{2i\pi}{n}}$.

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 $k \wedge n = 1$.

Démonstration

On a en effet $\mathbb{Z}/n\mathbb{Z} = \{a \cdot \bar{1}, a \in \mathbb{Z}\} = \langle \bar{1} \rangle$ fini.

Si $k \wedge n = 1$, alors on a une relation de Bézout $ku + nv = 1$ avec $u, v \in \mathbb{Z}$. Alors pour tout $a \in \mathbb{Z}$, $a = auk + nva \equiv auk \pmod{n}$ donc $\bar{a} = au\bar{k}$ donc $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle$.

Si, réciproquement, $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle$, alors on a $a \in \mathbb{Z}$ tel que $\bar{1} = a\bar{k} = \overline{ak}$ donc on a $\ell \in \mathbb{Z}$ tel que $1 = ak + n\ell$ donc $n \wedge k = 1$ par théorème de Bézout. ■

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° 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 – $f : \begin{matrix} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{matrix}$ est un morphisme de groupe donc son noyau est de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}$.

Soit $m = 0$ et a n'est pas d'ordre fini (sa seule puissance égale à e est a^0 .)

Soit $m > 0$ et m est le plus petit élément > 0 du noyau de f : il s'agit de l'ordre de a .

Exemple : À observer sur un dessin

E 8 – Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{5}$ est d'ordre 6 et $\bar{2}$ 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 $k \in m\mathbb{Z}$ ie m divise k .
- $\langle a \rangle = \{a^k, k \in [0, m - 1]\}$ et $|\langle a \rangle| = m$.

**Démonstration**

- Avec $f: \begin{cases} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{cases}$, $\text{Ker } f = m\mathbb{Z}$ d'où le résultat.
- On a déjà $\{a^k, k \in \llbracket 0, m-1 \rrbracket\} \subset \langle a \rangle$.
Puis, si $k \in \mathbb{Z}$, par division euclidienne, on a $q, r \in \mathbb{Z}$ tel que $k = mq + r$ avec $0 \leq r \leq m-1$ et alors $a^k = (a^m)^q * a^r = a^r$ d'où l'autre inclusion.
Puis, les termes sont deux à deux distincts car si $a^k = a^\ell$ avec $0 \leq k \leq \ell \leq m-1$, alors $a^{\ell-k} = e$ donc par minimalité de m , $k = \ell$.
D'où le cardinal égal à 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 $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration

Si G est engendré par a et infini, $f: \begin{cases} (\mathbb{Z}, +) & \longrightarrow & (G, *) \\ k & \longmapsto & a^k \end{cases}$ alors f est un morphisme de groupes surjectif car $G = \langle a \rangle$, et injectif car si $k \in \text{Ker } f$, $a^k = 1$ donc a d'ordre fini, donc G est fini.

Si G est engendré par a et de cardinal n , alors a est d'ordre n , donc $a^n = e$, $f: \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow & (G, *) \\ \bar{k} & \longmapsto & a^k \end{cases}$ est bien définie (quel que soit le représentant k de \bar{k} , la valeur de a^k est la même car $a^n = e$), est un morphisme de groupe et est surjectif, donc est un isomorphisme car $n = |\mathbb{Z}/n\mathbb{Z}| = |G|$. ■

Théorème 4 : de Lagrange (HP mais très classique)

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

Démonstration

On montre que la relation définie par $x\mathcal{R}y \iff x^{-1} * y \in H$ est une relation d'équivalence sur G (facile).
Puis on montre que toutes les classes d'équivalence ont même cardinal : celui de H . En effet, il s'agit des $xH = \{x * h, h \in H\}$ et l'application (translation) $f: h \mapsto x * h$ est une bijection de H sur xH (de réciproque $h \mapsto x^{-1} * h$).
Comme les classes d'équivalences forment une partition de G , $|G| = n|H|$ où n est le nombre de classes, d'où le résultat. ■

Propriété 18 : de l'ordre

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

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

Démonstration

- $\langle a \rangle$ est un sous-groupe de G , donc d'ordre fini. Donc on a $i < j$ tel que $a^i = a^j$ et $a^{j-i} = e$ avec $j-i \in \mathbb{N}^*$.
- L'ordre de a est la cardinal du sous-groupe $\langle a \rangle$ de G , donc d'après le théorème de Lagrange (HP), il divise celui de G .
Seule la démonstration dans le cas commutatif est au programme.

En effet, dans ce cas, on considère le produit $\left(\prod_{x \in G} x\right) \in G$ et on effectue le changement de variable (bijectif) $x \mapsto a * x$.

Par commutativité, on obtient $\prod_{x \in G} x = \prod_{x \in G} (a * x) = a^{|G|} \prod_{x \in G} x$. Comme $\prod_{x \in G} x$ est régulier (car inversible), on en déduit que $a^{|G|} = e$.

(iii) Conséquence du (ii). ■

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 $\overline{ab} = \overline{cd}$.

Démonstration

Comme pour la somme : $a \equiv c [n]$ et $b \equiv d [n]$ implique $ab \equiv cd [n]$. ■

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 $\bar{a} \times \bar{b} = \overline{ab}$, 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.

Démonstration

On a déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ a une structure de groupe abélien.

Reste à voir que \times est associative, distributive sur $+$, commutative et admet un neutre $\bar{1}$ de façon similaire à ce qui a été vu pour $+$. ■

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 $k \wedge n = 1$.

Démonstration

\bar{k} est inversible si et seulement s'il existe $\ell \in \mathbb{Z}$ tel que $\overline{k\ell} = \bar{k}\bar{\ell} = \bar{1}$ si et seulement si $k\ell \equiv 1 [n]$ si et seulement s'il existe $u \in \mathbb{Z}$ tel que $1 = k\ell + un$, ce qui permet de conclure par théorème de Bézout. ■



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 .

**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 n est premier.

Démonstration

On élimine le cas $n = 1$ car $\mathbb{Z}/1\mathbb{Z} = \{0\}$. On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si pour tout $k \in \llbracket 1, n-1 \rrbracket$, \overline{k} est inversible si et seulement si pour tout $k \in \llbracket 1, n-1 \rrbracket$, k est premier avec n si et seulement si les seuls diviseurs positifs de n sont 1 et n si et seulement si $n \geq 2$ 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.

Démonstration

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

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

2^e formulation

- (i) $k \equiv \ell \pmod{nm}$ donc $nm \mid (k - \ell)$ donc $n \mid (k - \ell)$ et $m \mid (k - \ell)$ donc $k \equiv \ell \pmod{n}$ et $k \equiv \ell \pmod{m}$.
- (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 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

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

On montre exactement de la même manière que

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

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 1^{re} 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 $\begin{cases} k \equiv 0 \pmod{n} \\ k \equiv 0 \pmod{m} \end{cases}$ donc $k \equiv 0 \pmod{nm}$ 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, $\text{Ker } f = \{0_{\mathbb{Z}/n\mathbb{Z}}\}$ et f est un isomorphisme. ■

Exercice 4 : CCINP 94

1. Énoncer le théorème de Bézout dans \mathbb{Z} .

2. Soit a et b deux entiers naturels premiers entre eux.

Soit $c \in \mathbb{N}$.

Prouver que : $(a \mid c \text{ et } b \mid c) \iff ab \mid c$.

3. On considère le système $(S) : \begin{cases} x \equiv 6 \pmod{17} \\ x \equiv 4 \pmod{15} \end{cases}$ dans lequel l'inconnue x appartient à \mathbb{Z} .

(a) Déterminer une solution particulière x_0 de (S) dans \mathbb{Z} .

(b) Déduire des questions précédentes la résolution dans \mathbb{Z} du système (S) .

1. Théorème de Bézout :

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

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \mid au + bv = 1.$$

2. Soit $(a, b) \in \mathbb{N}^2$. On suppose que $a \wedge b = 1$.

Soit $c \in \mathbb{N}$.

Prouvons que $ab \mid c \implies a \mid c$ et $b \mid c$.

Si $ab \mid c$ alors $\exists k \in \mathbb{Z} \mid c = kab$.

Alors, $c = (kb)a$ donc $a \mid c$ et $c = (ka)b$ donc $b \mid c$.



Prouvons que $(a|c \text{ et } b|c) \implies ab|c$.

$a \wedge b = 1$ donc $\exists(u, v) \in \mathbb{Z}^2 / au + bv = 1$. (1)

De plus $a|c$ donc $\exists k_1 \in \mathbb{Z} / c = k_1 a$. (2)

De même, $b|c$ donc $\exists k_2 \in \mathbb{Z} / c = k_2 b$. (3)

On multiplie (1) par c et on obtient $cau + cbv = c$.

Alors, d'après (2) et (3), $(k_2 b)au + (k_1 a)bv = c$, donc $(k_2 u + k_1 v)(ab) = c$ et donc $ab|c$.

On a donc prouvé que $(a|c \text{ et } b|c) \iff ab|c$.

3. (a) **Première méthode** (méthode générale) :

Soit $x \in \mathbb{Z}$.

$$\begin{aligned} x \text{ solution de (S)} &\iff \exists(k, k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ x = 4 + 15k' \end{cases} \\ &\iff \exists(k, k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ 6 + 17k = 4 + 15k' \end{cases} \end{aligned}$$

Or $6 + 17k = 4 + 15k' \iff 15k' - 17k = 2$.

Pour déterminer une solution particulière x_0 de (S), il suffit donc de trouver une solution particulière (k_0, k'_0) de l'équation $15k' - 17k = 2$.

Pour cela, cherchons d'abord, une solution de l'équation $15u + 17v = 1$.

17 et 15 sont premiers entre eux.

Déterminons alors un couple (u_0, v_0) d'entiers relatifs tel que $15u_0 + 17v_0 = 1$.

On a : $17 = 15 \times 1 + 2$ puis $15 = 7 \times 2 + 1$.

Alors $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15 \times 1) = 15 - 17 \times 7 + 15 \times 7 = 15 \times 8 - 17 \times 7$

Donc $8 \times 15 + (-7) \times 17 = 1$

Ainsi, $16 \times 15 + (-14) \times 17 = 2$.

On peut prendre alors $k'_0 = 16$ et $k_0 = 14$.

Ainsi, $x_0 = 6 + 17 \times k_0 = 6 + 17 \times 14 = 244$ est une solution particulière de (S).

Deuxième méthode :

En observant le système (S), on peut remarquer que $x_0 = -11$ est une solution particulière.

Cette méthode est évidemment plus rapide mais ne fonctionne pas toujours.

$$(b) \ x_0 \text{ solution particulière de (S) donc } \begin{cases} x_0 = 6 & [17] \\ x_0 = 4 & [15] \end{cases}.$$

$$\text{On en déduit que } x \text{ solution de (S) si et seulement si } \begin{cases} x - x_0 = 0 & [17] \\ x - x_0 = 0 & [15] \end{cases}$$

c'est-à-dire x solution de (S) $\iff (17|x - x_0 \text{ et } 15|x - x_0)$.

Or $17 \wedge 15 = 1$ donc d'après 2., x solution de (S) $\iff (17 \times 15)|x - x_0$.

Donc l'ensemble des solutions de (S) est $\{x_0 + 17 \times 15k, k \in \mathbb{Z}\} = \{244 + 255k, k \in \mathbb{Z}\}$.

3

Indicatrice d'Euler

Définition 14 : Indicatrice d'Euler

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

Remarque

R 14 – $\varphi(1) = 1$.

R 15 – Si $n \geq 2$, $\varphi(n)$ 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

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

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

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

Démonstration

En effet, tous les entiers entre 1 et $p - 1$ sont non divisibles par p donc premier avec lui. Puis les entiers premiers avec p^k sont les entiers n'admettant pas p comme diviseur premier. Combien y a-t-il de multiple de p entre 1 et p^k ? Autant que de $\ell \in \mathbb{N}$ tel que $1 \leq \ell p \leq p^k$, c'est-à-dire, ℓ étant entier, $1 \leq \ell p \leq p^{k-1}$ soit exactement p^{k-1} . D'où, finalement, $\varphi(p) = p^k - p^{k-1}$. ■

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

**Démonstration**

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

$$|U_{\mathbb{Z}/nm\mathbb{Z}}| = |U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}}| = |U_{\mathbb{Z}/n\mathbb{Z}}| \times |U_{\mathbb{Z}/m\mathbb{Z}}|.$$

Corollaire 4 : Produit de plus de deux termes

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

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

Démonstration

Récurrence.

Corollaire 5 : Expression à l'aide des diviseurs premiers

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

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

Exercice 5 : La même formule, avec des probabilités

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

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

$$1. \mathbb{P}(A_d) = \frac{|A_d|}{|\Omega|} = \frac{\frac{n}{d}}{n} = \frac{1}{d}.$$

2. (a) Si p_1, \dots, p_ℓ sont des diviseurs premiers deux à deux distincts de n , comme ils sont premiers,

$$\bigcap_{j=1}^{\ell} A_{p_j} = A_{p_1 \cdots p_\ell}.$$

$$\mathbb{P}\left(\bigcap_{j=1}^{\ell} A_{p_j}\right) = \mathbb{P}(A_{p_1 \cdots p_\ell}) = \frac{1}{p_1 \cdots p_\ell} = \prod_{j=1}^{\ell} \mathbb{P}(A_{p_j}).$$

(b) Les \bar{A}_p sont aussi indépendants, $A = \bigcap_{p \in P} \bar{A}_p$, $\mathbb{P}(A) = \frac{\varphi(n)}{n} = \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.

Exercice 6 : Une identité remarquable (et classique)

- 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 $1 \leq q \leq n$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?
- Montrer que, si $n \in \mathbb{N}^*$, $n = \sum_{k|n} \varphi(k)$.

1. Notons F_k l'ensemble des nombres rationnels de la forme $\frac{q}{m}$ où $1 \leq q \leq m$ qui s'écrivent sous forme irréductible avec k au dénominateur et $E_k = \{\ell \in \llbracket 0, k-1 \rrbracket \mid \ell \wedge k = 1\}$ si $k \neq 1$ (remarquons qu'alors $0 \notin E_k$), $E_1 = \{1\}$.

L'application $f : \begin{array}{l} E_k \longrightarrow F_k \\ \ell \longmapsto \frac{\ell}{k} \end{array}$ est bijective^a. En effet,

- si $k = 1$, f est l'identité de $F_1 = E_1 = \{1\}$;
- sinon,
 - ★ elle est bien définie car si $\ell \in E_k$, $\frac{\ell}{k}$ est un nombre rationnel de la forme $\frac{q}{m}$ car $k|m$ avec $1 \leq q \leq m$ car $\frac{\ell}{k} \in]0, 1]$, qui s'écrit sous forme irréductible avec k au dénominateur car $\ell \wedge k = 1$ et donc $f(\ell) \in F_k$;
 - ★ elle est injective car si $\ell, \ell' \in E_k$ tels que $f(\ell) = f(\ell')$, alors $\frac{\ell}{k} = \frac{\ell'}{k}$ donc $\ell = \ell'$;
 - ★ elle est surjective car si $r \in F_k$, $r \in \mathbb{Q} \cap]0, 1]$ et r s'écrit forme irréductible avec k au dénominateur, donc on a $l \in \llbracket 1, k \rrbracket$ avec $k \wedge l = 1$ tel que $r = \frac{\ell}{k}$. Comme $k \neq 1$, $\ell \neq k$ donc $\ell \in \llbracket 1, k-1 \rrbracket$, $\ell \in E_k$ et donc $r = f(\ell)$.

Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1 \leq q \leq m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0 \leq l \leq k-1$ et $k \wedge l = 1$ si $k \neq 1$, 1 sinon : il y en a donc $\varphi(k)$.

2. Si on note $F = \left\{ \frac{q}{m} ; 1 \leq q \leq m \right\}$, alors $F = \bigsqcup_{k|m} F_k$ car tout rationnel de F s'écrit de manière unique sous forme irréductible avec un diviseur de m au dénominateur.

Donc $|F| = \sum_{k|m} |F_k|$, et comme $|F| = |\llbracket 1, m \rrbracket| = m$, $m = \sum_{k|m} \varphi(k)$ d'après la question précédente.

a. On peut aller un peu plus vite oralement en invoquant simplement l'existence et l'unicité de la forme irréductible des fractions.

Théorème 6 : d'Euler

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

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

Démonstration

$\bar{a} \in U_{\mathbb{Z}/n\mathbb{Z}}$ qui est un groupe multiplicatif, donc $\bar{a}^{|\mathbb{Z}/n\mathbb{Z}|} = \bar{a}^{\varphi(n)} = \bar{1}$. ■

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),

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

Démonstration

Théorème d'Euler avec $\varphi(p) = p - 1$. ■

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 .

Démonstration : Non exigible¹

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