

Algèbre modulaire

Extrait du programme officiel :

CONTENUS

CAPACITÉS & COMMENTAIRES

Compléments sur les groupes

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

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.	Notation \mathbb{F}_p lorsque p est premier.
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.	Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.
Indicatrice d'Euler φ . Calcul à l'aide de la décomposition en produits de facteurs premiers.	Relation $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux ; expression de $\varphi(p^k)$ pour p premier.
Théorème d'Euler.	Lien avec le petit théorème de Fermat.

Plan du cours

27 Algèbre modulaire	1
I Congruences	2
II Le groupe $\mathbb{Z}/n\mathbb{Z}$	2
III Anneau $\mathbb{Z}/n\mathbb{Z}$	5
1 Structure	5
2 Théorème Chinois	6
3 Indicatrice d'Euler	8



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

$\forall a \in \mathbb{Z}, \exists ! r \in \llbracket 0, n-1 \rrbracket, a \equiv r [n]$. 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 $n = \overline{a_k \dots a_1 a_0}^{10}$ 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 : $3|n \iff 3 \mid \sum_{i=0}^k a_i$

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

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

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

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

Divisibilité par 11 : $11|n \iff 11 \mid (a_0 - a_1 + a_2 - a_3 + \dots) = \sum_{i=0}^k (-1)^i a_i$

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

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

Remarque

R1 – \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 : $k \equiv r \pmod{n}$ donc $\bar{k} = \bar{r} = \bar{r + p n}$ pour tout $p \in \mathbb{Z}$.

Définition 3 : Surjection canonique

L'application surjective $\begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \bar{k} \end{cases}$ 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 $a \equiv c \pmod{n}$ et $b \equiv d \pmod{n}$ implique $a + b \equiv c + d \pmod{n}$.

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

Définition 4 : 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 5 : 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 $a, b \in \mathbb{Z}$, $\bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a}$,
- d'élément neutre $\bar{0}$ car pour tout $a \in \mathbb{Z}$, $\bar{a} + \bar{0} = \overline{a + 0} = \bar{a}$,
- associative car si $a, b, c \in \mathbb{Z}$,

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

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

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

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

Remarque

R2 – On a alors facilement, pour $k \in \mathbb{Z}$, $k \cdot \bar{a} = \overline{k a}$.

**Exemple**E1 – Table d'addition dans $\mathbb{Z}/4\mathbb{Z}$.**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 $k \wedge n = 1$.

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

R3 – 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

E2 – Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n = 5$ par exemple.

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

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 $n = |\mathbb{Z}/n\mathbb{Z}| = |G|$. ■

 **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 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.

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 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 $k \wedge n = 1$.

**Démonstration**

\bar{k} est inversible si et seulement s'il existe $\ell \in \mathbb{Z}$ tel que $\overline{k\ell} = \overline{k\ell} = \bar{1}$ 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 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 tête », soit en utilisant l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre k et n .

Exemple

E3 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E4 – 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 note alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Démonstration

On élimine le cas $n = 1$ car $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$. On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si pour tout $k \in \llbracket 1, n-1 \rrbracket$, \bar{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 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

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

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.

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

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

Puis

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

2^e 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 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

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

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 $\begin{cases} k \equiv 0 [n] \\ k \equiv 0 [m] \end{cases}$ 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, $\text{Ker } f = \{0_{\mathbb{Z}/nm\mathbb{Z}}\}$ 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

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

Remarque

R4 – $\varphi(1) = 1$.

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

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

Propriété 10 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

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

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

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

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 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).

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 $k \in \mathbb{Z}$ tel que

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

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

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

et

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

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

$$(a \bmod n, b \bmod m) = f(k \bmod nm) = g(k \bmod nm)$$

donc 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,

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

Corollaire 3 : Produit de plus de deux termes

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

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

Démonstration

Récurrence. ■

Corollaire 4 : Expression à l'aide des diviseurs premiers

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

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

Exercice 2 : 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 $A_d = \{kd, k \in \Omega \text{ et } kd \in \Omega\}$.

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 $\varphi(n) = n \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.

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, $A = \bigcap_{p \in P} \bar{A}_p$ est l'ensemble des entiers de $\llbracket 1, n \rrbracket$ premiers avec n , donc

$$\mathbb{P}(A) = \frac{\varphi(n)}{n} = \prod_{p \in P} \left(1 - \frac{1}{p}\right).$$

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 $1 \leq q \leq n$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?

Formulation équivalente : combien y en a-t-il dans \mathbb{U}_n de complexes d'ordre exactement k ?

Formulation équivalente : combien y en a-t-il dans $\mathbb{Z}/n\mathbb{Z}$ d'éléments d'ordre exactement k ?

2. 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 $E_k = \{\ell \in \llbracket 1, k \rrbracket, \ell \wedge k = 1\}$.

L'application $f : \begin{cases} E_k & \longrightarrow F_k \\ \ell & \longmapsto \frac{\ell}{k} \end{cases}$ 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 sous forme irréductible avec k au dénominateur, donc on a $l \in \llbracket 1, k \rrbracket$ avec $k \wedge l = 1$ tel que $r = \frac{l}{k}$. 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 2 : d'Euler

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

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

Démonstration

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

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),

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

Démonstration

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

Exercice 4 : CCINP 86**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 $(\mathbb{N}^*)^3$.

Démonstration : Non exigible¹

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