27

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

I Congruences

Définition 1 : Rappel : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b \ [n]$ lorsque $n|(a-b)$ ie 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

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

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

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

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

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble (quotient) des n classes d'équivalences de $\cdot \equiv \cdot \ [n]$, 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 1 – $\overline{k}$ 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 3 : 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 $\overline{a+b} = \overline{c+d}$.

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 4 : Loi $+$

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

Propriété 4 : 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 $a, b \in \mathbb{Z}$, $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{a}+\overline{b}$,
- d'élément neutre $\overline{0}$ car pour tout $a \in \mathbb{Z}$, $\overline{a}+\overline{0} = \overline{a+0} = \overline{a}$,
- associative car si $a, b, c \in \mathbb{Z}$,
$$\left(\overline{a}+\overline{b}\right)+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\left(\overline{b}+\overline{c}\right),$$
- 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 $k \equiv \ell\ [n]$, alors $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}\ell\pi}{n}}$ ne dépend pas du choix du représentant de $\overline{k}$.

Donc $f : \left|\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}_n, \times) \\ \overline{k} & \longmapsto & \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \end{array}\right.$ est

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

Remarque

R 2 – 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 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
$$x=a_1^{\varepsilon_1}*\cdots*a_k^{\varepsilon_k}.$$
- Soit $a\in G$. Le sous-groupe **engendré par** a noté $\langle a\rangle$ plutôt que $\langle\{a\}\rangle$ est
$$\langle a\rangle=\left\{a^k,\ k\in\mathbb{Z}\right\}$$
  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 5 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

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

Démonstration

On a en effet $\mathbb{Z}/n\mathbb{Z}=\{a\cdot\overline{1},a\in\mathbb{Z}\}=\langle\overline{1}\rangle$ 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 $a\in\mathbb{Z}$, $a=auk+nva\equiv auk\ [n]$ donc $\overline{a}=au\overline{k}$ donc $\mathbb{Z}/n\mathbb{Z}=\langle\overline{k}\rangle$.
Si, réciproquement, $\mathbb{Z}/n\mathbb{Z}=\langle\overline{k}\rangle$, alors on a $a\in\mathbb{Z}$ tel que $\overline{1}=a\overline{k}=\overline{ak}$ donc on a $\ell\in\mathbb{Z}$ tel que $1=ak+n\ell$ donc $n\wedge k=1$ par théorème de Bézout. ■

Remarque

R 3 – 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 2 – Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n=5$ par exemple.

Propriété 6 : 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, $f : \left|\begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,*)\\ k & \longmapsto & a^k\end{array}\right.$ alors f est un morphisme de groupes surjectif car $G=\langle a\rangle$, et injectif car si $k\in\operatorname{Ker} f$, $a^k=1$ 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 $a^n=e$, $f : \left|\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z},+) & \longrightarrow & (G,*)\\ \overline{k} & \longmapsto & a^k\end{array}\right.$ est bien définie (quel que soit le représentant k de $\overline{k}$, 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 $n=|\mathbb{Z}/n\mathbb{Z}|=|G|$.

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

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

Propriété 7 : 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 $\overline{1}$ de façon similaire à ce qui a été vu pour $+$.

Propriété 8 : 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 $k\wedge n=1$.

Démonstration

$\overline{k}$ est inversible si et seulement s'il existe $\ell\in\mathbb{Z}$ tel que $\overline{k\ell}=\overline{k\ell}=\overline{1}$ 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 $\overline{k}$ 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 3 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E 4 – 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 $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si pour tout $k \in [\![1, n-1]\!]$, $\overline{k}$ est inversible si et seulement si pour tout $k \in [\![1, n-1]\!]$, k est premier avec n si et seulement si les seuls diviseurs positifs de n sont 1 et n si et seulement si $n \geqslant 2$ premier. ■

2 Théorème Chinois

Théorème 1 : 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.

Le résultat s'étant 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

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

Puis

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

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

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

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 1 : CCINP 94

3 Indicatrice d'Euler

Définition 7 : Indicatrice d'Euler

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

Remarque

R4 – $\varphi(1) = 1$.

R5 – 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).

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

Propriété 9 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

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

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

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

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 $1 \leqslant \ell p \leqslant p^k$, c'est-à-dire, ℓ étant entier, $1 \leqslant \ell p \leqslant p^{k-1}$ soit exactement p^{k-1}.
D'où, finalement, $\varphi(p) = p^k - p^{k-1}$. ■

Propriété 10 : 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

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

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,

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

■

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 $\Omega = [\![1, n]\!]$ 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 $\varphi(n) = n \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.**

---

1. $\mathbb{P}(A_d) = \dfrac{|A_d|}{|\Omega|} = \dfrac{\frac{n}{d}}{n} = \dfrac{1}{d}$.
2. (a) Si $p_1, \dots, p_\ell$ 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 $\overline{A}_p$ sont aussi indépendant, $A = \bigcap_{p \in P} \overline{A}_p$, $\mathbb{P}(A) = \dfrac{\varphi(n)}{n} = \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.

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

---

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

   L'application $f : \left| \begin{array}{ccc} E_k & \longrightarrow & F_k \\ \ell & \longmapsto & \frac{\ell}{k} \end{array} \right.$ 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 $1 \leqslant q \leqslant m$ 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 $l \in [\![1, k]\!]$ avec $k \wedge \ell = 1$ tel que $r = \frac{\ell}{k}$. Comme $k \neq 1$, $\ell \neq k$ donc $\ell \in [\![1, k-1]\!]$, $\ell \in E_k$ et donc $r = f(\ell)$.

   Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0 \leqslant l \leqslant k-1$ et $k \wedge l = 1$ si $k \neq 1$, 1 sinon : il y en a donc $\varphi(k)$.
2. Si on note $F = \left\{\frac{q}{m} \; ; \; 1 \leqslant q \leqslant m\right\}$, 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 $|F| = |[\![1, m]\!]| = m$, $\boxed{m = \sum_{k|m} \varphi(k)}$ 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

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

Démonstration

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

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