

Arithmétique et $\mathbb{Z}/n\mathbb{Z}$

I. Relations d'équivalence et ensembles quotients

Avant de calculer « modulo n », il faut savoir identifier des objets. C'est précisément le rôle d'une relation d'équivalence. En effet, elle regroupe les éléments d'un ensemble en paquets disjoints. Ensuite, on travaille sur les paquets eux-mêmes, et non plus sur les éléments.

Définition :

Une relation binaire $\mathcal{R}$ sur un ensemble E est une **relation d'équivalence** si elle est :

- réflexive : $\forall x \in E, x \mathcal{R} x$;
- symétrique : $\forall x, y \in E, x \mathcal{R} y \Rightarrow y \mathcal{R} x$;
- transitive : $\forall x, y, z \in E, (x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow x \mathcal{R} z$.

La **classe** de x est $\bar{x} = \{y \in E \mid x \mathcal{R} y\}$. L'**ensemble quotient** $E/\mathcal{R}$ est l'ensemble de toutes les classes.

Proposition :

Les classes d'équivalence forment une **partition** de E : elles sont non vides, leur réunion vaut E , et deux classes sont soit égales, soit disjointes. De plus, $\bar{x} = \bar{y} \Leftrightarrow x \mathcal{R} y$.

Démonstration :

D'abord, par réflexivité, $x \in \bar{x}$, donc chaque classe est non vide et la réunion des classes vaut E . Ensuite, supposons $x \mathcal{R} y$. Si $z \in \bar{y}$, alors $y \mathcal{R} z$, donc $x \mathcal{R} z$ par transitivité, et $z \in \bar{x}$. Ainsi $\bar{y} \subset \bar{x}$, et l'inclusion inverse vient de la symétrie. Enfin, si $z \in \bar{x} \cap \bar{y}$, alors $x \mathcal{R} z$ et $y \mathcal{R} z$, donc $x \mathcal{R} y$ et $\bar{x} = \bar{y}$. Deux classes qui se rencontrent sont donc égales.

L'application $\pi : E \rightarrow E/\mathcal{R}, x \rightarrow \bar{x}$, s'appelle la **projection canonique**. Elle est surjective par construction. Tout élément d'une classe en est un **représentant**.

Attention :

Définir une application sur $E/\mathcal{R}$ par une formule en x exige de vérifier que le résultat ne dépend pas du représentant choisi. On dit alors que l'application est **bien définie**. Par exemple, sur $\mathbb{Z}/3\mathbb{Z}$, la formule $\bar{x} \rightarrow \overline{2^x}$ n'a pas de sens : $\bar{0} = \bar{3}$, mais $2^0 = 1$ et $2^3 = 8 \equiv 2 \pmod{3}$.

Exemple :

Sur $\mathbb{R}$, posons $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$. C'est une relation d'équivalence, car $\mathbb{Z}$ contient 0, est stable par opposé et par somme. Chaque classe contient exactement un réel de $[0, 1[$, à savoir la partie fractionnaire. Autrement dit, $\mathbb{R}/\mathbb{Z}$ s'identifie à $[0, 1[$, c'est-à-dire à un cercle.

II. Congruences : l'arithmétique modulo n

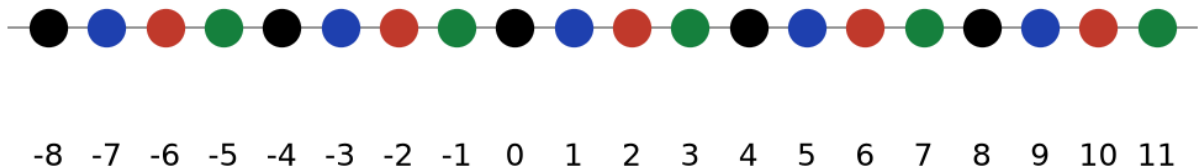
On fixe un entier $n \geq 1$. Les congruences traduisent l'idée de calculer « au reste près ». Elles généralisent le calcul des heures sur une horloge.

Définition :

Deux entiers a et b sont **congrus modulo n** si n divise $b - a$. On note $a \equiv b \pmod{n}$. De façon équivalente, a et b ont le même reste dans la division euclidienne par n .

La congruence est une relation d'équivalence sur $\mathbb{Z}$. En effet, $n \mid 0$; si $n \mid b - a$, alors $n \mid a - b$; enfin, si $n \mid b - a$ et $n \mid c - b$, alors n divise la somme $c - a$. Par division euclidienne, chaque entier est congru à un unique $r \in \{0, 1, \dots, n-1\}$. Il y a donc exactement n classes. Comme le montre la figure ci-dessous pour $n = 4$, les classes découpent $\mathbb{Z}$ en quatre familles qui se répètent périodiquement.

● classe $\overline{0}$ ● classe $\overline{1}$ ● classe $\overline{2}$ ● classe $\overline{3}$



Proposition :

La congruence est **compatible** avec l'addition et la multiplication : si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors

$$a + b \equiv a' + b' \pmod{n} \text{ et } ab \equiv a' b' \pmod{n}.$$

Par récurrence, $a^k \equiv (a')^k \pmod{n}$ pour tout $k \in \mathbb{N}$.

Démonstration :

Écrivons $a' = a + un$ et $b' = b + vn$. Alors $a' + b' = a + b + (u+v)n$. De plus, $a' b' = ab + (av + bu + uvn)n$. Les deux différences sont donc des multiples de n .

Exemple :

Comme $10 \equiv 1 \pmod{9}$, on a $10^k \equiv 1 \pmod{9}$ pour tout k . Par conséquent, un entier est congru à la somme de ses chiffres modulo 9. De même, $10 \equiv -1 \pmod{11}$: un entier est congru modulo 11 à la somme alternée de ses chiffres, en partant des unités.

Attention :

On ne simplifie pas librement une congruence. Par exemple, $2 \times 3 \equiv 2 \times 0 \pmod{6}$, mais $3 \not\equiv 0 \pmod{6}$. La simplification par c n'est permise que si c est premier avec n .

III. Construction de l'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Le quotient et ses opérations

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la congruence modulo n . Ainsi

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, et ces n classes sont distinctes. La compatibilité établie plus haut permet alors de définir des opérations sur les classes.

Théorème :

Les formules $\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \times \bar{b} = \overline{ab}$ définissent bien deux lois sur $\mathbb{Z}/n\mathbb{Z}$. Muni de ces lois, $\mathbb{Z}/n\mathbb{Z}$ est un **anneau commutatif**, de zéro $\bar{0}$ et d'unité $\bar{1}$. De plus, la projection $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux surjectif, de noyau $n\mathbb{Z}$.

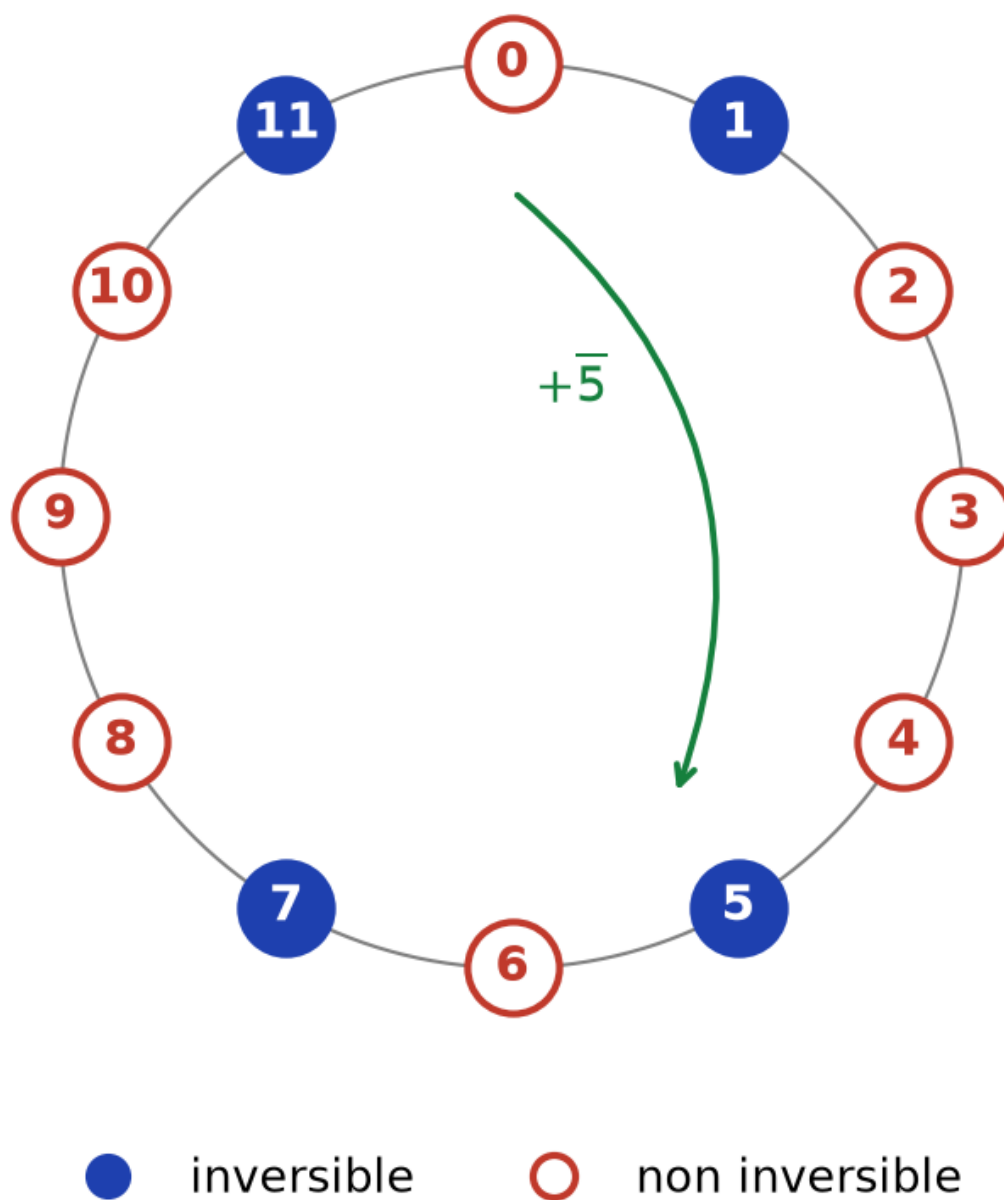
Démonstration :

D'abord, les lois sont bien définies : si $\bar{a} = \bar{a'}$ et $\bar{b} = \bar{b'}$, la proposition de compatibilité donne $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$. Ensuite, chaque axiome d'anneau se transporte depuis $\mathbb{Z}$. Par exemple, pour la distributivité :

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a(b+c)} = \overline{ab+ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

Enfin, $\pi(a+b) = \pi(a) + \pi(b)$ et $\pi(ab) = \pi(a)\pi(b)$ par définition des lois. Son noyau est $\{a \mid \bar{a} = \bar{0}\} = n\mathbb{Z}$.

C'est le premier exemple d'anneau obtenu par **passage au quotient**. On retrouvera ce procédé avec les anneaux quotients par un idéal. La figure ci-dessous représente $\mathbb{Z}/12\mathbb{Z}$ comme une horloge. Ajouter $\bar{5}$ revient à tourner de cinq crans. Les classes en bleu sont celles qui admettent un inverse, comme on va le voir.



2. Éléments inversibles

Dans un anneau, un élément x est inversible s'il existe y avec $xy = 1$. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe des inversibles.

Théorème :

Pour $a \in \mathbb{Z}$, la classe $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(a, n) = 1$.

Démonstration :

Supposons $\bar{a} \bar{u} = \bar{1}$. Il existe alors $v \in \mathbb{Z}$ tel que $au - 1 = vn$, soit $au - vn = 1$. Tout diviseur commun à a et n divise donc 1. Réciproquement, si $\text{pgcd}(a, n) = 1$, le théorème de Bézout fournit u, v avec $au + nv = 1$. En passant aux classes, $\bar{a} \bar{u} = \bar{1}$.

Méthode :

Pour inverser $\bar{a}$ modulo n :

1. on applique l'algorithme d'Euclide à n et a jusqu'au reste 1 ;
2. on remonte les divisions pour écrire $1 = au + nv$;
3. on conclut : $\bar{a}^{-1} = \bar{u}$, qu'on ramène dans $\{0, \dots, n-1\}$;
4. on vérifie en calculant au modulo n .

Exemple :

Inversons 17 modulo 60. D'abord, $60 = 3 \times 17 + 9$, puis $17 = 9 + 8$ et $9 = 8 + 1$. En remontant :

$$1 = 9 - 8 = 2 \times 9 - 17 = 2 \times 60 - 7 \times 17.$$

Donc $\bar{17}^{-1} = \bar{-7} = \bar{53}$. En effet, $17 \times 53 = 901 = 15 \times 60 + 1$.

Une classe non nulle et non inversible est un **diviseur de zéro**. En effet, si $d = \text{pgcd}(a, n) > 1$ et $n \nmid a$, alors $\bar{a} \times \overline{n/d} = \overline{(a/d)} \bar{n} = \bar{0}$, avec $\overline{n/d} \neq \bar{0}$.

Proposition :

Soient $a, b \in \mathbb{Z}$ et $d = \text{pgcd}(a, n)$. L'équation $\bar{a}x = \bar{b}$ admet une solution dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $d \mid b$. Dans ce cas, elle en admet exactement d , qui forment une seule classe modulo n/d .

Démonstration :

Si $ax = b + kn$, alors d divise $ax - kn = b$. Réciproquement, si $d \mid b$, écrivons $a = da_1$, $b = db_1$, $n = dn_1$ avec $\text{pgcd}(a_1, n_1) = 1$. Alors $n \mid ax - b$ équivaut à $n_1 \mid a_1x - b_1$. Autrement dit, $x \equiv a_1^{-1}b_1 \pmod{n_1}$, où l'inverse est pris modulo n_1 . Cette classe modulo n_1 contient exactement d classes modulo n .

3. Le corps $\mathbb{Z}/p\mathbb{Z}$

Théorème :

Soit $n \geq 2$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un **corps** si et seulement si n est premier. Il est alors noté $\mathbb{F}_p$ lorsque $n = p$.

Démonstration :

Si p est premier et $p \nmid a$, alors $\text{pgcd}(a, p) = 1$. Par conséquent, toute classe non nulle est inversible. Réciproquement, si $n = rs$ avec $1 < r, s < n$, alors $\bar{r}\bar{s} = \bar{0}$ avec $\bar{r} \neq \bar{0}$ et $\bar{s} \neq \bar{0}$. L'anneau n'est donc pas intègre, et ce n'est pas un corps.

La figure ci-dessous compare les tables de multiplication de $\mathbb{Z}/6\mathbb{Z}$ et de $\mathbb{Z}/7\mathbb{Z}$. Dans $\mathbb{Z}/6\mathbb{Z}$, des produits de classes non nulles s'annulent. En revanche, dans $\mathbb{Z}/7\mathbb{Z}$, chaque ligne contient une fois $\bar{1}$ et jamais $\bar{0}$.

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

$\mathbb{Z}/6\mathbb{Z}$ (classes non nulles)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\mathbb{Z}/7\mathbb{Z}$ (classes non nulles)

■ produit nul ■ produit égal à $\bar{1}$

IV. Indicatrice d'Euler, théorèmes d'Euler et de Fermat

1. L'indicatrice d'Euler

Définition :

L'**indicatrice d'Euler** de $n \geq 1$ est $\varphi(n) = \text{card}\{k \in \{1, \dots, n\} \text{ s.t. } \text{pgcd}(k, n) = 1\}$.
D'après la partie III, c'est le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition :

Si p est premier et $k \geq 1$, alors $\varphi(p^k) = p^k - p^{k-1}$. Si $\text{pgcd}(m, n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$. Par suite, si $n = p_1^{k_1} \dots p_r^{k_r}$,

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

La première formule s'obtient en retirant les p^{k-1} multiples de p compris entre 1 et p^k . La multiplicativité découle du théorème chinois, démontré en partie V.

Exemple :

On a $360 = 2^3 \times 3^2 \times 5$. Donc $\varphi(360) = 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96$.

2. Théorème d'Euler et petit théorème de Fermat

Théorème :

(Théorème d'Euler) Si $\text{pgcd}(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Démonstration :

Notons $G = (\mathbb{Z}/n\mathbb{Z})^\times$ et $\alpha = \bar{a} \in G$. L'application $x \rightarrow \alpha x$ est une bijection de G dans G , de réciproque $x \rightarrow \alpha^{-1}x$. Par conséquent, le produit de tous les éléments de G ne change pas :

$$\prod_{x \in G} x = \prod_{x \in G} (\alpha x) = \alpha^{\varphi(n)} \prod_{x \in G} x.$$

Le produit étant inversible, on le simplifie. Il reste $\alpha^{\varphi(n)} = \bar{1}$.

Corollaire :

(Petit théorème de Fermat) Soit p premier. Si $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.
Pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \pmod{p}$.

En effet, $\varphi(p) = p - 1$. Pour la seconde forme, on multiplie par a ; si $p \mid a$, les deux membres sont nuls.

Remarque :

La réciproque du petit théorème de Fermat est fausse. Par exemple, $2^{10} = 1024 = 3 \times 341 + 1$, donc $2^{340} \equiv 1 \pmod{341}$, alors que $341 = 11 \times 31$ n'est pas premier.

3. Calculer une puissance modulo n

Méthode :

Pour calculer a^k modulo n :

1. si $\text{pgcd}(a, n) = 1$, on réduit l'exposant modulo $\varphi(n)$ (ou modulo un exposant m connu tel que $a^m \equiv 1$) ;

2. on écrit l'exposant restant en base 2 ;
3. on calcule les carrés successifs $a, a^2, a^4, a^8, \dots$, chacun réduit modulo n ;
4. on multiplie les carrés qui correspondent aux chiffres 1 de l'écriture binaire.

Cette **exponentiation rapide** demande de l'ordre de $2\log_2 k$ multiplications, au lieu de $k - 1$.

Exemple :

Calculons 3^{2026} modulo 1000. Comme $\varphi(1000) = 400$ et $2026 = 5 \times 400 + 26$, on a $3^{2026} \equiv 3^{26}$. Ensuite, $3^{10} = 59049 \equiv 49$, donc $3^{20} \equiv 49^2 = 2401 \equiv 401$. Enfin, $3^{26} \equiv 401 \times 729 = 292329 \equiv 329 \pmod{1000}$.

V. Le théorème chinois

Le théorème chinois permet de ramener un problème modulo mn à deux problèmes plus petits, modulo m et modulo n . C'est donc un outil de décomposition.

Théorème :

(**Théorème chinois**) Soient $m, n \geq 1$ premiers entre eux. L'application

$$\psi : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x \bmod mn \rightarrow (x \bmod m, x \bmod n)$$

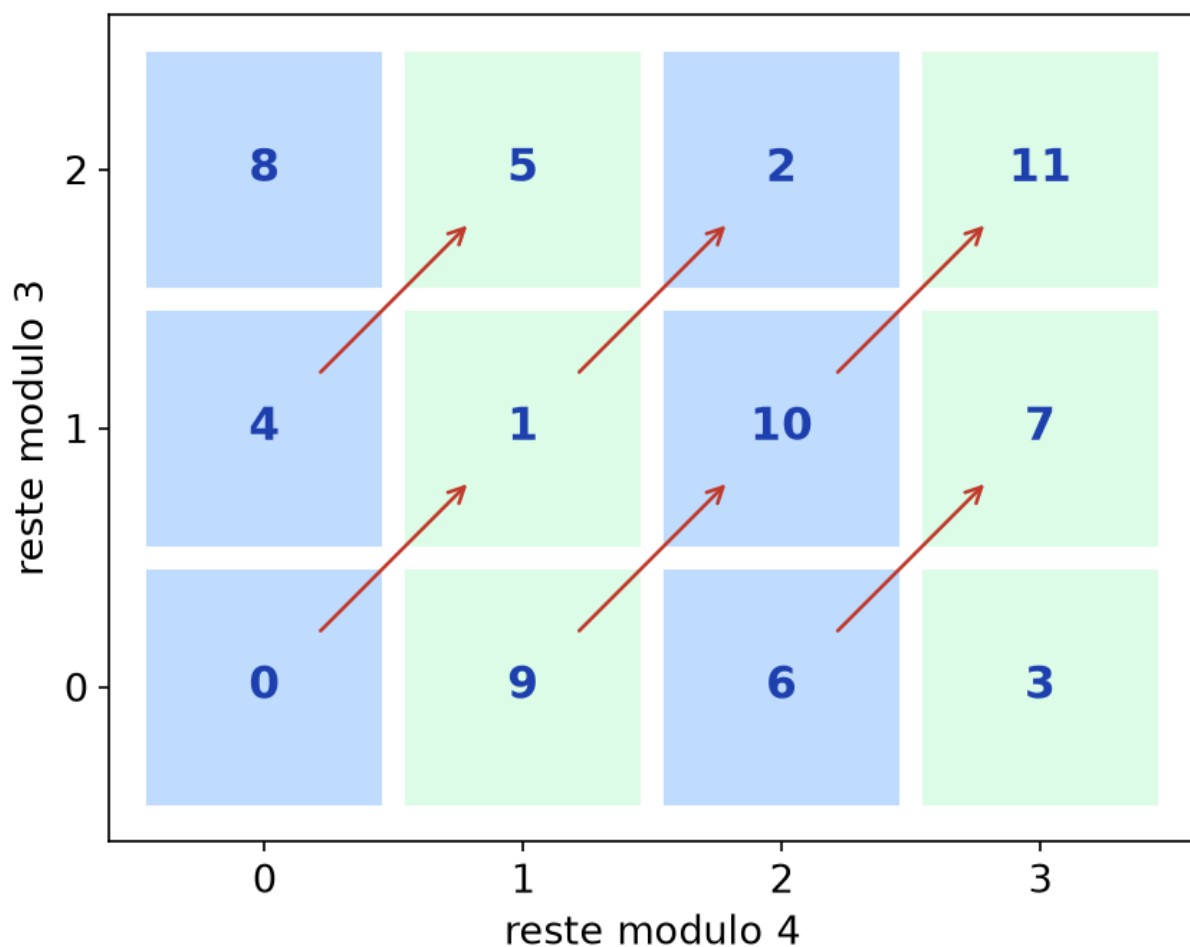
est bien définie, et c'est un **isomorphisme d'anneaux**. En particulier, pour tous a, b , le système

$x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a une unique solution modulo mn .

Démonstration :

D'abord, ψ est bien définie : si $x \equiv x' \pmod{mn}$, alors $x \equiv x' \pmod{m}$ et modulo n . C'est un morphisme d'anneaux, car les lois se calculent sur les représentants. Ensuite, si $\psi(\bar{x}) = (0, 0)$, alors $m \mid x$ et $n \mid x$. Comme m et n sont premiers entre eux, $mn \mid x$ par le lemme de Gauss. Ainsi ψ est injective. Enfin, les deux ensembles ont mn éléments, donc ψ est bijective.

La figure ci-dessous illustre l'isomorphisme $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Chaque entier de 0 à 11 occupe une case différente de la grille 3×4 . Ajouter 1 fait avancer d'une case en diagonale, avec retour au bord opposé.



Méthode :

Pour résoudre $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ avec $\text{pgcd}(m, n) = 1$:

1. on trouve par Bézout u, v tels que $mu + nv = 1$;
2. on pose $x_0 = bmu + anv$: en effet $nv \equiv 1 \pmod{m}$ et $mu \equiv 1 \pmod{n}$;
3. les solutions sont les $x_0 + kmn$, $k \in \mathbb{Z}$.

Avec plus de deux modules deux à deux premiers entre eux, on procède de même, ou bien on fusionne les équations deux par deux.

Exemple :

Réolvons $x \equiv 2 \pmod{3}$ et $x \equiv 3 \pmod{5}$. On a $3 \times 2 + 5 \times (-1) = 1$. Donc $x_0 = 3 \times 6 + 2 \times (-5) = 8$. Vérification : $8 = 2 \times 3 + 2$ et $8 = 5 + 3$. Les solutions sont les $8 + 15k$.

Corollaire :

Si $\text{pgcd}(m, n) = 1$, alors ψ induit un isomorphisme de groupes $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Par conséquent, $\varphi(mn) = \varphi(m)\varphi(n)$.

En effet, un couple est inversible dans un anneau produit si et seulement si ses deux composantes le sont. Un isomorphisme d'anneaux envoie donc les inversibles sur les inversibles.

Remarque :

Si $d = \text{pgcd}(m, n) > 1$, le système a des solutions si et seulement si $a \equiv b \pmod{d}$. Dans ce cas, elles forment une seule classe modulo $\text{ppcm}(m, n)$.

VI. Carrés dans $\mathbb{F}_p$

Soit p un nombre premier impair. On cherche à savoir quels éléments de $\mathbb{F}_p$ sont des carrés. Cette question gouverne notamment la résolution des équations du second degré dans $\mathbb{F}_p$.

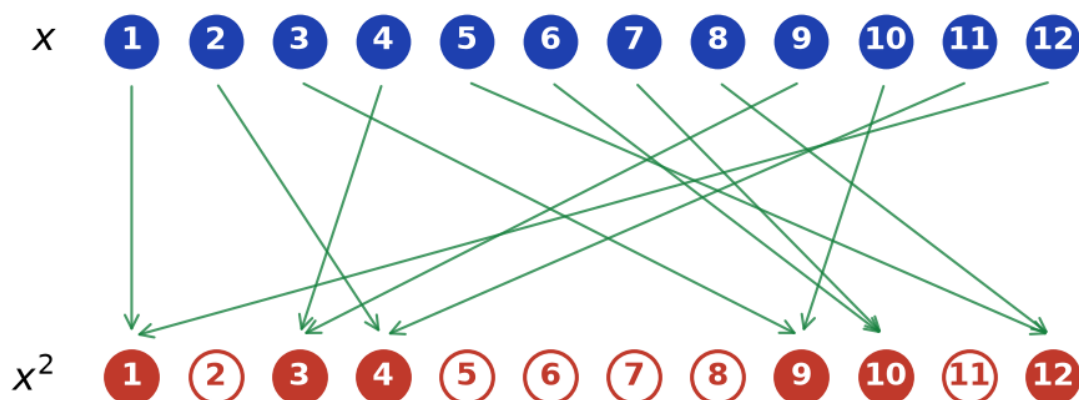
Proposition :

L'application $x \rightarrow x^2$ de $\mathbb{F}_p^\times$ dans lui-même est exactement « deux pour un ». Par conséquent, $\mathbb{F}_p^\times$ contient exactement $\frac{p-1}{2}$ carrés.

Démonstration :

Si $x^2 = y^2$, alors $(x-y)(x+y) = 0$. Comme $\mathbb{F}_p$ est un corps, donc intègre, on obtient $y = x$ ou $y = -x$. De plus, $x \neq -x$ car $2x \neq 0$ lorsque p est impair. Chaque carré non nul a donc exactement deux racines. Ainsi, les $p-1$ éléments de $\mathbb{F}_p^\times$ fournissent $\frac{p-1}{2}$ carrés.

La figure ci-dessous illustre ce fait dans $\mathbb{F}_{13}$. Deux flèches arrivent sur chacun des six carrés 1, 3, 4, 9, 10, 12. En revanche, aucune flèche n'atteint les six autres éléments.



Théorème :

(Critère d'Euler) Soit $a \in \mathbb{F}_p^\times$. Alors $a^{\frac{p-1}{2}} = 1$ si a est un carré, et $a^{\frac{p-1}{2}} = -1$ sinon.

Démonstration :

Posons $b = a^{\frac{p-1}{2}}$. D'après Fermat, $b^2 = a^{p-1} = 1$, donc $b = \pm 1$. Si $a = x^2$, alors $b = x^{p-1} = 1$. Ainsi, les $\frac{p-1}{2}$ carrés sont racines du polynôme $X^{\frac{p-1}{2}} - 1$. Or ce polynôme, sur le corps $\mathbb{F}_p$, a au plus $\frac{p-1}{2}$ racines. Ses racines sont donc exactement les carrés. Par conséquent, un non-carré vérifie $b \neq 1$, c'est-à-dire $b = -1$.

Exemple :

Le critère donne aussitôt : -1 est un carré de $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, soit $p \equiv 1 \pmod{4}$. Ainsi -1 est un carré modulo 13 , car $5^2 = 25 \equiv -1$. En revanche, ce n'est pas un carré modulo 7 .

Enfin, pour résoudre $ax^2 + bx + c = 0$ avec $a \neq 0$ dans $\mathbb{F}_p$, on procède comme dans $\mathbb{R}$. Le nombre 2 est inversible, donc la forme canonique reste valable. On pose $\Delta = b^2 - 4ac$. Il y a deux racines si Δ est un carré non nul, une si $\Delta = 0$, aucune sinon.

VII. Application au chiffrement RSA

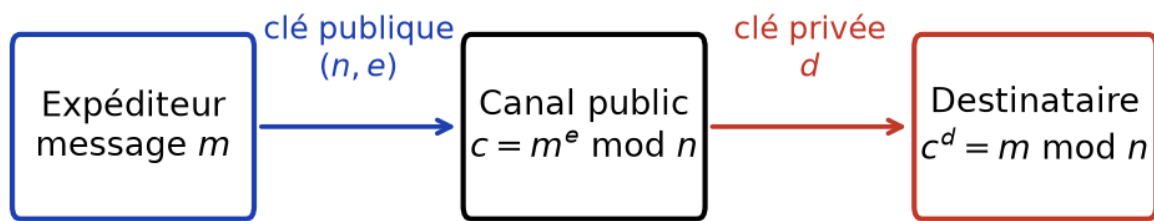
Le chiffrement RSA est un système à **clé publique**. N'importe qui peut chiffrer un message, mais seul le détenteur d'une clé secrète peut le déchiffrer. Sa sécurité repose sur un fait expérimental : multiplier deux grands nombres premiers est facile, tandis que factoriser leur produit semble très difficile.

Définition :

Le destinataire choisit deux grands nombres premiers distincts p et q , et pose $n = pq$. Ensuite, il choisit e premier avec $\varphi(n) = (p-1)(q-1)$ et calcule d tel que $ed \equiv 1 \pmod{\varphi(n)}$. La **clé publique** est (n, e) ; la **clé privée** est d .

- Chiffrement d'un message $m \in \{0, \dots, n-1\}$: $c = m^e \bmod n$.
- Déchiffrement : $m = c^d \bmod n$.

Le schéma ci-dessous résume les échanges. Seuls n , e et c circulent en public.



$n = pq$, $ed \equiv 1 \pmod{\varphi(n)}$; seul le destinataire connaît p et q

Théorème :

Avec les notations précédentes, $m^{ed} \equiv m \pmod{n}$ pour tout entier m .

Démonstration :

Écrivons $ed = 1 + k(p-1)(q-1)$ avec $k \in \mathbb{N}$. Travaillons d'abord modulo p . Si $p \mid m$, les deux membres sont nuls. Sinon, Fermat donne $m^{p-1} \equiv 1$, donc $m^{ed} = m(m^{p-1})^{k(q-1)} \equiv m \pmod{p}$. De même, $m^{ed} \equiv m \pmod{q}$. Enfin, p et q sont premiers entre eux : le théorème chinois donne $m^{ed} \equiv m \pmod{pq}$.

Exemple :

Prenons $p = 5$, $q = 11$, donc $n = 55$ et $\varphi(n) = 40$. Avec $e = 3$, on trouve $d = 27$, car $81 = 2 \times 40 + 1$. Le message $m = 7$ se chiffre en $7^3 = 343 \equiv 13 \pmod{55}$. Le déchiffrement $13^{27} \pmod{55}$ redonne bien 7 .

Remarque :

Connaître $\varphi(n)$ revient à connaître p et q . En effet, $p + q = n - \varphi(n) + 1$ et $pq = n$: ce sont les racines d'un trinôme. C'est pourquoi $\varphi(n)$ doit rester secret. En pratique, p et q ont plusieurs centaines de chiffres.

Ce qu'il faut retenir

- Une relation d'équivalence partitionne un ensemble en classes ; toute application définie sur le quotient doit être **bien définie**.
- La congruence modulo n est compatible avec $+$ et $\times$; on ne simplifie que par un entier premier avec n .
- $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif à n éléments, obtenu par passage au quotient.
- $\bar{a}$ est inversible si et seulement si $\text{pgcd}(a, n) = 1$; on calcule l'inverse par Bézout.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
- $\varphi(n) = n \prod (1 - 1/p)$; si $\text{pgcd}(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$ (Euler), et $a^{p-1} \equiv 1 \pmod{p}$ (Fermat).
- On calcule une puissance modulo n en réduisant l'exposant, puis par exponentiation rapide.
- Théorème chinois : si $\text{pgcd}(m, n) = 1$, alors $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- Dans $\mathbb{F}_p$, p impair, il y a $\frac{p-1}{2}$ carrés non nuls, détectés par le critère d'Euler.
- RSA : $c = m^e$, $m = c^d$ modulo $n = pq$, avec $ed \equiv 1 \pmod{\varphi(n)}$.

Questions fréquentes sur arithmétique et $\mathbb{Z}/n\mathbb{Z}$

Pourquoi faut-il vérifier qu'une opération est bien définie sur $\mathbb{Z}/n\mathbb{Z}$?

Une classe possède une infinité de représentants. Une formule écrite avec un représentant n'a de sens que si le résultat ne dépend pas de ce choix. Par exemple, $\bar{x} \rightarrow \overline{2^x}$ n'est pas définie sur $\mathbb{Z}/3\mathbb{Z}$, car 2^0 et 2^3 ne sont pas congrus modulo 3.

Comment calcule-t-on l'inverse d'une classe modulo n ?

La classe $\bar{a}$ est inversible si et seulement si $\text{pgcd}(a, n) = 1$. On applique alors l'algorithme d'Euclide étendu pour écrire $au + nv = 1$. L'inverse est $\bar{u}$, qu'on vérifie en calculant au modulo n .

Quelle différence entre le théorème d'Euler et le petit théorème de Fermat ?

Le théorème d'Euler affirme $a^{\varphi(n)} \equiv 1 \pmod{n}$ dès que a est premier avec n . Le petit théorème de Fermat en est le cas particulier $n = p$ premier, où $\varphi(p) = p - 1$. Sa réciproque est fausse, comme le montrent 341 ou 561.

Le théorème chinois s'applique-t-il si les modules ne sont pas premiers entre eux ?

L'isomorphisme $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ exige $\text{pgcd}(m, n) = 1$. Sinon, un système de deux congruences a des solutions si et seulement si $a \equiv b$ modulo le pgcd. Dans ce cas, les solutions forment une seule classe modulo le ppcm.

Pour aller plus loin en L2

- Les énoncés : [exercices de maths en L2 sur arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre précédent : [Polynômes d'endomorphismes et trigonalisation](#)
- Chapitre suivant : [Groupes, sous-groupes et morphismes](#)
- Tester vos connaissances : [QCM de maths en L2 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L2](#) et la [licence de maths de L1 à L3](#)