

HAI507I

Calcul formel et scientifique

« Structures mathématiques »

Pascal Giorgi

Université de Montpellier
Faculté des Sciences



1. Les entiers modulaires

2. Anneaux, corps et groupes

Opérations de base

■ $\mathbb{Z} : 3 + 4 = 7; \quad 6 \times (-4) = -24; \quad 3 - 8 = -5$

■ $\mathbb{Q} : \frac{2}{3} + \frac{4}{5} = \frac{22}{15}; \quad \frac{7}{4} \times \frac{5}{6} = \frac{35}{24}; \quad \frac{2}{5} / \frac{11}{9} = \frac{18}{55}$

■ $\mathbb{R} : 2.35 + (-3.567) = -1.217; \quad 6.43 \times 12.2 = 78.446; \quad \pi/e = 1.15572\dots$

Pourquoi pas de division dans \mathbb{Z} ?

⇒ on ne parle pas de division Euclidienne (pour l'instant)

Opérations de base

- \mathbb{Z} : $3 + 4 = 7$; $6 \times (-4) = -24$; $3 - 8 = -5$
- \mathbb{Q} : $\frac{2}{3} + \frac{4}{5} = \frac{22}{15}$; $\frac{7}{4} \times \frac{5}{6} = \frac{35}{24}$; $\frac{2}{5} / \frac{11}{9} = \frac{18}{55}$
- \mathbb{R} : $2.35 + (-3.567) = -1.217$; $6.43 \times 12.2 = 78.446$; $\pi/e = 1.15572\dots$

Pourquoi pas de division dans \mathbb{Z} ?

⇒ on ne parle pas de division Euclidienne (pour l'instant)

Loi interne

- une opération est **interne** si le résultat reste dans le même ensemble que les entrées
 - ▶ \mathbb{Z} : $+$, $-$, \times sont internes, mais $/$ ne l'est pas!!!
 - ▶ \mathbb{Q}, \mathbb{R} : $+$, $-$, \times , $/$ sont toutes internes

Une opération et son inverse

Naturellement, $+$ va avec $-$ et \times avec $/$

\Rightarrow pourquoi ?

Une opération et son inverse

Naturellement, $+$ va avec $-$ et \times avec $/$

\Rightarrow pourquoi ?

Opération inverse

■ $c = a + b \Leftrightarrow a = c - b$

■ $f = d \times e \Leftrightarrow d = f / e$ ssi $e \neq 0$

Une opération et son inverse

Naturellement, $+$ va avec $-$ et \times avec $/$

\Rightarrow pourquoi ?

Opération inverse

$$\blacksquare c = a + b \Leftrightarrow a = c - b$$

$$\blacksquare f = d \times e \Leftrightarrow d = f/e \text{ ssi } e \neq 0$$

\Rightarrow L'opération inverse permet d'annuler l'opération :

$$\blacksquare (a + b) - b = a$$

$$\blacksquare (d \times e)/e = d$$

- L'inverse de a pour **l'addition** est l'unique élément b tel que $a + b = 0$
 - ▶ On le note $-a$; et on dit que **0 est le neutre pour l'addition**
 $\hookrightarrow a + 0 = a$
- L'inverse de a pour **la multiplication** est l'unique élément b tel que $a \times b = 1$
 - ▶ on le note : a^{-1} , et on dit que **1 est le neutre pour la multiplication**
 $= \hookrightarrow a \times 1 = a$
 - ▶ on dit simplement inverse

Division euclidienne dans \mathbb{Z}

Division de a par $b \Rightarrow$ quotient q et reste r tels que

- $a = b \times q + r$

- $0 \leq r < b$

Écriture unique : si $a < 0$ on impose que $r \geq 0$

Division euclidienne dans \mathbb{Z}

Division de a par $b \Rightarrow$ quotient q et reste r tels que

- $a = b \times q + r$

- $0 \leq r < b$

Écriture unique : si $a < 0$ on impose que $r \geq 0$

Exemple : $123/37 = \dots$ et $-107/37 = \dots$

Réduction modulo n

- La réduction de a modulo n correspond au reste de la division euclidienne de a par n
- on note cette opération : $a \bmod n$ ou $a \% n$ (en sage)

exemple : $18 \bmod 5 = 3$ ou $-18 \bmod 5 = 2$

Réduction modulo n

- La réduction de a modulo n correspond au reste de la division euclidienne de a par n
- on note cette opération : $a \bmod n$ ou $a \% n$ (en sage)

exemple : $18 \bmod 5 = 3$ ou $-18 \bmod 5 = 2$

Opérations modulo n

- L'addition modulo n de a et b est : $(a + b) \bmod n$
- L'opposé modulo n de a est : $(-a) \bmod n$
- La multiplication modulo n de a et b est : $(a \times b) \bmod n$

L'ensemble des entiers $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers $\{0, 1, 2, \dots, n-1\}$ muni des opérations modulo n

On parle d'arithmétique modulaire (on note les opérations sans le modulo) :

L'ensemble des entiers $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers $\{0, 1, 2, \dots, n-1\}$ muni des opérations modulo n

On parle d'arithmétique modulaire (on note les opérations sans le modulo) :

ex : $\mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

■ $7+5=2$

■ $7*4=8$

■ $3-7=6$

L'ensemble des entiers $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers $\{0, 1, 2, \dots, n-1\}$ muni des opérations modulo n

On parle d'arithmétique modulaire (on note les opérations sans le modulo) :

ex : $\mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

■ $7+5=2$

■ $7*4=8$

■ $3-7=6$

Autres exemples : $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/24\mathbb{Z}$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

■ $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ?$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

■ $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \bmod 10$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

- $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \bmod 10$
- $\mathbb{Z}/10\mathbb{Z} : 5^{-1} = ?$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

- $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \bmod 10$
- $\mathbb{Z}/10\mathbb{Z} : 5^{-1} = ? \rightarrow$ pas d'inverse, il n'existe aucun $b \in \mathbb{Z}/10\mathbb{Z}$ tel que $5 \times b = 1$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

- $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \bmod 10$
- $\mathbb{Z}/10\mathbb{Z} : 5^{-1} = ? \rightarrow$ pas d'inverse, il n'existe aucun $b \in \mathbb{Z}/10\mathbb{Z}$ tel que $5 \times b = 1$

\Rightarrow dans $\mathbb{Z}/n\mathbb{Z}$ tous les éléments ne sont pas inversibles

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

■ $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \pmod{10}$

■ $\mathbb{Z}/10\mathbb{Z} : 5^{-1} = ? \rightarrow$ pas d'inverse, il n'existe aucun $b \in \mathbb{Z}/10\mathbb{Z}$ tel que $5 \times b = 1$

\Rightarrow dans $\mathbb{Z}/n\mathbb{Z}$ tous les éléments ne sont pas inversibles

$\mathbb{Z}/11\mathbb{Z} :$

$1^{-1} = 1 ; 2^{-1} = 6 ; 3^{-1} = 4 ; 4^{-1} = 3 ; 5^{-1} = 9 ; 6^{-1} = 2 ;$

$7^{-1} = 8 ; 8^{-1} = 7 ; 9^{-1} = 5 ; 10^{-1} = 10 ; 0^{-1} = \text{X} ;$

Inverse et division dans $\mathbb{Z}/n\mathbb{Z}$

La division est une conséquence de l'inversion : $a/b = a \times (1/b) = a \times b^{-1}$

L'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ est l'unique $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

Exemple

■ $\mathbb{Z}/10\mathbb{Z} : 3^{-1} = ? \rightarrow 3^{-1} = 7$ car $3 \times 7 = 1 \bmod 10$

■ $\mathbb{Z}/10\mathbb{Z} : 5^{-1} = ? \rightarrow$ pas d'inverse, il n'existe aucun $b \in \mathbb{Z}/10\mathbb{Z}$ tel que $5 \times b = 1$

\Rightarrow dans $\mathbb{Z}/n\mathbb{Z}$ tous les éléments ne sont pas inversibles

$\mathbb{Z}/11\mathbb{Z} :$

$1^{-1} = 1 ; 2^{-1} = 6 ; 3^{-1} = 4 ; 4^{-1} = 3 ; 5^{-1} = 9 ; 6^{-1} = 2 ;$

$7^{-1} = 8 ; 8^{-1} = 7 ; 9^{-1} = 5 ; 10^{-1} = 10 ; 0^{-1} = \text{X} ;$

\Rightarrow 0 n'est jamais inversible!!!

Quels sont les inversibles dans $\mathbb{Z}/n\mathbb{Z}$

$a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $\text{pgcd}(a, n) = 1$

Démonstration.

via théorème Bezout : si $\text{pgcd}(a, b) = g$ alors il existe u, v tels que $a \times u + b \times v = g$

Comme $\text{pgcd}(a, n) = 1 \Rightarrow a \times u + n \times v = 1$ donc $u = a^{-1} \bmod n$



Quels sont les inversibles dans $\mathbb{Z}/n\mathbb{Z}$

$a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $\text{pgcd}(a, n) = 1$

Démonstration.

via théorème Bezout : si $\text{pgcd}(a, b) = g$ alors il existe u, v tels que $a \times u + b \times v = g$

Comme $\text{pgcd}(a, n) = 1 \Rightarrow a \times u + n \times v = 1$ donc $u = a^{-1} \bmod n$



L'algorithme $\text{EUCLIDEETENDU}(a, b)$ permet de calculer (g, u, v) tels que :

- $g = \text{pgcd}(a, b)$
- $au + bv = g$ (coefficients de Bézout)

Algorithme d'Euclide étendu

On considère deux entiers $a > b$

EUCLIDEETENDU(a, b)

1. Si $b = 0$: renvoyer $(a, 1, 0)$
2. $(q, r) = \text{DIVISIONEUCLIDIENNE}(a, b)$
3. $(d_1, u_1, v_1) = \text{EUCLIDEETENDU}(b, r)$
4. Renvoyer $(d_1, v_1, u_1 - qv_1)$

Idées générale : $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$

Algorithme d'Euclide étendu

On considère deux entiers $a > b$

EUCLIDEETENDU(a, b)

1. Si $b = 0$: renvoyer $(a, 1, 0)$
2. $(q, r) = \text{DIVISIONEUCLIDIENNE}(a, b)$
3. $(d_1, u_1, v_1) = \text{EUCLIDEETENDU}(b, r)$
4. Renvoyer $(d_1, v_1, u_1 - qv_1)$

Idées générale : $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$

■ comme $r = a - qb$ on a $d_1 = u_1b + v_1(a - qb)$

Algorithme d'Euclide étendu

On considère deux entiers $a > b$

EUCLIDEETENDU(a, b)

1. Si $b = 0$: renvoyer $(a, 1, 0)$
2. $(q, r) = \text{DIVISIONEUCLIDIENNE}(a, b)$
3. $(d_1, u_1, v_1) = \text{EUCLIDEETENDU}(b, r)$
4. Renvoyer $(d_1, v_1, u_1 - qv_1)$

Idées générale : $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$

- comme $r = a - qb$ on a $d_1 = u_1b + v_1(a - qb)$
- qui se réécrit $d_1 = v_1a + (u_1 - qv_1)b$

Algorithme d'Euclide étendu

On considère deux entiers $a > b$

EUCLIDEETENDU(a, b)

1. Si $b = 0$: renvoyer $(a, 1, 0)$
2. $(q, r) = \text{DIVISIONEUCLIDIENNE}(a, b)$
3. $(d_1, u_1, v_1) = \text{EUCLIDEETENDU}(b, r)$
4. Renvoyer $(d_1, v_1, u_1 - qv_1)$

Idées générale : $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$

- comme $r = a - qb$ on a $d_1 = u_1b + v_1(a - qb)$
- qui se réécrit $d_1 = v_1a + (u_1 - qv_1)b$

⇒ La complexité de l'algorithme est de $O(\log^3(a))$

Cas p premier

Si p est premier, $\text{pgcd}(a, p) = 1$ pour tout $0 < a < p$

- tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles
 - on calcule dans $\mathbb{Z}/p\mathbb{Z}$ « comme dans \mathbb{Q} », même structure (un corps)
-

Cas p premier

Si p est premier, $\text{pgcd}(a, p) = 1$ pour tout $0 < a < p$

- tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles
 - on calcule dans $\mathbb{Z}/p\mathbb{Z}$ « comme dans \mathbb{Q} », même structure (un corps)
-

Cas n non premier

Si k divise n , $\text{pgcd}(k, n) = k$

- tous les élt de $\mathbb{Z}/n\mathbb{Z}$ ayant un diviseur commun non trivial avec n ne sont pas inversibles
- on ne peut calculer dans $\mathbb{Z}/n\mathbb{Z}$ que « comme dans \mathbb{Z} », même structure (un anneau)

Opérations et possibles inverses

- \mathbb{Z} : addition, multiplication, opposé, ~~inverse~~
- \mathbb{Q} : addition, multiplication, opposé, inverse
- \mathbb{R} : addition, multiplication, opposé, inverse
- $\mathbb{Z}/n\mathbb{Z}$: addition, multiplication, opposé, ~~inverse~~ (n non premier)
- $\mathbb{Z}/p\mathbb{Z}$: addition, multiplication, opposé, inverse (p premier)

⇒ Quand il n'y a pas d'inverse on parle de structure d'anneau, sinon c'est un corps

1. Les entiers modulaires

2. Anneaux, corps et groupes

Structures algébriques de base

Definition

Un anneau est un ensemble \mathcal{A} dans lequel

- on dispose de deux **opérations internes** : **addition**(+) et **multiplication**(\times)
- tout élément possède un opposé
- plus des conditions (commutativité, associativité, distributivité) :

$$a + b = b + a; (a \times b) \times c = a \times (b \times c), a \times (b + c) = a \times b + a \times c; (a + b) \times c = a \times c + b \times c$$

Structures algébriques de base

Definition

Un anneau est un ensemble \mathcal{A} dans lequel

- on dispose de deux **opérations internes** : **addition**(+) et **multiplication**(\times)
- tout élément possède un opposé
- plus des conditions (commutativité, associativité, distributivité) :
$$a + b = b + a; (a \times b) \times c = a \times (b \times c), a \times (b + c) = a \times b + a \times c; (a + b) \times c = a \times c + b \times c$$

Definition

un corps est un ensemble \mathcal{K} pour lequel

- $(\mathcal{K}, +, \times)$ est un anneau
- tout élément **non-nul** de \mathcal{K} possède un inverse

⇒ le neutre pour la multiplication doit être différent du neutre pour l'addition

Exemples d'anneau est de corps

Anneaux

- \mathbb{Z}
- $\mathbb{Z}/n\mathbb{Z}$ (n non premier)
- $\mathbb{R}[X]$: polynômes à coeffs réel
- $\mathcal{A}[X]$: polynômes à coeffs dans l'anneau \mathcal{A}
- $\mathcal{M}_n(\mathbb{Z})$: matrices à coeffs entiers

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 3 & 4 \end{bmatrix}$$

Corps

- $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ avec p premier
- \mathbb{R}, \mathbb{C}
- \mathbb{Q} : les rationnels
- $\mathbb{R}(X)$: fract rationnelles à coeffs réels

$$\frac{1.2 + 3X}{2X} + \frac{2}{1 + X} = \frac{1.5X^3 + 2.1X^2 + 0.6X + 2}{X + 1}$$

- $\mathcal{K}(X)$: fract rationnelles à coeff dans \mathcal{K}
-

Exemples d'anneau est de corps

Anneaux

- \mathbb{Z}
- $\mathbb{Z}/n\mathbb{Z}$ (n non premier)
- $\mathbb{R}[X]$: polynômes à coeffs réel
- $\mathcal{A}[X]$: polynômes à coeffs dans l'anneau \mathcal{A}
- $\mathcal{M}_n(\mathbb{Z})$: matrices à coeffs entiers

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 3 & 4 \end{bmatrix}$$

Corps

- $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ avec p premier
- \mathbb{R}, \mathbb{C}
- \mathbb{Q} : les rationnels
- $\mathbb{R}(X)$: fract rationnelles à coeffs réels

$$\frac{1.2 + 3X}{2X} + \frac{2}{1+X} = \frac{1.5X^3 + 2.1X^2 + 0.6X + 2}{X+1}$$

- $\mathcal{K}(X)$: fract rationnelles à coeff dans \mathcal{K}

Attention :

- \mathbb{N} n'est ni un anneau ni un corps
- $GL_n(\mathbb{Q})$: les matrices inversibles $n \times n$ sur \mathbb{Q} ne forment ni un anneau ni un corps

Propriété : si a, b sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ alors $a \times b$ aussi

$$\Rightarrow (a \times b)^{-1} = a^{-1} \times b^{-1}$$

Retour à $\mathbb{Z}/n\mathbb{Z}$ avec n non premier

Propriété : si a, b sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ alors $a \times b$ aussi

$$\Rightarrow (a \times b)^{-1} = a^{-1} \times b^{-1}$$

Conséquences

Soit $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$

- \times est une opération interne de $(\mathbb{Z}/n\mathbb{Z})^*$
- \times est une opération inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$
- $+$ n'est pas une opération interne!!!

Exemple : $(\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$

Groupe multiplicatif

Definition

Un groupe multiplicatif est un ensemble G dans lequel

- on dispose d'une loi interne \times
- tout élément possède un inverse

$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ est donc un groupe multiplicatif !!!

Groupe multiplicatif

Definition

Un groupe multiplicatif est un ensemble G dans lequel

- on dispose d'une loi interne \times
- tout élément possède un inverse

$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ est donc un groupe multiplicatif !!!

Remarques :

- 0 ne peut pas appartenir à un groupe multiplicatif
- Définition similaire d'un groupe additif (avec $+$ comme loi interne)

Exemple de groupes multiplicatifs : $\{-1, 1\}$, $\mathbb{Q}^* = \mathbb{Q}/\{0\}$,

Groupe multiplicatif

Definition

Un groupe multiplicatif est un ensemble G dans lequel

- on dispose d'une loi interne \times
- tout élément possède un inverse

$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ est donc un groupe multiplicatif !!!

Remarques :

- 0 ne peut pas appartenir à un groupe multiplicatif
- Définition similaire d'un groupe additif (avec $+$ comme loi interne)

Exemple de groupes multiplicatifs : $\{-1, 1\}$, $\mathbb{Q}^* = \mathbb{Q}/\{0\}$, et plein d'autres, des idées ?

Definition

La fonction indicatrice d'Euler $\phi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ associe à un entier naturel non-nul n , le nombre d'entiers plus petit que n qui sont premiers avec lui.

$$\phi(n) = \text{card}\{x \in \mathbb{N}^* / x < n \text{ et } \gcd(x, n) = 1\}$$

Remarques :

- $\phi(n)$ donne la taille du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$
- quand p est premier $\phi(p) = p - 1$
- quand $n = p \times q$ avec p, q premiers $\phi(n) = (p - 1) \times (q - 1)$

Definition

La fonction indicatrice d'Euler $\phi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ associe à un entier naturel non-nul n , le nombre d'entiers plus petit que n qui sont premiers avec lui.

$$\phi(n) = \text{card}\{x \in \mathbb{N}^* / x < n \text{ et } \gcd(x, n) = 1\}$$

Remarques :

- $\phi(n)$ donne la taille du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$
- quand p est premier $\phi(p) = p - 1$
- quand $n = p \times q$ avec p, q premiers $\phi(n) = (p - 1) \times (q - 1)$

$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ est un groupe cyclique : $\forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^*, \alpha^{\phi(n)} = 1$

Une application concrète : chiffrement RSA

Méthode utilisant une clé publique (connue de tous) pour chiffrer et une clé privée (connue uniquement par son propriétaire) pour déchiffrer.

⇒ protocole cryptographique utilisé dans les cartes bancaires ou https

Une application concrète : chiffrement RSA

Méthode utilisant une clé publique (connue de tous) pour chiffrer et une clé privée (connue uniquement par son propriétaire) pour déchiffrer.

⇒ protocole cryptographique utilisé dans les cartes bancaires ou https

Principe :

■ Génération des clés

1. On choisit 2 premiers p, q aléatoires et on calcule $N = p \times q$ et $\phi(N) = (p - 1) \times (q - 1)$
2. On choisit un entier $e < N$ aléatoire tq $\gcd(e, \phi(N)) = 1 \longrightarrow$ clé publique (e, N)
3. On calcule $d = e^{-1} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^* \longrightarrow$ clé privée (d)

Une application concrète : chiffrement RSA

Méthode utilisant une clé publique (connue de tous) pour chiffrer et une clé privée (connue uniquement par son propriétaire) pour déchiffrer.

⇒ protocole cryptographique utilisé dans les cartes bancaires ou https

Principe :

■ Génération des clés

1. On choisit 2 premiers p, q aléatoires et on calcule $N = p \times q$ et $\phi(N) = (p - 1) \times (q - 1)$
2. On choisit un entier $e < N$ aléatoire tq $\gcd(e, \phi(N)) = 1 \rightarrow$ clé publique (e, N)
3. On calcule $d = e^{-1} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^* \rightarrow$ clé privée (d)

■ chiffrement d'un message clair $m \in \mathbb{Z}/N\mathbb{Z} : c \leftarrow m^e \bmod N$

Une application concrète : chiffrement RSA

Méthode utilisant une clé publique (connue de tous) pour chiffrer et une clé privée (connue uniquement par son propriétaire) pour déchiffrer.

⇒ protocole cryptographique utilisé dans les cartes bancaires ou https

Principe :

■ Génération des clés

1. On choisit 2 premiers p, q aléatoires et on calcule $N = p \times q$ et $\phi(N) = (p - 1) \times (q - 1)$
2. On choisit un entier $e < N$ aléatoire tq $\gcd(e, \phi(N)) = 1 \rightarrow$ clé publique (e, N)
3. On calcule $d = e^{-1} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^* \rightarrow$ clé privée (d)

■ chiffrement d'un message clair $m \in \mathbb{Z}/N\mathbb{Z} : c \leftarrow m^e \bmod N$

■ déchiffrement d'un message chiffré $c : m' \leftarrow c^d \bmod N$

Une application concrète : chiffrement RSA

Méthode utilisant une clé publique (connue de tous) pour chiffrer et une clé privée (connue uniquement par son propriétaire) pour déchiffrer.

⇒ protocole cryptographique utilisé dans les cartes bancaires ou https

Principe :

■ Génération des clés

1. On choisit 2 premiers p, q aléatoires et on calcule $N = p \times q$ et $\phi(N) = (p - 1) \times (q - 1)$
2. On choisit un entier $e < N$ aléatoire tq $\gcd(e, \phi(N)) = 1 \rightarrow$ clé publique (e, N)
3. On calcule $d = e^{-1} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^* \rightarrow$ clé privée (d)

■ chiffrement d'un message clair $m \in \mathbb{Z}/N\mathbb{Z} : c \leftarrow m^e \bmod N$

■ déchiffrement d'un message chiffré $c : m' \leftarrow c^d \bmod N$

Remarque :

les clés vivent dans $(\mathbb{Z}/\phi(N)\mathbb{Z})^*$ alors que les messages sont dans $(\mathbb{Z}/N\mathbb{Z})^*$

Justification de RSA

Pourquoi ça marche ?

- $m' = (m^e)^d \in \mathbb{Z}/N\mathbb{Z} \implies m' = m^{1+k\phi(N)} = m$ car $ed = 1 \bmod \phi(N)$ et $m^{\phi(N)} = 1 \bmod N$
- le calcul de $c = m^e$ et $m' = c^d$ dans $\mathbb{Z}/n\mathbb{Z}$ est facile : $O(\log^3 N)$ opérations sur les bits

Justification de RSA

Pourquoi ça marche ?

- $m' = (m^e)^d \in \mathbb{Z}/N\mathbb{Z} \implies m' = m^{1+k\phi(N)} = m$ car $ed = 1 \bmod \phi(N)$ et $m^{\phi(N)} = 1 \bmod N$
- le calcul de $c = m^e$ et $m' = c^d$ dans $\mathbb{Z}/n\mathbb{Z}$ est facile : $O(\log^3 N)$ opérations sur les bits

Pourquoi c'est sûr ?

- un attaquant ne connaît que e , N et c et il doit trouver un m tq $c = m^e$ dans $\mathbb{Z}/N\mathbb{Z}$
 \hookrightarrow Pb du logarithme discret (**très difficile**) : $m = \log_e(c) \bmod N$

Justification de RSA

Pourquoi ça marche ?

- $m' = (m^e)^d \in \mathbb{Z}/N\mathbb{Z} \implies m' = m^{1+k\phi(N)} = m$ car $ed = 1 \bmod \phi(N)$ et $m^{\phi(N)} = 1 \bmod N$
- le calcul de $c = m^e$ et $m' = c^d$ dans $\mathbb{Z}/n\mathbb{Z}$ est facile : $O(\log^3 N)$ opérations sur les bits

Pourquoi c'est sûr ?

- un attaquant ne connaît que e , N et c et il doit trouver un m tq $c = m^e$ dans $\mathbb{Z}/N\mathbb{Z}$
 \hookrightarrow Pb du logarithme discret (**très difficile**) : $m = \log_e(c) \bmod N$
- idées d'attaque :
 - ▶ brute force : on teste tous les $m \in \mathbb{Z}/N\mathbb{Z}$: **trop coûteux**, complexité de $O(N)$
 - ▶ factoriser N pour trouver $\phi(N)$ puis la clé secrète d : **trop coûteux**, complexité de $O(\sqrt{N})$

\Rightarrow toutes les attaques ont une complexité exponentielle ou sous-exponentielle

Groupe, anneau, corps

- **Groupe multiplicatif** : multiplication interne et tous les éléments sont inversibles
- **Anneau** : addition/multiplication internes et tous les éléments ont un opposé
- **Corps** : anneau dans lequel tous les éléments non-nul sont inversibles

Remarques

- un corps privé de 0 est un groupe multiplicatif
- $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour tout n , est un corps si n est premier
- Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ forment le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ qui a $\phi(n)$ éléments

