Structures mathématiques

HAI507I – Calcul formel et scientifique

Bruno Grenet

Université de Montpellier – Faculté des Sciences

1. Les entiers modulaires

2. Anneaux, corps et groupes

Calcul dans $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{Z}$

Opérations de base

- $\mathbb{Z}$: $3 + 4 = 7$; $6 \times (-4) = -24$; $3 - 8 = -5$
- $\mathbb{Q}$: $\frac{2}{3} + \frac{4}{5} = 22/15$; $\frac{7}{4} \times \frac{5}{6} = 35/24$; $\frac{2}{5}/\frac{11}{9} = 18/55$
- $\mathbb{R}$: $2,35 + (-3,567) = -1,217$; $6,43 \times 12,2 = 78,446$; $\pi/e = 1,15572...$

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 l'entrée
  - $\mathbb{Z}$: $+, -, \times$ sont internes, mais $/$ ne l'est pas
  - $\mathbb{Q}, \mathbb{R}$: $+, -, \times, /$ sont internes

Opérations et inverses

Naturellement, $+$ va avec $-$ et $\times$ avec $/$: pourquoi ?

Opération inverse

- $c = a + b \Leftrightarrow a = c - b$
- $c = a \times b \Leftrightarrow a = c/b$ (si $b \neq 0$)

$\rightarrow$ $-$ est l'opération inverse de $+$, et $/$ l'opération inverse de $\times$

Élément inverse

- L'*inverse de a pour l'addition* est l'unique élément b tel que $a + b = 0$
  - Noté $-a$; 0 est le *neutre pour l'addition* $\rightarrow a + 0 = a$
  - On dit plutôt *opposé*
- L'*inverse de a pour la multiplication* est l'unique élément b tel que $a \times b = 1$
  - Noté a^{-1} ; 1 est le *neutre pour la multiplication* : $a \times 1 = a$
  - On dit simplement *inverse*

Calculs *modulo n*

123 | 37
111 | 3
12
r
q

Division euclidienne dans $\mathbb{Z}$

- Division de a par b : quotient q et reste r tels que
  - $a = bq + r$
  - $0 \leq r < b$
- Attention au cas de $a < 0 \to$ on veut $r \geq 0$ quand même
- Remarque : écriture unique

Réduction *modulo n*

- La réduction *modulo n* de $a \in \mathbb{Z}$ est le reste dans la division euclidienne de a par n
- Notation : $a \bmod n$ $\longrightarrow$ a % n

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

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

- Remarque : on note les opérations sans le « $\bmod n$ »

$n = 10$

$\mathbb{Z}/_{10}\mathbb{Z} = \{0, \ldots, 9\}$

$7 + 5 = 2$

$3 \times 8 = 4$

$-7 = 3$

$\mathbb{Z}/_{24}\mathbb{Z}$

$23 + 5 = 4$

$10 \times 5 = 2$

$-3 = 21$

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

Inverse de a dans $\mathbb{Z}/n\mathbb{Z}$: $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \times b = 1$

$\mathbb{Z}/_{10}\mathbb{Z}$: $3^{-1} \overset{?}{=} 7$ car $3 \times 7 = 1$

$5^{-1} \overset{?}{=} \times$

$\mathbb{Z}/_{11}\mathbb{Z}$: $1^{-1} = 1$ $2^{-1} = 6$ $3^{-1} = 4$ $4^{-1} = 3$ $5^{-1} = 9$ $0^{-1} = \times$

$6^{-1} = 2$ $7^{-1} = 8$ $8^{-1} = 7$ $9^{-1} = 5$ $10^{-1} = 10$

Algorithme d'Euclide étendu

EUCLIDEETENDU(a, b) $(a > b)$

1. Si $b = 0$: renvoyer $(a, 1, 0)$ → $a = a \times 1 + b \times 0$
2. $(q, r) \leftarrow$ DIVISIONEUCLIDIENNE(a, b) → $a = bq + r$
3. $(d, u_1, v_1) \leftarrow$ EUCLIDEETENDU(b, r) $d = u_1 b + v_1 r$
4. Renvoyer $(d, v_1, u_1 - qv_1)$

↳ $v_1 a + (u_1 - q v_1) b = v_1 (bq + r) + (u_1 - v_1 q) b = v_1 r + u_1 b = d$

$\Theta(\log a \log b)$

↳ $\boxed{\Theta(\log^3 a)}$

Propriété

- EUCLIDEETENDU(a, b) renvoie (d, u, v) tels que
  - $d = \text{PGCD}(a, b)$
  - $d = au + bv$ (*coefficients de Bézout*)

Conséquence

- Si $\text{PGCD}(a, n) = 1$, il existe u, v tels que $au + nv = 1 \rightarrow a \times u \bmod n = 1$
- Si a a un inverse *modulo* n, alors $\text{PGCD}(a, n) = 1$

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

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

Cas p premier

Si p est premier, $\text{PGCD}(a, p) = 1$ pour tout $a \neq 0$ $a \in \mathbb{Z}/_p\mathbb{Z}$

- Tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles
- On peut calculer dans $\mathbb{Z}/p\mathbb{Z}$ « comme dans $\mathbb{Q}$ »

Cas n non premier

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

- Certains éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ ne sont pas inversibles
- On ne peut calculer dans $\mathbb{Z}/n\mathbb{Z}$ que « comme dans $\mathbb{Z}$ »

1. Les entiers modulaires

2. Anneaux, corps et groupes

Opérations et leurs inverses

Opérations et inverses possibles

- $\mathbb{Z}$: 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)

Définitions

- Un anneau est un ensemble A dans lequel
  - on dispose des deux opérations internes addition & multiplication
  - tout élément possède un opposé
  - plus quelques conditions à respecter : $a \times (b + c) = a \times b + a \times c, \ldots$
- Un corps est un ensemble K dans lequel
  - on dispose des deux opérations internes addition & multiplication
  - tout élément possède un opposé
  - tout élément *non nul* possède un inverse   + élément neutre de l'addition
  - plus les mêmes quelques conditions

Exemples d'anneaux et de corps

Rien

$\mathbb{N}$

Anneaux

$\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ (n non premier)

$\mathbb{R}[X]$

$A[X]$ où A est un anneau

$M_n(\mathbb{R})$: matrices n lignes n colonnes à coeff. dans $\mathbb{R}$

$M_n(A)$ où A est un anneau

Fcts de $\mathbb{R}$ dans $\mathbb{R}$

Corps

$\mathbb{Z}/7\mathbb{Z} \rightsquigarrow \mathbb{Z}/p\mathbb{Z}$ (p premier)

$\mathbb{R}$ $\qquad$ $\mathbb{C}$

$\mathbb{Q}$

$\mathbb{R}(X)$: fractions rationnelles

$K(X)$ où K est un corps

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

Remarque

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

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

Conséquence

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

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

$$\left(\mathbb{Z}/10\mathbb{Z}\right)^\times = \{1, 3, 7, 9\}$$

Groupe multiplicatif

Définition

Un groupe multiplicatif est un ensemble G dans lequel

- on dispose d'**une** opération interne : multiplication
- tout élément possède un inverse

Remarques

- 0 ne peut pas être dans un groupe multiplicatif
- Définition similaire de groupe *additif*

Exemples de groupes multiplicatifs

$(\mathbb{Z}/n\mathbb{Z})^\times$ $\{-1, 1\}$ $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$

$\mathbb{R}^\times$

$K^\times := K \setminus \{0\}$ où K est un corps

$GL_n(K)$: matrices inversibles sur K

RSA

- Méthode de *chiffrement à clef publique*
  - Une clef *publique* pour chiffrer, connue de tout le monde
  - Une clef *privée* pour déchiffrer, connue uniquement de son propriétaire
- Version présentée ici non sûre, mais idée principale

Principe

- Génération des clefs :
  - On choisit deux premiers p, q aléatoires
  - On calcule $N = p \times q$ et $\varphi(N) = (p-1) \times (q-1)$
  - On choisit $e \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^\times$, aléatoire $\to$ *clef publique* (e, N)
  - On calcule $d = e^{-1} \in \mathbb{Z}/\varphi(N)\mathbb{Z} \to$ *clef privée* e d

  $\mathcal{O}(\log^k N)$
- Chiffrement d'un message clair $m \in \mathbb{Z}/N\mathbb{Z}$: $c \leftarrow m^e$ $(= m \times m \times \cdots \times m)$
- Déchiffrement d'un message chiffré c : $\tilde{m} \leftarrow c^d$

  $\mathcal{O}(\log^k N)$

Remarque

- Travail avec deux « $\mathbb{Z}/n\mathbb{Z}$ » : $n = N$ et $n = \varphi(N)$

Justification de RSA

Pourquoi ça marche ?

- $\tilde{m} = c^d = (m^e)^d = m^{e\times d} = m^{1+k\varphi(N)} = m \times (m^{\varphi(N)})^k = m \times 1 = m$
  - Admis : pour tout $m \in \mathbb{Z}/N\mathbb{Z}$, $\boxed{m^{\varphi(N)} = 1}$
- Avec la clef publique : il suffit de calculer m^d dans $\mathbb{Z}/N\mathbb{Z} \to$ exponentiation rapide
- Avec la clef privée : il suffit de calculer $m^e \to$ idem

Pourquoi c'est sûr ?

- Un attaquant connaît d, N et c et cherche m tel que $m^d = c$ dans $\mathbb{Z}/N\mathbb{Z}$
- Hypothèse (non démentie) : étant donné d, N, c, difficile de calculer m
- Exemples d'approches pour l'attaquant :
  - Trouver directement m : tester tous les m possibles ? $\to \mathcal{O}(N)$
  - Factoriser N, calculer $\varphi(N)$ et inverser d dans $\mathbb{Z}/\varphi(N)\mathbb{Z} \to e$
  - Calculer directement $\varphi(N)$ sans factoriser

$\to \mathcal{O}(\sqrt{N}) \to$ ou mieux

Conclusion

Groupes, anneaux, corps

- Groupe multiplicatif : multiplication interne, inverse pour tous les éléments
- Anneau : addition et multiplication internes, opposé pour tous les éléments
- Corps : addition et multiplication internes, opposé pour tous les éléments, inverse pour tous les éléments non nuls

Remarque

- Corps : anneau tel que tout élément non nul est inversible
- Corps privé de $0 \to$ groupe multiplicatif

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

- Anneau pour tout n ; corps si n est premier
- Inversibles de $\mathbb{Z}/n\mathbb{Z}$: $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe multiplicatif