Arithmétique modulaire

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

5 octobre 2016

Arithmétique modulaire

Le "groupe de l'horloge"

Heures :

- $2h + 5h = 7h$
- $9h + 4h = 1h \quad \text{mod } 12h$
- $8h + 12h = 8h$

Minutes :

- $45 + 25 = 10 \quad \text{mod } 60 \text{ min}$
- $50 + 30 = 20 \quad \text{mod } 60 \text{ min}$

Addition modulaire $\mathbb{Z}_7$

Notation : $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $2 + 4 = 6$
- $4 + 5 = 9 = 7 + 2 = 2 \mod 7$
- $3 + 4 = 0$

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Groupe additif $(\mathbb{Z}_n, +)$

$(\mathbb{Z}_n, +)$ forme un **groupe commutatif d'ordre** n.

Définition

Un groupe est un couple ensemble-loi de composition $(\mathbb{G}, \star)$ qui vérifie

- **associativité :** $\forall a, b, c, \in \mathbb{G}$: $(a \star b) \star c = a \star (b \star c)$
- **élement neutre :** $\exists e \in \mathbb{G}, \forall a \in \mathbb{G}$: $a \star e = e \star a = a$
- **inversion :** $\forall a \in \mathbb{G}, \exists b \in \mathbb{G}$: $a \star b = b \star a = e$

Propriétés

- **commutativité :** $\forall a, b, c, \in \mathbb{G}$: $a \star b = b \star a$
- **ordre de $\mathbb{G}$:** nombre d'éléments du groupe $\mathbb{G}$

Multiplication modulaire $\mathbb{Z}_7$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $3 \times 5 = 5 + 5 + 5 = 10 + 5$
  $= 3 + 5 = 8 = 7 + 1$
  $= 1 \mod 7$
- $3 \times 5 = 15 = 2 \cdot 7 + 1$
  $= 1 \mod 7$
- $6 \times 4 = 24 = 3 \cdot 7 + 3 = 3 \mod 7$

$\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication modulaire $\mathbb{Z}_7$ et $\mathbb{Z}_8$

$\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Anneau $(\mathbb{Z}_n, +, \cdot)$

$(\mathbb{Z}_n, +, \cdot)$ forme un **anneau commutatif**.

Définition

Un anneau est un triplet, ensemble et deux lois de composition, $(\mathbb{G}, +, \cdot)$ qui vérifie

- $(\mathbb{G}, +)$ est un groupe commutatif avec élement neutre 0
- **associativité :** $\forall a, b, c, \in \mathbb{G}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **élement neutre :** $\exists e \in \mathbb{G}, \forall a \in \mathbb{G}$: $a \cdot e = e \cdot a = a$
- **distributivité :** $\forall a, b, c \in \mathbb{G}$: $a \cdot (b + c) = a \cdot b + a \cdot c$

Propriétés

- **anneau commutatif :** $\forall a, b, c, \in \mathbb{G}$: $a \cdot b = b \cdot a$
- **élément inversible :** $a \neq 0$ est inversible par rapport à $\cdot$ si $\exists b \in \mathbb{G}$: $a \cdot b = b \cdot a = e$

Inverse modulaire $\mathbb{Z}_7$

Inverse de a modulo n :

L'entier $b = a^{-1}$ tel que $a \times b = 1 \mod n$

Notation : $\mathbb{Z}_n^* =$ L'ensemble des éléments inversibles de $\mathbb{Z}_n$

- $\mathbb{Z}_7^\star = \{1, 2, 3, 4, 5, 6\}$
- $3^{-1} = 5 \mod 7$
- $4^{-1} = 2 \mod 7$
- $6^{-1} = 6 \mod 7$

$\mathbb{Z}_7^\star$

$\times$	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

Inverse modulaire $\mathbb{Z}_8$

- 2,4 et 6 sont *non-inversibles*
- 1,3,5 et 7 sont *inversibles* (et leur propre inverse !)
- attention aux écritures
  - éviter ~~$3 = 1/3$~~
  - proscrire ~~$\sqrt{1} = 3$~~
- écrire $3^{-1} = 3$

$\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Inverse modulaire $\mathbb{Z}_6$

Que faire avec $\mathbb{Z}_6$?

- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
- $5^{-1} = 5 \bmod 6$
- $4^{-1} =?? \bmod 6$

  L'inverse de 4 *n'est pas défini* modulo 6

$\mathbb{Z}_6$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Il « reste » $\{1, 5\}$: $\mathbb{Z}_6^\star$

$\times$	1	5
1	1	5
5	5	1