Mathématiques pour l'informatique 1

Cours 7 - Arithmétique modulaire

Émilie Charlier

Université de Liège

Arithmétique modulaire

Definition

Pour tout naturel $m \geq 2$, nous notons $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. Nous définissons deux opérations binaires sur cet ensemble, appelée addition modulo m et multiplication modulo m :

$$+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,\ (i,j) \mapsto \mathrm{MOD}(i+j, m)$$

et

$$\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,\ (i,j) \mapsto \mathrm{MOD}(i \cdot j, m).$$

Autrement dit, pour tous $i, j \in \mathbb{Z}_m$, on a

$$i +_m j = \mathrm{MOD}(i+j, m) \quad \text{et} \quad i \cdot_m j = \mathrm{MOD}(ij, m).$$

Tables d'addition et de multiplication dans $\mathbb{Z}_5$ et $\mathbb{Z}_6$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	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

Dans la suite de cette section, m désigne toujours un entier ≥ 2.

Faire des calculs dans $\mathbb{Z}_m$ peut rapidement s'avérer fastidieux si l'on ne remarque pas qu'il revient au même d'effectuer les calculs dans $\mathbb{Z}$ et de "réduire modulo m" à la fin (ou à n'importe quel moment qui nous arrange d'ailleurs). Ceci est l'objet du résultat pratique suivant.

Proposition

Soient $x, y, k \in \mathbb{Z}$. Alors

1. $\mathrm{MOD}(x, m) = \mathrm{MOD}(y, m) \iff x - y$ est multiple de m.
2. $\mathrm{MOD}(x + km, m) = \mathrm{MOD}(x, m)$.
3. $\mathrm{MOD}(x + y, m) = \mathrm{MOD}(\mathrm{MOD}(x, m) + y, m)$
4. $\mathrm{MOD}(x \cdot y, m) = \mathrm{MOD}(\mathrm{MOD}(x, m) \cdot y, m)$

Démonstration

Supposons que

$$x = qm + r \quad \text{et} \quad y = q'm + r',$$

avec $q, q' \in \mathbb{Z}$ et $r, r' \in \mathbb{Z}_m$. On a donc

$$r = \mathrm{MOD}(x, m) \quad \text{et} \quad r' = \mathrm{MOD}(y, m).$$

1. $\mathrm{MOD}(x, m) = \mathrm{MOD}(y, m) \iff x - y$ est multiple de m.

On a $x - y = (q - q')m + r - r'$.

Comme $r - r' \in \{-m + 1, \ldots, 0, \ldots, m - 1\}$, on obtient que

$$\begin{aligned} x - y \text{ est multiple de } m &\iff r - r' \text{ est multiple de } m \\ &\iff r - r' = 0 \\ &\iff r = r' \\ &\iff \mathrm{MOD}(x, m) = \mathrm{MOD}(y, m). \end{aligned}$$

2. $\mathrm{MOD}(x + km, m) = \mathrm{MOD}(x, m)$.

Le point 2 découle directement du point 1.

3. $\mathrm{MOD}(x+y,m) = \mathrm{MOD}(\mathrm{MOD}(x,m)+y,m)$
4. $\mathrm{MOD}(x\cdot y,m) = \mathrm{MOD}(\mathrm{MOD}(x,m)\cdot y,m)$

On a

$$x+y = qm+r+y \quad \text{et} \quad xy = qmy+ry.$$

En utilisant le point 2, on obtient

$$\mathrm{MOD}(x+y,m) = \mathrm{MOD}(r+y,m) \quad \text{et} \quad \mathrm{MOD}(xy,m) = \mathrm{MOD}(ry,m),$$

comme souhaité. □

Ce résultat implique que toute égalité dans $\mathbb{Z}$ est aussi vérifiée "modulo m".

Par exemple, l'égalité $27 = 2 \cdot 8 + 11$ donne

- $1 = 0 \cdot_2 0 +_2 1$ dans $\mathbb{Z}_2$
- $0 = 2 \cdot_3 2 +_3 2$ dans $\mathbb{Z}_3$
- $3 = 2 \cdot_4 0 +_4 3$ dans $\mathbb{Z}_4$
- $2 = 2 \cdot_5 3 +_5 1$ dans $\mathbb{Z}_5$
- etc.

Propriétés de l'addition et la multiplication modulaires

Proposition

Pour tout $i, j, k \in \mathbb{Z}_m$, nous avons

1.	$(i +_m j) +_m k = i +_m (j +_m k)$	associativité de $+_m$
2.	$(i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$	associativité de $\cdot_m$
3.	$i \cdot_m (j +_m k) = i \cdot_m j \ +_m \ i \cdot_m k$	distributivité de $\cdot_m$ sur $+_m$
4.	$i +_m j = j +_m i$	commutativité de $+_m$
5.	$i \cdot_m j = j \cdot_m i$	commutativité de $\cdot_m$
6.	$0 +_m i = i +_m 0 = i$	0 est neutre pour $+_m$
7.	$1 \cdot_m i = i \cdot_m 1 = i$	1 est neutre pour $\cdot_m$
8.	$i +_m (m - i) = 0$ si $i \neq 0$	l'opposé de $i \neq 0$ est $m - i$

Démonstration

Cela découle des mêmes propriétés sur les entiers et de la proposition précédente.

Remarques

- L'associativité permet de donner du sens aux écritures

$$i +_m j +_m k \quad \text{et} \quad i \cdot_m j \cdot_m k$$

  puisque l'ordre dans lequel on effectue ces opérations n'a pas d'importance.
- L'addition par un élément de $\mathbb{Z}_m$ est injective :

$$i +_m j = i +_m k \implies j = k.$$

- On ne peut pas définir un ordre $<$ de $\mathbb{Z}_m$ tel que

$$x < y \implies \forall z,\ x + z < y + z.$$

Nous avons facilement identifié les opposés des éléments de $\mathbb{Z}_m$: l'opposé d'un élément i de $\mathbb{Z}_m$ est simplement $m - i$ si $i \neq 0$ et 0 sinon.

Déterminer les inverses est par contre plus délicat.

Lemme

Soient $i, j, j' \in \mathbb{Z}_m$. Alors $i \cdot_m j = i \cdot_m j' = 1 \implies j = j'$.

Démonstration.

Supposons que $i \cdot_m j = i \cdot_m j' = 1$.

En utilisant la proposition précédente, on en déduit que

$$\begin{aligned} j &= j \cdot_m 1 \\ &= j \cdot_m (i \cdot_m j') \\ &= (j \cdot_m i) \cdot_m j' \\ &= (i \cdot_m j) \cdot_m j' \\ &= 1 \cdot_m j' \\ &= j'. \end{aligned}$$

Le lemme précédent nous dit que si un élément possède un inverse, alors celui-ci est unique.

Definition

Un élément i de $\mathbb{Z}_m$ est inversible modulo m s'il existe j dans $\mathbb{Z}_m$ tel que $i \cdot_m j = 1$.

Au vu du lemme précédent, il ne peut exister qu'un seul tel élément j et lorsqu'il existe, celui-ci est appelé l'inverse de i modulo m.

On dit aussi que i est un élément inversible de $\mathbb{Z}_m$.

Exemples

- Dans le cas de $\mathbb{Z}_6$, seuls 1 et 5 sont inversibles modulo 6.

  On vérifie en effet que dans la table de multiplication, les lignes correspondants aux éléments 0, 2, 3 et 4 ne contiennent pas l'élément 1, mais que 1 apparaît bien dans les lignes correspondants à 1 et 5.

$\cdot_6$	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

- Dans le cas de $\mathbb{Z}_5$, toutes les lignes de la table de multiplication, excepté celle de 0, contiennent 1.

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ceci montre que tous les éléments non nuls de $\mathbb{Z}_5$ sont inversibles.

Caractérisation des éléments inversibles de $\mathbb{Z}_m$

Théorème

Un élément i de $\mathbb{Z}_m$ est inversible modulo m si et seulement si i et m sont premiers entre eux.

Démonstration.

Soit i un élément inversible de $\mathbb{Z}_m$.

Alors il existe $j \in \mathbb{Z}_m$ tel que $i \cdot_m j = 1$, càd tel que $\mathrm{MOD}(ij, m) = 1$.

Il existe donc $q \in \mathbb{N}$ tel que $ij = qm + 1$, et donc tel que $ij - qm = 1$.

Par le théorème de Bézout, i et m sont premiers entre eux.

Réciproquement, soit i un élément de $\mathbb{Z}_m$ premier avec m.

Par le théorème de Bézout, il existe $a, b \in \mathbb{Z}$ tels que $1 = ai + bm$.

On obtient que $1 = \mathrm{MOD}(ai, m) = \mathrm{MOD}(a, m) \cdot_m i$.

Donc i est inversible dans $\mathbb{Z}_m$ et son inverse est $\mathrm{MOD}(a, m)$. □

Exemples

- Dans le cas de $\mathbb{Z}_6$, seuls 1 et 5 sont inversibles modulo 6.

  En effet, les éléments de $\mathbb{Z}_6$ premiers avec 6 sont exactement 1 et 5.
- Dans le cas de $\mathbb{Z}_5$, tous les éléments non nuls sont inversibles modulo 5.

  En effet, tous les éléments non nuls de $\mathbb{Z}_5$ sont premiers avec 5.

Remarque importante
La preuve du théorème précédent montre que la recherche d'un inverse modulaire peut de faire à l'aide de l'algorithme d'Euclide.

Ceci sera très utile pour résoudre des équations dans $\mathbb{Z}_m$.

Ces exemples sont des cas particuliers du résultat général suivant.

Théorème

Tous les éléments non nuls de $\mathbb{Z}_m$ sont inversibles si et seulement si m est un nombre premier.

Démonstration.

Ceci découle directement du théorème précédent et du fait que m est premier avec $1, 2, \ldots, m-1$ si et seulement si m est un nombre premier. □

Remarque
La multiplication par un élément quelconque de $\mathbb{Z}_m$ n'est pas toujours injective !

Par exemple, on a $2 \cdot_6 1 = 2 \cdot_6 4$ dans $\mathbb{Z}_6$.

Néanmoins, il est vrai que la multiplication par un élément inversible de $\mathbb{Z}_m$ est injective.

Proposition
Pour tout $i \in \mathbb{Z}_m$ inversible modulo m, la fonction

$$\mathbb{Z}_m \to \mathbb{Z}_m,\ j \mapsto i \cdot_m j$$

est injective.

Démonstration.
Soit k l'inverse de i dans $\mathbb{Z}_m$ et soient $j, j' \in \mathbb{Z}_m$ tels que $i \cdot_m j = i \cdot_m j'$.

Alors $j = k \cdot_m i \cdot_m j = k \cdot_m i \cdot_m j' = j'$. □

Consignes pour les exercices

- Vous n'avez pas le droit d'utiliser de calculatrice !

  Il faudra donc d'être efficace, et ne pas passer en revue toutes les valeurs possibles pour x.
- Lorsqu'on demande de résoudre une équation du type

$$ax + b = 0$$

  dans $\mathbb{Z}_m$, les opérations de multiplication et d'addition doivent être interprétées comme étant réellement $\cdot_m$ et $+_m$.

Exercices

1. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{21}$.

   Comme $\mathrm{pgcd}(10, 21) = 1$, nous savons que 10 est inversible dans $\mathbb{Z}_{21}$.

   Puisque $21 - 2 \cdot 10 = 1$, on obtient que $\mathrm{MOD}(-2, 21) = 19$ est l'inverse de 10 dans $\mathbb{Z}_{21}$.

   Ainsi, en supposant que $x \in \mathbb{Z}_{21}$, on a les équivalences suivantes :

$$\begin{aligned} 10 \cdot_{21} x +_{21} 8 = 0 &\iff 10 \cdot_{21} x = 13 \\ &\iff x = 19 \cdot_{21} 13 \\ &\iff x = \mathrm{MOD}(19 \cdot 13, 21) \\ &\iff x = \mathrm{MOD}((-2) \cdot (-8), 21) \\ &\iff x = 16. \end{aligned}$$

   L'équation $10x + 8 = 0$ a donc 16 comme unique solution dans $\mathbb{Z}_{21}$.

2. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{12}$.

Comme $\mathrm{pgcd}(10, 12) = 2$, 10 n'est pas inversible dans $\mathbb{Z}_{12}$.

En supposant que $x \in \mathbb{Z}_{12}$, on a les équivalences suivantes :

$$
\begin{aligned}
10 \cdot_{12} x +_{12} 8 = 0 \quad &\Longleftrightarrow \quad 10 \cdot_{12} x = 4 \\
&\Longleftrightarrow \quad \mathrm{MOD}(10x, 12) = 4 \\
&\Longleftrightarrow \quad \exists q \in \mathbb{Z},\ 10x = 12q + 4 \\
&\Longleftrightarrow \quad \exists q \in \mathbb{Z},\ 5x = 6q + 2 \\
&\Longleftrightarrow \quad \mathrm{MOD}(5x, 6) = 2 \\
&\Longleftrightarrow \quad 5 \cdot_6 \mathrm{MOD}(x, 6) = 2.
\end{aligned}
$$

Comme $\mathrm{pgcd}(5,6) = 1$, nous savons que 5 est inversible dans $\mathbb{Z}_6$.

L'inverse de 5 dans $\mathbb{Z}_6$ est 5 puisque $5 \cdot_6 5 = 1$.

On obtient les équivalences suivantes :

$$\begin{aligned} 5 \cdot_6 \mathrm{MOD}(x,6) = 2 &\iff \mathrm{MOD}(x,6) = 5 \cdot_6 2 \\ &\iff \mathrm{MOD}(x,6) = 4 \\ &\iff \exists q \in \mathbb{Z},\ x = 6q + 4 \\ &\iff x = 4 \ \text{ ou } \ x = 10. \end{aligned}$$

Les solutions de l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{12}$ sont donc 4 et 10.

3. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{15}$.

Comme $\mathrm{pgcd}(10, 15) = 5$, 10 n'est pas inversible dans $\mathbb{Z}_{15}$.

En supposant que $x \in \mathbb{Z}_{15}$, on a les équivalences suivantes :

$$\begin{aligned} 10 \cdot_{15} x +_{15} 8 = 0 \quad &\Longleftrightarrow \quad 10 \cdot_{15} x = 7 \\ &\Longleftrightarrow \quad \mathrm{MOD}(10x, 15) = 7 \\ &\Longleftrightarrow \quad \exists q \in \mathbb{Z},\ 10x = 15q + 7 \end{aligned}$$

Mais si on a $7 = 10x - 15q$ avec $x, q \in \mathbb{Z}$, alors 7 doit nécessairement être un multiple de $\mathrm{pgcd}(10, 15) = 5$.

Comme ce n'est pas le cas (7 n'est pas multiple de 5), on obtient donc qu'il ne peut exister d'entiers x et q tels que $10x = 15q + 7$.

Par conséquent, l'équation $10x + 8 = 0$ n'a pas de solution dans $\mathbb{Z}_{15}$.