
CRY 2024

Groupes

Alexandre Duc


1. Groupe Additif \mathbb{Z}_m
2. Inverse Modulaire
3. Groupe Multiplicatif \mathbb{Z}_m^*
4. Fonction Indicatrice d'Euler
5. Ordres et Générateurs

Groupe

Définition (Groupe)

Un **groupe** (\mathbb{G}, \star) est un ensemble \mathbb{G} muni d'une opération \star qui vérifie les propriétés suivantes :


- Pour tous les éléments $a, b \in \mathbb{G}$, le résultat de $a \star b$ appartient également à \mathbb{G} (**Loi Interne**).
- Pour tous les éléments $a, b, c \in \mathbb{G}$, l'égalité $(a \star b) \star c = a \star (b \star c)$ est vraie (**Associativité**).
- Il existe un élément $e \in \mathbb{G}$ tel que pour tout $a \in \mathbb{G}$, on a $a \star e = e \star a = a$ (**Élément Neutre**).
- Pour tout élément $a \in \mathbb{G}$, il existe un élément $b \in \mathbb{G}$ tel que $a \star b = b \star a = e$ (**Élément Symétrique**).

 Un groupe (\mathbb{G}, \star) pour lequel $a \star b = b \star a$ pour tout $a, b \in \mathbb{G}$ est appelé **commutatif**, ou **abélien**.

Groupe Additif \mathbb{Z}_m

Théorème (Groupe Abélien)

L'ensemble $\mathbb{Z}_m = \{0, 1, \dots, m-2, m-1\}$ muni de l'addition modulo m , où $m > 0$ est un entier naturel non-nul, est un groupe abélien.

 On appelle parfois l'élément symétrique d'un groupe additif, un **opposé** ou un **inverse additif**.

Élément Symétrique

Question

Quel est l'élément symétrique de 12 dans \mathbb{Z}_{15} ?

Quel est l'élément symétrique de 0 dans \mathbb{Z}_7 ?

Addition et Soustraction Modulaires

Exemples

Prenons $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

- $-5 \equiv 1 \pmod{6}$ vu que $1 + 5 \equiv 0 \pmod{6}$.
- $4 - 3 \equiv 4 + (-3) \equiv 4 + 3 \equiv 1 \pmod{6}$.
- $5 - 2 \equiv 5 + (-2) \equiv 5 + 4 \equiv 3 \pmod{6}$.

1. Groupe Additif \mathbb{Z}_m

2. Inverse Modulaire

3. Groupe Multiplicatif \mathbb{Z}_m^*

4. Fonction Indicatrice d'Euler

5. Ordres et Générateurs

But

But

Nous allons essayer de définir un groupe multiplicatif modulo n .
Pour cela, nous devons définir ce qu'est un inverse multiplicatif.

Inverse Modulaire

Définition (Inverse Modulaire)

Un entier a est **inversible** modulo m si l'équation $ax \equiv 1 \pmod{m}$ possède une solution $x \in \mathbb{Z}$.

- 👉 $ax \equiv 1 \pmod{m}$ possède une solution $x \in \mathbb{Z}$ si l'équation $ax + ym = 1$ possède une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
- 👉 On note a^{-1} **l'inverse modulaire** (ou inverse multiplicatif) de a .

Inverse Modulaire

Théorème (Inverse Modulaire)

a est inversible modulo m si et seulement si $\text{pgcd}(a, m) = 1$.

Calcul de l'Inverse Modulaire

Pour **calculer** l'inverse de a modulo m (lorsqu'il existe) :

- Trouver **l'identité de Bézout** $ax + my = 1$ à l'aide de l'algorithme d'Euclide étendu.
- L'inverse modulaire de a est $a^{-1} \equiv x \pmod{m}$.

Inverse Modulaire

Exemples

- $12^{-1} \equiv 310 \pmod{3719}$ car on a $1 = (-1) \cdot 3719 + 310 \cdot 12$.
- $1345^{-1} \equiv 1609 \pmod{2322}$ car $1 = 413 \cdot 2322 - 713 \cdot 1345$.
- Un nombre entier est inversible modulo 15 s'il ne possède pas de facteur premier avec 15. Ainsi, les nombres inversibles modulo 15 sont $\{1, 2, 4, 7, 8, 11, 13, 14\}$. En effet,
 $1^2 \equiv 2 \cdot 8 \equiv 4^2 \equiv 7 \cdot 13 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$.

Multiplication Modulaire

- Il n'est **pas toujours possible** de simplifier les équations du type $ac \equiv bc \pmod{m}$ en écrivant $a \equiv b \pmod{m}$.
- Par exemple, $3 \cdot 12 \equiv 3 \cdot 2 \pmod{6}$, mais $12 \not\equiv 2 \pmod{6}$.
- Par contre, $3 \cdot 12 \equiv 3 \cdot 2 \pmod{5}$ peut être simplifié en $12 \equiv 2 \pmod{5}$, car 3 et 5 ne possèdent pas de facteur en commun.
- 👉 On peut simplifier une équation du type $ac \equiv bc \pmod{m}$ uniquement lorsque c et m sont premiers entre eux.
- 👉 La simplification correspond à un **division** par c , ce qui est une **multiplication par l'inverse modulaire**.

Arithmétique modulaire

Propriétés

Voici quelques propriétés utiles lorsque l'on effectue des calculs modulaires :

- $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m.$
- $ab \bmod m = (a \bmod m)(b \bmod m) \bmod m.$
- $a^b \bmod m = (a \bmod m)^b \bmod m.$

1. Groupe Additif \mathbb{Z}_m
2. Inverse Modulaire
3. Groupe Multiplicatif \mathbb{Z}_m^*
4. Fonction Indicatrice d'Euler
5. Ordres et Générateurs

Autres groupes ?


Question

- Est-ce que l'ensemble $\{0, 2, 4, 6, 8\}$ muni de l'addition modulo 10 est un groupe ?
- Est-ce que l'ensemble $\{0, 1, \dots, m-1\}$ muni de la multiplication modulo $m > 1$ est un groupe ?
- Est-ce que l'ensemble $\{2, 4, 6, 8\}$ muni de la multiplication modulo 10 est un groupe ?

Groupe Multiplicatif \mathbb{Z}_m^*

Théorème (Groupe Multiplicatif \mathbb{Z}_m^*)

L'ensemble $\mathbb{Z}_m^* = \{1 \leq a \leq m : \text{pgcd}(a, m) = 1\}$ muni de la multiplication modulo m , où $m > 0$ est un entier naturel non-nul, est un groupe abélien.

 L'addition n'a pas de sens dans un groupe multiplicatif!

Groupe Multiplicatif \mathbb{Z}_m^*

Exemples

- $\mathbb{Z}_6^* = \{1, 5\}$ et $1^2 \equiv 5^2 \equiv 1 \pmod{6}$.
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ et $1^2 \equiv 11^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{12}$.
- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ et $1^2 \equiv 2 \cdot 4 \equiv 3 \cdot 5 \equiv 6^2 \equiv 1 \pmod{7}$.

Groupe Multiplicatif \mathbb{Z}_p^*

Théorème (Groupe Multiplicatif \mathbb{Z}_p^*)

Pour p premier, l'ensemble $\{1, 2, \dots, p-1\}$ muni de la multiplication modulo p est un groupe abélien et est noté \mathbb{Z}_p^* .

- 👉 Il est ainsi possible de multiplier et de diviser (c'est-à-dire de multiplier par l'inverse modulaire) modulo p dans \mathbb{Z}_p^* .
- 👉 Pour un nombre $a \in \mathbb{Z}_p^*$, on notera $a^i \bmod p$ l'opération $\underbrace{a \cdot a \cdots a}_{i \text{ fois}} \bmod p$, opération que l'on appelle **exponentiation modulaire**.
- 👉 Pour un nombre $c = a^b \bmod p$, on dit que b est le **logarithme discret** en base a de c modulo p .

Groupe Multiplicatif \mathbb{Z}_p^*

Exemples

- $2/5 \pmod{7} \equiv 2 \cdot (5^{-1}) \pmod{7} \equiv 2 \cdot 3 \pmod{7} \equiv 6 \pmod{7}$
- $5^3 \pmod{7} = 6$. Donc le logarithme discret en base 5 de 6 modulo 7 est 3.

1. Groupe Additif \mathbb{Z}_m
2. Inverse Modulaire
3. Groupe Multiplicatif \mathbb{Z}_m^*
4. Fonction Indicatrice d'Euler
5. Ordres et Générateurs

Indicatrice d'Euler

Définition (Indicatrice d'Euler)

On note $\varphi(n)$ le nombre d'éléments dans $\{1, \dots, n\}$ qui sont premiers avec n .

Par exemple :

- $\varphi(1) = 1$
- $\varphi(2) = 1$
- $\varphi(3) = 2$
- $\varphi(4) = 2$
- $\varphi(12) = 4$
- $\varphi(17) = 16$
- $\varphi(100) = 40$
- $\varphi(65537) = 65536$

Calcul de l'Indicatrice d'Euler

- Si p est un nombre premier, alors $\varphi(p) = p - 1$.
- Si p est premier et $k > 1$, $\varphi(p^k) = (p - 1)p^{k-1}$.
- Si $\text{pgcd}(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$
- 👉 Si $p \neq q$ sont des nombres premiers, alors $\varphi(pq) = (p - 1)(q - 1)$.

Calcul de l'Indicatrice d'Euler

Méthode Condensée

$$\varphi(n) = n \prod_{p \text{ premier divise } n} \left(1 - \frac{1}{p}\right)$$

- Par exemple :

$$\varphi(12) = 12 \cdot \prod_{p \in \{2,3\}} \left(1 - \frac{1}{p}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

1. Groupe Additif \mathbb{Z}_m
2. Inverse Modulaire
3. Groupe Multiplicatif \mathbb{Z}_m^*
4. Fonction Indicatrice d'Euler
5. Ordres et Générateurs

Ordre d'un Groupe

Définition (Ordre d'un Groupe)

Dans un groupe fini, **l'ordre du groupe** est le **nombre d'éléments dans ce groupe**.

- L'ordre du groupe additif \mathbb{Z}_{12} est de 12.
- L'ordre du groupe multiplicatif \mathbb{Z}_7^* est de 6.


Question

Quel est l'ordre du groupe multiplicatif \mathbb{Z}_{12}^* ?

Ordre d'un Élément

Définition (Ordre d'un Élément)

Dans un groupe fini (noté multiplicativement), l'**ordre d'un élément** $a \in \mathbb{G}$ est le plus petit exposant entier $i \geq 1$ tel que $a^i = 1$.

 Si \mathbb{G} a n éléments et s'il existe un élément $g \in \mathbb{G}$ tel que g, g^2, g^3, \dots, g^n soient tous différents, on dit que \mathbb{G} est un **groupe cyclique**, et l'élément g est appelé un **générateur** (ou élément primitif) du groupe \mathbb{G} .

Ordre d'un Élément

Exemples

Par exemple, pour \mathbb{Z}_7^* :

- L'ordre de 1 est égal à 1.
- L'ordre de 2 est égal à 3, puisque $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$.
- L'ordre de 3 est égal à 6, puisque $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$. 3 est donc un générateur de \mathbb{Z}_7^* .

Théorème de Lagrange

Théorème (Joseph-Louis Lagrange, 1771)

L'ordre $\text{ord}(a)$ d'un élément a d'un groupe fini divise l'ordre du groupe (le nombre d'éléments du groupe).

En poursuivant avec l'exemple de \mathbb{Z}_7^* , on observe que $\text{ord}(1) = 1$, $\text{ord}(2) = 3$, $\text{ord}(3) = 6$, $\text{ord}(4) = 3$, $\text{ord}(5) = 6$ et $\text{ord}(6) = 2$, qui divisent tous le nombre d'éléments de \mathbb{Z}_7^* , qui est égal à 6.

Problème

Question

Montrer que 2 n'est pas un générateur de \mathbb{Z}_{17}^* .

Théorème de Fermat-Euler

Le théorème suivant est appelé le **petit théorème de Fermat**.

Théorème (Pierre de Fermat, 1640)

Si p est un nombre premier, et si a est un entier non-divisible par p , alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Il a été généralisé par le mathématicien bâlois Leonhard Euler :

Théorème (Leonhard Euler, 1761)

Si n est un entier naturel et a **un entier premier avec n** , alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Exercice

Question

Calculez à la main

$$7^{123456} \bmod 13$$

et

$$7^{1234569} \bmod 15$$

Conséquence

Conséquence

Si $\text{pgcd}(a, n) = 1$, $a^b \pmod n \equiv a^{b \bmod \varphi(n)} \pmod n$.

Problème

Question

Quels sont les trois derniers chiffres de 9^{9999} ?

Solutions

Élément Symétrique

Question

Quel est l'élément symétrique de 12 dans \mathbb{Z}_{15} ?

Quel est l'élément symétrique de 0 dans \mathbb{Z}_7 ?

Solution

3

0

Autres groupes ?

Question

- Est-ce que l'ensemble $\{0, 2, 4, 6, 8\}$ muni de l'addition modulo 10 est un groupe ?
- Est-ce que l'ensemble $\{0, 1, \dots, m-1\}$ muni de la multiplication modulo $m > 1$ est un groupe ?
- Est-ce que l'ensemble $\{2, 4, 6, 8\}$ muni de la multiplication modulo 10 est un groupe ?

Solution

- Oui.
- Non. 0 n'est pas inversible ainsi que parfois d'autres éléments.
- Oui. L'élément neutre est le 6.

Problème

Question

Montrer que 2 n'est pas un générateur de \mathbb{Z}_{17}^* .

Solution

L'ordre de \mathbb{Z}_{17}^* est de 16. On calcule alors simplement l'ordre de 2 qui doit diviser 16. $2^2 = 4, 2^4 = 16, 2^8 = 1$. L'ordre de 2 est de 8 et n'est donc pas un générateur.

Exercice

Question

Calculez à la main

$$7^{123456} \bmod 13$$

et

$$7^{123456} \bmod 15$$

Solution

Le petit théorème de Fermat nous permet de simplifier l'exposant modulo $p - 1$ et le théorème d'Euler de simplifier l'exposant modulo $\varphi(n)$ lorsque la base est première avec le module. Nous obtenons donc

$$7^{123456} \bmod 13 = 7^0 = 1$$

et

$$7^{1234569} \bmod 15 = 7^{1234569 \bmod 8} \bmod 15 = 7^1 = 7$$

Problème

Question

Quels sont les trois derniers chiffres de 9^{9999} ?

Solution

On cherche à calculer

$$9^{9999} \bmod 1000 = 9^{9999 \bmod 400} \bmod 1000 = 9^{-1} \bmod 1000 = 889.$$