

Arithmétique modulaire

Pierre Mathonet

Département de Mathématique
Faculté des Sciences

Liège, novembre 2019

Les vérifications et notations

Proposition 6.1.1

Pour tout entier m supérieur ou égal à 2, la relation d'égalité modulo m est une relation d'équivalence.

Preuve : Simple exercice.

Définition 6.1.2

On appelle \mathbb{Z}_m le quotient $\mathbb{Z}/\equiv_m = \mathbb{Z}/m\mathbb{Z}$.

Remarque : L'ensemble $m\mathbb{Z}$ est constitué des multiples de m .

Quelques exemples

- Les horloges n'ont que douze heures. Alors, si à 10h, on ajoute 4 heures, on se retrouve à 2h : les horloges comptent **modulo 12h**.
- Les interrupteurs à poussoir classiques comptent **modulo 2** impulsions.
- On peut imaginer des interrupteurs plus sophistiqué, avec 0 : éteint, 1 : faible, 2 : moyenne, 3 : fort, 4 : insoutenable, 5 : éteint. On compte les impulsions **modulo 5**.

Définition 6.1.1

Soit m un entier supérieur ou égal à 2. On définit la relation d'égalité modulo m dans \mathbb{Z} par $x \equiv_m y$, si et seulement si, il existe $k \in \mathbb{Z}$ tel que $y = x + km$. On dit alors que y est égal (ou congru) à x modulo m et on note aussi $x = y \pmod{m}$.

Division et cardinal de \mathbb{Z}_m

Proposition 6.1.2

Pour tout $n \in \mathbb{Z}$ et $d \in \mathbb{Z}_0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ satisfaisant les conditions

- 1 $n = qd + r$;
- 2 $0 \leq r < |d|$.

Existence : Traiter le cas $d > 0$ (diviser -17 par 5 ...), puis passer à $d < 0$.

Unicité : Supposer que $n = q_1d + r_1 = q_2d + r_2$, montrer PA que $r_1 = r_2$...

Proposition 6.1.3

Pour tout entier $m \geq 2$, l'application f qui à $[x]$, ($x \in \mathbb{Z}$) associe le reste de la division de x par m est une bijection entre \mathbb{Z}_m et $\{0, \dots, m-1\}$. En particulier, le cardinal de \mathbb{Z}_m est m .

4 **Preuve :** L'application est bien définie, injective, et surjective.

Addition dans \mathbb{Z}_m

Définition 6.1.3

L'addition de \mathbb{Z}_m est l'application

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m : ([x], [y]) \mapsto [x] + [y] = [x + y].$$

Oui mais Raoul...

Proposition 6.1.4

L'addition dans \mathbb{Z}_m est bien définie. De plus, elle munit \mathbb{Z}_m d'une structure de groupe commutatif.

Définition 6.1.4

La multiplication de \mathbb{Z}_m est l'application

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m : ([x], [y]) \mapsto [x] \cdot [y] = [x \cdot y].$$

Oui mais Raoul...

Proposition 6.1.5

La multiplication dans \mathbb{Z}_m est bien définie. De plus, elle permet de munir \mathbb{Z}_m d'une structure d'anneau commutatif.

5

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Les champs \mathbb{Z}_p

On regarde les tables de multiplications de \mathbb{Z}_3 et \mathbb{Z}_4 :

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

On voit que \mathbb{Z}_3 est un champ et pas \mathbb{Z}_4 . En effet :

Proposition 6.2.2

Tout corps est intègre.

et donc

Proposition 6.2.3

Pour tout $m \geq 2$, si m n'est pas premier, alors \mathbb{Z}_m n'est pas un corps.

7

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Une petite application : critères de divisibilité

Divisibilité par 3 :

Divisibilité par 3

Un nombre n est divisible par 3 ssi la somme de ses chiffres est divisible par 3.

Exemple : 2148 est divisible par 3 car $2 + 1 + 4 + 8 = 15$ car 2148 est divisible par 3 ssi $[2148] = [0]$, dans \mathbb{Z}_3 . Mais on a

$$[2148] = [2 \cdot 10^3 + 1 \cdot 10^2 + 4 \cdot 10 + 8] = [2] \cdot [10]^3 + [1] \cdot [10]^2 + [4][10] + [8],$$

et puisque $[10] = [1]$, on a

$$[2148] = [2] + [1] = [4] + [8] = [2 + 4 + 1 + 8].$$

Preuve en général : On a $n = a_l \dots a_0$ si, et seulement si, $n = \sum_{k=0}^l a_k 10^k$. On a alors

$$[n] = \sum_{k=0}^l [a_k][10]^k = \sum_{k=0}^l [a_k] = [\sum_{k=0}^l a_k],$$

6

et on conclut de la même façon.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Inversibilité et résolution d'équations

Proposition 6.2.5

Dans un anneau $(A, +, 0, \cdot, 1)$ on considère l'équation $ax + b = 0$. Les cas suivants peuvent se produire.

- ① Si a est inversible, alors cette équation admet la solution unique $-a^{-1}b$;
- ② En général, cette équation n'admet une solution que si b est dans l'image de l'application de multiplication à gauche par a définie par $G_a : A \rightarrow A : x \mapsto ax$;
- ③ En général, si cette équation admet une solution x_0 , alors l'ensemble de ses solutions est donné par

$$S = \{x_0 + y : ay = 0\}.$$

Preuve : Cas particulier d'un résultat sur les systèmes linéaires en algèbre.

8

Exemples : Dans \mathbb{Z}_4 , l'équation $2x = 3$ n'est pas compatible, alors que $2x = 2$ admet deux solutions. Trouvez d'autres exemples dans \mathbb{Z}_6 .

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Les dernières questions, et une définition

- 1 Quand l'anneau \mathbb{Z}_m est-il un champ ?
- 2 Si \mathbb{Z}_m n'est pas un champ, alors quand un élément de \mathbb{Z}_m est-il inversible ?
- 3 Dans les deux cas, comment calculer l'inverse d'un élément $a \in \mathbb{Z}_m$, lorsqu'il existe ?

Définition 6.2.2

Si $a, b \in \mathbb{Z}$ sont non nuls, alors le plus grand commun diviseur (PGCD) de a et b est le nombre entier d strictement positif satisfaisant :

- 1 $d|a$ et $d|b$;
- 2 Si $c|a$ et $c|b$, alors $c \leq d$.

Ce nombre est noté $\text{pgcd}(a, b)$.

Définition 6.2.3

Pour tous $a, b \in \mathbb{Z}_0$, on définit l'ensemble des diviseurs positifs de a et b :

$$E_{a,b} = \{c \in \mathbb{Z} : c > 0, c|a \text{ et } c|b\}$$

9

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Existence, unicité, et calcul

Proposition 6.2.6

Si $a, b \in \mathbb{Z}$ sont non nuls, alors le plus grand commun diviseur de a et b existe et est unique.

Existence : $E_{a,b} \subset \{1, \dots, |a|\}$. **Unicité :** Habituelle.

Remarque : $\max E_{a,0} = |a|$.

Proposition 6.2.7

Pour tous $a, b \in \mathbb{Z}_0$, on a

$$\text{pgcd}(a, b) = \text{pgcd}(-a, b) = \text{pgcd}(a, -b) = \text{pgcd}(-a, -b).$$

Intérêt : On se ramène à deux nombres positifs pour calculer le pgcd.

10

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

L'algorithme d'Euclide I

Proposition 6.2.8

Pour tous $a, b \in \mathbb{Z}_0$ et tout $m \in \mathbb{Z}$, on a
 $\text{pgcd}(a, b) = \text{pgcd}(a, b + ma)$.

Intérêt : Si $b > a$, on remplace b par le reste de la division de b par a , et on a un nombre plus petit.

Exemple : Calculer le pgcd de 246 et 752.

Proposition 6.2.9 - Algorithme d'Euclide

Soient deux nombres entiers a, b tels que $b \geq a > 0$. On pose $a = r_0$ et on écrit la suite de divisions

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{j-1} &= r_jq_{j+1} + r_{j+1} \\ &\vdots \\ r_{j-1} &= r_jq_{j+1} + 0. \end{aligned}$$

11 Alors le dernier reste non nul r_j est le pgcd de a et b .

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Le théorème de Bezout

Théorème de Bezout

Si $a, b \in \mathbb{Z}$ sont non nuls et si $d = \text{pgcd}(a, b)$, alors il existe $x_0, y_0 \in \mathbb{Z}$ tels que $d = ax_0 + by_0$.

Preuve : Preuve existentielle dans les notes, mais dans l'algorithme d'Euclide, chaque reste est une combinaison entière des deux précédents.

Algorithme complet

Si $a, b \in \mathbb{Z}_0$ sont tels que $\text{pgcd}(a, b) = d$, on complète l'algorithme d'Euclide :

$$\begin{aligned} b &= aq_1 + r_1 & r_1 &= b - aq_1 \\ a &= r_1q_2 + r_2 & r_2 &= a - r_1q_2 \\ r_1 &= r_2q_3 + r_3 & r_3 &= r_1 - r_2q_3 \\ &\vdots & &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j & r_j &= r_{j-2} - r_{j-1}q_j \\ r_{j-1} &= r_jq_{j+1} + 0. & & \end{aligned}$$

12 On sait que $d = r_j$. On remplace successivement les restes par leur valeur en fonction des restes précédents. Cela permet d'exprimer r_j en fonction de a et b .

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Les résultats

Définition 6.2.4

Deux nombres entiers non nuls sont premiers entre eux si leur pgcd vaut 1.

Proposition 6.2.10

Deux nombres entiers non nuls a et b sont premiers entre eux si, et seulement si, il existe $x_0, y_0 \in \mathbb{Z}$ tels que $ax_0 + by_0 = 1$.

Proposition 6.2.11

L'élément $x = [a] \in \mathbb{Z}_m \setminus \{0\}$ est inversible si, et seulement si, a est premier avec m .

Comment inverser $[a]$? On cherche $[b]$ tel que $ab + km = 1$...

Exemple : Calculer l'inverse de 11 dans \mathbb{Z}_{26} .

Proposition 6.2.12

L'anneau \mathbb{Z}_p est un champ si, et seulement si p est premier.