TD 8 : Arithmétique modulaire

christina.boura@uvsq.fr

16 novembre 2020

1 Définition

Rappel : On dit définit la relation *d'équivalence modulo* n par

$$a \equiv b \mod n \quad \Leftrightarrow \quad n \mid (a-b).$$

On note $\bar{a}$ la *classe d'équivalence* de a modulo n, ou simplement a lorsque cela est clair du contexte.

1. Montrer qu'il s'agit bien d'une relation d'équivalence.

   On doit montrer que cette relation sur $\mathbb{Z}$ est réflexive, symétrique et transitive.

   Réflexive : Pour tout $a \in \mathbb{Z}$ on a que $a \equiv a \mod n$ puisque n'importe quel entier positif n divise toujours $(a-a) = 0$.

   Symétrique On doit montrer que pour tout $a, b \in \mathbb{Z}$, si $a \equiv b \mod n$ alors $b \equiv a \mod n$. On suppose que $a \equiv b \mod n$. Par définition, on a qu'il existe un entier $k \in \mathbb{Z}$ tel que $(a-b) = k \cdot n \Rightarrow b - a = \ell \cdot n$, avec $\ell = -k$. On voit donc bien que $n \mid (b-a)$.

   Transitive On doit montrer que pour tout $a, b, c \in \mathbb{Z}$, si $a \equiv b \mod n$ et $b \equiv c \mod n$ alors $a \equiv c \mod n$. On suppose que $a \equiv b \mod n$ et $b \equiv c \mod n$. Alors il existe des entiers k, ℓ tels que $(a-b) = k \cdot n$ et $(b-c) = \ell \cdot n$. On voit que

   $$(a-c) = (a-b) + (b-c) = k \cdot n + \ell \cdot n = (k+\ell) \cdot n = m \cdot n,$$

   avec $m = k + \ell \in \mathbb{Z}$. On conclut alors que $n \mid (a-c)$.

2. Donner la classe d'équivalence de $-3 \mod 7$.

   $$\begin{aligned} \overline{-3} &= \{n \in \mathbb{Z} \quad : \quad n \equiv -3 \mod 7\} \\ &= \{\ldots, -17, -10, -3, 4, 11, 18, \ldots\}. \end{aligned}$$

3. Lesquelles des égalités suivantes sont vraies ? Lesquelles sont fausses ?

   — $6 = 4 \mod 2$: Vrai, car $2 \mid (6-4) = 2$
   — $5 = -5 \mod 12$: Faux, car $12 \nmid (5-(-5)) = 10$
   — $11 = -2 \mod 13$: Vrai, car $13 \mid (11-(-2)) = 13$
   — $24 = 0 \mod 12$: Vrai, car $12 \mid (24-0) = 24$

4. Montrer que la définition est équivalente à

   $$a \equiv b \mod n \quad \Leftrightarrow \quad \exists c.\ a = b + cn.$$

   En effet,

   $$a \equiv b \mod n \quad \Leftrightarrow \quad n \mid (a-b) \quad \Leftrightarrow \quad \exists c.\ (a-b) = cn \quad \Leftrightarrow \quad \exists c.\ a = b + cn.$$

5. Montrer que pour $n = 2$, la définition est équivalente à

$$a \equiv b \mod 2 \quad \Leftrightarrow \quad 2 \mid (a+b).$$

On calcule :

$$\begin{aligned} a \equiv b \mod 2 &\Leftrightarrow 2 \mid (a-b) \Leftrightarrow \exists k \in \mathbb{Z} : (a-b) = 2k \\ &\Leftrightarrow \exists k \in \mathbb{Z} : (a-b) + 2b = 2k + 2b \\ &\Leftrightarrow \exists k \in \mathbb{Z} : (a+b) = 2(k+b) \\ &\Leftrightarrow 2 \mid (a+b). \end{aligned}$$

6. Soit n un entier quelconque, montrer les deux propriétés suivantes :
   - Si $a \equiv b \mod n$ alors pour tout entier c on a $a + c \equiv b + c \mod n$,

     Il faut montrer que $n \mid (a+c) - (b+c) = a - b$, ce qui est vrai puisque on a supposé que $a \equiv b \mod n$.
   - Si $a \equiv b \mod n$ alors pour tout entier c on a $ac \equiv bc \mod n$.

     Il faut montrer que $n \mid (ac - bc) = (a-b)c$. Puisque on a supposé que $a \equiv b \mod n$ on sait qu'il existe un $k \in \mathbb{Z}$ tel que $(a-b) = k \cdot n$. Par conséquent,

     $$(ac - bc) = k \cdot n \cdot c = (k \cdot c) \cdot n = m \cdot n,$$

     avec $m = k \cdot c \in \mathbb{Z}$.

2 Structure additive

1. Calculer un représentant pour les sommes suivantes
   - $5 + 5 \equiv 0 \mod 10$
   - $-1 + 4 \equiv 3 \mod 6$
   - $9 - 15 \equiv 1 + 1 \equiv 2 \mod 4$.
2. Calculer un représentant pour les produits suivants
   - $3 \cdot 3 \equiv 9 \equiv 2 \mod 7$
   - $-1 \cdot 9 \equiv -1 \cdot 4 \equiv -4 \equiv 1 \mod 5$
   - $14 \cdot 12 \equiv -1 \cdot -3 \equiv 3 \mod 15$.
3. Calculer les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$. A quels opérateurs du calcul des propositions correspondent-elles ?

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

   La table de l'addition correspond à l'opérateur OU-EXCLUSIF ou XOR, tandis que la multiplication correspond au ET logique.
4. Calculer les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$.

+	**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

x	**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

5. Calculer le résultat des expressions suivantes
   - $3 \cdot (4+7) \equiv 3 \cdot 0 \equiv 0 \mod 11$
   - $4 - 4 \cdot 12 \equiv 4 - 4 \cdot 1 \equiv 0 \mod 11$
   - $(1234 + 789) \cdot 12 \equiv (4+9) \cdot 2 \equiv 3 \cdot 2 \equiv 6 \mod 10$.

3 Structure multiplicative

Voici la table de multiplication de $\mathbb{Z}/15\mathbb{Z}$. À partir de maintenant on va arrêter d'écrire $\mod n$ partout : lorsque le module est clair du contexte, on se contentera d'écrire $6 + 8 = -1$, plutôt que $6 + 8 = -1 \mod 15$.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

1. Quel est l'inverse (multiplicatif) de 2, 4, 7 ?

   L' inverse (multiplicatif) de 2, 4, 7 est respectivement 8, 4 et 13.

2. Trouver un élément qui n'a pas d'inverse multiplicatif. $\mathbb{Z}/15\mathbb{Z}$ est-il un corps ?

   $3 \in \mathbb{Z}/15\mathbb{Z}$ n'a pas d'inverse multiplicatif. $\mathbb{Z}/15\mathbb{Z}$ n'est donc pas un corps puisque tous les éléments non-nuls ne sont pas inversibles.

3. Combien d'éléments contient $(\mathbb{Z}/15\mathbb{Z})^*$ (le groupe des éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$?

$$(\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 6, 7, 11, 13, 14\}.$$

   Il contient donc 8 éléments.

4. Calculer 3^3, 5^4 et 2^7.
   - $3^3 = 3^2 \cdot 3 \equiv 9 \cdot 3 \equiv 12 \mod 15$.
   - $5^4 = 5^2 \cdot 5^2 \equiv 10 \cdot 10 \equiv 10 \mod 15$.
   - $2^7 = 2^2 \cdot 2^2 \cdot 2^2 \cdot 2 \equiv 4 \cdot 4 \cdot 4 \cdot 2 \equiv 1 \cdot 8 \equiv 8 \mod 15$.

4 Corps finis

1. Calculer la table de multiplication de $\mathbb{Z}/7\mathbb{Z}$. Quels sont les éléments inversibles ? $\mathbb{Z}/7\mathbb{Z}$ est-il un corps ?

x	**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

   Tous les éléments de $\mathbb{Z}/7\mathbb{Z}$ sauf 0 sont inversibles. $\mathbb{Z}/7\mathbb{Z}$ est donc un corps.

2. Calculer toutes les puissances de 3 $\mod 7$.

   - $3^0 \equiv 1 \mod 7$
   - $3^1 \equiv 3 \mod 7$
   - $3^2 \equiv 9 \equiv 2 \mod 7$
   - $3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \mod 7$
   - $3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \mod 7$
   - $3^5 \equiv 3^2 \cdot 3^3 \equiv 2 \cdot 6 \equiv 5 \mod 7$
   - $3^6 \equiv 3^2 \cdot 3^2 \cdot 3^2 \equiv 2^3 \equiv 1 \mod 7$

   Rappel : Soit $(A, +, \times)$ et soit un élément $a \in A$, avec $a \neq 0$. On dit que a est un diviseur de 0, s'il existe $b \in A$, $b \neq 0 : ab = 0$.

3. Montrer que si $n = ab$, alors $a \mod n$ est un diviseur de zéro.

$$n = ab \quad \Leftrightarrow \quad ab \equiv 0 \mod n \quad \Leftrightarrow \quad a \text{ est un diviseur de } 0.$$

4. Montrer que un élément est inversible si et seulement s'il n'est pas un diviseur de zéro.

   Soit a un élément inversible. Forcément $a \neq 0$ et il existe un élément a^{-1} tel que $a \cdot a^{-1} = a^{-1} \cdot a \equiv 1 \mod n$. Soit $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \cdot b \equiv 0 \mod n \Rightarrow (a \cdot a^{-1}) \cdot b \equiv 0 \mod n \Rightarrow 1 \cdot b \equiv 0 \mod n \Rightarrow b = 0$. L'inverse est laissé comme exercice.

5. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.