Arithmétique modulaire

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.
2. Donner la classe d'équivalence de $-3 \mod 7$.
3. Lesquelles des égalités suivantes sont vraies ? Lesquelles sont fausses ?

$$6 = 4 \mod 2, \quad 5 = -5 \mod 12, \quad 11 = -2 \mod 13, \quad 24 = 0 \mod 12.$$

4. Montrer que la définition est équivalente à

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

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

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

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

2. Structure additive

1. Calculer un représentant pour les sommes suivantes

$$5 + 5 \mod 10, \quad -1 + 4 \mod 6, \quad 9 - 15 \mod 4.$$

2. Calculer un représentant pour les produits suivants

$$3 \cdot 3 \mod 7, \quad -1 \cdot 9 \mod 5, \quad 14 \cdot 12 \mod 15.$$

3. Calculer les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$. A quels opérateurs du calcul des propositions correspondent-elles ?
4. Calculer les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$.
5. Calculer le résultat des expressions suivantes

$$3 \cdot (4 + 7) \mod 11, \quad 4 - 4 \cdot 12 \mod 11, \quad (1234 + 789) \cdot 12 \mod 10.$$

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 ?
2. Trouver un élément qui n'a pas d'inverse multiplicatif. $\mathbb{Z}/15\mathbb{Z}$ est-il un corps ?
3. Combien d'éléments contient $(\mathbb{Z}/15\mathbb{Z})^*$ (le *groupe des éléments inversibles* de $\mathbb{Z}/15\mathbb{Z}$) ?
4. Calculer 3^3, 5^4 et 2^7.

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 ?
2. Calculer toutes les puissances de $3 \mod 7$.
3. Montrer que si $n = ab$, alors $a \mod n$ est un diviseur de zéro.
4. Montrer que un élément est inversible si et seulement s'il n'est pas un diviseur de zéro.
5. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.