TD 3

Entiers modulo n et Congruences linéaires

Esercice 1. Soit $a, b, n, n' \in \mathbb{Z}$, avec $n, n' > 0$ et $n' \mid n$. Montrer que si $a \equiv b \pmod{n}$, alors $a \equiv b \pmod{n'}$.

Esercice 2. Lister les éléments de l'ensemble $(\mathbb{Z}/20\mathbb{Z})^\times$ et pour chacun de ces éléments déterminer son inverse modulo 20.

Esercice 3. Déterminer si 46 est inversible modulo 651 et, en cas affirmatif, calculer son inverse.

Esercice 4. Démontrer que si $n \in \mathbb{Z}_{>0}$ n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.

Esercice 5. On souhaite démontrer le *Petit Théorème de Fermat* :

Soit p un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$. Alors $a^{p-1} \equiv 1 \pmod{p}$.

(a) Montrer que l'application

$$\begin{array}{rccc} \tau_a : & \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times & \to & \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \\ & x & \mapsto & ax. \end{array}$$

est bien définie et est une bijection.

(b) Soit $S = \{1, 2, \ldots, p-1\}$. Justifier que

$$\prod_{x \in S} ax \equiv \prod_{x \in S} x \pmod{p},$$

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

Remarque : Pour ceux qui ont envie d'aller plus loin, on peut ajuster cette démonstration pour montrer le Théorème d'Euler *:*

Soient $n \in \mathbb{Z}_{>0}$ et $a \in \mathbb{Z}$ tel que $\operatorname{pgcd}(a, n) = 1$. *Alors*

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

où $\varphi(n)$ est la fonction indicatrice d'Euler (définie en cours).

Exercice 6. *(du CC du 23/10/24)* On rappelle que si p est un nombre premier et $p \mid ab$, avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$. De plus, on utilise la notation standard pour la factorielle $n! := n(n-1)(n-2)\cdots 1$.

(a) Pour chaque élément de $(\mathbb{Z}/11\mathbb{Z})^\times$, déterminer son inverse. Une fois tous les inverses déterminés, expliquez pourquoi, il est possible de calculer 10! modulo 11 sans effectuer aucun produit supplémentaire.

(b) Soit $a \in \mathbb{Z}$ et soit p un nombre premier. Montrer que $a^2 \equiv 1 \pmod{p}$ si et seulement si $a \equiv 1 \pmod{p}$ ou $a \equiv p-1 \pmod{p}$.

(c) En déduire que $(p-2)! \equiv 1 \pmod{p}$ et conclure que $(p-1)! \equiv -1 \pmod{p}$.

Vous venez alors de démontrer le *Théorème de Wilson* :

Si p est un nombre premier, alors $(p-1)! \equiv -1 \pmod{p}$.

Esercice 7.

(a) Résoudre dans $\mathbb{Z}$ les congruences suivantes :

- $21z \equiv 12 \pmod{30}$,
- $14z \equiv 5 \pmod{21}$,
- $15z \equiv 9 \pmod{25}$,
- $z + 4 \equiv 16z + 13 \pmod{18}$.

(b) Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$\begin{cases} 5z \equiv 2 \pmod{3} \\ 3z \equiv 4 \pmod{7} \\ 3z \equiv 7 \pmod{8} \end{cases}, \qquad \begin{cases} 6z \equiv 9 \pmod{15} \\ 22z \equiv 55 \pmod{77} \\ 3z \equiv 2 \pmod{13} \\ 27z \equiv 9 \pmod{36} \end{cases}.$$

Exercice 8. *(du CC du 23/10/24)* Le théorème chinois des restes est ainsi nommé parce que sa première formulation remonte à un texte du III ou IV siècle après J.-C. du mathématicien et astronome chinois Sun Zi. La première preuve générale et constructive de ce théorème est apparu beaucoup plus tard, dans l'ouvrage *Shùshū Jiŭzhāng* (« Traité mathématique en neuf chapitres ») du mathématicien chinois Qin Jiushao. On sait que ce livre a été publié dans le XIIIe siècle et que l'année de publication n satisfait les conditions suivantes :

- n est impair.
- le reste de la division de n par 9 est 5 ;
- $11 \mid (2n+3)$;

Dans quelle année le livre *Shùshū Jiŭzhāng* a-t-il été publié ?

Esercice 9. Détérminer un couple d'entiers a, b tels que la congruence linéaire

$$az \equiv b \pmod{319}$$

a exactement 11 solutions distinctes modulo 319.

Esercice 10. Montrer qu'il n'existe pas d'entiers x, y qui satisfont l'équation

$$7x^3 + 2 = y^3.$$