Université de Tours
Licence 2 Mathématiques

TD 5 : Congruences, Structure de $\mathbb{Z}/n\mathbb{Z}$

Arithmétique — Semestre 3

Exercice 1 (Partiel 2018)
Soit $n \in \mathbb{N}$, $n \geq 2$. On dit qu'un entier $a \in \mathbb{Z}$ est inversible modulo n si et seulement si il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$. L'inverse de a est alors le reste de la division euclidienne de b par n.

1. Montrer que 0 n'est pas inversible modulo n et que 1 est inversible modulo n.
2. Montrer que si a et α sont inversibles modulo n alors $a\alpha$ est inversible modulo n.
3. Montrer que a est inversible modulo n si et seulement si $\mathbf{pgcd}\,(a, n) = 1$.
4. Calculer l'inverse de 5 modulo 7.

Exercice 2 (Puissances et racines)

1. Calculer 5^{11} modulo 14 et 4^{13} modulo 23 à l'aide de la méthode des carrés successifs.
2. Déterminer $x, y \in \mathbb{Z}$ tels que

$$x^5 \equiv 11 \mod 13 \quad \text{et} \quad y^7 \equiv 5 \mod 36$$

Exercice 3
Résoudre les trois systèmes de congruences suivants :

$$\begin{cases} 3x + 4y \equiv 5 \mod 13 \\ 2x + 5y \equiv 7 \mod 13 \end{cases} \qquad \begin{cases} x + y \equiv 26 \mod 28 \\ 27x + y \equiv 4 \mod 28 \end{cases}$$

$$\begin{cases} x + y \equiv 5 \mod 17 \\ 2x + 2y \equiv 7 \mod 17 \end{cases}$$

Exercice 4 (Théorème chinois)
Résoudre les systèmes suivants

$$\begin{cases} x \equiv 4 \mod 11 \\ x \equiv 3 \mod 17 \end{cases} \qquad \begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \end{cases} \qquad \begin{cases} x \equiv 0 \mod 2 \\ x \equiv 0 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}$$