2M220 – Arithmétique, 2014-2015 François Lê
Université Pierre et Marie Curie francois.le@imj-prg.fr

TD n° 4 – Arithmétique dans $\mathbf{Z}/n\mathbf{Z}$

Exercice 1

1. Rappeler la structure d'anneau de $\mathbf{Z}/n\mathbf{Z}$.
2. Écrire les tables de multiplication de $\mathbf{Z}/4\mathbf{Z}$ et de $\mathbf{Z}/5\mathbf{Z}$.
3. Ces anneaux sont-ils intègres ? Sont-ils des corps ?

Exercice 2

1. Soit $n \in \mathbf{Z}$. Montrer que n^2 est congru soit à 0, soit à 1 modulo 4.
2. Soient $a, b \in \mathbf{Z}$. Montrer que $3 | a \wedge b \iff 3 | a^2 + b^2$.

Exercice 3
Soit $\overline{a_r \dots a_0}$ l'écriture décimale d'un entier naturel n.

1. Montrer que n est divisible par 3 si et seulement si $a_0 + a_1 + \cdots + a_r$ est divisible par 3.
2. Montrer que n est divisible par 11 si et seulement si $a_0 - a_1 + \cdots + (-1)^r a_r$ est divisible par 11.

Exercice 4
Soient $P \in \mathbf{Z}[X]$ un polynôme à coefficients entiers, et $a, b \in \mathbf{Z}$ deux entiers. Montrer que si $a \equiv b \mod n$, alors $P(a) \equiv P(b) \mod n$. En utilisant ce résultat, montrer que les polynômes $X^3 - X + 1$ et $X^3 + X^2 - X + 1$ n'admettent pas de racines entières.

Exercice 5

1. Montrer que 7 divise $3^{105} + 4^{105}$.
2. Trouver le reste dans la division euclidienne de 5^{10} par 19.
3. Montrer que 41 divise $2^{20} - 1$.
4. Trouver le chiffre des dizaines et le chiffre des unités de 2^{29}.
5. Trouver le chiffre des unités de 7^{7^7}.

Exercice 6
Décrire le groupe $(\mathbf{Z}/20\mathbf{Z})^\times$. Déterminer l'inverse de $\overline{17}$.

Exercice 7
Traduire les équations suivantes en termes de $\mathbf{Z}/n\mathbf{Z}$ et les résoudre :

1. $35x \equiv 7 \mod 4$
2. $22x \equiv 33 \mod 5$
3. $7x \equiv 5 \mod 19$
4. $4x \equiv 13 \mod 47$

5. $ax \equiv b \mod n$, avec a, b et n entiers.
6. $10x \equiv 6 \mod 14$

Exercice 8
Par récurrence, montrer qu'il existe une suite d'entiers $(x_n)_{n\geqslant 0}$ telle que pour tout $n \geqslant 0$,

$$\begin{cases} x_{n+1} & \equiv & x_n & \mod 7^{n+1} \\ x_n^2 & \equiv & 2 & \mod 7^{n+1} \end{cases}$$

Exercice 9
Résoudre les systèmes suivants et les interpréter avec le théorème des restes chinois.

$$(a) \begin{cases} x \equiv 4 \mod 9 \\ x \equiv 2 \mod 7 \end{cases} \qquad (b) \begin{cases} 7x \equiv 5 \mod 19 \\ 3x \equiv 1 \mod 11 \end{cases} \qquad (c) \begin{cases} 35x \equiv 7 \mod 4 \\ 22x \equiv 33 \mod 5 \end{cases}$$

Exercice 10
Résoudre le système suivant :

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 5 \mod 7 \\ x \equiv 9 \mod 13 \end{cases}$$