# 2. $\mathbb{Z}/n\mathbb{Z}$ et Petit Théorème de Fermat

**Exercice 2.1** (Preuve élémentaire du petit théorème de Fermat)

1. Montrer que pour tout couple d'entiers $a$ et $b$ et tout $p$ premier, on a :
$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$
2. En déduire le petit théorème de Fermat :
$$n^p = n \pmod{p}.$$

**Exercice 2.2** Résoudre dans $\mathbb{Z}$ :

$$x^{2003} \equiv 5 \pmod{23}, \qquad x^{665} \equiv 2 \pmod{7}, \qquad 7777 \cdot x^{5555} \equiv 2222 \pmod{13}$$

**Exercice 2.3** (Théorème de Wilson 1.) Soit $p$ un nombre premier.

1. Quels sont les éléments du corps $\mathbb{Z}/p\mathbb{Z}$ tels que $\alpha^2 = 1$ ?
2. Démontrer la première partie du théorème de Wilson : $p$ divise $(p-1)! + 1$.
*Indication* : regrouper chaque élément avec son inverse dans $\overline{(p-1)!} \in \mathbb{Z}/p\mathbb{Z}$.

**Exercice 2.4** (Théorème de Wilson 2.)

1. Soit $p$ un nombre premier. On considère les polynômes suivants à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ :
$$P(X) = (X-(p-1))\,(X-(p-2))\cdots(X-2)\cdot(X-1) \quad \text{et} \quad Q(X) = X^{p-1} - 1.$$
Montrer que $1, 2, \ldots, p-1$ sont racines de $Q$ et en déduire que $P(X) = Q(X)$.
2. En déduire que $(p-1)! \equiv -1 \pmod{p}$.
3. Réciproquement, soit $n \geq 2$ un entier tel que :
$$(n-1)! \equiv -1 \pmod{n}.$$
Montrer que $n$ est premier.

**Exercice 2.5** Déterminer le reste de la division euclidienne de :

a) 26! par 29, b) 26! par 58.

**Exercice 2.6**

1. Calculer les tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 5$ et $n = 6$.
2. Lister les éléments inversibles dans chaque cas. Quels sont les indicateurs d'Euler $\varphi(n)$ ?

**Exercice 2.7** Calculer la valeur $\varphi(m)$ de l'indicateur d'Euler pour :

a) $m = 27$ b) $m = 13$ c) $m = p^k$ ($p$ premier) d) $m = 12$
e) $m = m_1 \times m_2$ tel que $\mathrm{PGCD}(m_1, m_2) = 1$ f) $m = 60$.

**Exercice 2.8**

1. Quel est l'ordre du groupe multiplicatif $(\mathbb{Z}/13\mathbb{Z})^\times$ ?
2. Quels sont les éléments $\alpha$ du corps $\mathbb{Z}/13\mathbb{Z}$ tels que :
$$\alpha^2 = 1, \qquad \alpha^3 = 1, \qquad \alpha^4 = 1, \qquad \alpha^5 = 1.$$
3. Soit $(\mathbb{Z}/15\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/15\mathbb{Z}$.
Quels sont les éléments de $(\mathbb{Z}/15\mathbb{Z})^\times$ ?
Quels sont les ordres des éléments de $(\mathbb{Z}/15\mathbb{Z})^\times$ ?

**Exercice 2.9**

1. Montrer que si $a$ est premier avec $n$, alors :
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$
Que devient cette relation si $n$ est un nombre premier ? En déduire que pour tout entier $a$ et tout nombre premier $p$, on a :
$$a^p \equiv a \pmod{p}.$$
2. Soient $a, n \geq 1$ deux entiers tels que :
$$a^{n-1} \equiv 1 \pmod{n}$$
et
$$a^l \not\equiv 1 \pmod{n}$$
pour tout diviseur strict $l$ de $n - 1$.
Montrer que $n$ est premier.

**Exercice 2.10** Énoncer l'analogue du petit théorème de Fermat pour $n = 12$.

**Exercice 2.11** Calculer le dernier chiffre de $7^{25}$. Même question avec $7^{100!}$.