#26

# $\mathbb{Z}/n\mathbb{Z}$



**Exercice 1.** *Équations linéaires*

Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ :

**1)** $\begin{cases} \dot{3}x + \dot{7}y = \dot{3} \\ \dot{6}x - \dot{7}y = \dot{0}. \end{cases}$

**2)** $x^2 - \dot{31}x + \dot{18} = \dot{0}$ (indication : $\dot{6}^2 = -\dot{1}$).

**Exercice 2.** *Équation algébrique*

**1)** Dresser la liste des cubes dans $\mathbb{Z}/13\mathbb{Z}$.

**2)** Soient $x, y, z \in \mathbb{Z}$ tels que $5x^3 + 11y^3 + 13z^3 = 0$. Montrer que 13 divise $x, y, z$.

**3)** L'équation : $5x^3 + 11y^3 + 13z^3 = 0$ a-t-elle des solutions entières ?

**Exercice 3.** *Ordre d'un entier modulo $n$*

**1)** Soient $n, p \geq 2$. Montrer que : $n \wedge p = 1 \iff \exists\, k > 0$ tel que $n^k \equiv 1\ [p]$.

**2)** Soit $n$ un entier impair non divisible par 5. Montrer qu'il existe un multiple de $n$ qui s'écrit 1...1 en base 10.

**Exercice 4.** *Théorème chinois*

Soient $n, p \in \mathbb{N}^*$ tels que $n \wedge p = 1$. Pour $x \in \mathbb{Z}$ on note $\overline{x}^{\,n}$, $\overline{x}^{\,p}$ et $\overline{x}^{\,np}$ les classes d'équivalence de $x$ modulo $n$, $p$ et $np$.

**1)** Montrer que l'application $\begin{array}{rccc} \phi : & \mathbb{Z}/(np\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \\ & \overline{x}^{\,np} & \longmapsto & (\overline{x}^{\,n}, \overline{x}^{\,p}) \end{array}$ est un morphisme d'anneaux.

**2)** En déduire que $\varphi(np) = \varphi(n)\varphi(p)$ ($\varphi$ = fonction d'Euler).

**3)** Vérifier que l'hypothèse $n \wedge p = 1$ est nécéssaire.

**Exercice 5.** *Théorème de Wilson*

Soit $n \in \mathbb{N}^*$. Montrer que $n$ est premier si et seulement si $(n-1)! \equiv -1\ [n]$.

**Exercice 6.** $(\mathbb{Z}/2^n\mathbb{Z})^*$

**1)** Montrer que pour tout entier $a$ impair et tout $n \geq 3$ : $a^{2^{n-2}} \equiv 1\ [2^n]$.

**2)** Le groupe $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^*$ est-il cyclique ?

**Exercice 7.** *Équation algébrique*

On note $E = \mathbb{Z}/p\mathbb{Z} \setminus \{\dot{0}, \dot{1}\}$ où $p$ est un nombre premier. Soit $\begin{array}{rccc} f : & E & \longrightarrow & E \\ & x & \longmapsto & \dot{1} - x^{-1} \end{array}$

**1)** Démontrer que $f$ est une permutation de $E$.

**2)** Chercher l'ordre de $f$ pour $\circ$.

**3)** En déduire que le nombre de points fixes de $f$ est congru à $\operatorname{card} E$ modulo 3.

**4)** Démontrer que ce nombre est inférieur ou égal à 2.

**5)** Combien l'équation $x^2 - x + \dot{1} = \dot{0}$ a-t-elle de racines dans $\mathbb{Z}/p\mathbb{Z}$ en fonction de $p$ ?

**6)** Pour $p = 37$, résoudre l'équation.

**Exercice 8.** *Carrés dans $\mathbb{Z}/p\mathbb{Z}$*

Soit $p$ un nombre premier impair. Montrer que $\dot{k}$ est un carré dans l'anneau $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $k^{(p+1)/2} \equiv k\ [p]$.

**Exercice 9.** *Test de primalité de Rabin-Miller*

Soit $n$ un entier premier impair supérieur ou égal à 3 : $n = q2^p + 1$ avec $p$ impair et soit $a \in \mathbb{Z}$ premier à $n$. On considère la suite $(b_0, b_1, \ldots, b_p)$ d'entiers compris entre 0 et $n-1$ définie par :

$$b_0 \equiv a^q \ [n], \quad b_1 \equiv b_0^2 \ [n], \quad \ldots, \quad b_p \equiv b_{p-1}^2 \ [n].$$

**1)** Montrer que $b_p = 1$.

**2)** Si $b_0 \neq 1$ montrer qu'il existe un indice $i$ tel que $b_i = n-1$.

**Exercice 10.** *Coefficients du binôme*

Soit $p$ un nombre premier. Montrer que $\sum_{k=0}^{p} C_p^k C_{p+k}^k \equiv 2^p + 1 \ [p^2]$.

**Exercice 11.** *Suite récurrente (Mines MP 2003)*

On considère la suite $(x_n)$ à valeurs dans $\mathbb{Z}/11\mathbb{Z}$ telle que pour tout $n$ on ait $x_{n+3} = 4(x_{n+2}+x_{n+1}+x_n)$. Déterminer les différents comportements possibles de $(x_n)$.

**Exercice 12.** *$-3$ est-il un carré ?*

Soit $p$ un nombre premier impair.

**1)** Montrer qu'une équation du second degré : $x^2 + ax + b = \dot{0}$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si son discriminant : $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

**2)** On suppose que $p \equiv 1 \ [3]$ : $p = 3q + 1$.

**a)** Montrer qu'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a^q \neq \dot{1}$.

**b)** En déduire que $-\dot{3}$ est un carré.

**3)** Réciproquement, on suppose que $-\dot{3}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Montrer que $p \equiv 1 \ [3]$.

**Exercice 13.** *Indicateur d'Euler*

Soit $n \geq 3$. Montrer que $\varphi(n)$ est pair et que $\sum_{\substack{1 \leq x \leq n \\ x \wedge n = 1}} x = \dfrac{n\varphi(n)}{2}$.

**Solutions des exercices**

**Exercice 1.**
**1)** $x = \dot{\overline{25}}$, $y = \dot{\overline{32}}$.
**2)** $x = \dot{\overline{15}}$ ou $\dot{\overline{16}}$.

**Exercice 2.**
**1)** $\dot{0}$, $\pm\dot{1}$, $\pm\dot{5}$.

**Exercice 5.**
Étudier le même produit dans $\mathbb{Z}/n\mathbb{Z}$

**Exercice 7.**
**2)** 3.
**6)** $\dot{\overline{11}}$, $\dot{\overline{27}}$.

**Exercice 10.**
Pour $1 \leq k < p$ : $k!\,C_{p+k}^k = (p+1)\dots(p+k) \equiv k!\ [p]$ donc $C_{p+k}^k \equiv 1\ [p]$. De plus $C_p^k \equiv 0\ [p]$ d'où $C_p^k C_{p+k}^k \equiv C_p^k\ [p^2]$.

Ensuite $(p-1)!\,C_{2p}^p = 2(p+1)\dots(p+p-1) \equiv 2(p-1)! + 2p\sum\limits_{i=1}^{p-1}\dfrac{(p-1)!}{i}\ [p^2] \equiv 2(p-1)!\Big(1+p\sum\limits_{i=1}^{p-1} i'\Big)\ [p^2]$ où $i'$ désigne l'inverse de $i$ modulo $p$. L'application $x \longmapsto x^{-1}$ est une permutation de $(\mathbb{Z}/p\mathbb{Z})^*$ donc $\sum\limits_{i=1}^{p-1} i' \equiv \dfrac{p(p-1)}{2}\ [p] \equiv 0\ [p]$, d'où $C_p^p C_{2p}^p \equiv 2\ [p^2]$.

Enfin $\sum\limits_{k=0}^{p} C_p^k C_{p+k}^k \equiv 1 + \sum\limits_{k=1}^{p-1} C_p^k + 2\ [p^2] \equiv 2^p + 1\ [p^2]$.

**Exercice 11.**
L'équation caractéristique, $X^3 = 4(X^2+X+1)$ admet trois racines distinctes dans $\mathbb{Z}/11Z$ : $1, 6, 8$. Donc $x_n$ est de la forme : $x_n = a + 6^n b + 8^n c$ avec $a, b, c \in \mathbb{Z}/11\mathbb{Z}$. On a $6^{10} \equiv 8^{10} \equiv 1\ [11]$, donc $(x_n)$ est périodique de période divisant 10. La plus petite période est 1 si $b = c = 0$, 10 sinon car les suites $(6^n)$ et $(8^n)$ ont 10 comme plus petite période modulo 11 et l'on a : $8(x_{n+1} - x_n) - 5(x_{n+2} - x_{n+1}) = 7\cdot 8^n c$ et $7(x_{n+2} - x_{n+1}) - (x_{n+1} - x_n) = 7\cdot 6^n b$.

**Exercice 12.**
**2) a)** Le nombre de solutions de l'équation $x^q = \dot{1}$ est inférieur ou égal à $q < p-1$.
**b)** $\dot{0} = a^{3q} - \dot{1} = (a^q - \dot{1})(a^{2q} + a^q + \dot{1})$ donc $a^{2q}$ est racine de $x^2 + x + \dot{1} = \dot{0}$, de discriminant $-\dot{3}$.
**3)** Il existe $x \in \mathbb{Z}/p\mathbb{Z}$ solution de $x^2 + x + \dot{1} = \dot{0}$, et un tel $x$ est d'ordre multiplicatif 3. Par le théorème de Lagrange, on en déduit $3 \mid p-1$.

**Exercice 13.**
Regrouper $x$ et $n - x$.