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

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) $x^2 - \dot{\overline{31}}x + \dot{\overline{18}} = \dot{0}$ (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 non nulles ?

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

1) Soient $n, p \geqslant 2$. Montrer que : $n \wedge p = 1 \Leftrightarrow \exists\, k > 0$ tel que $n^k \equiv 1 \pmod{p}$.

2) Soit n un entier impair non divisible par 5. Montrer qu'il existe un multiple de n qui s'écrit $1 \dots 1$ 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 Φ : $\begin{cases} \mathbb{Z}/(np\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \\ \overline{x}^{\,np} & \longmapsto & (\overline{x}^{\,n}, \overline{x}^{\,p}) \end{cases}$ est un morphisme d'anneaux.

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

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

Exercice 5. *Théorème de Wilson*
Soit $n \geqslant 2$. Montrer que n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.

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

1) Montrer que pour tout entier a impair et tout $n \geqslant 3$: $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.

2) Le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$ 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 impair. Soit f : $\begin{cases} E & \longrightarrow & E \\ x & \longmapsto & \dot{1} - x^{-1}. \end{cases}$

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 $k^{(p+1)/2} \equiv k \pmod{p}$.

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 $(b_0, b_1, \dots, b_p)$ d'entiers compris entre 0 et $n-1$ définie par :

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

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 $\sum_{k=0}^{p}\binom{p}{k}\binom{p+k}{k} \equiv 2^p+1 \pmod{p^2}$.

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 $p\equiv 1 \pmod 3$: $p=3q+1$.
  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 $p\equiv 1 \pmod 3$.

Exercice 13. *Indicateur d'Euler*
Soit $n\geqslant 3$. Montrer que $\varphi(n)$ est pair et que la somme des entiers de $[\![1,n]\!]$ premiers à n est égale à $\frac{1}{2}n\varphi(n)$.

Exercice 14. *Thm de Dirichlet*
Soit p un nombre premier, $n\in\mathbb{N}^*$, et $N=\dfrac{(np)^p-1}{np-1}$.
1) Montrer que N est premier avec $np-1$.
2) Soit q premier divisant N. Montrer que np est premier à q, et déterminer l'ordre de $\dot{\overline{np}}$ dans $(\mathbb{Z}/q\mathbb{Z})^*$. En déduire $q\equiv 1 \pmod p$.
3) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo p.

Exercice 15. *$3^m-13\times 2^n=1$, Centrale MP 2010*
Pour $n\in\mathbb{N}^*$ on note $v_2(n)$ l'exposant de 2 dans la décomposition de n en facteurs premiers.
1) Calculer $v_2(3^k+1)$ pour k impair.
2) Calculer $v_2(3^k-1)$ pour k impair.
3) On considère l'équation $(E)\Leftrightarrow 3^m-13\times 2^n=1$.
  a) Résoudre (E) quand m est impair.
  b) Soit (m,n) une solution avec m pair. On écrit $m=q2^\alpha$ avec q impair et $\alpha\in\mathbb{N}^*$. Déterminer les valeurs de 3^q+1.
  c) Déterminer l'ordre de 3 dans le groupe $(\mathbb{Z}/13\mathbb{Z})^*$.
  d) Résoudre (E) lorsque m est pair.

solutions

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 $1 \leqslant kp$: $k!\,\binom{p+k}{k} = (p+1)\dots(p+k) \equiv k! \,(\mathrm{mod}\, p)$ donc $\binom{p+k}{k} \equiv 1 \,(\mathrm{mod}\, p)$. De plus $\binom{p}{k} \equiv 0 \,(\mathrm{mod}\, p)$ d'où $\binom{p}{k}\binom{p+k}{k} \equiv \binom{p}{k} \,(\mathrm{mod}\, p^2)$.

Ensuite

$$\begin{aligned}(p-1)!\binom{2p}{p} = 2(p+1)\dots(p+p-1) &\equiv 2(p-1)! + 2p\sum_{i=1}^{p-1}\frac{(p-1)!}{i} \,(\mathrm{mod}\, p^2)\\ &\equiv 2(p-1)!\Big(1 + p\sum_{i=1}^{p-1} i'\Big) \,(\mathrm{mod}\, p^2)\end{aligned}$$

où i' désigne l'inverse de i modulo p. L'application $x \mapsto x^{-1}$ est une permutation de $(\mathbb{Z}/p\mathbb{Z})^*$ donc $\sum_{i=1}^{p-1} i' \equiv \frac{1}{2}p(p-1) \,(\mathrm{mod}\, p) \equiv 0 \,(\mathrm{mod}\, p)$, d'où $\binom{p}{p}\binom{2p}{p} \equiv 2 \,(\mathrm{mod}\, p^2)$.

Enfin $\sum_{k=0}^{p}\binom{p}{k}\binom{p+k}{k} \equiv 1 + \sum_{k=1}^{p-1}\binom{p}{k} + 2 \,(\mathrm{mod}\, p^2) \equiv 2^p + 1 \,(\mathrm{mod}\, p^2)$.

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 $6^{10} \equiv 8^{10} \equiv 1 \,(\mathrm{mod}\, 11)$, 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 : $8(x_{n+1} - x_n) - 5(x_{n+2} - x_{n+1}) = 7 \times 8^n c$ et $7(x_{n+2} - x_{n+1}) - (x_{n+1} - x_n) = 7 \times 6^n b$.

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 $n - x$.

Exercice 14.

1) $N = 1 + (np) + \ldots + (np)^{p-1} \equiv p \,(\mathrm{mod}\, np - 1)$.

2) $kq = N = 1 + \ell np$ dont $q \wedge np = 1$. On a aussi $(np)^p - 1 = N(np-1) \equiv 0 \,(\mathrm{mod}\, q)$ donc $\dot{\overline{np}}$ est d'ordre 1 ou p. Or $np - 1$ et N n'ont aucun facteur non trivial en commun, donc $np \not\equiv 1 \,(\mathrm{mod}\, q)$ et $O(\dot{\overline{np}}) = p$. Alors p divise $q - 1$ d'après le théorème de Lagrange, d'où $q \equiv 1 \,(\mathrm{mod}\, p)$.

3) Sinon, prendre $n =$ le produit de ces nombres.

Exercice 15.

1) $3^2 \equiv 1 \pmod 8$ donc $3^k + 1 \equiv 4 \pmod 8$ et $v_2(3^k + 1) = 2$.

2) $= 1$.

3) a) $(m, n) = (3, 1)$.

b) $(3^q)^{2^\alpha} - 1 = (3^q - 1)(3^q + 1)((3^{2q})^{2^{\alpha-1}-1} + \ldots + 1) = 13 \times 2^n$ donc $\frac{1}{4}(3^q + 1)$ est un diviseur de 13 et $3^q + 1 = 4$ ou $4 \times 13 = 52$. On en déduit $q = 1$ et $m = 2^\alpha$.

c) Cet ordre divise 12 d'après le théorème de Lagrange. Après essais on trouve l'ordre 3.

d) $3^m \equiv 1 \pmod{13}$ donc m est un multiple de 3 et aussi une puissance de 2 ; il n'y a pas de solution.