Exercice 1.

Soit p un nombre premier impair.

1. Dénombrer les carrés de $\mathbb{Z}/p\mathbb{Z}$.

2. Si $x \in Z/p\mathbb{Z}^*$, montrer que x est un carré *si et seulement si* $x^{(p-1)/2} = 1$.

Exercice 2.

Soient p un nombre premier et q dans $\mathbb{N}^*$ premier avec p. Pour tout entier naturel n non nul, on note t_n l'ordre de $\overline{q}$ dans le groupe $\mathbb{Z}/p^n\mathbb{Z}$. Montrer que $(t_{n+1}/t_n)_{n\geqslant 1}$ est stationnaire.

Exercice 3.

Soient $n \geqslant 2$ et U l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/2^n\mathbb{Z}$.

1. Etablir que U est un sous-groupe multiplicatif de $\mathbb{Z}/2^n\mathbb{Z}$.

2. Calculer $x^{2^{n-2}}$ pour tout $x \in U$.

3. Trouver le plus petit entier naturel non nul k tel que

$$3^k \equiv 1 \left[2^n\right]$$

4. Etablir que U est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.

Exercice 4.

Soit p un nombre premier supérieur ou égal à 5. On écrit

$$\sum_{i=1}^{p-1} \frac{1}{i} = \frac{m}{(p-1)!}$$

avec $m \in \mathbb{N}$.

1. Montrer que

$$\begin{array}{rccc} \phi : & \mathbb{Z}/p\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/p\mathbb{Z}^* \\ & x & \longmapsto & \dfrac{1}{x} \end{array}$$

est une bijection.

2. En déduire que p^2 divise m. On pourra utiliser l'égalité :

$$2 \cdot \sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{p-1} \frac{p}{i \cdot (p-i)}$$

Exercice 5.

Montrer que la somme de trois carrés d'entiers impairs n'est pas le carré d'un entier.

Exercice 6.

Soient $P \in \mathbb{Z}[X]$ et p un nombre entier premier et impair.

1. Montrer que, pour tous $x, h \in \mathbb{Z}$,

$$P(x+h) \equiv P(x) + h \cdot P'(x) \left[h^2\right]$$

2. Soit $a \in \mathbb{Z}$ tel que $P(a) \equiv 0\ [p]$ et $P'(a) \neq 0\ [p]$. Etablir l'existence d'une suite d'entiers relatifs $(x_n)_{n\geqslant 0}$ telle que

$$\forall n \in \mathbb{N},\ P(x_n) \equiv 0 \left[p^{n+1}\right]$$

3. Soit γ un entier non multiple de p. Pour tout entier naturel n, on note (E_n) l'équation

$$(E_n) :\ x^2 \equiv \gamma \left[p^{n+1}\right]$$

On suppose que (E_0) possède une solution. Etablir que, pour tout entier naturel n, (E_n) possède une solution.

4. Soit $n \in \mathbb{N}^*$. Combien y-a-t-il de carrés dans $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$?

Exercice 7.

Soient p un nombre premier impair et $n \in \mathbb{N}$. Etablir que

$$(1+p)^{p^n} \equiv 1 + p^{n+1} \left[p^{n+2}\right]$$

Exercice 8.

Soient p un nombre premier, a et b deux entiers tels que $a \wedge p = 1$. Pour tout entier naturel n, on considère l'équation

$$(E_n) :\ a \cdot x + b \equiv 0 \left[p^n\right]$$

1. Etablir que, pour tout entier naturel n, (E_n) possède au moins une solution.

2. Comment trouver une solution particulière de (E_{n+1}) à partir d'une solution particulière de (E_n) ?

3. Résoudre l'équation (E_n) pour tout $n \in \mathbb{N}$.

Exercice 9.

Soit p un nombre premier impair.

1. Montrer que le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est égal à $\frac{p-1}{2}$.

2. On suppose que $p \equiv 1\,[4]$.

2.a. Prouver l'existence de $n \in \mathbb{Z}$ tel que $n^2 \equiv -1\,[p]$.

2.b. Montrer qu'il existe $(a,b) \in \mathbb{Z}^2$ tel que

$$0 < b < \sqrt{p} \quad \text{et} \quad \left| b \cdot \frac{n}{p} - a \right| \leqslant \frac{1}{\sqrt{p}}$$

2.c. En déduire que

$$p = (b \cdot n - a \cdot p)^2 + b^2$$

Exercice 10.

Soit p un nombre premier de la forme $p = 3u+1$ avec $u \in \mathbb{N}$.

1. Prouver l'existence $a \in \mathbb{F}_p^*$ tel que $a^u \neq 1$.

2. En déduire que -3 est un carré dans $\mathbb{F}_p$.