

Problème :

Préliminaires :

1. On veut montrer que si $n \in \mathbb{N}$ n'est pas un carré parfait (le carré d'un entier naturel), alors \sqrt{n} est irrationnel. On suppose par l'absurde que $\sqrt{n} = \frac{a}{b}$ avec $a \wedge b = 1$.
 - a. Justifier l'existence d'un nombre premier p divisant b .
 - b. Montrer que p divise a^2 puis que p divise a et conclure.
2. Soit p un nombre premier et $k \in [1, p-1]$.
 - a. En étudiant $k!(p-k)! \binom{p}{k}$, montrer que p divise le coefficient binomial $\binom{p}{k}$.
 - b. En déduire que :

$$\forall (a, b) \in \mathbb{Z}^2, (a+b)^p \equiv a^p + b^p \pmod{p}.$$
3. On dit que d est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si l'équation $(x \pmod{p})^2 = d \pmod{p}$ admet au moins une solution dans $\mathbb{Z}/p\mathbb{Z}$.
 - a. Enumérer les carrés de $\mathbb{Z}/11\mathbb{Z}$ puis ceux de $\mathbb{Z}/17\mathbb{Z}$.
 - b. Vérifier que 2 est un carré dans $\mathbb{Z}/17\mathbb{Z}$ mais pas dans $\mathbb{Z}/11\mathbb{Z}$ puis que 3 est carré dans $\mathbb{Z}/11\mathbb{Z}$ mais pas dans $\mathbb{Z}/17\mathbb{Z}$.
4. Soit $n \geq 2$. Montrer que $\sum_{k=0}^{n-1} \exp\left(\frac{2ik\pi}{n}\right) = 0$.

Partie 1 :

Soit δ un nombre complexe fixé. On note \mathcal{A}_δ l'ensemble des sous-anneaux de $(\mathbb{C}, +, \times)$ contenant δ et on définit $\mathbb{Z}[\delta] = \bigcap_{A \in \mathcal{A}_\delta} A$.

1.
 - a. Montrer que $\mathbb{Z}[\delta]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
 - b. Montrer que si B est un sous-anneau de $(\mathbb{C}, +, \times)$ contenant δ , alors $\mathbb{Z}[\delta] \subset B$.

On vient de montrer que $\mathbb{Z}[\delta]$ est le plus petit sous-anneau de $(\mathbb{C}, +, \times)$ contenant δ .

2.
 - a. Que dire de $\mathbb{Z}[\delta]$ lorsque $\delta \in \mathbb{Z}$?
 - b. Montrer que $\mathbb{Z}[\delta] = \{P(\delta) \mid P \in \mathbb{Z}[X]\}$, où $\mathbb{Z}[X]$ est l'ensemble des polynômes à coefficients entiers.
 - c. L'écriture d'un élément $a \in \mathbb{Z}[\delta]$ sous la forme $P(\delta)$ est-elle unique en général (on pourra par exemple envisager le cas $\delta = i$)?

Soit alors un entier p premier et impair.

On définit sur $\mathbb{Z}[\delta]$ la relation suivante dite de congruence modulo p et notée \mathcal{R}_p :

$$\forall (a, b) \in \mathbb{Z}[\delta]^2, a \mathcal{R}_p b \text{ si et seulement si } \exists c \in \mathbb{Z}[\delta], a - b = pc.$$

3.
 - a. Montrer qu'il s'agit d'une relation d'équivalence.

On note alors $\mathbb{Z}[\delta]/(p)$ l'ensemble des classes d'équivalence pour cette relation de congruence modulo p et on note $\dot{x} \in \mathbb{Z}[\delta]/(p)$ la classe de $x \in \mathbb{Z}[\delta]$ pour cette relation d'équivalence.

- b. Définir des lois $+_p$ et \times_p sur $\mathbb{Z}[\delta]/(p)$ telles que

- le triplet $(\mathbb{Z}[\delta]/(p), +_p, \times_p)$ soit un anneau,
- l'application $\phi : \mathbb{Z}[\delta] \rightarrow \mathbb{Z}[\delta]/(p)$ définie par $\phi(a) = \dot{a}$ soit un morphisme surjectif d'anneaux.

Dans la suite du problème, les lois $+_p$ et \times_p de $\mathbb{Z}[\delta]/(p)$ seront simplement notées $+$ et \times .

On fait remarquer qu'en s'inspirant de la question **2.** des préliminaires, on peut démontrer que :

$$\forall (\dot{a}, \dot{b}) \in (\mathbb{Z}[\delta]/(p))^2, (\dot{a} + \dot{b})^p = \dot{a}^p + \dot{b}^p.$$

Partie 2 :

On suppose dans cette partie que le nombre complexe δ vérifie les conditions $\delta \notin \mathbb{Z}$ et $\delta^2 \in \mathbb{Z}$. On note $d = \delta^2$. L'anneau $\mathbb{Z}[\delta]$ est donc un anneau minimal dans lequel d admet une racine carrée.

L'entier p est toujours premier et impair.

L'anneau $\mathbb{Z}[\delta]/(p)$ peut alors être assimilé à un anneau modulo p auquel on a ajouté une racine de d .

Lorsque $a \in \mathbb{C}$, \bar{a} désigne le conjugué de a dans \mathbb{C} .

1. Montrer que $\mathbb{Z}[\delta] = \{n + \delta m \mid (n, m) \in \mathbb{Z}^2\}$.
2. Montrer que la décomposition d'un élément $a \in \mathbb{Z}[\delta]$ sous la forme $a = n + \delta m$ avec $(n, m) \in \mathbb{Z}^2$ est unique. On pourra distinguer deux cas selon que $d < 0$ et $d > 0$.

On suppose toujours p premier impair et on suppose que $d \wedge p = 1$.

3. Montrer que $\forall \dot{a} \in \mathbb{Z}[\delta]/(p), \dot{a}^2 = 0 \Rightarrow a = 0$.

Pour tout $a \in \mathbb{Z}[\delta]$, si $a = n + \delta m$, on note $a^c = n - \delta m$ et $N(a) = a \times a^c$.

4. Montrer que pour tout $a \in \mathbb{Z}[\delta]$, $N(a) \in \mathbb{Z}$.
5. Montrer que a est inversible dans $\mathbb{Z}[\delta]/(p)$ si et seulement si p ne divise pas $N(a)$ dans \mathbb{Z} .
6. Montrer que si d n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors $\mathbb{Z}[\delta]/(p)$ est un corps.

Partie 3 :

Le but de cette partie est de chercher à quelle(s) condition(s), (-1) , 2 et 3 sont des carrés dans $\mathbb{Z}/p\mathbb{Z}$ en discutant de la classe de congruence de p modulo 4 , modulo 8 ou modulo 12 . Les résultats obtenus dans cette partie sont des cas particuliers d'un théorème plus général démontré dans la partie 4.

On considère l'application :

$$q : \begin{cases} ((\mathbb{Z}/p\mathbb{Z})^*, \times) & \rightarrow & ((\mathbb{Z}/p\mathbb{Z})^*, \times) \\ (x \bmod p) & \mapsto & (x \bmod p)^2 \end{cases}$$

1. Montrer que q est un morphisme de groupes. Déterminer son noyau.
2. Montrer que

$$\text{Card}((\mathbb{Z}/p\mathbb{Z})^*) = \text{Card}(\text{Ker } q) \cdot \text{Card}(\text{Im } q).$$

3. En déduire qu'il y a exactement $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$.
4. Montrer que

$$\forall x \in \mathbb{Z}, x \wedge p = 1 \Rightarrow x^{\varphi(p)} \equiv 1 \pmod{p}.$$

(on précisera la valeur de $\varphi(p)$).

5. En déduire que $x^{(p-1)/2}$ est congru à 1 ou (-1) modulo p .
6. Par un argument d'inclusion et de cardinalité, en déduire que :

$$x^{(p-1)/2} \equiv 1 \pmod{p} \text{ si et seulement si } (x \bmod p) \text{ est un carré non nul de } \mathbb{Z}/p\mathbb{Z}.$$

7. a. Montrer que (-1) est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p est congru à 1 modulo 4.
 b. Retrouver que 2 est un carré modulo 17 mais pas modulo 11 en calculant $2^{(p-1)/2}$ modulo p pour $p = 11$ puis $p = 17$.

Soient des entiers n et n' non divisibles par p .

8. Montrer que :

- si n et n' sont des carrés de $\mathbb{Z}/p\mathbb{Z}$, alors nn' l'est aussi.
- si n est un carré de $\mathbb{Z}/p\mathbb{Z}$ et n' n'est pas un carré de $\mathbb{Z}/p\mathbb{Z}$, alors nn' n'est pas un carré de $\mathbb{Z}/p\mathbb{Z}$.
- si n et n' ne sont pas des carrés de $\mathbb{Z}/p\mathbb{Z}$, alors nn' l'est.

9. Soit $j = \exp\left(\frac{2i\pi}{3}\right)$. On suppose en plus $p \neq 3$.

- a. Montrer que j est inversible dans $\mathbb{Z}[j]/(p)$. On pose $b = j - j^{-1}$, élément de $\mathbb{Z}[j]/(p)$.
 b. Calculer b^2 et en déduire que (-3) est un carré de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $b^p = b$.
 c. Exprimer b^p en fonction de j^p et j^{-p} et en déduire une condition nécessaire et suffisante sur p pour que (-3) soit un carré de $\mathbb{Z}/p\mathbb{Z}$.
 d. À l'aide de la question 8., en déduire que :

$$3 \text{ est un carré de } \mathbb{Z}/p\mathbb{Z} \text{ si et seulement si } p \equiv \pm 1 \pmod{12}.$$

10. Soit $\omega = \exp\left(i\frac{\pi}{4}\right)$, vu comme élément de $\mathbb{Z}[\omega]/(p)$. En adaptant la preuve précédente et en considérant $b = \omega + \omega^{-1}$, montrer que 2 est un carré de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv \pm 1 \pmod{8}$.

Partie 4 :

Le nombre p est toujours un nombre premier impair.

On définit la fonction de Legendre $L_p : \mathbb{Z} \rightarrow \{-1, 0, 1\}$ telle que

$$L_p(a) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \\ 0 & \text{si } a \equiv 0 \pmod{p} \\ -1 & \text{sinon} \end{cases}$$

On peut aussi définir une fonction $\mathcal{L}_p : \mathbb{Z}/p\mathbb{Z} \rightarrow \{-1, 0, 1\}$ en posant $\mathcal{L}_p(a \bmod p) = L_p(a)$.

En pratique, on notera L_p l'une ou l'autre de ces fonctions.

On rappelle les principaux résultats des parties précédentes :

- $L_p(n) \equiv n^{(p-1)/2} \pmod{p}$ (question 6.).
- $L_p(-1) = 1$ si et seulement si $p \equiv \pm 1 \pmod{4}$ (question 7.a).
- $L_p(nn') = L_p(n)L_p(n')$ (question 8.)

Soit $\zeta = \exp\left(\frac{2i\pi}{p}\right)$.

On définit la somme de Gauss relative à p par le nombre complexe $G = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} L_p(a)\zeta^a$.

Par exemple, si $p = 3$, alors $G = \zeta + \zeta^2 = i\sqrt{3}$.

De même, si $p = 5$, $G = \zeta - \zeta^2 - \zeta^3 + \zeta^4 = 2 \cos(2\pi/5) - 2 \cos(4\pi/5) = \sqrt{5}$.

1. a. Justifier que pour $(a, t) \in \mathbb{Z}^2$, $L_p(a^2t) = L_p(t)$.
 b. Montrer que

$$\sum_{(a,b) \in ((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(ab)\zeta^{a+b} = L_p(-1)(p-1) - \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^* \setminus \{-1\}} L_p(t)$$

(on pourra poser $b = at$ où $t \in (\mathbb{Z}/p\mathbb{Z})^*$).

c. Justifier que $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(a) = 0$ et en déduire que

$$G^2 = (-1)^{(p-1)/2} p.$$

2. Soient p et q deux nombres premiers impairs distincts.

a. En distinguant éventuellement les cas, justifier que :

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^*, \forall q \in \mathbb{N}, (L_p(a))^q = L_p(a) = L_p(q) \cdot L_p(qa).$$

b. En posant $t = aq$, montrer que

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} (L_p(a)\zeta^a)^q \bmod q = L_p(q) \cdot G \bmod q.$$

c. En utilisant la question **2.b** des préliminaires, montrer que

$$G^q \equiv L_p(q)G \bmod q.$$

d. Montrer que

$$\left((G^2)^{(q-1)/2} \cdot G \right) \bmod q = \left((-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L_q(p) \cdot G \right) \bmod q.$$

3. En déduire que

$$L_p(q) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L_q(p).$$