

Algèbre et théorie des nombres

Examen

Durée : 2 heures 30

Ni document ni calculatrice. Le barème est indicatif. Le sujet est recto-verso.

I - Arithmétique (4 points)

1. Déterminer les inverses de $\bar{4}$ et $\bar{9}$ dans le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$.
2. En déduire le reste de la division euclidienne de $2^{1998} + 3^{2008}$ par 11.

II - Permutations (3 points).

Les permutations σ et τ de S_9 suivantes sont-elles conjuguées ?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 7 & 8 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$$

et

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 2 & 5 & 6 & 4 & 3 & 9 & 8 \end{pmatrix}.$$

Tourner la page S.V.P

III - Problème (15 points)

Le but de ce problème est de déterminer quels sont les entiers $n \in \mathbb{N}$ qui sont sommes de deux carrés, c'est-à-dire tels que $n = a^2 + b^2$ avec $a, b \in \mathbb{N}$.

A. Carrés du corps $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier différent de 2. On note

$$(\mathbb{Z}/p\mathbb{Z})^{*2} = \{x^2 : x \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Montrer que si $a \in (\mathbb{Z}/p\mathbb{Z})^{*2}$ alors $a^{(p-1)/2} = 1$.
2. Vérifier que $(\mathbb{Z}/p\mathbb{Z})^{*2}$ est un sous-groupe du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.
3. En utilisant le morphisme ϕ de $(\mathbb{Z}/p\mathbb{Z})^*$ vers $(\mathbb{Z}/p\mathbb{Z})^{*2}$ défini par $\phi(x) = x^2$, montrer que

$$|(\mathbb{Z}/p\mathbb{Z})^{*2}| = \frac{p-1}{2}.$$

4. En déduire que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^*$, on a $a \in (\mathbb{Z}/p\mathbb{Z})^{*2}$ si et seulement si $a^{(p-1)/2} = 1$.
5. Montrer que -1 est un carré de $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $p \equiv 1 \pmod{4}$.

Pour la suite du problème, on note $S = \{n \in \mathbb{N} : n = a^2 + b^2; a, b \in \mathbb{N}\}$ et on considère l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

muni de la norme N qui à $z \in \mathbb{Z}[i]$ associe $N(z) = z\bar{z}$. On rappelle que $\mathbb{Z}[i]$ est un anneau euclidien relativement à la norme N .

B. Le théorème des deux carrés pour un nombre premier.

1. Vérifier qu'un entier $n \in S$ si et seulement s'il existe $a \in \mathbb{Z}[i]$ tel que $n = N(a)$. En déduire que si deux entiers n et m sont dans S alors $nm \in S$.
2. À l'aide de la norme, montrer que les éléments inversibles de $\mathbb{Z}[i]$ sont $1, -1, i$ et $-i$.
3. Fixons un nombre premier p . Montrer que $p \in S$ si et seulement si p est réductible dans $\mathbb{Z}[i]$.
4. Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$.
5. En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si le polynôme $X^2 + 1$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.
6. A l'aide de la partie A, montrer que $p \in S$ si et seulement si p est réductible dans $\mathbb{Z}[i]$ si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.

C. Le théorème des deux carrés.

Soit $n \in \mathbb{N}^*$. On considère la décomposition en facteurs premiers de n ,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

1. Montrer que si α_i est pair pour chaque $p_i \equiv 3 \pmod{4}$ alors $n \in S$.
2. Réciproquement supposons que $n \in S$. Soit p un nombre premier divisant n et irréductible dans $\mathbb{Z}[i]$. Montrer que p^2 divise n .
3. Conclure.