UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen (10 juin 2011 — 2e session)

Les notes de cours et de TD, ainsi que les calculatrices, sont autorisées. Les téléphones portables sont interdits.

Durée : 2 heures

Sauf mention explicite du contraire, toutes les réponses doivent être accompagnées d'une démonstration.

Exercice 1

Pour quels polynômes $P \in \mathbb{Z}[X]$ l'équation $y^2 = 3P(x) + 2$ a-t-elle des solutions dans $\mathbb{Z}^2$?

Exercice 2

Soit x un entier relatif, soit $n = x^2 - x + 1$ et soit p un diviseur premier de n.

1. Montrer que -3 est un carré modulo p.
2. En déduire que $p = 3$ ou $p \equiv 1 \pmod 3$.

Exercice 3

1. Énoncer un critère (condition suffisante) d'irréductibilité des polynômes dans $\mathbb{Z}[X]$. (Il n'est pas demandé de démontrer le critère).
2. Existe-t-il un entier algébrique de degré 100 ?

Exercice 4

Le nombre $\cos(\pi/12)$ est-il un nombre algébrique ?

Exercice 5

Soit p un nombre premier impair. Le but de ce problème est de donner un algorithme permettant de résoudre explicitement le problème des deux carrés, i.e. trouver $x, y \in \mathbb{N}$ tels que $x^2 + y^2 = p$ quand $p \equiv 1 \pmod 4$.

1. Rappeler rapidement pourquoi il n'existe pas de tels entiers si $p \equiv 3 \pmod 4$. On suppose désormais que $p \equiv 1 \pmod 4$.

TSVP →

2. Posons $p = 1 + 2^e m$, avec $e, m \in \mathbb{N}$ et m impair. Soit $s \in \mathbb{F}_p^\times$ tel que $s^m \neq 1$. Montrer qu'il existe un entier $d \geqslant 0$ tel que $(s^m)^{2^d} = 1$.
3. Quels sont $x \in \mathbb{F}_p$ tels que $x^2 = 1$? (Rappel : la réponse doit être complètement démontrée).
4. En prenant pour d le plus petit entier naturel tel que $(s^m)^{2^d} = 1$, montrer que si $d \geqslant 2$ alors $(s^m)^{2^{d-2}}$ est une racine carré de -1 dans $\mathbb{F}_p$.
5. Montrer qu'il y a au plus $2m = \frac{p-1}{2^{e-1}}$ éléments $s \in \mathbb{F}_p^\times$ tels que $d < 2$. (On pourra montrer que ce sont des racines d'un polynôme bien choisi).

   Si $p \equiv 1 \pmod 4$, en prenant s au hasard, équiprobablement, dans $\mathbb{F}_p^\times$, on a donc au moins une chance sur deux d'avoir $d \geqslant 2$ et donc d'en déduire une racine carrée de -1. Si $d < 2$, on recommence jusqu'à tomber sur un s qui convient.
6. Soit α une racine carrée de -1 dans $\mathbb{F}_p$. On considère l'application

$$\Phi \colon \begin{cases} \mathbb{Z}[i] & \longrightarrow & \mathbb{F}_p \\ a + ib & \longmapsto & a + \alpha b. \end{cases}$$

   Montrer que c'est un morphisme d'anneaux.
7. Montrer que son noyau $\ker \Phi$ est l'idéal engendré par p et $A - i$, où $A \in \mathbb{Z}$ est un relèvement de α (autrement dit, A est un entier dont la classe modulo p est α).
8. Démontrer l'existence d'un générateur g de l'idéal $\ker \Phi$.
9. Montrer que g est de norme p dans $\mathbb{Z}[i]$.
10. Conclure.
11. En suivant la stratégie décrite dans les questions précédentes, écrire 97 comme somme de deux carrés.