2010–2011

UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen (17 décembre 2010 — 1re session)

Documents et calculatrice sont autorisés. Les téléphones portables sont interdits.

Durée : 2 heures

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

Exercice 1

Soit p un nombre premier congru à 1 modulo 3.

1. Montrer que $\mathbb{F}_p^\times$ a un élément x d'ordre exactement 3.
2. Calculer $(2x+1)^2$ dans $\mathbb{F}_p$.
3. En déduire le symbole de Legendre $\left(\frac{-3}{p}\right)$.

Exercice 2

L'équation $y^2 = 41x + 3$ a-t-elle une solution dans $\mathbb{Z}^2$?

Exercice 3

1. Soit $n \in \mathbb{N}$, tel que $n \equiv 3 \pmod 4$. Montrer qu'il existe un diviseur premier p de n tel que $p \equiv 3 \pmod 4$.
2. Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation $y^2 = x^3 + 7$. Par réduction modulo 4, montrer que x est impair.
3. Calculer $(x+2)((x-1)^2+3)$.
4. En déduire que l'équation $y^2 = x^3 + 7$ n'a pas de solution entière. (On pourra appliquer la première question à $(x-1)^2+3$).

TSVP →

Exercice 4

Soit p un nombre premier impair, et soit $\zeta \in \mathbb{C}$ une racine p-ième primitive de l'unité.

1. Rappeler la définition du discriminant Δ de la base $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$, et montrer que
$$\Delta = (-1)^{\frac{p-1}{2}} \prod_{\substack{1 \leqslant i,j \leqslant p-1 \\ i \neq j}} \left(\zeta^i - \zeta^j\right).$$

2. Montrer que
$$\Delta = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{p-1} \left(1 - \zeta^k\right)^{p-2}.$$

3. En déduire que $\Delta = (-1)^{\frac{p-1}{2}} p^{p-2}$. (On pourra penser à la décomposition en produit de facteurs de degré 1 du polynôme $\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{C}[X]$.)

4. Dans le cas $p = 3$, en déduire l'anneau des entiers de $\mathbb{Q}(\zeta)$.

5. Dans le cas $p = 5$, montrer que $\frac{1+\zeta+\zeta^3}{5}$ n'est pas un entier algébrique.

Exercice 5

Résoudre l'équation diophantienne $x^2 - 30y^2 = 1$, $(x, y) \in \mathbb{Z}^2$.