UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen — Seconde session

Durée : 2h
Les notes de cours et de TD sont autorisées. Les calculatrices et les téléphones sont interdits.

Exercice 1

Le but de cet exercice est de montrer que si $n > 2$ est un entier impair et $a \in \mathbb{Z}$, alors on ne peut pas avoir $a^{n-1} \equiv -1 \pmod{n}$.

On note ici v_2 la valuation 2-adique : si $x \in \mathbb{Z} \setminus \{0\}$, alors $v_2(x)$ est le plus grand entier $v \geqslant 0$ tel que $2^v \mid x$.

Dans toute la suite de l'exercice, n désigne un entier impair > 2 et a un entier.

1. Soit p un nombre premier impair. On suppose qu'il existe un entier $k \geqslant 0$ tel que $a^k \equiv -1 \pmod{p}$. On note e l'ordre de a dans $\mathbb{F}_p^\times$. Montrer que $e \mid (2k)$ et $e \nmid k$.
2. En déduire que $v_2(e) = 1 + v_2(k)$.
3. En déduire que $p \equiv 1 \pmod{2^{1+v_2(k)}}$.
4. On suppose maintenant qu'il existe un entier $k' \geqslant 0$ tel que $a^{k'} \equiv -1 \pmod{n}$. Montrer que $n \equiv 1 \pmod{2^{1+v_2(k')}}$.
5. En déduire qu'on ne peut pas avoir $a^{n-1} \equiv -1 \pmod{n}$.

Exercice 2

1. Montrer qu'il n'y a qu'une seule forme quadratique en deux variables à cœfficients entiers, $aX^2 + bXY + cY^2$, positive et de discriminant -3, qui soit réduite.
2. En déduire que la forme $X^2 + XY + Y^2$ représente proprement un entier $N > 0$ si et seulement si -3 est un carré modulo $4N$. (Indication : on pourra considérer une forme qui représente N au point $(X, Y) = (1, 0)$).
3. Soit p un nombre premier impair. Déduire de la question précédente qu'il existe $x, y \in \mathbb{Z}$ tels que $x^2 + xy + y^2 = p$ si et seulement si $p = 3$ ou $p \equiv 1 \pmod{3}$.

Exercice 3

Le but de cet exercice est de résoudre l'équation diophantienne $x^2 + 2 = 3^n$ (avec $x \geqslant 0$ et $n \geqslant 0$ entiers).

On note $K = \mathbb{Q}(\sqrt{-2})$. Rappelons que l'anneau des entiers de K est $\mathscr{O}_K = \mathbb{Z}[\sqrt{-2}]$, et que c'est un anneau euclidien.

1. On considère x et n vérifiant l'équation. Montrer que x et n sont impairs. (Indication : on pourra réduire modulo 4).
2. Décomposer 3^n en produit d'irréductibles de l'anneau $\mathscr{O}_K$.
3. Montrer que $x + \sqrt{-2}$ et $x - \sqrt{-2}$ sont premiers entre eux dans l'anneau $\mathscr{O}_K$.
4. En déduire qu'il existe $\varepsilon_0, \varepsilon_1 \in \{\pm 1\}$ tels que $x - \sqrt{-2} = \varepsilon_0(1 - \varepsilon_1\sqrt{-2})^n$. (Les propriétés de l'anneau $\mathscr{O}_K$ employées devront être mentionnées explicitement).
5. On pose $a = 1 + \sqrt{-2}$ et $b = 1 - \sqrt{-2}$. Montrer que $a = 2 - b$, $\sqrt{-2} = 1 - b$, $2x = \varepsilon_0(a^n + b^n)$ et $-2\sqrt{-2} = \varepsilon_0\varepsilon_1(a^n - b^n)$.
6. Montrer que l'anneau $\mathscr{O}_K/b\mathscr{O}_K$ est isomorphe à $\mathbb{F}_3$.
7. Montrer que $\varepsilon_0\varepsilon_1 = 1$. (Indication : utiliser les résultats des deux questions précédentes). En déduire que $-2\sqrt{-2} = a^n - b^n$.
8. Montrer que $a^{2^v} \equiv 1 - 2^v(\sqrt{-2} + 2) \pmod{2^{v+2}}$ dans $\mathscr{O}_K$, pour tout entier $v \geqslant 2$. (Indication : procéder par récurrence sur v, à l'aide de la formule de binôme).
9. On considère maintenant deux solutions x_0, n_0 et x_1, n_1 de l'équation diophantienne, avec $n_1 > n_0$. On note v le plus grand entier tel que $2^v \mid (n_1 - n_0)$, et on suppose $v \geqslant 2$. Montrer que $a^{n_1 - n_0} \equiv 1 + (n_1 - n_0)(\sqrt{-2} + 2) \pmod{2^{v+2}}$.
10. En déduire que $a^{n_1} \equiv a^{n_0} + (n_1 - n_0)(\sqrt{-2} + 2)a^{n_0} \pmod{2^{v+2}}$, puis, en calculant $a^{n_1} - b^{n_1}$, que $0 \equiv 2(n_1 - n_0)(\varepsilon_0 x_0 - 2)\sqrt{-2} \pmod{2^{v+2}}$.
11. En déduire que $2^{v+1} \mid (n_1 - n_0)$, que qui contredit la définition de v. Montrer que chaque classe de congruence modulo 4 contient au plus un entier $n \geqslant 0$ tel que $3^n - 2$ soit un carré.
12. Quelles sont les solutions de l'équation $x^2 + 2 = 3^n$, avec x et n des entiers positifs ? (La réponse doit bien sûr être démontrée).