

DM 1
À remettre le 12 février

Dans tout le problème, $\left(\frac{x}{p}\right)$ désigne le résidu quadratique (ou symbole de Legendre) de x modulo un nombre premier p .

Exercice 1. Le but de cet exercice est de montrer que l'équation

$$2y^2 = x^4 - 17 \quad (1)$$

n'a pas de solution dans $\mathbb{Q}^2$.

1. Montrer que cela équivaut à montrer que l'équation

$$2u^2 = v^4 - 17w^4 \quad (2)$$

n'a pas de solution $(u, v, w) \in \mathbb{Z}^3$ avec $v \wedge w = 1$.

2. On suppose, par l'absurde, que (2) admet une solution $(u, v, w) \in \mathbb{Z}^3$ avec $v \wedge w = 1$.
 - (a) Montrer que 17 ne divise pas u . En déduire que $\left(\frac{u}{17}\right) = -1$ (on pourra montrer que 2 n'est pas une puissance 4ième modulo 17).
 - (b) Soit p un nombre premier impair divisant u . Montrer que 17 est un carré modulo p . En déduire que p est un carré modulo 17. En considérant tous les facteurs premiers de u , conclure que $\left(\frac{u}{17}\right) = +1$, d'où une contradiction.

Exercice 2. Soit p un nombre premier différent de 2. Le but de cet exercice est d'établir une formule pour le nombre N_p de solutions dans $\mathbb{F}_p^2$ de l'équation $x^2 + y^2 = 1$.

1. Pour $a \in \mathbb{F}_p$, exprimer le nombre de solutions dans $\mathbb{F}_p$ de l'équation $x^2 = a$ en fonction du symbole de Legendre $\left(\frac{a}{p}\right)$.
2. En déduire que $N_p = \sum_{a+b=1} \left[1 + \left(\frac{a}{p}\right)\right] \left[1 + \left(\frac{b}{p}\right)\right]$
3. Soit $b \in \mathbb{F}_p \setminus \{0\}$. En remarquant que l'application $a \mapsto ab$ est une bijection de $\mathbb{F}_p$ dans lui-même, montrer que $\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = \sum_{a \in \mathbb{F}_p} \left(\frac{ab}{p}\right)$. En déduire que $\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = 0$ (choisir b tel que $\left(\frac{b}{p}\right) \neq 1$).
4. Déduire de ce qui précède que

$$N_p = p + \sum_{a+b=1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right). \quad (3)$$

T.S.V.P.

5. En remarquant que $\sum_{a+b=1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \sum_{\substack{a+b=1 \\ b \neq 0}} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ et que $\left(\frac{b}{p}\right) = \left(\frac{b^{-1}}{p}\right)$ si $b \neq 0$, montrer que l'équation (3) équivaut à

$$N_p = p + \sum_{\substack{a \in \mathbb{F}_p \\ a \neq 1}} \left(\frac{a(1-a)^{-1}}{p} \right). \quad (4)$$

6. En remarquant que l'application $a \mapsto a(1-a)^{-1}$ est une bijection de $\mathbb{F}_p \setminus \{1\}$ sur $\mathbb{F}_p \setminus \{-1\}$, conclure que

$$N_p = p - (-1)^{\frac{p-1}{2}} = \begin{cases} p-1 & \text{si } p \equiv 1 \pmod{4} \\ p+1 & \text{si } p \equiv 3 \pmod{4} \end{cases}.$$