UNIVERSITÉ DE BORDEAUX I 2006-2007
MASTER DE MATHÉMATIQUES *1ère année*
**Option : Théorie des nombres.**

**Corrigé du DM 1**

**Exercice 1.**

1. Clairement, une solution $(u,v,w) \in \mathbb{Z}^3$ de (2), induit, en divisant par $w^4$, une solution rationnelle de (1) ($x = \frac{v}{w}$ et $y = \frac{u}{w^2}$). Inversement, supposons que (1) admette une solution $(x,y) = (\frac{a}{b}, \frac{c}{d}) \in \mathbb{Q}^2$. On suppose en outre que $a \wedge b = c \wedge d = 1$. En chassant les dénominateurs, on obtient

$$2c^2b^4 = a^4d^2 - 17b^4d^2.$$

En particulier, $d^2|2c^2b^4$, d'où $d^2|2b^4$ ( puisque $c \wedge d = 1$) et $b^4|a^4d^2$ soit $b^4|d^2$ (puisque $a \wedge b = 1$). Ainsi, $d^2 = b^4$ ou $2b^4$, mais cette deuxième option est exclue puisque $2$ n'est pas un carré dans $\mathbb{Q}$. Donc $d^2 = b^4$, et en simplifiant on obtient

$$2c^2 = a^4 - 17b^4$$

qui est bien une solution de (2) du type demandé.

2. (a) Si $17$ divisait $u$, alors $v^4 - 17w^4$ serait divisibles par $17^2$ ce qui impliquerait que $v$ et $w$ soient divisibles par $17$, en contradiction avec l'hypothèse $v \wedge w = 1$. Modulo $17$, l'équation (2) devient

$$2u^4 \equiv v^4 \mod 17.$$

Si $u$ était un carré modulo $17$, on en déduirait que $2$ est un puissance $4$ième modulo $17$. Or l'équation $x^2 = 2$ possède deux solutions modulo $17$, à savoir $6$ et $-6$, et aucune des deux n'est un carré : on peut le vérifier "à la main" ou utiliser les propriétés du symbole de Legendre, dont la loi de réciprocité quadratique, pour calculer

$$\left(\frac{-6}{17}\right) = (-1)^{\frac{17-1}{2}} \left(\frac{6}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = -1.$$

En conclusion, $\left(\frac{u}{17}\right) = -1$

(b) Si $p$ est un premier divisant $u$ (et donc nécessairement distinct de $17$ d'après la question précédente), alors on a $v^4 \equiv 17w^4 \mod p$. Si $p$ divisait $v$ ou $w$, alors il diviserait les deux ($p \neq 17$) ce qui est contraire à l'hypothèse $v \wedge w = 1$. Donc $w$ est inversible modulo $p$, d'où l'on déduit que $17$ est un carré modulo $p$. La loi de réciprocité quadratique entraîne alors que

$$\left(\frac{p}{17}\right) = (-1)^{\frac{17-1}{2}\frac{p-1}{2}} \left(\frac{17}{p}\right) = +1.$$

Comme par ailleurs $\left(\frac{2}{17}\right) = +1$, on conclut, en décomposant $u$ en produit de facteurs premiers, que $\left(\frac{u}{17}\right) = +1$, d'où la contradiction.

**Exercice 2.**

1. Le nombre de solutions dans $\mathbb{F}_p$ de l'équation $x^2 = a$ est $0$ si $a$ n'est pas un carré, $1$ si $a = 0$ et $2$ si $a$ est un carré non nul. Dans tous les cas, on constate que ce nombre coïncide avec $1 + \left(\frac{a}{p}\right)$.
2. On a donc
$$N_p = \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=1}} \#\left\{x \in \mathbb{F}_p \mid x^2 = a\right\} \#\left\{x \in \mathbb{F}_p \mid x^2 = b\right\} = \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=1}} \left[1 + \left(\frac{a}{p}\right)\right]\left[1 + \left(\frac{b}{p}\right)\right].$$
3. On a, pour tout $b \in \mathbb{F}_p \setminus \{0\}$,
$$\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) = \sum_{a\in\mathbb{F}_p} \left(\frac{ab}{p}\right) = \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right) \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right),$$
d'où
$$\left(1 - \left(\frac{b}{p}\right)\right) \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) = 0,$$
soit, en choisissant $b$ tel que $\left(\frac{b}{p}\right) \neq 1$,
$$\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) = 0.$$
4. Immédiat.
5. C'est clair.
6. On a donc
$$N_p = p + \sum_{\substack{a\in\mathbb{F}_p \\ a\neq 1}} \left(\frac{a(1-a)^{-1}}{p}\right) = p + \sum_{\substack{a\in\mathbb{F}_p \\ a\neq -1}} \left(\frac{a}{p}\right) = p + \left(\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\right) - \left(\frac{-1}{p}\right) = p - (-1)^{\frac{p-1}{2}}$$
puisque $\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) = 0$.