Arithmétique des formes quadratiques et théorème de Hasse-Minkowski

Exercice 1 Déterminer si 2024 est un carré modulo 2953. On remarquera que 2953 est premier.

Exercice 2 Soit p un nombre premier impair. Soit C le nombre de carrés modulo p appartenant à l'intervalle $\{1,\dots,\frac{p-1}{2}\}$, et soit N celui des non carrés.

1) Montrer que, si $p \equiv 1 \mod 4$, alors $C = \frac{p-1}{4}$.
2) Montrer que $C = N$ si, et seulement si, $p \equiv 1 \mod 4$.

On cherche à montrer que, si $p \equiv 3 \mod 8$ et $p \neq 3$, alors $C \equiv N \mod 3$. Pour ce faire, on introduit :

$$\alpha = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a, \quad \beta = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a, \quad \gamma = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

3) Montrer que $\alpha = \left[1 - \left(\frac{-1}{p}\right)\right]\beta + p\left(\frac{-1}{p}\right)\gamma$.
4) Montrer que $\alpha = \left(\frac{2}{p}\right)\left[2\left(1 - \left(\frac{-1}{p}\right)\right)\beta + p\left(\frac{-1}{p}\right)\gamma\right]$.
5) En déduire que, si $p \equiv 3 \mod 8$, alors $p\gamma = 3\beta$.
6) Conclure.

Exercice 3 Soient $\alpha, \beta \in \mathbb{F}_p^\times$. On cherche à calculer le nombre S de solutions de l'équation $\alpha x^2 + \beta y^2 = 1$ dans $\mathbb{F}_p^2$.

1) Soit $a \in \mathbb{F}_p$. Montrer que le nombre de solutions de l'équation $x^2 = a$ dans $\mathbb{F}_p$ est $N_a := 1 + \left(\frac{a}{p}\right)$.
2) En déduire que :

$$S = \sum_{\substack{a,b \in \mathbb{F}_p \\ \alpha a + \beta b = 1}} N_a N_b,$$

puis que $S = p + \left(\frac{\beta}{p}\right) J$, avec :

$$J := \sum_{a \in \mathbb{F}_p} \left(\frac{a(1-\alpha a)}{p}\right).$$

3) Montrer que :

$$J = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a^{-1} - \alpha}{p}\right),$$

puis que $S = p - \left(\frac{-\alpha\beta}{p}\right)$.

Exercice 4 *(Théorème de Chevalley-Warning)* Soit $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré d avec $0 < d < n$. Soit :

$$V = \{(x_1, ..., x_n) \in \mathbb{F}_q^n | P(x_1, ..., x_n) = 0\}.$$

1) Soient $Q = 1 - P^{q-1} \in \mathbb{F}_q$ et $S = \sum_{x \in \mathbb{F}_q^n} Q(x)$. Montrer que $S = |V|$ dans $\mathbb{F}_q$.
2) Montrer que $S = 0$.
3) Déduire de ce qui précède que P admet un zéro non trivial dans $\mathbb{F}_q^n$.
4) Par contre, il existe un polynôme $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré n dont l'unique zéro dans $\mathbb{F}_q^n$ est $(0, ..., 0)$. Pouvez-vous exhiber un tel polynôme? Vous pourrez vous aider de la fonction norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Exercice 5 Soit p un nombre premier impair. Soit $u \in \mathbb{Z}_p^\times$ un élément qui n'est pas un carré. On considère la forme quadratique :

$$q_0(X, Y, Z, T) = X^2 - uY^2 - pZ^2 + upT^2.$$

1) Montrer que q_0 est anisotrope dans $\mathbb{Q}_p$.
2) Soit maintenant q une forme quadratique anisotrope en 4 variables sur $\mathbb{Q}_p$.
   a) Montrer que q est isométrique à l'une des formes quadratiques suivantes :

$$X^2 - uY^2 - pZ^2 + puT^2, -X^2 + uY^2 + pZ^2 - puT^2,$$
$$X^2 - uY^2 + pZ^2 - puT^2, -X^2 + uY^2 - pZ^2 + puT^2.$$

   b) Montrer que les formes quadratiques $X^2 - uY^2$ et $-X^2 + uY^2$ sont isomoétriques.
   c) Conclure que q est isométrique à q_0.

Exercice 6 Soient q une forme quadratique et $a \in k$. Montrer que, si l'équation $q = a$ a des solutions dans tous les $\mathbb{Q}_p$ et dans $\mathbb{R}$, alors elle a des solutions dans $\mathbb{Q}$.

Exercice 7 Soit a un nombre rationnel. Montrer que a est somme de trois cubes de nombres rationnels si, et seulement si, il n'est pas de la forme $4^n(8m-1)r^2$ avec $n, m \in \mathbb{N}$ et $r \in \mathbb{Q}$.

Exercice 8 Montrer que l'équation $(t^2 - 13)(t^2 - 17)(t^2 - 221) = 0$ admet des solutions réelles, des solutions dans $\mathbb{Q}_p$ pour tout nombre premier p, mais pas de solutions rationnelles.

Exercice 9 Soient K une extension de degré 4 de $\mathbb{Q}$ et $\alpha \in K \smallsetminus \mathbb{Q}$ tel que $a := \alpha^2 \in \mathbb{Q}$. On choisit une $\mathbb{Q}$-base $(\omega_1, \omega_2, \omega_3, \omega_4)$ de K et on considère l'équation :

$$N_{K/\mathbb{Q}}(w\omega_1 + x\omega_2 + y\omega_3 + z\omega_4) = c(t^2 - a), \tag{1}$$

où w, x, y, z, t sont les variables et $c \in \mathbb{Q}^\times$ est fixé.

1) Vérifier qu'il s'agit d'une équation polynomiale à coefficients rationnels. On suppose dans la suite de l'exercice qu'elle a des solutions dans $\mathbb{R}$.
2) Montrer que l'équation :
$$u^2 - av^2 = c \tag{2}$$
admet une solution rationnelle.
3) Montrer que l'ensemble des solutions rationnelles de l'équation (2) est dense dans l'ensemble des solutions réelles de cette même équation.
4) Montrer qu'il existe une solution rationnelle (u_0, v_0) de (2) telle que l'équation :
$$\frac{1}{t-\alpha} N_{K/\mathbb{Q}(\alpha)}(w\omega_1 + x\omega_2 + y\omega_3 + z\omega_4) = u_0 + v_0\alpha$$
admet des solutions réelles.
5) Conclure que l'équation (1) admet une solution rationnelle.