TD 10 : Formes quadratiques binaires

Exercice 1. [Discriminants fondamentaux]

Un entier $D \equiv 0, 1 \mod 4$ est un discriminant fondamental si toute forme de discriminant D est primitive.

(a) Si $D \equiv 1 \mod 4$, montrer que D est un discriminant fondamental si et seulement si il est sans facteur carré.

(b) Si $D \equiv 0 \mod 4$, montrer que D est un discriminant fondamental si et seulement si $D/4 \equiv 2, 3 \mod 4$ et $D/4$ est sans facteur carré.

Exercice 2. [Discriminants carrés]

Soit $k \in \mathbb{N}^*$ et $D = k^2$.

(a) Pour $q = (a, b, c)$ de discriminant D, donner explicitement une solution non nulle de $q(x, y) = 0$.

(b) Montrer que $q \overset{+}{\sim} (0, k, c)$ pour un certain c entre 0 et $k - 1$.

(c) Montrer que c est entièrement déterminé par q, et en déduire que $h(D) = k$.

Exercice 3. [Calculs de nombres de classes]

(a) Calculer $h(D)$ pour $D = 5, 8, 12$ grâce à la preuve du théorème de Lagrange.

(b) Montrer que pour $0 > D \geq -11$, $h(D) = 1$ grâce à la réduction de Gauss.

(c) Calculer $h(D)$ pour $D = -23, -24$.

(d) Montrer que $h(-163) = 1$ en considérant les $(b^2 + 163)/4$ avec $|b| \leq 7$ pair.

Exercice 4. [Formes ambigües]

Pour $q = (a, b, c)$, on note $q^{opp} = (a, -b, c)$, dite la forme opposée. Elle est dite ambigüe si $q^{opp} \overset{+}{\sim} q$.

(a) Montrer que $q_1 \overset{+}{\sim} q_2$ si et seulement si $q_1^{opp} \overset{+}{\sim} q_2^{opp}$. L'opposé d'une classe d'équivalence propre C en est donc une également, on la note C^{opp}.

(b) Supposons que $D < 0$, montrer qu'une forme réduite (a, b, c) de discriminant D est ambigüe si et seulement si $b = 0$, $b = a$ ou $c = a$.

(c) Pour τ la fonction « nombre de diviseurs positifs », montrer que le nombre de formes réduites ambigües de discriminant D avec $b = 0$ est $\tau(-D/4)$.

(d) Montrer que les formes réduites (a, b, c) telles que $b = a$ ou $c = a$ sont en bijection avec les formes (a, a, c) telles que $1 \leq a \leq 2c$.

(e) Soit $t(D)$ le nombre de diviseurs premiers de D. Montrer que le nombre $A(D)$ de formes primitives (a, a, c) telles que $1 \leq a \leq 2c$ est égal à $2^{t(D)}$ si $D \equiv 1 \mod 4$.

(f) En déduire le nombre de classes ambigües de $\mathrm{Cl}(D)$ pour $D = -19, -23, -27$.