TD 5 : Formes quadratiques binaires et révision

Exercice 1. [Formes primitives et discriminants fondamentaux]

Une forme quadratique $q(x,y) = ax^2+bxy+cy^2$ est dite primitive si $\text{pgcd}(a,b,c) = 1$. Un entier $D \equiv 0,1 \mod 4$ est un discriminant fondamental si toute forme de discriminant D est primitive.

(a) Montrer que pour tout D, la forme quadratique q_D est primitive.

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

(c) 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 qu'il n'y a qu'une seule classe d'équivalence de formes de discriminant D.

Exercice 3. [Discriminants positifs]

Soit $D > 0$ et congru à 0 ou 1 modulo 4, non carré.

(a) Pour $D = 5,8,9$, montrer qu'il n'existe à équivalence près qu'une seule forme quadratique.

(b) Pour $D = 12$, montrer qu'il existe exactement deux classes d'équivalences de formes quadratiques.

Exercice 4. [Nombres premiers représentés par une forme quadratique]

Dans cet exercice, on cherche les nombres premiers p tels que $p = q(x,y)$, avec $q(x,y) = x^2 + 5y^2$.

(a) Expliquer pourquoi ce n'est pas évident via les corps quadratiques.

(b) Montrer qu'il existe exactement deux classes d'équivalence de formes quadratiques positives de discriminant -20, et en donner des représentants.

(c) Montrer que si p est représenté par q, alors p est congru à $1,3,7$ ou 9 modulo p.

(d) Réciproquement, supposons que p est congru à 1,3,7 ou 9 modulo 20. Montrer que soit q soit l'autre classe d'équivalence représente p.

(e) En choisissant a tel que $a^2 = -5 \mod p$, montrer que la forme quadratique $q_a(x,y) = (ay+px)^2 + 5y^2$ représente p ou $2p$.

(f) Déterminer suivant la congruence de p modulo 4 si q_a représente p ou $2p$.

(g) En déduire que $p = q(x,y)$ si et seulement si p est congru à 1 ou 9 modulo 20.

Exercice 5. |Théorème de Dirichlet faible]

Le but de cet exercice est de démontrer que pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers $p \equiv 1 \mod n$.

(a) Montrer qu'il suffit de prouver que pour tout $n \in \mathbb{N}^*$, il existe un nombre premier $p \equiv 1 \mod n$.

(b) Montrer que pour ϕ_n le n-ième polynôme cyclotomique, $|\phi_n(n)| > 1$ pour $n > 2$.

(c) Soit p un diviseur premier de $\phi_n(n)$. Montrer qu'il est premier à n.

(d) Soit t l'ordre de n modulo p, supposons par l'absurde que $t < n$. Montrer que $\phi_n(n)$ divise $(n^n - 1)/(n^t - 1)$ et en déduire une contradiction.

(e) Conclure que p est congru à 1 modulo n.