UNIVERSITÉ DE RENNES 1

Théorie des nombres

TP3 : Formes quadratiques binaires

Le but de l'exercice consiste à déterminer si un entier n est proprement représenté par une forme quadratique binaire définie positive donnée q. On represente une forme quadratique binaire $ax^2 + bxy + cy^2$ par la liste (ou le triplet) de 3 entiers $q = [a, b, c]$

1. Ecrire une procédure qui calcule le discriminant d'une forme quadratique $q = [a, b, c]$. Verifier sur $q = [1, 2, 3]$ et sur d'autres exemples.
2. Ecrire une procédure `est_definie_positive(q)` qui determine si une forme quadratique $q = [a, b, c]$ est définie positive (elle doit renvoyer un booléen True/False). Verifier sur $q = [1, 2, 3]$ et sur d'autres exemples. Combien y-a-t il de formes quadratiques définies positives telles que $0 \leq a, |b|, c \leq 50$?
3. Ecrire une procédure `action(q,P)` qui étant donnée une forme quadratique $q = [a, b, c]$ et une matrice $P \in SL_2(\mathbb{Z})$, renvoie le triplet $q' = [a', b', c']$ correspondant à la forme $q' = q \circ P$.
   Tester avec les matrices $P1 = (x, y) \mapsto (x + y, y)$, $P2 = (x, x + y)$, et $P3 = (-y, x)$ sur $q = [1, 2, 3]$.
4. Ecrire une procédure `est_reduite(q)` qui renvoie un booléen True/False selon que la forme quadratique definie positive $q = [a, b, c]$ est réduite (renvoyer False si elle n'est pas definie positive).
   Tester sur $q = [1, 2, 3], [3, 2, 1], [1, 1, 1], [1, -1, 1]$.
   Combien y-a-t il de formes quadratiques définies positives réduites telles que $0 \leq a, |b|, c \leq 50$?
5. Montrer que $[a, b, c]$ est équivalente à $[c, -b, a]$ en donnant la matrice P (de determinant 1) correspondante (il n'y a rien a programmer).
6. Programmer la reduction d'une forme quadratique binaire definie positive : écrire une procedure `reduire(q)` qui, etant donne $q = [a, b, c]$ renvoie un couple (q', P) où $P \in SL_2(\mathbb{Z})$, $q' = q \circ P$, et q' est reduite.
   On pourra vérifier que $\det(P) = 1$, et que q' est reduite avec la procédure deja ecrite.
7. Verifier que la forme réduite de $q(x, y) = 17x^2 + 50xy + 37y^2$ est $q'(x, y) = x^2 + 4y^2$ et que celle de $2x^2 - 2xy + 3y^2$ est $2x^2 + 2xy + 3y^2$. Quelle est la forme réduite de $[131, 165, 52]$?
8. Définir une procedure `sont_equivalentes(p,q)` qui détermine si les deux formes quadratiques binaires définies positives p, q sont équivalentes (elle doit renvoyer un booléen True/False).
   Parmi les formes quadratiques suivantes, dire lesquelles sont équivalentes entre elles :
   $$q_1 = [12, 19, 8], q_2 = [62, 77, 24], q_3 = [24, 19, 4], q_4 = [52, -173, 144]$$
9. Ecrire une procédure `representants(D,n)` qui, étant donné un entier $D < 0$ et $n \in \mathbb{Z}$, produit la liste de toutes les formes quadratiques binaires réduites, de discriminant D, et qui représentent proprement n. On veut une liste sans répétition.
   Pour trouver toutes les racines carrées d'un élément $a \in \mathbb{Z}/k\mathbb{Z}$, utiliser la méthode `a.sqrt(all=True)`.

Pour $D = -55$, vérifier qu'on trouve une forme réduite pour $n = 11$, aucune pour $n = 12$, et deux pour $n = 13$.

10. pour toutes les valeurs de $D \geq -100$ congrues à 0 ou 1 mod 4, donner le nombre des formes quadratiques reduites représentant 11. Pouquoi se restreint-on a $D \equiv 0, 1 \mod 4$?

    Pourquoi ne trouve-t-on jamais plus de 2 formes reduites (tester pour $D \geq -1000$) ? Dans quelles conditions s'attend on à ne trouver qu'au plus 2 formes réduites ?

    Trouver un couple (D, n) qui donne au moins 5 formes réduites.

11. Etant donné $n \in \mathbb{Z}$ et q une forme quadratique binaire définie positive, écrire une procédure qui détermine si q représente n proprement en utilisant la liste ci-dessus.
12. Est-ce que 7892 est proprement représenté par $[62, 77, 24]$?
13. Donner tous les nombres $n \leq 200$ qui sont représentés par la forme quadratique $x^2 + 7y^2$.
14. En utilisant les matrices de changements de base donnees par la procedure de reduction, programmer une variante qui donne une valeur x, y tq $q(x, y) = n$ lorsqu'il existe.
15. On veut maintenant savoir si n est representé par q (peu importe que ce soit proprement ou non). Programmer une procédure qui détermine si c'est le cas.