Opgaven 4

Opgave 12.
Implementeer (bij voorkeur in MAGMA) het tijdens het college behandelde algoritme dat de vectoren in een rooster tot een zekere lengte bepaald. (Het algoritme wordt soms het *Fincke-Pohst algoritme* genoemd.)

`Input`: Gram matrix van het rooster, grens M voor de normen van de roostervectoren.

`Output`: Lijst van paren (tuples) met als eerste component een vector en als tweede component de norm van de vector (handig om later vectoren van een bepaalde lengte uit de lijst te vissen).

Opmerkingen:

- Maak de functie robuust tegen onverwachte input, bijvoorbeeld tegen matrices die niet symmetrisch of niet positief definiet zijn.
- De nulvector hoort niet in de lijst.
- Je mag zelf beslissen of je van elk paar $(v, -v)$ slechts één vector of beide vectoren teruggeeft (maar natuurlijk wel consistent).

Bepaal voor de roosters A_n en D_n met $2 \leq n \leq 8$ de aantallen van vectoren van lengte 2, 4 en 6. Controleer je resultaten door deze aantallen met combinatorische argumenten ook theoretisch te berekenen.

Opgave 13.
Het wortelrooster (of Gosset rooster) E_8 is gegeven door

$$E_8 = D_8^+ := \{v \in \mathbb{R}^n \mid \sum_{i=1}^{8} v_i \in 2\mathbb{Z}, \text{ alle } v_i \in \mathbb{Z} \text{ of alle } v_i \in \frac{1}{2} + \mathbb{Z}\}.$$

(i) Bepaal een roosterbasis van E_8, de Gram matrix F van E_8 met betrekking tot deze basis en toon aan dat E_8 zelfdual is, dus dat $\det(F) = 1$ is (de determinant mag je met MAGMA bepalen).

(ii) Vergelijk de Hermite invariante $\gamma_8(E_8)$ met de Hermite invarianten van A_8 en D_8.

Opgave 14.
Zij x een minimale vector van E_8, dan is

$$E_7 := \{v \in E_8 \mid v \cdot x = 0\}$$

een 7-dimensionaal deelrooster van E_8. Als $x = (\frac{1}{2}, \ldots, \frac{1}{2})^{tr}$ gekozen wordt, is

$$E_7 = \{v \in E_8 \mid \sum_{i=1}^{8} v_i = 0\}.$$

(i) Bepaal een roosterbasis van E_7, de Gram matrix F van E_7 met betrekking tot deze basis en toon aan dat $E_7^{\#}/E_7 \cong C_2$.

(ii) Laat zien dat E_7 126 minimale vectoren heeft. Gebruik hiervoor je implementatie uit Opgave 12 en controleer dit met behulp van de theoretische beschrijving van de vectoren.

(iii) Vergelijk de Hermite invariante $\gamma_7(E_7)$ met de Hermite invarianten van A_7 en D_7.

Opgave 15.
Laten x en y minimale vectoren van E_8 zijn met $x \cdot y = 1$, d.w.z. x en y spannen een 2-dimensionaal hexagonaal rooster op. Dan is

$$E_6 := \{v \in E_8 \mid v \cdot x = v \cdot y = 0\}$$

een 6-dimensionaal deelrooster van E_8 en ook een deelrooster van E_7. Als $x = (\frac{1}{2}, \ldots, \frac{1}{2})^{tr}$ en $y = (1, 0, \ldots, 0, 1)^{tr}$ gekozen wordt, is

$$E_6 = \{v \in E_8 \mid \sum_{i=1}^{8} v_i = v_1 + v_8 = 0\}.$$

(i) Bepaal een roosterbasis van E_6, de Gram matrix F van E_6 met betrekking tot deze basis en toon aan dat $E_6^{\#}/E_6 \cong C_3$.

(ii) Laat zien dat E_6 72 minimale vectoren heeft.

(iii) Vergelijk de Hermite invariante $\gamma_6(E_6)$ met de Hermite invarianten van A_6 en D_6.

Opgave 16.
Twee lineair onafhankelijke vectoren $v, w \in \mathbb{R}^2$ heten *paargewijs gereduceerd* als $\|v\|^2 \leq \|w\|^2$ en $|v \cdot w| \leq \frac{1}{2}\|v\|^2$.

(i) Laat zien dat iteratie van de volgende twee stappen een willekeurige roosterbasis (v, w) van een 2-dimensionaal rooster L in een paarsgewijs gereduceerde basis transformeert:

  (a) Als $\|v\| > \|w\|$, verruil v en w.

  (b) Vervang w door $w - \lfloor \frac{v \cdot w}{\|v\|^2} \rceil v$.
  (Met $\lfloor x \rceil$ noteren we het gehele getal dat het dichtst bij x ligt, voor $x \in \frac{1}{2} + \mathbb{Z}$ wordt meestal in de richting van 0 afgerondt.)

(ii) Beschrijf de meetkundige betekenis van de reductie stap (b).

(iii) Laat zien dat paargewijs gereduceerde vectoren LLL-gereduceerd zijn.

(iv) Bewijs dat de kortere vector v van een paarsgewijs gereduceerde basis noodzakelijk een minimale vector van L is.

Webpagina: http://www.math.ru.nl/∼souvi/kristgroep_05