# Geometric Algorithms and Cryptography

Miroslav Kureš

May 11, 2020

**Geometric Algorithms and Cryptography.** *(The test. Solution time: 60 minutes.)*

**1.** The lattice $\mathcal{L}_1$ in $\mathbb{R}^2$ is given by its generator matrix

$$Z_1 = \begin{pmatrix} 1 & -16 \\ 4 & 1 \end{pmatrix}$$

and the lattice $\mathcal{L}_2$ is given by its generator matrix

$$Z_2 = \begin{pmatrix} 2 & 7 \\ 3 & 4 \end{pmatrix}$$

Decide whether $\mathcal{L}_1$ is a sublattice of $\mathcal{L}_2$ or whether $\mathcal{L}_2$ is a sublattice of $\mathcal{L}_1$. If you find that one lattice is a sublattice of the other, then compute the quotient group (i.e. $\mathcal{L}_1/\mathcal{L}_2$ or $\mathcal{L}_2/\mathcal{L}_1$).

**2.** Draw a sketch of the Voronoi tesselation of the lattice $\mathcal{L}_2^*$ (the dual lattice of $\mathcal{L}_2$ above).

---

**1.**

$$\begin{aligned} \mathcal{L}_1 &= \{(a+4b, -16a+b)\,; a, b \in \mathbb{Z}\}\,, \\ \mathcal{L}_2 &= \{(2c+3d, 7c+4d)\,; c, d \in \mathbb{Z}\}\,. \end{aligned}$$

For given integers $a$ and $b$ one can find $c = -4a-b$ and $d = 3a+2b$, which are also integers. It follows $\mathcal{L}_1 \subseteq \mathcal{L}_2$. On the other hand, for given integers $c$ and $d$ we find $a$ and $b$ which are not integers in general. Hence $\mathcal{L}_1 \subset \mathcal{L}_2$.

The area of the parallelogram formed by the elements of generator matrix $Z_1$ is 65 and the area of the parallelogram formed by the elements of generator matrix $Z_2$ is 13. Therefore, the quotient group has order 5 and such a group exists only one: the cyclic group $\mathbb{Z}_5$.

**2.**

$$Z_2^* = \left(Z_2^{-1}\right)^{\mathsf{T}} = \begin{pmatrix} -\frac{4}{13} & \frac{3}{13} \\ \frac{7}{13} & -\frac{2}{13} \end{pmatrix}$$

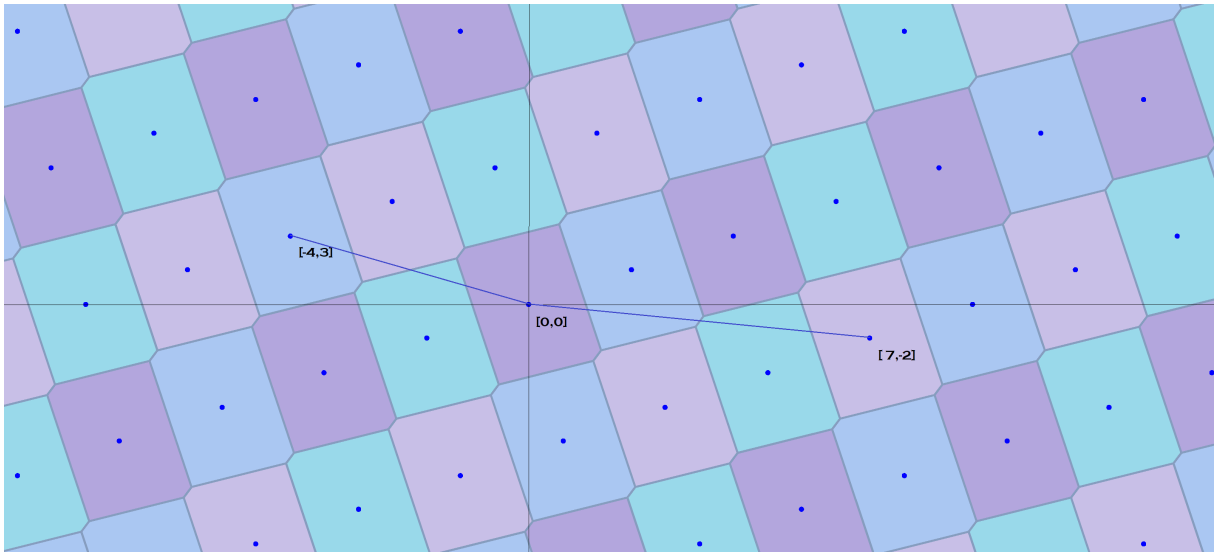


Figure 1: We see the lattice endpoints of $\mathcal{L}_2^*$ and hexagonal Voronoi cells. The lattice generators based on the matrix $Z_2^*$ are drawn, too. The scale unit is $\frac{1}{13}$.