Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: May 25, 2010

Computer Algebra

Spring 2010

Assignment Sheet 7

Exercise 1

Let $B = (b_1, \ldots, b_n)$ be a lattice basis and let $b_1^\star, \ldots, b_n^\star$ be its Gram-Schmidt orthogonalisation, that is, $b_j^\star$ is the orthogonal projection of b_j onto the orthogonal complement of $\langle b_1, \ldots, b_{j-1} \rangle$. Prove that for all $v \in \Lambda(B) \setminus \{0\}$, one has

$$|v| \geq \min_{j=1}^{n} |b_j^\star|$$

Exercise 2

Consider the problem of approximating a line in the plane with arbitrary slope $\alpha \in \mathbb{R}$ by a line with rational slope $\frac{p}{q}$, with $p \in \mathbb{Z}$ and small $q \in \mathbb{N}$. Prove that for every $\alpha \in \mathbb{R}$ and $Q \geq 2$ there exist $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, $1 \leq q \leq Q$ such that $|\alpha - \frac{p}{q}| \leq \frac{1}{qQ}$.

Hint: Consider the lattice generated by $\begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}$ and use Minkowski's theorem.

Exercise 3

In this exercise you will prove that a prime number p with $p \equiv 1 \pmod 4$ can be written as the sum of two squares $p = a^2 + b^2$ with $a, b \in \mathbb{N}$.

1. Prove that the equation $q^2 \equiv -1 \pmod p$ has a solution.
2. Let q be an arbitrary such solution and consider the lattice Λ generated by $\begin{pmatrix} 1 & 0 \\ q & p \end{pmatrix}$, and the disk of radius $\sqrt{2p - \varepsilon}$ around 0 for a small $\varepsilon > 0$.
   a) Prove that $|v|^2$ is divisible by p for each $v \in \Lambda$.
   b) Prove that there exists a $v \in \Lambda \setminus \{0\}$ with $|v|^2 = p$.
   c) Conclude that p is the sum of two squares.

Exercise 4
We say that a subgroup $G \subset \mathbb{R}^n$ is a discrete subgroup if there exists a $\delta > 0$ such that the distance between any two points in G is at least δ, i.e. G has no accumulation points. Prove that every lattice $\Lambda \subset \mathbb{R}^n$ is a discrete subgroup.

Exercise 5
Let $G \subset \mathbb{R}^n$ be a discrete subgroup. Prove that G is a lattice.

Hint: One can prove the following lemma: Let $v \in G$ and let $U = \langle v \rangle$ be the subspace of $\mathbb{R}^n$ spanned by v. Let $\pi : \mathbb{R}^n \to U^\perp$ be the orthogonal projection onto the orthogonal complement of U. Then $\pi(G)$ is a discrete subgroup.