

Problem Set 2

Instructor: Daniele Micciancio

Due on: Tue. Feb 7, 2012

Problem 1

Let $\mathbf{U} \in \mathbb{Z}^{n \times n}$ be an integer matrix such that $\det(\mathbf{U}) = \pm 1$. Prove that \mathbf{U} is unimodular, according to the definition used in class, i.e., there is an integer matrix $\mathbf{V} \in \mathbb{Z}^{n \times n}$ such that $\mathbf{UV} = \mathbf{I}$. [Hint: use the fact that any full rank integer lattice $\Lambda \subseteq \mathbb{Z}^n$ contains $\det(\Lambda) \cdot \mathbb{Z}^n$ as a sublattice.]

Problem 2

Let $\Lambda \subseteq \Lambda'$ be two full rank lattices. Prove that if $\det(\Lambda) = \det(\Lambda')$ then $\Lambda = \Lambda'$. Prove also that if $\Lambda \neq \Lambda'$, then $\det(\Lambda) \geq 2 \det(\Lambda')$. [Hint: use the result from Problem 1.]

Problem 3

Let $\Lambda_0 = \mathcal{L}(\mathbf{B})$ be a full rank lattice with basis vectors of length at most $\|\mathbf{b}_i\| \leq \beta$, and let $\Lambda_0 \subset \Lambda_1 \subset \dots \subset \Lambda_m$ a sequence of lattices with minimum distance $\lambda_1(\Lambda_i) \geq 1$. Prove that the length of the sequence is at most $m \leq n \cdot \lg(\sqrt{n}\beta)$

Problem 4

Minkowski's convex body theorem shows that the minimum distance of an n -dimensional lattice is at most $\lambda(\Lambda) \leq 2(\det(\Lambda)/V_n)^{1/n}$, where V_n is the volume of the n -dimensional ball. Prove that the covering radius of a lattice (defined in homework 1) satisfies a similar lower bound $\rho(\Lambda) \geq (\det(\Lambda)/V_n)^{1/n}$. [Hint: use an argument similar to the proof of Blichfeldt theorem.]

Problem 5

Let $\Lambda \subset \mathbb{R}^n$ be a full rank lattice and $\mathbf{v} \in \Lambda$ a lattice vector. Prove that $\Lambda \cup (\Lambda + \frac{\mathbf{v}}{2})$ is also a lattice. [Use the HNF for integer matrices.]

Problem 6

Let Λ a full rank lattice such that $\rho(\Lambda) > 2\lambda(\Lambda)$. Prove that if \mathbf{h} is a point in space at distance at least $(\rho + 2\lambda)/2 < \rho$ from the lattice, and $\mathbf{v} \in \Lambda$ is a lattice point within distance ρ from $2\mathbf{h}$, then $\mathbf{v}/2$ is at distance at least $\lambda(\Lambda)$ from the lattice.

Problem 7

Prove that for every full rank lattice Λ there is a lattice $\Lambda' \supseteq \Lambda$ such that $\rho(\Lambda') \leq 2\lambda(\Lambda) \leq 2\lambda(\Lambda')$. Conclude that $\lambda(\Lambda') = \Theta((\det(\Lambda')/V_n)^{1/n})$, i.e., Minkowski's bound on the minimum distance is tight within a constant factor. [Hint: use the results from the previous problems.]