Geometry of Numbers
Foundations and Algorithmic Aspects

University of Sydney, Department of Mathematics and Statistics
Damien Stehlé

First assignment, due 02/09/2008

This assignment will represent 20% of the overall mark.

1 Minima and Gram-Schmidt orthogonalisation

Let $\vec{b}_1, \ldots, \vec{b}_d$ be a basis of a lattice L. Let $\vec{b}_1^*, \ldots, \vec{b}_d^*$ be the Gram-Schmidt orthogonalisation of the $\vec{b}_i$'s and $\lambda_1, \ldots, \lambda_d$ be the successive minima of L.

1. Show that it is not true in general that $\lambda_d \geq \max_i \|\vec{b}_i^*\|$.
2. Show that for any $j \leq d$, we have $\lambda_j \geq \min_{i \geq j} \|\vec{b}_i^*\|$.

2 Recovering a basis

Let L be a d-dimensional lattice and $\vec{b}_1, \ldots, \vec{b}_d$ be linearly independent vectors of L. Show that there exists a basis $\vec{c}_1, \ldots, \vec{c}_d$ of L such that

$$\max_i \|\vec{c}_i\| \leq \sqrt{d} \cdot \max_i \|\vec{b}_i\|.$$

We suggest the following steps.

1. Show that there exists a basis $\vec{B}_1, \ldots, \vec{B}_d$ of L such that for any i, we have $\mathrm{Span}_{j \leq i}(\vec{b}_j) = \mathrm{Span}_{j \leq i}(\vec{B}_j)$.
2. Let $\vec{b}_1^*, \ldots, \vec{b}_d^*$ (resp. $\vec{B}_1^*, \ldots, \vec{B}_d^*$) be the Gram-Schmidt orthogonalisation of the $\vec{b}_i$'s (resp. the $\vec{B}_i$'s). Show that for any i, we have $\|\vec{B}_i^*\| \leq \|\vec{b}_i^*\|$.
3. Derive the $\vec{c}_i$'s from the $\vec{B}_i$'s.

3 Thue's theorem

Let p and m be two non-zero integers. Using a two-dimensional lattice, show that there exists a non-zero pair of integers x_1, x_2 such that

$$x_2 = mx_1 \bmod p \quad \text{and} \quad |x_1|, |x_2| \leq \sqrt{p}.$$

4 HKZ-reduction

Let d grow to infinity. Show that for any Hermite-Korkine-Zolotarev-reduced basis $\vec{b}_1, \ldots, \vec{b}_d$, we have $\|\vec{b}_d^*\| \geq \exp\left(-\frac{1+o(1)}{4} \ln^2 d\right) \|\vec{b}_1\|$, where $\vec{b}_1^*, \ldots, \vec{b}_d^*$ is the Gram-Schmidt orthogonalisation of the $\vec{b}_i$'s. Hint: use Minkowski's theorem.