Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 3: Lattices
Due in class Monday, September 17

References. Neukirch, Sections 1.4 and 1.5. For LLL (and in general if you're interested in algorithms in number theory) see Cohen's *A Course in Computational Algebraic Number Theory*, especially Chapter 2. For more on lattices in general, the magnum opus is *Sphere Packings, Lattices and Groups* by Conway and Sloane.

Please submit any *seven* of the following problems.

Lattices.

1. Neukirch I.4.1 (modified): Show that a $\mathbb{Z}$-submodule Γ of $\mathbb{R}^n$ is a (complete) lattice if and only if Γ is discrete and $\mathbb{R}^n/\Gamma$ is compact.

2. Let $a, b, c \in \mathbb{Z}$ be nonzero, pairwise coprime integers not all of the same sign. Suppose that the equation $ax^2+by^2+cz^2 \equiv 0 \pmod{2|abc|}$ has a solution with $\gcd(x, y, z, 2abc) = 1$. Show that there exists a subgroup L of $\mathbb{Z}^3$ of index $2|abc|$ such that for every $(x, y, z) \in L$, $ax^2 + by^2 + cz^2 \equiv 0 \pmod{2|abc|}$.

3. (Hasse-Minkowski theorem) In the notation of the previous problem, make $\mathbb{Z}^3$ into a lattice under the norm $|(x, y, z)| = |a|x^2 + |b|y^2 + |c|z^2$. Prove that there is a nonzero element (x, y, z) of L satisfying $|x| \leq \sqrt{|bc|}$, $|y| \leq \sqrt{|ca|}$, $|z| \leq \sqrt{|ab|}$, and that in fact this triple is a nonzero solution of $ax^2 + by^2 + cz^2 = 0$.

The Minkowski space of a number field.

1. Neukirch I.5.2: Show that the convex, centrally symmetric set

$$X_t = \{(z_\tau) \in K_\mathbb{R} | \sum_\tau |z_\tau| < t\}$$

has volume $\mathrm{Vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$, where r and $2s$ are the numbers of real and complex embeddings.

2. Neukirch I.5.3: Show that in every ideal $\mathfrak{a} \neq 0$ of $\mathfrak{o}_K$ there exists an $a \neq 0$ such that

$$|\operatorname{Norm}(a)| \leq M[\mathfrak{o}_K : \mathfrak{a}],$$

where $M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{Disc}(K)|}$.

3. Let K be a number field such that $|\operatorname{Disc}(K)| = 1$. Prove that $K = \mathbb{Q}$. (Hint: use the previous exercise.)

Interlude: The LLL algorithm. In this section, we describe a constructive version of Minkowski's lattice point theorem, due to Lenstra, Lenstra and Lovász (LLL). This result gives a weaker bound than Minkowski's theorem, but yields a highly practical algorithm for finding short vectors in a lattice.

Let $\vec{v}_1, \dots, \vec{v}_n$ be a basis of the lattice L. Let $\vec{w}_1, \dots, \vec{w}_n$ be the Gram-Schmidt orthogonalization of this basis; namely, $\vec{w}_1 = \vec{v}_1$ and

$$\vec{w}_i = \vec{v}_i - \sum_{j=1}^{i-1} \frac{\vec{v}_i \cdot \vec{w}_j}{\vec{w}_j \cdot \vec{w}_j} \vec{w}_j.$$

(Note that the $\vec{w}_i$ will not necessarily lie in L itself, only in the real vector space $L \otimes_{\mathbb{Z}} \mathbb{R}$.) Put $\mu_{i,j} = (\vec{v}_i \cdot \vec{w}_j)/(\vec{w}_j \cdot \vec{w}_j)$ for $1 \leq j < i \leq n$. We say the basis is *LLL-reduced* if

$$|\mu_{i,j}| \leq \frac{1}{2} \qquad 1 \leq j < i \leq n \tag{1}$$

and

$$|\vec{w}_i + \mu_{i,i-1} \vec{w}_{i-1}|^2 \leq \frac{3}{4} |\vec{w}_{i-1}|^2 \tag{2}$$

for $i = 2, \dots, n$.

1. Let $\vec{v}_1, \dots, \vec{v}_n$ be an LLL-reduced basis of the lattice L. Prove that

$$\mathrm{Vol}(L) \leq \prod_{i=1}^{n} |\vec{v}_i| \leq 2^{n(n-1)/4} \, \mathrm{Vol}(L)$$
$$|\vec{v}_j| \leq 2^{(i-1)/2} |\vec{w}_i| \qquad 1 \leq j < i \leq n$$
$$|\vec{v}_1| \leq 2^{(n-1)/4} \, \mathrm{Vol}(V)^{1/n}.$$

2. Let $\vec{v}_1, \dots, \vec{v}_n$ be an arbitrary basis of the lattice L, and set $k = 2$. Show that the following algorithm necessarily terminates, and that the resulting basis is LLL-reduced.

   (a) For $i = 2, \dots, n$, replace $\vec{v}_i$ by itself plus a suitable linear combination of $\vec{v}_1, \dots, \vec{v}_{i-1}$ so that $|\mu_{i,j}| \leq 1/2$ for $j < i$.

   (b) If (2) holds for $i = 2, \dots, n$, stop. Otherwise, choose the smallest i for which (2) fails, then switch $\vec{v}_{i-1}$ and $\vec{v}_i$ and go back to (a).

   (Hint: consider how the quantity $\prod_{i=1}^{n} |\vec{w}_i|^{n-i}$ changes.)

3. Write a Magma program to convert an arbitrary basis of a lattice into an LLL-reduced basis. Your program should also call the built-in Magma function to perform LLL reduction and compare answers.

4. Suppose you are given an LLL-reduced basis $\vec{v}_1, \vec{v}_2, \vec{v}_3$ of a rank 3 lattice. Give an algorithm for finding the shortest nonzero vector in the lattice. (Hint: you can write down a finite list of linear combinations of basis vectors such that the shortest vector must appear in this list.)