Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 4: Lattices
Due in class Monday, September 24

References. Neukirch, Sections 1.5 and 1.6.

Please submit *nine* problems. Do not include both of the final two (Magma-based) problems.

Leftover Problem on Minkowski Space.

1. (Hermite's Theorem) Prove that for any positive integer N, there are only finitely many number fields K (of all degrees) such that $|\operatorname{Disc}(K)| \leq N$. (Hint: use one of last week's homework problems to deduce a lower bound on the discriminant.)

Class Numbers.

1. Neukirch I.6.3: Show that in every ideal class of a number field K of degree n and signature (r, s), there exists an integral ideal $\mathfrak{a}$ of absolute norm at most $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{Disc}(K)|}$. (Hint: imitate the proof given in class, but replace the invocation of Minkowski with a result from last week's homework.)

2. Use the previous exercise to deduce that every ideal class of the number field $\mathbb{Q}[x]/(x^5 - x + 1)$ contains an ideal of absolute norm at most 3. (Hint: first compute the discriminant of the polynomial $x^5 - x + 1$. You may use Magma for that step if you wish.)

3. Prove that the number field $\mathbb{Q}[x]/(x^5 - x + 1)$ contains no ideals of norm 2 or 3. Conclude from the previous exercise that it has class number 1. (Hint: prove that if there is an ideal $\mathfrak{a}$ of prime absolute norm p, then $x^5 - x + 1$ must have a root modulo p.)

4. Neukirch I.6.6: Let $\mathfrak{a}$ be an integral ideal of K and $\mathfrak{a}^m = (a)$. Show that $\mathfrak{a}$ becomes a principal ideal in the field $L = K(\sqrt[m]{a})$, in the sense that $\mathfrak{a}\mathfrak{o}_L = (\alpha)$ for some α.

5. Neukirch I.6.7: Show that, for every number field K, there exists a finite extension L of K such that every ideal of K becomes a principal ideal in L.

Class Groups of Quadratic Fields.

The class groups of quadratic fields were first studied by Gauss, before the language of algebraic number theory had been developed. He studied them in terms of binary quadratic forms, which we now take a look at.

Throughout this section, D will denote a *fundamental discriminant*, i.e., a number of one of the following forms:

(a) m, where m is squarefree and congruent to 1 mod 4;

(b) $4m$, where m is squarefree and congruent to 3 mod 4;

(c) $8m$, where m is squarefree and odd.

A *binary quadratic form* of discriminant D is an expression of the form $ax^2 + bxy + cy^2$ where $b^2 - 4ac = D$. Two binary quadratic forms $ax^2 + bxy + cy^2$ and $a'x^2 + b'xy + c'y^2$ are said to be *equivalent* if there exists an integer matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ of determinant 1 such that $a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2 = \pm(a'x^2 + b'xy + c'y^2)$.

1. Put $K = \mathbb{Q}(\sqrt{D})$. Show that the map
$$ax^2 + bxy + cy^2 \mapsto \mathbb{Z}a + \mathbb{Z}\frac{b + \sqrt{D}}{2}$$
of binary quadratic forms to ideals of $\mathfrak{o}_K$ induces a bijection between equivalence classes of forms and ideal classes of $\mathfrak{o}_K$.

2. Use the previous exercise to define a multiplication operation on equivalence classes of binary quadratic forms that translates into the multiplication of ideal classes.

3. Prove that every binary quadratic form is equivalent to a form $ax^2 + bxy + cy^2$ where $0 < a \leq |c|$ and $-a/2 < b \leq a/2$. Such a form is called *reduced.* Optional: show that we can choose the form so that there do not exist $x, y \in \mathbb{Z}$ such that $0 < |ax^2 + bxy + cy^2| < a$.

4. Suppose $ax^2 + bxy + cy^2$ is a reduced binary quadratic form of discriminant D. Prove that the corresponding ideal class has order 2 in the class group if and only if D is even and $b = 0$, or D is odd and $a = b$. (Hint: the inverse of the class corresponding to $ax^2 + bxy + cy^2$ corresponds to $ax^2 - bxy + cy^2$. You may also use the optional clause of the previous problem.)

5. (A theorem of Gauss) Prove that the largest power of 2 dividing the class number of $\mathbb{Q}(\sqrt{D})$ is 2^{n-1}, where n is the number of distinct prime factors of D.

6. Use Magma to find all the imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ for $D \leq 10^5$ with class number 2. (Hint: you won't have to write your own function to compute the class number.) In fact, the complete list of imaginary quadratic fields of a given class number is now provably known for class numbers up to about 24.

7. Use Magma to compute the class numbers of the real quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D \leq 10^5$, or more if you can. (Hint: see previous hint.) Look at how many of the fields with $D \leq N$ have class number 1, as a function of N, and make a conjecture about how this number depends on N for N sufficiently large. (This conjecture will be unsolved!)