Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lecture 10: Fun Facts about Class Numbers
September 19, 2001

Reference. Neukirch, Section 1.6.

Outline of lecture.

1. General warning: if $K \subset L$ are number field, there is a map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ induced by the map of ideal groups sending an integral ideal $\mathfrak{a}$ to $\mathfrak{a}\mathfrak{o}_L$. But the map on class group is not injective! E.g., $\mathbb{Q}(\sqrt{-5}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$, the former has class number 2, the latter has class number 1. See also the homework.

2. The class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ is bounded above by $O(\sqrt{D})$, and is bounded below by $O(D^{1/2-\epsilon})$—but the lower bound is not effective. (Siegel) The best effective known lower bound is $O((\log D)^{1-\epsilon})$ (Goldfeld).

3. The only imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ of class number 1 are for $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$. The complete list of class number N is known for some other small values of N, using Goldfeld's lower bound.

4. On the other hand, it is conjectured that there are infinitely many real quadratic fields $\mathbb{Q}(\sqrt{D})$ of class number 1. The upper bound $O(\sqrt{D})$ is thus much further from the truth in this case.

5. There are conjectures (Cohen-Lenstra) about the probability that the class number of a quadratic field (real or imaginary) is divisible by a prime p. For $p = 2$, this is understood by work of Gauss (see homework). For $p = 3$, this is basically understood by Davenport-Heilbronn. Beyond that, we know almost nothing.

6. For cyclotomic fields $\mathbb{Q}(\zeta_n)$, the class number grows with n, but is much harder to compute than in the cyclotomic case. However...

7. The prime p is called *regular* if p does not divide the class number of $\mathbb{Q}(\zeta_p)$. A theorem of Kummer states that p is regular if and only if p does not divide any of the numerators of the Bernoulli numbers $B_2, B_4, \dots, B_{p-3}$. (A more precise result is due to Herbrand and Ribet.)

8. Kummer proved Fermat's Last Theorem for regular primes. The basic idea is that if $y^p = z^p - x^p = (z-x)(z-\zeta x)\cdots(z-\zeta^{p-1}x)$, then each of the ideal classes $(z-x), (z-\zeta x), \dots, (z-\zeta^{p-1}x)$ is a p-th power in the class group. But if p is regular, then an ideal whose p-th power is principal is itself principal!

9. It is conjectured (Vandiver's conjecture) that the class number of the maximal real subfield of $\mathbb{Q}(\zeta_p)$ is *never* divisible by p.