Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 10: Cyclotomic Fields
Due in class *Wednesday*, November 14

Please submit nine of the following problems.

Leftover Problems about Ramification/Splitting.

1. Prove that $\mathbb{Q}(\sqrt{-5})$ has exactly one quadratic extension which is everywhere unramified, and find it. (This has something to do with class numbers; we'll get back to this next term.)

2. Let f be a monic polynomial over $\mathbb{Z}$ of degree greater than 1. Suppose that f has a root modulo p for all primes p. Prove that f cannot be irreducible. (Hint: if G is a finite group and H is a proper subgroup, the union of the conjugates of H cannot be all of G.)

Cyclotomic Fields.

1. Prove that the sign of the discriminant of the number field K with signature (r, s) equals $(-1)^s$. (You'll need this for the next problem.)

2. Calculate the discriminant of $\mathbb{Q}(\zeta_n)$ for n arbitrary. (Hint: choose an integral basis by multiplying together integral bases of $\mathbb{Q}(\zeta_{p^m})$ for each prime power p^m dividing n. Then reduce to the computation we did in class.)

3. Neukirch exercise I.10.1: Prove that for every natural number n, there are infinitely many primes congruent to 1 modulo n, without invoking Dirichlet's theorem on primes in arithmetic progressions. (Hint: let ϕ_n be the minimal polynomial of ζ_n. Prove that every prime divisor of $\phi_n(m)$, for $m \in \mathbb{Z}$, is congruent to 1 modulo n.)

4. Neukirch exercise I.10.2: Prove that for every finite abelian group A, there exists a Galois extension $L/\mathbb{Q}$ with Galois group A.

Interlude on Fermat's Last Theorem.

Throughout this section, let $p \geq 5$ be a regular prime, that is, a prime that does not divide the class number of $\mathbb{Q}(\zeta_p)$. Our goal is to prove part of Fermat's Last Theorem for the exponent p. Namely, if x, y, z are rational integers, none divisible by p, and p is regular as assumed above, we will prove that $x^p + y^p + z^p \neq 0$. As usual, we may assume x, y, z are pairwise coprime (if $x^p + y^p + z^p = 0$ and two of x, y, z have a common prime factor, so does the third).

1. Let x and y be relatively prime rational integers such that x, y and $x^p + y^p$ are not divisible by p. Prove that the ideals $(x + \zeta^i y)$ are pairwise coprime for $i = 0, \ldots, p-1$.

2. Suppose $x^p + y^p + z^p = 0$ and that p is regular. Prove that for $i = 0, \ldots, p-1$, there exists a unit ϵ_i and an integer $\alpha_i \in \mathbb{Z}[\zeta_p]$ such that $x + \zeta^i y = \epsilon_i \alpha_i^p$. (Hint: the assumption that p is regular means that the p-th power map is a bijection on the class group.)

3. Let $\lambda = 1 - \zeta$. Show that $\mathrm{Norm}(\lambda) = p$, so that every element of $\mathbb{Z}[\zeta_p]$ is congruent to a rational integer modulo λ. Then show that if $a \equiv b \pmod{\lambda}$ for $a, b \in \mathbb{Z}[\zeta_p]$, then $a^p \equiv b^p \pmod{p}$. (Hint: use the fact that as ideals, $(\lambda)^{p-1} = (p)$.)

4. Suppose $x + \zeta y = \epsilon \alpha^p$ for some unit ϵ and some integer α in $\mathbb{Z}[\zeta_p]$. Prove that there exists a rational integer g such that $x\zeta^g + y\zeta^{g+1} \equiv x\zeta^{-g} + y\zeta^{-g-1} \pmod{p}$. (Hint: write ϵ as a power of ζ times an element of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, i.e., a real number; we saw this on a previous homework. Also note that α^p is congruent to a rational integer modulo p.)

5. Assume the conditions of the previous problem, and also assume x and y are not divisible by p. Prove that if $x\zeta^g + y\zeta^{g+1} \equiv x\zeta^{-g} + y\zeta^{-g-1} \pmod{p}$ for some rational integer g, then $2g \equiv -1 \pmod{p}$. (Hint: first rule out the possibilities $g \equiv 0 \pmod{p}$ and $g \equiv -1 \pmod{p}$. Then use the fact that $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ form an integral basis to conclude that $g, g+1, -g, -g-1$ cannot be distinct modulo p.)

6. Suppose that $p \geq 5$ is regular and that $x^p + y^p + z^p = 0$ for pairwise coprime rational integers x, y, z, none divisible by p. Conclude from the above that $x \equiv y, y \equiv z, z \equiv x \pmod{p}$ and thus obtain a contradiction.