Algebraic Number Theory
MATH 512

Assignment 3

Throughout this assignment, you may use the following: Suppose L/K and F/K are extensions of number fields. If $\mathfrak{p}$ is a prime of K that is unramified (resp. split completely) in L/K, then $\mathfrak{P}$ is unramified (resp. split completely) in FL/F for any prime $\mathfrak{P}$ of F above $\mathfrak{p}$.

1. Let k be a positive, square-free integer that is not congruent to 3 mod 4, and let p be a prime not dividing $2k$. Let $L = \mathbb{Q}(\sqrt{-k})$ and let M/L be an abelian extension such that the primes of L that split completely in M are exactly the primes of L that are principal. (Such an M exists and is unique – it is called the Hilbert class field of L.) Show that the following are equivalent:
(i) There exist $x, y \in \mathbb{Z}$ such that $x^2 + ky^2 = p$.
(ii) p splits completely in M.

2. Let $L = \mathbb{Q}(\sqrt{-6})$. Show that every prime of L is unramified in $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.

3. Let L be as in question 2.
(a) Compute the order of the class-group of L.
(b) Using the fact that the field M of question 1 satisfies $\mathrm{Gal}(M/L) \simeq \mathrm{Cl}(L)$, and also that M is the maximal abelian extension of L in which all primes of L are unramified, deduce that $M = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.
(c) Show that if p is any rational prime, then the equation $x^2 + 6y^2 = p$ has an integral solution $(x, y) \in \mathbb{Z}^2$ if and only if $p \equiv 1$ mod 24 or $p \equiv 7$ mod 24.

4. Let p be an odd prime. By considering the decomposition of p in the field $L = \mathbb{Q}(\zeta_8)$ **(and using no other method)**, prove that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

5. In the proof of Lemma 43, we claimed the existence of a positive integer l admitting integers i, j with $1 \le i < j \le l$ for which $\gamma_i \gamma_j^{-1}$ is a unit. Show that one may take

$$l = 1 + \sum_{k=1}^{\llbracket (3b)^n \rrbracket} k^n,$$

where b and n are as in the proof of the lemma, and for a real number x, $\llbracket x \rrbracket$ is the greatest integer strictly less then x.

Remark on 3(b): In general, the Hilbert class field of a number field L is actually the maximal abelian extension of L in which all prime ideals are unramified and all so-called "infinite primes" (which we have not discussed) split completely. This second condition is automatically satisfied for extensions of the field L of question 3.