Problem set 9 – Math 699 – Algebraic number theory

(1) For $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$, show that $\mathbf{Q}(\sqrt{d})$ has class number 1. (These are the only 9 imaginary quadratic fields of class number 1. More generally, a *CM field* is a totally imaginary quadratic extension of a totally real field, and Stark has conjectured that there are only finitely many CM fields of class number 1.)

(2) For $m = 3, 4, 5, 7, 8, 9, 12$, show that $\mathbf{Q}(\zeta_m)$ has class number 1. (If $m \equiv 2 \pmod 4$, then $\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{m/2})$, so this list of m's is all cyclotomic fields with $m \leq 12$, except 11. This latter one has Minkowski constant $58.96\ldots$, and so would be a bit more work, though it's not so much work to show that you'd only have to check the 10 primes above 23.)

(3) Determine the class group of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$. (Question (4c) of Problem Set 8 will help.)

(4) (Murty–Esmonde, Exercise 6.5.24) In this exercise, you'll construct a family of imaginary quadratic fields whose class number goes to infinity. (In his *Disquisitiones Arithmeticae*, Gauss conjectured that as the discriminant of an imaginary quadratic field goes to (minus) infinity, so does its class number. This was proved by Heilbronn in 1934. Gauss also conjectured that there are infinitely many real quadratic fields of class number 1. This remains open (bonus points for solving!).)

   (a) Let $\ell \equiv 11 \pmod{12}$ be prime. Show that $p = 3$ splits in $K = \mathbf{Q}(\sqrt{-\ell})$.

   (b) Show that if $\ell > 3^n$ and $\alpha \in \mathcal{O}_K$ has norm 3^m with $m < n$, then m is even.

   (c) Suppose $\ell > 3^n$ and let $\mathfrak{p}$ be one of the primes above 3 in $\mathbf{Q}(\sqrt{-\ell})$. Show that $\mathfrak{p}^m$ can't be principal for $m < n$. Conclude that $[\mathfrak{p}] \in C\ell(K)$ has order at least n. (In the next exercise, you'll prove that there are infinitely many primes $\ell \equiv 11 \pmod{12}$.)

(5) (Murty, *Primes in certain arithmetic progressions*) Dirichlet's theorem on primes in arithmetic progression states that, for any $a, m \in \mathbf{Z}_{\geq 1}$ with $\gcd(a, m) = 1$, there are infinitely many primes $\ell \equiv a \pmod m$. Dirichlet introduced the L-functions of Dirichlet characters and generalized Euler's proof of the infinitude of primes to prove this theorem. For certain pairs (a, m), there is a more elementary proof along the lines of Euclid's proof of the infinitude of primes, such a proof is called 'Euclidean'. In part (a), you'll go through this proof for the pair $(1, 4)$ which is a standard result proved in an elementary number theory course. Then, you'll do it for $(11, 12)$. Ram

Murty's paper shows that there is a "Euclidean" proof for (a, m) if and only if $a^2 \equiv 1 \pmod{m}$.

(a) Suppose that $S = \{p_1, \ldots, p_k\}$ is a set of primes that are 1 (mod 4). Consider $N = 4(p_1 \cdots p_k)^2 + 1$. Show that if $p|N$, then $p \notin S$ and -1 is a square modulo p, and hence that p is another prime that is 1 (mod 4).

(b) Go to Ram Murty's website (`http://www.mast.queensu.ca/~murty/index2.html`) and download his paper. Extract from it the polynomial required for the pair $(11, 12)$, and maybe go through the proof that there are infinitely many primes $\equiv 11 \pmod{12}$.