ALGEBRAIC NUMBER THEORY

PRACTICE PROBLEMS

We will start with problems related to the presentation of primes by binary quadratic forms.

(1) Show that every prime $p \equiv 1 \bmod 4$ is the sum of two squares.
(2) Show that every prime $p \equiv 1, 3 \bmod 8$ has the form $p = c^2 + 2d^2$.
(3) Show that if $p \equiv 1, 2, 4 \bmod 7$, then $4p = x^2 + 7y^2$.
(4) Show that primes $p \equiv \pm 1 \bmod 5$ can be written in the form $p = x^2 + 5y^2$.
(5) Show that primes $p \equiv \pm 1 \bmod 12$ can be written in the form $\pm p = a^2 - 3b^2$. Show that the $+$ sign holds if and only if $p \equiv 1 \bmod 12$.
(6) Let p, q be a primes, and assume that $q \equiv 1 \bmod 4$ and that $(\frac{-q}{p}) = 1$. Show that $p^h = x^2 + qy^2$, where h denotes the class number of $K = \mathbb{Q}(\sqrt{-q}\,)$. Show that $p^{h/2} = c^2 + qd^2$ if $p \equiv 1 \bmod 4$, and $2p^{h/2} = c^2 + qd^2$ if $p \equiv 3 \bmod 4$.

The first few problems boil down to showing that certain rings of integers have class number 1, hence are principal ideal domains. The fourth problem is more demanding: class number 1 only gives you $\pm 4p = x^2 + 5y^2$; now you have to invoke units. In the fifth problem, you will have to invoke congruences modulo 4 or modulo 3. The last problem is more demanding. The equation $2p^{h/2} = c^2 + qd^2$ suggests you should look at the prime ideal $(2, 1 + \sqrt{-q}\,)$ and its ideal class.

A second class of problems consists of computations of the class group for a given field. One of the problems is showing that certain classes are not trivial, i.e., that certain ideals are not principal. If K is complex, this is in general easy; for real quadratic fields, you have to use congruences or, in cases such as $\mathbb{Q}(\sqrt{79}\,)$, unit estimates.

Finally, there are problems related to class number divisibility.

(1) Show that $\mathbb{Q}(\sqrt{-m}\,)$, where $m \equiv 1 \bmod 4$, has odd class number if and only if $m = 1$.
(2) Show that $\mathbb{Q}(\sqrt{2p}\,)$ has even class number if $p \equiv 1 \bmod 4$.
(3) Show that $\mathbb{Q}(\sqrt{pq}\,)$ has even class number if $p \equiv q \equiv 1 \bmod 4$.

The first problem should be easy. The second problem is just as easy if $p \equiv 5 \bmod 8$; if $p \equiv 1 \bmod 8$, write $2p = e^2 + f^2$ for odd integers e, f, and consider the ideal $(e + \sqrt{2p}\,)$.