MATH 154. HOMEWORK 9

0. Read the handout on using norms to get relations in the class group. See H. Cohen's book *A Course in Computational Algebraic Number Theory* for much more on computing class groups, unit groups, etc.

1. (*i*) Prove that $K = \mathbf{Q}(\sqrt{-30})$ has Minkowski constant < 7, and class group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ by considering primes over 2, 3, 5. (Hint: show $(\sqrt{-30}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ for prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_5$ over 2, 3, and 5 respectively.)

(*ii*) Prove $\mathbf{Q}(\sqrt{-51})$ has class number 2 (used in a handout to show $y^2 = x^3 - 51$ has no $\mathbf{Z}$-solutions, a subtle fact since we saw that there are $\mathbf{Q}$-solutions, and even a solution in $\mathbf{Z}/m\mathbf{Z}$ for every $m > 0$.)

2. Let $K = \mathbf{Q}(\sqrt{79})$, so $\mathscr{O}_K = \mathbf{Z}[\sqrt{79}]$. Prove $h_K = 3$ as follows.

(*i*) Show that K has Minkowski constant less than 9, and by factoring (2), (3), (5), and (7), and computing $\mathrm{N}_{K/\mathbf{Q}}(a + \sqrt{79})$ for $a = 8, 9, 10$ show that $\mathrm{Cl}(K)$ is generated by the class either of the two primes over 3. Then use $a = 5$ to show that each prime over 3 has cube that is principal.

(*ii*) It remains to show primes over 3 are not principal. Assuming to the contrary, deduce $-17+2\sqrt{79} = u\alpha^3$ for some $u \in \mathscr{O}_K^\times$ and $\alpha = a + b\sqrt{79}$ with $a, b \in \mathbf{Z}$ such that $a^2 - 79b^2 = \pm 3$. (Hint: for $x = -17 + 2\sqrt{79}$ we have $x\overline{x} = -3^3$ and $3 \nmid x$ in $\mathscr{O}_K$.) Let $\varepsilon = 80 + 9\sqrt{79}$; you may accept that this is a fundamental unit (i.e., it generates $\mathscr{O}_K^\times$ up to a sign). Deduce that for a suitable choice of α we have $\alpha^3 = (-17 + 2\sqrt{79})\varepsilon^i$ for some $i \in \{0, 1, 2\}$. By expanding $(a + b\sqrt{79})^3$, get a contradiction for each i. (Be careful for $i = 2$.)

3. Prove $\mathbf{Q}(\sqrt{-210})$ has class group $(\mathbf{Z}/2\mathbf{Z})^3$ (generated by the unique primes over any three of 2, 3, 5, 7).

4. Let $K = \mathbf{Q}(\sqrt{10})$, so $\mathscr{O}_K = \mathbf{Z}[\sqrt{10}]$.

(*i*) Prove that the ideals $(4+\sqrt{10})$ and $(4-\sqrt{10})$ in $\mathscr{O}_K$ are distinct, and by studying the (non-principal!) prime factorizations of 2 and 3 in $\mathscr{O}_K$ show that these are the only two ideals with norm 6.

(*ii*) Let $\varepsilon = 3 + \sqrt{10}$; this is a fundamental unit. (Beware that $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = -1$.) Prove that solutions to $x^2 - 10y^2 = 6$ in $\mathbf{Z}^+$ are precisely the pairs of integers (x, y) such that $x + y\sqrt{10}$ is equal to $(4 + \sqrt{10})\varepsilon^{2n}$ with $n \geq 0$ or $(4 - \sqrt{10})\varepsilon^{2n}$ with $n > 0$. (In other words, for other n such numbers have the form $a + b\sqrt{10}$ with $a \leq 0$ or $b \leq 0$, whereas all numbers of the indicated types have the form $a+b\sqrt{10}$ with $a, b > 0$.) Using this, give (with rigorous yet non-tedious justification) the solutions with three smallest values for $y \in \mathbf{Z}^+$.

5. Consider the equations $x^2 - 82y^2 = \pm 2$. Prove as follows that these have no solutions in $\mathbf{Z}$. (This *cannot* be proved by congruential methods, because there are solutions in $\mathbf{Q}$, such as $(10/3, 1/3)$, and even in $\mathbf{Z}/m\mathbf{Z}$ for all $m > 0$.)

(*i*) Let $K = \mathbf{Q}(\sqrt{82})$, so $\mathscr{O}_K = \mathbf{Z}[\sqrt{82}]$ has fundamental unit $\varepsilon = 9 + \sqrt{82}$. (Note that $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = -1$.) Check that $(2) = \mathfrak{p}_2^2$ for a prime $\mathfrak{p}_2 = (2, \sqrt{82})$, and prove that it is equivalent to show $\mathfrak{p}_2$ is not principal.

(*ii*) If $\mathfrak{p}_2 = (\alpha)$, show that $\alpha^2 = 2u$ for some $u \in \mathscr{O}_K^\times$. Prove that $\mathrm{N}_{K/\mathbf{Q}}(u) = 1$ (i.e., not -1), and deduce $u = \pm\varepsilon^{2n}$ for some $n \in \mathbf{Z}$ to conclude that one of ± 2 is a square in K, yielding from that a contradiction.

What's next? The next topic to learn about (via reading) is p-adic numbers. Begin with Chapters 1 and 3 of Koblitz' book *p-adic Numbers, p-adic Analysis, and Zeta Functions* (do some exercises therein!) and then various books called *Algebraic Number Theory* according to your taste: Chapters 7-8 in the notes on the website of Milne at the University of Michigan, Chapter II in the ("geometric") book by Neukirch, Chapters II-III in the book by Lang, and/or Chapter I and parts of Chapter II in the book (edited) by Cassels-Fröhlich. The book *Local Fields* by Serre gives a systematic albeit theoretical treatment in Chapters I–IV (skipping §4-§6 in Chapter II on a first reading) with good exercises. Then on to class field theory!

Supplementing this, one should learn more commutative algebra (especially tensor products and localization) in Math 210A and 210B and more comprehensively in the book *Introduction to Commutative Algebra* by Atiyah & MacDonald (with excellent exercises), and some ideas in algebraic geometry over an algebraically closed field as in Math 145 and 210B or Chapters 1-6 in the book *Algebraic Curves* by Fulton (with excellent exercises, and freely available on his Michigan website). After that, one can learn about elliptic curves from Silverman's *The Arithmetic of Elliptic Curves* to see how algebraic geometry, p-adic fields, and algebraic number theory merge to explore the rich structure of points on smooth plane curves of degree 3 (itself a test case for higher-degree curves and higher-dimensional "algebraic varieties"). Then on to schemes!