Algebraic Number Theory 88-798
Question Sheet 3
Due Dec. 23, 2008

Please feel free to e-mail me at `mschein@math.biu.ac.il` with any questions of translation or otherwise.

(1) Let K be a number field and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathcal{O}_K$. Recall that we say that $\mathfrak{a}$ divides $\mathfrak{b}$, denoted $\mathfrak{a}|\mathfrak{b}$, if there is an ideal $\mathfrak{c}$ of $\mathcal{O}_K$ such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. Prove that $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

(2) Let $K = \mathbb{Q}(\sqrt{65})$. Determine the class number h_K by the following steps. (For this particular field there is a simpler way of finding the class number, but the point of the exercise is to illustrate a method that works for more complicated number fields.) Define the set

$$S = \{x \in \mathcal{O}_K : N_{K/\mathbb{Q}}(x) = \pm 2\}.$$

(a) Write down a unit $u \in \mathcal{O}_K^*$ such that u is not a root of unity. Show that multiplication by u and u^{-1} preserves S.

(b) Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$ be the two embeddings of K into $\mathbb{R}$, and consider the map

$$\begin{aligned} \lambda : \mathcal{O}_K \backslash \{0\} &\to \mathbb{R} \times \mathbb{R} \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|) \end{aligned}$$

as in class. Consider the action of u and u^{-1} on S by multiplication and write down a number $c > 0$ such that if $S \neq \varnothing$, then there exists $x \in S$ with

$$\lambda(x) \in \{(z_1, z_2) \in \mathbb{R} \times \mathbb{R} : |z_1| < c, |z_2| < c\}.$$

(c) Now find an integer $N \in \mathbb{Z}$ such that if $x = a + b\sqrt{65} \in S$ is the element found in the previous section, then $|a| < N$ and $|b| < N$.

(d) Since $a, b \in \frac{1}{2}\mathbb{Z}$, there are only finitely many possibilities for x. It is easy to program a computer to check all of them and see that none of them has norm ± 2. Therefore $S = \varnothing$. Using this, prove that $h_K = 2$.
Hint: Prove that $3\mathcal{O}_K$ is prime and that $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$.

(3) Let $d > 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$.

(a) If $D = d_K$, then show that $x, y \in Z$ are solutions of Pell's equation $x^2 - Dy^2 = \pm 4$ if and only if $\frac{1}{2}(x + y\sqrt{D}) \in \mathcal{O}_K^*$.

(b) Say that a solution (x, y) of Pell's equation is positive if $x \geq 0$ and $y \geq 0$. Show that there exists a positive solution (x, y) that is minimal in the sense that if (x', y') is any other positive solution, then $x' \geq x$ and $y' \geq y$. If (x, y) is this minimal positive solution, then show that

$$u = \frac{1}{2}(x + y\sqrt{D})$$

is a fundamental unit of K. (In other words, $\mathcal{O}_K^* = \{\pm u^k : k \in \mathbb{Z}\}$.)

(c) Now we will see an application of number theory to history. Read the following text from an ancient manuscript about the Battle of Hastings, which took place in 1066 between William the Conqueror and his Normans, who had just invaded England, and the Saxons led by King Harold II. Determine how many men were in the Saxon army.

"The men of Harold stood well together, as was their wont, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon warhatchet would break his lance and cut through his coat of mail. When Harold threw himself into the fray the Saxons were one mighty square of men shouting the battle cries 'Ut!,' 'Olicrosse!' and 'Godemite!' "

In other words, find the minimal $N > 1$ such that $N = x^2 = 13y^2 + 1$ for $x, y \in \mathbb{Z}$.

Note: This problem appeared in H.E. Dudeney's *Mathematical Amusements* in 1917. Its solution is larger by an order of magnitude than the actual number of participants in the Battle of Hastings. Please direct all complaints about this to Dudeney and not to me.