Algebraic Number Theory (88-798)
5777 Semester B
Question Sheet 3
Due 17/5/2017, כ״א באייר תשע״ז

(1) Find the class number of the field $\mathbb{Q}(\sqrt{6})$.

(2) Let p be a prime number such that $p \equiv 2 \bmod 3$, and let $K = \mathbb{Q}(\sqrt{-p})$. Suppose that $p > 3^m$. Prove that $h_K > m$.

Hint: Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal dividing $3\mathcal{O}_K$. Consider its class in Cl_K.

(3) Let $K = \mathbb{Q}(\sqrt{65})$. The purpose of this and the three following exercises is to determine the class number h_K, illustrating a technique that can be used quite generally. Define the set

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

Find a unit $u \in \mathcal{O}_K^*$ that is not a root of unity and show that multiplication by u and u^{-1} preserves S.

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

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

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

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

(5) Find an integer N such that if $x = a + b\sqrt{65} \in S$ is the element found in the previous exercise, then $|a| < N$ and $|b| < N$.

Since $x \in \mathcal{O}_K$ and therefore $a, b \in \frac{1}{2}\mathbb{Z}$, there are only finitely many elements $x = a + b\sqrt{65} \in \mathcal{O}_K$ satisfying the condition that $|a|, |b| < N$. Write a simple computer program to check that none of these elements have norm ± 2. (If you don't know how to program, don't bother.) Conclude that $S = \varnothing$.

(6) Use the fact that $S = \varnothing$ to prove that $h_K = 2$.

Hint: It may be helpful to prove that $3\mathcal{O}_K$ is prime and that $2\mathcal{O}_K$ decomposes into a product of two distinct prime ideals.

(7) Prove that 26 is the only natural number that is the successor of a perfect square and the predecessor of a perfect cube.

(8) Let $d > 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$. 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 $\frac{1}{2}(x + y\sqrt{D}) \in \mathcal{O}_K^*$.

(9) 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 $K = \mathbb{Q}(\sqrt{d})$. (In other words, $\mathcal{O}_K^* = \{\pm u^k : k \in \mathbb{Z}\}$.)

(10) 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 war hatchet would break his lance and cut through his coat of mail. After Harold joined his men and threw himself into the fray the Saxons were one mighty square of men shouting the battle cries 'Ut!' 'Olicrosse!' and 'Godemite!' "

Note: This problem appeared in H.E. Dudeney's *Mathematical Amusements* in 1917. Its solution is not historically accurate.

(11) Let A be a Dedekind domain and K its field of fractions. Let L/K be a finite separable extension of fields, and let B be the integral closure of A in L. Prove that B is a Dedekind domain.

Hint: Generalize the proof we gave in class that $\mathcal{O}_K$ is a Dedekind domain when K is a number field. The incomparability theorem from commutative algebra is useful here.