Problem Sheet 6

Problem 1

Let $K/\mathbb{Q}$ be a quadratic extension of discriminant D. For $\mathfrak{a} \subseteq K$ a fractional ideal, set

$$Q_{\mathfrak{a}} : \mathfrak{a} \longrightarrow \mathbb{Z},\ a \longmapsto \frac{N_{K/\mathbb{Q}}(a)}{N_{K/\mathbb{Q}}(\mathfrak{a})}.$$

(a) Show that $Q_{\mathfrak{a}}(a) = n$ has a solution if and only if there is an ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ in the ideal class of $\mathfrak{a}^{-1}$ such that $N_{K/\mathbb{Q}}(\mathfrak{b}) = n$.

(b) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be representatives for the elements of the class group Cl_K. Prove that, for $p \nmid D$,

$$p \text{ split in } K \quad \Leftrightarrow \quad \exists i, a \in \mathfrak{a}_i \ \text{ s.th. } \ Q_{\mathfrak{a}_i}(a) = p.$$

(c) Conclude that, for $p \neq 2, 5$,

$$\begin{cases} X^2 + 5Y^2 = p & \text{has a solution } \Leftrightarrow \ p \equiv 1, 9 \mod 20 \\ 2X^2 + 2XY + 3Y^2 = p & \text{has a solution } \Leftrightarrow \ p \equiv 3, 7 \mod 20. \end{cases}$$

Problem 2

Find the class number $h_{\mathbb{Q}(\sqrt{m})}$ for $m = 5, 6, -7, -13$ and -23.

Problem 3

Let $K = \mathbb{Q}(\sqrt[3]{m})$ with m square-free and $m \not\equiv \pm 1 \mod 9$.

(a) Show that $\mathbb{Z}[\sqrt[3]{m}]$ is the ring of integers in K.

(b) Compute the class number of K for $m = 3, 5$.

Problem 4

Let $K_1, K_2/\mathbb{Q}$ be quadratic fields with discriminants $D_1 \neq D_2$. Describe (with proof) the decomposition behavior of primes in the composite field $K := K_1 K_2$ in terms of D_1 and D_2.

Hint: You may freely use that every quadratic extension of $\mathbb{Q}$ embeds into a cyclotomic extension. This is especially useful for the study of the decomposition behavior of $p = 2$.