HW 2: Elliptische Kurven II

- Hand in by November 22nd.

Exercise 1. Let $n \geq 1$, let $s \geq 1$, and let $p_1, \ldots, p_s$ be prime numbers. Show (without appealing to Hermite's theorem) that the set of equivalence classes of irreducible polynomials $f(x) = x^n - a$ with $a \in \mathbb{Z}$ with good reduction outside $\{p_1, \ldots, p_s\}$ is finite.

Exercise 2. Let d be a squarefree integer with $d \neq 0, 1$. Let $K = \mathbb{Q}(\sqrt{d})$ with ring of integers O_K.

1. Compute O_K^* for all negative d. Conclude that O_K^* is finite.
2. Show O_K^* is infinite for $d = 5$.
3. Let $p \nmid 2d$ be a prime number. Show that (p) is a prime ideal if and only if

$$\left(\frac{d}{p}\right) = -1.$$

Exercise 3. Prove or disprove.

1. If K is a field, then the polynomial ring $K[x, y]$ in two variables is a Dedekind domain.
2. If K is a number field and $\mathfrak{a}$ is an ideal of O_K such that $N(\mathfrak{a})$ is a prime number, then $\mathfrak{a}$ is a prime ideal.
3. If $K = \mathbb{Q}(\sqrt{-5})$ and $\mathfrak{p}$ is the ideal $(2, 1 + \sqrt{-5})$ in O_K, then $\mathfrak{p}$ is a prime ideal, $\mathfrak{p}$ is not a principal ideal, and $\mathfrak{p}^2$ is a principal ideal.
4. Let K be a quadratic field extension of $\mathbb{Q}$. Let $x \in K$. Then x is integral over $\mathbb{Q}$ if and only if $N_{K/\mathbb{Q}}(x)$ and $Tr_{K/\mathbb{Q}}(x)$ are integers.

Exercise 4. Compute the class number of $\mathbb{Q}(\sqrt{-5})$.

Exercise 5. Let $d \geq 1$ be a squarefree integer such that $d \equiv 3 \mod 4$. Show that the Pell equation $x^2 - dy^2 = 1$ has infinitely many solutions with $x, y \in \mathbb{Z}$.

Exercise 6. Show that $1 + \sqrt{2}$ is a fundamental unit in $\mathbb{Q}(\sqrt{2})$.