Exercise Sheet 4
Algebraic Number Theory

October 8, 2025

Exercise 1 (Quadratic reciprocity, again)**.** Recall that the quadratic reciprocity law says that for all distinct *odd prime* numbers p, q it holds that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. In this exercise we give a second proof of this result, which historically is the sixth published proof by Gauss. Define

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} (\frac{a}{p}) e^{\frac{2\pi a i}{p}}.$$

1. Prove that for all $a.b \in \mathbb{Z}$ with $(ab, p) = 1$ one has
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
2. Prove that
$$\tau^2 = (-1)^{\frac{p-1}{2}} p.$$
Hint: Recall from Exercise Sheet 3 the Euler criterion. **Remark** By Galois theory, $\mathbb{Q}[\tau] \subseteq \mathbb{Q}[e^{\frac{2\pi i}{p}}]$ is the unique quadratic extension (of $\mathbb{Q}$) in $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$. That was the historical motivation for considering the quadratic Gauss sum.
3. Prove that the ideals generated by q and τ are coprime in $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$.
4. Prove that
$$\tau^{q-1} \equiv \left(\frac{q}{p}\right) \mod q.$$
5. Conclude

Exercise 2. Consider the Diophantine equation

$$Y^2 = X^3 - 2. \tag{1}$$

We are interested in integer solutions of this equation.

1. Show that $\mathbb{Z}[\sqrt{-2}]$ is an euclidean domain, hence a PID.
2. Use the above information to find all integer solutions of (1).