Elementary Number Theory - Exercise 6a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Determine the quadratic residues modulo 11.

Problem 2. Let p be an odd prime. Show that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Problem 3. Let p be an odd prime and $\gcd(p, ab) = 1$. Show that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Problem 4. Compute the following Legendre symbols.

$$\left(\frac{14}{11}\right); \quad \left(\frac{2}{5}\right); \quad \left(\frac{256}{17}\right); \quad \left(\frac{18}{19}\right); \quad \left(\frac{10}{1009}\right).$$

Problem 5. Let p be an odd prime and $\gcd(a, p) = 1$. Show that

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

where a^{-1} denotes the inverse of a modulo p.

Problem 6. Let p be an odd prime. For $n \in \mathbb{Z}$ we define the *Gauss sum*

$$G_p(n) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) e^{2\pi i a n/p},$$

where the sum runs over an arbitrary system of representatives for $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Check that the sum is well-defined, that is, independent of the chosen system of representatives for $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Show that

$$G_p(n) = \begin{cases} \left(\frac{n}{p}\right) G_p(1), & \text{if } p \nmid n, \\ 0, & \text{if } p \mid n. \end{cases}$$

3. Show that

$$G_p(1)^2 = \left(\frac{-1}{p}\right) p.$$

Deduce that $G_p(1) = \pm\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $G_p(1) = \pm i\sqrt{p}$ if $p \equiv 3 \pmod 4$.
Hint: The sum $\sum_{a=0}^{p-1} e^{2\pi i n a/p}$ vanishes unless $p \mid n$.

Problem 7 (sage)**.** 1. Write a program that computes the Legendre symbol $\left(\frac{a}{p}\right)$ by "brute force", that is, by checking if $x^2 \equiv a \pmod p$ has a solution. We will see a more efficient method in the next lecture.

2. We have seen above that $G_p(1) = \pm\sqrt{p}$ or $G_p(1) = \pm i\sqrt{p}$, depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Compute the Gauss sum $G_p(1)$ for several values of p and come up with a conjecture what the sign should be (the correct sign was determined by Gauss).