Elementary Number Theory - Exercise 6b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Use Gauss' Lemma to show that the quadratic congruence $x^2 \equiv 3 \pmod{31}$ has no solutions.

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8, \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Hint: Gauss' Lemma.

Problem 3. Let $p > 7$ be a prime.

1. Determine $\left(\frac{5}{p}\right)$ in terms of the class of p modulo 5.
2. Determine $\left(\frac{7}{p}\right)$ in terms of the class of p modulo 28.

Hint: Use quadratic reciprocity.

Problem 4. Compute $\left(\frac{83}{137}\right)$ using the Jacobi symbol (without completely factoring the numerator).

Problem 5.

1. Show that a prime $p > 3$ is either 1 or -1 modulo 6.
2. Let $p > 3$ be a prime. Prove that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 6, \\ -1, & p \equiv -1 \pmod 6. \end{cases}$$

3. Show that there are infinitely many primes $p \equiv 1 \pmod 6$.
   Hint: Consider $m = 12(p_1 \cdots p_k)^2 + 1$, where $p_1, \dots, p_k$ are the primes $\equiv 1 \pmod 6$.

Problem 6. Let $p \neq q$ be odd primes, and put $p^* = \left(\frac{-1}{p}\right) p$. Show that the quadratic reciprocity law can equivalently be written as

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Problem 7 (sage)**.** Write a program that computes the Jacobi symbol, using the method from the lecture (that is, without factoring the numerator).