Algebraic Number Theory

Exercises Tutorium 1

Dr. Tom Bachmann — Winter Semester 2021–22

Exercise 1. Determine the quadratic residues and non-residues modulo 3, 5, 7, 11.

Exercise 2. Prove that there are an equal number of quadratic residues and non-residues modulo any (odd) prime. Deduce that the Legendre symbol $\left(\frac{d}{p}\right)$ is a multiplicative function of d.

Exercise 3. Prove that the finite abelian group $\mathbb{F}_p^\times$ is cyclic. Deduce that:

(1) The Legendre symbol is multiplicative.
(2) $\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod{p}$.
(3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

The quadratic reciprocity law states that for odd primes p, q one has

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

and one also knows that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Exercise 4. Determine $\left(\frac{23}{59}\right)$, $\left(\frac{10}{1009}\right)$, $\left(\frac{261}{2017}\right)$ and $\left(\frac{-77}{9967}\right)$. [You may use that the "denominators" are all prime.]

Exercise 5. Let $p > 3$. Prove that -3 is a square mod p if and only if $p \equiv 1(6)$.