1. **Homework, week 1, due September 12**

1. Compute the Legendre symbols

\[
\left(\frac{17}{31}\right), \left(\frac{31}{17}\right), \left(\frac{23}{191}\right), \left(\frac{191}{23}\right).
\]

Show that they verify quadratic reciprocity.

2. Write the polynomial

\[P(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\]

in \(\mathbb{F}_{11}[X]\) as a product of irreducible factors. Same problem with \(P(X) \in \mathbb{F}_3[X]\). (Hint: use Galois theory.)

3. A **quadratic field** is an extension of \(\mathbb{Q}\) of degree 2. Let \(d \in \mathbb{Z}\) and assume \(d\) is not a square in \(\mathbb{Q}\). Let \(\sqrt{d} \in \mathbb{C}\) be a square root of \(d\), and define \(\mathbb{Q}(\sqrt{d})\) to be the subfield of \(\mathbb{C}\) consisting of elements of the form \(a + b\sqrt{d} \mid a, b \in \mathbb{Q}\) (you may want to verify that \(\mathbb{Q}(\sqrt{d})\) is a field if you haven’t seen this previously).

   (a) Prove that \(\mathbb{Q}(\sqrt{d})\) is a quadratic field. Show that every quadratic field is of the form \(\mathbb{Q}(\sqrt{d})\) for some integer \(d\). Show that \(\mathbb{Q}(\sqrt{d})\) is a Galois extension of \(\mathbb{Q}\) and determine its Galois group, indicating the action of non-trivial elements of \(\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})\) on the typical element \(a + b\sqrt{d}\).

   (b) Let \(d\) and \(d'\) be two integers that are not squares in \(\mathbb{Q}\). Show that \(\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})\) if and only if \(d/d'\) is a square in \(\mathbb{Q}\). Use this result to give a complete (infinite) list of all quadratic fields.

   (c) Let \(P(x) = ax^2 + bx + c \in \mathbb{Z}[x]\), with \(a \neq 0\), and assume \(P\) is irreducible in \(\mathbb{Q}[x]\). Let \(\Delta = b^2 - 4ac\) be the discriminant of \(P\). Show that \(\mathbb{Q}(\sqrt{\Delta})\) is a splitting field for \(P\). What are the possible values of \(\Delta\) modulo 4?

   (d) Conversely, let \(d \in \mathbb{Z}\) be a square-free integer (in other words, if \(p\) is a prime dividing \(d\) then \(p^2\) does not divide \(d\)). Find a monic polynomial \(Q \in \mathbb{Z}[x]\) with splitting field \(\mathbb{Q}(\sqrt{d})\). If \(d \equiv 1 \pmod{4}\) show that \(Q\) can be taken to have discriminant \(d\); if \(d \equiv 2 \pmod{4}\) or \(d \equiv 3 \pmod{4}\) show that \(Q\) can be taken to have discriminant \(4d\).

4. For any positive integer \(n\), the Euler function \(\phi(n)\) is the number of positive integers less than or equal to \(n\) that are relatively prime to \(n\). (So \(\phi(1) = 1, \phi(2) = 1, \phi(3) = 2\), etc.)
(a) Show that for any positive integer $n$,
\[ n = \sum_{d|n} \phi(d). \]

(b) Let $A$ be an abelian group with $n$ elements. Suppose that for every $d \mid n$ the number of elements of $A$ of order $d$ is at most $d$. Show that $A$ is cyclic.

(c) Let $p$ be a prime and let $k$ be a field of characteristic $p$. Let $n$ be a positive integer prime to $p$. Show that the polynomial $X^n - 1$ in $k[X]$ has no multiple roots.

(c) Let $p$ be a prime, and let $k$ be a finite field of characteristic $p$. Show that the multiplicative group $k^\times$ of $k$ is a cyclic group.