Directions: Solve the following problems. See the course syllabus and the Homework Webpage on the course website for general directions and guidelines.

1. [6.15] Show that $\left|\sum_{a=m}^{n}\left(\frac{a}{p}\right)\right| < \sqrt{p}(1+\ln p)$. [Hint: use the relation $\left(\frac{a}{p}\right) g = g_a$ and sum. The inequalities $\sin x \geq \frac{2}{\pi}x$ for any acute angle x and $H_n \leq 1 + \ln n$, where $H_n = 1 + 1/2 + 1/3 + \cdots + 1/n$, will be useful.]

2. [7.1] Use the method of Möbius inversion to show that a finite subgroup of the multiplicative group of a field is cyclic.

3. [7.16] Calculate the monic irreducibles of degree 4 in $\mathbb{Z}/2\mathbb{Z}$.

4. Let K and F be finite fields with $[K : F] = n$. Prove that if γ is a generator of K^*, then γ has degree n over F.

5. Let K be an extension of $\mathbb{Z}/3\mathbb{Z}$ of degree 12, and let a_n be the number of elements $\alpha \in K^*$ such that α has degree n over $\mathbb{Z}/3\mathbb{Z}$. Determine the sequence $(a_1, a_2, \ldots, a_{12})$ explicitly. Of the elements having degree 12, how many are generators?

6. [7.{3,4,5}] Let F be a field with q elements and suppose that $q \equiv 1 \pmod{n}$.

   (a) Show that for $\alpha \in F^*$, the equation $x^n = \alpha$ has either no solutions or n solutions.

   (b) Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.

   (c) Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$, show that the equation $x^n = \alpha$ has n solutions in K. Hint: show that $n(q-1) \mid q^n - 1$ and use the fact that $\alpha^{q-1} = 1$.

7. [7.{8,6,7}] Squares in fields.

   (a) In a field with 2^n elements, what is the subgroup of squares?

   (b) Let $K \supset F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F, then it is also not a square in K.

   (c) Generalize part (b) by showing that if α is not a square in F, then it is not a square in each extension of odd degree and it is a square in each extension of even degree.

8. [7.{12,15}] Extensions and linear factors.

   (a) Use Proposition 7.2.1 to show that given a field k and a polynomial $f(x) \in k[x]$ there is a field $K \supset k$ such that $[K : k]$ is finite and $f(x)$ factors into monic polynomials of degree 1 in $K[x]$.

   (b) Suppose that $\gcd(q, n) = 1$ for integers q and n and let F be a field with q elements. Show that if K is an extension in which $x^n - 1$ factors into monic polynomials of degree 1, then $x^n - 1$ has distinct roots in K. [Hint: formal differentiation. Make sure you use that $\gcd(q, n) = 1$ since it is not true otherwise.]

   (c) Let f be the smallest degree of an extension K of F such that $x^n - 1$ splits into linear factors in K. Show that f is the order of q modulo n (i.e. f is the smallest positive integer t such that $q^t \equiv 1 \pmod{n}$). [Hint: to show that $q^f \equiv 1 \pmod{n}$, argue that the roots of $x^n - 1$ form a subgroup of K^* and apply Lagrange's theorem. To show that f is the smallest such integer, let t be an integer satisfying $q^t \equiv 1 \pmod{n}$ and set $K' = \{\alpha \in K\colon\ \alpha^{q^t} = \alpha\}$. Argue that K' is a subfield of K of degree at most t and still $x^n - 1$ splits into linear factors in K'.]