1 In this assignment, and throughout the rest of the semester, we will adopt the notation $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ to denote the field of order p. We had previously called this field $\mathbb{Z}_p$ or $\mathbb{Z}/p\mathbb{Z}$.

(a) Prove that every element of $\mathbb{F}_p$ has a unique pth root in $\mathbb{F}_p$. That is, if $a \in \mathbb{F}_p$, then there exists exactly one element $b \in \mathbb{F}_p$ such that $b^p = a$. [HINT: Consider the map $a \mapsto a^p$.]

(b) Let $a \in \mathbb{F}_p$. Prove that the polynomial $x^p + a$ is reducible in $\mathbb{F}_p[x]$. Factor it as a product of irreducible polynomials.

2 An element a in a field F is called a **primitive nth root of unity** if n is the smallest positive integer such that $a^n = 1$. For example, i is a primitive 4th root of unity in $\mathbb{C}$, whereas -1 is not a primitive 4th root of unity (even though $(-1)^4 = 1$).

(a) Find all primitive 4th roots of unity in $\mathbb{F}_5$.

(b) Find all primitive 3rd roots of unity in $\mathbb{F}_7$.

(c) Find all primitive 6th roots of unity in $\mathbb{F}_7$.

(d) Use Lagrange's Theorem to prove that if n does not divide $p-1$, then $\mathbb{F}_p$ contains no nth roots of unity. [In fact, the converse is true: If n divides $p-1$, then $\mathbb{F}_p$ contains a (primitive) pth root of unity. We will prove this later.]

3

(a) List all monic irreducible polynomials of degree 2 in $\mathbb{F}_2[x]$.

(b) List all monic irreducible polynomials of degree 3 in $\mathbb{F}_2[x]$.

(c) List all monic irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$.

4 Factor the following polynomials as a product of irreducible polynomials in $\mathbb{F}_5[x]$.

(a) $x^3 + x^2 + x + 1$

(b) $x^4 + 4x^2 + 3$

(c) $x^5 + 2x^4 + 3x^3 + 3x^2 + 4x + 2$