II

Finite Fields and Quadratic Residues

In this chapter we shall assume familiarity with the basic definitions and properties of a field. We now briefly recall what we need.

1. A *field* is a set $\mathbf{F}$ with a *multiplication* and *addition* operation which satisfy the familiar rules — associativity and commutativity of both addition and multiplication, the distributive law, existence of an additive identity 0 and a multiplicative identity 1, additive inverses, and multiplicative inverses for everything except 0. The following examples of fields are basic in many areas of mathematics: (1) the field $\mathbf{Q}$ consisting of all rational numbers; (2) the field $\mathbf{R}$ of real numbers; (3) the field $\mathbf{C}$ of complex numbers; (4) the field $\mathbf{Z}/p\mathbf{Z}$ of integers modulo a prime number p.
2. A *vector space* can be defined over any field $\mathbf{F}$ by the same properties that are used to define a vector space over the real numbers. Any vector space has a *basis*, and the number of elements in a basis is called its *dimension*. An *extension field*, i.e., a bigger field containing $\mathbf{F}$, is automatically a vector space over $\mathbf{F}$. We call it a *finite extension* if it is a finite dimensional vector space. By the *degree* of a finite extension we mean its dimension as a vector space. One common way of obtaining extension fields is to *adjoin* an element to $\mathbf{F}$: we say that $\mathbf{K} = \mathbf{F}(\alpha)$ if $\mathbf{K}$ is the field consisting of all rational expressions formed using α and elements of $\mathbf{F}$.
3. Similarly, the *polynomial ring* can be defined over any field $\mathbf{F}$. It is denoted $\mathbf{F}[X]$; it consists of all finite sums of powers of X with coefficients in $\mathbf{F}$. One adds and multiplies polynomials in $\mathbf{F}[X]$ in the same way as one does with polynomials over the reals. The *degree* d of a polynomial