10

Finite Fields in General, and $GF(2^8)$ in Particular

Although many readers may not have heard these words before (in a mathematical context), *rings* and *fields* are names for generic number systems that possess a number of important arithmetic axioms. Both require that there be two operations on an underlying set of elements: addition and multiplication. Some familiar axioms like associativity and the distributive law are required, and there must be an additive identity (0) and a multiplicative identity (1). Fields are rings with an additional requirement that it is always possible to divide by any nonzero element; thus rings are more general objects. Examples of fields include the real numbers, the rational numbers (all fractions), and $\mathbb{Z}_p$, whenever p is prime. Examples of rings that are not fields include the integers $\mathbb{Z}$ and $\mathbb{Z}_n$, whenever $n > 1$ is composite. A finite field is a field whose underlying set is a finite set, such as $\mathbb{Z}_p$, whenever p is prime, which contains p elements. It turns out that any finite field must contain p^n elements, where p is a prime and n is a positive integer, and that for any such p and n, there is always a unique finite field with p^n elements. This unique finite field is denoted $GF(p^n)$. We show how to construct any $GF(p^n)$ using a concrete procedure involving polynomials with coefficients in $\mathbb{Z}_p$. The process is entirely analogous to the way that $\mathbb{Z}_p$ was constructed from the integers. Finite fields are useful number systems in constructing cryptosystems. We also make some specialized comments about $GF(2^4)$ and $GF(2^8)$, since both of these finite fields play important roles in the next chapter.

Binary Operations

Definition 10.1

A **binary operation** on any nonempty set S is simply a function whose domain is the set of all ordered pairs of elements of S and whose codomain is S.

Rather than using a notation such as $f(s_1, s_2)$ for a specific binary operation to be applied to an ordered pair of elements s_1, s_2, it is more common to adopt a symbol for the binary operation and simply place the symbol between the elements. For example, if we adopt the "triangle" symbol $\triangle$ for a certain binary operation, the image on an ordered pair s_1, s_2 would be denoted as $s_1 \triangle s_2$.

Example 10.1

(a) Here are some very familiar examples of binary operations: the addition operation (+) that is defined on many sets of numbers, such as the integers $\mathbb{Z}$, the mod n integers $\mathbb{Z}_n$, and also on the set of all matrices of a fixed size (whose entries are in a fixed set, such as the real numbers or the integers).

(b) The following equation defines a binary operation, which we denote by the "triangle" symbol $\triangle$ on the set of positive integers $\mathbb{Z}_+$: $a \triangle b = a + a \cdot b^2$. Thus, for example, $2 \triangle 3 = 2 + 2 \cdot 3^2 = 20$.

As can be imagined from part (b) of this example, there is no limit to the number of binary operations that can be conceived. Any nonempty set can be endowed with binary operations. If these binary operations satisfy some useful axioms, this can lead to some new and interesting number systems.

Rings

A ring is a nonempty set with two binary operations that are called addition (+) and multiplication (·) which satisfy many of the common arithmetic properties of the integers $\mathbb{Z}$, which we think of as a prototypical ring. The following definition specifies the required properties. Although the definition is long, it is really not so complicated since all of the axioms are familiar ones that we deal with in typical mathematical calculations. It should be helpful to the reader to think about the integers while reading this definition.

Definition 10.2

A **ring** is a set R that is endowed with two binary operations: addition (+) and multiplication (·), and for which the following axioms hold, where a, b, c denote generic elements of R.

1. *Commutativity of Addition.* $a + b = b + a$.
2. *Associativity of Addition.* $(a + b) + c = a + (b + c)$.
3. *Additive Identity.* There exists in R an **additive identity** element, denoted as 0 and called **zero**, that satisfies $a + 0 = a$.

4. *Additive Inverses.* For each ring element a, there exists a corresponding **additive inverse**, denoted as $-a$, that satisfies $a+(-a)=0$.
5. *Commutativity of Multiplication.* $a \cdot b = b \cdot a$.
6. *Associativity of Multiplication.* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
7. *Multiplicative Identity.* There exists in R a **multiplicative identity** element, denoted as 1 and called **one**, that satisfies $a \cdot 1 = a$.
8. *Distributive Law.* $a \cdot (b+c) = a \cdot b + a \cdot c$.

A ring is sometimes formally denoted as a triple $(R,+,\cdot)$, or simply as R, if its two binary operations are clear from the context.

Note: In some books, the definition of a ring does not include Axiom 5 (commutativity of multiplication) and/or Axiom 7 (multiplicative identity). In such treatments, what we call a ring might be called a commutative ring and/or a commutative ring with identity. Since we will only be needing to work with rings that satisfy all of the above axioms, we avoid this more threadbare definition.*

Example 10.2

The integers $\mathbb{Z}$ and the modular integers $\mathbb{Z}_n$ (with $n > 1$ a positive integer) when endowed with their usual addition and multiplication are rings. From our early school days, we know that the integers satisfy all of the above ring axioms. As was pointed out in Chapter 2, the modular integers $\mathbb{Z}_n$ inherit each of these axioms from the integers. Other familiar examples of rings include the real numbers $\mathbb{R}$ and the rational numbers $\mathbb{Q}$, which is the set of all real numbers that are expressible as fractions of integers (with the denominator being nonzero).

Definition 10.3

Let R be a ring, and a, b be elements of R. Just as in ordinary arithmetic, we define **subtraction** in a ring by the following equation:

$$a - b \triangleq a + (-b)$$

In other words, subtracting b from a is the same as adding the additive inverse of b to a. Also, a nonzero element a has a (**multiplicative**) **inverse**

* With our definition, we could use phrases such as "noncommutative ring" and/or "ring without identity" to describe some of these more general systems. An example of a noncommutative ring is the set of all square matrices (with real number, integer, or modular integer entries) of a certain size. We show in Chapter 4 that all of the ring axioms are satisfied, with the exception of commutativity of matrix multiplication. An example of a commutative ring without identity is the set of all even integers $2\mathbb{Z} = \{0, \pm 2, \pm 4, \cdots\}$. All of the other ring axioms are inherited from the ring $\mathbb{Z}$, but $2\mathbb{Z}$ does not contain the multiplicative identity 1.

(also we say a is **invertible**) if there exists another element $a^{-1} \in R$ (called the **inverse** of a) with the property that

$$a \cdot a^{-1} = 1$$

If a is invertible, we define **division** by a as simply multiplying by its inverse.

The set of all **invertible elements** in a ring R is denoted as $R^\times$.

Exercise for the Reader 10.1

Let R be a ring. Show that the set of invertible elements $R^\times$ satisfies the following axioms (with multiplication as a binary operation inherited from R):

1. *Closure under Multiplication.* If $a, b \in R^\times$, then $a \cdot b \in R^\times$.
2. *Closure under Inverses.* If $a \in R^\times$, then $a^{-1} \in R^\times$.
3. *Multiplicative Identity.* $1 \in R^\times$.

Many other familiar algebra rules are consequences of the ring axioms. The following proposition gives a sampling of this phenomenon; other examples will appear in the exercises. When working with rings, it is customary to use the axioms without always specifying them. We do this often with commutativity and associativity. For example, commutativity of multiplication allows us to restate the distributive law $a \cdot (b+c) = a \cdot b + a \cdot c$ as $(a+b) \cdot c = a \cdot c + b \cdot c$.

Proposition 10.1

Let R be a ring. The following identities are valid for any $a, b, c \in R$:

(1) $0 \cdot a = 0$.
(2) Additive inverses and multiplicative inverses are unique.
(3) $-(-a) = a$.
(4) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $(-a)(-b) = ab$.
(5) $a \cdot (b-c) = a \cdot b - a \cdot c$.

Proof: We will prove parts (1) and (4); the proofs of parts (2), (3), and (5) will be left as exercises at the end of the chapter (Exercise 23).

(1) Using the distributive law, we may write $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. If we subtract $0 \cdot a$ from both sides we are left with $0 \cdot a = 0$.

(2) Using the distributive law, we have $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$, where the last equation is true from part (1). It follows that $a \cdot (-b)$ is an additive inverse of $a \cdot b$, and since additive inverses are unique by part (2), we must have $a \cdot (-b) = -(a \cdot b)$. An analogous argument shows that $(-a) \cdot b = -(a \cdot b)$. The last identity follows from two applications of the first, and by using part (3):

$$(-a)(-b) = -a(-b) = -(-ab) = ab. \quad \square$$

Fields

We were brought up (in our work with the real numbers) with the notion that we cannot divide by zero, but it is possible to divide by any nonzero number. A field is a ring with this additional axiom.

Definition 10.4

A **field** F is a ring in which every nonzero element is invertible. A **finite field** is a field having a finite number of elements.

Examples

Example 10.3

With the usual binary operations of addition and multiplication, the ring of real numbers $\mathbb{R}$ and the ring of rational numbers $\mathbb{Q}$ are fields, because every nonzero element is invertible. (For a nonzero rational number a/b, the inverse is just the reciprocal fraction b/a.)

Example 10.4

The ring of integers $\mathbb{Z}$ is not a field. For example, the integer 2 does not have an inverse in $\mathbb{Z}$; that is, there is no *integer* k such that $2 \cdot k = 1$.

Example 10.5

We learned in Chapter 2 that whenever p is prime, every nonzero element of $\mathbb{Z}_p$ is invertible (since it is relatively prime to p); thus, $\mathbb{Z}_p$ is a finite field. If $n > 1$ is composite, however, there will always be nonzero elements of $\mathbb{Z}_n$ that are not relatively prime to n and, hence, (from Proposition 2.11) will not be invertible. Thus, whenever n is composite, the ring $\mathbb{Z}_n$ is not a field.

Exercise for the Reader 10.2

Let the set $F = \{0,1,a\}$ of three elements have addition defined using the ring axioms and $1+1=a$, $a+a=1$, $1+a=0$, and multiplication defined using the ring axioms and $a \cdot a = 1$.

(a) Fill in complete addition and multiplication tables for F.

(b) Is F a field? Explain your answer.

The fields in Example 10.5 are already familiar. The main purpose of this chapter is to learn about some new finite fields. The following theorem tells us all of the possible sizes for a finite field, and that finite fields are uniquely determined by their size. Since a proof of this theorem would require quite a diversion, we refer the interested reader to any decent book on abstract algebra, such as [Hun-96] or [Her-96]. We will

soon provide a procedure that will, in principle, allow us to construct any finite field.

Theorem 10.2: Inventory of Finite Fields

If F is a finite field with at least two elements, then there exists a prime p such that the number of elements of F is a power of p; that is, $|F| = p^n$, for some positive integer n.* Conversely, for any such prime power p^n, there exists a finite field having p^n elements, and this field is unique.† The unique field with p^n elements is denoted as $GF(p^n)$ and is called the **Galois field with p^n elements**, in honor of the youth prodigy mathematician Évariste Galois‡ (see Figure 10.1), who made significant contributions to the theory of fields.

Figure 10.1

* Technically, there is a field with just one element, but it is not a very interesting one and will henceforth be ignored in our developments.

† By saying a field with a certain number of elements is unique, the technical mathematical concept is that of *isomorphism*. More precisely, if F and F' are both fields with the same number p^n (by Theorem 10.2) elements, then there exists a bijective function $\Phi : F \to F'$ that preserves addition and multiplication and takes the 0/1 element of F to the 0/1 element of F'. Preserving addition means that $\Phi(a+b) = \Phi(a) + \Phi(b)$, for any two elements $a, b \in F$. Preserving multiplication means that $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$, for any two elements $a, b \in F$ Such a function Φ is called a *field isomorphism*, and F and F' are said to be *isomorphic* if an isomorphism exists between them. Informally, all this means is that the elements of F can be relabeled as the elements of F', in such a way that when this is done, the addition and multiplication tables for F become those for F'. In cases where two fields F and F' are isomorphic, we will sometimes abuse notation a bit and simply say (as is common in practice) that they are equal: $F = F'$.

‡ Evariste Galois grew up in a small town outside of Paris, where his father was the mayor. Starting from his school days, Galois was definitely a nonconformist. He rarely kept up with his assignments, and his extraordinary mathematical aptitude and intelligence were not noticed until he began his college studies. His literature professor did not believe that Galois had much intelligence at all until he heard from colleagues about Galois's superior mathematical talents. Galois tried to get into the top French mathematics university (École Polytechnique), but after failing the entrance exam on several attempts, he opted for the lesser École Normale. As a student, he published his first mathematical paper at the age of 17, and that same year he wrote another paper on a very difficult topic that was sent to the illustrious French mathematician Augustus Cauchy to referee. Galois did not take the time to carefully write up his work, and although it impressed many in the mathematical community, even the top mathematicians were often not able to follow his reasoning and needed him to revise his papers before they could be further considered. As he continued to flourish as a professional mathematician while he was a still student, he was also quite politically active during a tumultuous era in the history of France. He was imprisoned twice for periods of several months for his political acts, which included making a public threat to the king. After his second prison release in 1832, he fell in love with a daughter of a prison physician (Stephanie-Felice du Motel), and circumstances surrounding this relationship led to his being challenged to a duel. He was compelled to accept the challenge. In the duel he was badly injured by a hit to the stomach and died the following day. Shortly before his death, Galois gathered his unpublished work and instructed a friend to pass them to Gauss and Carl Gustav Jacobi (1804–1851, another top-notch German mathematician). With his papers, he wrote a note that said: "*il se trouvera, j'espère, des gens qui trouveront leur profit à défchiffrer tout ce gâchis*" (I hope that later some people will find it to their advantage to decipher all this mess). His work was indeed not only published but was soon after recognized to contain some most significant mathematical breakthroughs of the century. Despite his tragically brief life, he is considered among the greatest French mathematicians to have ever lived.

Figure 10.1 Evariste Galois (1811–1832), French mathematician.

We have had quite a bit of experience with the field $GF(p)$, which is just $\mathbb{Z}_p$. We give now an abstract formulation of the smallest new finite field $GF(2^2)$, which has only four elements. After this we give a more general and intuitive construction that will allow us to construct any of the finite fields $GF(p^n)$.

Example 10.6

Consider the set F of all 2-bit strings: $F = \{00, 01, 10, 11\}$. We define addition on F as simply XORing a pair of 2-bit strings (and will write addition using the XOR symbol $\oplus$ rather than the ordinary addition symbol +). Thus, for example, $10 \oplus 11 = 01$. We define multiplication of elements of F (denoted by the usual symbol $\cdot$) using the ring axioms with 01 being the multiplicative identity, and by the rules $10 \cdot 10 = 11$, $11 \cdot 11 = 10$, and $10 \cdot 11 = 01$.

(a) Fill in complete addition and multiplication tables for F.
(b) Show that F is a field and, thus, (by Theorem 10.2) must be $GF(4)$.

Solution: Part (a): Note that 00 is the additive identity since $00 \oplus ab = ab$. This, together with the given multiplication information, allows us to completely fill out the addition and multiplication tables, which are shown in Table 10.1 and Table 10.2.

Part (b): Looking through the eight ring axioms of Definition 10.2 that need verification, from the tables of part (a), it is clear that both addition and multiplication are commutative [(1) and (5)], that 00 is the additive identity (3), and that 01 is the multiplicative identity (7). The associativity of addition axiom (2) follows from the associativity of XOR [Proposition 7.1(2)]. To verify that multiplication is associative (Axiom 7), note that the identity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ is clearly true if any of a, b, or c is either zero (00) or one (01). So we need only check the remaining eight instances of this identity (where a, b, and c each runs

TABLE 10.1 Addition Table for Field F of Example 10.6

$\oplus$	**00**	**01**	**10**	**11**
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

TABLE 10.2 Multiplication Table for Field F of Example 10.6

$\cdot$	**00**	**01**	**10**	**11**
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

through 10 and 11), less the two where $a = b = c$, which are also clearly true. Here are the verifications of these six:

$(10 \cdot 10) \cdot 11 = 10 = 10 \cdot (10 \cdot 11)$,
$(10 \cdot 11) \cdot 10 = 10 = 10 \cdot (11 \cdot 10)$,

$(11 \cdot 10) \cdot 10 = 10 = 11 \cdot (10 \cdot 10)$,
$(10 \cdot 11) \cdot 11 = 11 = 10 \cdot (11 \cdot 11)$,
$(11 \cdot 10) \cdot 11 = 11 = 11 \cdot (10 \cdot 11)$, and
$(11 \cdot 11) \cdot 10 = 11 = 11 \cdot (11 \cdot 10)$.

The last ring axiom to check is the distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c$. Of the $4^3 = 64$ possible instances of this equation, some are clearly valid: in cases where any of a, b, or c is zero (00), or if a is 1 (01). Also, since we already know addition is commutative, if we know the distributive law in the case, say, $b = 10$ and $c = 11$, there is no need to check it when the values are reversed to $b = 11$ and $c = 10$. This reduces the number of equations that need to be checked to only $2 \cdot 6 = 12$. This routine verification is left to the next exercise for the reader.*

Finally, to show that the ring F is a (finite) field, we need to show that every nonzero element has a multiplicative inverse. This is clear from the multiplication table, which tells us that $01^{-1} = 01$, $10^{-1} = 11$ and $11^{-1} = 10$. By Theorem 10.2, it follows that $F = GF(4)$.

Exercise for the Reader 10.3

Verify the 12 remaining cases of the distributive law verification in the solution of Example 10.6

* With a bit more thought, it is easy to eliminate half of these 12 in which $b = c$, since both sides of the distributive law will involve an XOR of identical strings and so will be 00.

$\mathbb{Z}_p[X]$ = the Polynomials with Coefficients in $\mathbb{Z}_p$

At this juncture, the creation of the finite field of Example 10.6 may have appeared quite contrived and mysterious, but we will now enter into a general construction procedure from which we will be able to produce this and all other finite fields. The relevant field operations will be nicely modeled with the addition and multiplication of polynomials that one learns about in high school mathematics courses. The only difference is that we now assume that the coefficients of the polynomials lie in $\mathbb{Z}_p$, for some prime number p.

Definition 10.5

Given a prime number p, a **polynomial** with coefficients in $\mathbb{Z}_p$ is any expression of the form

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots a_1 X + a_0$$

where $n \geq 0$ is an integer, X is an **indeterminate** (a formal symbol), and the **coefficients** $a_n, a_{n-1}, \cdots, a_1, a_0$ are elements of $\mathbb{Z}_p$. Any term with a zero coefficient may be omitted, $1 \cdot X^k$ may be written simply as X^k, and X^0 may be written as 1. Thus, we may express a polynomial using the compact sigma notation as follows:

$$f = \sum_{i=0}^{n} a_i X^i$$

The **zero polynomial** arises when all coefficients above are zero, and it can be written simply as 0. For a nonzero polynomial f, with the above representation, if $a_n \not\equiv 0 (\text{mod } p)$, then we say that the polynomial has **degree** n, and we write this as $\deg(f) = n$. So the degree is the highest exponent of the indeterminant appearing in the expression of the polynomial that has a nonzero coefficient.* A polynomial of degree zero is also called a **constant polynomial**. The set of all polynomials with coefficients in $\mathbb{Z}_p$ in the indeterminant X is denoted by $\mathbb{Z}_p[X]$. Two polynomials in $\mathbb{Z}_p[X]$ are **equal** if all corresponding coefficients are equal (mod p).

Example 10.7

The following are polynomials in $\mathbb{Z}_2[X]$: 0, X, $X+1$, X^2+X+1. The polynomials X and $X+1$ have degree 1, while the polynomial X^2+X+1 has degree 2. We point out that $X^2+X+1 = X^2-X+1 = X^2-X-1$ in $\mathbb{Z}_2[X]$ because $-1 \equiv 1 (\text{mod } 2)$.

* It will be convenient to define the degree of the zero polynomial as $-\infty$, as is customarily done in the literature.

Addition and Multiplication of Polynomials in $\mathbb{Z}_p[X]$

The following definition shows how to add and multiply polynomials in $\mathbb{Z}_p[X]$. The procedure is exactly like the one that is taught in high school, except that the coefficient arithmetic needs to be done in $\mathbb{Z}_p$. Here is a simple motivating example involving polynomials in $\mathbb{Z}_2[X]$ [recall $2 \equiv 0 \pmod 2$]:

$$(X^2+X+1)+(X+1) = X^2+2X+2 = X^2$$

$$\begin{aligned}(X^2+X+1)\cdot(X+1) &= (X^2+X+1)\cdot X + (X^2+X+1)\cdot 1\\ &= X^3+X^2+X+X^2+X+1\\ &= X^3+1\end{aligned}$$

Definition 10.6 Addition and Multiplication of Polynomials in $\mathbb{Z}_p[X]$

Suppose that $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$ are polynomials in $\mathbb{Z}_p[X]$.

(1) We define the **sum** $f+g$ to be the polynomial $\sum_{i=0}^{N} c_i X^i$ with $N = \max(n,m)$, and $c_i \equiv a_i + b_i \pmod p$.

(2) We define the **product** $f \cdot g$ to be the polynomial $\sum_{i=0}^{n+m} d_i X^i$ with $d_i \equiv \sum_{j=0}^{i} a_j \cdot b_{i-j} \pmod p$. (As usual, we take coefficients that do not appear in the expressions of f and g to be zero.)

Note that the coefficients d_i in (2) come from multiplying all combinations of terms in f with terms in g such that the total degree adds up to i; this is based on the algebraic identity $X^j \cdot X^k = X^{j+k}$. Indeed:

$$a_j X^j \cdot b_{i-j} X^{i-j} = a_j b_{i-j} X^{j+(i-j)} = a_j b_{i-j} X^i$$

To see why the coefficient formula in (2) really gives the same result as when we use the standard polynomial multiplication rules that were learned in high school, let us redo the example $(X^2+X+1)\cdot(X+1)$ that was done above. The coefficients of the first polynomial are $a_2 = a_1 = a_0 = 1$, and those for the second are $b_1 = b_0 = 1$. The degrees of the two polynomials are $n = 2$ and $m = 1$, respectively. The coefficients of the product $\sum_{i=0}^{n+m} d_i X^i$, as given in (2), are as follows:

$$d_3 \equiv \sum_{j=0}^{3} a_j \cdot b_{i-j} \equiv a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 \equiv 1\cdot 0 + 1\cdot 0 + 1\cdot 1 + 0\cdot 1 \equiv 1 \pmod 2$$

$$d_2 \equiv \sum_{j=0}^{2} a_j \cdot b_{i-j} \equiv a_0 b_2 + a_1 b_1 + a_2 b_0 \equiv 1\cdot 0 + 1\cdot 1 + 1\cdot 1 \equiv 0 \pmod 2$$

$$d_1 \equiv \sum_{j=0}^{1} a_j \cdot b_{i-j} \equiv a_0 b_1 + a_1 b_0 \equiv 1 \cdot 1 + 1 \cdot 1 \equiv 0 (\text{mod } 2)$$

$$d_0 \equiv \sum_{j=0}^{0} a_j \cdot b_{i-j} \equiv a_0 b_0 \equiv 1 \cdot 1 \equiv 1 (\text{mod } 2)$$

Thus, $\sum_{i=0}^{n+m} d_i X^i = 1 + X^3$, as we obtained above.

In performing polynomial multiplications by hand, it is often convenient to distribute the multiplications among the terms of one of the factors (as one does in high school polynomial multiplications and as we did in the motivating examples), but doing the coefficient arithmetic mod p. We will soon give a theorem that shows such distributive laws remain valid in $\mathbb{Z}_p[X]$ arithmetic.

Exercise for the Reader 10.4

Perform the following polynomial computations:

(a) $(X^5 + 4X^3 + 2) + (3X^3 + 2X)$ and $(X^5 + 4X^3 + 2) \cdot (3X^3 + 2X)$ in $\mathbb{Z}_5[X]$

(b) $(X^n + X^{n-1} + X^{n-2} + \cdots + X + 1) \cdot (X - 1)$ in $\mathbb{Z}_p[X]$, where n is any positive integer and p is any prime

The **leading term** of any nonzero polynomial is the term of highest degree (= the degree of the polynomial) that has a nonzero coefficient. It is clear that when we multiply two nonzero polynomials, the leading term of the product is the product of the leading terms of the factors.* Since the coefficients are nonzero elements in a field $\mathbb{Z}_p$, their product must be nonzero (see Exercise for the Reader 10.1). Thus the degree of the product of two nonzero polynomials is the sum of the degree of the two polynomials. We enunciate this important observation as the following.

Proposition 10.3

If p is a prime, and f and g are polynomials in $\mathbb{Z}_p[X]$, then $\deg(fg) = \deg(f) + \deg(g)$.†

Vector Representation of Polynomials

Although we discuss this topic more thoroughly in the computer implementation material at the end of the chapter, we briefly indicate here how polynomials can be easily stored and manipulated on a computer. It is often

* In terms of the coefficient formula in (2) of Definition 10.6, this means that the formula $d_{n+m} \equiv \sum_{j=0}^{n+m} a_j \cdot b_{n+m-j} (\text{mod } p)$ really has only a single term in the sum (corresponding to $j = n$), since if $j > n$, $a_j = 0$ whereas if $j < n$, then $n + m - j > m$, so $b_{n+m-j} = 0$. Thus, $d_{n+m} \equiv a_n \cdot b_m (\text{mod } p)$.

† Note that this identity is true even if one of the polynomials is the zero polynomial, since in this case their product will also be the zero polynomial, and $-\infty + A = -\infty$, for any real number A.

convenient to store a polynomial $f = a_n X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0 \in \mathbb{Z}_p[X]$ by the $\mathbb{Z}_p$ vector of its coefficients: $f = \sum_{i=0} a_i X^i \sim [a_n, a_{n-1}, \cdots, a_1, a_0]$. The addition and multiplication operations can be converted into corresponding operations on such vectors. Suppose that $g = \sum_{i=0}^{m} b_i X^i \sim [b_m, b_{m-1}, \cdots, b_1, b_0]$ is another polynomial in $\mathbb{Z}_p[X]$. From the definition of addition of polynomials, we may write:

$$f + g \sim [c_N, c_{N-1}, \cdots, c_1, c_0] \tag{10.1}$$

where $N = \max(n, m)$, and $c_i \equiv a_i + b_i \pmod{p}$ for $1 \le i \le N$.

To understand the vector version of polynomial multiplication, we first see how it will work if we multiply $f \neq 0$ by a **monomial**, which is a nonzero polynomial consisting of a single term, $b_k X^k$:

$$f \cdot X^k = (a_n X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0) \cdot X^k =$$
$$a_n X^{n+k} + a_{n-1}X^{n+k-1} + \cdots a_1 X^{1+k} + a_0 X^k$$

In vector notation, this multiplication becomes

$$[a_n, a_{n-1}, \cdots, a_1, a_0] \cdot [b_k, \underbrace{0, 0, \cdots, 0}_{k \text{ zeros}}] = b_k [a_n, a_{n-1}, \cdots, a_1, a_0, \underbrace{0, 0, \cdots, 0}_{k \text{ zeros}}] \tag{10.2}$$

where the latter scalar/vector multiplication is done mod p. By (repeatedly) using the distributive law, a general polynomial multiplication can be broken down into a sum of multiplications of a polynomial by a monomial:

$$f \cdot g = f \cdot \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{m} f \cdot b_i X^i \Rightarrow f \cdot g$$

$$\sim \sum_{i=0}^{m} b_i [a_n, a_{n-1}, \cdots, a_1, a_0, \underbrace{0, 0, \cdots, 0}_{i \text{ zeros}}] \tag{10.3}$$

Thus, with this method of storing polynomials along with the associated Equation 10.1 and Equation 10.3 for their addition and multiplication, we have an efficient means for manipulating polynomials on computing platforms. This will serve as a basis for the computer implementation of soon-to-be developed arithmetic of finite fields.

$\mathbb{Z}_p[X]$ Is a Ring

With the addition and multiplication operations defined above, it is not hard to show that $\mathbb{Z}_p[X]$ is a ring. The proof that the ring axioms are satisfied will be left to Exercise 25.

Theorem 10.4

If p is any prime number, then $\mathbb{Z}_p[X]$ is a ring. The zero polynomial is the zero element, and the constant polynomial 1 serves as the multiplicative identity.

Divisibility in $\mathbb{Z}_p[X]$

We are now ready to discuss some aspects of the rich divisibility theory for the ring $\mathbb{Z}_p[X]$ that very nicely parallels that which was developed in Chapter 2 for the ring $\mathbb{Z}$ of integers. Before reading on, the reader would do well to take a few moments to glance back over the first several pages of Chapter 2.

Recall that earlier in this chapter, we computed $(X^2+X+1)\cdot(X+1)=X^3+1$ in $\mathbb{Z}_2[X]$. We say that either of the polynomials on the left is a *factor* or *divides* the polynomial on the right, and use the integer notation for divisibility. So we could write, for example, $(X^2+X+1)\mid X^3+1$. Here is the general definition (cf. Definition 2.1).

Definition 10.7

Suppose that f and g are polynomials in $\mathbb{Z}_p[X]$ with $f\neq 0$. We say that f **divides** g (written as $f\mid g$) if there is another polynomial $h\in\mathbb{Z}_p[X]$ such that $g=fh$. This can also be expressed by saying f is a **factor** of g, or g is a **multiple** of f. If f does not divide g, we write $f\nmid g$.

The next result records some simple facts about polynomial divisibility.

Theorem 10.5

Suppose that f, g, and h are polynomials in $\mathbb{Z}_p[X]$, for some prime p.

(a) If $f\mid g$ and $g\neq 0$, then $\deg(f)\leq\deg(g)$.
(b) *Divisibility is transitive.* If $f\mid g$ and $g\mid h$, then $f\mid h$.
(c) If $f\mid g$ and $f\mid h$, then $f\mid sg+th$ for any polynomials $s,t\in\mathbb{Z}_p[X]$.

Proof: Part (a): If $f\mid g$, then $g=fH$ for some $H\in\mathbb{Z}_p[X]$. By Proposition 10.3, it follows that $\deg(g)=\deg(f)+\deg(H)$. Since $\deg(H)\geq 0$ (because H cannot be the zero polynomial), the previous equation implies that $\deg(g)\geq\deg(f)$.

Parts (b) and (c): The proofs of the corresponding parts of Theorem 2.1 for integers work equally well in the setting of polynomials. □

Example 10.8

(a) For which prime numbers p (if any) is it true that $X+1\mid(X^2-1)$ in $\mathbb{Z}_p[X]$?
(b) For which prime numbers $p<10$ is it true that $X+1\mid(X^2+1)$ in $\mathbb{Z}_p[X]$?

Solution: Part (a): Some readers might remember the factorization identity $X^2-1=(X+1)(X-1)$. (If not, it is easily checked by multiplying out the right product.) Any such polynomial identity that is valid for ordinary polynomials (with integer arithmetic) will automatically be valid in any $\mathbb{Z}_p[X]$ (because if the coefficients are equal as integers, then they will certainly be equal mod p). Thus, $X+1 \mid (X^2-1)$ in $\mathbb{Z}_p[X]$ for any prime number p.

Part (b): If $X+1 \mid (X^2+1)$ $\mathbb{Z}_p[X]$, then there would be a polynomial $f \in \mathbb{Z}_p[X]$ such that $X^2+1=f\cdot(X+1)$. By Proposition 10.3, we must have deg(f) = 1, so $f=aX+b$ for some coefficients $a,b \in \mathbb{Z}_p$, $a \not\equiv 0$. Since

$$X^2+1=f\cdot(X+1)=(aX+b)(X+1)=aX^2+(a+b)X+b$$

we can compare coefficients to conclude that $a \equiv 1$, $a+b \equiv 0$, and $b \equiv 1$. Substituting the outer two equations into the middle equation shows that this is possible if, and only if, $2 \equiv 0 (\mathrm{mod}\, p)$. Thus, $X+1 \mid (X^2+1)$ in $\mathbb{Z}_p[X]$, only in the case $p = 2$. Also, we have shown that the polynomial identity $X^2+1=(X+1)(X+1)=(X+1)^2$ (which we know is false in ordinary arithmetic) is true in $\mathbb{Z}_2[X]$.

We next would like to define *irreducible* polynomials, which play the same role in $\mathbb{Z}_p[X]$ as primes play in the ring of integers. Since all nonzero elements of $\mathbb{Z}_p$ have inverses, it follows that the leading coefficient of any nonzero polynomial in $\mathbb{Z}_p[X]$ always can be factored out, so we may always assume that the leading coefficient of any polynomial to be factored is 1. Moreover, by Proposition 10.3, no polynomial of positive degree can have an inverse in $\mathbb{Z}_p[X]$. Thus, the units in $\mathbb{Z}_p[X]$, $\mathbb{Z}_p[X]^\times$ are just the set of (nonzero) constant polynomials.

Definition 10.8

A polynomial f in $\mathbb{Z}_p[X]$ of positive degree is said to be **irreducible** in $\mathbb{Z}_p[X]$ if f has no polynomial factor $g \in \mathbb{Z}_p[X]$ with $0 < \deg(g) < \deg(f)$.

Exercise for the Reader 10.5

(a) For which prime numbers p (if any) is it true that X^2-1 is irreducible in $\mathbb{Z}_p[X]$?

(b) For which prime numbers p (if any) is it true that X^2+1 is irreducible in $\mathbb{Z}_p[X]$?

We next develop some more systematic mechanisms for testing divisibility relations that can be used to determine whether a given polynomial is irreducible.

The Division Algorithm for $\mathbb{Z}_p[X]$

We need an efficient way to determine whether a polynomial g divides into another polynomial f, whenever $0 < \deg(g) < \deg(f)$. This is provided by a following division algorithm that very nicely corresponds to the one we developed for integers in Chapter 2, except that the "sizes" of polynomials are gauged by their degrees. The mechanics of this polynomial division algorithm are just as those for polynomial long division that are taught in high school, so before formally stating the algorithm, we motivate it by performing the division $(X^4+X^3+1) \div (X^2+1)$ in $\mathbb{Z}_2[X]$. The process is displayed with the usual schematic diagram that one learns about in high school; see Figure 10.2. With reference to this diagram, the steps taken are as follows (the only difference with the high school algorithm is that the coefficient arithmetic is performed mod 2): We first put the **divisor** X^2+1 on the left side of the long division symbol ⟌ and, after inserting zero coefficients as placeholders in the **dividend** $X^4+X^3+1 \rightarrow X^4+X^3+0\cdot X^2+0\cdot X+1$, we put this on the right and under the top of the division symbol. We next divide the leading term of the dividend $(=X^4)$ by the leading term of the divisor $(=X^2)$ to obtain the *first quotient* X^2 (because $X^2\cdot X^2 = X^4$) and put this quotient X^2 directly over X^4 on top of the long division symbol ⟌.

Next, we multiply this first quotient with the divisor to obtain $X^2(X^2+1) = X^4+X^2$, and subtract this result from the dividend to obtain the current remainder: X^3+X^2+1.* The current remainder is lined up two rows below the dividend in the diagram. Since the degree of this current remainder $(=3)$ is at least as large as that of the divisor $(=2)$, we repeat this process and divide the leading term of the current remainder $(=X^3)$ by the leading term of the divisor $(=X^2)$ to obtain the *second quotient* X (because $X\cdot X^2 = X^3$) and put this quotient X directly over X^3 on top of the long division symbol ⟌. We then multiply this second quotient with the divisor to obtain $X(X^2+1) = X^3+X$, and subtract this result from the previous remainder to obtain the current remainder: X^2+X+1. This current remainder is lined up two rows below the previous one in the diagram. Since the degree of the current remainder $(=2)$ is the same

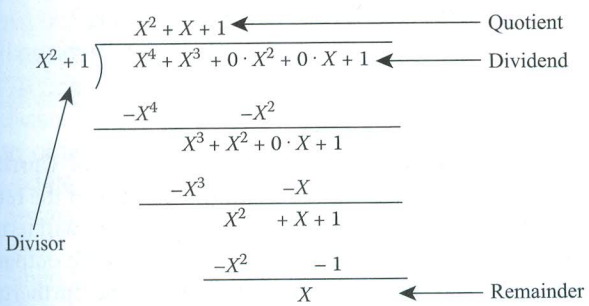

Figure 10.2 Schematic diagram of the polynomial division $(X^4+X^3+1) \div (X^2+1)$ in the ring $\mathbb{Z}_2[X]$.

* We remind the reader that we are working in mod 2 arithmetic with the coefficients, so that $-X^2 = X^2$.

as that of the divisor, we need to repeat the process once more. We obtain the third and last quotient of 1 (since the leading coefficient of the current remainder and the divisor are the same), which is placed directly over $0 \cdot X^2$ on top of the long division symbol $\overline{)}$. We then multiply this third quotient with the divisor to obtain $1 \cdot (X^2+1) = X^2+1$, and subtract this result from the previous remainder to obtain the current remainder, X. This current remainder is lined up two rows below the previous one in the diagram. Since the degree of this current remainder is less than that of the divisor, the algorithm terminates, and produces the result that $(X^4+X^3+1) \div (X^2+1) = X^2+X+1$ Remainder X, which corresponds to the equation $X^4+X^3+1 = (X^2+X+1)\cdot(X^2+1)+X$. This example had the luxury of working in $\mathbb{Z}_2$, where the only nonzero number (1) is its own inverse, and adding it is the same as subtracting it. The following note explains how to deal with finding monomial quotients in the general ring $\mathbb{Z}_p[X]$.*

Note: If p is any prime, and aX^ℓ, bX^k are two nonzero monomials in $\mathbb{Z}_p[X]$ with $\ell \geq k$, then the quotient $aX^\ell \div bX^k$ is $ab^{-1}X^{\ell-k}$. In the case $p = 2$, this simply becomes $X^\ell \div X^k = X^{\ell-k}$. In most of our divisions, the divisor will have a leading coefficient of 1, so that there is no need to find $b^{-1} \pmod p$.

Algorithm 10.1: Division Algorithm in $\mathbb{Z}_p[X]$

Input: Two polynomials $f, g \in \mathbb{Z}_p[X]$ with $g \neq 0$.

Output: Two polynomials $q, r \in \mathbb{Z}_p[X]$ that satisfy $f = q \cdot g + r$, with $\deg(r) < \deg(g)$.

As in the analogous Proposition 2.4 for integers, f is called the **divisor**, g is called the **dividend**, q the **quotient**, and r the **remainder**.

Step 1. Initialize the current remainder CurrRem = f, and the Quotient = 0.

Step 2. Divide the leading coefficient of CurrRem by that of g, call the result as QuotTemp. Update Quotient → Quotient + QuotTemp.

Step 3. Update CurrRem → CurrRem – QuotTemp · g.

Step 4. If deg(CurrRem) ≥ deg(g), go back to Step 2, otherwise assign outputs: q = Quotient, r = CurrRem, and exit algorithm.

Note that in Step 3, since the leading coefficients of CurrRem, and QuotTemp · g have been designed to match, the degrees of the remainders go down in each iteration, so it follows that the algorithm will terminate. It is also not hard to show using the distributive law that the outputted quotient and remainder do indeed satisfy $f = q \cdot g + r$, and furthermore that the quotient and remainder are the unique polynomials that satisfy this

* Readers who are solely interested in the aspects of polynomials for AES may skip over comments regarding polynomial arithmetic in $\mathbb{Z}_p[X]$, for specific values of $p > 2$.

equation under the condition that $\deg(r) < \deg(g)$; see Exercise 32. This result will be used often, so we enunciate it as the following proposition.*

Proposition 10.6: The Division Algorithm

Suppose that p is a prime, and that $f, g \in \mathbb{Z}_p[X]$, with $g \neq 0$. Then there exist unique polynomials $q, r \in \mathbb{Z}_p[X]$ that satisfy $f = q \cdot g + r$, with $\deg(r) < \deg(g)$. These polynomials can be determined by Algorithm 10.1.

Example 10.9

Find the quotient and remainder when the division algorithm is applied to the following polynomial division in $\mathbb{Z}_5[X]$: $(X^4 + 3X + 2) \div (X^2 + 2)$.

Solution: The division algorithm is summarized by the schematic diagram shown here. A more detailed outline of the steps follows.

$$
\begin{array}{r|l}
X^2 + 2 & X^2 + 3 \\
\hline
 & X^4 + 0X^3 + 0X^2 + 3X + 2 \\
 & -X^4 \quad\quad - 2X^2 \\
\hline
 & \quad\quad 3X^2 + 3X + 2 \\
 & \quad\quad -3X^2 \quad\quad -1 \\
\hline
 & \quad\quad\quad\quad 3X + 1
\end{array}
$$

Step 1. Initialize CurrRem = $X^4 + 3X + 1$, Quotient = 0.

Step 2. First we divide the leading coefficient of the divisor (= X^2) into that of the current remainder (= X^4) to obtain the temporary quotient (= X^2). We add this to update the quotient, which is now Quotient = X^2.

Step 3. CurrRem gets updated to $X^4 + 3X + 2 - X^2(X^2 + 2) = 3X^2 + 3X + 2$ in $\mathbb{Z}_5[X]$. Since this has degree $2 \geq 2 = \deg(X^2 + 2)$, we return to Step 2 (for the second and final iteration).

Step 2. *Second iteration.* We divide the leading coefficient of the divisor (= X^2) into that of the current remainder (= $3X^2$) to obtain the temporary quotient (= 3). We add this to update the quotient, which is now Quotient = $X^2 + 3$.

Step 3. *Second iteration.* CurrRem gets updated to $3X^2 + 3X + 2 - 3(X^2 + 2) = 3X + 1$.

Step 4. Since CurrRem has degree $1 < 2 = \deg(X^2 + 2)$, the algorithm terminates with the outputs: q = Quotient = $X^2 + 3$, and r = Remainder = $3X + 1$.

* Although the statement of this proposition is not an algorithm, it is common practice to refer to this statement as "the division algorithm." Compare with Proposition 2.4.

Exercise for the Reader 10.6

Use the division algorithm (Algorithm 10.1) to perform the indicated polynomial divisions:

(a) $X^5+1 \div X^3+1$ in $\mathbb{Z}_2[X]$

(b) $X^5+4X^2 \div X^2+5$ in $\mathbb{Z}_7[X]$

Computing Note: Algorithm 10.1 can easily get quite complicated and time consuming. But since each step is easily translated into a corresponding vector operation based on additions and multiplications of polynomials whose vector counterparts were described earlier, Algorithm 10.1 is easily implemented on a computing platform. Details are provided in the computer implementation material at the end of the chapter.

The next Exercise for the Reader will allow the reader to discover that $g \mid f$ if, and only if, the remainder r in the above division is zero. (Just as was the case for the integers.)

Exercise for the Reader 10.7

Show that if we have two polynomials $f, g \in \mathbb{Z}_p[X]$, with $0 < \deg(g) \leq \deg(f)$, then $g \mid f$ if, and only if, the remainder r of the division algorithm (Algorithm 10.1) is the zero polynomial.

The result of this exercise for the reader provides one brute-force algorithm for determining whether a given polynomial is irreducible, which we summarize as an algorithm.

Algorithm 10.2: Brute-Force Irreducibility Test for Polynomials in $\mathbb{Z}_p[X]$

Input: A polynomial $f \in \mathbb{Z}_p[X]$ of degree at least 2 which we suspect might be irreducible.*

Output: Either a nontrivial factor of f (showing that it is not irreducible) or a statement that f is irreducible.

Step 1. Initialize the factor degree deg = 1 (the smallest possible degree of a nontrivial factor).

Step 2. Run through all polynomials g having degree deg and leading coefficient 1: $g = X^{\deg} + a_{\deg-1}X^{\deg-1} + \cdots + a_1X + a_0$, where the deg coefficients $a_{\deg-1}, \cdots, a_1, a_0$ range through all possible mod p integers. Apply the division algorithm to $f \div g$. If the remainder r of such a division ever turns out to be zero, then (by Exercise for the Reader 10.7) the quotient q will be a nontrivial factor of f. So output this quotient and exit the algorithm.

Step 3. Update deg $\rightarrow$ deg + 1. If this new value of deg is greater than floor(deg(f)/2), declare f as irreducible and exit the algorithm; otherwise, return to Step 2.

* Any polynomial of degree 1 in $\mathbb{Z}_p[X]$ is irreducible. (Why?)

The reason that (in Step 3) f can be declared irreducible if no nontrivial factor has been found of degree $\leq \text{floor}(\deg(f)/2)$ is because of Proposition 10.3. For polynomials of small degree (say, up to 5 or maybe 7) and $p = 2$ (our main modulus for our use of finite fields), this algorithm is feasible for hand computations. When testing a polynomial of degree 5 with $p = 2$, for example, there could be up to three division algorithms to perform.* Using computer implementations, the algorithm continues to be effective for testing polynomials of moderate degree (for example, for polynomials up to degree 20 or so, with $p = 2$, a computer can perform Algorithm 10.2 in less than a second). Exercise 25 presents a quick method to check whether a given first-degree polynomial is a factor of a given polynomial, and this method could be embellished into Algorithm 10.1.

Exercise for the Reader 10.8

(a) Use Algorithm 10.2 to determine whether the polynomial $X^3 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$.

(b) Use Algorithm 10.2 to determine whether the polynomial $X^4 + X^3 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$.

Congruences in $\mathbb{Z}_p[X]$ Modulo a Fixed Polynomial

We may define congruences in $\mathbb{Z}_p[X]$, modulo any nonzero polynomial $m \in \mathbb{Z}_p[X]$, just as we defined congruences in $\mathbb{Z}$ modulo any nonzero integer n.

Definition 10.9

Two polynomials $f, g \in \mathbb{Z}_p[X]$ are said to be **congruent** mod(ulo) a third (nonzero) polynomial $m \in \mathbb{Z}_p[X]$ if $m \mid (f - g)$. In this case, we write $f \equiv g (\text{mod}\, m)$.

It follows from the fact that $\mathbb{Z}_p[X]$ is a ring that all of the favorable properties of the congruence relations for integers (see, for example, Propositions 2.8–2.10) also carry over to hold for congruences modulo a polynomial. The proofs are essentially identical to those given in Chapter 2 in the setting of integers.

* Any factor with no constant term, such as $X^2 + X$, need not be checked with the division algorithm, since it factors into polynomials of smaller degree that have already been checked.

Example 10.10

Find a polynomial in $\mathbb{Z}_2[X]$ of degree less than 3 that is congruent to $X^5 + X \pmod{X^3 + X + 1}$.

Solution: Do this problem using two different methods:

Method 1: Reduction Method. In the notation of Definition 10.8, we have $m = X^3 + X + 1$. Since $m \mid (m - 0)$, we have $m \equiv 0 (\text{mod}\, m)$, or $X^3 + X + 1 \equiv 0$, which implies (subtracting $X + 1$ from both sides) that $X^3 \equiv -X - 1 \equiv X + 1$ (since the coefficient work is done mod 2). Using this congruence twice, we can perform the following reductions of $X^5 \pmod{X^3 + X + 1}$:

$$X^5 + X \equiv X^3 \cdot X^2 + X \equiv (X + 1)X^2 + X \equiv X^3 + X^2 + X$$
$$X^3 + X^2 + X \equiv (X + 1) + X^2 + X \equiv X^2 + 1$$

We have thus shown that $X^5 \equiv X^2 + 1 \pmod{X^3 + X + 1}$.

Method 2: Division Algorithm. By the division algorithm, any polynomial $f \in \mathbb{Z}_p[X]$ can be expressed as $f = q \cdot m + r$, where $q, r \in \mathbb{Z}_p[X]$ with $\deg(r) < \deg(m)$. It follows that $f \equiv r$, its remainder on division by m. Thus, the answer to the question of the example will be the remainder in the $\mathbb{Z}_2[X]$ polynomial division $(X^5 + X) \div (X^3 + X + 1)$, shown in schematic.

$$\begin{array}{r|l} & X^2 \quad\quad +1 \\ \hline X^3 + X + 1 & X^5 + 0X^4 + 0X^3 + 0X^2 + X + 0 \\ & \underline{-X^5 \quad\quad - X^3 \; - X^2} \\ & \quad\quad\quad\quad X^3 \; + X^2 + X \; + 0 \\ & \quad\quad\quad\quad \underline{-X^3 \quad\quad - X \; - 1} \\ & \quad\quad\quad\quad\quad\quad X^2 \quad\quad +1 \end{array}$$

The remainder is the same as the answer obtained by Method 1, as expected.

Exercise for the Reader 10.9

Find a polynomial in $\mathbb{Z}_2[X]$ of degree less than 4 that is congruent to $X^7 + X^4 + X^2 + X \pmod{X^4 + X + 1}$.

Building Finite Fields from $\mathbb{Z}_p[X]$

We finally have all of the machinery needed to construct all of the finite fields $GF(p^n)$ of Theorem 10.2. The process nicely parallels how the fields $GP(p) = \mathbb{Z}_p$ were constructed from the integers in Chapter 2. Table 10.3 indicates the correspondences between the two processes. Just as we were able to build the finite ring $\mathbb{Z}_m$ from the infinite ring

TABLE 10.3 Parallels between Constructions of Finite Fields $GF(p)$ from $\mathbb{Z}$ and $GF(p^n)$ from $\mathbb{Z}_p[X]$

	Integers	Polynomials
Infinite ring	$\mathbb{Z}$	$\mathbb{Z}_p[X]$
Fixed ring element	m (integer > 1)	m (polynomial of degree > 0)
Finite modular ring	$\mathbb{Z}_m$ (has m elements)	$\mathbb{Z}_p[X](\text{mod}\, m)$ (has $p^{\deg(m)}$ elements)
When is finite modular ring a field?	$\mathbb{Z}_m$ is a field if, and only if, $m = a$ prime p	$\mathbb{Z}_p[X](\text{mod}\, m)$ is a field if, and only if, m is an irreducible polynomial

$\mathbb{Z}$, using congruence modulo a positive integer $m > 1$, we will be able to build a finite ring from $\mathbb{Z}_p[X]$ for each nonconstant polynomial $m \in \mathbb{Z}_p[X]$.

The finite polynomial rings are described in the following.

Definition 10.10: ***Finite Polynomial Rings from*** $\mathbb{Z}_p[X]$

If p is a prime number and m is a nonconstant polynomial in $\mathbb{Z}_p[X]$, then the set $\mathbb{Z}_p[X](\text{mod}\, m)$ is defined to be the set of all polynomials in $\mathbb{Z}_p[X]$ having degree less than $\deg(m)$. Thus, $\mathbb{Z}_p[X](\text{mod}\, m)$ consists of all possible remainders that can arise when any polynomial in $\mathbb{Z}_p[X]$ is divided by m. The addition and multiplication binary operations in $\mathbb{Z}_p[X](\text{mod}\, m)$ (which we denote by their usual symbols "+" and "·") are performed by first doing the corresponding usual polynomial operations, and then converting the answer to a polynomial in $\mathbb{Z}_p[X](\text{mod}\, m)$.

The most important facts about $\mathbb{Z}_p[X](\text{mod}\, m)$ are provided in the following theorem, whose proof is similar to the corresponding proofs in Chapter 2, and will be left to the exercises.

Theorem 10.7

If p is a prime number and m is nonconstant polynomial in $\mathbb{Z}_p[X]$, then $\mathbb{Z}_p[X](\text{mod}\, m)$ is a ring consisting of the $p^{\deg(m)}$ polynomials in $\mathbb{Z}_p[X]$ that have degree less than $\deg(m)$. This ring will be a field precisely when m is irreducible, in which case (by Theorem 10.2) we will have $\mathbb{Z}_p[X](\text{mod}\, m) = GF(p^{\deg(m)})$.

As a set,

$$\mathbb{Z}_p[X](\text{mod}\, m) = \{a_{\deg(m)-1}X^{\deg(m)-1} + a_{\deg(m)-2}X^{\deg(m)-2} + \cdots + a_1X + a_0 : a_i \in \mathbb{Z}_p\} \quad (10.4)$$

also has the vector representation

$$\mathbb{Z}_p[X](\text{mod}\, m) = \{[a_{\deg(m)-1}, a_{\deg(m)-2}, \cdots, a_1, a_0] : a_i \in \mathbb{Z}_p\} \qquad (10.5)$$

The latter representation leads to an efficient way to code addition and multiplication in $\mathbb{Z}_p[X](\text{mod}\, m)$, and this concept is expounded upon in the computer implementation material at the end of this chapter. Note that addition in $\mathbb{Z}_p[X](\text{mod}\, m)$ is just ordinary polynomial addition (since the degree of a sum of two polynomials is no greater than the maximum degree of the two polynomials); it is the product of $\mathbb{Z}_p[X](\text{mod}\, m)$ that is new.

The above development shows that we can construct $GF(p^n)$ provided that we can find an irreducible polynomial m in $\mathbb{Z}_p[X]$ with $\deg(m) = n$. It can be shown that irreducible polynomials of any degree exist in $\mathbb{Z}_p[X]$, and Algorithm 10.2 can be used to find them. Let us first show how this method can be used to construct the field with four elements $GF(2^2)$ that was constructed in Example 10.6 using a more ad hoc scheme.

Example 10.11

(a) Show that there is only one irreducible polynomial $m \in \mathbb{Z}_2[X]$ that has degree 2.
(b) Create addition and multiplication tables for the finite field $GF(4) = \mathbb{Z}_2[X](\text{mod}\, m)$, where m is the irreducible polynomial of part (a).

Solution: Part (a): Of the four degree-2 polynomials in $\mathbb{Z}_2[X]$: $X^2, X^2+1, X^2+X, X^2+X+1$, the first three factor as $X^2 = X \cdot X$, $X^2 + X = X(X+1)$, and (as was seen in Example 10.8) $X^2+1 = (X+1)(X+1)$ in $\mathbb{Z}_2[X]$. This leaves only one possibility: $m = X^2 + X + 1$. To show that m is irreducible, we can verify that there will be a nonzero remainder when m is divided by either of the two degree-1 polynomials in $\mathbb{Z}_2[X]$. Applying the division algorithm (Algorithm 10.1), to either of the divisions of m by X or $X+1$ produces the same result: $m = X^2 + X + 1 = X \cdot (X+1) + 1$. Since the remainder (= 1) is nonzero, it follows that m is irreducible in $\mathbb{Z}_2[X]$.

Part (b): Tables 10.4 and 10.5 show the addition and multiplication tables for $\mathbb{Z}_2[X](\text{mod}\, X^2+X+1) = \{0, 1, X, X+1\}$.

TABLE 10.4 Addition Table for Field $GF(4) = \mathbb{Z}_2[X](\text{mod}\, X^2+X+1) = \{0, 1, X, X+1\}$ of Example 10.11

+	**0**	**1**	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

TABLE 10.5 Multiplication Table for Field $GF(4) = \mathbb{Z}_2[X] \pmod{X^2 + X + 1} = \{0, 1, X, X+1\}$ of Example 10.11

·	**0**	**1**	***X***	***X* + 1**
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
***X* + 1**	0	$X+1$	1	X

Notice that these tables are identical with Tables 10.1 and 10.2 for the field F of Example 10.6, with the identifications $00 \leftrightarrow 0, 01 \leftrightarrow 1, 10 \leftrightarrow X, 11 \leftrightarrow X+1$, and since these identifications correspond exactly to the vector representation of polynomials, Tables 10.1 and 10.2 simply give the vectorized version of these tables.

Exercise for the Reader 10.10

Create addition and multiplication tables for the finite ring $\mathbb{Z}_2[X] \pmod{X^2}$, and use one of these tables to provide one piece of evidence that demonstrates that $\mathbb{Z}_2[X] \pmod{X^2}$ is not a field.

The Fields $GF(2^4)$ and $GF(2^8)$

We now present constructions of the 16-element finite field $GF(2^4)$ and of the 256-element finite field $GF(2^8)$. These fields will play crucial roles in the scaled-down AES and the full AES cryptosystems of the next chapter. Thus, from a cryptographic perspective, the construction and understanding of these two fields is the main purpose of this chapter.

Example 10.12: *The Field* $GF(16)$

(a) Show that the degree-4 polynomial $m = X^4 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$. Thus, $\mathbb{Z}_2[X] \pmod{X^4 + X + 1}$ must be (by Theorems 10.2 and 10.7) $GF(2^4)$, the unique finite field of 16 elements.

(b) Perform the following multiplications in $\mathbb{Z}_2[X] \pmod{X^4 + X + 1}$: $(X+1) \cdot X$, $(X^3 + X + 1) \cdot (X^2 + X)$, $(X^2 + X + 1) \cdot (X^5 + 1)$.

(c) Using the hexadecimal representation for the polynomials in $\mathbb{Z}_2[X] \pmod{X^4 + X + 1}$ that derives from the standard binary/hex correspondence of Table 6.1, create a multiplication table for the finite field $GF(2^4) = \mathbb{Z}_2[X] \pmod{X^4 + X + 1}$.

Solution: Part (a): We use Algorithm 10.2. The only degree-1 polynomials (in $\mathbb{Z}_2[X]$) are X and $X+1$. Certainly X is not a factor of m. Since the division algorithm (Algorithm 10.1) applied to the division $m \div (X+1)$ produces a remainder of 1, we know $X+1$ is not a factor. We now move on to check for degree-2 factors. The possibilities are $X^2, X^2+X, X^2+1, X^2+X+1$. We need check only the last two of these. Since the division algorithm produces respective remainders of X and 1, it follows that none of these are factors. Algorithm 10.2 now terminates with the conclusion that m is irreducible.

Part (b): Since $(X+1)\cdot X = X^2+X$ has degree less than 3, no further reductions are needed.

The other two products will need to be reduced after performing the usual multiplication process in $\mathbb{Z}_2[X]$:

$$
\begin{aligned}
(X^3+X+1)\cdot(X^2+X) &\equiv (X^3+X+1)\cdot X^2 + (X^3+X+1)\cdot X \\
&\equiv X^5 + X^3 + \cancel{X^2} + X^4 + \cancel{X^2} + X \\
&\equiv X^4 \cdot X + X^4 + X^3 + X \\
&\equiv (X+1)\cdot X + (X+1) + X^3 + X \\
&\quad (\text{since } X^4 \equiv X+1) \\
&\equiv X^2 + X + (X+1) + X^3 + X \\
&\equiv X^3 + X^2 + X + 1 \quad \text{in } \mathbb{Z}_2[X] \ (\text{mod } X^4+X+1)
\end{aligned}
$$

$$
\begin{aligned}
(X^2+X+1)\cdot(X^3+1) &\equiv (X^2+X+1)\cdot X^3 + (X^2+X+1)\cdot 1 \\
&\equiv X^5 + X^4 + X^3 + X^2 + X + 1 \\
&\equiv (X+1)\cdot X + (X+1) + X^3 + X^2 + X + 1 \\
&\quad (\text{since } X^4 \equiv X+1) \\
&\equiv \cancel{X^2} + \cancel{X} + \cancel{X} + \cancel{1} + X^3 + \cancel{X^2} + X + \cancel{1} \\
&\equiv X^3 + X \quad \text{in } \mathbb{Z}_2[X] \ (\text{mod } X^4+X+1)
\end{aligned}
$$

Part (c): Table 10.6 shows a natural representation of the 16 $\mathbb{Z}_2[X]$ polynomials (of degree less than 4) using the 16 hexadecimal characters that is based on the binary correspondence (see Table 6.1) and the vector representation of polynomials that was developed in this chapter. Such efficient representations will be used in the coding of AES cryptosystems in the next chapter. They also help to make the multiplication table for $GF(2^4)$ that is shown in Table 10.5 much more concise than if we had used polynomials instead. For example,

TABLE 10.6 Hexadecimal and Binary Representation for the Polynomials in $GF(16)$

Polynomial	Binary	Hex
0	0000	0
1	0001	1
X	0010	2
$X+1$	0011	3
X^2	0100	4
X^2+1	0101	5
X^2+X	0110	6
X^2+X+1	0111	7
X^3	1000	8
X^3+1	1001	9
X^3+X	1010	A
X^3+X+1	1011	B
X^3+X^2	1100	C
X^3+X^2+1	1101	D
X^3+X^2+X	1110	E
X^3+X^2+X+1	1111	F

in the hex notation of Table 10.6, the three $GF(2^4)$ multiplications that were computed in part (b) can be economically represented as:

$$(X+1)\cdot X = X^2+6 \;\rightarrow\; 3\cdot 2 = 6$$
$$(X^3+X+1)\cdot(X^2+X) \equiv X^3+X^2+X+1 \;\rightarrow\; B\cdot 6 = F$$
$$(X^2+X+1)\cdot(X^3+1) \equiv X^3+X \rightarrow 7\cdot 9 = A$$

In Table 10.7, the complete multiplication table for $GF(2^4)$ is given, in which one can find the three multiplications of part (b).

Exercise for the Reader 10.11

Using the hex notation of Table 10.6, perform the following computations in $GF(16)$:

(a) $6+D$

(b) $D\cdot(4+A^2)$

(c) $A\cdot B\cdot C\cdot D$

We point out that there are two other degree-4 irreducible polynomials in $\mathbb{Z}_2[X]$: X^4+X^3+1 and $X^4+X^3+X^2+X+1$. Each of these would, by

TABLE 10.7 Multiplication Table $GF(16)$ Using the Hexadecimal Notation of Table 10.6.

.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Theorem 10.7, give rise to the "same" finite field $GF(16)$. The polynomial $X^4 + X + 1$ was chosen because the reduction operation (in modular polynomial multiplication) proceeds more efficiently than with the other two. Similar comments apply to the choice of degree-8 polynomial that is made in the following construction of $GF(256)$.

Example 10.13

(*The Field GF(256)*).
It can be shown that the degree-8 polynomial $m = X^8 + X^4 + X^3 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$ (see Computer Exercise 4). Thus, $\mathbb{Z}_2[X] \pmod{X^8 + X^4 + X^3 + X + 1}$ must be (by Theorems 10.2 and 10.7) $GF(2^8)$, the unique finite field of 256 elements.

(a) Perform the following multiplication in $\mathbb{Z}_2[X] \pmod{X^8 + X^4 + X^3 + X + 1}$: $(X^6 + X + 1) \cdot (X^4 + X)$.

(b) Develop binary/hex correspondence for elements of $GF(2^8)$ similar to what was done in Table 6.1 for the finite field $GF(2^4) = \mathbb{Z}_2[X] \pmod{X^4 + X + 1}$, where each element of $GF(2^8)$ is represented by a string of two hex characters. Represent the computation done in part (b) using this notation, and then compute $79 + A4$ in $GF(2^8)$.

Solution: Part (a): As with any modular polynomial multiplication, we first multiply the polynomials in $\mathbb{Z}_2[X]$, and then reduce powers that the result will have degree at most 7 = deg(m) – 1.

$$
\begin{aligned}
(X^6+X+1)\cdot(X^4+X) &\equiv (X^6+X+1)\cdot X^4+(X^6+X+1)\cdot X \\
&\equiv X^{10}+X^5+X^4+X^7+X^2+X \\
&\equiv (X^4+X^3+X+1)\cdot X^2+X^7+X^5+X^4+X^2+X \\
&\qquad (\text{mod } X^8+X^4+X^3+X+1) \\
&\equiv (X^6+X^5+X^3+X^2)+X^7+X^5+X^4+X^2+X \\
&\equiv (X^6+X^5+X^3+X^2)+X^7+X^5+X^4+X^2+X \\
&\equiv X^7+X^6+X^4+X^3+X
\end{aligned}
$$

Part (b): As explained earlier, any element of $GF(2^8)$ naturally corresponds to its binary string of coefficients:

$$a_7X^7+a_6X^7+\cdots+a_1X+a_0 \sim [a_7,a_{7-1},\cdots,a_1,a_0] \sim a_7a_6a_5a_4a_3a_2a_1a_0$$

We can then use the natural binary/hex correspondence (shown in Table 10.6) to convert the half strings of the first and last four bits into their hex equivalents

$$a_7a_6a_5a_4a_3a_2a_1a_0 \rightarrow [a_7a_6a_5a_4]\,[a_3a_2a_1a_0] \rightarrow H_1H_2$$

where H_1, H_2 is each a single hexadecimal character.

Making this conversion in the computation of part (b), the steps are as follows:

$$
\begin{aligned}
&(X^6+X+1)\cdot(X^4+X) \equiv X^7+X^6+X^4+X^3+X \\
&\rightarrow ([0100][0011])\cdot([0001][0010]) \equiv [1101][1010] \\
&\rightarrow 43\cdot 12 \equiv \texttt{DA}
\end{aligned}
$$

Since adding polynomials in $GF(2^8)$ corresponds to XORing their bit strings, we perform the addition `79 + A4` by working directly on the corresponding bit strings:

```
79 + A4 → ([0111][1001]) ⊕ ([1010][0100]) = ([1101]
[1101]) → DD
```

Exercise for the Reader 10.12

Using the hex notation, perform the following computations in $GF(256)$:

(a) `64+CB`

(b) $\texttt{AA}^2$

(c) `A4·(B9+12)`

The Euclidean Algorithm for Polynomials

We have discussed efficient algorithms for computing sums and products in the rings $\mathbb{Z}_p[X] (\text{mod } m)$, where m is any nonconstant polynomial in $\mathbb{Z}_p[X]$, but the question naturally arises about how to find inverses (when they exist). Of course, for such important and relatively small fields such as $GF(16)$ and $GF(256)$, look-up tables for the inverses could be easily constructed. But at this point, we do not yet have a method for computing such inverses, except by trial and error or if we have a multiplication table at our hands. For example, from Table 10.7, we see that $\mathrm{D} \cdot 4 = 1$, from which we conclude that $\mathrm{D}^{-1} = 4$ in $GF(16)$.

We recall from Chapter 2 that to compute inverses of an element $a \in \mathbb{Z}_n$, we could apply the Euclidean algorithm (Algorithm 2.1) to compute $\gcd(a,n) = r$, and that a^{-1} if, and only if, this gcd is 1. Furthermore, in case $r = 1$, a^{-1} could be found by working backwards through the steps of the Euclidean algorithm to eventually compute a^{-1}. This latter process was formalized in the extended Euclidean algorithm (Algorithm 2.2). Since the Euclidean algorithm is based on the division algorithm for integers, and we have a polynomial analogue for this, this whole program turns out to extend very nicely to the setting of polynomials. The sizes of polynomials are measured by their degrees. The following example will illustrate this algorithm.

Example 10.14

Compute the inverse of the element F4 in $GF(256)$.

Solution: We need to work with polynomials, so we convert as explained in Example 10.13:

$$\mathrm{F4} \rightarrow [1111][0100] \rightarrow X^7 + X^6 + X^5 + X^4 + X^2$$

The polynomial version of the Euclidean algorithm, which we use here for the computation of $\gcd(X^8 + X^4 + X^3 + X + 1, X^7 + X^6 + X^5 + X^4 + X^2)$, follows the same strategy of repeatedly applying the division algorithm until we get a zero remainder.

$$\text{remainder} \rightarrow \text{divisor} \rightarrow \text{dividend} \rightarrow \text{not used}$$

$$X^8 + X^4 + X^3 + X + 1 = (X+1)(X^7 + X^6 + X^5 + X^4 + X^2) + (X^2 + X + 1)$$
$$X^7 + X^6 + X^5 + X^4 + X^2 = (X^5 + X^2 + X + 1)(X^2 + X + 1) + 1$$

Since we have reached a remainder of 1, the Euclidean algorithm terminates to tell us the gcd is 1. We already knew this (Why?), but we next work backwards with the above equations to express the remainder as a polynomial combination of the original two polynomials. (Throughout the computations below, please remember that all coefficient work is mod 2, so $-X^k \equiv X^k$.)

$$X^7 + X^6 + X^5 + X^4 + X^2 = (X^5 + X^2 + X + 1)(X^2 + X + 1) + 1 \Rightarrow$$
$$1 = (X^7 + X^6 + X^5 + X^4 + X^2) + (X^5 + X^2 + X + 1)(X^2 + X + 1)$$

Next, we use the first division algorithm equation:

$$X^8 + X^4 + X^3 + X + 1 = (X+1)(X^7 + X^6 + X^5 + X^4 + X^2) + (X^2 + X + 1) \Rightarrow X^2 + X + 1 = (X^8 + X^4 + X^3 + X + 1) + (X+1)(X^7 + X^6 + X^5 + X^4 + X^2)$$

to substitute into the previous equation to produce:

$$\begin{aligned} 1 &= (X^7 + X^6 + X^5 + X^4 + X^2) \\ &\quad + (X^5 + X^2 + X + 1)[(X^8 + X^4 + X^3 + X + 1) \\ &\quad + (X+1)(X^7 + X^6 + X^5 + X^4 + X^2)] \\ &= (X^5 + X^2 + X + 1)(X^8 + X^4 + X^3 + X + 1) \\ &\quad + [1 + (X^5 + X^2 + X + 1)(X+1)](X^7 + X^6 + X^5 + X^4 + X^2) \\ &= (X^5 + X^2 + X + 1)(X^8 + X^4 + X^3 + X + 1) \\ &\quad + [X^6 + X^5 + X^3](X^7 + X^6 + X^5 + X^4 + X^2) \end{aligned}$$

From this (and the definition of polynomial congruence), it follows that

$$[X^6 + X^5 + X^3](X^7 + X^6 + X^5 + X^4 + X^2) \equiv 1 \pmod{X^8 + X^4 + X^3 + X + 1}$$

Thus we have found that $(X^7 + X^6 + X^5 + X^4 + X^2)^{-1} \equiv X^6 + X^5 + X^3 \rightarrow$ [0110] [1000]. In hex notation: $\texttt{F4}^{-1} = \texttt{68}$ in $GF(256)$.

Exercise for the Reader 10.13

Use the Euclidean algorithm (polynomial version) to compute the following inverses:

(a) $\texttt{A}^{-1}$ in $GF(16)$

(b) $\texttt{1A}^{-1}$ in $GF(256)$

Check your answer for part (a) with Table 10.7.

The analogies—with many of the properties of the ring integers $\mathbb{Z}$ and those for the rings of polynomials $\mathbb{Z}_p[X]$—go further than those we have developed in this chapter. For example, there is a corresponding theory of unique factorization in $\mathbb{Z}_p[X]$ in terms of irreducible polynomials. Interested readers may consult any good book on abstract algebra for more on these topics; see, for example, [Hun-96] or [Her-96]. Exercise 31 will give an irreduciblity testing algorithm based on the Euclidean algorithm for polynomials that is much more efficient than Algorithm 10.1 for testing irreducibility of modular polynomials of high degree. Computer Exercise 10 will make some efficiency comparisons.

Chapter 10 Exercises

1. In each part, a set S along with an addition and multiplication operation is specified. Determine whether an S is a ring. If S is not a ring, identify at least one of the ring axioms that is violated. If a ring is formed, identify the additive and multiplicative identities.
   (a) The set $S = \{0\}$, with the binary operations $0+0=0$, $0\cdot 0=0$.
   (b) The subset $S=\{0,3\}$ of $\mathbb{Z}_6$ with addition and multiplication taken as those operations in $\mathbb{Z}_6$.
   (c) The subset $S=\{0,2,4,6,8\}$ of even integers in $\mathbb{Z}_{10}$ with addition and multiplication taken as those operations in $\mathbb{Z}_{10}$. (That these are binary operations on S comes from the fact that adding or multiplying even numbers in $\mathbb{Z}_{10}$ always produces an even number in $\mathbb{Z}_{10}$.)

   Note: In parts (b) and (c), the addition and multiplication binary operators come from known rings, being restricted to some subset. Thus, many of the ring axioms will automatically be inherited to hold true (when restricted to a smaller set of elements), and so need not be checked.

2. In each part, a set S along with an addition and multiplication operation is specified. Determine whether an S is a ring. If S is not a ring, identify at least one of the ring axioms that is violated. If a ring is formed, identify the additive and multiplicative identities.
   (a) The subset $S=\{0,2\}$ of $\mathbb{Z}_4$, with addition and multiplication taken as those operations in $\mathbb{Z}_4$.
   (b) The set of all nonnegative integers $\mathbb{Z}_{\geq 0}$, with addition and multiplication taken as those operations in $\mathbb{Z}$.
   (c) The set S of all real numbers of the form $a+b\sqrt{2}$, where $a,b\in\mathbb{Q}$, with addition and multiplication taken as those operations in $\mathbb{R}$. (Recall that $\mathbb{Q}$ is the field of rational numbers, i.e., numbers expressible as fractions of integers.)

   Note: In each part, the addition and multiplication binary operators come from known rings, being restricted to some subset. Thus, many of the ring axioms will automatically be inherited to hold true (when restricted to a smaller set of elements), and so need not be checked.

3. For each of the number systems of Exercise 1 that was found to be a ring, determine whether it is a field.

4. For each of the number systems of Exercise 2 that was found to be a ring, determine whether it is a field.

5. (a) Let $\mathbb{Z}_2^3$ be the set of all length-3 binary vectors, and let addition and multiplication operations be defined by using the corresponding $\mathbb{Z}_2$ operations on the separate components:

$[a,b,c]+[a',b',c']=[a+a' \pmod 2,\ b+b' \pmod 2, c+c' \pmod 2]$
$[a,b,c]\cdot[a',b',c']=[a\cdot a' \pmod 2,\ b\cdot b' \pmod 2, c\cdot c' \pmod 2]$

Notice that addition simply XORs the vectors. For example, $[1,0,1]+[1,1,0]=[0,1,1]$ and $[1,0,1]\cdot[1,1,0]=[1,0,0]$.

(b) Show that $\mathbb{Z}_2{}^3$ is a ring.
(c) Extend the result of part (a) to $\mathbb{Z}_2{}^k$, the set of all length-k binary vectors, where $k > 1$ is an integer.
(d) Does the result of part (a) continue to hold true for $\mathbb{Z}_n{}^k$, the set of all length-k vectors of entries in $\mathbb{Z}_n$, where $k, n > 1$ are integers (and addition and multiplication of vectors is defined using the corresponding $\mathbb{Z}_n$ operations on the separate components)?

6. Refer back to the definitions and notation of Exercise 5.
(a) Construct a multiplication table for $\mathbb{Z}_2{}^3$. Identify the set of invertible elements $(\mathbb{Z}_2{}^3)^\times$, and explain why $\mathbb{Z}_2{}^3$ is not a field.
(b) Identify the set of invertible elements $(\mathbb{Z}_2{}^k)^\times$ when $k > 1$ is an integer.
(c) In the case $k, n > 1$ are integers and $\mathbb{Z}_n{}^k$, determine the corresponding set of invertible elements $(\mathbb{Z}_n{}^k)^\times$.

7. Perform the indicated polynomial additions:
(a) $(X^5+X^3+1)+(X^3+X+1)$ in $\mathbb{Z}_2[X]$
(b) $(4X^3+3X^2+9)+(8X^3+5X+5)$ in $\mathbb{Z}_{11}[X]$
(c) $(4X^3+3X^2+2X+1)+(3X^3+5X+5)$ in $\mathbb{Z}_7[X]$

8. Perform the indicated polynomial additions:
(a) $(X^5+X^3+X^2+X+1)+(X^3+X^2+X+1)$ in $\mathbb{Z}_2[X]$
(b) $(4X^3+3X^2+6)+(5X^3+5X+5)$ in $\mathbb{Z}_7[X]$
(c) $(2X^3+X^2+2)+(2X^3+2X+1)$ in $\mathbb{Z}_3[X]$

9. Perform the indicated polynomial multiplications:
(a) $(X^5+X^3+1)\cdot(X+1)$ in $\mathbb{Z}_2[X]$
(b) $(4X^3+3X^2+9)\cdot(8X^3+5X)$ in $\mathbb{Z}_{11}[X]$
(c) $(4X^3+3X^2+1)\cdot(3X^3+5X+5)$ in $\mathbb{Z}_7[X]$

10. Perform the indicated polynomial multiplications:
(a) $(X^5+X^3+X^2+X+1)\cdot(X^2+1)$ in $\mathbb{Z}_2[X]$
(b) $(4X^3+6)\cdot(5X^3+5X+5)$ in $\mathbb{Z}_7[X]$
(c) $(2X^3+X^2+2)\cdot(2X^3+2X+1)$ in $\mathbb{Z}_3[X]$

11. Use the division algorithm (Algorithm 10.1) to perform the indicated polynomial divisions:
(a) $X^5+X^3+X^2+1 \div X^2+1$ in $\mathbb{Z}_2[X]$
(b) $X^4+X^3+X^2+1 \div X+1$ in $\mathbb{Z}_2[X]$
(c) $X^5+4X^2+7X \div X^2+2X$ in $\mathbb{Z}_{11}[X]$
(d) $X^5+2X^2+1 \div 2X^2+1$ in $\mathbb{Z}_3[X]$

12. Use the division algorithm (Algorithm 10.1) to perform the indicated polynomial divisions:
    (a) $X^5 + X^3 + X^2 + 1 \div X + 1$ in $\mathbb{Z}_2[X]$
    (b) $X^6 + X^3 + X^2 + 1 \div X^3 + 1$ in $\mathbb{Z}_2[X]$
    (c) $X^5 + 5X^2 + 6 \div X^2 + 4X$ in $\mathbb{Z}_5[X]$
    (d) $X^5 + 3X^2 + 2 \div 2X^2 + 1$ in $\mathbb{Z}_5[X]$

13. (a) Use Algorithm 10.2 to determine whether the polynomial $X^3 + X^2 + 1$ is irreducible in $\mathbb{Z}_2[X]$.
    (b) Use Algorithm 10.2 to determine whether the polynomial $X^5 + X^4 + X^2 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$.

14. (a) Use Algorithm 10.2 to determine whether the polynomial $X^3 + X^2 + 1$ is irreducible in $\mathbb{Z}_2[X]$.
    (b) Use Algorithm 10.2 to determine whether the polynomial $X^4 + X^3 + 1$ is irreducible in $\mathbb{Z}_2[X]$.

15. (a) Find a polynomial in $\mathbb{Z}_2[X]$ of degree less than 6 that is congruent to $X^{10} + X^9 + 1 \pmod{X^6 + X^3 + X^2 + 1}$.
    (b) Find a polynomial in $\mathbb{Z}_7[X]$ of degree less than 4 that is congruent to $X^6 + 2X^4 + 3X \pmod{X^4 + 5X + 1}$.

16. (a) Find a polynomial in $\mathbb{Z}_2[X]$ of degree less than 4 that is congruent to $X^8 + X^4 + X \pmod{X^4 + X^2 + 1}$.
    (b) Find a polynomial in $\mathbb{Z}_5[X]$ of degree less than 4 that is congruent to $X^6 + 2X^4 + 3X \pmod{X^4 + 3X^3 + 1}$.

17. (a) Is the ring $\mathbb{Z}_3[X] \pmod{X^3 + X + 1}$ a field? Explain your answer.
    (b) Compute $(2X^2 + X + 2) + (2X + 1)$ and $(2X^2 + X + 2) \cdot (2X + 1)$ in $\mathbb{Z}_3[X] \pmod{X^3 + X + 1}$.

18. (a) Is the ring $\mathbb{Z}_3[X] \pmod{X^3 + X^2 + X + 1}$ a field? Explain your answer.
    (b) Compute $(2X^2 + X + 2) + (2X + 1)$ and $(2X^2 + X + 2) \cdot (2X + 1)$ in $\mathbb{Z}_3[X] \pmod{X^3 + X^2 + X + 1}$.

19. Using hex notation, perform the following computations in *GF*(256):
    (a) `E1+24`
    (b) 12^2
    (c) `4D·(C7+1F)`

20. Using hex notation, perform the following computations in *GF*(256):
    (a) `74+AE`
    (b) $0F^2$
    (c) `CD·(CE+F5)`

21. Use the polynomial Euclidean algorithm to determine whether the following inverses exist. In cases where an inverse exists, find it.
    (a) The element $X+1$ in $\mathbb{Z}_2[X] \pmod{X^2}$
    (b) The element $X+1$ in $\mathbb{Z}_3[X] \pmod{X^3+X+1}$
    (c) The element 9 in $GF(16)$
    (d) The element 1D in $GF(256)$

22. Use the polynomial Euclidean algorithm to determine whether the following inverses exist. In cases where an inverse exists, find it.
    (a) The element $X+1$ in $\mathbb{Z}_3[X] \pmod{X^2}$
    (b) The element $X+1$ in $\mathbb{Z}_3[X] \pmod{X^3+X^2+X+1}$
    (c) The element C in $GF(16)$
    (d) The element 2E in $GF(256)$

23. Prove parts (2), (3), and (5) of Proposition 10.1.

24. Prove Theorem 10.4.

25. *Roots of Polynomials in* $\mathbb{Z}_p[X]$. We say that a modular integer $r \in \mathbb{Z}_p$ is a *root* (or a *zero*) of a polynomial $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}_p[X]$ if $f(r) \triangleq \sum_{i=0}^{n} a_i r^i \equiv 0 \pmod{m}$.
    (a) Find all roots of the following polynomials:
        (i) X^3+X^2+X+1 in $\mathbb{Z}_2[X]$
        (ii) X^3+2X^2+2X+1 in $\mathbb{Z}_3[X]$
        (iii) X^3+2X^2+2X+1 in $\mathbb{Z}_5[X]$
        (iv) X^5+2X^2+4X+1 in $\mathbb{Z}_7[X]$
    (b) Show that $r \in \mathbb{Z}_p$ is a *root* (or a *zero*) of a polynomial $f \in \mathbb{Z}_p[X]$ if, and only if, $X-r$ is a factor of f. Thus, a polynomial $f \in \mathbb{Z}_p[X]$ of degree at least 2 that has a root $r \in \mathbb{Z}_p$ cannot be irreducible.
    (c) Use the result of part (b) to obtain any partial factorizations of the polynomials given in part (a) that are obtainable from roots.

26. (a) Suppose that $m \in \mathbb{Z}_p[X]$ is a polynomial of positive degree and that $f_1, f_2, g_1, g_2 \in \mathbb{Z}_p[X]$ are polynomials that satisfy $f_1 \equiv f_2, g_1 \equiv g_2 \pmod{m}$. Show that (i) $f_1 + f_2 \equiv g_1 + g_2 \pmod{m}$, and that (ii) $f_1 \cdot f_2 \equiv g_1 \cdot g_2 \pmod{m}$,
    (b) Prove Theorem 10.7.

27. *Integral Domains.* A ring R is called an *integral domain* if the product of two nonzero elements is always nonzero, i.e., $a, b \in R, a \neq 0, b \neq 0 \Rightarrow ab \neq 0$. Note that the ring $\mathbb{Z}$ of integers is an example of an integral domain.
    (a) Show that a field is always an integral domain.
    (b) For which positive integers $n > 1$ is the ring of modular integers $\mathbb{Z}_n$ an integral domain?
    (c) If p is a prime, is $\mathbb{Z}_p[X]$ an integral domain?
    (d) Show that if m is a nonconstant polynomial in $\mathbb{Z}_p[X]$, where p is a prime, then the ring $\mathbb{Z}_p[X] \pmod{m}$ is an integral domain if, and only if, m is irreducible in $\mathbb{Z}_p[X]$.

28. *Products of Rings.*
   (a) Suppose that $R=(R,+_R,\cdot_R)$ and $S=(S,+_S,\cdot_S)$ are rings. We let $R\times S$ be the set of all vectors $[r,s]$, where $r\in R$ and $s\in S$, and define addition and multiplication on $R\times S$ componentwise: $[r,s]+[r',s']=[r+_R r',s+_S s']$, $[r,s]\cdot[r',s']=[r\cdot_R r',s\cdot_S s']$. Show that $R\times S$ is a ring; it is called the product ring of the rings R and S.
   (b) If, in part (a), both R and S are fields, is their product ring $R\times S$ also a field? Explain your answer.

29. Suppose that R is a ring with at least two elements. Is it possible to have $1=0$ (i.e., for the additive and multiplicative identity to coincide)? Either provide an example showing this is possible or carefully use the ring axioms to prove that such an example is not possible.

   Note: Exercise 1(a) shows it to be possible if R has just one element.

30. Show that -1 has a square root modulo a prime p if, and only if, $p\equiv 1 \pmod 4$.

   Suggestion: Let g be a primitive root mod p. By Euler's theorem and Proposition 8.6, it follows that $g^{(p-1)/2}\equiv -1$. If a is a square root of -1, write $a\equiv g^j$, and obtain $g^{2j}\equiv g^{(p-1)/2} \pmod p$. Use Proposition 8.5(c).

31. *Ben-Or's Irreducibility Determination Algorithm for Polynomials in $\mathbb{Z}_p[X]$.* The following is an efficient algorithm for checking irreducibility of polynomials in $\mathbb{Z}_p[X]$. It can be used in place of Algorithm 10.2 for checking irreducibility of higher degree polynomials. See Theorem 3.20 of [LiNi-86] for a proof of its correctness.
   (a) Use Ben Or's algorithm to redo Exercise 13.
   (b) Use Ben Or's algorithm to show that the polynomial $m=X^8+X^4+X^3+X+1$, that was used in the construction of $GF(256)$, is irreducible in $\mathbb{Z}_2[X]$.

Algorithm 10.3: Ben Or's Irreducibility Test

Input: A polynomial $f\in\mathbb{Z}_p[X]$, of degree at least 2 that we suspect might be irreducible.

Output: Either a nontrivial factor of f (showing that it is not irreducible) or a statement that f is irreducible.

Step 1. Initialize the index $i=1$, and the test polynomial $h=X^p$.

Step 2. Compute the polynomial $H\triangleq h-X \pmod f$, and then use the polynomial Euclidean algorithm to compute $g\triangleq \gcd(f,H)$. If g is a nonconstant polynomial, output g as a nontrivial factor of f and exit the algorithm.

Step 3. Update $i \to i + 1$. If this new value of i is greater than floor(deg(f) / 2), declare f as irreducible and exit the algorithm; otherwise, update $h \to h^p (= X^{p^i})$ and return to Step 2.

31. $\mathbb{Z}_n[X]$. Suppose that, in Definition 10.5 of modular polynomials, we allow the modulus to be any integer $n > 1$, rather than a prime. The resulting systems $\mathbb{Z}_n[X]$ that arise satisfy some but not all of the properties of $\mathbb{Z}_p[X]$. This exercise elaborates on some similarities and differences.
    (a) Show that Proposition 10.3 will never hold for $\mathbb{Z}_n[X]$, if $n > 1$ is composite.
    (b) Show that $\mathbb{Z}_n[X]$ is a ring (i.e., Theorem 10.4 continues to hold).
    (c) Does the division algorithm (Proposition 10.6) hold in $\mathbb{Z}_n[X]$?
    (d) If $n > 1$ is composite, show that $\mathbb{Z}_n[X]$ is never an integral domain (see Exercise 27).

32. Prove Proposition 10.6.

Chapter 10 Computer Implementations and Exercises

Computer Storage and Arithmetical Operations on Polynomials. As pointed out in the text, vectors of coefficients are very efficient means for storing and manipulating polynomials on computers. The basic storage strategy is as follows:

Polynomial in $\mathbb{Z}_p[X]$	Vector of integers mod p
$a_n X^n + a_{n-1} X^{n-1} + \cdots a_1 X + a_0$	$[a_n, a_{n-1}, \cdots, a_1, a_0]$

1. *Program for Polynomial Addition in $\mathbb{Z}_p[X]$.*
    (a) Write a program with syntax `Answer=ZpPolyAdd(px, qx, p)` that will add two polynomials mod p (i.e., in $\mathbb{Z}_p[X]$). The first two inputs, `px` and `qx`, are vectors representing the polynomials to be added, and the third input variable is the modulus `p`. The output, `Answer`, is a vector representing the sum of the inputted polynomials. If the sum is the zero polynomial, the output should be [0]; otherwise, the output should have a nonzero first component (so that the degree of the sum is one less than the length of the output vector).
    (b) Run your program on the polynomial additions of Chapter Exercise 7.

2. *Program for Polynomial Multiplication in $\mathbb{Z}_p[X]$.*
    (a) Write a program with syntax `Answer=ZpPolyMult(px, qx, p)` that will multiply two polynomials mod p (i.e., in