Appendices to Quadratic Number Theory

J. L. Lehman

Contents

APPENDIX A

Number Systems

Throughout the text, we assume various familiar properties of addition, multiplication, and order within the set of integers, and in several other number systems. In Appendix A, we outline a construction of the integers, rational numbers, real numbers, and complex numbers by which these properties can be established as theorems.

Natural Numbers from Sets

To begin this development, we assume no knowledge of integers or any other type of numbers. We demonstrate that we can define a set with all the properties of the nonnegative integers using only the existence of the null set and other sets that can be constructed from the null set. (A more complete and precise development would require listing the axioms of set theory that we assume in this process.)

DEFINITION. Let $\mathbb{N}$ be a collection of sets that has the following properties.

(1) The null set, $\varnothing$, is an element of $\mathbb{N}$.
(2) If a set a is an element of $\mathbb{N}$, then there is a set $S(a) = a \cup \{a\}$ in $\mathbb{N}$.
(3) If M is a subset of $\mathbb{N}$ with the properties that (i) $\varnothing \in M$, and (ii) $a \in M$ implies that $S(a) \in M$, then M equals the set $\mathbb{N}$.

We call $\mathbb{N}$ the set of *natural numbers*.

The elements of $\mathbb{N}$ are sets, but we denote them by small letters to make it easier to distinguish between elements of $\mathbb{N}$ and subsets of $\mathbb{N}$. If a is in $\mathbb{N}$, we refer to $S(a)$ as the *successor* of a. Notice that $x \in S(a)$ if and only if either $x \in a$ or $x = a$, so that $a \subseteq S(a)$ and $a \in S(a)$ are both true statements.

Although we assume no properties of integers, it may be illuminating to index the elements of $\mathbb{N}$ as follows.

(1) We write $\varnothing$ alternatively as a_0.
(2) Then $S(a_0)$ equals $\varnothing \cup \{\varnothing\} = \{\varnothing\} = \{a_0\}$. Notice that this is not equal to the null set, since this set contains one element, namely a_0. We write $S(a_0)$ as a_1.
(3) Now $S(a_1) = a_1 \cup \{a_1\} = \{a_0\} \cup \{a_1\} = \{a_0, a_1\}$. We write $S(a_1)$ as a_2.
(4) So then $S(a_2) = a_2 \cup \{a_2\} = \{a_0, a_1\} \cup \{a_2\} = \{a_0, a_1, a_2\}$. We write $S(a_2)$ as a_3.

Continuing in this way, we see that $S(a_n) = \{a_0, a_1, \ldots, a_n\}$, and we index this set by the digit or sequence of digits traditionally used for $n + 1$. Eventually, we will replace the symbol a_n by n, but for now, we continue to regard these objects as sets.

Order Relation on Natural Numbers. Subset inclusion provides a partial order relation on the elements of $\mathbb{N}$. We first explore some properties of this relation.

PROPOSITION A.1. *Every element of* $\mathbb{N}$ *aside from* $\varnothing$ *is the successor of some element of* $\mathbb{N}$.

PROOF. The null set $\varnothing$ cannot be the successor of any $b \in \mathbb{N}$ since $S(b)$ contains b as an element, while $\varnothing$ contains no elements. Now consider the set $M = \{\varnothing\} \cup \{S(b) \mid b \in \mathbb{N}\}$, a subset of $\mathbb{N}$.

Note that $\varnothing$ is an element of M, and if a is in M, then $S(a)$ is in M by definition, since $a \in \mathbb{N}$. Therefore, $M = \mathbb{N}$ by condition (3) in the definition of $\mathbb{N}$, and so every element of $\mathbb{N}$ except $\varnothing$ is the successor of some element of $\mathbb{N}$. □

Our next result compiles some useful statements for later proofs.

LEMMA A.2. *Let a and b be elements of $\mathbb{N}$. Then the following statements are true.*

(1) *If $a \in b$, then $a \subseteq b$.*
(2) *If $a \in S(b)$, then $a \subseteq b$.*
(3) *If $a \in b$, then $S(a) \subseteq b$.*
(4) *If $a \subseteq S(b)$ and $a \not\subseteq b$, then $a = S(b)$.*

PROOF. To prove statement (1), we let a be a fixed element of $\mathbb{N}$ and define M to be the set of all b in $\mathbb{N}$ for which the statement "if $a \in b$, then $a \subseteq b$" is true. Note that $\varnothing$ is in M since a cannot be an element of $\varnothing$, and an implication with a false hypothesis is true by definition. Then if b is an element of M, we will show that $S(b)$ must also be in M. Note that $b \in M$ if and only if $a \notin b$ or $a \subseteq b$. We want to show that, under this assumption, either $a \notin S(b)$ or $a \subseteq S(b)$. If $a \subseteq b$, then $a \subseteq S(b)$, since b is a subset of $S(b)$. So suppose instead that $a \notin b$. If $a \notin S(b)$ also, we are done, so assume that $a \in S(b)$. But the only element of $S(b) = b \cup \{b\}$ that is not also an element of b is the set b itself, so it follows that $a = b$. In that case, $a \subseteq S(b)$. Therefore, $M = \mathbb{N}$ by definition, and we conclude that statement (1) is true for all a and b in $\mathbb{N}$.

For statement (2), suppose that $a \in S(b) = b \cup \{b\}$. By definition, either $a \in b$ or $a = b$. But if $a \in b$, then $a \subseteq b$ by statement (1), while if $a = b$, then $a \subseteq b$ by standard properties of sets. So $a \subseteq b$ in any case.

For statement (3), assume that $a \in b$. Then $a \subseteq b$ by statement (1). Since each element of a is in b, and a itself is an element of b, then $S(a) = a \cup \{a\} \subseteq b$.

Finally, for statement (4), suppose that $a \in \mathbb{N}$ is a subset of $S(b)$, but not of b. Then there is an element in a that is not in b. Since any such element must be in $S(b) = b \cup \{b\}$, we conclude that $b \in a$. But then $S(b) \subseteq a$ by statement (3), and since we are given that $a \subseteq S(b)$, it follows that $a = S(b)$. □

PROPOSITION A.3. *For all $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$.*

PROOF. Let a and b be elements of $\mathbb{N}$ and assume that $S(a) = S(b)$. Since $a \in S(a)$ and $b \in S(b)$, then $a \in S(b)$ and $b \in S(a)$. But then statement (2) of Lemma A.2 implies that $a \subseteq b$ and $b \subseteq a$, so that $a = b$. □

COROLLARY A.4. *For all $a \in \mathbb{N}$, $a \neq S(a)$. Equivalently, $a \notin a$ for all $a \in \mathbb{N}$.*

PROOF. Let M be the set of all a in $\mathbb{N}$ for which $a \neq S(a)$. Then $\varnothing \in M$, since, as noted earlier, $S(\varnothing)$ contains $\varnothing$ as an element, while $\varnothing$ contains no elements. Now if $S(a) = S(S(a))$, then $a = S(a)$ follows immediately from Proposition A.3. So if $S(a) \notin M$, then $a \notin M$, or equivalently, if $a \in M$, then $S(a) \in M$. Thus $M = \mathbb{N}$, and $a \neq S(a)$ for all a in $\mathbb{N}$. Note that $S(a) = a \cup \{a\} = a$ if and only if a is an element of a, so the second claim of this corollary is also established. □

PROPOSITION A.5. *Let a and b be elements of $\mathbb{N}$. If $a \subseteq b$ and $a \neq b$, then $S(a) \subseteq b$.*

PROOF. Let a be a fixed element of $\mathbb{N}$ and let M be the set of all b for which the statement "if $a \subseteq b$ and $a \neq b$, then $S(a) \subseteq b$" is true. Using logical equivalences, we can also write

$$M = \{b \in \mathbb{N} \mid S(a) \subseteq b \text{ or } a = b \text{ or } a \not\subseteq b\}.$$

Note that $\varnothing \in M$, since either $a = \varnothing$ or $a \not\subseteq \varnothing$. Now we show that if b is in M, then $S(b)$ is in M. If $S(a) \subseteq b$, then since $b \subseteq S(b)$, we conclude that $S(a) \subseteq S(b)$. If $a = b$, then $S(a) = S(b)$, so

that, in particular, $S(a) \subseteq S(b)$. Finally, if $a \not\subseteq b$, then either $a \not\subseteq S(b)$, or $a = S(b)$ by part (4) of Lemma A.2. So if $b \in M$, then in any case, one of the three statements $a \not\subseteq S(b)$, $a = S(b)$, or $S(a) \subseteq S(b)$ must be true, and so $S(b)$ is in M. □

We are now in a position to prove our main results concerning order in the set $\mathbb{N}$.

THEOREM A.6. *For all $a, b \in \mathbb{N}$, either $a \subseteq b$ or $b \subseteq a$.*

PROOF. Let a be a fixed element of $\mathbb{N}$ and let $M = \{b \in \mathbb{N} \mid a \subseteq b \text{ or } b \subseteq a\}$. Then $\varnothing \in M$ since $\varnothing \subseteq a$ is true for every set a. So now let b be some element of $\mathbb{N}$ for which either $a \subseteq b$ or $b \subseteq a$ is true. If $a \subseteq b$, then $a \subseteq S(b)$ follows immediately. If $a \not\subseteq b$, then $b \subseteq a$ but $b \neq a$, and Proposition A.5 implies that $S(b) \subseteq a$. So $b \in M$ implies that $S(b) \in M$, and so $M = \mathbb{N}$. □

Theorem A.6 shows that the partial order relation of set inclusion is a total order relation on $\mathbb{N}$. We now use the notation $a \leq b$ (or $b \geq a$) interchangeably with $a \subseteq b$ when $a, b \in \mathbb{N}$. If $a \leq b$ and $a \neq b$, we write $a < b$ (or $b > a$). Proposition A.5 and Corollary A.4 imply that this is equivalent to the statement that $S(a) \leq b$.

COROLLARY A.7 (Trichotomy Property). *For all $a, b \in \mathbb{N}$, exactly one of the following statements is true: $a < b$, $b < a$, or $a = b$.*

PROOF. This follows from the result that set containment is a total order relation on $\mathbb{N}$. □

THEOREM A.8 (Well-Ordering Principle). *Every nonempty subset of $\mathbb{N}$ has a least element. That is, if $T \subseteq \mathbb{N}$ and $T \neq \varnothing$, then there is an element a in T such that $a \leq b$ for all b in T.*

PROOF. Let T be a subset of $\mathbb{N}$, and consider the set $M = \{a \in \mathbb{N} \mid a \leq b \text{ for all } b \in T\}$. Notice that a common element of M and T must be a least element of T by definition, so suppose instead that $M \cap T = \varnothing$. We show that under this assumption, $M = \mathbb{N}$. First note that $\varnothing \in M$ since $\varnothing \leq b$ (that is, $\varnothing \subseteq b$) for all b in T. Now let a be an element in M, so that $a \leq b$ for all $b \in T$. Since we assume that $a \notin T$, we can say that $a < b$ for all $b \in T$. But then Proposition A.5 implies that $S(a) \leq b$ for all b in T, so that $S(a) \in M$. Thus $M = \mathbb{N}$, and so T is empty. We conclude that a nonempty subset of $\mathbb{N}$ must have a least element. □

Addition of Natural Numbers. We can use the definition of $\mathbb{N}$ in terms of successors to define operations on $\mathbb{N}$ recursively.

PROPOSITION A.9. *We can define an operation of addition on $\mathbb{N}$ by saying that for all $a, b \in \mathbb{N}$,*

(1) $a + \varnothing = a$,
(2) $a + S(b) = S(a + b)$.

PROOF. For a fixed a in $\mathbb{N}$, let M be the set of all $b \in \mathbb{N}$ for which $a + b$ is an element of $\mathbb{N}$. Condition (1) implies that $\varnothing$ is in M, and condition (2) implies that if b is in M, then $S(b)$ is in M. So $M = \mathbb{N}$, and addition is thus an operation on $\mathbb{N}$. □

In proofs below, we will refer to conditions (1) and (2) of Proposition A.9 as (A1) and (A2) respectively.

EXAMPLE. Since $a_2 = S(a_1)$, we have that $a_3 + a_2 = S(a_3 + a_1)$ by (A2). Similarly, since $a_1 = S(a_0)$, then $a_3 + a_1 = S(a_3 + a_0) = S(a_3 + \varnothing) = S(a_3)$ by (A2) and (A1). So $a_3 + a_2 = S(S(a_3)) = S(a_4) = a_5$. ◊

In the following propositions, we establish the main algebraic properties of addition in $\mathbb{N}$.

LEMMA A.10. *For all a in $\mathbb{N}$, $\varnothing + a = a$.*

PROOF. Let M be the set of all $a \in \mathbb{N}$ for which $\varnothing + a = a$. Then $\varnothing \in M$, since $\varnothing + \varnothing = \varnothing$ by (A1). Now let a be in M. Then $\varnothing + S(a) = S(\varnothing + a) = S(a)$ by (A2) and the assumption that $a \in M$. So $M = \mathbb{N}$ and $\varnothing + a = a$ for all $a \in \mathbb{N}$. □

In future proofs of this type, rather than explicitly defining a subset M of $\mathbb{N}$, we will speak of proving a statement about all $a \in \mathbb{N}$ by *induction*. By this, we mean that the statement is true when $\varnothing$ is substituted for a, and that under the assumption (called the *inductive hypothesis*) that the statement is true for some $a \in \mathbb{N}$, it is also true with $S(a)$ in place of a.

LEMMA A.11. *For every a and b in $\mathbb{N}$, $S(a) + b = S(a + b)$.*

PROOF. Let a be an element of $\mathbb{N}$ and proceed by induction on b. First note that

$$S(a) + \varnothing = S(a) = S(a + \varnothing),$$

both equations by (A1). Now suppose that $S(a) + b = S(a + b)$ for some b in $\mathbb{N}$. Then

$$\begin{array}{rcll} S(a) + S(b) & = & S(S(a) + b) & \text{by (A2)} \\ & = & S(S(a + b)) & \text{by the inductive hypothesis} \\ & = & S(a + S(b)) & \text{by (A2).} \end{array}$$

So by induction, $S(a) + b = S(a + b)$ for all a and b in $\mathbb{N}$. □

PROPOSITION A.12. *Addition is commutative on $\mathbb{N}$. That is, $a + b = b + a$ for all $a, b \in \mathbb{N}$.*

PROOF. We let a be a fixed element of $\mathbb{N}$ and use induction on b. First note that

$$a + \varnothing = a = \varnothing + a$$

by (A1) and Lemma A.10. Now suppose that $a + b = b + a$ for some element $b \in \mathbb{N}$. Then

$$\begin{array}{rcll} a + S(b) & = & S(a + b) & \text{by (A2)} \\ & = & S(b + a) & \text{by the inductive hypothesis} \\ & = & S(b) + a & \text{by Lemma A.11.} \end{array}$$

Thus addition is commutative by induction. □

PROPOSITION A.13. *Addition is associative on $\mathbb{N}$. That is, $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{N}$.*

PROOF. We let a and b be fixed elements of $\mathbb{N}$ and use induction on c. First note that

$$a + (b + \varnothing) = a + b = (a + b) + \varnothing,$$

both equations by (A1). Suppose now that $a + (b + c) = (a + b) + c$ for some $c \in \mathbb{N}$. Then $a + (b + S(c)) = a + S(b + c) = S(a + (b + c))$, while $(a + b) + S(c) = S((a + b) + c)$, all equations by (A2). These two are equal under the inductive hypothesis. Thus addition is associative. □

PROPOSITION A.14. *Addition has the following cancellation property: For all $a, b, c \in \mathbb{N}$, if $a + c = b + c$, then $a = b$.*

PROOF. Again we use induction on c. First note that if $a + \varnothing = b + \varnothing$, then $a = b$ is true since $a + \varnothing = a$ and $b + \varnothing = b$ by (A1). Suppose now that for some $c \in \mathbb{N}$, the assumption that $a + c = b + c$ implies that $a = b$. Then suppose that $a + S(c) = b + S(c)$. By (A2), it follows that $S(a + c) = S(b + c)$, so that $a + c = b + c$ by Proposition A.3. But then we must conclude that $a = b$ by the inductive hypothesis. So the cancellation property holds for all a, b, and c in $\mathbb{N}$. □

PROPOSITION A.15. *If a and b are elements of $\mathbb{N}$, then $a \leq b$ if and only if there is an element $c \in \mathbb{N}$ such that $a + c = b$.*

PROOF. We first show that $a \leq a + c$ for all $c \in \mathbb{N}$. If $c = \varnothing$, then $a + c = a \geq a$. Suppose for some $c \in \mathbb{N}$ that $a \leq a + c$. Then $a + S(c) = S(a + c) \geq a + c \geq a$. (As usual, $a + c$ is a subset of its successor $S(a + c)$.) The result follows by induction on c.

For the converse, we use induction on b. The statement "If $a \leq b$, then there is a $c \in \mathbb{N}$ such that $a + c = b$" is vacuously true when $b < a$, so we begin the induction process with the case in which $b = a$. But in that case, we can let $c = \varnothing$ since $a + \varnothing = a$ by (A1).

So now suppose that for some b with $a \leq b$, we know that $a + c = b$ for some $c \in \mathbb{N}$. We want to establish the existence of a $d \in \mathbb{N}$ such that $a + d = S(b)$. But $S(b) = S(a + c) = a + S(c)$ by (A2). Thus we can let $d = S(c)$. □

Multiplication of Natural Numbers. Now we can define multiplication of natural numbers recursively as follows. (As in Proposition A.9, induction shows that these conditions define an operation on $\mathbb{N}$.)

DEFINITION. We define an operation of *multiplication* on $\mathbb{N}$ by saying that for all $a, b \in \mathbb{N}$,

(1) $a \cdot \varnothing = \varnothing$,
(2) $a \cdot S(b) = a \cdot b + a$.

We refer to the conditions (1) and (2) of this definition as (M1) and (M2) respectively. In most proofs of the properties of multiplication, we will apply the algebraic properties of addition established above without step-by-step explanations.

EXAMPLE. Since $a_2 = S(a_1)$, we have that $a_3 \cdot a_2 = a_3 \cdot S(a_1) = a_3 \cdot a_1 + a_3$ by (M2). Likewise, since $a_1 = S(a_0)$, then $a_3 \cdot a_1 = a_3 \cdot S(a_0) + a_3 = a_3 \cdot S(\varnothing) + a_3 = (a_3 \cdot \varnothing + a_3) + a_3 = (\varnothing + a_3) + a_3 = a_3 + a_3$, using (M2), (M1), and properties of addition. Note that $a_3 + a_3 = a_3 + S(a_2) = S(a_3 + a_2) = S(a_5) = a_6$, using a previous example. So $a_3 \cdot a_2 = a_6$. ◊

LEMMA A.16. *For all $a, b \in \mathbb{N}$, we have that $\varnothing \cdot a = \varnothing$ and $S(a) \cdot b = a \cdot b + b$.*

PROOF. By (M1), $\varnothing \cdot \varnothing = \varnothing$. Assuming that $\varnothing \cdot a = \varnothing$ for some a in $\mathbb{N}$, then

$$\begin{aligned} \varnothing \cdot S(a) &= \varnothing \cdot a + \varnothing && \text{by (M2)} \\ &= \varnothing + \varnothing && \text{by the inductive hypothesis} \\ &= \varnothing && \text{by (A1).} \end{aligned}$$

So $\varnothing \cdot a = \varnothing$ for all $a \in \mathbb{N}$ by induction.

Now let a be a fixed element of $\mathbb{N}$. First note that $S(a) \cdot \varnothing = \varnothing = a \cdot \varnothing + \varnothing$, using (M1) and properties of addition. Suppose now that $S(a) \cdot b = a \cdot b + b$ for some $b \in \mathbb{N}$. Then

$$\begin{aligned} S(a) \cdot S(b) &= S(a) \cdot b + S(a) && \text{by (M2)} \\ &= (a \cdot b + b) + S(a) && \text{by the inductive hypothesis} \\ &= a \cdot b + S(a + b) && \text{by properties of addition} \\ &= (a \cdot b + a) + S(b) && \text{by properties of addition} \\ &= a \cdot S(b) + S(b) && \text{by (M2)} \end{aligned}$$

which shows by induction that $S(a) \cdot b = a \cdot b + b$ for all $a, b \in \mathbb{N}$. □

PROPOSITION A.17. *Mulitplication is commutative on $\mathbb{N}$. That is, $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{N}$.*

PROOF. We fix a in $\mathbb{N}$ and use induction on b. First we have that $a \cdot \varnothing = \varnothing = \varnothing \cdot a$ by (M1) and Lemma A.16. Now assuming that $a \cdot b = b \cdot a$ for some b in $\mathbb{N}$, we have that $a \cdot S(b) = a \cdot b + a$ by (M2), while $S(b) \cdot a = b \cdot a + a$ by Lemma A.16. Thus under the assumption that $a \cdot b = b \cdot a$, it follows that $a \cdot S(b) = S(b) \cdot a$. So multiplication is commutative for all $a, b \in \mathbb{N}$ by induction. □

PROPOSITION A.18. *Multiplication is distributive over addition on $\mathbb{N}$. That is, $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{N}$.*

PROOF. We use induction on a. First note that $\varnothing \cdot (b+c) = \varnothing = \varnothing + \varnothing = \varnothing \cdot b + \varnothing \cdot c$, by Lemma A.16 and properties of addition. Now suppose for some a that $a \cdot (b+c) = a \cdot b + a \cdot c$. Then

$$\begin{aligned} S(a) \cdot (b+c) &= a \cdot (b+c) + (b+c) && \text{by Lemma A.16} \\ &= (a \cdot b + a \cdot c) + (b+c) && \text{by the inductive hypothesis} \\ &= (a \cdot b + b) + (a \cdot c + c) && \text{by properties of addition} \\ &= S(a) \cdot b + S(a) \cdot c && \text{by Lemma A.16.} \end{aligned}$$

Thus $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{N}$ by induction. □

PROPOSITION A.19. *Mulitplication is associative on* $\mathbb{N}$. *That is,* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* $a, b, c \in \mathbb{N}$.

PROOF. We use induction on c. First note that $a \cdot (b \cdot \varnothing) = a \cdot \varnothing = \varnothing = (a \cdot b) \cdot \varnothing$ by (M1). Now suppose that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for some $c \in \mathbb{N}$. Then

$$\begin{aligned} a \cdot (b \cdot S(c)) &= a \cdot (b \cdot c + b) && \text{by (M2)} \\ &= a \cdot (b \cdot c) + a \cdot b && \text{by Proposition A.18} \\ &= (a \cdot b) \cdot c + (a \cdot b) && \text{by the inductive hypothesis} \\ &= (a \cdot b) \cdot S(c) && \text{by (M2).} \end{aligned}$$

Thus $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{N}$ by induction. □

PROPOSITION A.20. *The element* $a_1 = S(\varnothing)$ *is the identity element of* $\mathbb{N}$ *under multiplication. That is,* $a \cdot a_1 = a$ *for all* a *in* $\mathbb{N}$.

PROOF. For all $a \in \mathbb{N}$, $a \cdot S(\varnothing) = a \cdot \varnothing + a = \varnothing + a = a$, using (M2), (M1), and Lemma A.10. □

PROPOSITION A.21. *For all* $a, b \in \mathbb{N}$, *if* $a \cdot b = \varnothing$, *then either* $a = \varnothing$ *or* $b = \varnothing$.

PROOF. Suppose that $a \cdot b = \varnothing$, but $b \neq \varnothing$. Then $b = S(c)$ for some element c in $\mathbb{N}$. So $a \cdot b = a \cdot S(c) = a \cdot c + a \geq a$ using (M2) and Proposition A.15. But now $a \subseteq a \cdot b$ under the assumption that $b \neq \varnothing$, and if $a \cdot b = \varnothing$, it follows that $a = \varnothing$. □

PROPOSITION A.22. *Multiplication has the following cancellation property: For all* a, b, *and* c *in* $\mathbb{N}$, *if* $a \cdot b = a \cdot c$ *and* $a \neq \varnothing$, *then* $b = c$.

PROOF. Without loss of generality, we may assume that $b \leq c$. Thus there is some d in $\mathbb{N}$ for which $b + d = c$ by Proposition A.15. So $a \cdot c = a \cdot (b+d) = a \cdot b + a \cdot d$ by Proposition A.18. Now $a \cdot b = a \cdot c$ implies that $a \cdot b + \varnothing = a \cdot b + a \cdot d$, so that $a \cdot d = \varnothing$ by Proposition A.14. Since $a \neq \varnothing$, we conclude that $d = \varnothing$ by Proposition A.21. So then $c = b + d = b + \varnothing = b$, as we wanted to show. □

Thus we see that $\mathbb{N}$ is a set whose elements satisfy addition, multiplication, and order properties that are identical to those that we typically *assume* are true about nonnegative integers. We will now change our notation as follows: Write $\varnothing = a_0$ simply as 0, then $S(a_0) = a_1$ as 1, $S(a_1) = a_2$ as 2, and so forth. Previous examples demonstrate that $3 + 2 = 5$ and $3 \cdot 2 = 6$. We assume in the remainder of Appendix A that all other specific calculations of addition and multiplication are similarly verified.

Integers from Natural Numbers

Let a and b be natural numbers. Propositions A.15 and A.14 imply that if $a \leq b$, then there is a unique solution in $\mathbb{N}$ of the equation $a + x = b$. We may view this value of x as the difference $b - a$. In this section, we extend this concept of subtraction to any pair of elements in $\mathbb{N}$ as a way of defining all integers.

PROPOSITION A.23. *On the set $\mathbb{N} \times \mathbb{N}$, define a relation $\sim$ by saying that $(a, b) \sim (c, d)$ if and only if $a + d = b + c$. The $\sim$ relation is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

PROOF. Let (a, b), (c, d), and (e, f) be elements of $\mathbb{N} \times \mathbb{N}$. Then

(1) $(a, b) \sim (a, b)$ because $a + b = b + a$ by the commutative property of addition in $\mathbb{N}$.
(2) If $(a, b) \sim (c, d)$, so that $a + d = b + c$, then $c + b = d + a$, implying that $(c, d) \sim (a, b)$.
(3) Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, so that $a + d = b + c$ and $c + f = d + e$. Then $(a + d) + f = (b + c) + f$ and $b + (c + f) = b + (d + e)$. Using the commutative and associative properties of addition in $\mathbb{N}$, we find that $(a + f) + d = (b + e) + d$. Then by the cancellation property of addition (Proposition A.14), we conclude that $a + f = b + e$, so that $(a, b) \sim (e, f)$.

Thus the $\sim$ relation is reflexive, symmetric, and transitive on $\mathbb{N} \times \mathbb{N}$. □

DEFINITION. Denote the equivalence class of an element $(a, b) \in \mathbb{N} \times \mathbb{N}$ under the $\sim$ relation as $[a, b]$. Then we define the set of *integers*, $\mathbb{Z}$, to be the set of distinct equivalence classes. That is,

$$\mathbb{Z} = \{[a, b] \mid a, b \in \mathbb{N}\},$$

where $[a, b] = [c, d]$ if and only if $(a, b) \sim (c, d)$, that is, $a + d = b + c$.

EXAMPLE. The set $[5, 2]$ contains all $(c, d) \in \mathbb{N} \times \mathbb{N}$ such that $5 + d = 2 + c$, which we can rewrite as $c = d + 3$. With $d \geq 0$, then

$$[5, 2] = \{(3, 0), (4, 1), (5, 2), (6, 3), (7, 4), \dots\}.$$

By general properties of equivalence classes, we know then that

$$[3, 0] = [4, 1] = [5, 2] = [6, 3] = [7, 4] = \cdots.$$

Similarly, $[1, 5]$ consists of all $(c, d) \in \mathbb{N} \times \mathbb{N}$ for which $1 + d = 5 + c$, or $d = c + 4$. Here we find that

$$[0, 4] = [1, 5] = [2, 6] = [3, 7] = [4, 8] = \cdots,$$

again with infinitely many distinct representations. ◊

Notice that $[5, 2]$ consists of all pairs $(c, d) \in \mathbb{N} \times \mathbb{N}$ for which $c - d = 3$. In a similar way, $[1, 5]$ seems to consist of all $(c, d) \in \mathbb{N} \times \mathbb{N}$ for which $c - d = -4$, although we have yet to define negative numbers. With the tacit understanding that the equivalence class $[a, b]$ corresponds to the difference $a - b$, we can define addition and multiplication on $\mathbb{Z}$ to be consistent with the following algebraic facts: $(a - b) + (c - d) = (a + c) - (b + d)$ and $(a - b)(c - d) = (ac + bd) - (ad + bc)$. But our definitions in the following proposition use only operations that we have defined in $\mathbb{N}$.

PROPOSITION A.24. *Let $[a, b]$ and $[c, d]$ be elements of $\mathbb{Z}$, and define the sum and product of these elements to be*

$$[a, b] + [c, d] = [a + c, b + d] \quad \textit{and} \quad [a, b] \cdot [c, d] = [ac + bd, ad + bc]$$

respectively. These operations of addition and multiplication are well-defined on $\mathbb{Z}$.

We illustrate the definitions of addition and multiplication, and what we mean in saying that these operations are well-defined before proving this proposition.

EXAMPLE. Using operations in $\mathbb{N}$, we find that $[5, 2] + [1, 5] = [5 + 1, 2 + 5] = [6, 7]$ while $[5, 2] \cdot [1, 5] = [5 \cdot 1 + 2 \cdot 5, 5 \cdot 5 + 2 \cdot 1] = [15, 27]$. However, a typical element of $\mathbb{Z}$ can be written in many different ways. For instance, $[5, 2] = [3, 0]$ and $[1, 5] = [0, 4]$. Now we find that $[3, 0] + [0, 4] = [3 + 0, 0 + 4] = [3, 4]$ and $[3, 0] \cdot [0, 4] = [3 \cdot 0 + 0 \cdot 4, 3 \cdot 4 + 0 \cdot 0] = [0, 12]$. But this does not contradict our previous calculations: $[6, 7] = [3, 4]$ since $6 + 4 = 7 + 3$, and $[15, 27] = [0, 12]$ since $15 + 12 = 27 + 0$. ◊

PROOF. First note that by the closure of $\mathbb{N}$ under addition and multiplication, $[a,b]+[c,d]$ and $[a,b]\cdot[c,d]$ are elements of $\mathbb{Z}$ when $[a,b]$ and $[c,d]$ are in $\mathbb{Z}$. To show that these operations are well-defined, we show that if $[a,b]=[e,f]$ and $[c,d]=[g,h]$ in $\mathbb{Z}$, then $[a,b]+[c,d]=[e,f]+[g,h]$ and $[a,b]\cdot[c,d]=[e,f]\cdot[g,h]$. The assumption that $[a,b]=[e,f]$ and $[c,d]=[g,h]$ means that $a+f=b+e$ and $c+h=d+g$. We must show that then $(a+c)+(f+h)=(b+d)+(e+g)$, so that $[a+c,b+d]=[e+g,f+h]$. But using the commutative and associative properties of addition in $\mathbb{N}$, we see that $(a+c)+(f+h)=(a+f)+(c+h)$ while $(b+d)+(e+g)=(b+e)+(d+g)$. These are equal by the assumed equations above.

For multiplication, we will show separately that

$$[a,b]\cdot[c,d]=[a,b]\cdot[g,h] \qquad \text{and} \qquad [a,b]\cdot[g,h]=[e,f]\cdot[g,h].$$

First $[a,b]\cdot[c,d]=[ac+bd,ad+bc]$ while $[a,b]\cdot[g,h]=[ag+bh,ah+bg]$. We find that

$$[ac+bd,ad+bc]=[ag+bh,ah+bg]$$

because $(ac+bd)+(ah+bg)=a(c+h)+b(d+g)=a(d+g)+b(c+h)=(ad+bc)+(ag+bh)$, using the commutative, associative, and distributive properties of addition and multiplication in $\mathbb{N}$ as well as the assumed equations. In a similar way, $[e,f]\cdot[g,h]=[eg+fh,eh+fg]$, and we find that $[ag+bh,ah+bg]=[eg+fh,eh+fg]$ because $(ag+bh)+(eh+fg)=(a+f)g+(b+e)h=(b+e)g+(a+f)h=(ah+bg)+(eg+fh)$. □

We gather the main algebraic properties of addition and multiplication in $\mathbb{Z}$ as the following theorem.

THEOREM A.25. *In $\mathbb{Z}$, the operations of addition and multiplication are commutative and associative, and multiplication is distributive over addition. The element $[0,0]\in\mathbb{Z}$ has the property that $[a,b]+[0,0]=[a,b]$ for all $[a,b]\in\mathbb{Z}$. For any $[a,b]\in\mathbb{Z}$, the element $[b,a]\in\mathbb{Z}$ has the property that $[a,b]+[b,a]=[0,0]$. The element $[1,0]\in\mathbb{Z}$ has the property that $[a,b]\cdot[1,0]=[a,b]$ for all $[a,b]\in\mathbb{Z}$. If $[a,b]\cdot[c,d]=[0,0]$, then either $[a,b]=[0,0]$ or $[c,d]=[0,0]$.*

PROOF. The commutative, associative, and distributive properties are left for Exercise 1 in Appendix A. For all $[a,b]\in\mathbb{Z}$, $[a,b]+[0,0]=[a+0,b+0]=[a,b]$, so that $[0,0]$ has the additive identity property. Notice that for $x,y\in\mathbb{N}$, $[x,y]=[0,0]$ if and only if $x+0=y+0$, that is, $x=y$. Now for any $[a,b]\in\mathbb{Z}$, $[a,b]+[b,a]=[a+b,b+a]=[0,0]$, since $a+b=b+a$ in $\mathbb{N}$. So $[b,a]$ is the additive inverse of $[a,b]$. The element $[1,0]$ has the multiplicative identity property because $[a,b]\cdot[1,0]=[a\cdot1+b\cdot0,a\cdot0+b\cdot1]=[a,b]$ for all $[a,b]\in\mathbb{Z}$.

Finally suppose that $[a,b]\cdot[c,d]=[ac+bd,ad+bc]=[0,0]$ in $\mathbb{Z}$ so that $ac+bd=ad+bc$ in $\mathbb{N}$. We want to show that either $[a,b]=[0,0]$ or $[c,d]=[0,0]$, that is, either $a=b$ or $c=d$. Suppose that $c\neq d$. Then either $c>d$ or $c<d$. In the first case, there is some $x\in\mathbb{N}$ such that $c=d+x$. So now $ac+bd=a(d+x)+bd=(ad+bd)+ax$ while $ad+bc=ad+b(d+x)=(ad+bd)+bx$. Since $ac+bd=ad+bc$, then by cancellation we obtain $ax=bx$. Now $x\neq0$ (otherwise $c=d+x=d$, contrary to our assumption), so by Proposition A.22, we conclude that $a=b$. We draw the same conclusion if $c<d$. So if $[c,d]\neq[0,0]$, we must conclude that $[a,b]=[0,0]$. □

DEFINITION. We refer to $[b,a]$ as the *negative* of $[a,b]$ and write $[b,a]=-[a,b]$.

The following proposition shows that we can treat $\mathbb{N}$ as a subset of $\mathbb{Z}$, in that there is a subset of $\mathbb{Z}$ that has all the properties of addition and multiplication that we established in $\mathbb{N}$.

PROPOSITION A.26. *Define a function $f:\mathbb{N}\to\mathbb{Z}$ by $f(a)=[a,0]$ for all $a\in\mathbb{N}$. Then*

1. *f is one-to-one.*
2. *$f(a+b)=f(a)+f(b)$ for all $a,b\in\mathbb{N}$.*
3. *$f(a\cdot b)=f(a)\cdot f(b)$ for all $a,b\in\mathbb{N}$.*

PROOF. First note that f is a function as defined, since a and 0 are elements of $\mathbb{N}$.

(1) Suppose that $f(a) = f(b)$, that is, $[a, 0] = [b, 0]$ in $\mathbb{Z}$. Then $a + 0 = 0 + b$, that is, $a = b$ in $\mathbb{N}$ by definition of equivalence classes.

(2) $f(a) + f(b) = [a, 0] + [b, 0] = [a + b, 0 + 0] = [a + b, 0] = f(a + b)$ by the definition of f and of addition in $\mathbb{Z}$.

(3) Similarly, $f(a) \cdot f(b) = [a, 0] \cdot [b, 0] = [a \cdot b + 0 \cdot 0, a \cdot 0 + 0 \cdot b] = [a \cdot b, 0] = f(a \cdot b)$. □

We saw in Proposition A.15 that if $b \leq a$ in $\mathbb{N}$, then there is some c in $\mathbb{N}$ so that $a = b + c$. The cancellation property of Proposition A.14 shows that c is unique. Notice that we then have $[a, b] = [c, 0]$ in $\mathbb{Z}$. Since $[c, 0]$ is the image of c under the function f defined in Proposition A.26, we can identify $[c, 0]$ with the natural number c. We will rewrite the integer $[a, b]$ as c in this situation. On the other hand, if $a \leq b \in \mathbb{N}$, then there is a unique d in $\mathbb{N}$ for which $b = a + d$. In this case, $[a, b] = [0, d]$. But since $[0, d] = -[d, 0]$, we can now denote this integer $[a, b]$ as $-d$. (Note that if $a = b$, then $[a, b]$ can be written either as 0 or -0.) So all elements of $\mathbb{Z}$ can be expressed uniquely using the symbols that we use for elements of $\mathbb{N}$ and the negative sign. Thus we will now use our familiar notation for integers.

Order Relation on Integers. By Proposition A.26, we can view $\mathbb{N}$ as a subset of $\mathbb{Z}$. We will also denote the set $\mathbb{N} - \{0\}$ as $\mathbb{Z}^+$.

PROPOSITION A.27. *The set $\mathbb{Z}^+$ has the following properties.*

(1) *$\mathbb{Z}^+$ is closed under addition.*
(2) *$\mathbb{Z}^+$ is closed under multiplication.*
(3) *For all $c \in \mathbb{Z}$, exactly one of the following statements is true: $c \in \mathbb{Z}^+$, $-c \in \mathbb{Z}^+$, or $c = 0$.*

PROOF. (1) Let a and b be elements of $\mathbb{Z}^+$, which we can also view as natural numbers. Then $a + b$ is a natural number, and Proposition A.15 shows that $a + b \geq a$. Since $a \neq 0$, then $a + b > 0$ and can be viewed as an element of Z^+.

(2) If a and b are in $\mathbb{Z}^+$, then we can view $a \cdot b$ as a natural number. But since $a \neq 0$ and $b \neq 0$, we also have $a \cdot b \neq 0$ by Proposition A.21. So $a \cdot b$ is an element of $\mathbb{Z}^+$.

(3) Let c be an integer, which we may write as $[a, b]$ for some natural numbers a and b. By the Trichotomy Property of natural numbers (Corollary A.7), exactly one of the following is true: $a > b$, $a < b$, or $a = b$. If $a > b$, then $a = b + c$ for some $c \neq 0$ in $\mathbb{N}$, and we can view c as an element of $\mathbb{Z}^+$. If $a < b$, then $[b, a] = -[a, b]$ is an element of $\mathbb{Z}^+$ in this same way. If $a = b$, then $[a, b] = [0, 0]$ can be written as 0 in $\mathbb{Z}$. □

If c is an integer, we say that c is *positive* if c is an element of $\mathbb{Z}^+$, and that c is *negative* if $-c$ is in $\mathbb{Z}^+$. Note that 0 is neither positive nor negative by this definition. We use the set $\mathbb{Z}^+$ to define an order relation on integers as follows.

DEFINITION. If a and b are integers, we abbreviate a sum of the form $a + (-b)$ as $a - b$, thus defining an operation of subtraction on integers. We then write $a > b$, or $b < a$, to mean that $a - b$ is an element of $\mathbb{Z}^+$.

The following properties of order are consequences of Proposition A.27. We leave their verification as Exercise 3.

PROPOSITION A.28. *Let a, b, and c be integers.*

(1) *Exactly one of the following is true: $a > b$, $a < b$, or $a = b$.*
(2) *If $a > b$ and $b > c$, then $a > c$.*
(3) *If $a > b$, then $a + c > b + c$.*
(4) *If $a > b$ and $c > 0$, then $ac > bc$.*
(5) *If $a > b$ and $c < 0$, then $ac < bc$.*

Rational Numbers from Integers

Just as an integer is defined as an equivalence class of pairs of nonnegative integers, we can now define a rational number as an equivalence class of pairs of integers (though using a different equivalence relation).

PROPOSITION A.29. *On the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$, define a relation $\sim$ by saying that $(a, b) \sim (c, d)$ if and only if $ad = bc$ in $\mathbb{Z}$. Then $\sim$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.*

PROOF. Let a, b, c, d, e, and f be integers, with b, d, and f not equal to 0.

(1) $(a, b) \sim (a, b)$ because $ab = ba$.
(2) Suppose that $(a, b) \sim (c, d)$, so that $ad = bc$. We can rewrite this equation as $cb = da$, so that $(c, d) \sim (a, b)$.
(3) Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, so that $ad = bc$ and $cf = de$. Multiplying the first equation by f and the second by b, we have that $adf = bcf$ and $bcf = bde$, from which it follows that $d(af) = d(be)$. Since d is not zero, we can cancel d from both sides of the equation and conclude that $af = be$. (This cancellation property is a consequence of properties of $\mathbb{Z}$ compiled in the preceding section.) Thus $(a, b) \sim (e, f)$. □

DEFINITION. We define a *rational number* to be an equivalence class of an element (a, b) in $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ under the relation $\sim$. We write the equivalence class of (a, b) as $\frac{a}{b}$, and we denote the set of all such equivalence classes as $\mathbb{Q}$.

Note that by the definition of equivalence classes, $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

EXAMPLE. The equivalence class of $(3, 4)$ is

$$\begin{aligned}\frac{3}{4} &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mid (3, 4) \sim (a, b)\} \\ &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mid 3b = 4a\} \\ &= \{\ldots, (-9, -12), (-6, -8), (-3, -4), (3, 4), (6, 8), (9, 12), \ldots\},\end{aligned}$$

so that

$$\cdots = \frac{-9}{-12} = \frac{-6}{-8} = \frac{-3}{-4} = \frac{3}{4} = \frac{6}{8} = \frac{9}{12} = \cdots.$$

♢

In the following proposition, we define operations of addition and multiplication on $\mathbb{Q}$, and we list some algebraic properties of the rational numbers.

PROPOSITION A.30. *On $\mathbb{Q}$, the following operations of addition and multiplication are well-defined:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Addition and multiplication are commutative and associative, and multiplication is distributive over addition. The element $\frac{0}{1}$ is an identity element for addition, and every $\frac{a}{b}$ in $\mathbb{Q}$ has an inverse under addition, namely $\frac{-a}{b}$. The element $\frac{1}{1}$ is an identity element for multiplication, and if $\frac{a}{b} \neq \frac{0}{1}$ in $\mathbb{Q}$, then $\frac{b}{a}$ is an inverse of $\frac{a}{b}$ under multiplication.

PROOF. We first prove that addition is well-defined. We want to show that if $\frac{a}{b} = \frac{e}{f}$ and $\frac{c}{d} = \frac{g}{h}$ in $\mathbb{Q}$, then $\frac{a}{b} + \frac{c}{d} = \frac{e}{f} + \frac{g}{h}$, that is, $\frac{ad+bc}{bd} = \frac{eh+fg}{fh}$. Using the definition of the equivalence relation defining $\mathbb{Q}$, we can rephrase this as follows: Assuming that $af = be$ and $ch = dg$, we want to show that $(ad + bc)fh = bd(eh + fg)$. But notice that $(ad + bc)fh = adfh + bcfh = (af)dh + bf(ch) =$

$(be)dh+bf(dg) = bdeh+bdfg = bd(eh+fg)$. The proof that multiplication is well-defined is similar and is left as an Exercise 4.

Now we prove that $\frac{-a}{b}$ is an additive inverse of $\frac{a}{b}$, leaving all other properties as Exercise 5. Let $\frac{a}{b}$ be an element of $\mathbb{Q}$. So a and b are integers with $b \neq 0$, and therefore $\frac{-a}{b}$ is also an element of $\mathbb{Q}$. By definition,

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b^2} = \frac{0}{b^2}.$$

But $\frac{0}{b^2} = \frac{0}{1}$ because $0 \cdot 1 = b^2 \cdot 0$. □

Given $\frac{a}{b}$ in $\mathbb{Q}$, we refer to $\frac{-a}{b}$ as its *negative*, also written as $-\frac{a}{b}$. We define subtraction on $\mathbb{Q}$ by saying that $\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + \left(-\frac{c}{d}\right)$. We can use this operation to define an order relation on $\mathbb{Q}$ by designating certain rational numbers to be positive, as we did with integers.

PROPOSITION A.31. *In $\mathbb{Q}$, define an element $\frac{a}{b}$ to be positive if $ab > 0$ in $\mathbb{Z}$, and denote the set of positive elements in $\mathbb{Q}$ as $\mathbb{Q}^+$. This property of rational numbers is well-defined, and $\mathbb{Q}^+$ has the following properties:*

1. *$\mathbb{Q}^+$ is closed under addition.*
2. *$\mathbb{Q}^+$ is closed under multiplication.*
3. *Given $\frac{a}{b}$ in $\mathbb{Q}$, exactly one of the following is true: $\frac{a}{b} \in \mathbb{Q}^+$, $-\frac{a}{b} \in \mathbb{Q}^+$, or $\frac{a}{b} = \frac{0}{1}$.*

PROOF. Suppose that $ab > 0$ and that $\frac{a}{b} = \frac{c}{d}$ in $\mathbb{Q}$, so that $ad = bc$. If we multiply both sides of this equation by bd, we obtain the equation $abd^2 = b^2cd$. Now with b and d nonzero, then $b^2 > 0$ and $d^2 > 0$. So if $ab > 0$, then $b^2cd > 0$, from which it follows that $cd > 0$.

So $\mathbb{Q}^+$ is a well-defined subset of $\mathbb{Q}$. Now suppose that $\frac{a}{b}$ and $\frac{c}{d}$ are positive. Then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ is positive, since $(ad + bc)bd = abd^2 + b^2cd > 0$ in $\mathbb{Z}$ as ab, cd, b^2 and d^2 are all positive integers. Likewise, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ is positive since $(ac)(bd) = (ab)(cd) > 0$ in $\mathbb{Z}$.

Finally let a and b be integers with $b \neq 0$. Then we know that in $\mathbb{Z}$, exactly one of the following is true: $ab \in \mathbb{Z}^+$, $-(ab) \in \mathbb{Z}^+$, or $ab = 0$. If $ab \in \mathbb{Z}^+$, then $ab > 0$, so that $\frac{a}{b} \in \mathbb{Q}^+$. If $-(ab) = (-a)b \in \mathbb{Z}^+$, then $-\frac{a}{b} \in \mathbb{Q}^+$. If $ab = 0$, then since $b \neq 0$, we must have $a = 0$. So $\frac{a}{b} = \frac{0}{1}$ since $a \cdot 1 = 0 = b \cdot 0$. □

Now in $\mathbb{Q}$, we say that $\frac{a}{b} > \frac{c}{d}$ if and only if $\frac{a}{b} - \frac{c}{d}$ is in $\mathbb{Q}^+$.

Finally, we note that $\mathbb{Q}$ has a subset with all the properties of the set $\mathbb{Z}$. We leave the proofs of these claims as Exercise 6.

PROPOSITION A.32. *The function $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(n) = \frac{n}{1}$ has the following properties.*

1. *f is one-to-one.*
2. *$f(m + n) = f(m) + f(n)$ for all $m, n \in Z$.*
3. *$f(m \cdot n) = f(m) \cdot f(n)$ for all $m, n \in Z$.*
4. *If $m > n$ in $\mathbb{Z}$, then $f(m) > f(n)$ in $\mathbb{Q}$.*

We will identify $\mathbb{Z}$ with the image of $\mathbb{Z}$ under f, and thus consider $\mathbb{Z}$ as a subset of $\mathbb{Q}$. From now on, we will denote a rational number of the form $\frac{a}{1}$ as a. We may also denote a given rational number by a single letter such as r.

Real Numbers from Rationals

If r and s are rational numbers with $r < s$, then $t = \frac{1}{2}(r + s) = \frac{r+s}{2}$ is also rational and $r < t < s$. (Both $t - r$ and $s - t$ equal $\frac{s-r}{2}$, which is positive.) It follows that between any two rational numbers, there are *infinitely many* other rationals. For example, between r and t is the rational number $u = \frac{r+t}{2}$, then $\frac{r+u}{2}$ is a rational number between r and u, and so forth. Nonetheless,

it was discovered by ancient Greek mathematicians that the set of rational numbers is somehow "incomplete," in that there are geometric quantities that cannot be expressed as ratios of integers. For instance, in any square, there is no unit of length such that both a side of the square and a diagonal of the square can be expressed as integer multiples of that length. In modern notation, if a side of a square has length s, then a diagonal of the square has length $s\sqrt{2}$—Greek geometers recognized that $\sqrt{2}$ cannot be written as a ratio of integers. In areas of mathematics in which continuity is important, it is necessary to extend the set of rational numbers to a larger set, called the real numbers.

There are several ways in which the real numbers can be constructed from rational numbers. In this section, we outline an elegant approach due to Dedekind, who began with the simple observation that every real number x separates the set of rational numbers into two nonempty, disjoint subsets—those rational numbers smaller than x and those greater than or equal to x. Dedekind's insight was that in the same way, certain types of subsets of the rational numbers determine corresponding real numbers, and thus real numbers can be *defined* as these type of subsets of the rationals.

DEFINITION. A nonempty, proper subset A of $\mathbb{Q}$ is called a *Dedekind cut*, or simply a *cut*, if the following two statements are true.

(1) For every x in A, if y is a rational number with $y < x$, then $y \in A$. (That is, A contains every rational number less than any particular element of A.)
(2) For every x in A, there is a $z \in A$ such that $x < z$. (That is, A has no *greatest element*.)

If $\overline{A} = \mathbb{Q} - A$ has a *least element*, that is, if there is some $z \in \overline{A}$ so that $z \leq x$ for all $x \in \overline{A}$, then we call A a *rational* cut. Otherwise, A is an *irrational* cut. We denote the set of all Dedekind cuts as $\mathbb{R}$.

In this section, we denote elements of $\mathbb{R}$, defined as sets of rational numbers, by capital letters, while rational numbers themselves are written with lower case letters. We will establish that $\mathbb{R}$ has the properties that are usually associated with the real numbers. We assume the usual properties of order in $\mathbb{Q}$ that follow from the definition of $\mathbb{Q}^+$ given in the preceding section.

EXAMPLE. If r is a rational number, let $A_r = \{x \in \mathbb{Q} \mid x < r\}$. We find that A_r is a rational cut. Here $r - 1$ is an element of A_r, while $r \notin A_r$, so that A_r is a nonempty, proper subset of $\mathbb{Q}$. If $x \in A_r$ and y is a rational number with $y < x$, then $y < r$ so that $y \in A_r$. On the other hand, $z = \frac{x+r}{2}$ is an element of A_r greater than x, so that A_r has no greatest element. However, r is the least element of $\overline{A_r}$, since $y \in \overline{A_r}$ implies that $r \leq y$ by definition.

In fact, every rational cut A can be expressed as A_r for some rational number r. For if r is the least element of $\overline{A}$, then $x < r$ implies that $x \notin \overline{A}$, so that $x \in A$. Conversely, if $x \in A$, then x must be smaller than r, since otherwise we would be forced to conclude that $r \in A$ by condition (1) of the definition of cuts. ◊

EXAMPLE. Let $A = \{x \in \mathbb{Q} \mid x^2 < 2\} \cup A_0$. Then A is an irrational cut. Here $1 \in A$, while $2 \notin A$. Let x be in A and let y be a rational number with $y < x$. If $y < 0$, then $y \in A_0$; otherwise, we have $0 \leq y < x$ with $x^2 < 2$, so that $y^2 < 2$ also. In either case, y is in A. On the other hand, if x is a positive rational number, consider the rational number $z = \frac{3x+4}{2x+3}$. We find that

$$z - x = \frac{3x+4}{2x+3} - x = \frac{(3x+4) - (2x^2+3x)}{2x+3} = \frac{2(2-x^2)}{2x+3},$$

and

$$2 - z^2 = \frac{(8x^2+24x+18) - (9x^2+24x+16)}{(2x+3)^2} = \frac{2-x^2}{(2x+3)^2}.$$

Now if $x \in A$, so that $x^2 < 2$, then $z - x$ and $2 - z^2$ are both positive, so that z is an element of A that is larger than x. But if $x \in \overline{A}$, so that $x^2 > 2$, then z is an element of $\overline{A}$ that is smaller than x.

(It is impossible for x^2 to equal 2. This can be established using properties of prime factorization in the integers that are independent of this construction of the real numbers.) ◊

In the preceding example, A consists precisely of those rational numbers x with $x < \sqrt{2}$, although we did not assume the existence of $\sqrt{2}$ or any other irrational number in this definition. For later reference, we may denote this set as $A_{\sqrt{2}}$.

PROPOSITION A.33. *Let A be a Dedekind cut. Then for all $x, y \in \mathbb{Q}$, if $x \in A$ and $y \in \overline{A}$, then $x < y$. If z is a positive rational number, then there is an element $x \in A$ for which $x + z \in \overline{A}$. In other words, every element of A is smaller than every element of $\overline{A}$, but we can find elements of A and $\overline{A}$ that are arbitrarily close to each other.*

PROOF. Let A be a cut, let $x \in A$, and let $y \in \mathbb{Q}$. If $y \leq x$, then $y \in A$ by the definition of a cut. So if $y \in \overline{A}$, we must conclude that $x < y$. Now let z be a positive rational number. Suppose on the contrary to the claim above that for every $x \in A$, $x + z$ is also in A. Notice that then $(x + z) + z = x + 2z$ is in A, and then $(x + 2z) + z = x + 3z$ is in A, and in general $x + nz$ is in A for every positive integer n. But now if y is a rational number, there is some integer n so that $x + nz$ is larger than y. It follows that y must be in A and so $A = \mathbb{Q}$, violating the definition of a cut. Thus there is an element x in A for which $x + z$ is in $\overline{A}$. □

The claim that we can select an integer n so that $x + nz$ is larger than an arbitrary rational number (when z is positive) is an application of the Archimedean principle. We outline a proof of this property of rational numbers as Exercises 7 and 8.

PROPOSITION A.34. *Let A and B be Dedekind cuts. Then either $A \subseteq B$ or $B \subseteq A$.*

PROOF. Suppose that B is not a subset of A, so that there is some $b \in B$ with $b \notin A$. Now if a is an element of A, Proposition A.33 implies that $a < b$. Since B is a cut and $b \in B$, it follows that $a \in B$, and so $A \subseteq B$. □

Set inclusion is thus a total order relation on $\mathbb{R}$. We write $A \leq B$ interchangeably with $A \subseteq B$ when A and B are Dedekind cuts, and write $A < B$ to mean that A is a proper subset of B. We say that $A \in \mathbb{R}$ is *positive* if $A_0 < A$, or equivalently if A contains a positive rational number, and denote the set of positive cuts as $\mathbb{R}^+$.

Operations on Dedekind Cuts. We next define an operation of addition on $\mathbb{R}$.

PROPOSITION A.35. *If A and B are Dedekind cuts, then $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$ is also a Dedekind cut.*

PROOF. Since A and B are nonempty, then $A + B$ is nonempty. If $x \in \overline{A}$ and $y \in \overline{B}$, then $x + y > a + b$ for every $a \in A$ and $b \in B$, so that $x + y \in \overline{A + B}$, and $A + B \neq \mathbb{Q}$. Now let $x \in A + B$, so that $x = a + b$ for some $a \in A$ and $b \in B$. If $y < x$, then $y = x + y - x = a + (b - (x - y))$. Since $b - (x - y) < b$, then $b - (x - y) \in B$, so that $y \in A + B$. On the other hand, since A and B are cuts, there are elements $a' \in A$ and $b' \in B$ with $a < a'$ and $b < b'$. Now $z = a' + b'$ is an element of $A + B$ greater than $x = a + b$. Thus $A + B$ is a Dedekind cut. □

The following special case illustrates this definition, and is useful for later results.

PROPOSITION A.36. *Let r and s be rational numbers. Then $A_r + A_s = A_{r+s}$.*

PROOF. The typical element of $A_r + A_s$ has the form $x + y$ where $x < r$ and $y < s$. Since then $x + y < r + s$, it follows that $A_r + A_s \subseteq A_{r+s}$. Conversely, let z be an element of A_{r+s}, so that $z < r + s$. Since $z - s < r$ and $z - r < s$, we find that $x = \frac{(z-s)+r}{2} < r$ and $y = \frac{(z-r)+s}{2} < s$. But now notice that $z = x + y$ is an element of $A_r + A_s$. Thus $A_{r+s} \subseteq A_r + A_s$ and so $A_r + A_s = A_{r+s}$. □

PROPOSITION A.37. *Addition of Dedekind cuts satisfies the following properties.*

(1) $A + B = B + A$ *for all* A *and* B *in* $\mathbb{R}$.
(2) $A + (B + C) = (A + B) + C$ *for all* $A, B, C \in \mathbb{R}$.
(3) *There is a* Z *in* $\mathbb{R}$ *such that for all* A *in* $\mathbb{R}$, $A + Z = A$.
(4) *For all* A *in* $\mathbb{R}$, *there is an element* $-A$ *in* $\mathbb{R}$ *so that* $A + (-A) = Z$.

PROOF. The commutative and associative properties are left as Exercise 9.

Let A be a Dedekind cut and let $Z = A_0 = \{x \in \mathbb{Q} \mid x < 0\}$. If $a \in A$ and $x \in Z$, then $a + x < a$, so that $a + x$ is in A. Thus $A + Z \subseteq A$. Conversely, let a be an element of A. Since A has no greatest element, there is some $x \in A$ with $a < x$. Now $a = x + (a - x)$ is in $A + Z$ since $a - x < 0$. Thus $A \subseteq A + Z$, and so $A = A + Z$. This proves statement (3).

If A is a rational cut, so that $A = A_r$ for some rational number r, define $-A$ to be A_{-r}. Then $A + (-A) = A_r + A_{-r} = A_0 = Z$ by Proposition A.36. If A is an irrational cut, define $-A$ to be the set of all rational numbers whose negatives are in $\overline{A}$, that is, $-A = \{x \in \mathbb{Q} \mid -x \in \overline{A}\}$. We find that $-A$ is a cut. Here $-A$ is clearly a nonempty, proper subset of $\mathbb{Q}$ since the same is true of $\overline{A}$. Let $x \in -A$ so that $-x \in \overline{A}$. If $y < x$, then $-y > -x$, so that $-y \in \overline{A}$ and y is in $-A$. On the other hand, since A is an irrational cut, there is some element of $\overline{A}$ smaller than $-x$. We can write this element as $-z$ for some $z \in \mathbb{Q}$. Then $z > x$ and $z \in -A$ by definition.

Now if $a \in A$ and $b \in -A$, so that $-b \in \overline{A}$, then $a < -b$ so that $a + b < 0$. Thus $A + (-A) \subseteq Z$. Conversely, let x be in Z so that $x < 0$. Then $-x$ is a positive rational number. By Proposition A.33, there is some $a \in A$ so that $a + (-x)$ is in $\overline{A}$. But then $-(a - x) = x - a$ is in $-A$. So now $x = a + (x - a) \in A + (-A)$, so that $Z \subseteq A + (-A)$. Therefore $A + (-A) = Z$ for irrational cuts as well, and statement (4) is proved. □

The subset $\mathbb{R}^+$ of positive cuts is closed under addition. For if a and b are positive rational numbers in A and B respectively, then $a + b$ is a positive element of $A + B$. If $A < Z$, so that $\overline{A}$ contains a negative rational number, then $-A$ is a positive cut. So $\mathbb{R}$ has the following *trichotomy* property. If A is a Dedekind cut, then exactly one of the following is true: A is in $\mathbb{R}^+$, $-A$ is in $\mathbb{R}^+$, or $A = Z$. We refer to Z as the *zero* cut; if $-A$ is positive, we say that A is a *negative* cut.

In defining multiplication, it is convenient to restrict our attention first to positive cuts.

LEMMA A.38. *If* A *is a positive cut, let* $A' = \{x \in A \mid x > 0\}$, *a nonempty set. If* A *and* B *are in* $\mathbb{R}^+$, *let* $A'B' = \{ab \mid a \in A' \text{ and } b \in B'\}$. *Then* $A'B'$ *is a nonempty, proper subset of* $\mathbb{Q}^+$ *with the property that for all* x *in* $A'B'$,

(1) *if* y *is a rational number with* $0 < y < x$, *then* $y \in A'B'$, *and*
(2) *there is an element* z *in* $A'B'$ *with* $x < z$.

PROOF. Let A' and B' be the sets of positive elements in the positive cuts A and B respectively. Then $A'B'$ is nonempty. If $x \in \overline{A}$ and $y \in \overline{B}$, then $xy > ab$ for all $a \in A'$ and $b \in B'$, so that xy is not in $A'B'$. Let x be an element of $A'B'$, say that $x = ab$ with $a \in A'$ and $b \in B'$. Let y be a rational number with $0 < y < x$. Then $0 < \frac{y}{x} < 1$, so that $0 < a \cdot \frac{y}{x} < a$. So then $y = \frac{y}{x} \cdot x = (a \cdot \frac{y}{x})b$ is an element of $A'B'$. On the other hand, we can select $a' > a$ in A' and $b' > b$ in B', and we find that $z = a'b'$ is an element of $A'B'$ greater than x. □

Now we can define multiplication of arbitrary elements of $\mathbb{R}$.

DEFINITION. Let A and B be Dedekind cuts and let Z be the zero cut. Then the *product* of A and B is defined as follows.

(1) If $A = Z$ or $B = Z$, then $AB = Z$.
(2) If A and B are positive cuts, then $AB = A'B' \cup \{x \in \mathbb{Q} \mid x \leq 0\}$, where A' and B' are as defined in Lemma A.38.

(3) If A is positive and B is negative, then $AB = -(A(-B))$.
(4) If A is negative, then $AB = -((-A)B)$.

Lemma A.38 makes it apparent that AB is a Dedekind cut when A and B are positive. The trichotomy property then implies that AB is defined in all other cases, with the result a Dedekind cut. So multiplication is an operation on $\mathbb{R}$. We note a special case to illustrate this definition, and for later use.

PROPOSITION A.39. *Let r and s be rational numbers. Then $A_r A_s = A_{rs}$.*

PROOF. We find that A_r is positive, negative, or zero in $\mathbb{R}$ precisely as r is positive, negative, or zero in $\mathbb{Q}$. If $r = 0$ or $s = 0$, then A_{rs} is the zero cut, and $A_r A_s$ is also $Z = A_0$ by part (1) of the definition of multiplication. Next suppose that r and s are both positive. Let x be an element of $A_r A_s$. If $x \leq 0$, then $x \in A_{rs}$ since $rs > 0$. If $x > 0$, then $x \in A'_r A'_s$ so that $x = ab$ for some $0 < a < r$ and $0 < b < s$. Then $ab < rs$ so that $x \in A_{rs}$. Thus $A_r A_s \subseteq A_{rs}$. Conversely, let x be an element of A_{rs}. If $x \leq 0$, then $x \in A_r A_s$ by part (2) of the definition of multiplication, so suppose that $0 < x < rs$. Notice that then $0 < \frac{x}{s} < r$. We can select a rational number t with $\frac{x}{s} < t < r$, so that $t \in A_r$. We then find that $\frac{x}{t} < s$, and so $\frac{x}{t} \in A_s$. So finally, $x = t \cdot \frac{x}{t} \in A_r A_s$. Thus $A_{rs} \subseteq A_r A_s$ and $A_r A_s = A_{rs}$.

Now let r be positive and s negative. By part (3) of the definition of multiplication, then $A_r A_s = -(A_r(-A_s)) = -(A_r A_{-s})$, using the definition of the negative of a cut from the proof of Proposition A.37. Now since r and $-s$ are positive, the argument above shows that $-(A_r A_{-s}) = -A_{r(-s)}$. But again by Proposition A.37, we then have $A_r A_s = -A_{r(-s)} = A_{-(r(-s))} = A_{rs}$, since $-(r(-s)) = rs$ in $\mathbb{Q}$. Finally let r be negative. By part (4) of the definition of multiplication and Proposition A.37, then $A_r A_s = -((-A_r)A_s) = -(A_{-r} A_s)$. Now since $-r$ is positive, the previous parts of this proof show that $-(A_{-r} A_s) = -(A_{(-r)s})$, independent of s. So then $A_r A_s = -(A_{(-r)s}) = A_{-(-r)s} = A_{rs}$ in this case as well. □

PROPOSITION A.40. *Multiplication of Dedekind cuts satisfies the following properties.*

(1) *$AB = BA$ for all $A, B \in \mathbb{R}$.*
(2) *$A(BC) = (AB)C$ for all $A, B, C \in \mathbb{R}$.*
(3) *$A(B + C) = (AB) + (AC)$ for all $A, B, C \in \mathbb{R}$.*
(4) *There is an element I in $\mathbb{R}$ such that for all $A \in \mathbb{R}$, $AI = A$.*
(5) *For all $A \in \mathbb{R}$ with $A \neq Z$, there is an $A^{-1} \in \mathbb{R}$ such that $AA^{-1} = I$.*

PROOF. Verification of the commutative, associative, and distributive properties is straightforward, though somewhat tedious because of the various cases to be considered. We leave proofs of those properties as Exercise 10.

Let $I = A_1 = \{x \in \mathbb{Q} \mid x < 1\}$. If $A = Z$, then $AI = A$ by part (1) of the definition of multiplication. Next let A be a positive cut. Since I is also positive, then $x \in AI$ if and only if either $x \leq 0$ or $x = ab$ for some $a > 0$ in A and $0 < b < 1$. If $x \leq 0$, then x is in A since A is positive. Otherwise, note that $x = ab < a$, so again x is in A. So $AI \subseteq A$. Conversely, let a be an element of A. If $a \leq 0$, then $a \in AI$ by definition, so suppose that $a > 0$. Now there is an element y in A with $a < y$, so that $0 < \frac{a}{y} < 1$. But then $a = y \cdot \frac{a}{y}$ is an element of AI. So $A \subseteq AI$ and $AI = A$, when A is positive. Finally, if A is negative, part (4) of the definition of multiplication implies that $AI = -((-A)I) = -(-A) = A$, using the fact that $-A$ is positive, along with properties of negatives of cuts. (See Exercise 11.) This proves statement (4).

To prove statement (5), first let A be a positive cut. If A is rational, so that $A = A_r$ for some positive $r \in \mathbb{Q}$, define A^{-1} to be $A_{(r^{-1})}$. Then $AA^{-1} = A_1 = I$ by Proposition A.39. If A is an irrational cut, let B be the set of all elements whose inverses are in $\overline{A}$, that is, $B = \{x \mid x^{-1} \in \overline{A}\}$, and let $A^{-1} = B \cup \{x \in \mathbb{Q} \mid x \leq 0\}$. We find that A^{-1} is a positive Dedekind cut. Here B is a

nonempty, proper subset of $\mathbb{Q}^+$ since the same is true of $\overline{A}$. Let x be a positive element of A^{-1}, so that x^{-1} is in $\overline{A}$. If $0 < y < x$, then $y^{-1} > x^{-1}$. But then $y^{-1} \in \overline{A}$ so that y is in A^{-1}. On the other hand, since A is an irrational cut, $\overline{A}$ contains an element smaller than x^{-1}. Since this element is positive, we can write it as z^{-1} for some rational z, and then $z > x$ in A^{-1}.

Now let x be a positive element of AA^{-1}, so that $x = ab$ for some $a > 0$ in A and $b > 0$ in A^{-1}. Then b^{-1} is in $\overline{A}$ by definition, so that $a < b^{-1}$. But then $ab < 1$, so that $x = ab$ is in I. Thus $AA^{-1} \subseteq I$. Conversely, let $0 < x < 1$. Since A is positive, we can select a $y > 0$ in A. Then let $z = y \cdot \frac{1-x}{x}$, which is a positive rational number. We can then select an element $a \in A$ such that $a + z \in \overline{A}$, and we may assume that $a \geq y$. (If $y > a$, then $y + z \in \overline{A}$ also, so we can simply replace a by y.) Now $x = a \cdot \frac{x}{a}$, and we claim that $\frac{x}{a}$ is a positive element of A^{-1}. Notice that $\frac{a}{x} - a = \frac{a-ax}{x} = a \cdot \frac{1-x}{x} \geq y \cdot \frac{1-x}{x} = z$, so that $\frac{a}{x} > a + z$ is in $\overline{A}$. Thus $\frac{x}{a}$ is in A^{-1} by definition. Since every positive element of I is in AA^{-1}, then $I \subseteq AA^{-1}$, and so $AA^{-1} = I$.

Finally, if A is a negative cut, let $A^{-1} = -(-A)^{-1}$, which exists as above since $-A$ is positive. So now using part (4) of the definition of multiplication, $AA^{-1} = -((-A)(-(-A)^{-1})) = -(-I) = I$, again using properties of negatives of cuts (Exercise 11). This establishes statement (5). □

PROPOSITION A.41. *Define a function $f : \mathbb{Q} \to \mathbb{R}$ by $f(r) = A_r$ for every $r \in \mathbb{Q}$. Then f has the following properties.*

(1) *f is one-to-one.*
(2) *If $r \leq s$ in $\mathbb{Q}$, then $f(r) \leq f(s)$ in $\mathbb{R}$.*
(3) *For all $r, s \in \mathbb{Q}$, $f(r + s) = f(r) + f(s)$.*
(4) *For all $r, s \in \mathbb{Q}$, $f(rs) = f(r) \cdot f(s)$.*

PROOF. Let r and s be rational numbers.

(1) Suppose that $f(r) = f(s)$ in $\mathbb{R}$, that is, that $A_r = A_s$. It follows that $r = s$, because if $r < s$, then $t = \frac{r+s}{2}$ is a rational number in A_s but not in A_r, and there is a similar contradiction if $r > s$.
(2) Suppose that $r \leq s$ in $\mathbb{Q}$. Then if $x \in A_r$, so that $x < r$, it immediately follows that $x < s$ and so $x \in A_s$. Thus $A_r \subseteq A_s$ and $A_r \leq A_s$ in $\mathbb{R}$.
(3) This was established as Proposition A.36.
(4) This was established as Proposition A.39. □

The following is the key property of the set $\mathbb{R}$.

THEOREM A.42 (Completeness Theorem). *Let $\mathbb{S}$ be a nonempty subset of $\mathbb{R}$ and suppose that $\mathbb{S}$ has an upper bound, that is, there is an element $B \in \mathbb{R}$ such that $A \leq B$ for all $A \in \mathbb{S}$. Then $\mathbb{S}$ has a least upper bound. That is, there is an element $C \in \mathbb{R}$ such that C is an upper bound for $\mathbb{S}$, and such that if B is also an upper bound for $\mathbb{S}$, then $C \leq B$.*

Note that the least upper bound C is not assumed to be an element of $\mathbb{S}$. The Completeness Theorem does not hold for $\mathbb{Q}$. For instance, the set S of rational numbers x for which $x^2 < 2$ is a nonempty subset with an upper bound, but does not have a least upper bound. No matter what y we select such that $y \geq x$ for all $x \in S$, we can find a rational number $z < y$ which is also an upper bound for S. (See the example above showing that $A_{\sqrt{2}}$ is an irrational cut for more details.)

PROOF. Let $\mathbb{S}$ be a nonempty subset of $\mathbb{R}$, and suppose that $A \leq B$ for all $A \in \mathbb{S}$. Define a set C by saying that $x \in C$ if and only if $x \in A$ for at least one of the elements A in $\mathbb{S}$. (In other words, C is the union of all the elements of $\mathbb{S}$.) Then we see as follows that C is a Dedekind cut. Here C is nonempty since $\mathbb{S}$ contains at least one cut. If b is an element in $\overline{B}$, then b cannot be in any set A in $\mathbb{S}$, and so $\overline{C}$ is nonempty. Let x be an element of C, so that x is in some cut $A \in \mathbb{S}$.

If $y < x$, then $y \in A$, so that $y \in C$. On the other hand, there is some $z \in A$ greater than x, and this z is also in C.

Now C is an element of $\mathbb{R}$ that has the property of being the least upper bound of $\mathbb{S}$. For if A is any element of $\mathbb{S}$, then A is a subset of C and so $A \leq C$. Let B be any upper bound of $\mathbb{S}$ so that $A \leq B$ for all $A \in \mathbb{S}$. Then $C \leq B$, since if c is an element of C, then $c \in A$ for some $A \in \mathbb{S}$. But then $c \in B$, so that $C \subseteq B$. □

In many real analysis texts, the Completeness Theorem is taken as an axiom of the real numbers, along with the properties of addition and multiplication in Propositions A.37 and A.40, the trichotomy property, and the closure of $\mathbb{R}^+$ under addition and multiplication that we proved above. All properties of real numbers can be derived from these axioms. We will now change our notation, and write the typical element of $\mathbb{R}$ as x, viewing it as a "number" in the usual way.

Complex Numbers from Reals

Now that we have constructed the set of real numbers, it is a relatively easy matter to define the complex numbers in terms of $\mathbb{R}$.

Definition. Let $\mathbb{R}$ be the set of real numbers. Then we define the set of complex numbers, denoted by $\mathbb{C}$, to be $\mathbb{R} \times \mathbb{R}$. If $x, y, w, z \in \mathbb{R}$, so that (x, y) and (w, z) are elements of $\mathbb{C}$, we define operations of addition and multiplication on $\mathbb{C}$ by:

$$(x, y) + (w, z) = (x + w, y + z) \qquad \text{and} \qquad (x, y) \cdot (w, z) = (xw - yz, xz + yw).$$

As in our previous constructions, we have defined the elements of $\mathbb{C}$ and operations on $\mathbb{C}$ in terms of sets requiring only previously defined numbers and operations. In this case, we do not need to define an equivalence relation on these objects—we have instead that $(x, y) = (w, z)$ in $\mathbb{C}$ if and only if $x = w$ and $y = z$ in $\mathbb{R}$.

The usual algebraic rules hold for addition and multiplication in $\mathbb{C}$.

Proposition A.43. *In the set $\mathbb{C}$, addition and multiplication are commutative and associative, and multiplication is distributive over addition. The element $(0, 0)$ has the property that $(x, y) + (0, 0) = (x, y)$ for all $(x, y) \in \mathbb{C}$. For all $(x, y) \in \mathbb{C}$, the element $(-x, -y) \in \mathbb{C}$ has the property that $(x, y) + (-x, -y) = (0, 0)$. The element $(1, 0)$ has the property that $(x, y) \cdot (1, 0) = (x, y)$ for all $(x, y) \in \mathbb{C}$. If $(x, y) \neq (0, 0)$, then the element $(w, z) = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$ has the property that $(x, y) \cdot (w, z) = (1, 0)$.*

Proof. Exercise 13. □

We can think of $\mathbb{R}$ as a subset of $\mathbb{C}$ in the same way as in several other examples in this appendix—$\mathbb{C}$ contains a subset that has all the algebraic properties of $\mathbb{R}$.

Proposition A.44. *Define a function $f : \mathbb{R} \to \mathbb{C}$ by $f(x) = (x, 0)$ for all $x \in \mathbb{R}$. Then*

1. *f is one-to-one.*
2. *$f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$.*
3. *$f(xy) = f(x) \cdot f(y)$ for all $x, y \in \mathbb{R}$.*

Proof. Exercise 14. □

We can identify the ordered pair $(x, 0)$ in $\mathbb{C}$ with $x \in \mathbb{R}$. Notice that the element $(0, 1)$ has the property that $(0, 1) \cdot (0, 1) = (-1, 0)$. We may write $(0, 1)$ as i, so that the preceding equation is $i^2 = -1$. Every element $(x, y) \in \mathbb{C}$ satisfies the equation $(x, y) = (x, 0) + (y, 0) \cdot (0, 1)$. Thus we can write the typical element of $\mathbb{C}$ uniquely as $x + yi$ with $x, y \in \mathbb{R}$, giving the set $\mathbb{C}$ its familiar form.

Appendix A Exercises.

1. Let $\mathbb{Z} = \{[a, b] \mid a, b \in \mathbb{N}\}$ with addition and multiplication defined as in Proposition A.24. Let $[a, b]$, $[c, d]$, and $[e, f]$ be elements of $\mathbb{Z}$.
   (a) Show that $[a, b] + [c, d] = [c, d] + [a, b]$.
   (b) Show that $[a, b] + ([c, d] + [e, f]) = ([a, b] + [c, d]) + [e, f]$.
   (c) Show that $[a, b] \cdot [c, d] = [c, d] \cdot [a, b]$.
   (d) Show that $[a, b] \cdot ([c, d] \cdot [e, f]) = ([a, b] \cdot [c, d]) \cdot [e, f]$.
   (e) Show that $[a, b] \cdot ([c, d] + [e, f]) = [a, b] \cdot [c, d] + [a, b] \cdot [e, f]$.
2. In $\mathbb{Z}$, let $[a, b] - [c, d] = [a + d, b + c]$. Show that this operation is well-defined.
3. Prove the properties listed in Proposition A.28 for order in the set of integers.
4. Show that the operation of multiplication given in Proposition A.30 is well-defined.
5. Let $\mathbb{Q}$ be the set of rational numbers.
   (a) Show that addition is commutative and associative in $\mathbb{Q}$.
   (b) Show that multiplication is commutative and associative in $\mathbb{Q}$.
   (c) Show that multiplication is distributive over addition in $\mathbb{Q}$.
   (d) Show that $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$ and that $\frac{a}{b} \cdot \frac{1}{1} = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$.
   (e) Show that if $\frac{a}{b} \neq \frac{0}{1}$, then $\frac{b}{a}$ is a rational number for which $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$.
6. Prove the properties given in Proposition A.32 of $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(n) = \frac{n}{1}$.
7. Show that if a and b are integers with $a > 0$, and n is the larger of 0 and $b + 1$, then $na \geq b$.
8. Show that if $r = \frac{a}{b}$ and $s = \frac{c}{d}$ are rational numbers with r positive, then there is an integer n so that $nr > s$. (Hint: Show that abd^2 is a positive integer, and use the preceding exercise to show that there is an integer n with $n(abd^2) > b^2cd$.)
9. Prove that addition of Dedekind cuts is commutative and associative, as claimed in Proposition A.37.
10. Let multiplication of Dedekind cuts be given as in this section.
    (a) Show that multiplication is commutative.
    (b) Show that multiplication is associative.
    (c) Show that multiplication is distributive over addition.
11. If A is a Dedekind cut, let $-A$ be the negative of A as given in Proposition A.37.
    (a) Show that $-(-A) = A$ for all Dedekind cuts A.
    (b) Show that $A(-B) = -AB$ and $(-A)B = -AB$ for all Dedekind cuts A and B.
12. Let A and B be Dedekind cuts with $A < B$. Show that there is a rational number r with the property that $A < A_r < B$.
13. Prove the properties of addition and multiplication in $\mathbb{C}$ given in Proposition A.43.
14. Prove the properties given in Proposition A.44 of the function $f : \mathbb{R} \to \mathbb{C}$ defined by $f(x) = (x, 0)$.

APPENDIX B

Elementary Number Theory

In Appendix A, we outlined a construction of the set of integers in which the basic algebraic properties of addition, multiplication, and order were established. We now review some arithmetic properties of integers that are typically encountered in a first course in number theory, with an emphasis on results and methods used in this text.

Divisibility in the Integers

In Theorem A.8, we proved that every nonempty subset of the positive integers has a least element. We use this fact to establish some basic properties of divisibility in the set of integers.

DEFINITION. If m and n are integers, we say that m *divides* n if there is an integer q so that $n = mq$.

The following theorem gives us a method of testing whether one integer divides another.

THEOREM B.1 (Division Algorithm). *If n and m are integers with $m > 0$, then there are unique integers q and r such that $n = mq + r$ and $0 \leq r < m$.*

PROOF. Let $T = \{n - mx \mid x \in \mathbb{Z}\}$ and let S be the set of nonnegative elements of T. We find that S is nonempty—if $n \geq 0$, then $n = n - m(0)$ is an element of S; if $n < 0$, then $n - m(n) = -n(m-1)$ is in S since $-n > 0$ and $m - 1 \geq 0$. If 0 is an element of S, then 0 is the least element of S. If not, then the well-ordering principle applies to S. So S has a least element in any case, which we can label as r. Note that $r = n - mq$ for some integer q by the definition of T. Thus $n = mq + r$ with $r \geq 0$. We also find that $r < m$ since otherwise $r - m = n - m(q+1)$ is an element of S smaller than r, contrary to assumption.

To show that q and r are unique, suppose that we also have $n = ms + t$ with $0 \leq t < m$. This implies that $m(q - s) = t - r$. But with $0 \leq r, t < m$, we find that $-m < t - r < m$. We must conclude that $q - s = 0$, so that $q = s$ and $r = t$, since otherwise $|m(q - s)| \geq m$. □

DEFINITION. If $n = mq + r$ with $0 \leq r < m$ as under the division algorithm, we write the *quotient* q as n div m and the *remainder* r as n mod m.

If m is positive, then m divides n if and only if $n \bmod m = 0$, and $-m$ divides n if and only if m divides n. If $m = 0$, then m divides n if and only if $n = 0$. Thus we can use the division algorithm to test divisibility of one integer by another in every case.

DEFINITION. If a and b are integers, let $\langle a \rangle = \{aq \mid q \in \mathbb{Z}\}$ and let $\langle a, b \rangle = \{as + bt \mid s, t \in \mathbb{Z}\}$. We say that n is a *multiple* of a if n is in $\langle a \rangle$, and that n is a *combination* of a and b if n is in $\langle a, b \rangle$.

THEOREM B.2. *Let a and b be integers. Then there is an integer d such that $\langle a, b \rangle = \langle d \rangle$. In this case, d has the following properties.*

(1) *d is a common divisor of a and b, that is, d divides a and d divides b.*
(2) *If c is a common divisor of a and b, then c divides d.*

PROOF. If $a = 0 = b$, then $\langle a, b\rangle = \{0\} = \langle 0\rangle$. If a and b are not both zero, then $\langle a, b\rangle$ must contain a positive integer, since a, b, $-a$, and $-b$ are elements of $\langle a, b\rangle$. (For instance, $-b = a(0) + b(-1)$.) So the set of positive elements in $\langle a, b\rangle$ is nonempty, and must contain a least element d by the well-ordering principle. We show that $\langle a, b\rangle = \langle d\rangle$ in this case.

By definition, $d \in \langle a, b\rangle$ implies that $d = as + bt$ for some integers s and t. Now for any q we see that $dq = a(sq) + b(tq) \in \langle a, b\rangle$, and so $\langle d\rangle \subseteq \langle a, b\rangle$. To show the reverse inclusion, let n be an element of $\langle a, b\rangle$, say $n = ax + by$ for some integers x and y. Since d is positive, we can apply the division algorithm to write $n = dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Note that $r = n - dq = a(x - sq) + b(y - tq)$ is an element of $\langle a, b\rangle$. If $r > 0$, this contradicts the definition of d as the smallest positive integer in $\langle a, b\rangle$, so we must conclude that $r = 0$, and then $n = dq$ is in $\langle d\rangle$. Thus $\langle a, b\rangle \subseteq \langle d\rangle$, and we conclude that $\langle a, b\rangle = \langle d\rangle$.

As noted, a and b are elements of $\langle a, b\rangle$, so if $\langle a, b\rangle = \langle d\rangle$, then d divides both a and b by definition. If c divides both a and b, say with $a = cq$ and $b = cr$, then $d = as + bt = c(qs + rt)$, so that c divides d. □

DEFINITION. Let a and b be integers. We say that $d \geq 0$ is the *greatest common divisor* of a and b, and write $d = \gcd(a, b)$, if d is a common divisor of a and b that is a multiple of every other common divisor of a and b. If $\gcd(a, b) = 1$, we say that a is *relatively prime* to b, or that a and b are *coprime*.

Theorem B.2 shows that if $d = \gcd(a, b)$, then d is a combination of a and b. This fact has several useful consequences for divisibility in the set of integers.

COROLLARY B.3. *If a and b are integers, then a is relatively prime to b if and only if there are integers s and t so that $as + bt = 1$.*

PROOF. Let $d = \gcd(a, b)$, so that $\langle a, b\rangle = \langle d\rangle$. If $d = 1$, then 1 is a combination of a and b. Conversely, if $as + bt = 1$ for some s and t, then 1 is in $\langle d\rangle$. It follows that d divides 1, and so $d = 1$ since $d \geq 0$. □

COROLLARY B.4. *Let a, b, and c be integers with $\gcd(a, b) = d$. If a divides bc, then a divides cd. In particular, if a divides bc with a and b coprime, then a divides c.*

PROOF. If a divides bc, then $bc = aq$ for some integer q. Let $\gcd(a, b) = d$, so that there are integers s and t with $d = as + bt$. Then

$$cd = c(as + bt) = acs + (bc)t = acs + (aq)t = a(cs + qt).$$

So a divides cd, since $cs + qt$ is an integer. □

COROLLARY B.5. *If a divides n and b divides n, and $\gcd(a, b) = d$, then ab divides nd. In particular, if a and b are coprime, then ab divides n.*

PROOF. We have that $n = bq$ for some integer q. So a divides bq and by Corollary B.4, then a divides qd, say that $qd = ar$ for some integer r. But now

$$nd = (bq)d = b(qd) = b(ar) = (ab)r,$$

and so ab divides nd. □

DEFINITION. If a and b are integers, we say that an integer $m \geq 0$ is the *least common multiple* of a and b, and write $m = \operatorname{lcm}(a, b)$, if

(1) a divides m and b divides m, and
(2) if a and b both divide n, then m divides n.

COROLLARY B.6. *If a and b are integers, then $|ab| = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.*

PROOF. Assume for simplicity that a and b are both nonnegative. If $a = 0 = b$, then $\operatorname{lcm}(a, b) = 0$, since 0 is the only common multiple of a and b. In all other cases, $d = \gcd(a, b)$ is positive, and we can consider the integer $m = \frac{ab}{d}$. Note that $m = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$ is a common multiple of a and b, since $\frac{b}{d}$ and $\frac{a}{d}$ are integers. If a and b both divide n, then Corollary B.5 shows that m divides n. Thus $m = \operatorname{lcm}(a, b)$ by definition. □

The Euclidean Algorithm. We now describe an efficient algorithm for calculating the greatest common divisor d of a pair of integers a and b, and for expressing d as a combination of a and b. This method is based on repeated application of the division algorithm, together with the following observations.

PROPOSITION B.7. *Let a and b be integers with $a \geq b \geq 0$.*

(1) *If $b > 0$ and $a = bq + r$ for some integers q and r, then $\gcd(a, b) = \gcd(b, r)$.*
(2) *If $b = 0$, then $\gcd(a, b) = a$.*

PROOF. For statement (1), we find that if $a = bq + r$, then

$$as + bt = (bq + r)s + bt = b(qs + t) + rt \quad \text{and} \quad bs + rt = bs + (a - bq)t = at + b(s - qt).$$

So $\langle a, b\rangle = \langle b, r\rangle$, and it follows that $\gcd(a, b) = \gcd(b, r)$. For statement (2), note that every integer divides 0, so that the common divisors of a and 0 are precisely the divisors of a. □

We will illustrate the procedure of the Euclidean algorithm with an example.

EXAMPLE. Let $a = 377$ and $b = 104$. If we divide a by b, we obtain the equation $377 = 104 \cdot 3 + 65$. Now part (1) of Proposition B.7 implies that $\gcd(377, 104) = \gcd(104, 65)$, and we can similarly divide 104 by 65 to obtain a still smaller pair of integers with the same greatest common divisor. We continue the process in the left-hand list of equations below, eventually obtaining 0 as a remainder.

$$\begin{array}{rcl} 377 &=& 104 \cdot 3 + 65 \\ 104 &=& 65 \cdot 1 + 39 \\ 65 &=& 39 \cdot 1 + 26 \\ 39 &=& 26 \cdot 1 + 13 \\ 26 &=& 13 \cdot 2 + 0 \end{array} \qquad \begin{array}{rcl} 65 &=& 377 - 104 \cdot 3 = a - 3b \\ 39 &=& 104 - 65 = b - (a - 3b) = -a + 4b \\ 26 &=& 65 - 39 = (a - 3b) - (-a + 4b) = 2a - 7b \\ 13 &=& 39 - 26 = (-a + 4b) - (2a - 7b) = -3a + 11b \end{array}$$

Proposition B.7 implies in turn that

$$\gcd(377, 104) = \gcd(104, 65) = \gcd(65, 39) = \gcd(39, 26) = \gcd(26, 13) = \gcd(13, 0) = 13,$$

with $\gcd(a, b)$ the last nonzero remainder in the left-hand column. Now we solve each equation for its remainder in the right-hand list. By substitution, we see that each remainder can be written as a combination of a and b. In particular, the last nonzero remainder, $\gcd(a, b)$, has that form. In this example, we conclude that $\gcd(377, 104) = 13 = 377(-3) + 104(11)$. ◊

We state the Euclidean algorithm in more formal terms as follows.

THEOREM B.8 (Euclidean Algorithm). *Let a and b be integers with $0 \leq b \leq a$. Let $r_{-2} = a$ and $r_{-1} = b$, let $s_{-2} = 1$ and $s_{-1} = 0$, and let $t_{-2} = 0$ and $t_{-1} = 1$. For $i \geq 0$, define the sequences r_i, s_i, t_i, and q_i recursively as follows. If $r_{i-1} \neq 0$, let*

$$q_i = r_{i-2} \operatorname{div} r_{i-1}, \quad r_i = r_{i-2} \bmod r_{i-1}, \quad s_i = s_{i-2} - s_{i-1}q_i, \quad \text{and} \quad t_i = t_{i-2} - t_{i-1}q_i.$$

Then there is an integer $k \geq -2$ such that $r_{k+1} = 0$, and in this case, $\gcd(a, b) = r_k = as_k + bt_k$.

PROOF. Note that r_i is a strictly decreasing sequence of nonnegative integers for $i \geq -2$, so must eventually take on the value zero. Let k be the largest integer for which $r_k \neq 0$. By Proposition B.7, we have that

$$\gcd(a,b) = \gcd(r_{-2}, r_{-1}) = \gcd(r_{-1}, r_0) = \cdots = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k.$$

Now we can show by induction that $r_i = as_i + bt_i$ for $-2 \leq i \leq k+1$. Clearly this is true for $i = -2$ and $i = -1$. Suppose that for some $0 \leq i \leq k+1$, the equation holds for both $i-2$ and $i-1$. Then by definition and the inductive hypothesis,

$$\begin{aligned} r_i = r_{i-2} - r_{i-1}q_i &= (as_{i-2} + bt_{i-2}) - (as_{i-1} + bt_{i-1})q_i \\ &= a(s_{i-2} - s_{i-1}q_i) + b(t_{i-2} - t_{i-1}q_i) = as_i + bt_i. \end{aligned}$$

In particular, $r_k = \gcd(a,b) = as_k + bt_k$. □

Solutions of Linear Equations. The Euclidean algorithm allows us to write $d = \gcd(a,b)$ as a combination of a and b in practice. Any multiple of d can then be similarly expressed. For example, since $13 = 377(-3) + 104(11)$ from the preceding example, then

$$n = 585 = 45 \cdot 13 = 45\,(377(-3) + 104(11)) = 377(45 \cdot -3) + 104(45 \cdot 11) = 377(-135) + 104(495).$$

This expression is not unique, but produces all other integer solutions of the equation $ax + by = n$, as we see in the following theorem.

THEOREM B.9. *Let a and b be integers (not both zero), and let s and t be a pair of integers for which $\gcd(a,b) = d = as + bt$. Let n be a multiple of d, say with $n = dr$ for some $r \in \mathbb{Z}$. Then all integer solutions of $ax + by = n$ are given by*

$$(x,y) = \left(sr + \frac{b}{d} \cdot q\,,\; tr - \frac{a}{d} \cdot q \right), \tag{B.1}$$

where q is an arbitrary integer.

Notice that $\frac{a}{d}$ and $\frac{b}{d}$ are integers since d is a positive common divisor of a and b.

PROOF. First note that any pair given by equation (B.1) does in fact satisfy $ax + by = n$:

$$a\left(sr + \frac{b}{d} \cdot q \right) + b\left(tr - \frac{a}{d} \cdot q \right) = asr + \frac{ab}{d} \cdot q + btr - \frac{ab}{d} \cdot q = (as + bt)r = dr = n.$$

Conversely, suppose that (x,y) is an integer pair for which $ax+by = n$. Then $ax+by = n = asr+btr$ so that $a(x-sr) = b(tr-y)$. Now b divides $a(x-sr)$, so that $\frac{b}{d}$ divides $x-sr$ by Corollary B.4. Thus there is an integer q so that $x - sr = \frac{b}{d} \cdot q$. Substituting this expression into $a(x-sr) = b(tr-y)$, we then see that $tr - y = \frac{a}{d} \cdot q$. Solving these equations for x and y gives us the formula of (B.1). □

EXAMPLE. All integer solutions of $377x + 104y = 585$ are given by

$$(x,y) = \left(-135 + \frac{104}{13} \cdot q\,,\; 495 - \frac{377}{13} \cdot q \right) = (-135 + 8q, 495 - 29q),$$

with q an integer. For instance, if $q = 17$, we find that $(x,y) = (1,2)$ is also a solution. We could then say that all solutions of $377x + 104y = 585$ are given by $(x,y) = (1 + 8q, 2 - 29q)$. (Now we obtain $(x,y) = (-135, -495)$ when $q = -17$, for example.) ◊

Prime Factorization. An integer $p > 1$ is called *prime* if its only positive divisors are 1 and p. If $n > 1$ is not prime, it is called *composite* Note that 1 is neither prime nor composite by definition. To conclude this section, we establish the uniqueness of prime factorization in the set of integers.

THEOREM B.10 (Euclid's Lemma). *Let p be a prime number, and suppose that p divides ab for some integers a and b. Then either p divides a or p divides b.*

PROOF. Let $d = \gcd(a, p)$. Since d is a positive divisor of p, either $d = p$ or $d = 1$. If $d = p$, then p divides a by definition. If $d = 1$ and p divides ab, then p divides b by Corollary B.4. □

When n is composite, then it is always possible to find integers a and b such that n divides the product ab without dividing either term in the product. In fact, if we let a be any positive divisor of n other than 1 and n, so that $n = ab$ for some integer b, then we have that n divides ab, but does not divide either a or b.

THEOREM B.11 (Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written as a product of primes. This product is unique, aside from the order of the factors.*

PROOF. We first establish the existence of such a factorization. If not every integer $n > 1$ can be written as a product of primes, we can assume that n is the smallest integer that cannot be so written. Then n must be composite, since we regard a prime number as a product of primes with just one factor. So n can be written as $n = ab$ with $1 < a, b < n$. But then, by assumption, a and b can be written as product of primes, and thus $n = ab$ has that property as well, contradicting our assumption.

Now suppose that there is an integer n larger than 1 that can be written in two ways as a product of primes, say that $n = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_\ell$ with each p_i and q_j prime. We may again take n to be as small as possible with this property. In particular, we can assume that $p_i \neq q_j$ for $1 \leq i \leq k$ and $1 \leq j \leq \ell$, since otherwise we could cancel that common term from both products and start over with the smaller resulting integer. Here p_1 divides n since $p_2 p_3 \cdots p_k$ is an integer, and so p_1 divides the product $q_1 q_2 \cdots q_\ell$. Applying Euclid's Lemma repeatedly, we can say that p_1 divides at least one term in that product. Rearranging those terms if necessary, we can assume that p_1 divides q_1. But q_1 is prime, so it has no positive divisors other than itself and 1. Since $p_1 > 1$, we must conclude that $p_1 = q_1$. This contradicts the assumption that no p_i is the same as any q_j. So in fact, the two expressions for n are the same, aside from rearrangement of the terms. □

The following notation and facts will occasionally be useful in reference to prime factorization.

DEFINITION. Let n be a positive integer and let p be a prime number. Then we write $e_p(n) = t$ if p^t divides n but p^{t+1} does not divide n. We refer to $e_p(n)$ as the *exponent* of p in n.

We can define a positive integer n by specifying $e_p(n) \geq 0$ for all primes p, as long as $e_p(n) = 0$ for all but finitely many primes. The uniqueness of prime factorization implies that then

$$n = \prod_p p^{e_p(n)},$$

where the product is taken over all primes. (All but finitely many terms of this product equal 1, so this infinite product is actually finite in practice.)

PROPOSITION B.12. *If m and n are positive integers, then $e_p(mn) = e_p(m) + e_p(n)$ for every prime number p.*

PROOF. Let $e_p(m) = s$ and $e_p(n) = t$, so that $m = p^s a$ and $n = p^t b$ for some positive integers a and b. Then $mn = p^s a \cdot p^t b = p^{s+t} ab$. If p divides ab, then p divides either a or b by Euclid's Lemma. But that is impossible since p^{s+1} does not divide m and p^{t+1} does not divide n. So we see that p^{s+t} divides mn but p^{s+t+1} does not divide mn, and conclude that $e_p(mn) = s + t = e_p(m) + e_p(n)$, as we wanted to show. □

COROLLARY B.13. *Let m and n be positive integers. Then the following statements are true.*

(1) *m divides n if and only if $e_p(m) \leq e_p(n)$ for every prime p.*
(2) *$e_p(\gcd(m, n)) = \min(e_p(m), e_p(n))$ for every prime p.*
(3) *$e_p(\text{lcm}(m, n)) = \max(e_p(m), e_p(n))$ for every prime p.*

PROOF. Let m and n be positive integers.

(1) Suppose that m divides n, say that $n = mq$ for some integer q, which is clearly positive. Then $e_p(n) = e_p(mq) = e_p(m) + e_p(q)$ for every prime p by Proposition B.12. Since $e_p(q) \geq 0$ for all p, it follows that $e_p(n) \geq e_p(m)$ for all p. Conversely, if $e_p(m) \leq e_p(n)$ for all p, then $e_p(n) - e_p(m) \geq 0$, with equality holding for all but finitely many primes p since $e_p(n) = 0$ in all but finitely many cases. So we can define a positive integer q by stating that $e_p(q) = e_p(n) - e_p(m)$ for all p, and then $n = mq$ by Proposition B.12. So m divides n.

(2) Let $d = \gcd(a, b)$. Since d divides a and d divides b, it follows that $e_p(d) \leq e_p(a)$ and $e_p(d) \leq e_p(b)$, that is, $e_p(d) \leq \min(e_p(a), e_p(b))$ for all primes p. If c is defined so that $e_p(c) = \min(e_p(a), e_p(b))$ for all p, then we find that c is a common divisor of a and b, so must divide d. But then $e_p(d) \geq \min(e_p(a), e_p(b))$ for all primes p, and our result follows. The proof of statement (3) is similar, and is omitted. □

Exercises on Divisibility in the Integers.

1. Show that for every integer a, $\gcd(a, a + 1) = 1$.
2. What possible values can $\gcd(a, a + 2)$ take on? Show that your answer is correct.
3. If $\gcd(a, b) = d$, show that $\gcd(\frac{ca}{d}, \frac{cb}{d}) = c$ for every positive integer c.
4. Let a and b be integers with $\gcd(a, b) = 1$. Show by induction that $\gcd(a^m, b) = 1$ for every nonnegative integer m. Explain why it follows that $\gcd(a^m, b^n) = 1$ for every pair of nonnegative integers m and n.
5. For each of the following pairs a and b, apply the Euclidean algorithm to calculate $d = \gcd(a, b)$ and to find integers s and t so that $as + bt = d$.
   (a) $a = 238$ and $b = 323$.
   (b) $a = 119$ and $b = 938$.
   (c) $a = 1019$ and $b = 1523$.
6. Find all integer solutions of each of the following linear equations.
   (a) $238x + 323y = 153$.
   (b) $119x + 938y = 658$.
   (c) $1019x + 1523y = 437$.
7. Let n be a positive integer. Show that n is a square (that is, of some positive integer) if and only if $e_p(n)$ is even for every prime p. More generally, show that n is a k-th power of a positive integer (for some $k \geq 2$) if and only if k divides $e_p(n)$ for every prime p.
8. Let n be a positive integer. Show that the number of positive divisors of n is $\prod_p (e_p(n)+1)$, where the product is taken over all primes p. (Hint: Use Corollary B.13.)
9. Let n be a positive integer. Show that n has an odd number of positive divisors if and only if n is a square.

Linear Congruences

The following variation on the definition of divisibility, introduced by Gauss, is particularly useful for stating and proving results about the set of integers.

DEFINITION. Let a, b, and m be integers, with m positive. We say that a is *congruent* to b *modulo* m, and write $a \equiv b \pmod{m}$, if m divides $a - b$. If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$.

The following proposition lists some important properties of congruence relations on the set of integers.

PROPOSITION B.14. *Let a, b, c, d, and m be integers, with $m > 0$. Then the following statements are true.*

(1) $a \equiv a \pmod{m}$.
(2) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.
(3) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.
(4) *If* $a \equiv c \pmod{m}$ *and* $b \equiv d \pmod{m}$, *then* $a + b \equiv c + d \pmod{m}$.
(5) *If* $a \equiv c \pmod{m}$ *and* $b \equiv d \pmod{m}$, *then* $ab \equiv cd \pmod{m}$.
(6) *If* $a \equiv b \pmod{m}$ *and d is a positive divisor of m, then* $a \equiv b \pmod{d}$.
(7) $a \equiv b \pmod{m}$ *if and only if* $a \bmod m = b \bmod m$, *that is, if and only if a and b have the same remainder, under the division algorithm, on division by m.*

PROOF. We prove statement (5), leaving the remaining proofs as Exercises 1–4. Suppose that $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, so that $a - c = mq$ and $b - d = mr$ for some integers q and r. Then

$$ab - cd = ab - cb + cb - cd = (a - c)b + c(b - d) = mqb + cmr = m(qb + cr),$$

and so $ab \equiv cd \pmod{m}$, since $qb + cr$ is an integer. □

Parts (1)–(3) of Proposition B.14 show that congruence modulo m is an equivalence relation on the set of integers. We write the set of all equivalence classes under this relation (which we also call *congruence classes* modulo m) as $\mathbb{Z}_m$. By definition, the congruence class of a modulo m is

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\} = \{x \in \mathbb{Z} \mid x = a + mq \text{ for some integer } q\}.$$

Part (7) of Proposition B.14 shows that $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$, and parts (4) and (5) show that the following operations of addition and multiplication are well-defined on $\mathbb{Z}_m$:

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab].$$

We usually write $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$ when it is clear that we are working modulo m.

We will often use the following property of congruence relations.

PROPOSITION B.15 (Congruence Cancellation Property). *Let a, b, and c be integers, let m be a positive integer, and let* $\gcd(a, m) = d$. *Then* $ab \equiv ac \pmod{m}$ *if and only if* $b \equiv c \pmod{\frac{m}{d}}$.

PROOF. Suppose first that $ab \equiv ac \pmod{m}$, so that m divides $ab - ac = a(b - c)$. If $d = \gcd(a, m)$, then Corollary B.4 implies that $\frac{m}{d}$ divides $b - c$.

Conversely, suppose that $b \equiv c \pmod{\frac{m}{d}}$, where $d = \gcd(a, m)$ for some integer a. Then $b - c = \frac{m}{d}q$ for some integer q, so that $ab - ac = a \cdot \frac{m}{d}q = m \cdot \frac{a}{d}q$. Since $\frac{a}{d}$ is an integer, we can conclude that $ab \equiv ac \pmod{m}$. □

EXAMPLE. If $10b \equiv 10c \pmod{48}$, it is not necessarily true that $b \equiv c \pmod{48}$. For instance, $10 \cdot 24 \equiv 10 \cdot 0 \pmod{48}$, but $24 \not\equiv 0 \pmod{48}$. The strongest conclusion we can be sure of is that $b \equiv c \pmod{24}$. ◊

Solving Linear Congruences. If $f(x)$ is a polynomial with integer coefficients, then repeated application of Proposition B.14 implies that $f(a) \equiv f(b) \pmod{m}$ when $a \equiv b \pmod{m}$. Solving a *polynomial congruence* $f(x) \equiv 0 \pmod{m}$ means finding all elements of $\mathbb{Z}_m$ that make this congruence true, and we interpret the *number of solutions* of $f(x) \equiv 0 \pmod{m}$ to be the number of distinct congruence classes of solutions. In this section, we consider an arbitrary *linear* congruence, traditionally written as $ax \equiv b \pmod{m}$, where a and b are integers and m is a positive integer. (We can also write this as $f(x) \equiv 0 \pmod{m}$ where $f(x) = ax - b$.) We can find all solutions of such a congruence with the same method used for linear equations in Theorem B.9.

THEOREM B.16. *Let a, b, and m be integers, with m positive, and let $d = \gcd(a, m)$. If d divides b, then the linear congruence $ax \equiv b \pmod{m}$ has d distinct solutions in $\mathbb{Z}_m$, and any two solutions of $ax \equiv b \pmod{m}$ are congruent modulo $\frac{m}{d}$. If d does not divide b, then $ax \equiv b \pmod{m}$ has no solutions.*

PROOF. Notice that x satisfies $ax \equiv b \pmod{m}$ if and only if there is some y so that (x, y) is a solution of $ax + my = b$. This equation has solutions if and only if $d = \gcd(a, m)$ divides b. If d divides b and (u, v) is a solution of $ax + my = b$ with $u \geq 0$ as small as possible, then Theorem B.9 implies that all solutions of $ax + my = b$ have the form $(x, y) = \left(u + \frac{m}{d} \cdot q\,,\ v - \frac{a}{d} \cdot q\right)$ where q is an integer. There are d distinct solutions for x in $\mathbb{Z}_m$, namely $x = u + \frac{m}{d} \cdot q$ for $0 \leq q < d$. □

EXAMPLE. Solutions of the congruence $266x \equiv 301 \pmod{413}$ are the same as the x-coordinates in integer solutions of $266x + 413y = 301$. We apply the Euclidean algorithm to $a = 266$ and $m = 413$ as follows.

$$\begin{array}{rcl@{\qquad}rcl} 413 &=& 266 \cdot 1 + 147 & 147 &=& 413 - 266 = m - a \\ 266 &=& 147 \cdot 1 + 119 & 119 &=& 266 - 147 = a - (m - a) = 2a - m \\ 147 &=& 119 \cdot 1 + 28 & 28 &=& 147 - 119 = (m - a) - (2a - m) = 2m - 3a \\ 119 &=& 28 \cdot 4 + 7 & 7 &=& 119 - 28 \cdot 4 = (2a - m) - 4(2m - 3a) = 14a - 9m \\ 28 &=& 7 \cdot 4 + 0 & & & \end{array}$$

We find that $\gcd(266, 413) = 7 = 266(14) + 413(-9)$. Since $301 = 7 \cdot 43$, solutions of $266x + 413y = 301$ exist, and have the general form

$$\left(43 \cdot 14 + \frac{413}{7} \cdot q\,,\ 43 \cdot -9 - \frac{266}{7} \cdot q\right) = (602 + 59q\,,\ -387 - 38q),$$

with q an arbitrary integer. The smallest nonnegative possibility for x is $602 + 59(-10) = 12$, and all solutions of $266x \equiv 301 \pmod{413}$ have the form $x = 12 + 59q$. There are seven *distinct* solutions in $\mathbb{Z}_{413}$, namely 12, 71, 130, 189, 248, 307, and 366. ◊

Thus we can solve an arbitrary linear congruence systematically, using the Euclidean algorithm. Often, we can also adopt a trial-and-error approach, using the congruence cancellation property.

EXAMPLE. Consider the congruence $60x \equiv 66 \pmod{111}$, where $a = 60$ and $b = 66$ have a common divisor of 6. We can cancel this common factor, but we must adjust the modulus $m = 111$ according to Proposition B.15. Since $\gcd(6, 111) = 3$, we find that $10x \equiv 11 \pmod{37}$. Now $\gcd(10, 11) = 1$, but we might cancel other factors of the linear coefficient by replacing 11 by an integer to which it is congruent modulo 37. For instance, $11 \equiv 48 \pmod{37}$, so that $2 \cdot 5x \equiv 2 \cdot 24 \pmod{37}$. This time, since $\gcd(2, 37) = 1$, we can cancel the common factor of 2 without affecting the modulus. So now $5x \equiv 24 \pmod{37}$. With some additional searching, $24 \equiv 61 \equiv 98 \equiv 135 \pmod{37}$, we can replace this congruence by $5x \equiv 5 \cdot 27 \pmod{37}$. We conclude that $x \equiv 27 \pmod{37}$ since $\gcd(5, 37) = 1$. So the solutions of our original congruence are of the form $x = 27 + 37q$ with $q \in \mathbb{Z}$. Note that there are three distinct solutions in $\mathbb{Z}_{111}$, as predicted by Theorem B.16, namely 27, 64, and 101. ◊

Systems of Linear Congruences. The preceding example demonstrates that if $\gcd(a, m) = d$ divides b, then the congruence $ax \equiv b \pmod{m}$ has the same solutions, in $\mathbb{Z}$, as $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. In the remainder of this section, we will assume that $\gcd(a, m) = 1$, so that $ax \equiv b \pmod{m}$ has a unique solution in $\mathbb{Z}_m$. In particular, if $\gcd(a, m) = 1$, we denote the solution of $ax \equiv 1 \pmod{m}$ in $\mathbb{Z}_m$ as a^{-1}, which we call the *inverse* of a modulo m. Note that the solution of $ax \equiv b \pmod{m}$ is congruent to $a^{-1}b$ modulo m. We will demonstrate that we can solve $ax \equiv b \pmod{m}$ in a systematic way if we can solve $ax \equiv b \pmod{p}$ for every prime p dividing m. While this method is not more efficient than the Euclidean algorithm approach, it suggests general results that we will see are helpful in solving quadratic congruences later in Appendix B.

THEOREM B.17 (Chinese Remainder Theorem). *Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers, that is, with $\gcd(m_i, m_j) = 1$ when $i \neq j$, and let $a_1, a_2, \ldots, a_k$ be a collection of integers, not necessarily distinct. Then there is a unique integer x modulo $m = m_1 m_2 \cdots m_k$ that simultaneously satisfies*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned} \tag{B.2}$$

PROOF. If x and y both satisfy all congruences in (B.2), then $x-y$ is divisible by $m_1, m_2, \ldots, m_k$. It follows that $x - y$ must be divisible by the least common multiple of these moduli. With those values *pairwise* relatively prime, it is not difficult to see that this least common multiple is $m = m_1 m_2 \cdots m_k$. So if a solution exists, it is unique modulo m. We show that a solution exists by constructing an example.

For $i = 1, 2, \ldots, k$, let $M_i = \frac{m}{m_i} = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$, the product of each of the moduli excluding m_i. Since m_j is relatively prime to m_i if $i \neq j$, we see that M_i is relatively prime to m_i. Thus M_i has an inverse modulo m_i, which we denote by M_i^{-1}. Now consider the integer

$$x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}. \tag{B.3}$$

Here $M_i M_i^{-1} \equiv 1 \pmod{m_i}$ for all i, but $M_i M_i^{-1} \equiv 0 \pmod{m_j}$ if $i \neq j$ since in that case m_j is a factor of M_i. Thus we find that $x \equiv a_1 \cdot 1 + a_2 \cdot 0 + \cdots + a_k \cdot 0 \equiv a_1 \pmod{m_1}$, and in a similar way, that x satisfies each congruence in (B.2). □

EXAMPLE. Consider the linear congruence $ax \equiv b \pmod{m}$ where $a = 331$, $b = 857$, and $m = 1071 = 3^2 \cdot 7 \cdot 17$. Any solution of this congruence must also satisfy $ax \equiv b \pmod{d}$ if d divides m. Consider $ax \equiv b \pmod{m_i}$ for $m_1 = 9$, $m_2 = 7$, and $m_3 = 17$. (We select these moduli because they are pairwise relatively prime and their product equals m.) Each resulting congruence simplifies greatly and can be solved relatively easily.

(1) $ax \equiv b \pmod{9}$ simplifies to $7x \equiv 2 \pmod{9}$, with $x = 8$ as its solution.
(2) $ax \equiv b \pmod{7}$ simplifies to $2x \equiv 3 \pmod{7}$, with solution $x = 5$.
(3) $ax \equiv b \pmod{17}$ simplifies to $8x \equiv 7 \pmod{17}$, with solution $x = 3$.

The solution of $ax \equiv b \pmod{1071}$ must simultaneously satisfy

$$\begin{aligned} x &\equiv r \pmod{9} \\ x &\equiv s \pmod{7} \\ x &\equiv t \pmod{17} \end{aligned} \tag{B.4}$$

with $r = 8$, $s = 5$, and $t = 3$. The Chinese Remainder Theorem shows that such an x must exist, and is unique modulo $m = 9 \cdot 7 \cdot 17 = 1071$. To illustrate the formula in the proof of Theorem B.17,

we find a general solution of system (B.4) in terms of r, s, and t. If $M_1 = 7 \cdot 17 = 119$, then M_1^{-1} is the solution of $119x \equiv 1 \pmod 9$, which we find to be $M_1^{-1} = 5$. Likewise, for $M_2 = 9 \cdot 17 = 153$, we find that $153x \equiv 1 \pmod 7$ has solution $M_2^{-1} = 6$. For $M_3 = 9 \cdot 7 = 63$, we find that $63x \equiv 1 \pmod{17}$ has solution $M_3^{-1} = 10$. So the general solution of system (B.4) is

$$x \equiv r \cdot 119 \cdot 5 + s \cdot 153 \cdot 6 + t \cdot 63 \cdot 10 \equiv 595r + 918s + 630t \pmod{1071}.$$

When $r = 8$, $s = 5$, and $t = 3$, we obtain $x \equiv 11240 \equiv 530 \pmod{1071}$. So $x = 530$ is the unique solution of $331x \equiv 857 \pmod{1071}$. ◊

The following variation on the Chinese Remainder Theorem is used several times in the text.

THEOREM B.18. *Let $a_1, a_2, \ldots, a_k$ be a collection of integers, and suppose that there are integers $q_1, q_2, \ldots, q_k$ so that $a_1q_1 + a_2q_2 + \cdots + a_kq_k = 1$. Let $b_1, b_2, \ldots, b_k$ be integers and let m be a positive integer. Then the system of congruences*

$$\begin{aligned} a_1x &\equiv b_1 \pmod m \\ a_2x &\equiv b_2 \pmod m \\ &\vdots \\ a_kx &\equiv b_k \pmod m. \end{aligned} \tag{B.5}$$

has a unique solution $x \equiv b_1q_1 + b_2q_2 + \cdots b_kq_k \pmod m$ if and only if $a_ib_j \equiv a_jb_i \pmod m$ for all $1 \le i, j \le k$.

PROOF. Suppose that x satisfies all congruences in (B.5). Then multiplying $a_jx \equiv b_j \pmod m$ by a_i and $a_ix \equiv b_i \pmod m$ by a_j, it follows that $a_ia_jx \equiv a_ib_j \equiv a_jb_i \pmod m$. Thus if a solution of (B.5) exists, then $a_ib_j \equiv a_jb_i \pmod m$ for all i and j. Now suppose that y also satisfies all congruences in (B.5). Then $a_i(x - y) \equiv 0 \pmod m$, so that $a_iq_i(x - y) \equiv 0 \pmod m$, and thus

$$(a_1q_1 + a_2q_2 + \cdots + a_kq_k)(x - y) = x - y \equiv 0 \pmod m.$$

Therefore, if a solution of (B.5) exists, it is unique modulo m.

Finally, suppose that $a_ib_j \equiv a_jb_i \pmod m$ for $1 \le i, j \le k$, and consider

$$x = b_1q_1 + b_2q_2 + \cdots + b_kq_k.$$

Then for each i,

$$\begin{aligned} a_ix &= a_ib_1q_1 + \cdots + a_ib_kq_k \\ &= (a_ib_1 - a_1b_i)q_1 + \cdots + (a_ib_k - a_kb_i)q_k + (a_1b_iq_1 + \cdots + a_kb_iq_k) \\ &\equiv 0 \cdot q_1 + \cdots + 0 \cdot q_k + b_i(a_1q_1 + \cdots + a_kq_k) \equiv b_i \pmod m. \end{aligned}$$

Thus a solution of (B.5) exists when $a_ib_j \equiv a_jb_i \pmod m$ for $1 \le i, j \le k$. □

Linear Congruences Modulo Prime Powers. If $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ with each p_i a distinct prime, the Chinese Remainder Theorem implies that we can solve $ax \equiv b \pmod m$ by solving each $ax \equiv b \pmod{p_i^{e_i}}$, as the preceding example illustrates. We now see that we for a prime p, we can use the solution of $ax \equiv b \pmod p$ to solve $ax \equiv b \pmod{p^e}$ for an arbitrary $e \ge 1$.

THEOREM B.19. *Let p be a prime number, let a be an integer not divisible by p, with a^{-1} the inverse of a modulo p, and let b be an integer. Define sequences b_i and q_i for $i \ge 0$ as follows. Let $b_0 = b$, and for $i \ge 0$, let*

$$q_i = a^{-1}b_i \bmod p \qquad \text{and} \qquad b_{i+1} = \frac{b_i - aq_i}{p}. \tag{B.6}$$

Then for every $e \geq 1$, the unique solution of $ax \equiv b \pmod{p^e}$ is given by

$$r_e = q_0 + q_1 p + \cdots + q_{e-1} p^{e-1}. \tag{B.7}$$

Note that each b_{i+1} is an integer, since q_i is the solution of $ax \equiv b_i \pmod{p}$.

PROOF. We show by induction on e that $ar_e = b - p^e b_e$ for all $e \geq 1$. First note that $ar_1 = aq_0 = b_0 - pb_1 = b - p^1 b_1$ by (B.7) and (B.6). Now suppose that $ar_e = b - p^e b_e$ for some $e \geq 1$. Since $r_{e+1} = r_e + q_e p^e$, we have that

$$ar_{e+1} = ar_e + aq_e p^e = b - p^e b_e + aq_e p^e = b - p^e(b_e - aq_e) = b - p^e \cdot pb_{e+1} = b - p^{e+1} b_{e+1},$$

using the inductive hypothesis and the definition of b_{e+1} in (B.6). So $ar_e = b - p^e b_e$ for all $e \geq 1$, and r_e must be the unique solution of $ax \equiv b \pmod{p^e}$. □

EXAMPLE. Let $p = 17$ and $a = 7$, so that $a^{-1} = 5$, the solution of $7x \equiv 1 \pmod{17}$. Let $b = 71$. The following table demonstrates the results of the algorithm of Theorem B.19. For example, $q_0 \equiv 5 \cdot 71 \equiv 355 \equiv 15 \pmod{17}$, so that $b_1 = \frac{71 - 7 \cdot 15}{17} = \frac{-34}{17} = -2$, and then $q_1 \equiv 5 \cdot -2 \equiv -10 \equiv 7 \pmod{17}$, and so forth.

i	0	1	2	3	4	5	6	7
b	71	-2	-3	-1	-5	-4	-6	-2
q	15	7	2	12	9	14	4	7

The table shows, for example, that $15 + 7 \cdot 17 + 2 \cdot 17^2 + 12 \cdot 17^3 = 59668$ satisfies the congruence $7x \equiv 71 \pmod{17^4}$, as can be verified by direct calculation. ◊

Notice in this example that $b_7 = b_1$, so that $q_7 = q_1$. The algorithm of Theorem B.19 shows that b_i and q_i then repeat the pattern of $1 \leq i \leq 6$ indefinitely. We can show that a similar periodicity occurs in a predictable way in all examples of linear congruences modulo prime powers. We require the following proposition and definition.

PROPOSITION B.20. *Let m be a positive integer, and let a be an integer with $\gcd(a, m) = 1$. Then there is a positive integer t so that $a^t \equiv 1 \pmod{m}$.*

PROOF. The positive integer powers of a cannot all be distinct modulo m, so there are integers $0 \leq s < r$ for which $a^r \equiv a^s \pmod{m}$. If $\gcd(a, m) = 1$, we can repeatedly apply the congruence cancellation property to conclude that $a^{r-s} \equiv 1 \pmod{m}$. So $t = r - s$ is a positive integer for which $a^t \equiv 1 \pmod{m}$. □

DEFINITION. If $\gcd(a, m) = 1$, the smallest $t > 0$ for which $a^t \equiv 1 \pmod{m}$ is called the *order* of a modulo m, written as $t = \mathrm{ord}_m(a)$.

THEOREM B.21. *Let p be a prime number, let a be a positive integer not divisible by p, with a^{-1} the inverse of a modulo p, and let b be an integer with $\gcd(a, b) = 1$. Define the sequences b_i and q_i for $i \geq 0$ as in (B.6). Let t be the order of p modulo a. Then there is a nonnegative integer m so that $b_{i+t} = b_i$ and $q_{i+t} = q_i$ for all $i \geq m$.*

PROOF. Let b_i and q_i be defined for $i \geq 0$ as in (B.6). We first show by induction that

$$\frac{b}{p^n} \geq b_n \geq \frac{a+b}{p^n} - a \tag{B.8}$$

for all $n \geq 0$. This is true for $n = 0$, since $b_0 = b$, so suppose we have that (B.8) is true for some $n \geq 0$. Using (B.6), we can substitute $pb_{n+1} + aq_n$ for b_n in (B.8). Subtracting aq_n from each term, and using the facts that $a > 0$ and $0 \leq q_n \leq p - 1$ for all n, we see that

$$\frac{b}{p^n} \geq \frac{b}{p^n} - aq_n \geq pb_{n+1} \geq \frac{a+b}{p^n} - a(1 + q_n) \geq \frac{a+b}{p^n} - ap.$$

Dividing through by p establishes (B.8) for $n+1$, and so for all $n \geq 0$ by induction.

Since $b_0 = b$ and $pb_{i+1} = b_i - aq_i$ by (B.6), we see inductively that $p^i b_i \equiv b \pmod{a}$ for all $i \geq 0$. If $\gcd(a,b) = 1$, it follows that $\gcd(a, b_i) = 1$. Furthermore, if t is the order of p modulo a, so that $p^t \equiv 1 \pmod{a}$, then $b_{i+t} \equiv b_i \pmod{a}$ for all $i \geq 0$. Let m be the smallest integer for which $p^m > |b|$. Then for any $i \geq m$, we have that $p^i > b$ and $a + b > b > -p^i$, so that (B.8) implies that $1 > b_i > -1 - a$. If $a > 1$, we can further conclude that $0 > b_i > -a$, since b_i is an integer with $\gcd(a, b_i) = 1$. But now the congruence $b_{i+t} \equiv b_i \pmod{a}$ implies the equation $b_{i+t} = b_i$, from which it follows that $q_{i+t} = q_i$, when $i \geq m$. If $a = 1$, the equations in (B.6) show that if $b_m = 0$, then $q_m = 0$ and $b_{m+1} = 0$, while if $b_m = -1$, then $q_i = p - 1$ and $b_{m+1} = -1$. Since $p^1 \equiv 1 \pmod{1}$ for every prime p, this proves our result for $a = 1$ as well. □

EXAMPLE. Let $p = 2$, $a = 45$, and $b = 71$, so that $a^{-1} = 1$. Under the algorithm of Theorem B.19, we see that $q_i = 0$ or 1 with the same parity as b_i, so that $b_{i+1} = \frac{b_i}{2}$ if b_i is even and $b_{i+1} = \frac{b_i - 45}{2}$ if b_i is odd. The results appear in the following table.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
b	71	13	−16	−8	−4	−2	−1	−23	−34	−17	−31	−38	−19	−32	−16
q	1	1	0	0	0	0	1	1	0	1	1	0	1	0	0

We find that $b_{14} = b_2$, so that $b_{i+12} = b_i$ and $q_{i+12} = q_i$ for $i \geq 2$. We leave it to the reader to verify that 2 has order twelve modulo 45. ♢

Exercises on Linear Congruences.

1. Show that congruence modulo m is an equivalence relation on the set of integers. (That is, show parts (1)–(3) of Proposition B.14.)
2. Show that if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$ (Proposition B.14, part (4)).
3. Show that if $a \equiv b \pmod{m}$ and d is a positive divisor of m, then $a \equiv b \pmod{d}$ (Proposition B.14, part (6)).
4. Show that $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$ (Proposition B.14, part (7)).
5. Find all solutions (in the appropriate set $\mathbb{Z}_m$) of each of the following linear congruences.
   (a) $238x \equiv 153 \pmod{323}$.
   (b) $119x \equiv 658 \pmod{938}$.
   (c) $1019x \equiv 437 \pmod{1523}$.

In Exercises 6–9, use the Chinese Remainder Theorem to solve the given congruence.

6. $47x \equiv 53 \pmod{77}$.
7. $49x \equiv 127 \pmod{253}$, given that $253 = 11 \cdot 23$.
8. $97x \equiv 23 \pmod{779}$, given that $779 = 19 \cdot 41$.
9. $3472x \equiv 2143 \pmod{4199}$, given that $4199 = 13 \cdot 17 \cdot 19$.

In Exercises 10–14, find the sequences b_i and q_i, as defined in Theorem B.19, for each of the following choices of p, a, and b. (Continue the sequences until a repeating pattern occurs.)

10. $p = 3$, $a = 5$, $b = -29$.
11. $p = 17$, $a = 2$, $b = 213$.
12. $p = 5$, $a = 14$, $b = -227$.
13. $p = 23$, $a = 10$, $b = 221$.
14. $p = 19$, $a = 12$, $b = 97$.

15. Use Theorem B.19 to solve $1937x \equiv 2144 \pmod{2401}$, given that $2401 = 7^4$.
16. Let m and n be relatively prime positive integers and suppose that $ms + nt = 1$ for some integers s and t. Show that $x = ant + bms$ satisfies the pair of congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

Quadratic Congruences Modulo Primes

In the remainder of Appendix B, we turn our attention to the next general case of polynomial congruences, $f(x) \equiv 0 \pmod{m}$ where $f(x)$ is a quadratic polynomial and m is a positive integer. We have seen that we can solve $ax \equiv b \pmod{m}$ in a systematic way by first solving $ax \equiv b \pmod{p}$ for every prime divisor p of m. We will find that the same is true for quadratic congruences. We can give a complete description of the *number* of solutions of an arbitrary quadratic congruence, and will note some ways of solving a congruence when solutions are known to exist.

Let $f(x) = ax^2 + bx + c$ with a, b, and c integers, and let p be a prime number. We may assume that p does not divide a, since otherwise $ax^2 + bx + c \equiv 0 \pmod{p}$ reduces to a linear congruence. It is also convenient to treat $p = 2$ separately. Proposition B.22, which follows an important general definition, lists the possibilities in this case. We leave its proof as Exercise 1 for this section.

DEFINITION. If $f(x) = ax^2 + bx + c$, define the *discriminant* of f to be $\Delta(f) = b^2 - 4ac$.

Notice that $\Delta(f)$ is congruent to either 0 or 1 modulo 4, since the same is true for every square. So one of the cases listed in the following proposition must occur.

PROPOSITION B.22. *Let $f(x) = ax^2 + bx + c$ with a odd, and let $\Delta = \Delta(f)$.*

(1) *If $\Delta \equiv 1 \pmod{8}$, then b is odd and c is even, and $f(x) \equiv 0 \pmod{2}$ has two solutions, $x = 0$ and $x = 1$, in $\mathbb{Z}_2$.*
(2) *If $\Delta \equiv 5 \pmod{8}$, then b and c are odd, and $f(x) \equiv 0 \pmod{2}$ has no solutions in $\mathbb{Z}_2$.*
(3) *If $\Delta \equiv 0 \pmod{4}$, then b is even, and $f(x) \equiv 0 \pmod{2}$ has one solution in $\mathbb{Z}_2$, namely $x = 0$ if c is even, and $x = 1$ if c is odd.*

When p is an *odd* prime, a quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ can be transformed into a specialized form by *completing the square*. Multiplying both sides of the congruence by $4a$ and adding $b^2 - 4ac$ to both sides yields

$$4a^2x^2 + 4abx + b^2 = (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{B.9}$$

Notice that $\gcd(4a, p) = 1$ if p is odd and does not divide a. So we can likewise cancel $4a$ from both sides of the resulting congruence by the congruence cancellation property, and no unwanted solutions of the original congruence are introduced. The situation is now analogous to that of solving a quadratic equation over the real numbers. In that case, the question of whether solutions exist is determined purely by whether the discriminant $\Delta(f) = b^2 - 4ac$ is greater than or equal to zero. If so, we can take square roots of both sides and solve for x, obtaining the familiar *quadratic formula*: $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. In our situation, we must determine whether Δ has a "square root modulo p" and then solve a linear congruence for x. We illustrate with an example.

EXAMPLE. Find all solutions of $2x^2 - 3x + 3 \equiv 0 \pmod{17}$.

Here $a = 2$, $b = -3$, and $c = 3$, so that $\Delta = b^2 - 4ac = -15$, and our congruence can be replaced by $(4x - 3)^2 \equiv -15 \pmod{17}$, as in (B.9). There is no integer whose square is -15, but we can replace -15 by any integer to which it is congruent modulo 17. By trial-and-error, we find that $-15 \equiv 2 \equiv 19 \equiv 36 \pmod{17}$, and recognize that $36 = (\pm 6)^2$. So two solutions of the original congruence are given by solving $4x - 3 \equiv 6 \pmod{17}$ and $4x - 3 \equiv -6 \pmod{17}$ for $x = 15$ and $x = 12$ respectively. (We will see in Proposition B.23 that these must be the only possibilities.) $\Diamond$

This example illustrates that the process of solving a quadratic congruence modulo an odd prime is fairly mechanical except for the step of determining whether $b^2 - 4ac$ is congruent to a square. So now, changing our notation, we will concentrate on quadratic congruences of the form $x^2 \equiv a \pmod{p}$ where p is an odd prime number and a is an integer.

For a fixed prime p, it is possible to solve a congruence of the form $x^2 \equiv a \pmod{p}$ by calculating $x^2 \bmod p$ for $0 \le x < p$, as in the table below for $p = 17$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^2	0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256
$x^2 \bmod 17$	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

We see, for instance, that $x^2 \equiv 15 \pmod{17}$ has two solutions, $x = 7$ and $x = 10$. (Any number congruent to one of these modulo 17, such as 24, is also a solution, but as before we take the number of solutions of $x^2 \equiv 12 \pmod{17}$ to mean the number of solutions in $\mathbb{Z}_{17}$.) We also have that $x^2 \equiv -2 \pmod{17}$ has the same two solutions, since $-2 \equiv 15 \pmod{17}$. On the other hand, $x^2 \equiv 11 \pmod{17}$ has no solutions since 11 does not appear in the last row of the table.

PROPOSITION B.23. *Let p be an odd prime and let a be an integer. If p does not divide a, then $x^2 \equiv a \pmod{p}$ has either two solutions or no solutions. If p divides a, then $x^2 \equiv a \pmod{p}$ has exactly one solution, namely $x = 0$.*

PROOF. We have seen by example that $x^2 \equiv a \pmod{p}$ might have no solutions. So suppose that $x^2 \equiv a \pmod{p}$ has a solution, say $x = b$. Then $-b$ is also a solution since $(-b)^2 = b^2$. If c is yet another solution, then $c^2 \equiv a \equiv b^2 \pmod{p}$, implying that p divides $c^2 - b^2 = (c - b)(c + b)$. Since p is prime, it follows that p divides $c - b$ or p divides $c + b$, that is, either $c \equiv b \pmod{p}$ or $c \equiv -b \pmod{p}$. So c must be the same solution as b or $-b$, and therefore $x^2 \equiv a \pmod{p}$ has a maximum of two distinct solutions.

It is possible, in the same way, that $-b$ is simply another name for the solution b, but that would imply that $b \equiv -b \pmod{p}$, so that p divides $b - (-b) = 2b$. Since $p \neq 2$ is prime, this occurs if and only if p divides b, so that $b \equiv 0 \pmod{p}$. But then $b^2 \equiv a \equiv 0 \pmod{p}$. So the congruence $x^2 \equiv a \pmod{p}$ has exactly one solution if $a \equiv 0 \pmod{p}$, but must have either two distinct solutions or no solutions if $a \not\equiv 0 \pmod{p}$. □

The following notation summarizes these possibilities.

DEFINITION. Let p be an odd prime and a any integer. Then the *Legendre symbol*, written as $\left(\frac{a}{p}\right)$, is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod{p} \text{ has two solutions,} \\ 0, & \text{if } x^2 \equiv a \pmod{p} \text{ has only one solution,} \\ -1, & \text{if } x^2 \equiv a \pmod{p} \text{ has no solutions.} \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$, then we say that a is a *quadratic residue* modulo p.

EXAMPLE. Referring to the table above, we have for instance that $\left(\frac{15}{17}\right) = 1$ and $\left(\frac{11}{17}\right) = -1$. ◊

Calculating Legendre Symbols. When $\left(\frac{a}{p}\right) = 1$, the Legendre symbol provides no information about the actual solutions of $x^2 \equiv a \pmod{p}$. In practice, it may be necessary to test whether $x^2 \equiv a \pmod{p}$ for $0 \le x \le \frac{p-1}{2}$, as in the proof of Proposition B.23. But in the remainder of this section, we develop a method of calculating Legendre symbols with very little computation. Thus we can know beforehand whether our search for solutions will be successful. We begin with some immediate consequences of the definition of Legendre symbols.

(1) $\left(\frac{a}{p}\right) = 0$ if and only if p divides a, from Proposition B.23.

(2) $\left(\frac{1}{p}\right) = 1$, since $x^2 \equiv 1 \pmod{p}$ always has two solutions, 1 and -1.
(3) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, since $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ then have the same solutions, and so the same number of solutions.

The following theorem helps to explain the definition of the Legendre symbol, and is key to establishing other important properties of these symbols.

THEOREM B.24 (Euler's Criterion). *Let p be an odd prime and a any integer. Then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

The claim is that $a^{\frac{p-1}{2}}$ is congruent to 1, 0, or -1 modulo p as $x^2 \equiv a \pmod{p}$ has two, one, or no solutions. Euler proved this result using properties of powers of integers modulo p. Here we will give an alternative proof due to Dirichlet (*Lectures on Number Theory*, §34), requiring only facts that we have established about linear congruences.

PROOF. For a prime p, let $\mathbb{Z}_p^\times = \{1, 2, 3, \ldots, p-1\}$, the elements of $\mathbb{Z}_p$ that are relatively prime to p. If p divides a, then $a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0 \pmod{p}$, and as noted above, $\left(\frac{a}{p}\right) = 0$. So let a be a fixed element of $\mathbb{Z}_p^\times$ instead.

For every $r \in \mathbb{Z}_p^\times$, let r' denote the solution in $\mathbb{Z}_p^\times$ of the linear congruence $rx \equiv a \pmod{p}$. (We know that this solution exists and is congruent to $r^{-1}a$ modulo p if $\gcd(r, p) = 1$.) Notice that $(r')' = r$, and that $r' = r$ if and only if r satisfies the congruence $x^2 \equiv a \pmod{p}$. As we have seen, there are precisely two such values if $\left(\frac{a}{p}\right) = 1$, which we can write as s and $t \equiv -s \pmod{p}$ for some $s \in \mathbb{Z}_p^\times$, and no such values if $\left(\frac{a}{p}\right) = -1$. In other words, if $\left(\frac{a}{p}\right) = 1$, then the set $\mathbb{Z}_p^\times$ consists of s, t, and $\frac{p-3}{2}$ pairs of distinct elements r and r', while if $\left(\frac{a}{p}\right) = -1$, then $\mathbb{Z}_p^\times$ has $\frac{p-1}{2}$ pairs of distinct elements r and r'.

Now consider the product P (calculated modulo p) of all the elements of $\mathbb{Z}_p^\times$, writing $\prod(rr')$ for the product of *distinct* pairs r and r' for which $rr' \equiv a \pmod{p}$. If $\left(\frac{a}{p}\right) = 1$, we have that

$$P \equiv s \cdot t \cdot \prod(rr') \equiv -a \cdot a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p}, \tag{B.10}$$

using the fact that $st \equiv s(-s) \equiv -a \pmod{p}$. On the other hand, if $\left(\frac{a}{p}\right) = -1$, then

$$P \equiv \prod(rr') \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{B.11}$$

We can rewrite (B.10) and (B.11) with the single congruence

$$-P \cdot \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{B.12}$$

But when we let $a = 1$, then (B.12) implies that $-P \equiv 1 \pmod{p}$, since $\left(\frac{1}{p}\right) = 1$ and every power of 1 equals 1. We conclude that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ for every $a \in \mathbb{Z}_p^\times$, since P is independent of the choice of a. □

As an aside, we note that this proof of Euler's Criterion produces the following classical result as a corollary, since $P = (p-1)!$. (The case of $p = 2$ must be verified separately.)

COROLLARY B.25 (Wilson's Theorem). *If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

EXAMPLE. To illustrate the idea of Dirichlet's proof, we consider three values of a with $p = 17$. Here $\mathbb{Z}_{17}^\times = \{1, 2, \ldots, 16\}$, and we will express the product P as 16!. If $a = 1$, then for each r in $\mathbb{Z}_{17}^\times$, we let r' denote the solution of $rx \equiv 1 \pmod{17}$, that is, the inverse of r modulo 17. For

example, $2' = 9$, and so $9' = 2$, since $2 \cdot 9 \equiv 1 \pmod{17}$. Notice that $1' = 1$ and $16' = 16$, since 1 and -1 are solutions of $x^2 \equiv 1 \pmod{17}$. In the following equation, we rearrange 16! to pair each element of $\mathbb{Z}_{17}^{\times}$ with its inverse.

$$\begin{aligned} 16! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \\ &= 1 \cdot (2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 16 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 16 \equiv -1 \pmod{17}. \end{aligned}$$

This confirms Wilson's Theorem for $p = 17$.

Now let $a = 2$, so that r' denotes the solution of $rx \equiv 2 \pmod{17}$ for each r in $\mathbb{Z}_{17}^{\times}$. For example, $1' = 2$ and $3' = 12$. We find that $6' = 6$ and $11' = 11$, since 6 and $11 \equiv -6 \pmod{17}$ satisfy $x^2 \equiv 2 \pmod{17}$, showing that $\left(\frac{2}{17}\right) = 1$. The following rearrangement of 16! pairs each r with this new value of r'.

$$\begin{aligned} 16! &= (1 \cdot 2) \cdot (3 \cdot 12) \cdot (4 \cdot 9) \cdot (5 \cdot 14) \cdot 6 \cdot (7 \cdot 10) \cdot (8 \cdot 13) \cdot 11 \cdot (15 \cdot 16) \\ &\equiv 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 6 \cdot 11 \equiv -2^8 \pmod{17}, \end{aligned}$$

using the fact that $6 \cdot 11 \equiv 6(-6) \equiv -6^2 \equiv -2 \pmod{17}$. Since we have already established that $16! \equiv -1 \pmod{17}$, it follows that $2^8 \equiv 1 \equiv \left(\frac{2}{17}\right) \pmod{17}$.

Finally, let $a = 3$ and let r' be the solution of $rx \equiv 3 \pmod{17}$ for each r. For example, $1' = 3$ and $2' = 10$. Here we find that r' is not the same as r for any r in $\mathbb{Z}_{17}^{\times}$, which indicates that $x^2 \equiv 3 \pmod{17}$ has no solutions and $\left(\frac{3}{17}\right) = -1$. Again, we can calculate 16! modulo 17 by pairing each r with its corresponding r'.

$$\begin{aligned} 16! &= (1 \cdot 3) \cdot (2 \cdot 10) \cdot (4 \cdot 5) \cdot (6 \cdot 9) \cdot (7 \cdot 15) \cdot (8 \cdot 11) \cdot (12 \cdot 13) \cdot (14 \cdot 16) \\ &\equiv 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \equiv 3^8 \pmod{17}. \end{aligned}$$

We conclude that $3^8 \equiv -1 \equiv \left(\frac{3}{17}\right) \pmod{17}$. Note that in each of these examples the terms of 16! are not changed, but only rearranged to illustrate a different conclusion. ♢

The importance of Euler's Criterion is not as a method of calculating Legendre symbols but instead as a help in establishing other results about these symbols, as the following proofs illustrate.

COROLLARY B.26. *If p is an odd prime and a and b are integers, then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

PROOF. Using Euler's Criterion and standard exponent rules, we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Every Legendre symbol is an element of the set $\{1, 0, -1\}$, and the product of two elements in that set is also in the set. Since $p \geq 3$, this congruence must be an equality. □

COROLLARY B.27. *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

PROOF. We have that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ by Euler's Criterion. Since an integer power of -1 is either 1 or -1, this congruence is actually an equality. The second equation above is the observation that if $p = 4t + 1$ for some integer t, then $\frac{p-1}{2} = 2t$ is even, and if $p = 4t + 3$, then $\frac{p-1}{2} = 2t + 1$ is odd. □

Corollary B.26 implies that we can restrict our attention to Legendre symbols $\left(\frac{q}{p}\right)$ where q is a prime number. Of course, $\left(\frac{q}{p}\right) = 0$ if and only if $q = p$, so we may assume that $q \neq p$. To conclude this section, we state two more results and illustrate how they provide a general method of calculating symbols of the form $\left(\frac{q}{p}\right)$. The proofs of these theorems, which are not at all obvious, appear in the next section.

THEOREM B.28. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

THEOREM B.29 (Quadratic Reciprocity Theorem). *Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right), & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

EXAMPLE. Consider the congruence $x^2 \equiv 30 \pmod{59}$. By Corollary B.26, we see that

$$\left(\frac{30}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{3}{59}\right)\left(\frac{5}{59}\right).$$

We look at these symbols separately.

Since $59 \equiv 3 \pmod 8$, Theorem B.28 implies immediately that $\left(\frac{2}{59}\right) = -1$.

Both 3 and 59 are congruent to 3 modulo 4, so Theorem B.29 implies that $\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right)$. But now we can simplify the resulting symbol, working modulo 3. Since $59 \equiv 2 \pmod 3$, we have that $-\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right)$. Now by Theorem B.28, $-\left(\frac{2}{3}\right) = -(-1) = 1$. So $\left(\frac{3}{59}\right) = 1$.

Finally, since $5 \equiv 1 \pmod 4$, Theorem B.29 implies that $\left(\frac{5}{59}\right) = \left(\frac{59}{5}\right) = \left(\frac{4}{5}\right)$. Now 4 is clearly a quadratic residue modulo 5, or we could note that $\left(\frac{4}{5}\right) = \left(\frac{2\cdot 2}{5}\right) = \left(\frac{2}{5}\right)^2$ by Corollary B.26. Whether $\left(\frac{2}{5}\right)$ is 1 or -1 (it is -1 by Theorem B.28), its square is 1. So $\left(\frac{5}{59}\right) = 1$.

So now

$$\left(\frac{30}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{3}{59}\right)\left(\frac{5}{59}\right) = -1 \cdot 1 \cdot 1 = -1.$$

By definition, this means that $x^2 \equiv 30 \pmod{59}$ has no solutions. ◊

This example illustrates how we can use the Legendre symbol to determine the number of solutions of a quadratic congruence modulo a particular prime. More importantly, the Quadratic Reciprocity Theorem allows us to answer more general questions about a particular congruence modulo *all* primes, as in the following example.

EXAMPLE. For what primes p does the congruence $x^2 \equiv 3 \pmod p$ have a solution?

Direct calculation shows that a solution exists when $p = 2$ or $p = 3$, so assume that $p > 3$. By definition, $x^2 \equiv 3 \pmod p$ has a solution if and only if $\left(\frac{3}{p}\right) = 1$. Now p is congruent to 1 or 3 modulo 4, and since $3 \equiv 3 \pmod 4$, quadratic reciprocity allows us to say that

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For $p \neq 3$, either $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$, and we find that $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = -1$. (We simply need to note that $1^2 \equiv 1 \pmod 3$ and $2^2 \equiv 1 \pmod 3$, or we could use Theorem B.28.) Combining this calculation with the previous formula for $\left(\frac{3}{p}\right)$, we conclude that

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{12} \text{ or } p \equiv 11 \pmod{12} \\ -1, & \text{if } p \equiv 5 \pmod{12} \text{ or } p \equiv 7 \pmod{12}. \end{cases}$$

(For example, if $p \equiv 11 \pmod{12}$, then $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$, so that $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$.) So $x^2 \equiv 3 \pmod p$ has a solution if and only if $p = 2$, $p = 3$, $p \equiv 1 \pmod{12}$, or $p \equiv 11 \pmod{12}$. ◊

Exercises on Quadratic Congruences Modulo Primes.

1. Verify the claims made for quadratic congruences modulo 2 in Proposition B.22. (Hint: Show that if b is an odd integer, then $b^2 \equiv 1 \pmod 8$.)
2. Complete the square and solve the following quadratic congruences.
   (a) $2x^2 - 5x + 7 \equiv 0 \pmod{19}$.
   (b) $x^2 + x - 3 \equiv 0 \pmod{13}$.
   (c) $5x^2 - 3x + 1 \equiv 0 \pmod{17}$.
3. Calculate the following Legendre symbols.
   (a) $\left(\frac{-13}{47}\right)$.
   (b) $\left(\frac{21}{71}\right)$.
   (c) $\left(\frac{55}{97}\right)$.
4. Find the *number* of solutions of each of the following quadratic congruences. (All moduli are prime numbers.)
   (a) $x^2 \equiv 6 \pmod{389}$.
   (b) $2x^2 - 13x + 7 \equiv 0 \pmod{719}$.
   (c) $7x^2 + 17x + 12 \equiv 0 \pmod{1607}$.
5. Assuming Theorem B.28, find a formula for the Legendre symbol $\left(\frac{-2}{p}\right)$ in terms of p, when p is an odd prime.
6. Assuming the Quadratic Reciprocity Theorem, find a formula for the Legendre symbol $\left(\frac{5}{p}\right)$ in terms of p, when $p \neq 2, 5$.
7. Repeat the method of Exercise 6 to find a formula for the symbol $\left(\frac{7}{p}\right)$ when $p \neq 2, 7$.
8. Let q be a prime number with $q \equiv 3 \pmod 4$. If $p \neq q$ is an odd prime, show that $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$.
9. For each of the following pairs a and p, find the solution of the congruence $rx \equiv a \pmod p$ for each r in $\mathbb{Z}_p^\times$, as in the proof of Euler's Criterion.
   (a) $a = 5$, $p = 7$.
   (b) $a = 8$, $p = 11$.
   (c) $a = 10$, $p = 17$.
10. By computing powers of 2, verify that the value of $\left(\frac{2}{p}\right)$ obtained from Euler's Criterion is the same as that given by Theorem B.28, for each odd prime $p < 50$.
11. Find all primes p that divide $x^2 + 5$ for some integer x.
12. Find all primes p that divide $x^2 + x + 1$ for some integer x.
13. Find all primes p that divide $2x^2 + 6x + 1$ for some integer x.
14. Find all primes p that divide $2x^2 - 5x + 2$ for some integer x.

The Quadratic Reciprocity Theorem

The connection between the number of solutions of $x^2 \equiv q \pmod p$ and of $x^2 \equiv p \pmod q$ when p and q are distinct odd primes, as stated in the Quadratic Reciprocity Theorem, was noticed in the late 18th century by Euler and Legendre. Neither was able to prove that it holds in general however. The first complete proof of quadratic reciprocity was given in 1801 by Gauss, who had

discovered the result independently. Gauss thought very highly of this result, referring to it as the *Theorema Aureum*, or Golden Theorem. He eventually gave six different proofs of this result, and more than 200 other proofs have been found since.

In this section, we will present a recent proof of the Quadratic Reciprocity Theorem due to Sey Y. Kim, requiring only Euler's Criterion and Wilson's Theorem as preliminaries. (Kim's proof first appeared in the January 2004 *American Mathematical Monthly*, and is reprinted in *Biscuits of Number Theory*, Dolciani Mathematical Expositions #34.) We first prove Theorem B.28 on the calculation of $\left(\frac{2}{p}\right)$, beginning with a preliminary result due to Gauss, which is used in many proofs of quadratic reciprocity. Although we require this lemma only in the special case of $a = 2$, it is just as easy to state and prove in general.

LEMMA B.30 (Gauss's Lemma). *Let p be an odd prime and let a be an integer relatively prime to p. Let n be the number of integers among a, $2a$, $3a, \ldots, \frac{p-1}{2}a$ whose remainders on division by p are larger than $\frac{p-1}{2}$. Then $\left(\frac{a}{p}\right) = (-1)^n$.*

EXAMPLE. Let $p = 29$, so that $\frac{p-1}{2} = 14$, and let $a = 17$. In the table below, we list ka for $1 \le k \le 14$. For each multiple of a, we calculate the remainder r on division of ka by p and the integer r' congruent to ka modulo p that is smallest in absolute value. Notice that $r' = r$ if $r \le \frac{p-1}{2}$ and $r' = r - p$ if $r > \frac{p-1}{2}$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ka	17	34	51	68	85	102	119	136	153	170	187	204	221	238
r	17	5	22	10	27	15	3	20	8	25	13	1	18	6
r'	−12	5	−7	10	−2	−14	3	−9	8	−4	13	1	−11	6

Now n is the number of elements in the r row that exceed 14, or equivalently, the number of negative elements in the r' row. Here we find that $n = 7$. The claim of Gauss's lemma is that then $\left(\frac{17}{29}\right) = (-1)^7 = -1$, so that 17 is not a quadratic residue modulo 29. An important observation is that the absolute values of the elements in the r' row represent all the integers 1 through 14 without repetition. We will see that this is not by accident. ◊

PROOF. Let p be an odd prime and let a be relatively prime to p. For $k = 1, 2, \ldots, \frac{p-1}{2}$, let $r_k = ka \bmod p$. None of the r_k's is zero, since otherwise p divides ka, but we know that $p \nmid a$ and $p \nmid k$ for $1 \le k \le \frac{p-1}{2}$. Label the remainders r_k less than or equal to $\frac{p-1}{2}$ as $v_1, \ldots, v_m$, and those larger than $\frac{p-1}{2}$ as $u_1, \ldots, u_n$ (so n is as defined in the statement of Gauss's Lemma). We first show that the numbers $v_1, \ldots, v_m, p - u_1, \ldots, p - u_n$ are the integers $1, 2, \ldots, \frac{p-1}{2}$ in some order.

We find that $1 \le p - u_i \le \frac{p-1}{2}$ for each i, so $v_1, \ldots, v_m, p - u_1, \ldots, p - u_n$ form a collection of $\frac{p-1}{2}$ integers between 1 and $\frac{p-1}{2}$. If we can show that no two of them are equal, then they must be some rearrangement of the numbers $1, 2, \ldots, \frac{p-1}{2}$. If $v_i = v_j$ for some i and j, then there are integers k and ℓ between 1 and $\frac{p-1}{2}$ such that ak and $a\ell$ have the same remainder on division by p, that is, $ak \equiv a\ell \pmod{p}$. But since $\gcd(a, p) = 1$, this means that $k \equiv \ell \pmod{p}$, and so $k = \ell$. Likewise, we cannot have $p - u_i = p - u_j$ if $i \ne j$. Finally, suppose that $v_i = p - u_j$ for some i and j, so that $v_i + u_j = p \equiv 0 \pmod{p}$. Then there are integers k and ℓ between 1 and $\frac{p-1}{2}$ such that $ak + a\ell \equiv v_i + u_j \pmod{p}$, or $a(k + \ell) \equiv 0 \pmod{p}$. Now since $\gcd(a, p) = 1$, it follows that $k + \ell$ is divisible by p. But that is impossible since $1 \le k, \ell \le \frac{p-1}{2}$.

Now consider the product of the numbers ka for $1 \le k \le \frac{p-1}{2}$. Notice that

$$a \cdot 2a \cdot 3a \cdots \frac{p-1}{2}a = a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (v_1 \cdots v_m) \cdot (u_1 \cdots u_n) \pmod{p} \tag{B.13}$$

because each term in the product is congruent modulo p to its remainder on division by p. On the other hand, since $\{1, 2, \ldots, \frac{p-1}{2}\} = \{v_1, \ldots, v_m, p-u_1, \ldots, p-u_n\}$,

$$\left(\frac{p-1}{2}\right)! = (v_1 \cdots v_m)(p-u_1)\cdots(p-u_n) \equiv (-1)^n (v_1 \cdots v_m)\cdot(u_1 \cdots u_n) \pmod{p} \tag{B.14}$$

using the fact that $p - u_i \equiv -u_i \pmod{p}$ and factoring out the n terms of -1 that result. Combining (B.13) and (B.14), we see that $(-1)^n \cdot \left(\frac{p-1}{2}\right)! \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. Since p does not divide $\left(\frac{p-1}{2}\right)!$ (a product of positive integers less than p), we can cancel that term from both sides of the congruence and conclude that $(-1)^n \equiv a^{\frac{p-1}{2}} \pmod{p}$. But $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ by Euler's Criterion. Since both $(-1)^n$ and $\left(\frac{a}{p}\right)$ are ± 1, the result of Lemma B.30 follows. □

We now prove Theorem B.28, which we restate below, as a consequence of Lemma B.30.

THEOREM. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

PROOF. Let p be an odd prime. Since $a = 2$ is relatively prime to p, Lemma B.30 implies that $\left(\frac{2}{p}\right) = (-1)^n$ where n is the number of elements in the set $S = \left\{2\cdot 1, 2\cdot 2, \ldots, 2\cdot\frac{p-1}{2}\right\} = \{2, 4, \ldots, p-1\}$ whose remainders on division by p exceed $\frac{p-1}{2}$. Each integer in S is itself a remainder, and the number of elements of S *not* exceeding $\frac{p-1}{2}$ is $\left\lfloor \frac{p-1}{4} \right\rfloor$. (In general, the number of positive multiples of k less than or equal to some positive integer m is $\left\lfloor \frac{m}{k} \right\rfloor$.) Since there are $\frac{p-1}{2}$ elements in S, we see that $n = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$.

Let $p = 8q + r$ with $0 \le r < 8$. (Since p is odd, r is 1, 3, 5, or 7.) Then

$$n = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \left(4q + \frac{r-1}{2}\right) - \left\lfloor 2q + \frac{r-1}{4} \right\rfloor = 2q + \left(\frac{r-1}{2} - \left\lfloor \frac{r-1}{4} \right\rfloor\right).$$

So then n has the same parity as

$$\frac{r-1}{2} - \left\lfloor \frac{r-1}{4} \right\rfloor = \begin{cases} 0 - \lfloor 0 \rfloor = 0, & \text{if } r = 1 \\ 1 - \left\lfloor \frac{1}{2} \right\rfloor = 1, & \text{if } r = 3 \\ 2 - \lfloor 1 \rfloor = 1, & \text{if } r = 5 \\ 3 - \left\lfloor \frac{3}{2} \right\rfloor = 2, & \text{if } r = 7. \end{cases}$$

That is, n is even if $p \equiv 1$ or $7 \pmod 8$, and n is odd if $p \equiv 3$ or $5 \pmod 8$. The formula for $\left(\frac{2}{p}\right)$ in Theorem B.28 follows. □

Proof of the Quadratic Reciprocity Theorem. Throughout this subsection, let p and q be distinct odd primes, and let

$$S = \left\{ a \in \mathbb{Z} \;\middle|\; 1 \le a \le \frac{pq-1}{2} \text{ and } \gcd(a, p) = 1 \right\} \text{ and } T = \left\{ a \in S \;\middle|\; \gcd(a, q) = 1 \right\}. \tag{B.15}$$

The set $T' = S - T$ consists of all multiples of q in S. Let s, t, and t' be the products of all elements in S, T, and T' respectively. Notice that we can also write T as

$$T = \left\{ a \in \mathbb{Z} \;\middle|\; 1 \le a \le \frac{pq-1}{2} \text{ and } \gcd(a, pq) = 1 \right\},$$

so that the set T and the product t are unchanged by interchanging p and q. We will prove the Quadratic Reciprocity Theorem by comparing the values of t modulo p, modulo q, and modulo pq.

LEMMA B.31. *Let p and q be distinct odd primes and let t be the product of all the elements in the set T defined as in* (B.15). *Then*

$$t \equiv \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod{p} \qquad \textit{and} \qquad t \equiv \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \pmod{q}.$$

PROOF. Consider S as defined in (B.15). On one hand, since $\frac{pq-1}{2} = \frac{q-1}{2} \cdot p + \frac{p-1}{2}$, we find that the elements of S reduced modulo p consist of $\frac{q-1}{2}$ copies of the set $\{1, 2, \ldots, p-1\}$ and an additional copy of $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. So the product of elements of S satisfies

$$s \equiv ((p-1)!)^{\frac{q-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{-1}{q}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod{p}, \tag{B.16}$$

since $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem and $(-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right)$ by Euler's Criterion.

On the other hand, since S is the union of the disjoint sets T and T', we have that $s = t \cdot t'$. With $\frac{pq-1}{2} = \frac{p-1}{2} \cdot q + \frac{q-1}{2}$, we see that $T' = \left\{1 \cdot q, 2 \cdot q, \ldots, \frac{p-1}{2} \cdot q\right\}$. Therefore,

$$s = t \cdot t' = t \cdot q^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv t \cdot \left(\frac{q}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod{p}, \tag{B.17}$$

since $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$, again by Euler's Criterion.

Combining (B.16) and (B.17), then $t \cdot \left(\frac{q}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{-1}{q}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. Since all terms in the product $\left(\frac{p-1}{2}\right)!$ are relatively prime to p, and $\left(\frac{q}{p}\right) = \pm 1$, we conclude that $t \equiv \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod{p}$, as we wanted to show. If the primes p and q are interchanged, the same argument establishes that $t \equiv \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \pmod{q}$. □

EXAMPLE. To illustrate the claims in this proof, let $p = 7$ and $q = 5$. Then

$$S = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17\},$$

with

$$T = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17\} \quad \text{and} \quad T' = \{5, 10, 15\}.$$

We see that, reduced modulo 7, the elements of S run from 1 through 6 twice, with three additional terms congruent to 1, 2, and 3. So $s \equiv (6!)^2 \cdot 3! \equiv (-1)^2 \cdot 3! \equiv \left(\frac{-1}{5}\right) \cdot 3! \pmod{7}$. But we also have $s = t \cdot t'$ where $t' = 5^3 \cdot 3! \equiv \left(\frac{5}{7}\right) \cdot 3! \pmod{7}$. We conclude that $t \equiv \left(\frac{-1}{5}\right)\left(\frac{5}{7}\right) \pmod{7}$.

Now if we let $p = 5$ and $q = 7$, then

$$S = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17\},$$

with

$$T = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17\} \quad \text{and} \quad T' = \{7, 14\}.$$

As claimed, this change does not affect the set T. Now looking at the product of the elements of S modulo 5, we see that $s \equiv (4!)^3 \cdot 2! \equiv (-1)^3 \cdot 2! \equiv \left(\frac{-1}{7}\right) \cdot 2! \pmod{5}$. But $s = t \cdot t'$ with $t' = 7^2 \cdot 2! \equiv \left(\frac{7}{5}\right) \cdot 2! \pmod{5}$. We conclude in the same way that $t \equiv \left(\frac{-1}{7}\right)\left(\frac{7}{5}\right) \pmod{5}$. ◊

Now we consider the set T, and the product t, modulo pq. Notice that for each integer n relatively prime to pq, either n or $-n$, but not both, is congruent modulo pq to an element of T.

LEMMA B.32. *Let p and q be distinct odd primes. Then the following statements are true.*

(1) $x^2 \equiv 1 \pmod{pq}$ *has four solutions. There is an element* b *in* T *so that these solutions are congruent modulo* pq *to* 1, -1, b, *and* $-b$.
(2) *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 1 \pmod 4$, *then* $x^2 \equiv -1 \pmod{pq}$ *has four solutions. There is an element* c *in* T *so that these solutions are congruent modulo* pq *to* c, $-c$, bc, *and* $-bc$, *where* b *is as in statement* (1). *On the other hand, if* $p \equiv 3 \pmod 4$ *or* $q \equiv 3 \pmod 4$, *then* $x^2 \equiv -1 \pmod{pq}$ *has no solutions.*

PROOF. The claims about the number of solutions of these congruences follow immediately from Corollary B.37 and the formula for the Legendre symbol $\left(\frac{-1}{p}\right)$ (Corollary B.27), which we proved using only Euler's Criterion. If a is a solution of $x^2 \equiv \pm 1 \pmod{pq}$, then $-a$ satisfies the same congruence, with $a \not\equiv -a \pmod{pq}$ since a is relatively prime to the odd number pq. If c satisfies $x^2 \equiv -1 \pmod{pq}$, then so does bc, since $(bc)^2 = b^2c^2 \equiv 1(-1) \equiv -1 \pmod{pq}$. □

EXAMPLE. Let $p = 5$ and $q = 13$. The congruence $x^2 \equiv 1 \pmod{65}$ has four solutions, found by solving all possible pairs of congruences $x \equiv \pm 1 \pmod 5$ and $x \equiv \pm 1 \pmod{13}$. Since p and q are both congruent to 1 modulo 4, the congruence $x^2 \equiv -1 \pmod{65}$ also has four solutions. We find that $x^2 \equiv -1 \pmod 5$ has solutions ± 2 and $x^2 \equiv -1 \pmod{13}$ has solutions ± 5. In general, a simultaneous solution of $t \equiv r \pmod 5$ and $t \equiv s \pmod{13}$ is given by $t = (26r - 25s) \bmod 65$. We compile the following tables.

r	s	$t = 26r - 25s$	$t \bmod 65$	r	s	$t = 26r - 25s$	$t \bmod 65$
1	1	1	1	2	5	−73	−8
1	−1	51	−14	2	−5	177	−18
−1	1	−51	14	−2	5	−177	18
−1	−1	−1	−1	−2	−5	73	8

In the notation of Lemma B.32, we have that $b = 14$, and we can let $c = 8$. Notice that $14 \cdot 8 = 112 \equiv -18 \pmod{65}$. ◊

Now every a in T has an inverse modulo pq since $\gcd(a, pq) = 1$. Define a' to be the unique element in T such that either $a' \equiv a^{-1} \pmod{pq}$ or $a' \equiv -a^{-1} \pmod{pq}$. We can describe a' as the unique solution of $ax \equiv \pm 1 \pmod{pq}$ in T. Notice that $(a')' = a$ for all $a \in T$, and that $a' = a$ precisely when a is a solution of $x^2 \equiv \pm 1 \pmod{pq}$.

LEMMA B.33. *Let* p *and* q *be distinct odd primes, let* T *be as in* (B.15), *and let* b *be as defined in Lemma B.32. Let* t *be the product of the elements of* T. *Then*

$$t \equiv \begin{cases} \pm 1 \pmod{pq}, & \text{if } p \equiv 1 \pmod 4 \text{ and } q \equiv 1 \pmod 4, \\ \pm b \pmod{pq}, & \text{if } p \equiv 3 \pmod 4 \text{ or } q \equiv 3 \pmod 4. \end{cases}$$

PROOF. Using the notation of Lemma B.32, the set T consists of pairs of *distinct* elements a and a' for which $aa' \equiv \pm 1 \pmod{pq}$, together with 1 and b in every case, and with c and either bc or $-bc$ when $p \equiv 1 \equiv q \pmod 4$. So we can write the product t as

$$t = \begin{cases} 1 \cdot b \cdot c \cdot (\pm bc) \cdot \prod(aa'), & \text{if } p \equiv 1 \pmod 4 \text{ and } q \equiv 1 \pmod 4, \\ 1 \cdot b \cdot \prod(aa'), & \text{if } p \equiv 3 \pmod 4 \text{ or } q \equiv 3 \pmod 4. \end{cases}$$

In both cases, the product is taken over representatives of each pair a and a' with $a \neq a'$, so that each term in the product is congruent to 1 or -1 modulo pq. So $t \equiv \pm b \pmod{pq}$ if $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. On the other hand, we find that $t \equiv \pm(b^2c^2) \equiv \pm 1 \pmod{pq}$, if $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$, since $b^2 \equiv 1 \pmod{pq}$ and $c^2 \equiv -1 \pmod{pq}$. □

EXAMPLE. When $p = 5$ and $q = 13$, then T contains 24 elements—the integers from 1 to 32 not divisible by 5 or 13. Aside from 1, $b = 14$, $c = 8$, and $-bc = 18$ as we found above, T consists

of ten pairs of different elements a and a' for which $aa' \equiv \pm 1 \pmod{65}$. The product of all the elements of T is presented below, with each a paired with its corresponding a', found by solving linear congruences.

$$\begin{aligned} t &= 1 \cdot 14 \cdot 8 \cdot 18 \cdot (2 \cdot 32)(3 \cdot 22)(4 \cdot 16)(6 \cdot 11)(7 \cdot 28)(9 \cdot 29)(12 \cdot 27)(17 \cdot 23)(19 \cdot 24)(21 \cdot 31) \\ &\equiv 1 \cdot 14 \cdot 8 \cdot 18 \cdot (-1) \cdot 1 \cdot (-1) \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \cdot 1 \cdot 1 \cdot 1 \equiv -1 \cdot 14 \cdot 8 \cdot 18 \pmod{65}. \end{aligned}$$

Since $18 \equiv -14 \cdot 8 \pmod{65}$, then $t \equiv (14^2)(8^2) \equiv 1(-1) \equiv -1 \pmod{65}$. In particular, with p and q congruent to 1 modulo 4, we find that $t \equiv \pm 1 \pmod{pq}$, as claimed in Lemma B.33. ◊

Now Lemma B.31 implies that $t \equiv \pm 1 \pmod{p}$ and $t \equiv \pm 1 \pmod{q}$. Notice that if $t \equiv 1 \pmod{p}$ and $t \equiv 1 \pmod{q}$, then $t \equiv 1 \pmod{pq}$, and if $t \equiv -1 \pmod{p}$ and $t \equiv -1 \pmod{q}$, then $t \equiv -1 \pmod{pq}$. On the other hand, if $t \equiv 1 \pmod{p}$ and $t \equiv -1 \pmod{q}$ or vice versa, then $t \equiv \pm b \pmod{pq}$ in the notation of Lemma B.32. So combining Lemmas B.31 and B.33, we conclude that $\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$ if and only if $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$, or since all the symbols are ± 1,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right), & \text{if } p \equiv 1 \pmod 4 \text{ and } q \equiv 1 \pmod 4 \\ -\left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right), & \text{if } p \equiv 3 \pmod 4 \text{ or } q \equiv 3 \pmod 4. \end{cases} \tag{B.18}$$

But by Corollary B.27, we have that

$$\left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) = \begin{cases} 1 \cdot \ \ 1 = \ \ 1, & \text{if } p \equiv 1 \pmod 4 \text{ and } q \equiv 1 \pmod 4, \\ 1 \cdot -1 = -1, & \text{if } p \equiv 1 \pmod 4 \text{ and } q \equiv 3 \pmod 4, \\ -1 \cdot \ \ 1 = -1, & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 1 \pmod 4, \\ -1 \cdot -1 = \ \ 1, & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases} \tag{B.19}$$

Combining (B.18) and (B.19) implies the following result, equivalent to the Quadratic Reciprocity Theorem.

THEOREM. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Jacobi Symbols. To conclude this section, we introduce a generalization of Legendre symbols, which is useful for computation.

DEFINITION. Let $b = p_1 p_2 \cdots p_k$ be an odd, positive integer, with each p_i an odd prime, not assumed to be distinct. Then for any integer a, the *Jacobi symbol* $\left(\frac{a}{b}\right)$ is defined as a product of Legendre symbols:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

EXAMPLE. Since $45 = 3 \cdot 3 \cdot 5$, we have that $\left(\frac{14}{45}\right) = \left(\frac{14}{3}\right)\left(\frac{14}{3}\right)\left(\frac{14}{5}\right)$, with the Legendre symbols calculated as usual. Here $\left(\frac{14}{3}\right) = \left(\frac{2}{3}\right) = -1$ and $\left(\frac{14}{5}\right) = \left(\frac{4}{5}\right) = 1$, so $\left(\frac{14}{45}\right) = (-1)(-1)(1) = 1$. ◊

We prove two results, as corollaries of Theorems B.28 and B.29 respectively, which show that Jacobi symbols can be simplified in a process that is identical to that of Legendre symbols.

COROLLARY B.34. *Let b be an odd, positive integer. Then*

$$\left(\frac{2}{b}\right) = \begin{cases} 1, & \text{if } b \equiv 1 \pmod 8 \text{ or } b \equiv 7 \pmod 8 \\ -1, & \text{if } b \equiv 3 \pmod 8 \text{ or } b \equiv 5 \pmod 8. \end{cases}$$

PROOF. Write $b = p_1 p_2 \cdots p_k$ where each p_i is an odd prime. Let k_1, k_3, k_5, and k_7 be the number of terms in this factorization congruent to 1, 3, 5, or 7 respectively modulo 8. Then by the definition of the Jacobi symbol and Theorem B.28, we see that

$$\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right) = (1)^{k_1}(-1)^{k_3}(-1)^{k_5}(1)^{k_7} = (-1)^{k_3+k_5}.$$

On the other hand, b itself is congruent to $(1)^{k_1}(3)^{k_3}(5)^{k_5}(7)^{k_7}$ modulo 8. Since $3^2 \equiv 1 \pmod 8$, $5^2 \equiv 1 \pmod 8$, and $7^2 \equiv 1 \pmod 8$, we see that both of these expressions depend entirely on the parity of k_3, k_5, and k_7 (1^{k_1} will be 1 in both expressions in any case). We can complete the proof by listing all the possibilities, as in the table below.

$k_3 \bmod 2$	$k_5 \bmod 2$	$k_7 \bmod 2$	$\left(\frac{2}{b}\right)$	$b \bmod 8$
0	0	0	1	1
0	0	1	1	7
0	1	0	−1	5
0	1	1	−1	3
1	0	0	−1	3
1	0	1	−1	5
1	1	0	1	7
1	1	1	1	1

We see from the table that $\left(\frac{2}{b}\right) = 1$ if $b \equiv 1 \pmod 8$ or $b \equiv 7 \pmod 8$, and $\left(\frac{2}{b}\right) = -1$ if $b \equiv 3 \pmod 8$ or $b \equiv 5 \pmod 8$, as we wanted to show. □

COROLLARY B.35. *Let a and b be odd, positive integers. Then*

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right), & \text{if } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right), & \text{if } a \equiv 3 \pmod 4 \text{ and } b \equiv 3 \pmod 4, \end{cases}$$

PROOF. If a and b have some prime divisor in common, then it is easy to see that $\left(\frac{a}{b}\right)$ and $\left(\frac{b}{a}\right)$ are both zero, so that *both* equations above hold in that case. So we assume that $\gcd(a, b) = 1$.

Let $b = p_1 p_2 \cdots p_k$ with each p_i an odd prime. Let r be the number of terms in this factorization that are congruent to 3 modulo 4. Notice that then $b \equiv (1)^{k-r}(3)^r \equiv 3^r \pmod 4$. Since $3^2 \equiv 1 \pmod 4$, we see that $b \equiv 1 \pmod 4$ if r is even, and $b \equiv 3 \pmod 4$ if r is odd.

Similarly, let $a = q_1 q_2 \cdots q_\ell$ with each q_i an odd prime, and let s be the number of these primes that are congruent to 3 modulo 4. Again, we can say that $a \equiv 1 \pmod 4$ if s is even, and $a \equiv 3 \pmod 4$ if s is odd. We assume that a and b are relatively prime, which means that no p_i is the same as any q_j.

By definition of the Jacobi symbol,

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

Corollary B.26 applies to each of the resulting Legendre symbols, for instance,

$$\left(\frac{a}{p_1}\right) = \left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\cdots\left(\frac{q_\ell}{p_1}\right).$$

So we see that $\left(\frac{a}{b}\right)$ is the product of Legendre symbols of the form $\left(\frac{q_i}{p_j}\right)$ with i varying from 1 to ℓ and j varying from 1 to k. (There are $k \cdot \ell$ symbols in that product.)

The Quadratic Reciprocity Theorem now applies to each of these Legendre symbols. We may write

$$\left(\frac{q_i}{p_j}\right) = e_{i,j}\left(\frac{p_j}{q_i}\right)$$

where $e_{i,j} = 1$ if $q_i \equiv 1 \pmod 4$ or $p_j \equiv 1 \pmod 4$, and $e_{i,j} = -1$ if $q_i \equiv 3 \pmod 4$ and $p_j \equiv 3 \pmod 4$. Notice that, using our notation above, $e_{i,j} = -1$ for exactly rs pairs i, j. Again using Corollary B.26 and the definition of the Jacobi symbol, we get that $\left(\frac{a}{b}\right) = (-1)^{rs}\left(\frac{b}{a}\right)$.

Finally then, we see that $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ if rs is even, and $\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ if rs is odd. But rs is even if r is even or s is even, and rs is odd if r is odd and s is odd. By what we noted above, then $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ if $a \equiv 1 \pmod 4$ or $b \equiv 1 \pmod 4$, and $\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ if $a \equiv 3 \pmod 4$ and $b \equiv 3 \pmod 4$. □

EXAMPLE. Consider the Legendre symbol $\left(\frac{133}{199}\right)$. Here 199 is prime, while 133 is not. But the preceding results show that we can treat 133 as if it is prime in computing this Legendre symbol.

$$\left(\frac{133}{199}\right) = \left(\frac{199}{133}\right) = \left(\frac{66}{133}\right) = \left(\frac{2}{133}\right)\left(\frac{33}{133}\right) = -\left(\frac{133}{33}\right) = -\left(\frac{1}{33}\right) = -1.$$

We use the fact that $133 \equiv 1 \pmod 4$ and $133 \equiv 5 \pmod 8$ in this sequence of equations. Here $\left(\frac{1}{b}\right) = 1$ for every odd, positive integer b. For instance, $\left(\frac{1}{33}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{11}\right) = 1 \cdot 1 = 1$. ◊

Jacobi symbols are useful in simplifying calculation of Legendre symbols, since we do not need to worry about completely factoring all terms in the process of simplification. (We must, however, have all terms odd and positive in applying these corollaries.) But Jacobi symbols do not have the same meaning as Legendre symbols in terms of the number of solutions of a quadratic congruence. In particular, if $\left(\frac{a}{b}\right) = 1$ with b *not* prime, we cannot assume that $x^2 \equiv a \pmod b$ has exactly two solutions. We will consider quadratic congruences modulo composite values in the next section.

Exercises on the Quadratic Reciprocity Theorem.

1. Use Gauss's Lemma to calculate the following Legendre symbols.
   (a) $\left(\frac{11}{17}\right)$.
   (b) $\left(\frac{2}{29}\right)$.
   (c) $\left(\frac{7}{31}\right)$.
2. Let T be defined as in (B.15) for some distinct odd primes p and q. Show that T contains exactly $\frac{(p-1)(q-1)}{2}$ elements.
3. For each of the following pairs of primes p and q, let T be defined as in (B.15) and let t be the product of the elements of T. Use the method of Lemma B.33 to calculate the the remainder of t on division by pq.
   (a) $p = 3$ and $q = 5$.
   (b) $p = 7$ and $q = 11$.
   (c) $p = 5$ and $q = 17$.
4. Calculate the following Legendre symbols.
   (a) $\left(\frac{26}{73}\right)$.
   (b) $\left(\frac{19}{97}\right)$.
   (c) $\left(\frac{42}{107}\right)$.
5. Calculate the following Jacobi symbols $\left(\frac{a}{b}\right)$ in two ways—first by factoring a and b and using the definition of the Jacobi symbol (together with the Quadratic Reciprocity Theorem and other facts about Legendre symbols), and then by applying Corollaries B.34 and B.35.
   (a) $\left(\frac{23}{35}\right)$.
   (b) $\left(\frac{67}{133}\right)$.

(c) $\left(\frac{266}{11063}\right)$, given that $11063 = 13 \cdot 23 \cdot 37$.

6. Let b be an odd positive integer. Show that
$$\left(\frac{-1}{b}\right) = \begin{cases} 1, & \text{if } b \equiv 1 \pmod 4 \\ -1, & \text{if } b \equiv 3 \pmod 4. \end{cases}$$
7. Find all odd primes p for which $\left(\frac{11}{p}\right) = 1$.
8. Find all odd primes p for which $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right)$.
9. Find all odd primes p for which $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right)$.
10. Find all odd primes p for which $\left(\frac{3}{p}\right) = \left(\frac{7}{p}\right)$.

Quadratic Congruences Modulo Composite Integers

Assuming that we can solve a quadratic congruence $f(x) \equiv 0 \pmod p$ where p is a prime number, we can then solve $f(x) \equiv 0 \pmod m$ for an arbitrary positive integer m. Our approach is similar to what we saw with linear congruences. First we show, using the Chinese Remainder Theorem, that it suffices to solve $f(x) \equiv 0 \pmod{p^e}$ where p is prime and e is a positive integer. Then we demonstrate that we can use solutions of $f(x) \equiv 0 \pmod p$ to solve $f(x) \equiv 0 \pmod{p^e}$ for any $e > 1$ by a recursive process. Our main results of this section apply to polynomial congruences of arbitrary degree.

THEOREM B.36. *Let $f(x)$ be a polynomial with integer coefficients. Let m and n be relatively prime positive integers. Then t satisfies $f(x) \equiv 0 \pmod{mn}$ if and only if $t \equiv r \pmod m$ and $t \equiv s \pmod n$ for some solution r of $f(x) \equiv 0 \pmod m$ and some solution s of $f(x) \equiv 0 \pmod n$.*

PROOF. Suppose first that t is a solution of $f(x) \equiv 0 \pmod{mn}$, so that mn divides $f(t)$. Then $f(t) \equiv 0 \pmod m$ and $f(t) \equiv 0 \pmod n$, so we can let $r = t$ and $s = t$. Conversely, suppose that $f(r) \equiv 0 \pmod m$ and $f(s) \equiv 0 \pmod n$, and that t is an integer such that $t \equiv r \pmod m$ and $t \equiv s \pmod n$. Then $f(t) \equiv f(r) \equiv 0 \pmod m$ and $f(t) \equiv f(s) \equiv 0 \pmod n$ by properties of congruence, and so $f(t)$ is a common multiple of m and n. Since $\gcd(m, n) = 1$, then $f(t)$ must be divisible by $\operatorname{lcm}(m, n) = mn$. That is, $f(t) \equiv 0 \pmod{mn}$. □

The implication of this theorem is that when m and n are relatively prime, we can obtain all solutions of $f(x) \equiv 0 \pmod{mn}$ by solving $f(x) \equiv 0 \pmod m$ and $f(x) \equiv 0 \pmod n$ separately, and then applying the Chinese Remainder Theorem to all such pairs of solutions. The following example illustrates this method.

EXAMPLE. Find all solutions of $x^2 - 3 \equiv 0 \pmod{407}$, where $407 = 11 \cdot 37$.

In a previous example, we saw that $\left(\frac{3}{p}\right) = 1$ if $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$. So both $x^2 - 3 \equiv 0 \pmod{11}$ and $x^2 - 3 \equiv 0 \pmod{37}$ have two solutions, which we find by direct calculation to be 5 and 6 (modulo 11), and 15 and 22 (modulo 37). Thus t satisfies $x^2 - 3 \equiv 0 \pmod{407}$ if and only if $t \equiv r \pmod{11}$ and $t \equiv s \pmod{37}$ where $r = 5$ or 6 and $s = 15$ or 22. Using the Chinese Remainder Theorem, the solution of $t \equiv r \pmod{11}$ and $t \equiv s \pmod{37}$ is congruent to $111r - 110s$ modulo 407. We compile the following table.

r	s	$t = 111r - 110s$	$t \bmod 407$
5	15	−1095	126
5	22	−1865	170
6	15	−984	237
6	22	−1754	281

Therefore $x^2 - 3 \equiv 0 \pmod{407}$ has four solutions: 126, 170, 237, and 281. ◊

Theorem B.36 is easily extended to more than two congruences if the moduli are *pairwise* relatively prime. In particular, this means that if $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with each p_i a distinct prime and each e_i a positive integer, then it suffices to solve $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for $1 \leq i \leq k$ in order to solve $f(x) \equiv 0 \pmod{m}$.

COROLLARY B.37. *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with each p_i a distinct prime number, and each e_i positive. Let $f(x)$ be a polynomial with integer coefficients and suppose that for $i = 1, 2, \ldots, k$, the congruence $f(x) \equiv 0 \pmod{p_i^{e_i}}$ has n_i solutions. Then $f(x) \equiv 0 \pmod{m}$ has $n_1 n_2 \cdots n_k$ solutions.*

PROOF. Theorem B.36 implies that there is a one-to-one correspondence between the set of solutions of $f(x) \equiv 0 \pmod{m}$ and the set of ordered k-tuples $(a_1, a_2, \ldots, a_k)$ where a_i is an element of $\mathbb{Z}_{p_i^{e_i}}$ that satisfies $f(x) \equiv 0 \pmod{p_i^{e_i}}$. □

Corollary B.37 also implies that if $f(x) \equiv 0 \pmod{p_i^{e_i}}$ has no solutions for at least one i, then $f(x) \equiv 0 \pmod{m}$ can have no solutions.

Prime Power Moduli. Next we show that if we have all solutions of $f(x) \equiv 0 \pmod{p}$ for some prime p, then we can solve $f(x) \equiv 0 \pmod{p^e}$ for every $e > 1$. The method is a step-by-step approach, building from solutions of $f(x) \equiv 0 \pmod{p}$ to those of $f(x) \equiv 0 \pmod{p^2}$, and then $f(x) \equiv 0 \pmod{p^3}$, and so forth until we reach the power of p of interest. We illustrate the approach with an example before stating the main theorem.

EXAMPLE. Let $f(x) = x^2+3x-2$. Find all solutions of $f(x) \equiv 0 \pmod{2197}$, where $2197 = 13^3$.

First consider $f(x)$ modulo 13. Completing the square transforms $x^2 + 3x - 2 \equiv 0 \pmod{13}$ into $(2x+3)^2 \equiv 17 \pmod{13}$, and since $17 \equiv 4 \pmod{13}$, this congruence has two solutions, which we calculate to be 4 and 6. Now any solution of $f(x) \equiv 0 \pmod{169}$ must also be a solution of $f(x) \equiv 0 \pmod{13}$, so must have the form $s = r + 13t$ where $r = 4$ or $r = 6$ and t is some integer. (We can assume that $0 \leq t < 13$ to find the distinct possibilities modulo 169.) Direct expansion shows that

$$f(s) = f(r + 13t) = (r + 13t)^2 + 3(r + 13t) - 2 = (r^2 + 3r - 2) + 13(2r + 3)t + 13^2 t^2.$$

Note that $r^2 + 3r - 2 = f(r)$ and $2r + 3 = f'(r)$, where $f'(x)$ is the derivative of $f(x)$. It follows that $f(s) \equiv 0 \pmod{169}$ if and only if $f(r) + 13f'(r)t \equiv 0 \pmod{169}$. For a particular value of r, this expression is a linear congruence in the variable t,

$$f'(r)t \equiv -\frac{f(r)}{13} \pmod{13}.$$

(Here we use the fact that 13 divides $f(r)$ to cancel 13, adjusting the modulus according to the congruence cancellation property.) Any solution t of this linear congruence produces a solution $s = r + 13t$ of $f(x) \equiv 0 \pmod{169}$, and all solutions must have that form. The following table summarizes the necessary calculations for each value of r.

r	$f(r)$	$-f(r)/13$	$f'(r)$	t	s
4	26	−2	11	1	17
6	52	−4	15	11	149

Now in a similar way, all solutions of $f(x) \equiv 0 \pmod{2197}$ must satisfy $f(x) \equiv 0 \pmod{169}$, so must have the form $s = r + 169t$ where $r = 17$ or $r = 149$. Here we find that

$$f(s) = f(r + 169t) = (r + 169t)^2 + 3(r + 169t) - 2 = (r^2 + 3r - 2) + 13^2(2r + 3)t + 13^4 t^2.$$

It follows that $f(s) \equiv 0 \pmod{2197}$ if and only if t satisfies

$$f'(r)t \equiv -\frac{f(r)}{169} \pmod{13},$$

again using cancellation and the fact that 169 divides $f(r)$. The following table summarizes these calculations.

r	$f(r)$	$-f(r)/169$	$f'(r)$	t	s
17	338	-2	37	1	186
149	22646	-134	301	11	2008

(The values of t are obtained by solving $37t \equiv -2 \pmod{13}$ and $301t \equiv -134 \pmod{13}$. Both congruences can be simplified substantially.) We conclude that $f(x) \equiv 0 \pmod{2197}$ has two solutions, 186 and 2008. ◊

The following theorem generalizes the approach and outcome of this example. The key is that the expansion of $f(r + p^e t)$ always follows a certain pattern that can be expressed in terms of the derivatives of $f(x)$. (This is the Taylor series expansion of $f(x)$, which we will take as an assumption. Of course, for a polynomial function $f(x)$, the Taylor series is likewise a polynomial with finitely many nonzero terms.) Note that this theorem, as with Theorem B.36, is true regardless of the degree of $f(x)$.

THEOREM B.38. *Let $f(x)$ be a polynomial with integer coefficients, let $f'(x)$ be its derivative, let p be a prime number, and let e be a positive integer. Then an integer s is a solution of the congruence $f(x) \equiv 0 \pmod{p^{e+1}}$ if and only if $s = r + p^e t$ where r satisfies $f(x) \equiv 0 \pmod{p^e}$ and t satisfies the linear congruence*

$$f'(r) \cdot t \equiv -\frac{f(r)}{p^e} \pmod{p}. \tag{B.20}$$

PROOF. Let e be a positive integer and let $s = r + p^e t$ for some integers r and t. Expanding integer powers of the sum $r + p^e t$ and grouping the resulting powers of t, we find that

$$f(s) = f(r) + f'(r)p^e t + \frac{f''(r)}{2}p^{2e}t^2 + \frac{f^{(3)}(r)}{3!}p^{3e}t^3 + \cdots \equiv f(r) + f'(r)p^e t \pmod{p^{e+1}}, \tag{B.21}$$

since $2e \geq e + 1$, so that all but the first two terms in the expansion are congruent to 0 modulo p^{e+1}. Now if $f(r) \equiv 0 \pmod{p^e}$, then by cancellation $f(s) \equiv 0 \pmod{p^{e+1}}$ if and only if t satisfies congruence (B.20). □

Congruence (B.20) of Theorem B.38 is a linear congruence modulo a prime number. It has a unique solution modulo p if its linear coefficient, $f'(r)$, is not divisible by p. On the other hand, if $f'(r)$ is divisible by p so that $\gcd(f'(r), p) = p$, then (B.20) has either p solutions or no solutions. The next example illustrates this possibility.

EXAMPLE. Let $f(x) = 3x^2 - 3x + 13$. Find all solutions of $f(x) \equiv 0 \pmod{343}$, where $343 = 7^3$.

Completing the square on $3x^2 - 3x + 13 \equiv 0 \pmod 7$ yields $(6x - 3)^2 \equiv -147 \pmod 7$. Since 7 divides -147, this congruence has a single solution, which we find to be 4. Notice that $f'(x) = 6x - 3$. Any solution of $f(x) \equiv 0 \pmod{49}$ must have the form $s = 4 + 7t$ where t satisfies $f'(4)t \equiv -\frac{f(4)}{7} \pmod 7$. Here $f(4) = 49$ and $f'(4) = 21$. The congruence $21t \equiv -7 \pmod 7$ has seven solutions since $\gcd(21, 7) = 7$ divides -7. (Alternatively, we could simplify the congruence as $0t \equiv 0 \pmod 7$, which is satisfied by all elements of $\mathbb{Z}_7$.) Thus $f(x) \equiv 0 \pmod{49}$ has seven solutions, all of the form $4 + 7t$ with $0 \leq t < 7$, namely 4, 11, 18, 25, 32, 39, and 46.

Now every solution of $f(x) \equiv 0 \pmod{343}$ has the form $s = r + 49t$ where r is one of the seven solutions of $f(x) \equiv 0 \pmod{49}$ calculated above. For each r, we must solve the congruence (B.20). The situation is simpler than it appears, however. Notice that each r value is congruent to 4 modulo 7. Thus it is also true that $f'(r) \equiv f'(4) \pmod 7$ in each case. We have already noted that $f'(4) \equiv 0 \pmod 7$, so each linear congruence $f'(r)t \equiv -\frac{f(r)}{49} \pmod 7$ has either seven

solutions or no solutions. We can summarize the data that we need in the following table, also verifying the remark about $f'(r)$.

r	$f(r)$	$-f(r)/49$	$f'(r)$
4	49	-1	21
11	343	-7	63
18	931	-19	105
25	1813	-37	147
32	2989	-61	189
39	4459	-91	231
46	6223	-127	273

Each $f'(r)$ is divisible by 7. For each r, $-\frac{f(r)}{49}$ is an integer (verifying that each r is a solution of $f(x) \equiv 0 \pmod{49}$), but is divisible by 7 in only two cases, for $r = 11$ and $r = 39$. Thus congruence (B.20) has seven solutions in those cases and no solutions in the other five cases. All solutions of $f(x) \equiv 0 \pmod{343}$ are given by $r + 49t$ where r is 11 or 39 and $0 \leq t < 7$. In total, there are fourteen solutions: 11, 39, 60, 88, 109, 137, 158, 186, 207, 235, 256, 284, 305, and 333. ◊

For a quadratic polynomial $f(x)$, the situation of the preceding example can occur only when $f(x) \equiv 0 \pmod{p}$ has precisely one solution.

LEMMA B.39. *Let $f(x) = ax^2 + bx + c$ and let p be a prime number that does not divide a. If $f(x) \equiv 0 \pmod{p}$ has just one solution r, then p divides $f'(r)$. If $f(x) \equiv 0 \pmod{p}$ has two incongruent solutions r and s, then neither $f'(r)$ nor $f'(s)$ is divisible by p.*

PROOF. If r and s are integers, then

$$f(s) - f(r) = (as^2 + bs + c) - (ar^2 + br + c) = a(s^2 - r^2) + b(s - r) = (s - r)(a(s + r) + b). \tag{B.22}$$

Note that for a fixed r in $\mathbb{Z}_p$, there is a unique s in $\mathbb{Z}_p$ satisfying $a(s + r) + b \equiv 0 \pmod{p}$, since p does not divide a. If $f(r) \equiv 0 \pmod{p}$, then it follows that $f(s) \equiv 0 \pmod{p}$ as well. If r is the only solution of $f(x) \equiv 0 \pmod{p}$, we must have $s = r$. But then $a(s + r) + b = 2ar + b = f'(r)$ is congruent to 0 modulo p by our assumption.

If, on the other hand, r and s are incongruent solutions of $f(x) \equiv 0 \pmod{p}$, equation (B.22) shows that p divides $a(s + r) + b$. If p also divides $f'(r) = 2ar + b$, we must conclude that p divides $(a(s + r) + b) - (2ar + b) = a(s - r)$. This is impossible since p does not divide a and $r \not\equiv s \pmod{p}$. A similar contradiction occurs if p divides $f'(s)$. □

COROLLARY B.40. *Let $f(x) = ax^2 + bx + c$ and let p be a prime number not dividing a. If r and s are incongruent solutions of $f(x) \equiv 0 \pmod{p}$, then $f(x) \equiv 0 \pmod{p^e}$ has exactly two solutions for every $e \geq 1$, one congruent to r modulo p and the other congruent to s modulo p.*

PROOF. We proceed by induction on e. The claim is trivially true when $e = 1$, so suppose that for some $e \geq 1$, we know that $f(x) \equiv 0 \pmod{p^e}$ has precisely two solutions, $r_e \equiv r \pmod{p}$ and $s_e \equiv s \pmod{p}$. Then $f'(r_e) \equiv f'(r) \pmod{p}$ and $f'(s_e) \equiv f'(s) \pmod{p}$, with neither derivative divisible by p, by Lemma B.39. So Theorem B.38 shows that $f(x) \equiv 0 \pmod{p^{e+1}}$ has precisely one solution r_{e+1} that is congruent to r_e modulo p^e (and so congruent to r modulo p), and one solution s_{e+1} congruent to s_e modulo p^e, and that these must be the only solutions of that congruence. The result follows by induction. □

The number of solutions of $f(x) \equiv 0 \pmod{p^e}$ is more difficult to predict directly from Theorem B.38 when $f(x) \equiv 0 \pmod{p}$ has just one solution. We will address this problem in the next section.

EXAMPLE. Let $f(x) = x^2+1$. Find a formula for the number of solutions of $f(x) \equiv 0 \pmod{m}$ in terms of the prime factorization of m.

If p is an odd prime, we know that $x^2 + 1 \equiv 0 \pmod{p}$ has two solutions when $\left(\frac{-1}{p}\right) = 1$. Corollary B.27 shows that this is the case if and only if $p \equiv 1 \pmod{4}$, and Corollary B.40 implies that then $f(x) \equiv 0 \pmod{p^e}$ also has two solutions for every $e \geq 1$. If $p \equiv 3 \pmod{4}$, then $f(x) \equiv 0 \pmod{p^e}$ has no solutions, since any solution would satisfy $x^2 + 1 \equiv 0 \pmod{p}$ as well, but $\left(\frac{-1}{p}\right) = -1$ in this case.

We find that $x^2 + 1 \equiv 0 \pmod{2}$ has $r = 1$ as its only solution. Notice that $f(1) = 1^2 + 1 = 2$ and $f'(1) = 2(1) = 2$. By Theorem B.38, any solution of $f(x) \equiv 0 \pmod{4}$ must be of the form $s = 1 + 2t$, where t satisfies $2t \equiv -1 \pmod{2}$. This congruence has no solutions. It follows that $f(x) \equiv 0 \pmod{2^e}$ can have no solutions for any $e \geq 2$.

Finally, we can apply Corollary B.37 to combine these results about prime powers. Let m be a positive integer, written as $m = 2^e \cdot p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, with each p_i a distinct odd prime. We allow e or k to be 0, but assume that $e_i > 0$ for $1 \leq i \leq k$. Then there are no solutions of $f(x) \equiv 0 \pmod{m}$ if $e \geq 2$ or if any p_i is congruent to 3 modulo 4. Otherwise, there are 2^k solutions. ◊

Exercises on Quadratic Congruences Modulo Composite Integers.

1. Find all solutions of $x^2 - 1 \equiv 0 \pmod{385}$, given that $385 = 5 \cdot 7 \cdot 11$.
2. Let $f(x) = x^2 + 9x - 11$. Find all solutions of $f(x) \equiv 0 \pmod{m}$ for each of the following values of m.
   (a) $m = 5$.
   (b) $m = 11$.
   (c) $m = 25 = 5^2$.
   (d) $m = 29$.
   (e) $m = 121 = 11^2$.
   (f) $m = 125 = 5^3$.
   (g) $m = 203 = 7 \cdot 29$.
   (h) $m = 275 = 5^2 \cdot 11$.
   (i) $m = 319 = 11 \cdot 29$.
   (j) $m = 1331 = 11^3$.
3. Let $f(x) = x^2 - x$. Show that if m has k distinct prime divisors, then $f(x) \equiv 0 \pmod{m}$ has precisely 2^k solutions. (These solutions x are said to be *idempotent* modulo m, meaning that they satisfy $x^2 \equiv x \pmod{m}$.)
4. Find all idempotent elements (as defined in the preceding exercise) modulo each of the following values of m.
   (a) $m = 35$.
   (b) $m = 72$.
   (c) $m = 105$.
   (d) $m = 385$.

Seeding Polynomials

In Theorem B.38, we introduced a systematic method of using solutions of $f(x) \equiv 0 \pmod{p}$ to solve $f(x) \equiv 0 \pmod{p^e}$ for all $e \geq 1$. We noted, however, that if $f(x) \equiv 0 \pmod{p}$ has a solution q for which p divides $f'(q)$, then the number of solutions of $f(x) \equiv 0 \pmod{p^e}$ might be hard to describe in general. In this section, we develop a revised procedure for solving $f(x) \equiv 0 \pmod{p^e}$ in these cases, and we will see that when $f(x)$ is quadratic, there is a formula for the number of solutions of $f(x) \equiv 0 \pmod{p^e}$ for an arbitrary prime number p and positive integer e that depends only on the discriminant of $f(x)$. The method is one that we can visualize.

For a fixed prime p and polynomial $f(x)$, we can present the solutions of $f(x) \equiv 0 \pmod{p^e}$, which we also call *roots* of $f(x)$ modulo p^e, in the form of a tree diagram for $e \geq 0$, as in Figure 1.

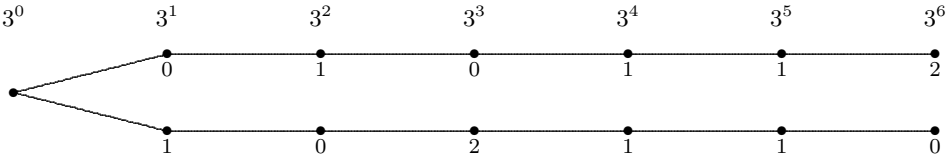

Figure 1: Roots of $x^2 + 5x + 3$ modulo 3^e for $e \leq 6$

Here each node under p^e represents a root r of $f(x)$ modulo p^e, calculated as

$$r = q_0 + q_1 p + q_2 p^2 + \cdots + q_{e-1} p^{e-1}, \tag{B.23}$$

where q_{i-1} is the label of the node under p^i in the path from the unlabeled node at the left to the node of interest. The unlabeled node corresponds to an empty sum, and indicates that 0 is always the unique root of $f(x)$ modulo $p^0 = 1$. The nodes under p^1 are solutions of $f(x) \equiv 0 \pmod{p}$, found by direct calculation. If $e > 0$ and $q = q_0$ is the first label in the path leading to the node representing r, then any nodes under p^{e+1} connected to r are labeled with solutions of

$$f'(q) \cdot t \equiv -\frac{f(r)}{p^e} \pmod{p}. \tag{B.24}$$

(Here we apply Theorem B.38, and the fact that $r \equiv q \pmod{p}$, so that $f'(r) \equiv f'(q) \pmod{p}$.) For example, the top node in Figure 1 under 3^5 indicates that $r = 0+1\cdot 3+0\cdot 3^2+1\cdot 3^3+1\cdot 3^4 = 111$ is a root of $f(x) = x^2 + 5x + 3$ modulo 3^5. The label of the node under 3^6 connected to this one is the solution of $f'(0) \cdot t \equiv -\frac{f(111)}{3^5} \pmod{3}$, that is, $5t \equiv -53 \pmod{3}$. This solution is $t = 2$, and so $0 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + 2 \cdot 3^5 = 597$ is a root of $f(x)$ modulo 3^6. We always take the solution(s) of congruence (B.24) to satisfy $0 \leq t < p$, so that (B.23) is the base p expansion of r. We also refer to this type of diagram as a *base p diagram* for $f(x)$.

Figure 1 illustrates the "well-behaved" pattern of a base p diagram for $f(x)$ when p does not divide $f'(q)$ for any root q of $f(x)$ modulo p, so that congruence (B.24) always has a unique solution. If p divides $f'(q)$, but p^2 does not divide $f(q)$, then (B.24) has no solutions when $e = 2$, and so $f(x)$ has no roots modulo p^e arising from q for any $e \geq 2$. However, if p^2 divides $f(q)$ and p divides $f'(q)$, then (B.24) has p solutions when $e = 2$, and can have either p solutions or no solutions for larger values of e. Figure 2, for an example that follows, illustrates this situation.

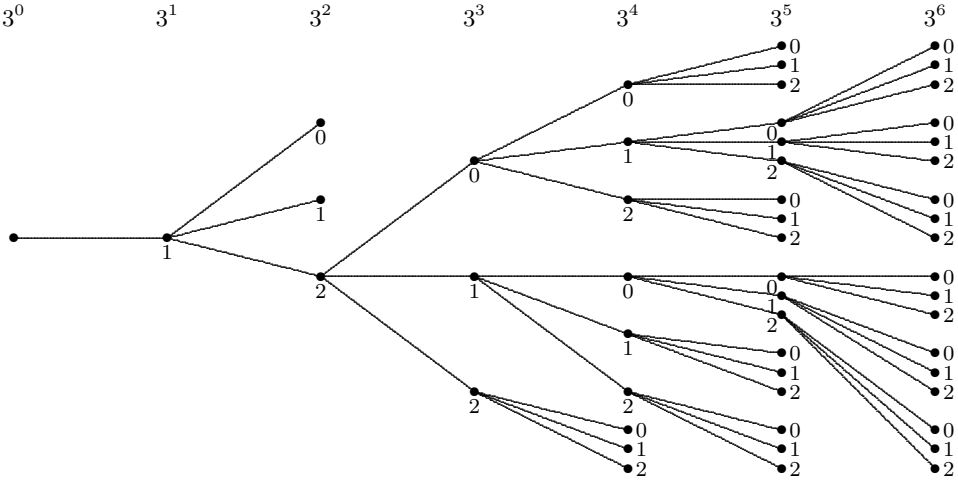

Figure 2: Roots of $x^2 + 31x - 23$ modulo 3^e for $e \leq 6$

EXAMPLE. Consider $f(x) = x^2 + 31x - 23$ and $p = 3$. Here $q = 1$ is the unique root of $f(x)$ modulo p, and p divides $f'(q) = 33$. Since 3^2 divides $f(1) = 9$, there are three roots of $f(x)$ modulo 3^2: $1 + 3t = 1, 4, 7$. Now 3^3 divides neither $f(1) = 9$ nor $f(4) = 117$, but does divide $f(7) = 243$. So there are no roots of $f(x)$ modulo 3^3 congruent to 1 or 4 modulo 9, but three such solutions congruent to 7 modulo 9, namely $7 + 3^2t = 7, 16, 25$. Continuing in this way produces the diagram of Figure 2, where nodes appear to branch off or die out at random. ◊

In this section, we demonstrate that the roots of $f(x)$ modulo p^e in this latter case are more predictable than they first appear, in that they arise in a precise way from those of a more well-behaved type. In fact, we will see that roots modulo 3^e of the polynomial in Figure 2 are determined, for sufficiently large e, by the roots of the polynomial illustrated in Figure 1.

Seeding Polynomials and the Seeding Map. Let $f(x)$ be a quadratic polynomial and let p be a prime number not dividing the leading coefficient of $f(x)$. As noted above, it is easy to describe the number of solutions of $f(x) \equiv 0 \pmod{p^e}$ for all $e \geq 0$ except when there is some q for which p^2 divides $f(q)$ and p divides $f'(q)$. The following proposition gives a criterion for when this situation occurs. We then develop a different approach to this case.

PROPOSITION B.41. *Let $f(x) = ax^2 + bx + c$ be a polynomial with discriminant $\Delta = b^2 - 4ac$, and let p be a prime number not dividing a. Then there is a unique integer q modulo p for which p^2 divides $f(q)$ and p divides $f'(q)$ if and only if $\Delta = p^2\Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod 4$.*

PROOF. If $f(x) = ax^2 + bx + c$, so that $f'(x) = 2ax + b$, then

$$f'(x)^2 - 4af(x) = \Delta \tag{B.25}$$

for all x. Suppose first that there is some q so that $f(q) = p^2c_0$ and $f'(q) = pb_0$. Then (B.25) shows that $\Delta = (pb_0)^2 - 4a \cdot p^2c_0 = p^2(b_0^2 - 4ac_0)$, with $\Delta_0 = b_0^2 - 4ac_0 \equiv b_0^2 \equiv 0$ or $1 \pmod 4$.

Conversely, suppose that $\Delta = p^2\Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod 4$. If p is odd, let q satisfy the linear congruence $2ax + b \equiv 0 \pmod p$, so that p divides $f'(q)$. Note that q is unique modulo p since $\gcd(2a, p) = 1$, and equation (B.25) shows that then p^2 divides $f(q)$. If $p = 2$, then a is odd and b is even (since Δ is even) and so $f(0) = c$ and $f(1) = a + b + c$ have opposite parity, while $f'(x) = 2ax + b$ is even for all x. Let $q = 0$ or $q = 1$ have the same parity as c, so that $f(q)$ is also even. Now (B.25) shows that $af(q) = \left(aq + \frac{b}{2}\right)^2 - \Delta_0$. With a odd, $f(q)$ even, and a square congruent to 0 or 1 modulo 4, as is Δ_0, we find that 4 must divide $f(q)$. □

DEFINITION. Let $f(x) = ax^2 + bx + c$ and let p be a prime number not dividing a. Suppose that $\Delta = b^2 - 4ac = p^2\Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod 4$, and let $0 \leq q < p$ be the integer for which $f(q) = p^2c_0$ and $f'(q) = pb_0$ with $b_0, c_0 \in \mathbb{Z}$. Then we define the *p-seeding polynomial* of $f(x)$ to be $f_0(x) = ax^2 + b_0x + c_0$.

We usually refer to $f_0(x)$ simply as the seeding polynomial of $f(x)$ if p is clear from context. The proof of Proposition B.41 shows that Δ_0 is the discriminant of $f_0(x)$.

THEOREM B.42. *Let $f(x) = ax^2 + bx + c$ and let p be a prime number not dividing a. Suppose that there is an integer $0 \leq q < p$ so that p^2 divides $f(q)$ and p divides $f'(q)$. Let $f_0(x)$ be the p-seeding polynomial of $f(x)$. In this case, for every $e \geq 2$, the mapping $\phi(r) = q + pr$ is a one-to-one correspondence between roots r of $f_0(x)$ modulo p^{e-2} and roots s of $f(x)$ modulo p^{e-1} for which p^e divides $f(s)$. Thus the roots of $f(x)$ modulo p^e are precisely of the form $q + pr + p^{e-1}t$, where $f_0(r) \equiv 0 \pmod{p^{e-2}}$ and $0 \leq t < p$.*

PROOF. Let $f(q) = p^2 c_0$ and $f'(q) = pb_0$, so that $f_0(x) = ax^2 + b_0 x + c_0$. Note that

$$f(q+pr) = a(q+pr)^2 + b(q+pr) + c = (aq^2 + bq + c) + p(2aq+b)r + ap^2 r^2$$
$$= f(q) + pf'(q)r + p^2 ar^2 = p^2(ar^2 + b_0 r + c_0) = p^2 \cdot f_0(r).$$

It follows that p^{e-2} divides $f_0(r)$ for some $e \geq 2$ if and only if p^e divides $f(q+pr)$. Consider the function $\phi(r) = q + pr$ between roots r of $f_0(x)$ modulo p^{e-2} and roots s of $f(x)$ modulo p^{e-1} for which p^e divides $f(s)$. This function is well-defined and injective since $r \equiv r_1 \pmod{p^{e-2}}$ if and only if $q + pr \equiv q + pr_1 \pmod{p^{e-1}}$. It is surjective since every solution s of $f(x) \equiv 0 \pmod{p^{e-1}}$ must satisfy $f(x) \equiv 0 \pmod{p}$, so has the form $s = q + pr$ for some r. As noted above, then p^e divides $f(s)$ if and only if p^{e-2} divides $f_0(r)$. For each such s, Theorem B.38 then produces p distinct solutions of $f(x) \equiv 0 \pmod{p^e}$, each of the form $s + p^{e-1}t = q + pr + p^{e-1}t$, with $0 \leq t < p$. □

We refer to the function ϕ from solutions of $f_0(x) \equiv 0 \pmod{p^{e-2}}$ to certain solutions of $f(x) \equiv 0 \pmod{p^{e-1}}$ as a *seeding map*. This function determines the "fertile" nodes in the base p diagram for $f(x)$, as illustrated in the following example.

EXAMPLE. Let $f(x) = x^2 + 27x + 1$ and let $p = 5$. We find that $q = 4$ is the unique root of $f(x)$ modulo 5, with $f(4) = 125 = 5^2 \cdot 5$ and $f'(4) = 35 = 5 \cdot 7$. So $f_0(x) = x^2 + 7x + 5$ is the seeding polynomial for $f(x)$. In Figure 3 below, we illustrate the seeding map by dotted lines between roots of $f_0(x)$ and roots of $f(x)$ modulo powers of $p = 5$. Notice that in base p form, the images of the seeding map are obtained by following the same sequence of node labels from 4 as from the unlabeled node in the domain. These images are precisely the nodes that branch into $p = 5$ new solutions modulo the next higher power of 5, while the "unseeded" nodes die out. ◊

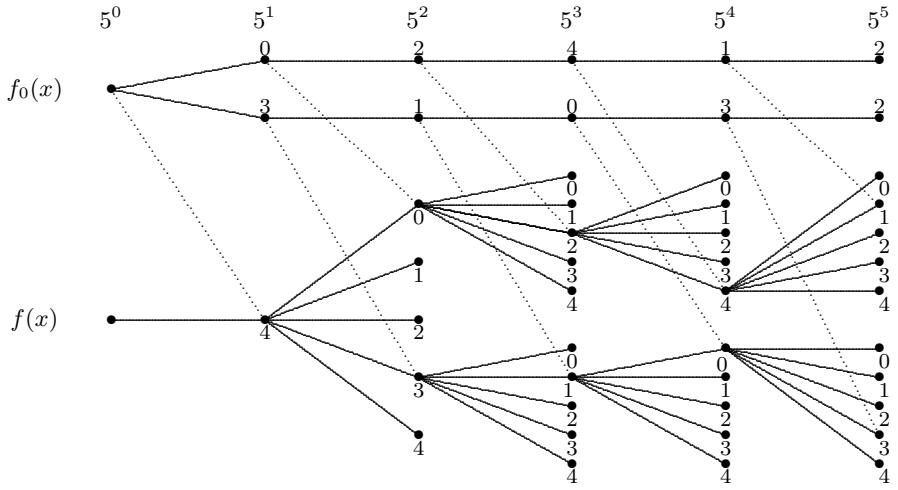

Figure 3: Roots of $f(x) = x^2 + 27x + 1$ and $f_0(x) = x^2 + 7x + 5$ modulo 5^e for $e \leq 5$

In this example, $f_0(x) \equiv 0 \pmod{5^e}$ has precisely two solutions for every $e \geq 1$. Theorem B.42 then implies that $f(x) \equiv 0 \pmod{5^e}$ has precisely $5 \cdot 2 = 10$ solutions for every $e \geq 3$. In the remainder of this section, we will see that when $f(x)$ is an arbitrary quadratic polynomial, we can similarly use seeding polynomials to count the number of solutions of $f(x) \equiv 0 \pmod{p^e}$ for every prime p and positive integer e.

The Number of Solutions of a Quadratic Congruence. If $f(x)$ is a polynomial with integer coefficients and m is a positive integer, we will denote by $n_m(f)$ the number of solutions of $f(x) \equiv 0 \pmod{m}$. (As always, this means the number of distinct congruence classes of such

solutions in $\mathbb{Z}_m$.) Corollary B.37 shows that if $m = p_1^{e_1} \cdots p_k^{e_k}$ with each p_i a distinct prime, then

$$n_m(f) = n_{p_1^{e_1}}(f) \cdots n_{p_k^{e_k}}(f),$$

so it suffices to calculate $n_{p^e}(f)$ when p is prime. In this subsection, we establish a formula for $n_{p^e}(f)$ that depends only on the discriminant of $f(x)$. We begin with the following observation.

COROLLARY B.43. *Let $f(x)$ be a quadratic polynomial and let p be a prime not dividing the leading coefficient of $f(x)$. Suppose that there is some integer $0 \leq q < p$ so that p^2 divides $f(q)$ and p divides $f'(q)$, and let $f_0(x)$ be the p-seeding polynomial of $f(x)$. Then for every integer $e \geq 2$,*

$$n_{p^e}(f) = p \cdot n_{p^{e-2}}(f_0). \tag{B.26}$$

PROOF. This is an immediate consequence of Theorem B.42, in which it is established that the roots of $f(x)$ modulo p^e are precisely of the form $q + pr + p^{e-1}t$, where $f_0(r) \equiv 0 \pmod{p^{e-2}}$ and $0 \leq t < p$. □

We can apply this result to arbitrary quadratic congruences modulo prime powers. The following terminology and notation are convenient here.

DEFINITION. Let $f(x)$ be a quadratic polynomial with discriminant $\Delta \neq 0$, and let p be a prime number. Define the *p-level* of $f(x)$ to be the largest nonnegative integer $\ell = \ell_p(f)$ so that $\Delta = p^{2\ell}\Delta_0$ with Δ_0 congruent to 0 or 1 modulo 4. In this case, write $f(x)$ also as $f_\ell(x)$, and if $\ell \geq k > 0$, recursively define $f_{k-1}(x)$ to be the p-seeding polynomial of $f_k(x)$.

If the prime p is clear from context, we refer to $\ell_p(f)$ simply as the *level* of $f(x)$. Note that the discriminant of $f_k(x)$ is $\Delta_k = p^{2k}\Delta_0$, so that k is the level of $f_k(x)$ for $0 \leq k \leq \ell$. If $k > 0$, we denote the unique root of $f_k(x)$ modulo p as q_k. We refer to $f_\ell(x), f_{\ell-1}(x), \ldots, f_1(x), f_0(x)$ as the sequence of seeding polynomials for $f(x)$.

EXAMPLE. Let $f(x) = x^2 + 30x + 33$, and let $p = 2$. Here $\Delta = 768 = 2^8 \cdot 3$, but since 3 is not congruent to 0 or 1 modulo 4, the level of $f(x)$ is $\ell = 3$, with $\Delta_0 = 12$. The sequence of seeding polynomials for $f(x)$ is as follows.

(1) $f_3(x) = x^2 + 30x + 33$, with $q_3 = 1$, so that $f_3(1) = 64 = 2^2 \cdot 16$ and $f_3'(1) = 32 = 2 \cdot 16$.
(2) $f_2(x) = x^2 + 16x + 16$, with $q_2 = 0$, so that $f_2(0) = 16 = 2^2 \cdot 4$ and $f_2'(0) = 16 = 2 \cdot 8$.
(3) $f_1(x) = x^2 + 8x + 4$, with $q_1 = 0$, so that $f_1(0) = 4 = 2^2 \cdot 1$ and $f_1'(0) = 8 = 2 \cdot 4$.
(4) $f_0(x) = x^2 + 4x + 1$.

Note that $f_0(x)$ has a unique root $q = 1$ modulo 2, but we cannot define a seeding polynomial for $f_0(x)$ since $f_0(1) = 6$ is not divisible by 2^2. ◊

If the discriminant of $f(x)$ is $\Delta = 0$, we can define an *infinite* sequence of seeding polynomials for $f(x)$, not necessarily distinct. Although the level of $f(x)$ is undefined, we will use the notation $f_\ell(x), f_{\ell-1}(x), \ldots$ for this sequence, as in the following example.

EXAMPLE. If $f(x) = 4x^2 - 44x + 121$ and $p = 7$, then the sequence of seeding polynomials for $f(x)$, all with discriminant 0, is as follows.

(1) Let $f_\ell(x) = f(x) = 4x^2 - 44x + 121$. Here $q_\ell = 2$ is the unique root of $f_\ell(x)$ modulo 7, with $f_\ell(2) = 49 = 7^2 \cdot 1$ and $f_\ell'(2) = -28 = 7 \cdot -4$.
(2) So $f_{\ell-1}(x) = 4x^2 - 4x + 1$ is the seeding polynomial of $f_\ell(x)$. We find that $q_{\ell-1} = 4$ is the unique root of $f_{\ell-1}(x)$, with $f_{\ell-1}(4) = 49 = 7^2 \cdot 1$ and $f_{\ell-1}'(2) = 28 = 7 \cdot 4$.
(3) Now $f_{\ell-2}(x) = 4x^2 + 4x + 1$ is the seeding polynomial of $f_{\ell-1}(x)$. Here $q_{\ell-2} = 3$ is the unique root of $f_{\ell-2}(x)$, with $f_{\ell-2}(3) = 49 = 7^2 \cdot 1$ and $f_{\ell-2}'(3) = 28 = 7 \cdot 4$.

Now $f_{\ell-k}(x) = 4x^2 + 4x + 1$ is the seeding polynomial of $f_{\ell-k+1}(x)$ for all $k \geq 3$. ◊

THEOREM B.44. *Let $f(x)$ be a quadratic polynomial with nonzero discriminant, let p be a prime not dividing the leading coefficient of $f(x)$, and let ℓ be the p-level of $f(x)$. Define the sequence of seeding polynomials for $f(x)$ as above. Let e be a nonnegative integer, and suppose that $e = 2k + r$ for some nonnegative k and r, with $k \leq \ell$. Then $n_{p^e}(f) = p^k \cdot n_{p^r}(f_{\ell-k})$. The same equation holds for all nonnegative k and r if the discriminant of $f(x)$ is zero.*

PROOF. If $k = 0$, then $e = r$ and the claim of this theorem is trivial since $f_\ell(x) = f(x)$. If $k = 1$, then $e \geq 2$ with $r = e - 2$, and $f_{\ell-1}(x)$ is the seeding polynomial of $f(x)$. The claim that $n_{p^e}(f) = p^1 \cdot n_{p^r}(f_{\ell-1})$ is then a restatement of equation (B.26) in Corollary B.43. If $k = 2$, then $e \geq 4$ with $r = e - 4$, and $f_{\ell-2}(x)$ is the seeding polynomial of $f_{\ell-1}(x)$, which is the seeding polynomial of $f(x)$. Now two applications of equation (B.26) show that

$$n_{p^e}(f) = p \cdot n_{p^{e-2}}(f_{\ell-1}) = p(p \cdot n_{p^{e-4}}(f_{\ell-2})) = p^2 \cdot n_{p^r}(f_{\ell-2}).$$

Continuing in this way establishes the claim for $n_{p^e}(f)$ when $e = 2k + r$ with $k \leq \ell$, and for all k and r when ℓ is undefined. □

EXAMPLE. Let $f(x) = x^2 + 30x + 33$, with $p = 2$, and with $f_3(x), f_2(x), f_1(x), f_0(x)$ the sequence of seeding polynomials for $f(x)$, as listed in an example above. We saw that each of these polynomials has a unique root modulo 2—in particular, $n_{2^0}(f) = 1 = n_{2^1}(f)$. For $e = 2$ and $e = 3$, we can apply Theorem B.44 with $k = 1$—we conclude that $n_{2^2}(f) = 2 = n_{2^3}(f)$. For $e = 4$ and $e = 5$, let $k = 2$—we find that $n_{2^4}(f) = 4 = n_{2^5}(f)$. Finally for $e \geq 6$, we can apply Theorem B.44 with $k = 3$. Since $f_0(x)$ has a unique root $q = 1$ modulo 2, but 2^2 does not divide $f_0(1) = 6$, we conclude that $n_{2^6}(f) = 8 = n_{2^7}(f)$, but that $n_{2^e}(f) = 0$ for $e \geq 8$. The following diagram illustrates these results, and the roots of $f(x)$ and its seeding polynomials modulo powers of 2. ◊

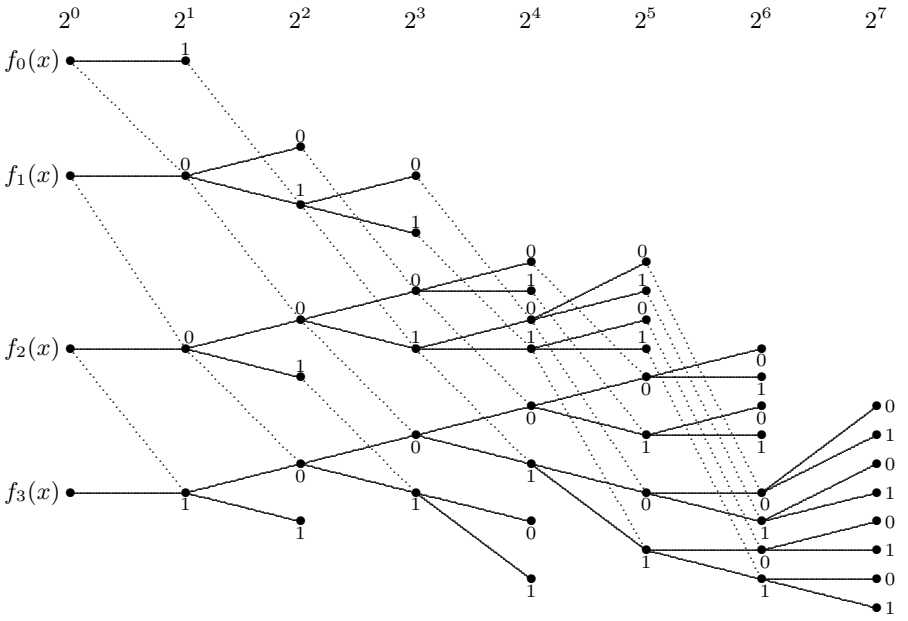

Figure 4: Roots of $f(x) = x^2 + 30x + 33$ (bottom) and its seeding polynomials modulo powers of 2

EXAMPLE. Let $f(x) = x^2 + 31x - 23$, with discriminant $\Delta = 1053 = 3^4 \cdot 13$, so that the 3-level of $f(x)$ is $\ell = 2$. We find that $q_2 = 1$ is the unique solution of $f(x) \equiv 0 \pmod 3$, with $f(1) = 9$ and $f'(1) = 33$, so that $f_1(x) = x^2 + 11x + 1$ is the seeding polynomial for $f(x) = f_2(x)$. Likewise, $q_1 = 2$ is the unique root of $f_1(x)$ modulo 3, with $f_1(2) = 27$ and $f_1'(2) = 15$, so that $f_0(x) = x^2 + 5x + 3$ is the seeding polynomial of $f_1(x)$. (Notice that $f_0(x)$ and $f_2(x)$ are the polynomials whose roots

modulo powers of 3 are illustrated in Figures 1 and 2 respectively.) In the following table, we list the number of roots of each of these polynomials modulo powers of 3.

e	0	1	2	3	4	5	6	7	$\cdots$
$n_{3^e}(f_0)$	1	2	2	2	2	2	2	2	$\cdots$
$n_{3^e}(f_1)$	1	1	3	6	6	6	6	6	$\cdots$
$n_{3^e}(f_2)$	1	1	3	3	9	18	18	18	$\cdots$

Here $n_{3^e}(f_1) = 3 \cdot n_{3^{e-2}}(f_0)$ and $n_{3^e}(f_2) = 3 \cdot n_{3^{e-2}}(f_1)$ for all $e \geq 2$, so we see that $n_{3^e}(f_2) = 9 \cdot n_{3^{e-4}}(f_0)$ for $e \geq 4$. (These claims are consistent with the data presented in Figure 2.) $\Diamond$

The preceding examples illustrate how a sequence of seeding polynomials for $f(x)$ typically leads us to a polynomial whose number of solutions modulo powers of p can be described in full. To conclude this section, we use this approach to derive a formula for $n_{p^e}(f)$ that is determined purely by the discriminant of $f(x)$. As noted previously, a general formula for $n_m(f)$, where m is any positive integer, follows from Corollary B.37. For these statements, it is convenient to extend the definition of the Legendre symbol as follows.

Definition. If Δ is an integer congruent to 0 or 1 modulo 4, then

$$\left(\frac{\Delta}{2}\right) = \begin{cases} 1, & \text{if } \Delta \equiv 1 \pmod 8, \\ -1, & \text{if } \Delta \equiv 5 \pmod 8, \\ 0, & \text{if } \Delta \equiv 0 \pmod 4. \end{cases}$$

We refer to $\left(\frac{\Delta}{2}\right)$ as a *Kronecker symbol*.

The following lemma summarizes results previously established.

Lemma B.45. *Let $f(x) = ax^2 + bx + c$ with $\Delta = b^2 - 4c$, and let p be a prime number not dividing a. Suppose that the p-level of $f(x)$ is zero, so that p^2 does not divide Δ, or (when $p = 2$) $\frac{\Delta}{4} \equiv 2$ or $3 \pmod 4$. Then the following statements are true.*

(1) *If $\left(\frac{\Delta}{p}\right) = 1$, then $n_{p^e}(f) = 2$ for all $e > 0$.*
(2) *If $\left(\frac{\Delta}{p}\right) = -1$, then $n_{p^e}(f) = 0$ for all $e > 0$.*
(3) *If $\left(\frac{\Delta}{p}\right) = 0$, then $n_p(f) = 1$ and $n_{p^e}(f) = 0$ for $e > 1$.*

Proof. Statements (1) and (2) follow from the process of completing the square, the definition of the Legendre symbol, Proposition B.22, and Corollary B.40. If p divides Δ, we see, as in the proof of Proposition B.41, that $f(x) \equiv 0 \pmod p$ has a unique solution q, with p divides $f'(q)$. But equation (B.25) shows that p^2 cannot divide $f(q)$, from which statement (3) follows. $\square$

Theorem B.46. *Let $f(x) = ax^2 + bx + c$, with discriminant $\Delta = b^2 - 4ac$, and let p be a prime number not dividing a. If $\Delta \neq 0$, let $\ell \geq 0$ be the largest integer for which $\Delta = p^{2\ell}\Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod 4$. Let e be a nonnegative integer. If $e > 2\ell$, then the following statements are true.*

(1) *If $\left(\frac{\Delta_0}{p}\right) = 1$, then $n_{p^e}(f) = 2p^\ell$.*
(2) *If $\left(\frac{\Delta_0}{p}\right) = -1$, then $n_{p^e}(f) = 0$.*
(3) *If $\left(\frac{\Delta_0}{p}\right) = 0$, then $n_{p^e}(f) = \begin{cases} p^\ell, & \text{if } e = 2\ell + 1, \\ 0, & \text{if } e > 2\ell + 1. \end{cases}$*

On the other hand, if $e \leq 2\ell$ is written as $e = 2k + r$ with $r = 0$ or $r = 1$, then $n_{p^e}(f) = p^k$. This equation also holds for all $e \geq 0$ if $\Delta = 0$.

PROOF. Let $f_\ell(x), f_{\ell-1}(x), \dots$ be the (finite or infinite) sequence of seeding polynomials for $f(x)$. Suppose first that $e = 2k + r$ with $0 \le k < \ell$ and $0 \le r < 2$. Theorem B.44 shows that $n_{p^e}(f) = p^k \cdot n_{p^r}(f_{\ell-k})$. But $n_{p^r}(f_{\ell-k}) = 1$ for $r = 0$ and $r = 1$, since the level of $f_{\ell-k}(x)$ is positive, so that $f_{\ell-k}(x) \equiv 0 \pmod{p}$ has a unique solution. Thus $n_{p^e}(f) = p^k$ in this case.

On the other hand, suppose that $e = 2\ell + r$ with $r \ge 0$. Now Theorem B.44 implies that $n_{p^e}(f) = p^\ell \cdot n_{p^r}(f_0)$. If $r = 0$, then $n_{p^r}(f_0) = 1$. If $r > 0$, our conclusions follow immediately from Lemma B.45. □

EXAMPLE. Let $f(x) = x^2 + x + 1801$, so that $\Delta = -7203 = 7^4(-3)$. In the notation of Theorem B.46, if $p = 7$, then $m = 2$ and $e = 4$. Since $\left(\frac{-3}{7}\right) = 1$, we find the number of roots of $f(x)$ modulo p^k is given by the following table

k	0	1	2	3	4	5	6	7
$n_{7^k}(f)$	1	1	7	7	49	98	98	98

with $n_{7^k}(f) = 98$ for all $k \ge 5$. ◊

Exercises on Seeding Polynomials.

1. Use Theorem B.38 to draw a base 3 diagram for $f(x) = x^2 - 2x - 8$. List all roots of $f(x)$ modulo 3^k for $k \le 4$.

In Exercises 2–6, for the given $f(x)$ and prime p, find the p-seeding polynomial $f_1(x)$ of $f(x)$. Find all roots of $f_1(x)$ modulo p^k for $k \le 4$, and use them to list all roots of $f(x)$ modulo p^k for $k \le 6$.

2. $f(x) = x^2 - 2x - 8$, with $p = 3$.
3. $f(x) = x^2 - 5x - 5$, with $p = 3$.
4. $f(x) = x^2 + 2x + 8$, with $p = 2$.
5. $f(x) = x^2 + 6x + 1$, with $p = 2$.
6. $f(x) = x^2 + 12x + 11$, with $p = 5$.

In Exercises 7–11, use Theorem B.46 to find the number of roots of $f(x)$ modulo p^k for all $k \ge 0$.

7. $f(x) = x^2 + 12x + 11$, with $p = 5$.
8. $f(x) = 7x^2 + 2x + 7$, with $p = 2$.
9. $f(x) = x^2 + 35x + 43$, with $p = 3$.
10. $f(x) = x^2 + 33x - 9$, with $p = 3$.
11. $f(x) = x^2 + 33x - 9$, with $p = 5$.
12. Find the complete sequence of seeding polynomials for $f(x) = x^2 + 61x + 19$, with $p = 3$. Use the results to find all roots of $f(x)$ modulo 3^k for $k \le 7$.
13. Each of our statements in this section about the number of roots of $f(x) = ax^2 + bx + c$ modulo powers of a prime p has been under the assumption that p does not divide a. Show that the following statements are true if we drop that restriction.
    (a) If p divides a and p does not divide b, show that $n_{p^e}(f) = 1$ for all $e \ge 0$.
    (b) If p divides a and p divides b, but p does not divide c, show that $n_{p^e}(f) = 0$ for all $e \ge 1$.
    (c) If p divides a, b, and c, show that $n_{p^e}(f) = p \cdot n_{p^{e-1}}(f_p)$ for all $e \ge 1$, where $f_p(x) = \frac{a}{p}x^2 + \frac{b}{p}x + \frac{c}{p}$.

Constructing Solutions of Quadratic Congruences

Using the Quadratic Reciprocity Theorem, together with other properties of Legendre symbols, we can determine whether $x^2 \equiv a \pmod{p}$ has a solution when p is an odd prime and a is an integer. We have not yet considered any method of finding those solutions, other than trial-and-error calculations. In this section, we will describe a procedure by which a solution of $x^2 \equiv a \pmod{p}$ can be constructed when $\left(\frac{a}{p}\right) = 1$. This approach requires calculation of large powers of a modulo p, which can be difficult to perform by hand. But large powers of an integer a can in fact be efficiently computed using a process of successive squaring. We will illustrate this method with an example, and will assume in the remainder of this section that all such powers are similarly calculated in practice (most likely by computer).

Example. Suppose that we want to find the remainder when 3^{5937} is divided by $m = 7639$. We first write the exponent $n = 5937$ as a sum of powers of 2, as in its binary representation. We can do this using repeated division by 2, as follows.

$$\begin{aligned} 5937 &= 1 + 2(2968) \\ 2968 &= 0 + 2(1484) \\ 1484 &= 0 + 2(742) \\ 742 &= 0 + 2(371) \\ 371 &= 1 + 2(185) \\ 185 &= 1 + 2(92) \\ 92 &= 0 + 2(46) \\ 46 &= 0 + 2(23) \\ 23 &= 1 + 2(11) \\ 11 &= 1 + 2(5) \\ 5 &= 1 + 2(2) \\ 2 &= 0 + 2(1) \\ 1 &= 1 + 2(0) \end{aligned}$$

By repeated substitution, we find that

$$5937 = 1 + 2(2968) = 1 + 2(0 + 2(1484)) = 1 + 0 \cdot 2 + 2^2(0 + 2(742)) = \cdots,$$

eventually arriving at the expression

$$5937 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + \cdots = 1 + 2^4 + 2^5 + 2^8 + 2^9 + 2^{10} + 2^{12}.$$

This sum is abbreviated by the base two representation of n as 1011100110001_2.

Let k be the largest exponent of 2 that appears in this representation, $k = 12$ in this case. As the second step, we calculate the remainder of 3^{2^i} on division by $m = 7639$ for $0 \le i \le k$. This is easier to do than it first appears—each entry in the second row of the following table is the square of the term that precedes it, reduced modulo m. For any a, we can see that $(a^{2^i})^2 = a^{2^i 2} = a^{2^{i+1}}$ by the usual exponent rules.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$3^{2^i} \bmod m$	3	9	81	6561	956	4895	5121	7593	2116	1002	3295	2006	5922

As the final step, we take the product of the terms from this list corresponding to the powers of 2 in the sum equaling n. The reasoning is that

$$\begin{aligned} 3^{5937} = 3^{2^0+2^4+2^5+2^8+2^9+2^{10}+2^{12}} &= 3^{2^0} \cdot 3^{2^4} \cdot 3^{2^5} \cdot 3^{2^8} \cdot 3^{2^9} \cdot 3^{2^{10}} \cdot 3^{2^{12}} \\ &\equiv 3 \cdot 956 \cdot 4895 \cdot 2116 \cdot 1002 \cdot 3295 \cdot 5922 \pmod{7639}. \end{aligned}$$

Partial products in this calculation can be reduced modulo 7639 to keep a handle on the computations. (For instance, $3 \cdot 956 \cdot 4895 = 14038860 \equiv 6017 \pmod{7639}$.) Here $3^{5937} \equiv 6 \pmod{7639}$. $\Diamond$

In practice, the three steps of this procedure—writing n as a sum of powers of 2, finding $a^{2^i} \bmod m$ by repeated squaring, and the multiplication of the required terms modulo m—can be done simultaneously. We summarize the algorithm in this way in the following proposition, omitting further proof.

PROPOSITION B.47. *Let m and n be positive integers and a an integer. Define four sequences, q_i, r_i, s_i, and t_i recursively for $i \geq 0$ as follows: Let $q_0 = n$ and for $i \geq 0$, let $q_{i+1} = q_i \operatorname{div} 2$ and let $r_i = q_i \bmod 2$. Let $s_0 = a$ and for $i \geq 0$, let $s_{i+1} = s_i^2 \bmod m$. Finally, let $t_0 = 1$ and for $i \geq 0$, let*

$$t_{i+1} = \begin{cases} t_i s_i \bmod m, & \text{if } r_i = 1 \\ t_i, & \text{if } r_i = 0. \end{cases}$$

Then there is some $k \geq 0$ such that $q_k = 0$, and in that case, t_k is equal to $a^n \bmod m$.

We now describe a method of constructing a solution of $x^2 \equiv a \pmod{p}$ when p is an odd prime and $\left(\frac{a}{p}\right) = 1$. This approach was developed independently by Alberto Tonelli and Daniel Shanks. We begin with the following observation.

PROPOSITION B.48. *Let p be an odd prime, and suppose that $p - 1 = 2^e \cdot q$ with q odd. Let a be an integer not divisible by p. If $t = a^q$, then the order of t modulo p is a divisor of 2^e, with $\operatorname{ord}_p(t) < 2^e$ if and only if $\left(\frac{a}{p}\right) = 1$.*

PROOF. If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. (This fact is known as *Fermat's Little Theorem*, established in Appendix C as a special case of Proposition C.4 applied to $\mathbb{Z}_p^\times$.) So

$$t^{2^e} = (a^q)^{2^e} = a^{2^e q} = a^{p-1} \equiv 1 \pmod{p},$$

and it follows that $\operatorname{ord}_p(t)$ divides 2^e, so equals 2^k for some $0 \leq k \leq e$. Note that

$$t^{2^{e-1}} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

by Euler's Criterion. If $\left(\frac{a}{p}\right) = 1$, it follows that $\operatorname{ord}_p(t) < 2^e$. If $\left(\frac{a}{p}\right) = -1$, then $\operatorname{ord}_p(t)$ must equal 2^e, since if $a^{2^k} \equiv 1 \pmod{p}$, then $a^{2^\ell} \equiv 1 \pmod{p}$ for all $\ell \geq k$. $\square$

Note that this proposition gives us a method of testing whether $\left(\frac{a}{p}\right)$ is 1 or -1, determined by a power of a. Whether or not this approach is practical depends on our ability to calculate powers of a modulo p.

PROPOSITION B.49. *Let p be an odd prime, with $p-1 = 2^e \cdot q$ and q odd. Let a be an integer for which $\left(\frac{a}{p}\right) = 1$. Suppose that we know integers b and t for which $b^2 \equiv at \pmod{p}$ with $\operatorname{ord}_p(t) = 2^k$ and $0 < k < e$. Then we can find integers b_1 and t_1 so that $b_1^2 \equiv at_1 \pmod{p}$, with $\operatorname{ord}_p(t_1) = 2^{k_1}$ and $0 \leq k_1 < k$.*

PROOF. Let c be an integer for which $\left(\frac{c}{p}\right) = -1$. (Such a value of c is not difficult to find in practice.) Let $r = c^{(p-1)/2^{k+1}}$ (note that 2^{k+1} divides $p - 1$ since $k < e$), and let $b_1 = br$ and $t_1 = tr^2$. Then

$$b_1^2 = b^2 r^2 \equiv atr^2 \equiv at_1 \pmod{p}.$$

Now note that $t_1^{2^{k-1}} = t^{2^{k-1}} \cdot r^{2^k}$. Since $\operatorname{ord}_p(t) = 2^k$, then $t^{2^{k-1}} \equiv -1 \pmod{p}$. Likewise,

$$r^{2^k} = \left(c^{\frac{p-1}{2^{k+1}}}\right)^{2^k} = c^{\frac{p-1}{2^{k+1}} \cdot 2^k} = c^{\frac{p-1}{2}} \equiv \left(\frac{c}{p}\right) \equiv -1 \pmod{p}.$$

It follows that $t_1^{2^{k-1}} \equiv -1 \cdot -1 \equiv 1 \pmod{p}$, thus the order of t_1 modulo p is a divisor of 2^{k-1} and must have the form 2^{k_1} with $0 \leq k_1 < k$. □

Now we can describe an algorithm that constructs a solution of $x^2 \equiv a \pmod{p}$, when such a solution exists. Assume that all calculations in the following process are carried out modulo p.

THEOREM B.50. *Let p be an odd prime, with $p - 1 = 2^e \cdot q$ and q odd. Let a be an integer not divisible by p. Let $t = t_0 = a^q$ and let $k = k_0$ be the smallest integer so that $t^{2^k} \equiv 1 \pmod{p}$. If $k = e$, then $x^2 \equiv a \pmod{p}$ has no solutions, so assume instead that $k < e$. Let c be some integer so that $\left(\frac{c}{p}\right) = -1$ and let $b_0 = a^{(q+1)/2}$. While k_i is greater than zero, let $r_i = c^{(p-1)/2^{k_i+1}}$, let $b_{i+1} = b_i \cdot r_i$, let $t = t_{i+1} = t_i \cdot r_i^2$, and let $k = k_{i+1}$ be the smallest integer so that $t^{2^k} \equiv 1 \pmod{p}$. Then there is an $i \geq 0$ for which $k_i = 0$, and in that case b_i is a solution of $x^2 \equiv a \pmod{p}$.*

PROOF. Proposition B.48 shows that k_0 exists, and that $\left(\frac{a}{p}\right) = 1$ if and only if $k_0 < e$. If that is the case, then $b_0^2 = a^{q+1} \equiv at_0 \pmod{p}$. Proposition B.49 and its proof imply that while k_i is greater than zero, then $b_{i+1}^2 \equiv at_{i+1} \pmod{p}$ and $0 \leq k_{i+1} < k_i$. Eventually, we must obtain a value of i so that $k_i = 0$, in which case $t_i = 1$ and $b_i^2 \equiv at_i \equiv a \pmod{p}$. □

As we have noted, the practicality of this algorithm depends on our ability to compute powers of an integer modulo p. When p is large, this approach is much more efficient (using a computer) than trial-and-error calculations. In the following example, we use a relatively small prime p to illustrate the steps of the algorithm.

EXAMPLE. Let $p = 113$, so that $p - 1 = 2^4 \cdot 7$. For our first calculation, let $a = 3$. Then $t = a^q = 3^7 \equiv 40 \pmod{113}$. We can find the smallest k for which $t^{2^k} \equiv 1 \pmod{p}$ by repeated squaring, using the fact that $(t^{2^i})^2 = t^{2 \cdot 2^i} = t^{2^{i+1}}$ for $i \geq 0$. In the following table, each entry of the second row is the square of the preceding entry.

i	0	1	2	3	4
t^{2^i}	40	18	98	112	1

Here we see that $k = 4 = e$, and so $x^2 \equiv 3 \pmod{113}$ has no solutions. (We could of course draw the same conclusion from the Legendre symbol $\left(\frac{3}{113}\right)$.) In the remaining parts of this example, we can let $c = 3$, and we will see that the powers of c that we need are already calculated in this table.

Now let $a = 2$. Since $113 \equiv 1 \pmod{8}$, we know that $x^2 \equiv 2 \pmod{113}$ has a solution, which we can construct by the algorithm of Theorem B.50. Beginning with $t_0 = 2^7 \equiv 15 \pmod{113}$, we then find k_0 by repeated squaring again.

i	0	1	2	3	4
t^{2^i}	15	112	1	1	1

Here $k_0 = 2$ satisfies $0 < k_0 < e$, so we know that a solution of $x^2 \equiv 2 \pmod{113}$ exists, but is not given by $b_0 = 2^{(7+1)/2} = 2^4 = 16$. (Note however that $b_0^2 = 256 \equiv 2 \cdot 15 \equiv at_0 \pmod{p}$, as should be the case.) So now we must calculate $r_0 = c^{(p-1)/2^{k_0+1}} = c^{(p-1)/2^3}$ modulo 113. Note that this is the same as $c^{2^1 \cdot 7} = (c^7)^2 \equiv 18 \pmod{113}$, the second entry in the second row of our first table. Thus we now have $b_1 = b_0 \cdot r_0 = 16 \cdot 18 \equiv 62 \pmod{113}$ and $t_1 = t_0 \cdot r_0^2 = 15 \cdot 18^2 \equiv 1 \pmod{113}$. Since $t_1 = 1$, then $k_1 = 0$ and the process terminates. We conclude that $b_1 = 62$ is a solution of $x^2 \equiv 2 \pmod{113}$, as is $-b_1 = -62 \equiv 51 \pmod{113}$. We can easily verify this claim.

As a final case for this example, let $a = 9$. Then $t_0 = 9^7 \equiv 18 \pmod{113}$ and we find from the following calculations that $k_0 = 3$.

i	0	1	2	3	4
t^{2^i}	18	98	112	1	1

Here we find that several iterations of the process are necessary, and we use the following table to keep track of the calculations.

i	0	1	2	3
b_i	7	54	68	110
t_i	18	98	112	1
k_i	3	2	1	0
r_i	40	18	98	

For example, we begin with $b_0 = 9^4 \equiv 7 \pmod{113}$, with $t_0 = 18$ and $k_0 = 3$ as already noted. Since $k_0 > 0$, we then calculate $r_0 = c^{(p-1)/2^4} = c^q = 40$, again using previous calculations. So now $b_1 = b_0 \cdot r_0 \equiv 54 \pmod{113}$ and $t_1 = t_0 \cdot r_0^2 \equiv 98 \pmod{113}$, from which we find that $k_1 = 2$. Thus $r_1 = c^{(p-1)/2^3} = (c^q)^2 = 18$, from which we obtain $b_2 \equiv 68 \pmod{113}$ and $t_2 \equiv 112 \pmod{113}$. Continuing in this way, we find that $t_3 = 1$, and so $b_3 = 110$ is a solution of $x^2 \equiv 9 \pmod{113}$. Here of course $110 \equiv -3 \pmod{113}$, and we have established that $x^2 \equiv 9 \pmod{113}$ has solutions ± 3. This case illustrates that the algorithm of Theorem B.50 generally does not recognize obvious solutions of a quadratic congruence when they exist. ◊

We conclude this section with two special cases of this algorithm. We prove these results as corollaries of Theorem B.50, although each can also be established by more independent means.

COROLLARY B.51. *Let p be a prime number with $p \equiv 3 \pmod 4$, and let a be an integer for which $\left(\frac{a}{p}\right) = 1$. Then $b = a^{\frac{p+1}{4}}$ is a solution of $x^2 \equiv a \pmod p$.*

PROOF. If $p \equiv 3 \pmod 4$, then $p - 1 = 2q$ with q odd. Let a be an integer with $\left(\frac{a}{p}\right) = 1$. With $e = 1$, a solution of $x^2 \equiv a \pmod p$ is given by $b = b_0 = a^{\frac{q+1}{2}}$ in the notation of Theorem B.50. (The order of t_0 must be a divisor of $2^{e-1} = 1$.) But if $p - 1 = 2q$, then

$$\frac{q+1}{2} = \frac{\frac{p-1}{2} + 1}{2} = \frac{p+1}{4},$$

and we obtain the given expression for b. □

EXAMPLE. Let $p = 79$ and $a = 2$, so that $\left(\frac{a}{p}\right) = 1$ since $79 \equiv 7 \pmod 8$. Corollary B.51 implies that 2^{20} is a solution of $x^2 \equiv 2 \pmod{79}$. We find that $2^{20} \equiv 9 \pmod{79}$, and can verify that $9^2 \equiv 2 \pmod{79}$. ◊

COROLLARY B.52. *Let p be a prime number with $p \equiv 5 \pmod 8$. Then $2^{\frac{p-1}{4}}$ is a solution of $x^2 \equiv -1 \pmod p$. If a is an integer for which $\left(\frac{a}{p}\right) = 1$, then $a^{\frac{p+3}{8}}$ is a solution of $x^2 \equiv a \pmod p$ or of $x^2 \equiv -a \pmod p$. If $a^{\frac{p+3}{8}}$ is a solution of $x^2 \equiv a \pmod p$, then $a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}$ satisfies $x^2 \equiv -a \pmod p$. Similarly, if $a^{\frac{p+3}{8}}$ is a solution of $x^2 \equiv -a \pmod p$, then $a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}$ satisfies $x^2 \equiv a \pmod p$. In either case we can solve both congruences.*

PROOF. If $p \equiv 5 \pmod 8$, then $p - 1 = 2^2 \cdot q$ with q odd, and $c = 2$ is an integer for which $\left(\frac{c}{p}\right) = -1$. For the first claim, we apply Theorem B.50 with $a = -1$, finding that $t_0 = (-1)^q = -1$ and $k_0 = 1$. So then with $c = 2$, we have that $r_0 = 2^q$ and $b_1 = b_0 \cdot r_0 = (-1)^{\frac{q+1}{2}} \cdot 2^q$. Here k_1 must equal 0, so b_1 satisfies $x^2 \equiv a \pmod p$. Since b_0 is 1 or -1, it follows that $2^q = 2^{\frac{p-1}{4}}$ is a solution of $x^2 \equiv -1 \pmod p$ in any case.

Now let a be an integer with $\left(\frac{a}{p}\right) = 1$, and let $t = t_0 = a^q$. Since $t^2 = a^{2q} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$, we know that $t \equiv 1 \pmod p$ or $t \equiv -1 \pmod p$. If $b = b_0 = a^{\frac{q+1}{2}}$, then $b^2 \equiv at \pmod p$ in either case. Therefore $b = a^{\frac{q+1}{2}} = a^{\frac{p+3}{8}}$ satisfies either $x^2 \equiv a \pmod p$ or $x^2 \equiv -a \pmod p$, as claimed.

The final claims follow by combining the first and second statements, or by applying the algorithm of Theorem B.50. □

EXAMPLE. Let $p = 61$. Here $2^{\frac{p-1}{4}} = 2^{15} \equiv 11 \pmod{61}$, and we find that $11^2 \equiv -1 \pmod{61}$. If $a = 3$, then $\left(\frac{a}{p}\right) = 1$, and $a^{\frac{p+3}{8}} \equiv 3^8 \equiv 34 \pmod{61}$. Now $34^2 \equiv -3 \pmod{61}$, and it follows that $34 \cdot 11 \equiv 8 \pmod{61}$ satisfies $x^2 \equiv 3 \pmod{61}$. ◊

Exercises on Constructing Solutions of Quadratic Congruences. In Questions 1–12, use the method of Theorem B.50 or one of its corollaries to find a solution of the given congruence. (Each modulus is a prime number.)

1. $x^2 \equiv 2 \pmod{17}$.
2. $x^2 \equiv 3 \pmod{23}$.
3. $x^2 \equiv -1 \pmod{29}$.
4. $x^2 \equiv 5 \pmod{29}$.
5. $x^2 \equiv -1 \pmod{37}$.
6. $x^2 \equiv 3 \pmod{37}$.
7. $x^2 \equiv 10 \pmod{37}$.
8. $x^2 \equiv 2 \pmod{41}$.
9. $x^2 \equiv 5 \pmod{41}$.
10. $x^2 \equiv -1 \pmod{41}$.
11. $x^2 \equiv 2 \pmod{47}$.
12. $x^2 \equiv 3 \pmod{47}$.

Legendre's Theorem

We conclude Appendix B with an application of quadratic congruences to the existence of solutions of a particular type of quadratic equation.

Let a, b, and c be nonzero integers, not all of the same sign, and consider the equation

$$ax^2 + by^2 + cz^2 = 0. \tag{B.27}$$

When does an equation of this form have a *primitive* solution, that is, an integer solution with $\gcd(x, y, z) = 1$? (Note that a trivial solution $(x, y, z) = (0, 0, 0)$ always exists, but is not primitive.) We begin with some restrictions that we can place on the coefficients a, b, and c.

We can assume that a, b, and c are squarefree. If d^2 is the largest square dividing a, for example, say with $a = d^2a'$, and (x, y, z) is a nontrivial solution of (B.27), then

$$0 = ax^2 + by^2 + cz^2 = a'(dx)^2 + by^2 + cz^2,$$

so that (dx, y, z) is a nontrivial solution of $a'x^2 + by^2 + cz^2 = 0$. Conversely, if (x, y, z) satisfies the latter equation, then

$$ax^2 + b(dy)^2 + c(dz)^2 = d^2(a'x^2 + by^2 + cz^2) = d^2 \cdot 0 = 0.$$

So (B.27) has a nontrivial solution if and only if there is a nontrivial solution of $a'x^2 + by^2 + cz^2 = 0$, in which the coefficient of x^2 is squarefree. Square factors can likewise be eliminated from the coefficients b and c.

We can further assume that a, b, and c are pairwise relatively prime. Clearly, a common divisor of a, b, and c can be canceled from (B.27) without affecting the solutions. Suppose then that some prime number p divides two of the coefficients, say a and c, but not the third. Then in any solution

(x, y, z) of (B.27), we must have $by^2 = -ax^2 - cz^2$ divisible by p. Since $p \nmid b$, then $p \mid y$. We conclude that if $ax^2 + by^2 + cz^2 = 0$, then

$$\frac{a}{p}x^2 + bp\left(\frac{y}{p}\right)^2 + \frac{c}{p}z^2 = 0.$$

Notice that since a, b, and c are squarefree and $p \nmid b$, the coefficients of $\frac{a}{p}x^2 + (bp)y^2 + \frac{c}{p}z^2$ are still squarefree, but only one is divisible by p. Conversely, if (x, y, z) satisfies $\frac{a}{p}x^2+(bp)y^2+\frac{c}{p}z^2 = 0$, then $ax^2 + b(py)^2 + cz^2 = 0$. Other prime common divisors of two of the coefficients can be eliminated in the same way.

Given these conditions on a, b, and c, we have the following necessary and sufficient conditions for the existence of primitive solutions of equation (B.27).

THEOREM B.53 (Legendre's Theorem). *Let a, b, and c be nonzero integers that are squarefree, pairwise relatively prime, and neither all positive nor all negative. Then $ax^2 + by^2 + cz^2 = 0$ has a primitive integer solution (x, y, z) if and only if the following three quadratic congruences each have solutions:*

$$x^2 \equiv -bc \pmod{|a|}, \qquad x^2 \equiv -ac \pmod{|b|}, \qquad x^2 \equiv -ab \pmod{|c|}. \tag{B.28}$$

EXAMPLE. Let r be a squarefree positive integer, not divisible by 2 or 3. Assuming Legendre's Theorem, find a criterion for r such that $2x^2 + 3y^2 = rz^2$ has a primitive solution.

Here we let $a = 2$, $b = 3$, and $c = -r$, so that the conditions of Legendre's Theorem are satisfied, and the congruences of (B.28) are $x^2 \equiv 3r \pmod 2$, $x^2 \equiv 2r \pmod 3$, and $x^2 \equiv -6 \pmod r$. The first congruence is solvable independent of r. The second has a solution if and only if $\left(\frac{2r}{3}\right) = 1$, which implies that $r \equiv 2 \pmod 3$ (or since r is odd, $r \equiv 5 \pmod 6$). The third congruence implies that for every prime p dividing r, $\left(\frac{-6}{p}\right) = 1$. We leave it as an exercise to show that $\left(\frac{-6}{p}\right) = 1$ if and only if p is congruent to 1, 5, 7, or 11 modulo 24.

The following table lists all $r < 100$ that satisfy these criteria, and verifies (by trial-and-error) that in each case, $2x^2 + 3y^2 = rz^2$ has a primitive solution.

r	x	y	z	r	x	y	z
5	1	1	1	53	5	1	1
11	2	1	1	59	4	3	1
29	1	3	1	77	1	5	1
35	4	1	1	83	2	5	1

Note that the requirement that $\left(\frac{-6}{p}\right) = 1$ for all primes p dividing r is stricter than the condition that $\left(\frac{-6}{r}\right) = 1$. For instance, if $r = 221$, then $221 \equiv 1 \pmod 4$, $221 \equiv 5 \pmod 8$, and $221 \equiv 2 \pmod 3$, so that $\left(\frac{-6}{221}\right) = \left(\frac{-1}{221}\right)\left(\frac{2}{221}\right)\left(\frac{3}{221}\right) = 1 \cdot (-1) \cdot \left(\frac{221}{3}\right) = 1$. But $221 = 13 \cdot 17$ and both $\left(\frac{-6}{13}\right) = -1$ and $\left(\frac{-6}{17}\right) = -1$. Since $x^2 \equiv -6 \pmod{13}$ has no solutions, $x^2 \equiv -6 \pmod{221}$ likewise has no solutions. ♢

We first show that the solvability of the congruences in (B.28) is necessary for the existence of a primitive solution of $ax^2 + by^2 + cz^2 = 0$.

PROOF OF LEGENDRE'S THEOREM (PART 1). Let a, b, and c be squarefree integers that are pairwise relatively prime. Suppose that $ax^2+by^2+cz^2 = 0$ has a solution with $\gcd(x, y, z) = 1$. We find that $\gcd(c, y)$ must equal 1. Otherwise, if a prime p divides c and y, then p would divide ax^2, and since $\gcd(a, c) = 1$, then $p \mid x$. But with $p \mid x$ and $p \mid y$, then p^2 must divide $ax^2 + by^2 = -cz^2$, so that p divides z, since c is squarefree. This contradicts the assumption that (x, y, z) is primitive.

Now $ax^2 + by^2 + cz^2 = 0$ implies that $ax^2 \equiv -by^2 \pmod{|c|}$. Multiplying both sides by a yields $a^2x^2 = (ax)^2 \equiv -aby^2 \pmod{|c|}$. Since $\gcd(c, y) = 1$, then y has an inverse modulo $|c|$, and

$(axy^{-1})^2 \equiv -ab \pmod{|c|}$. So the congruence $x^2 \equiv -ab \pmod{|c|}$ must have a solution. The other congruences of (B.28) are established similarly. □

The proof of the sufficiency of the congruences in (B.28) is much more difficult. We will follow a method due to Mordell, adapted from *A Course in Number Theory* (Rose, 1988), requiring several preliminary results.

LEMMA B.54. *Let n be a positive integer. Let r, s, and t be positive real numbers, not all integers, such that $rst = n$. Then for all $a, b, c \in \mathbb{Z}$, the congruence $ax + by + cz \equiv 0 \pmod{n}$ has a solution $(x_0, y_0, z_0) \neq (0, 0, 0)$ with $|x_0| < r$, $|y_0| < s$, and $|z_0| < t$.*

PROOF. Consider the set S of triples (x, y, z) such that $0 \leq x \leq \lceil r \rceil - 1$, $0 \leq y \leq \lceil s \rceil - 1$, and $0 \leq z \leq \lceil t \rceil - 1$. (Here $\lceil r \rceil$ is the smallest integer greater than or equal to r. Notice that $\lceil r \rceil - 1 = \lfloor r \rfloor$ unless r is an integer, in which case $\lceil r \rceil - 1 = r - 1$. In any case, $\lceil r \rceil - 1 < r$.) There are $\lceil r \rceil$ possibilities for x, $\lceil s \rceil$ for y, and $\lceil t \rceil$ for z, so that the number of elements in S is $\lceil r \rceil \cdot \lceil s \rceil \cdot \lceil t \rceil$. Since r, s, and t are not all integers, $\lceil r \rceil \cdot \lceil s \rceil \cdot \lceil t \rceil$ is strictly larger than $rst = n$.

So S contains more than n elements. There are n possibilities for $(ax + by + cz) \bmod n$, so we conclude that S must contain at least two different triples, (x_1, y_1, z_1) and (x_2, y_2, z_2), such that $ax_1 + by_1 + cz_1 \equiv ax_2 + by_2 + cz_2 \pmod{n}$. But now $ax_0 + by_0 + cz_0 \equiv 0 \pmod{n}$, where $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, and $z_0 = z_1 - z_2$. Since $(x_1, y_1, z_1) \neq (x_2, y_2, z_2)$, then $(x_0, y_0, z_0) \neq (0, 0, 0)$. Also, since $0 \leq x_1, x_2 < r$, then $|x_0| < r$, and similar statements are true for the other two terms. □

The key to this proof is that S contains more than n elements, while $\mathbb{Z}_n$ contains exactly n elements. Thus a function from S to $\mathbb{Z}_n$, specifically the function that sends each triple (x, y, z) to the least residue of $ax + by + cz$ modulo n, cannot be one-to-one, and so must send two triples to the same element. This is an example of the *Pigeonhole Principle*, sometimes stated informally as follows: If more than n pigeons fly into n pigeonholes, at least one pigeonhole contains two or more pigeons. This obvious observation is often a surprisingly powerful tool in proving statements in number theory.

LEMMA B.55. *Let a, b, and c be squarefree integers that are pairwise relatively prime. Suppose that the congruences of* (B.28) *each have solutions. Then there are integers a_1, b_1, c_1, a_2, b_2, and c_2 such that $ax^2 + by^2 + cz^2 \equiv (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) \pmod{|abc|}$ for all integers x, y, and z.*

PROOF. Suppose that $x^2 \equiv -bc \pmod{|a|}$, $x^2 \equiv -ac \pmod{|b|}$, and $x^2 \equiv -ab \pmod{|c|}$ have solutions r, s, and t respectively. Since a, b, and c are pairwise relatively prime, we can let b^{-1} be the inverse of b modulo $|a|$, c^{-1} the inverse of c modulo $|b|$, and a^{-1} the inverse of a modulo $|c|$. Then working modulo $|a|$, we have

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \equiv b^{-1}b(by^2 + cz^2) \\ &\equiv b^{-1}(b^2y^2 - (-bc)z^2) \equiv b^{-1}((by)^2 - (rz)^2) \\ &\equiv b^{-1}(by - rz)(by + rz) \equiv (y - b^{-1}rz)(by + rz) \pmod{|a|}. \end{aligned}$$

Modulo $|b|$,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + cz^2 \equiv c^{-1}c(ax^2 + cz^2) \\ &\equiv c^{-1}(acx^2 + c^2z^2) \equiv c^{-1}(-(sx)^2 + (cz)^2) \\ &\equiv c^{-1}(cz - sx)(cz + sx) \equiv (z - c^{-1}sx)(cz + sx) \pmod{|b|}. \end{aligned}$$

And modulo $|c|$,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + by^2 \equiv a^{-1}a(ax^2 + by^2) \\ &\equiv a^{-1}(a^2x^2 + aby^2) \equiv a^{-1}((ax)^2 - (ty)^2) \\ &\equiv a^{-1}(ax - ty)(ax + ty) \equiv (x - a^{-1}ty)(ax + ty) \pmod{|c|}. \end{aligned}$$

In other words, modulo $|a|$, $|b|$, and $|c|$ separately, the quadratic term $ax^2 + by^2 + cz^2$ is congruent to a product of two linear terms in x, y, and z.

Now since a, b, and c are pairwise relatively prime, it is possible to find an integer a_1 so that $a_1 \equiv 0 \pmod{|a|}$, $a_1 \equiv -c^{-1}s \pmod{|b|}$, and $a_1 \equiv 1 \pmod{|c|}$, that is, a_1 is congruent to the coefficient of x in the first linear term of each product above. Likewise, we can select b_1 so that $b_1 \equiv 1 \pmod{|a|}$, $b_1 \equiv 0 \pmod{|b|}$, and $b_1 \equiv -a^{-1}t \pmod{|c|}$, and so forth. But then we find that $(a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z)$ is congruent to $ax^2 + by^2 + cz^2$ modulo $|a|$, modulo $|b|$, and modulo $|c|$, and thus modulo $|abc|$. □

EXAMPLE. We consider an example to illustrate the computations in this proof. Let $a = 2$, $b = 3$, and $c = -53$, which we have seen satisfy the conditions of Legendre's Theorem. We can select $r = 1$ as a solution of $x^2 \equiv 159 \pmod 2$, $s = 1$ to satisfy $x^2 \equiv 106 \pmod 3$, and $t = 10$ to satisfy $x^2 \equiv -6 \pmod{53}$. The inverse of b modulo a can be chosen as $b^{-1} = 1$; the inverse of c modulo b is $c^{-1} = 1$; the inverse of a modulo $|c|$ is $a^{-1} = 27$.

Following the calculations in the proof of Lemma B.55, we then find that

$$\begin{aligned} 2x^2 + 3y^2 - 53z^2 &\equiv [(0)x + (1)y + (-1)z] \cdot [(0)x + (3)y + (1)z] \pmod 2 \\ 2x^2 + 3y^2 - 53z^2 &\equiv [(-1)x + (0)y + (1)z] \cdot [(1)x + (0)y + (-53)z] \pmod 3 \\ 2x^2 + 3y^2 - 53z^2 &\equiv [(1)x + (-270)y + (0)z] \cdot [(2)x + (10)y + (0)z] \pmod{53} \end{aligned}$$

Using the Chinese Remainder Theorem, a simultaneous solution of $x \equiv \ell \pmod 2$, $x \equiv m \pmod 3$, and $x \equiv n \pmod{53}$ is given by $x \equiv 159\ell + 106m + 54n \pmod{318}$. Selecting the coefficients of x, of y, and of z in the two terms of the products above in turn as ℓ, m, and n, we compile the following table.

ℓ	m	n	$v = 159\ell + 106m + 54n$	$v \bmod 318$
0	−1	1	−52	266
1	0	−270	−14421	207
−1	1	0	−53	265
0	1	2	214	214
3	0	10	1017	63
1	−53	0	−5459	265

We conclude that $2x^2 + 3y^2 - 53z^2 \equiv (266x + 207y + 265z)(214x + 63y + 265z) \pmod{318}$ for all integers x, y, and z. ◊

In this example, we followed the computations in the proof of Lemma B.55 exactly as given. But we also could have replaced the entries in the columns headed by ℓ, m, and n by their least residues modulo 2, 3, and 53 respectively to simplify some calculations.

PROOF OF LEGENDRE'S THEOREM (PART 2). We now show that the congruences of (B.28) are sufficient to guarantee the existence of a primitive solution of $ax^2 + by^2 + cz^2 = 0$. Since a, b, and c are not all of the same sign, we can assume without loss of generality, by renaming variables and multiplying through by -1 if necessary, that a and b are positive and c is negative. We note a special case first—if $a = 1$, $b = 1$, and $c = -1$, then the congruences of (B.28) are all solvable,

and $x^2 + y^2 - z^2 = 0$ has primitive solutions, such as $(1, 0, 1)$. So we suppose that a, b, and $-c$ are positive squarefree integers, pairwise relatively prime, and not all equal to 1, and that

$$x^2 \equiv -bc \pmod{a}, \qquad x^2 \equiv -ac \pmod{b}, \qquad x^2 \equiv -ab \pmod{|c|}$$

all have solutions.

By Lemma B.55, we know that there are integers a_1, b_1, c_1, a_2, b_2, and c_2 so that

$$ax^2 + by^2 + cz^2 \equiv (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) \pmod{|abc|} \tag{B.29}$$

for all x, y, and z. Let $r = \sqrt{-bc}$, $s = \sqrt{-ac}$, and $t = \sqrt{ab}$. Notice that r, s, and t are all positive real numbers, and that not all of them are integers, since a, b, and $-c$ are pairwise relatively prime, squarefree, and not all 1. Note also that $rst = |abc|$. Thus we have the conditions needed for Lemma B.54, and we can conclude that there is a triple of integers $(x_0, y_0, z_0) \neq (0, 0, 0)$ with $|x_0| < r$, $|y_0| < s$, and $|z_0| < t$ so that $a_1x_0 + b_1y_0 + c_1z_0 \equiv 0 \pmod{|abc|}$. Since (B.29) holds for all triples, we then immediately have that $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{|abc|}$.

Now since $x_0^2 < r^2 = -bc$, $y_0^2 < s^2 = -ac$, and $c < 0$, we have that

$$ax_0^2 + by_0^2 + cz_0^2 \leq ax_0^2 + by_0^2 < a(-bc) + b(-ac) = -2abc = 2|abc|.$$

But likewise, since $a > 0$, $b > 0$, $c < 0$, and $z_0^2 < t^2 = ab$, we see that

$$ax_0^2 + by_0^2 + cz_0^2 \geq cz_0^2 > c(ab) = abc = -|abc|.$$

With $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{|abc|}$ and $-|abc| < ax_0^2 + by_0^2 + cz_0^2 < 2|abc|$, it follows that either $ax_0^2 + by_0^2 + cz_0^2 = 0$ or $ax_0^2 + by_0^2 + cz_0^2 = |abc| = -abc$. In the first case, we have a nontrivial solution of $ax^2 + by^2 + cz^2 = 0$, as we wanted to find. So we assume instead that $ax_0^2 + by_0^2 + cz_0^2 = -abc$.

Finally then, let $x_1 = x_0z_0 - by_0$, $y_1 = y_0z_0 + ax_0$, and $z_1 = z_0^2 + ab$. Notice that $z_1 > 0$, so that $(x_1, y_1, z_1) \neq (0, 0, 0)$. Now we find that

$$\begin{aligned} ax_1^2 + by_1^2 + cz_1^2 &= a(x_0z_0 - by_0)^2 + b(y_0z_0 + ax_0)^2 + c(z_0^2 + ab)^2 \\ &= (ax_0^2z_0^2 - 2abx_0y_0z_0 + ab^2y_0^2) + (by_0^2z_0^2 + 2abx_0y_0z_0 + a^2bx_0^2) \\ &\qquad +(cz_0^4 + 2abcz_0^2 + a^2b^2c) \\ &= z_0^2(ax_0^2 + by_0^2 + cz_0^2) + ab(ax_0^2 + by_0^2 + cz_0^2) + (abc)z_0^2 + (abc)ab \\ &= (ax_0^2 + by_0^2 + cz_0^2 + abc)(z_0^2 + ab). \end{aligned}$$

But assuming that $ax_0^2 + by_0^2 + cz_0^2 = -abc$, we then have $ax_1^2 + by_1^2 + cz_1^2 = 0$. So in any case, the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial solution. □

Example. Again let $a = 2$, $b = 3$, and $c = -53$. In a previous example, we saw that

$$2x^2 + 3y^2 - 53z^2 \equiv (266x + 207y + 265z)(214x + 63y + 265z) \pmod{318}$$

for all x, y, and z, which is in the form of (B.29). Let $r = \sqrt{-bc} = \sqrt{159}$, $s = \sqrt{-ac} = \sqrt{106}$, and $t = \sqrt{ab} = \sqrt{6}$. By Lemma B.54, there is a triple of integers $(x_0, y_0, z_0) \neq (0, 0, 0)$ with $|x_0| < r < 13$, $|y_0| < s < 11$, and $|z_0| < t < 3$ so that $266x_0 + 207y_0 + 265z_0 \equiv 0 \pmod{318}$. Following the proof of Lemma B.54, we could calculate the least residue of $266x + 207y + 265z$ modulo 318 for all $0 \leq x < 13$, $0 \leq y < 11$, and $0 \leq z < 3$. With $13 \cdot 11 \cdot 3 = 429$ triples, there must be at least two that produce the same least residue modulo 318. That pair in turn gives a solution of $266x_0 + 207y_0 + 265z_0 \equiv 0 \pmod{318}$. Alternatively, with few choices available for z, we can proceed by trial-and-error. We find for instance that the linear equation $266x + 207y = 265$ has $x = 8$ and $y = -9$ as a solution. So $(x_0, y_0, z_0) = (8, -9, -1)$ satisfies $266x_0 + 207y_0 + 265z_0 \equiv 0 \pmod{318}$, and satisfies the inequalities above.

Now by (B.29), it follows that $(8, -9, -1)$ also satisfies $2x^2 + 3y^2 - 53z^2 \equiv 0 \pmod{318}$. We find that $2 \cdot 8^2 + 3 \cdot (-9)^2 - 53 \cdot (-1)^2 = 318$. (As noted in the proof, with the restrictions on x_0, y_0, and z_0, the only possibilities are 0 and $-abc = 318$ as in this case.) To find a solution of

$2x^2 + 3y^2 - 53z^2 = 0$, we make the adjustment given in the proof. Let $x_1 = x_0z_0 - by_0 = 19$, $y_1 = y_0z_0 + ax_0 = 25$, and $z_1 = z_0^2 + ab = 7$. We find that $2 \cdot 19^2 + 3 \cdot 25^2 - 53 \cdot 7^2 = 0$, so we have constructed a nontrivial solution of that quadratic form. ◊

Exercises on Legendre's Theorem. In Exercises 1–5, use Legendre's Theorem to decide whether the given equation has primitive solutions. (Note that in some cases, adjustments to the coefficients are necessary before Legendre's Theorem applies.)

1. $3x^2 + 5y^2 - 107z^2 = 0$.
2. $3x^2 - 7y^2 + 3z^2 = 0$.
3. $12x^2 - 15y^2 + 20z^2 = 0$.
4. $10x^2 - 13y^2 + 133z^2 = 0$.
5. $10x^2 - 11y^2 + 21z^2 = 0$.

In Exercises 6–10, find a criterion for r so that the given equation has nontrivial integer solutions. Assume that r is positive, squarefree, and relatively prime to the coefficients of x^2 and y^2.

7. $x^2 + y^2 = rz^2$.
8. $x^2 - y^2 = rz^2$.
9. $x^2 + 2y^2 = rz^2$.
10. $x^2 + 5y^2 = rz^2$.
11. $3x^2 + 5y^2 = rz^2$.

APPENDIX C

Algebraic Systems

Our emphasis in this text is on questions that can be phrased in terms of integers. An overarching theme, however, is that some of these problems can be more easily approached by working in larger sets of numbers, particularly domains of *quadratic integers*. In this appendix, we review some of the definitions and theorems concerning these and other abstract algebraic structures, with emphasis on results that we use in the body of the text.

Groups

A binary operation $*$ on a set A is a function from $A \times A$ to A, that is, a rule that assigns to each ordered pair of elements a and b in A one and only one element, written as $a * b$, in the set A. (To emphasize that $a * b$ must be an element of A, we may say that A is *closed* under the $*$ operation.) Operations that satisfy certain algebraic properties are of particular importance. We list some of the most important potential properties of operations in the following definition.

DEFINITION. Let $*$ be an operation on a set A.

(1) If $a * b = b * a$ for every $a, b \in A$, we say that $*$ is *commutative*.
(2) If $a * (b * c) = (a * b) * c$ for every $a, b, c \in A$, we say that $*$ is *associative*.
(3) If there is an element e in A with the property that $a * e = a$ and $e * a = a$ for every $a \in A$, we call e an *identity* element for A under $*$, and we say that $*$ has the *identity property*.
(4) If e is an identity element for A under $*$, then we say that $*$ has the *inverse property* if for every $a \in A$, there is an element $b \in A$ so that $a * b = e$ and $b * a = e$.

DEFINITION. Let G be a set on which an operation $*$ is defined. We say that G is a *group* under $*$ if $*$ has the associative, identity, and inverse properties. If $*$ is also commutative, we say that G is an *abelian group* under $*$.

Examples of groups that we encounter in the text include the set $\mathbb{Z}$ of integers under addition, the set $\mathbb{Z}_m$ of congruence classes modulo a positive integer m under modular addition, the set $\mathbb{Z}_m^\times$ of units in $\mathbb{Z}_m$ under modular multiplication, unimodular matrices under matrix multiplication, and the ideal class group of a quadratic domain under multiplication. When making general statements about groups or abelian groups, we will typically write the operation of G as multiplication, the identity element as 1, and the inverse of an element a as a^{-1}. This notation must of course be interpreted correctly in individual examples of groups.

The following proposition lists some additional properties that hold in every example of a group. We leave the proof of these claims as Exercises 1–4.

PROPOSITION C.1. *Let G be a group under an operation written as multiplication. Then the following statements are true.*

(1) *For all $a, b, c \in G$, if $ab = ac$, then $b = c$. Likewise, if $ba = ca$, then $b = c$.*
(2) *The identity element of G is unique.*
(3) *For all $a \in G$, the inverse of a is unique.*
(4) *If a and b are elements of G, then $(ab)^{-1} = b^{-1}a^{-1}$.*

If a is an element of a group G, then we can define a^n for all integers n as follows. We let $a^0 = 1$ and then for $n > 0$, define $a^n = a \cdot a^{n-1}$ recursively. If $n = -m$ is negative, we let $a^n = (a^{-1})^m$, where a^{-1} is the inverse of a. Using associativity of the operation in G, we can show that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$. If a and b are elements in an *abelian* group, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. (In general, $(ab)^2 = (ab)(ab)$ is not necessarily the same as $a^2b^2 = (aa)(bb)$, so this last claim is not usually true in a nonabelian group.)

PROPOSITION C.2. *Let G be a group with finitely many elements. Then for all $a \in G$, there is an integer $t > 0$ so that $a^t = 1$. If t is the smallest positive integer with this property, then $a^n = 1$ if and only if t divides n, and $a^r = a^s$ if and only if $r \equiv s \pmod{t}$.*

PROOF. Let a be an element of G, and consider a, a^2, $a^3, \ldots$, which are elements of G by closure. If G has finitely many elements, there must be integers r and s with $0 < s < r$ so that $a^r = a^s$. Then $a^s \cdot a^{r-s} = a^s \cdot 1$ so that $a^{r-s} = 1$ by part (1) of Proposition C.1. So $t = r - s$ is a positive integer for which $a^t = 1$.

Now let t be the smallest positive integer for which $a^t = 1$. If $n = tq$, then $a^n = (a^t)^q = 1^q = 1$. Conversely, suppose that n is an integer for which $a^n = 1$. In $\mathbb{Z}$, we can write $n = tq + r$ for some integers q and r with $0 \leq r < t$. We find that $a^n = a^{tq+r} = (a^t)^q a^r = 1^q \cdot a^r = a^r$, using the exponent properties mentioned above. Thus $a^r = 1$, and to avoid contradicting the definition of t, we must have $r = 0$, so that t divides n. Finally, if $a^r = a^s$, we conclude as above that $a^{r-s} = 1$. By the previous statement, this is true if and only if t divides $r - s$, that is, $r \equiv s \pmod{t}$. □

DEFINITION. If a is an element of a group G, and $a^t = 1$ for some positive integer t, we refer to the smallest positive integer with that property as the *order* of a in G, and write $t = \text{ord}(a)$. If no such t exist (which by Proposition C.2 can occur only in an infinite group), we say that a has *infinite order* in G. We also refer to the number of elements in G as the *order* of G, written as $|G|$.

PROPOSITION C.3. *Let a be an element of finite order t in a group G. Then for every integer k, the order of a^k in G is $\frac{t}{\gcd(k,t)}$.*

PROOF. Suppose first that $k = d$ is a positive divisor of t, say with $t = dq$. Then $(a^d)^q = a^{dq} = 1$, and q is the smallest positive power for which that is true. (If $0 < r < q$, then $0 < dr < dq = t$, so $(a^d)^r = 1$ would violate the definition of the order of a in G.) So in this case, the order of $a^k = a^d$ is $q = \frac{t}{d} = \frac{t}{\gcd(k,t)}$.

Now it will suffice to show that if $\gcd(k, t) = d$, then $(a^k)^n = 1$ if and only if $(a^d)^n = 1$. If $\gcd(k, t) = d$, then d divides k, say with $k = ds$ for some integer s. So if $(a^d)^n = 1$, then $(a^k)^n = (a^{ds})^n = ((a^d)^n)^s = 1^s = 1$. For the converse, note first that if $\gcd(k, t) = d$, then we can write $d = kq + tr$ for some integers q and r. Now if $(a^k)^n = 1$, then $(a^d)^n = (a^{kq+tr})^n = (a^{kq} \cdot (a^t)^r)^n = ((a^k)^n)^q = 1^q = 1$. (Here we use the fact that $a^t = 1$ by definition of the order of a in G.) □

PROPOSITION C.4. *Let G be an abelian group of order $|G| = n$. Then $a^n = e$, the identity element of G, for every $a \in G$.*

PROOF. Write the elements of G as $\{a_1, a_2, \ldots, a_n\}$, and let a be an element of G. Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$ obtained by multiplying each element of G by a. By closure, S is a subset of G. But S contains n distinct elements, since if $aa_i = aa_j$ for some i, j, then $a_i = a_j$ by the cancellation property of Proposition C.1. So S is the same as G. Now the product (under the operation of G) of all elements of S must equal the product of all elements of G. That is, $aa_1 \cdot aa_2 \cdots aa_n = a_1 a_2 \cdots a_n$ in G. Since the operation of G is commutative, we can rearrange the product on the left-hand side as $a^n(a_1 a_2 \cdots a_n)$. With $a^n(a_1 a_2 \cdots a_n) = 1 \cdot (a_1 a_2 \cdots a_n)$, we conclude that $a^n = 1$ by cancellation. □

Proposition C.4 is also true in finite nonabelian groups, but a different proof is required, which we will outline in the next subsection.

Normal Subgroups and Factor Groups. The following definition allows us to use one group to construct other examples of groups.

DEFINITION. A subset H of a group G is called a *subgroup* of G if H is a group under the operation of G. If N is a subgroup of G, we say that N is *normal* in G if for all n in N and a in G, the element $a^{-1}na$ is in N.

Note that if H is a subset of G, then H is a subgroup of G if and only if the following are true:

(1) H contains the identity element, 1, of G.
(2) For every a in H, the inverse, a^{-1}, of a, as defined in G, is also in H.
(3) For every a and b in H, the product ab is an element of H.

If G is an abelian group, then every subgroup of G is normal.

EXAMPLE. If a is an element of a group G, define $\langle a\rangle$ to be the set of all integer powers of a, that is, $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$. The exponent rules listed above show that $\langle a\rangle$ is a subgroup of G. We call $\langle a\rangle$ the *cyclic subgroup* of G *generated by* a. ◊

We can use a subgroup N of G to define an equivalence relation on G. When N is a *normal* subgroup of G, there is a group structure on the set of equivalence classes under that relation.

DEFINITION. Let N be a subgroup of a group G. If a and b are elements of G, we say that a is *congruent* to b modulo N, and write $a \equiv b \pmod N$, if $a^{-1}b$ is an element of N.

PROPOSITION C.5. *Let N be a subgroup of a group G. Then the operation of congruence modulo N defined above is an equivalence relation on N. If N is normal in G, and G/N is the set of all distinct equivalence classes of elements of G under congruence modulo N, then the operation $[a]\cdot[b] = [ab]$ on G/N is well-defined, and makes G/N into a group.*

PROOF. Let N be a subgroup of G, and let a, b, c, and d be elements of G with $a \equiv c \pmod N$ and $b \equiv d \pmod N$, so that $a^{-1}c$ and $b^{-1}d$ are elements of N. If N is normal in G, then $b^{-1}(a^{-1}c)b$ is an element of N, and so $(b^{-1}(a^{-1}c)b)(b^{-1}d)$ is in N by closure. But then we find that

$$(b^{-1}(a^{-1}c)b)(b^{-1}d) = (b^{-1}a^{-1})c(bb^{-1})d = (ab)^{-1}(cd)$$

is in N, which implies that $ab \equiv cd \pmod N$. This shows that multiplication of equivalence classes is well-defined when N is normal in G. We leave the other claims of this proposition as Exercises 5 and 6. □

DEFINITION. We refer to G/N as the *factor group* of G modulo N.

If N is a subgroup of G (normal or otherwise), then equivalence classes under congruence modulo N have the following property. If a is an element of G, then $[a] = \{an \mid n \in N\}$. We also write this set as aN and call it the *(left) coset* of N in G determined by a. Properties of equivalence classes ensure that $aN = bN$ if b is an element of aN, while aN has no elements in common with bN otherwise. Furthermore, two cosets of N in G must have the same number of elements, namely the number of elements of N, since $an_1 = an_2$ for n_1 and n_2 in N if and only if $n_1 = n_2$. In other words, the cosets of N partition G into a collection of subsets all of the same size. If G is finite, and there are k distinct cosets of N in G, it follows that $|G| = k \cdot |N|$, so that $|N|$ divides $|G|$. In particular, if a is an element of a finite group G, then $\text{ord}(a) = |\langle a\rangle|$ divides $|G|$. If $|G| = n$, it follows that $a^n = 1$ by Proposition C.2.

Homomorphisms and Isomorphisms. We often need to compare two examples of groups, for instance to show that a given group has properties in common with a more familiar group. The following definition gives us a precise method of doing so.

DEFINITION. Let G_1 and G_2 be groups. A function $\phi : G_1 \to G_2$ is called a *homomorphism* if $\phi(ab) = \phi(a) \cdot \phi(b)$ for every pair of elements a and b in G_1. When ϕ is a homomorphism, we say that ϕ is an *isomorphism* if ϕ is both injective (that is, if $\phi(a) = \phi(b)$ for a and b in G_1, then $a = b$) and surjective (for every c in G_2, there is some a in G_1 so that $\phi(a) = c$). We say that G_1 is *isomorphic* to G_2 if there is some isomorphism ϕ from G_1 to G_2.

PROPOSITION C.6. *Let $\phi : G_1 \to G_2$ be a homomorphism. Then the following are true.*

(1) *$\phi(1) = 1$, that is, ϕ takes the identity element of G_1 to the identity element of G_2.*
(2) *$\phi(a^{-1}) = \phi(a)^{-1}$ for all a in G_1.*
(3) *If H_1 is a subgroup of G_1, then $\phi(H_1) = \{\phi(a) \mid a \in G_1\}$ is a subgroup of G_2.*
(4) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a)$ is in $H_2\}$ is a subgroup of G_1.*

PROOF. We prove statements (1) and (4), leaving the other proofs as Exercises 7 and 8. For (1), note that $a = a \cdot 1$ for all a in G_1. So we must have $\phi(a) = \phi(a \cdot 1) = \phi(a) \cdot \phi(1)$ by the definition of a homomorphism. But note that $\phi(a) = \phi(a) \cdot 1$ as an element of G_2. Since $\phi(a) \cdot \phi(1) = \phi(a) \cdot 1$, we must have $\phi(1) = 1$ by cancellation.

For statement (4), let H_2 be a subgroup of G_2, and let $H_1 = \phi^{-1}(H_2)$ as defined above. We know that H_2 must contain the identity element of G_2, and statement (1) says that the identity element of G_1 is taken to that element by ϕ. By definition, the identity element of G_1 is then in $H_1 = \phi^{-1}(H_2)$. Let a be an element of H_1, so that $\phi(a) = c$ is in H_2. Then, assuming statement (2), $\phi(a^{-1}) = c^{-1}$. Since c^{-1} is in H_2, then a^{-1} is in H_1 by definition. Finally, suppose that a and b are in H_1, so that $\phi(a) = c$ and $\phi(b) = d$ are elements of H_2. Then $\phi(ab) = \phi(a) \cdot \phi(b) = cd$, and since cd is an element of H_2 by closure, it follows that ab is in H_1. So H_1 is a subgroup of G_1. □

PROPOSITION C.7. *Let $\phi : G_1 \to G_2$ be a homomorphism. Define the kernel of ϕ to be the set of all elements of G_1 that ϕ takes to the identity element of G_2, and the define the image of ϕ to be the set of all elements of G_2 that equal $\phi(a)$ for some a in G_1. We write these sets as*

$$\mathrm{Ker}(\phi) = \{a \in G_1 \mid \phi(a) = 1\} \qquad \text{and} \qquad \mathrm{Im}(\phi) = \{\phi(a) \mid a \text{ is in } G_1\}.$$

Then $\mathrm{Ker}(\phi)$ is a normal subgroup of G_1, and $\mathrm{Im}(\phi)$ is a subgroup of G_2.

PROOF. Since G_1 is a subgroup of itself, then $\mathrm{Im}(\phi) = \phi(G_1)$ is a subgroup of G_2 by part (3) of Proposition C.6. Similarly, if 1 is the identity element of G_2, then $H_2 = \{1\}$ is a subgroup of G_2, so that $\mathrm{Ker}(\phi) = \phi^{-1}(H_2)$ is a subgroup of G_1 by Proposition C.6, part (4). To show that $\mathrm{Ker}(\phi)$ is normal in G_1, let n be an element of $\mathrm{Ker}(\phi)$ and let a be an arbitrary element of G_1. Then we find that

$$\phi(a^{-1}na) = \phi(a^{-1}) \cdot \phi(n) \cdot \phi(a) = \phi(a)^{-1} \cdot 1 \cdot \phi(a) = 1$$

in G_2, using part (2) of Proposition C.6 and the fact that $\phi(n) = 1$ if n is in $\mathrm{Ker}(\phi)$. It follows that $a^{-1}na$ is in $\mathrm{Ker}(\phi)$ by definition, and so $\mathrm{Ker}(\phi)$ is normal in G_1. □

THEOREM C.8 (Fundamental Homomorphism Theorem). *Let $\phi : G_1 \to G_2$ be a homomorphism and let $K = \mathrm{Ker}(\phi)$. Then $\psi : G_1/K \to \mathrm{Im}(\phi)$ defined by $\psi(aK) = \phi(a)$ is an isomorphism.*

PROOF. We need to show that ψ is a well-defined bijective (that is, both injective and surjective) homomorphism.

(1) *ψ is well-defined:* Suppose that $aK = bK$, so that $a^{-1}b$ is an element of K. Then $1 = \phi(a^{-1}b) = \phi(a)^{-1}\phi(b)$, so that $\phi(a) = \phi(b)$, that is, $\psi(aK) = \psi(bK)$.

(2) *ψ is a homomorphism:* If aK and bK are elements of G_1/K, then

$$\psi(aK \cdot bK) = \psi((ab)K) = \phi(ab) = \phi(a) \cdot \phi(b) = \psi(aK) \cdot \psi(bK),$$

using the fact that ϕ is a homomorphism.

(3) *ψ is injective:* Suppose that $\psi(aK) = \psi(bK)$, so that $\phi(a) = \phi(b)$. Then $1 = \phi(a)^{-1}\phi(a) = \phi(a)^{-1}\phi(b) = \phi(a^{-1}b)$. It follows that $a^{-1}b$ is an element of K, and so $aK = bK$.

(4) *ψ is surjective:* If c is an element of $\mathrm{Im}(\phi)$, then by definition $c = \phi(a)$ for some a in G_1. But then $c = \psi(aK)$, so that c is in the image of ψ. □

Exercises on Groups.

1. Let a, b, and c be elements of a group G. Show that if $ab = ac$, then $b = c$.
2. Show that the identity element of a group must be unique. (Hint: If e and f are identity elements for G, then $ae = a = af$ for all a in G. Use the preceding exercise.)
3. Show that each element a of a group G has a unique inverse in G. (Hint: Assume that b and c are both inverses of a, and use Exercise 1 again.)
4. Show that $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$ for any pair of elements a and b in a group G, so that $(ab)^{-1} = b^{-1}a^{-1}$.
5. If N is a subgroup of a group G, show that the relation of congruence modulo N is an equivalence relation on G. That is, show that $a \equiv a \pmod N$ for all a in G; that if $a \equiv b \pmod N$, then $b \equiv a \pmod N$ is also true; and that if $a \equiv b \pmod N$ and $b \equiv c \pmod N$, then $a \equiv c \pmod N$.
6. Let N be a normal subgroup of a group G. Show that the set G/N is a group under the operation $[a] \cdot [b] = [ab]$.
7. Let $\phi : G_1 \to G_2$ be a homomorphism. Show that $\phi(a^{-1}) = \phi(a)^{-1}$ for every a in G_1.
8. Let $\phi : G_1 \to G_2$ be a homomorphism and let H_1 be a subgroup of G_1. Show that $\phi(H_1) = \{\phi(a) \mid a \in H_1\}$ is a subgroup of G_2.

Finite Abelian Groups

In this section, we restrict our attention to abelian groups of finite order. We will use factor groups to establish a classification of the structure of such groups. We first introduce the following definition.

DEFINITION. Let G be a finite abelian group. We say that a subset $\{a_1, a_2, \ldots, a_k\}$ of G is a *basis* for G of *type* $(n_1, n_2, \ldots, n_k)$ if each a_i has order n_i in G, and if every element of G can be written uniquely as $a_1^{r_1}a_2^{r_2}\cdots a_k^{r_k}$ with $0 \le r_i < n_i$ for $i = 1, 2, \ldots, k$.

Note that if G has a basis of type $(n_1, n_2, \ldots, n_k)$, then $|G| = n_1 n_2 \cdots n_k$.

EXAMPLE. Let $G = \mathbb{Z}_{13}^{\times}$. Then $\{2\}$ is a basis for G of type (12), since the powers of 2,

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1,$$

include all elements of G exactly once. A basis for G is typically not unique—for example, one can verify that $\{6\}$ is also a basis for $G = \mathbb{Z}_{13}^{\times}$ of type (12). In fact, a group might have bases of different types. We leave it to the reader to verify that the set $\{3, 5\}$ is a basis for $\mathbb{Z}_{13}^{\times}$ of type $(3, 4)$, that is, every element can be written uniquely as $3^r \cdot 5^s$ with $0 \le r < 3$ and $0 \le s < 4$. ◊

We will show that a finite abelian group G always has a basis, and that the type of the basis is unique under the following restriction.

DEFINITION. Suppose that $\{a_1, a_2, \ldots, a_k\}$ is a basis of type $(n_1, n_2, \ldots, n_k)$ for some abelian group G. We say that this basis has *descending divisor* type if n_{i+1} divides n_i for $i = 1, \ldots, k-1$ and if $n_k > 1$ when $k > 1$.

We need several preliminary results to prove the existence and uniqueness of this basis type.

LEMMA C.9. *Let a and b be elements of a finite abelian group G, and suppose that* $\text{ord}(a) = q$ *and* $\text{ord}(b) = r$ *are relatively prime. Then* $\text{ord}(ab) = qr$.

PROOF. Let $\text{ord}(ab) = s$. Since G is abelian, then $(ab)^{qr} = (a^q)^r \cdot (b^r)^q = 1^r \cdot 1^q = 1$, so that s divides qr. On the other hand, $1 = ((ab)^s)^r = a^{rs} \cdot (b^r)^s = a^{rs}$, implying that q divides rs. Since $\gcd(q, r) = 1$, it follows that q divides s. Similarly, $1 = ((ab)^s)^q = (a^q)^s \cdot b^{qs} = b^{qs}$, implying that r divides qs, and then r divides s. Now s is a common multiple of q and r, and since $\gcd(q, r) = 1$, it follows that qr divides s. Therefore $s = qr$. □

LEMMA C.10. *Let a and b be elements of a finite abelian group G with* $\text{ord}(a) = s$ *and* $\text{ord}(b) = t$. *Then there is an element of G whose order is* $\text{lcm}(s, t)$, *the least common multiple of s and t.*

PROOF. For a prime number p, recall that $e_p(n)$ is the largest nonnegative integer e so that p^e divides n. We can define integers q and r by saying that

$$e_p(q) = \begin{cases} e_p(s), & \text{if } e_p(s) \geq e_p(t) \\ 0, & \text{if } e_p(s) < e_p(t) \end{cases} \quad \text{and} \quad e_p(r) = \begin{cases} 0, & \text{if } e_p(s) \geq e_p(t) \\ e_p(t), & \text{if } e_p(s) < e_p(t) \end{cases}$$

for every prime p. Then the following statements are true.

(1) q divides s and r divides t, since $e_p(q) \leq e_p(s)$ and $e_p(r) \leq e_p(t)$ for every prime p.
(2) q and r are relatively prime, since either $e_p(q) = 0$ or $e_p(r) = 0$ for every prime p.
(3) $qr = \text{lcm}(s, t)$, since $e_p(q) + e_p(r)$ is the larger of $e_p(s)$ and $e_p(t)$ for every prime p.

Now we find that $\text{ord}(a^{s/q}) = q$ and $\text{ord}(b^{t/r}) = r$. Since $\gcd(q, r) = 1$, Lemma C.9 implies that $a^{s/q} \cdot b^{t/r}$ is an element of G of order $qr = \text{lcm}(s, t)$. □

LEMMA C.11. *Let G be a finite abelian group. Suppose that t is the largest order of an element of G. If a is an element of G, then* $\text{ord}(a)$ *divides t. Thus $a^t = 1$ for every a in G.*

PROOF. Let a be an element of G and suppose that $\text{ord}(a) = s$. By Lemma C.10, G contains an element of order $\text{lcm}(s, t)$. Since $\text{lcm}(s, t) \geq t$, we must conclude that $\text{lcm}(s, t) = t$ to avoid contradicting the definition of t. But then s divides t by definition. The final claim is then a consequence of Proposition C.2. □

LEMMA C.12. *Let G be a finite abelian group, with t the largest order of an element of G. Let a be an element for which* $\text{ord}(a) = t$, *and let $N = \langle a \rangle$, the cyclic subgroup of G generated by a. Let b be an element of G, and suppose that $[b]$ has order s as an element of the factor group G/N. Then s divides t, and $[b]$ contains an element whose order in G is s.*

By definition, the order of $[b]$ in G/N is the smallest positive integer s such that $[b]^s = [b^s] = [1] = 1 \cdot N = N$. We can also say that the order of $[b]$ in G/N is the smallest positive integer s such that $b^s \in N$.

PROOF. Let n be the order of b in G. Note that $[b]^n = [b^n] = [1]$ in G/N, so it follows that s divides n. Likewise, s divides $\text{ord}(c)$ for any element c in $[b]$. By Lemma C.11, we know that n divides t, so then s divides t, say that $t = sq$ for some integer q. Now $[1] = [b]^s = [b^s]$ implies that b^s is an element of $N = \langle a \rangle$, that is, $b^s = a^m$ for some integer m. Notice that $1 = b^t = (b^s)^q = (a^m)^q = a^{mq}$, implying that $\text{ord}(a) = t$ divides mq. So now $mq = tr = sqr$, or $m = sr$, for some integer r. But then $b^s = a^m = (a^r)^s$, so that $(ba^{-r})^s = 1$ in G. Since $a^{-r} \in N$,

then $c = ba^{-r}$ is an element of $[b]$ whose order divides s. But s divides $\text{ord}(c)$ as noted above, and so $\text{ord}(c) = s$. □

Lemma C.12 implies that if $N = \langle a \rangle$ for some element a of maximal order in a finite abelian group G, then we can select a representative b from each equivalence class in G/N so that b has the same order in G as $[b]$ has in G/N. This is not generally true for all subgroups of G. For example, let $G = \mathbb{Z}_5^\times = \{1, 2, 3, 4\}$, and let $N = \langle 4 \rangle = \{1, 4\}$. We can write $G/N = \{[1], [2]\}$, and $[2]$ has order two in G/N since $[2]^2 = [4] = [1]$. But both potential representatives of $[2]$, namely 2 and 3, have order four in G.

The Fundamental Theorem of Finite Abelian Groups. We can now state and prove our main results on the structure of finite abelian groups.

THEOREM C.13. *If G is a finite abelian group, then G has a basis of descending divisor type.*

PROOF. We proceed by induction on $|G|$. If $|G| = 1$, then $\{1\}$ is a basis for G with descending divisor type (1). So assume that G is a nontrivial finite abelian group, and that every abelian group with fewer than $|G|$ elements has a basis of descending divisor type.

Let a be an element having maximal order t in G. Then $N = \langle a \rangle$ is a nontrivial subgroup of G, so that G/N is an abelian group with $|G/N| < |G|$. By the inductive hypothesis, G/N has a basis $\{[a_1], [a_2], \ldots, [a_k]\}$ of descending divisor type $(n_1, n_2, \ldots, n_k)$. Lemma C.12 implies that each n_i divides t. Furthermore, we can assume by the same lemma that each class representative a_i has order n_i in G. We now show that $\{a, a_1, a_2, \ldots, a_k\}$ is a basis for G.

If b is an element of G, we can write $[b]$ as $[a_1]^{r_1} \cdot [a_2]^{r_2} \cdots [a_k]^{r_k} = [a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k}]$, using the definition of the operation in G/N. Since $N = \langle a \rangle$, it follows that there is an integer r such that $b = a^r a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k}$. If $b = a^s a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}$ also, then we find that

$$[b] = [a_1]^{r_1} \cdot [a_2]^{r_2} \cdots [a_k]^{r_k} = [a_1]^{s_1} \cdot [a_2]^{s_2} \cdots [a_k]^{s_k},$$

implying, since $\{[a_1], [a_2], \ldots, [a_k]\}$ is a basis for G/N, that $r_i \equiv s_i \pmod{n_i}$ for $i = 1, \ldots, k$. Since a_i has order n_i in G, it follows that $a^r = a^s$ by cancellation in G, and so $r \equiv s \pmod{t}$. So $\{a, a_1, a_2, \ldots, a_k\}$ is a basis for G of descending divisor type $(t, n_1, n_2, \ldots, n_k)$ (or descending divisor type (t) if $n_1 = 1$). The result follows for all finite abelian groups G by induction. □

We will establish the uniqueness of the descending divisor type of a finite abelian group after the following lemma.

LEMMA C.14. *Let G be an abelian group with a basis $\{a_1, a_2, \ldots, a_k\}$ of type $(n_1, n_2, \ldots, n_k)$. Then for every positive integer t, the number of elements x in G for which $x^t = 1$ is*

$$\gcd(n_1, t) \cdot \gcd(n_2, t) \cdots \gcd(n_k, t).$$

PROOF. Note that $(a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k})^t = a_1^{tr_1} a_2^{tr_2} \cdots a_k^{tr_k}$ in an abelian group. This product equals the identity element 1 if and only if $tr_i \equiv 0 \pmod{n_i}$ for $i = 1, \ldots, k$. Corollary B.4 shows that if n_i divides tr_i, then $\frac{n_i}{\gcd(n_i, t)}$ divides r_i. There are precisely $\gcd(n_i, t)$ values of r_i with $0 \le r_i < n_i$ for which this is true. The conclusion follows by the multiplicative counting principle. □

THEOREM C.15. *Let G be a finite abelian group, with two bases having descending divisor types $(n_1, n_2, \ldots, n_k)$ and $(m_1, m_2, \ldots, m_\ell)$ respectively. Then $k = \ell$ and $n_i = m_i$ for $i = 1, \ldots, k$.*

PROOF. If $|G| = n$, we have $n_1 \cdot n_2 \cdots n_k = n = m_1 \cdot m_2 \cdots m_\ell$. Letting $t = n_1$, and applying Lemma C.14 to each basis, we have that

$$\gcd(n_1, n_1) \cdots \gcd(n_k, n_1) = \gcd(m_1, n_1) \cdots \gcd(m_\ell, n_1),$$

which implies, since $(n_1, n_2, \ldots, n_k)$ has descending divisor type, that

$$n = n_1 \cdots n_k = \gcd(m_1, n_1) \cdots \gcd(m_\ell, n_1).$$

But $\gcd(m_i, n_1) \leq m_i$ for $1 \leq i \leq \ell$, so we must conclude that $\gcd(m_1, n_1) = m_1$, that is, m_1 divides n_1. The same argument, using $t = m_1$, shows that n_1 divides m_1. So $m_1 = n_1$. Repeating this process with $t = n_2$ and $t = m_2$ then shows that those two values must be equal. Continuing in this way, we conclude that the two basis types must be identical. □

If a finite abelian group G has a basis of descending divisor type $(n_1, n_2, \ldots, n_k)$, we also say that $(n_1, n_2, \ldots, n_k)$ are the *invariant factors* of G. Theorems C.13 and C.15 show that every finite abelian group has a unique collection of invariant factors. (It generally has more than one basis of that type, however.) This result is referred to as the *Fundamental Theorem of Finite Abelian Groups*. The following example illustrates how we might determine the invariant factors of a finite abelian group in practice.

EXAMPLE. Suppose that G is an abelian group with 32 elements. In this case, Theorem C.13 implies that G has a basis of type $(2^{e_1}, 2^{e_2}, \ldots, 2^{e_k})$ where $e_1 \geq e_2 \geq \cdots \geq e_k \geq 1$ and $32 = 2^{e_1} \cdot 2^{e_2} \cdots 2^{e_k}$. The number of distinct possibilities is the same as the number of ways of writing $5 = e_1 + e_2 + \cdots + e_k$, with $e_1 \geq e_2 \geq \cdots \geq e_k \geq 1$. We find that there are seven possibilities,

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1,$$

corresponding to the following potential collections of invariant factors of G:

$$(32), \qquad (16,2), \qquad (8,4), \qquad (8,2,2), \qquad (4,4,2), \qquad (4,2,2,2), \qquad (2,2,2,2,2).$$

We can use Lemma C.14 to determine which of these seven possibilities is actually true for a given group G. Applying Lemma C.14 with $t = 2$, we find that if G has invariant factors $(2^{e_1}, 2^{e_2}, \ldots, 2^{e_k})$, then the number of elements x in G with $x^2 = 1$ is 2^k. For instance, if $x^2 = 1$ has 16 solutions in G, then $k = 4$, and the only possible invariant factor collection for G is $(4, 2, 2, 2)$. If $x^2 = 1$ has $2^3 = 8$ solutions, then G has invariant factor type either $(8, 2, 2)$ or $(4, 4, 2)$. Since the first calculation is inconclusive in this case, we may apply Lemma C.14 again with $t = 4$. If G has invariant factor type $(8, 2, 2)$, then $x^4 = 1$ has $\gcd(8, 4) \cdot \gcd(2, 4) \cdot \gcd(2, 4) = 4 \cdot 2 \cdot 2 = 16$ solutions, while if G has invariant factor type $(4, 4, 2)$, we find that all 32 elements of G satisfy $x^4 = 1$. The following table summarizes the number of solutions of $x^t = 1$ for $t = 2$ and $t = 4$, and shows that each invariant factor type is determined by looking at these two cases.

t	(32)	$(16,2)$	$(8,4)$	$(8,2,2)$	$(4,4,2)$	$(4,2,2,2)$	$(2,2,2,2,2)$
2	2	4	4	8	8	16	32
4	4	8	16	16	32	32	32

◊

EXAMPLE. If G is an abelian group with $200 = 2^3 \cdot 5^2$ elements, possible invariant factor forms are obtained by combining all such forms for $2^3 = 8$ (namely, (8), $(4, 2)$, and $(2, 2, 2)$) and for $5^2 = 25$ (which are (25) and $(5, 5)$). If in each case we match up the highest powers of 2 and 5, and then the next highest powers, and so forth, we obtain six possibilities, each in descending divisor form. These possibilities are listed in the following table, along with the number of solutions in each corresponding group of $x^t = 1$ for $t = 2$ and $t = 5$. Those two calculations are sufficient to determine the invariant factors of an abelian group with 200 elements.

t	(200)	$(100,2)$	$(50,2,2)$	$(40,5)$	$(20,10)$	$(10,10,2)$
2	2	4	8	2	4	8
5	5	5	5	25	25	25

◊

Exercises on Finite Abelian Groups.

1. For each of the following subsets S of $G = \mathbb{Z}_{19}^{\times}$, indicate whether or not S is a basis for G. If so, what is its type?
   (a) $S = \{2\}$.
   (b) $S = \{4, 18\}$.
   (c) $S = \{7, 8\}$.
2. For each of the following values of n, find all invariant factor types of abelian groups having n elements.
   (a) $n = 16$.
   (b) $n = 24$.
   (c) $n = 36$.
   (d) $n = 60$.
3. Find the invariant factor type of $G = \mathbb{Z}_{17}^{\times}$.
4. Find the invariant factor type of $G = \mathbb{Z}_{40}^{\times}$. (Note: $|G| = 16$.)
5. Find the invariant factor type of $G = \mathbb{Z}_{35}^{\times}$. (Note: $|G| = 24$.)

Rings

Our next definition introduces terminology for various algebraic systems on which two interrelated operations are defined.

DEFINITION. Let R be a set on which operations of *addition* and *multiplication* are defined. That is, for every $a, b \in R$, there is an element $a + b$ in R and an element $a \cdot b = ab$ in R. We say that R is a *ring* under these operations if

(1) R is an abelian group under addition,
(2) the multiplication operation is associative, and
(3) multiplication is *distributive* over addition, that is, for all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

We denote the identity element of R under addition as 0, and call it the *zero element* of R. For all $a \in R$, we denote the inverse of a under addition as $-a$, and call it the *negative* of a in R. We abbreviate an element $a + (-b)$ as $a - b$, thus defining a subtraction operation on R. If the multiplication operation of R is commutative, we call R a *commutative ring*. If R has an identity element under multiplication, we typically denote that element as 1, and we say that R is a *ring with unity*.

Certain other properties of a ring follow from those listed in this definition.

PROPOSITION C.16. *Let R be a ring with zero element 0. Let a be an element of R and let $-a$ be its negative. Then for every $b \in R$,*

(1) $0 \cdot b = 0 = b \cdot 0$.
(2) $-a \cdot b = -ab$ *and* $b \cdot (-a) = -ba$.

PROOF. Let b be an element of R.

(1) We can write $0 \cdot b = 0 \cdot b + 0$ since $0 \cdot b$ is an element of R and 0 is the identity element under addition. But on the other hand, $0 \cdot b = (0 + 0) \cdot b = 0 \cdot b + 0 \cdot b$, using the identity property of 0 and the distributive property. Now $0 \cdot b + 0 = 0 \cdot b + 0 \cdot b$ implies that $0 \cdot b = 0$ by Proposition C.1, part (1). The proof that $b \cdot 0 = 0$ is similar.

(2) Notice that $-a \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$, using the distributive property, the inverse property of $-a$ under addition, and part (1). But by definition, $-ab$ is the element of R

such that $ab + (-ab) = 0$. This element is unique by Proposition C.1, part (3), so we conclude that $-a \cdot b = -ab$. The proof that $b \cdot (-a) = -ba$ is similar. □

The following special cases are particularly important types of rings.

DEFINITION. Let R be a commutative ring with unity element $1 \neq 0$. We call R an *integral domain* if it has the following *zero divisor* property: For all $a, b \in R$, if $ab = 0$, then either $a = 0$ or $b = 0$ in R. We call R a *field* if every *nonzero* element of R has an inverse under multiplication. That is, for every $a \in R$, if $a \neq 0$, then there is an a^{-1} in R such that $aa^{-1} = 1$.

Note that the set $R = \{0\}$ is a ring if $0 + 0 = 0$ and $0 \cdot 0 = 0$. In this case, 0 serves as a unity element for R. The condition that $1 \neq 0$ in the preceding definition rules out this *trivial* ring from being an integral domain or field. We leave it as an exercise to show that every field is an integral domain.

EXAMPLE. For every positive integer m, the set $\mathbb{Z}_m$ of equivalence classes under congruence modulo m is a commutative ring with unity under the operations of modular addition and multiplication. If m is prime, then $\mathbb{Z}_m$ is a field, an application of Theorem B.16. If m is composite, then $\mathbb{Z}_m$ is not an integral domain, since if $m = ab$ for integers $1 < a, b < m$, then a and b are nonzero elements of $\mathbb{Z}_m$ for which $ab = 0$ in $\mathbb{Z}_m$. If $m = 1$, then $\mathbb{Z}_m = \{0\}$ is not an integral domain or field, as noted above. ◊

Let R be a ring with unity element 1. We say that an element a in R is a *unit* if a has an inverse under multiplication in the ring R. In this situation, the inverse of a is unique, since if $ab = 1 = ba$ and $ac = 1 = ca$ for elements b and c in R, then $b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$. We denote the inverse of a unit a as a^{-1}.

PROPOSITION C.17. *Let R be a ring with unity. Denote by $R^\times$ the set of all units in R. Then $R^\times$ is a group under the operation of multiplication in R.*

PROOF. We first show that $R^\times$ is closed under multiplication. Suppose that a and b are units in R, say with inverses a^{-1} and b^{-1} respectively. Then we see that ab is a unit in R. Consider the element $b^{-1}a^{-1}$. We have that $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$, using associativity of multiplication in R and the definition of the unity element. In a similar way, $(b^{-1}a^{-1})(ab) = 1$.

Now multiplication is associative in $R^\times$ since that is true in R. The unity element of R is in $R^\times$ since $1 \cdot 1 = 1$, and is the identity element for $R^\times$. If a is in $R^\times$, then so is a^{-1}, since $a^{-1} \cdot a = 1 = a \cdot a^{-1}$. Thus $R^\times$ is a group under multiplication. □

In a ring with unity, if $ab = ac$ or $ba = ca$ with a a unit, then $b = c$. In an integral domain, we can make the following stronger statement.

PROPOSITION C.18. *Let R be an integral domain. Let a, b, and c be elements of R. If $ab = ac$ and $a \neq 0$ in R, then $b = c$.*

PROOF. Suppose that $ab = ac$ in R with $a \neq 0$. Then $ab + (-ac) = ac + (-ac) = 0$ by the definition of $-ac$. By part (2) of Proposition C.16 and the distributive property, we have that $ab + (-ac) = ab + a(-c) = a(b + (-c))$ But since R is an integral domain, with $a(b + (-c)) = 0$ and $a \neq 0$, we conclude that $b + (-c) = 0$. Adding c to both sides of this equation, we see that $b = c$. □

In a typical integral domain, not every nonzero element is a unit. For instance, the only units in $\mathbb{Z}$ are 1 and -1. However, for finite sets we have the following result.

PROPOSITION C.19. *A finite integral domain is a field.*

PROOF. Let R be an integral domain with n elements. We need to show that every nonzero element of R has an inverse under multiplication, that is, that all nonzero elements are units in R. Write $R = \{a_1, a_2, \ldots, a_n\}$, and let a be a nonzero element of R. Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. We know that $S \subseteq R$ by closure, but that S has n distinct elements, since if $aa_i = aa_j$ then $a_i = a_j$ by Proposition C.18. But then $S = R$. Since R contains a unity element 1, then 1 must be an element of S. That is, $1 = aa_i$ for some i, so that $a_i = a^{-1}$ by definition. Thus every nonzero element of R has an inverse in R. □

Subrings and Ring Homomorphisms. We can carry over certain definitions introduced for groups to rings as follows.

DEFINITION. Let R be a ring and let S be a subset of R. We say that S is a *subring* of R if S is a ring under the same definitions of addition and multiplication as in R.

The following proposition indicates how we can test whether a subset of a ring is a subring. We leave the proof of this proposition as Exercises 4–6.

PROPOSITION C.20. *Let S be a subset of a ring R. Then S is a subring of R if the following are true.*

(1) *0 is an element of S.*
(2) *For every a in S, the element $-a$ (as defined in R) is also in S.*
(3) *For every a and b in S, the sum $a + b$ is in S.*
(4) *For every a and b in S, the product ab is in S.*

If R is an integral domain, and S is a subring of R, then S is also an integral domain if and only if S contains 1, the unity element of R. If R is a field, and S is a subring of R, then S is also a field if 1 is in S, and for every $a \neq 0$ in S, the inverse of a (as defined in R) is also in S.

The definition of homomorphisms and isomorphisms can likewise be carried over to rings.

DEFINITION. Let R_1 and R_2 be rings. A function $\phi : R_1 \to R_2$ is called a *(ring) homomorphism* if $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a) \cdot \phi(b)$ for every pair of elements a and b in R_1. We say that a homomorphism $\phi : R_1 \to R_2$ is an *isomorphism* if ϕ is bijective. If there is some isomorphism from R_1 to R_2, we say that R_1 is *isomorphic* to R_2.

Note that a ring homomorphism is also a homomorphism between the groups R_1 and R_2 under addition. So properties of group homomorphisms apply to this definition. For example, if $\phi : R_1 \to R_2$ is a homomorphism, then $\phi(0) = 0$ and $\phi(-a) = -\phi(a)$ for all a in R_1. (Here we use parts (1) and (2) of Proposition C.6.)

DEFINITION. Let $\phi : R_1 \to R_2$ be a ring homomorphism. Then we define the *kernel* of ϕ to be $\text{Ker}(\phi) = \{a \in R_1 \mid \phi(a) = 0\}$. We define the *image* of ϕ to be $\text{Im}(\phi) = \{\phi(a) \mid a \text{ is in } R_1\}$.

PROPOSITION C.21. *If $\phi : R_1 \to R_2$ is a ring homomorphism, then* $\text{Ker}(\phi)$ *is a subring of R_1 and* $\text{Im}(\phi)$ *is a subring of R_2.*

PROOF. Exercise 7. □

Exercises on Rings.

1. Show that every field is an integral domain.
2. Let $R = M_2(\mathbb{R})$ be the set of all 2×2 matrices with real number entries. Show that R is a ring under matrix addition and multiplication. Is R an integral domain?
3. Let $R = \mathcal{F}(\mathbb{R})$ be the set of all functions $f : \mathbb{R} \to \mathbb{R}$. Show that R is a ring under function addition and multiplication. Is R an integral domain?

4. Let R be a ring and let S be a subset of R. Show that S is subring of R if S contains 0, S contains the negative of each element of S, and S is closed under addition and multiplication.
5. Let R be an integral domain and let S be a subring of R. Show that S is also an integral domain if S contains 1, the unity element of R.
6. Let R be a field and let S be a subring of R. Show that S is also a field if S contains 1, and S contains the inverse of every nonzero element of S.
7. Let $\phi : R_1 \to R_2$ be a ring homomorphism. Show that $\text{Ker}(\phi)$ is a subring of R_1 and $\text{Im}(\phi)$ is a subring of R_2.

Ideals of Integral Domains

The following proves to be a key definition in considering properties of divisibility in integral domains.

DEFINITION. A nonempty subset A of an integral domain D is called an *ideal* of D if A has the following properties.

(1) If a and b are in A, then $a + b$ is in A.
(2) If $a \in A$, then $-a \in A$.
(3) If $a \in A$ and $r \in D$, then $ar \in A$.

Conditions (1) and (2) can be combined by saying that A is closed under subtraction, that is, if a and b are elements of A, then $a - b$ is also in A. An ideal A always contains $0 = a - a$, since A is nonempty. Condition (3) implies that A is closed under multiplication, so that A is a subring of D. An ideal A of D is typically not an integral domain however, since A is not required to contain the unity element of D. In fact, if A is an ideal of D and A contains 1, then A contains $1 \cdot r = r$ for all r in D, that is, A is the same as D.

PROPOSITION C.22. *Let a and b be elements of an integral domain D. Then the following statements are true.*

(1) *The set $\langle a \rangle = \{ax \mid x \in D\}$ of multiples of a is an ideal of D. If A is an ideal of D and a is an element of A, then $\langle a \rangle$ is a subset of A.*
(2) *The set $\langle a, b \rangle = \{ax + by \mid x, y \in D\}$ of combinations of a and b is an ideal of D. If A is an ideal of D and a and b are elements of A, then $\langle a, b \rangle$ is a subset of A.*

PROOF. Note that $\langle a \rangle = \langle a, 0 \rangle$ for every a in D, so it will suffice to prove statement (2). Let a and b be elements of D. Then $0 = a(0) + b(0)$ is in $\langle a, b \rangle$, so that $\langle a, b \rangle$ is nonempty. If x, y, x', and y' are elements of D, so that $ax + by$ and $ax' + by'$ are in $\langle a, b \rangle$, we find that $(ax + by) - (ax' + by') = a(x - x') + b(y - y')$ is in $\langle a, b \rangle$ also, so that $\langle a, b \rangle$ is closed under subtraction. If r is an element of D, then $(ax + by)r = a(xr) + b(yr)$ is in $\langle a, b \rangle$. So $\langle a, b \rangle$ is an ideal of D. Now let A be some ideal of D and suppose that $a, b \in A$. Then for any x and y in D, we see that ax and by are in A by the multiplicative property of ideals, and then $ax + by \in A$ by closure of an ideal under addition. So $\langle a, b \rangle$ is a subset of A. □

DEFINITION. We say that an ideal A is a *principal ideal* of D if $A = \langle a \rangle$ for some a in D. Notice that $\langle 0 \rangle = \{0\}$ and $\langle 1 \rangle = D$ are principal ideals of every integral domain D. If A is an ideal of D, we say that A is *nontrivial* if $A \neq \{0\}$, and that A is *proper* if $A \neq D$.

EXAMPLE. Let $A = \langle 6, 15 \rangle$ in $\mathbb{Z}$. We can show that A is equal to a principal ideal, namely that $A = \langle 3 \rangle$. Since $6 = 3(2)$ and $15 = 3(5)$, then 6 and 15 are elements of $\langle 3 \rangle$, so that $\langle 6, 15 \rangle \subseteq \langle 3 \rangle$ by Proposition C.22. Conversely, note that $3 = 6(3) + 15(-1)$ is an element of $\langle 6, 15 \rangle$, and so $\langle 3 \rangle \subseteq \langle 6, 15 \rangle$, again by Proposition C.22. ◊

Operations on Ideals. Ideals of an integral domain can be combined in various ways to produce other examples of ideals.

DEFINITION. Let A and B be ideals of an integral domain D.

(1) The *intersection* of A and B is $A \cap B = \{c \in D \mid c \in A \text{ and } c \in B\}$.
(2) The *sum* of A and B is $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

PROPOSITION C.23. *Let A and B be ideals of an integral domain D. Then*

(1) *$A \cap B$ is an ideal of D, and if C is an ideal of D with $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$.*
(2) *$A + B$ is an ideal of D, and if C is an ideal of D with $A \subseteq C$ and $B \subseteq C$, then $A + B \subseteq C$.*

PROOF. We leave the proof of (1) as Exercise 2. The set $A+B$ contains $0+0 = 0$, so is nonempty. If $a_1 + b_1$ and $a_2 + b_2$ are elements of $A + B$, then $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$ is in $A + B$, since A and B are closed under subtraction. If $a + b$ is in $A + B$ and r is in D, then $(a + b)r = ar + br$ is in $A + B$, since A and B both have the multiplicative property of ideals. Finally, if $A \subseteq C$ and $B \subseteq C$ for some ideal C of D, and $a \in A$ and $b \in B$, then $a + b$ is an element of C by the closure of an ideal under addition. Therefore, $A + B$ is a subset of C. □

EXAMPLE. In $\mathbb{Z}$, let $A = \langle 6 \rangle$ and $B = \langle 15 \rangle$. We can show as follows that $A \cap B = \langle 30 \rangle$. Since $30 = 6(5)$ and $30 = 15(2)$, we see that $30 \in A \cap B$, and so $\langle 30 \rangle \subseteq A \cap B$. Conversely, suppose that $x \in A \cap B$, so that $x = 6q$ and $x = 15r$ for some integers q and r. It follows that $2q = 5r$, so that $r = 2t$ is even. But now $x = 30t$ is an element of $\langle 30 \rangle$, so we find that $A \cap B \subseteq \langle 30 \rangle$.

In a similar way, $A + B = \langle 3 \rangle$. First note that $3 = 6(3) + 15(-1)$ is an element of $A + B$, so that $\langle 3 \rangle \subseteq A + B$. Conversely, the typical element of $A + B$ has the form $x = 6q + 15r$ for some integers q and r. But then $x = 3(2q + 5r)$ is an element of $\langle 3 \rangle$, and so $A + B \subseteq \langle 3 \rangle$. ◊

Note that if a and b are elements of D, it is not generally the case that $\langle a \rangle + \langle b \rangle = \langle a + b \rangle$. In fact, one can show that $\langle a \rangle + \langle b \rangle = \langle a, b \rangle$, so that a sum of principal ideals is not necessarily a principal ideal.

We can also multiply ideals. We first make the following more general definition.

DEFINITION. Let A be an ideal of an integral domain D, and let S be a nonempty subset of D. Then we define the *product* of A and S to be the set of all finite sums of products of elements of A with elements of S, that is, $AS = \{a_1 s_1 + a_2 s_2 + \cdots + a_n s_n \mid a_i \in A \text{ and } s_i \in S \text{ for } 1 \leq i \leq n\}$.

PROPOSITION C.24. *Let A be an ideal and S a nonempty subset of an integral domain D. Then AS is an ideal of D, and is contained in A.*

PROOF. First note that each product $a_i s_i$ is in A, since A is an ideal of D, and so the typical finite sum of such products is also in A. So AS is a subset of A. The set AS contains $0 \cdot s = 0$, so is nonempty. The sum of two finite sums of products is likewise a finite sum of products, so AS is closed under addition. If $c = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n$ is in AS, then $-c = (-a_1)s_1 + (-a_2)s_2 + \cdots + (-a_n)s_n$ is in AS, since each $-a_i$ is in A. Finally, if $r \in D$, then $cr = (a_1 r)s_1 + (a_2 r)s_2 + \cdots + (a_n r)s_n$ is in AS, since each $a_i r \in A$. So AS is an ideal of D. □

It is necessary to allow *sums* of products of elements of A and S in AS, rather than just products themselves, in order for AS to be closed under addition and subtraction. Note however that if $S = \{s\}$, then the typical element of AS is

$$a_1 s + a_2 s + \cdots + a_n s = (a_1 + a_2 + \cdots + a_n)s = as,$$

where a is an arbitrary element of A. In this case, we also write AS as sA. More generally, if $S = \{s_1, s_2, \ldots, s_n\}$ if finite, then $AS = s_1 A + s_2 A + \cdots + s_n A$.

If $S = B$ is also an ideal of D, then AB is an ideal contained in $A \cap B$. So multiplication is an operation on the collection of all ideals of D. Note that $AB = \{0\}$ if and only if either $A = \{0\}$ or $B = \{0\}$. The following properties are left as exercises.

(1) Ideal multiplication is commutative: $AB = BA$ for all ideals A, B of D.
(2) Ideal multiplication is associative: $(AB)C = A(BC)$ for all ideals A, B, C of D.
(3) The *improper* ideal D is an identity element: $AD = A$ for all ideals A of D.
(4) If $B = \langle b \rangle$ is a principal ideal, then $AB = bA$.
(5) If $A = \langle a \rangle$ and $B = \langle b \rangle$ are both principal ideals, then $AB = \langle ab \rangle$.

If A and B are ideals of an integral domain D, we will say that B divides A if there is an ideal C of D for which $A = BC$. Note that if B divides A, then A must be a subset of B, since BC is always a subset of B. The following is a partial converse of this statement—if A is contained in a *principal* ideal B, then B divides A.

PROPOSITION C.25. *Let A be an ideal of an integral domain D, and let r be an element of D. If $A \subseteq \langle r \rangle$, then there is an ideal C of D for which $A = rC$.*

PROOF. Let A be an ideal of D contained is some principal ideal $\langle r \rangle$. If $r = 0$, then $\langle r \rangle = \{0\}$, so that $A = \{0\}$. In this case, we can write $A = rC$ for any ideal C of D. So suppose that $r \neq 0$. Now if a is in A, it follows that $a = rx$ for some $x \in D$, and so r divides a in D. Consider the set $C = \{x \in D \mid rx \text{ is an element of } A\}$, which is thus a nonempty subset of D. If x and y are in C, so that $rx = a_1$ and $ry = a_2$ are elements of A, then $x - y$ is in C, since $r(x-y) = rx - ry = a_1 - a_2$ is an element of A. Likewise, if x is in C, so that $rx = a$ is in A, and s is in D, then xs is in C, since $r(xs) = (rx)s = as$ is in A. Thus C is an ideal of D. If x is in C, then rx is in A by definition, and so rC is a subset of A. Conversely, if a is in A, then $a = rx$ for some x in D, as noted above. But then x is in C by definition, so that a is an element of rC. Thus $A \subseteq rC$, and we conclude that $A = rC$. □

Exercises on Ideals of Integral Domains.

1. Show that if D is a field, and A is an ideal of D, then either $A = \{0\}$ or $A = D$.
2. If A and B are ideals of D, show that $A \cap B$ is also an ideal of D.
3. If a and b are elements of D, show that $\langle a \rangle + \langle b \rangle = \langle a, b \rangle$.
4. If A is an ideal of D and $S = \{s, t\}$ is a subset of D, show that $AS = sA + tA$.
5. If A and B are ideals of D, show that $AB = \{0\}$ if and only if $A = \{0\}$ or $B = \{0\}$.
6. Let A, B, and C be ideals of D.
   (a) Show that $AB = BA$.
   (b) Show that $(AB)C = A(BC)$.
   (c) Show that $AD = A$.
7. If A is an ideal and $B = \langle b \rangle$ is a principal ideal of D, show that $AB = bA$.
8. If $A = \langle a \rangle$ and $B = \langle b \rangle$ are principal ideals of D, show that $AB = \langle ab \rangle$.
9. If A and B are ideals of an integral domain D, and there is an element $c \neq 0$ in D so that $cA = cB$, show that A must equal B.

Divisibility in Integral Domains

The following definitions generalize concepts of prime factorization from integers to arbitrary integral domains.

DEFINITION. Let D be an integral domain, and let a, b, and u be elements of D.

(1) We say that b *divides* a if there is an element c in D such that $a = bc$.
(2) We say that u is a *unit* in D if u divides 1.
(3) We say that a and b are *associates* in D if a divides b and b divides a.
(4) Let p be an element of D that is neither 0 nor a unit. We say that p is *irreducible* in D if whenever $p = ab$ for some $a, b \in D$, either a or b is a unit. We say that p is *prime* in D if whenever p divides a product ab of elements of D, either p divides a or p divides b.

The units in D are precisely the elements of D that have an inverse under multiplication, and we find that a and b are associates in D if and only if $b = au$ for some unit u in D (Exercise 1). Associate elements of D are interchangeable for questions about divisibility and multiplication in D. The terms *irreducible* and *prime* are not synonymous in all examples of integral domains, but we can make the following statement.

PROPOSITION C.26. *Let D be an integral domain. If p is a prime element in D, then p is irreducible in D.*

PROOF. Let p be a prime element of D, and suppose that $p = ab$ for some $a, b \in D$. Then p divides ab, since $ab = p \cdot 1$, so either p divides a or p divides b by the definition of prime. We can assume without loss of generality that p divides a, say that $a = pc$ for some c in D. But now $p = ab = (pc)b = p(cb)$, and since $p \neq 0$ it follows that $cb = 1$. So b is a unit by definition, and we conclude that p is irreducible in D. □

The definitions above can be rephrased in terms of principal ideals. We leave the claims of the following proposition as Exercises 6–10.

PROPOSITION C.27. *Let D be an integral domain.*

(1) *If a and b are elements of D, then b divides a if and only if $\langle a \rangle$ is a subset of $\langle b \rangle$.*
(2) *An element u of D is a unit if and only if $\langle u \rangle = D$.*
(3) *Elements a and b of D are associates if and only if $\langle a \rangle = \langle b \rangle$.*
(4) *An element p that is neither 0 nor a unit in D is prime if and only if $ab \in \langle p \rangle$ implies that either $a \in \langle p \rangle$ or $b \in \langle p \rangle$.*
(5) *An element p that is neither 0 nor a unit in D is irreducible if and only if whenever $\langle p \rangle \subseteq \langle q \rangle \subseteq D$, then either $\langle q \rangle = \langle p \rangle$ or $\langle q \rangle = D$.*

Irreducible Factorization in Integral Domains. In this subsection, we define three types of integral domains, each generalizing a property that holds in the domain of integers.

DEFINITION. Let $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, the set of nonnegative integers, and let D be an integral domain. A function $f : D \to \mathbb{N}$ is called a *Euclidean function* for D if it has the following properties:

(1) $f(a) = 0$ if and only if $a = 0$.
(2) $f(ab) = f(a) \cdot f(b)$ for all $a, b \in D$.
(3) For every a and b in D with $b \neq 0$, there are elements q and r in D, with $f(r) < f(b)$, such that $a = bq + r$.

We say that D is a *Euclidean domain* if it has a Euclidean function.

DEFINITION. An integral domain D is called a *principal ideal domain* if every ideal of D is a principal ideal.

DEFINITION. An integral domain D is called a *unique factorization domain* if every element of D that is neither zero nor a unit can be written in some way as a product of irreducible elements of D, and this factorization is unique up to order and unit multiples. In other words, if $a = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell$, with each p_i and q_j irreducible in D, then $k = \ell$ and we can renumber the subscripts in such a way so that q_i is an associate of p_i for $1 \leq i \leq k$.

THEOREM C.28. *Suppose that D is an integral domain with the property that every element of D that is neither zero nor a unit can be written in some way as a product of irreducible elements of D. Then D is a unique factorization domain if and only if every irreducible element of D is prime.*

PROOF. Suppose first that every irreducible element of D is prime, and that some element a of D can be written in two ways as a product of irreducible elements, say $a = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell$ with each p_i and q_j irreducible in D. We may assume that no p_i is an associate of any q_j, since otherwise that pair of elements could be canceled from this equation. But now p_1 divides the product $q_1 \cdot q_2 \cdots q_\ell$, and since p_1 is irreducible, and so prime by assumption, we can can conclude that p_1 divides at least one term q_j in this product, so that $q_j = p_1 b$ for some b in D. But with q_j irreducible, and p_1 not a unit by definition, we must conclude that b is a unit, and so q_j is an associate of p_1, contrary to assumption. So the two factorizations of a are identical, aside from the order of the terms and multiplication by units.

For the converse, suppose that D contains an irreducible element p that is not prime in D. By definition, that means that there is a pair of elements u and v in D so that p does not divide u and p does not divide v, but p divides uv, say with $uv = pw$ for some w in D. The elements u, v, and w cannot be zero or units in D under these assumptions. So u, v, and w can all be written in some way as a product of irreducible elements in D. No term in those products for u or v can be an associate of p, since otherwise p divides u or p divides v, contrary to assumption. But now we have uv written as a product of irreducibles with no associate of p included, while pw is a product of irreducibles including p. So the element uv has two essentially distinct irreducible factorizations, and D cannot be a unique factorization domain. □

We now show that a Euclidean domain is both a principal ideal domain and a unique factorization domain.

THEOREM C.29. *Every Euclidean domain is a principal ideal domain.*

PROOF. Let D be a Euclidean domain, with f an associated Euclidean function, and let A be an ideal of D. If $A = \{0\}$, then $A = \langle 0 \rangle$ is principal, so suppose that A contains a nonzero element of D. We can select an element $b \neq 0$ in A such that $f(b)$ is as small as possible among all nonzero elements of A. We show in this case that $A = \langle b \rangle$, and so every ideal of D is a principal ideal.

Since b is in A, then $\langle b \rangle \subseteq A$ by Proposition C.22. For the reverse inclusion, let a be an element of A. Since D is Euclidean and $b \neq 0$, there are elements q and r in D for which $a = bq + r$, with $f(r) < f(b)$. Note that $r = a - bq$ is an element of A, by the closure properties of an ideal. If $r \neq 0$, then $f(r) < f(b)$ contradicts the definition of b as a nonzero element in A with $f(b)$ as small as possible. So we must conclude that $r = 0$, so that $a = bq \in \langle b \rangle$. Therefore, $A \subseteq \langle b \rangle$, and $A = \langle b \rangle$ is principal. □

DEFINITION. Elements a and b of an integral domain D are called *coprime* if $\langle a, b \rangle = D$.

PROPOSITION C.30. *Let a, b, and c be elements of a principal ideal domain D. Suppose that a divides bc in D, and that a and b are coprime. Then a divides c in D.*

PROOF. If $\langle a, b \rangle = D$, then $1 = as + bt$ for some $s, t \in D$. Suppose that a divides bc, say that $bc = aq$ for some q in D. Then we have that

$$c = c \cdot 1 = c(as + bt) = acs + (bc)t = acs + aqt = a(cs + qt),$$

so that a divides c. □

THEOREM C.31. *If D is a principal ideal domain, then every irreducible element of D is also prime in D.*

PROOF. Let D be a principal ideal domain and let p be an irreducible element in D. Suppose that p divides ab for some $a, b \in D$, and consider the ideal $\langle a, p\rangle$ of D. Since every ideal of D is principal, there is some d in D so that $\langle a, p\rangle = \langle d\rangle$. Now p is an element of $\langle a, p\rangle$, so $p = dq$ for some $q \in D$. Since p is irreducible, it follows that either q or d is a unit in D. If q is a unit, then p and d are associates. But a is an element of $\langle a, p\rangle$, so that d divides a, and thus p must also divide a. On the other hand, if d is a unit, then we find that $\langle d\rangle = D$, so that a and p are coprime. Now Proposition C.30 applies—since p divides ab and $\langle a, p\rangle = D$, we conclude that p divides b. So when p divides ab, then either p divides a or p divides b, and p is prime by definition. □

THEOREM C.32. *Every Euclidean domain is a unique factorization domain.*

PROOF. Let D be a Euclidean domain, with f an associated Euclidean function. We can show that every element a of D that is neither zero nor a unit can be written in some way as a product of irreducible elements. If not, we can assume that a cannot be so expressed, and that $f(a)$ is as small as possible among all such elements. This element a is not irreducible, since we view an irreducible element as being a product of irreducibles with just one term. So we can write $a = bc$ in D, with neither b nor c a unit. The definition of a Euclidean function implies that $f(x) = 1$ is and only if x is a unit of D. So now we find that $1 < f(b), f(c) < f(a)$. By assumption, then b and c can be written as products of irreducible elements of D. But then $a = bc$ has that property as well.

The conclusion that D is a unique factorization domain now follows immediately from Theorem C.28, Theorem C.29, and Theorem C.31. □

Exercises on Divisibility in Integral Domains.

1. Show that a and b are associates in D if and only if $b = au$ for some unit u of D.
2. Define $\sim$ on D by saying that $a \sim b$ if and only if a is an associate of b. Show that $\sim$ is an equivalence relation on D. That is, $\sim$ is reflexive ($a \sim a$ for all $a \in D$), symmetric (if $a \sim b$, then $b \sim a$), and transitive (if $a \sim b$ and $b \sim c$, then $a \sim c$).
3. Show that if a is an associate of b, and c is an associate of d in D, then a divides c if and only if b divides d.
4. Show that if a is an associate of b, and c is an associate of d, then ac is an associate of bd in D.
5. Show that if f is a Euclidean function for D, then $f(a) = 1$ if and only if a is a unit in D.
6. If a and b are elements of D, show that b divides a if and only if $\langle a\rangle \subseteq \langle b\rangle$.
7. If u is an element of D, show that u is a unit in D if and only if $\langle u\rangle = D$.
8. Show that elements a and b of D are associates if and only if $\langle a\rangle = \langle b\rangle$.
9. Let p be an element of D that is neither 0 nor a unit. Show that p is prime in D if and only if $ab \in \langle p\rangle$ implies that either $a \in \langle p\rangle$ or $b \in \langle p\rangle$.
10. Let p be an element of D that is neither 0 nor a unit. Show that p is irreducible in D if and only if whenever $\langle p\rangle \subseteq \langle q\rangle \subseteq D$, either $\langle q\rangle = \langle p\rangle$ or $\langle q\rangle = D$.

Congruence Relations on Integral Domains

We can generalize the congruence relations on integers to arbitrary integral domains using the definition of ideals.

DEFINITION. Let M be an ideal of an integral domain D. If a and b are elements of D, we say that a is *congruent* to b *modulo* M, and write $a \equiv b \pmod{M}$, if $a - b$ is an element of M.

The following proposition lists some properties of this relation. We leave the proofs of these claims as Exercises 1–6.

PROPOSITION C.33. *Let M be an ideal of an integral domain D. The following statements are true about the relation of congruence modulo M.*

(1) *Congruence modulo M is an equivalence relation on D. That is,*
   (a) $a \equiv a \pmod{M}$ *for all a in D.*
   (b) *For all $a, b \in D$, if $a \equiv b \pmod{M}$, then $b \equiv a \pmod{M}$.*
   (c) *For all $a, b, c \in D$, if $a \equiv b \pmod{M}$ and $b \equiv c \pmod{M}$, then $a \equiv c \pmod{M}$.*
(2) *If M is contained in an ideal N of D, then $a \equiv b \pmod{M}$ implies that $a \equiv b \pmod{N}$.*
(3) *If $M = \langle m \rangle$ is a principal ideal, then $a \equiv b \pmod{M}$ if and only if m divides $a - b$ in D. (In this case, we also write $a \equiv b \pmod{M}$ as $a \equiv b \pmod{m}$.)*
(4) *If $m = 0$, then $a \equiv b \pmod{m}$ if and only if $a = b$.*
(5) *If m is a unit in D, then $a \equiv b \pmod{m}$ is true for all $a, b \in D$.*
(6) *If m and n are associates in D, then $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{n}$.*

PROPOSITION C.34. *Let M be an ideal of an integral domain D. Suppose that $a \equiv b \pmod{M}$ and $c \equiv d \pmod{M}$ for some $a, b, c, d \in D$. Then $a + c \equiv b + d \pmod{M}$ and $ac \equiv bd \pmod{M}$.*

PROOF. We prove the claim for multiplication, leaving the corresponding statement for addition as Exercise 7. Suppose that $a \equiv b \pmod{M}$ and $c \equiv d \pmod{M}$, so that $a-b$ and $c-d$ are elements of M. Then $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$ is also an element of M, using the multiplicative and additive properties of ideals. So $ac \equiv bd \pmod{M}$ by definition. □

Factor Rings. If M is an ideal of D, then the equivalence class of an element a of D under congruence modulo M has the form $a+M = \{a+m \mid m \in M\}$. We write the set of all such distinct equivalence classes as D/M, or when $M = \langle m \rangle$, we may write D/M as D_m. If M is apparent from context, we also write the congruence class $a+M$ as $[a]$, or, when confusion is unlikely, simply as a. Proposition C.34 shows that the following operations of addition and multiplication,

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab],$$

are well-defined on the set D/M. One can verify that D/M has all the properties of a ring under the operations of addition and multiplication defined here. We refer to D/M as the *factor ring* of D modulo M. Identity elements for addition and multiplication are provided by $[0]$ and $[1]$ respectively, and the additive inverse of any class $[a]$ can be written as $[-a]$.

Note that the identity elements $[0]$ and $[1]$ might be equal. In general, $[a] = [0]$ if and only if $a = a - 0$ is an element of M, so $[1] = [0]$ when $1 \in M$. But in that case, $a \cdot 1 = a$ must be in M for all $a \in D$, so that $M = D$. So $[1] \neq [0]$ if M is a *proper* ideal of D, that is, $M \neq D$.

Additional attributes of D/M are determined by certain corresponding properties of the ideal M, as in the following definition and results.

DEFINITION. Let M be a proper ideal of an integral domain D.

(1) We say that M is a *prime* ideal of D if whenever M contains a product ab of elements of D, either a or b must be an element of M.
(2) We say that M is a *maximal* ideal of D if there is no proper ideal of D that properly contains M. That is, if N is an ideal of D with $M \subseteq N$, then either $N = M$ or $N = D$.

The following alternative characterization of prime ideals is useful as well.

PROPOSITION C.35. *A proper ideal P of an integral domain D is a prime ideal if and only if it has the following property: For all ideals A and B of D, if AB is a subset of P, then either $A \subseteq P$ or $B \subseteq P$.*

PROOF. Let P be a prime ideal of D, and suppose that $AB \subseteq P$ for some ideals A and B of D, but that A is not a subset of P. Then there is some element a in A but not in P. For every

$b \in B$, the element ab is in AB, and so is in P. Since P is prime but a is not in P, then b must be in P. But with this true of every $b \in B$, it follows that B is a subset of P.

Conversely, suppose that P is a proper ideal of D with the property that whenever $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$ (where A and B are ideals of D). Suppose that ab is an element of P for some $a, b \in D$. Then $\langle ab \rangle$ is a subset of P, but we know that $\langle ab \rangle = \langle a \rangle \langle b \rangle$. By our assumption, either $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$, but then either $a \in P$ or $b \in P$. So P is a prime ideal of D. □

THEOREM C.36. *Let m be an element of an integral domain D. Then*

(1) *m is prime as an element of D if and only if $\langle m \rangle$ is a prime ideal of D, and*
(2) *m is irreducible in D if and only if $\langle m \rangle$ is maximal among principal ideals of D, that is, if $\langle m \rangle \subseteq \langle n \rangle$ for some $n \in D$, then either $\langle n \rangle = \langle m \rangle$ or $\langle n \rangle = D$.*

Statement (2) implies that if D is a principal ideal domain, and m is irreducible in D, then $\langle m \rangle$ is maximal in D.

PROOF. This is a restatement of parts (4) and (5) of Proposition C.27. □

THEOREM C.37. *Let M be an ideal of an integral domain D. Then the following are true.*

(1) *M is a prime ideal of D if and only if D/M is an integral domain.*
(2) *M is a maximal ideal of D if and only if D/M is a field.*

PROOF. We can assume, as noted above, that D/M has all the properties of a commutative ring with unity, and that $[1] \neq [0]$ in D/M when M is a proper ideal of D.

(1) Let M be a prime ideal and suppose that $[a] \cdot [b] = [ab] = [0]$ in D/M. Then ab is an element of M, and since M is prime, then either $a \in M$ or $b \in M$. Thus either $[a] = [0]$ or $[b] = [0]$, and we conclude that D/M is an integral domain. Conversely, if D/M is an integral domain and ab is in M, then $[ab] = [a] \cdot [b] = [0]$ in D/M, from which we conclude that $[a] = 0$ or $[b] = [0]$. That is, either $a \in M$ or $b \in M$.

(2) Let M be a maximal ideal, and suppose that $[a] \neq [0]$ in D/M, that is, a is an element of D not in M. Let $N = M + \langle a \rangle = \{m + aq \mid m \in M \text{ and } q \in D\}$, an ideal of D. If m is in M, then $m + a(0)$ is in N. But N contains $0 + a(1) = a$, which is not in M. So N properly contains M, and since M is maximal, this implies that $N = D$. In particular, 1 is an element of N, so that $1 = m + ab$ for some $m \in M$ and $b \in D$. But then $ab - 1$ is an element of M, which implies that $[1] = [ab] = [a] \cdot [b]$ in D/M. So $[a]$ has an inverse under multiplication in D/M, namely $[b]$. This shows that D/M is a field.

Conversely, let D/M be a field, and suppose that N is an ideal of D that properly contains M. Then N contains an element a not in M, so that $[a] \neq [0]$ in D/M. Now $[a]$ has an inverse under multiplication, that is, $[a] \cdot [b] = [ab] = [1]$ for some $[b] \in D/M$. It follows that $ab - 1 = m$ for some m in M, or equivalently, $ab - m = 1$. But since $a \in N$ and $m \in M \subseteq N$, we must conclude that 1 is an element of N by properties of ideals. It follows that N equals the entire domain D, and we conclude that there is no proper ideal of D that properly contains M, so that M is maximal. □

If $m > 1$ in $\mathbb{Z}$, we find that $\langle m \rangle$ is both prime and maximal if and only if m is prime. So $\mathbb{Z}_m$ is a field if m is prime, but is not an integral domain if m is composite. (The trivial ideal $\langle 0 \rangle = \{0\}$ is prime but not maximal, as we have noted, while the improper ideal $\langle 1 \rangle = \mathbb{Z}$ is neither prime nor maximal by definition.)

Theorem C.37 shows that a maximal ideal of an integral domain is always a prime ideal. The converse is not generally true, but the following special case is an immediate consequence of Proposition C.19.

COROLLARY C.38. *Let M be an ideal of an integral domain D. If M is prime in D, and D/M is finite, then M is also maximal in D.*

Exercises on Congruence Relations on Integral Domains.

1. Show that congruence modulo M is an equivalence relation on D.
2. Show that if N is an ideal of D, and $M \subseteq N$, then $a \equiv b \pmod{M}$ implies that $a \equiv b \pmod{N}$.
3. If $M = \langle m \rangle$ for some m in D, show that $a \equiv b \pmod{M}$ if and only if m divides $a - b$ in D.
4. If $M = \{0\}$, show that $a \equiv b \pmod{M}$ if and only if $a = b$.
5. If $M = \langle u \rangle$ for some unit u in D, show that $a \equiv b \pmod{M}$ is true for all $a, b \in D$.
6. If $M = \langle m \rangle$ and $N = \langle n \rangle$, and m and n are associates in D, show that $a \equiv b \pmod{M}$ if and only if $a \equiv b \pmod{N}$.
7. If $a \equiv b \pmod{M}$ and $c \equiv d \pmod{M}$, show that $a + c \equiv b + d \pmod{M}$.

Finite Fields

We conclude this appendix with a classification of finite fields, beginning with the following general definition.

DEFINITION. Let R be a ring with unity element 1. If 1 has finite order n in the group R under addition, we say that the *characteristic* of R is n. If 1 has infinite order in R under addition, we say that R has *characteristic zero*. We write the characteristic of R as $\operatorname{char} R$.

So if $\operatorname{char} R = n$, then the sum of n copies of 1 equals 0 in R. We will write this as $n \cdot 1 = 0$. (This is not to be confused with the multiplication operation in R. The positive integer n is not necessarily an element of the ring R.) Note that $\operatorname{char} R = 0$ is possible only in an infinite ring.

PROPOSITION C.39. *Let R be a ring with unity element* 1. *If* $\operatorname{char} R = n$, *then* $n \cdot a = 0$ *for every a in R.*

PROOF. In R, we have that

$$n \cdot a = a + a + \cdots + a = a \cdot 1 + a \cdot 1 + \cdots + a \cdot 1 = a(1 + 1 + \cdots + 1) = a \cdot 0 = 0,$$

by the definition of the unity element and the distributive property. (Each sum above contains n terms.) □

It follows that if $\operatorname{char} R = n$, then n is the maximum order of an element of the additive group R.

PROPOSITION C.40. *If R is an integral domain, then the characteristic of R is either* 0 *or a prime number.*

PROOF. Suppose that R is an integral domain with positive characteristic n. If $n = 1$, then $1 = 0$ by definition, but this cannot be true in an integral domain. If $n = \ell m$ with $1 < \ell, m < n$, then $0 = n \cdot 1 = (\ell m) \cdot 1 = (\ell \cdot 1)(m \cdot 1)$. (This is an application of the distributive property in R.) But if R is an integral domain, this implies that either $\ell \cdot 1 = 0$ or $m \cdot 1 = 0$. Either possibility contradicts the definition of n. Thus we must conclude that n is prime. □

In particular, the characteristic of every finite integral domain is prime. Recall from Proposition C.19 that a finite integral domain is a field.

PROPOSITION C.41. *Let F be a field with n elements. Then $n = p^k$ for some prime p and positive integer k. That is, the number of elements in a finite field must be a power of a prime.*

PROOF. As we have seen above, the characteristic of F is prime, say p, and this must be the maximum order of all elements in the abelian group F under addition. It follows that if $(n_1, n_2, \ldots, n_k)$ is the invariant factor type of F under addition, then $n_1 = p$. Since each invariant factor divides n_1, we conclude that $(p, p, \ldots, p)$ is the invariant factor type of F under addition (here with k terms of p for some positive integer k). But then F has $p \cdot p \cdots p = p^k$ elements. □

EXAMPLE. We have seen that $\mathbb{Z}_p$ is a field if p is prime. We may also write $\mathbb{Z}_p$ as $\mathbb{F}_p$ to emphasize this fact. ◊

We illustrate an important general property of fields of prime characteristic with the following example, before stating a more precise result.

EXAMPLE. Suppose that $\operatorname{char} F = 5$, and that 1 is the unity element of F. Consider the subset $S = \{0, 1, 1+1, 1+1+1, 1+1+1+1\}$ of F. Note that these five elements of F must be distinct. (For instance, if $1+1 = 1+1+1+1$, then $0 = 1+1$ by cancellation, contradicting the assumption that 1 has order five in the group F under addition.) This set is closed under addition and multiplication in F, and those operations act in the same way as addition and multiplication modulo 5. For example,

$$(1+1+1)+(1+1+1) = (1+1+1+1+1)+1 = 0+1 = 1,$$

and

$$(1+1+1)(1+1+1) = (1+1+1)+(1+1+1)+(1+1+1) = 1+1+1+1,$$

using only the distributive property and other properties that hold in every field. If we rename $1+1$ as 2, then $1+1+1$ as 3, and $1+1+1+1$ as 4, we find that S has all the properties of $\mathbb{F}_5$. (For instance, the equations above now would say $3+3 = 1$ and $3 \cdot 3 = 4$ in F, as in $\mathbb{F}_5$.) In this way, we can view $\mathbb{F}_5$ as a *subfield* of this field of characteristic 5. ◊

The following proposition summarizes this idea. We leave its proof as Exercise 1.

PROPOSITION C.42. *Let F be a finite field of characteristic p, having unity element 1. Then the function $f : \mathbb{F}_p \to F$ defined by $f(a) = a \cdot 1$ is a well-defined injective ring homomorphism. We may view $\mathbb{F}_p$ as a subfield of F by labeling each $f(a)$ as a in F.*

In general, if F is a subfield of a field E, we also say that E is an *extension field* of F. The preceding proposition then states that every field of characteristic p is an extension field of $\mathbb{F}_p$.

Polynomials over Fields. We now describe a method of constructing examples of fields with p^k elements where $k > 1$. To do so, we need to define rings of polynomials over a field. We will leave many details for the reader to consider or prove.

DEFINITION. A *polynomial* over a field F is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

where each a_i is an element of F, and $a_i = 0$ for all but finitely many $i \geq 0$. If n is the largest integer for which $a_n \neq 0$, we say that the *degree* of $f(x)$ is n, written $\deg(f) = n$, and that a_n is the *leading coefficient* of $f(x)$. When the leading coefficient of $f(x)$ is 1, we say that $f(x)$ is *monic*. If every coefficient of $f(x)$ is 0, we call $f(x)$ the *zero polynomial*—the degree and leading coefficient of the zero polynomial are undefined. The set of all polynomials over F is written as $F[x]$.

Writing the exponents of x in increasing order is convenient in making general definitions, but we will usually employ decreasing order when writing specific examples of polynomials. We may view a polynomial $f(x)$ in $F[x]$ as a function into which we can substitute elements of F (or elements of some larger field, as we will see). But two polynomials are considered equal only when they have the same coefficients for each corresponding power of x. For instance, $f(x) = x^2 + 1$

and $g(x) = x + 1$ are not equal in $\mathbb{F}_2[x]$, even though as functions they do the same thing to both elements of $\mathbb{F}_2$. Note however that $f(x) = x^2 + 2$ and $g(x) = x^2 - 1$ are equal in $\mathbb{F}_3[x]$, because $2 = -1$ in $\mathbb{F}_3$.

DEFINITION. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ be elements of $F[x]$ for some field. We define the *sum* of $f(x)$ and $g(x)$ to be

$$f(x) + g(x) = (f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots.$$

We define the *product* of $f(x)$ and $g(x)$ to be $f(x)g(x) = (f \cdot g)(x) = c_0 + c_1x + c_2x^2 + \cdots$, where for each $n \geq 0$,

$$c_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}.$$

PROPOSITION C.43. *If F is a field, then $F[x]$ is an integral domain under the preceding definitions of polynomial addition and multiplication. The units of $F[x]$ are precisely the polynomials of degree zero.*

PROOF. First note that the sum and product of two polynomials are in fact elements of $F[x]$. If $\deg(f) = m$ and $\deg(g) = n$, then $\deg(f+g) \leq \max(m, n)$, or could be undefined. The coefficient of x^{m+n} in $(f \cdot g)(x)$ is

$$c_{m+n} = a_0b_{m+n} + \cdots + a_{m-1}b_{n+1} + a_mb_n + a_{m+1}b_{n-1} + \cdots + a_{m+n}b_0 = a_mb_n,$$

since at least one term in each other product making up this sum is 0. If $a_m \neq 0$ and $b_n \neq 0$ in F, then $c_{n+m} \neq 0$. But one can see by the same type of calculation that $c_i = 0$ if $i > m + n$. So $\deg(f \cdot g) = \deg(f) + \deg(g)$ if $f(x)$ and $g(x)$ are not the zero polynomial. Note that this shows that the product of two nonzero elements of $F[x]$ is not zero.

The zero polynomial has the property of an additive identity element for $F[x]$, and the inverse of $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ under addition is the *negative* of $f(x)$, that is,

$$-f(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \cdots.$$

The multiplicative identity element for $F[x]$ is $u(x) = 1 + 0x + 0x^2 + \cdots$ (which we will write simply as 1), a polynomial of degree zero. Note that if $\deg(f) > 0$, then $f(x)$ cannot have an inverse under multiplication in $F[x]$ since in that case $\deg(f \cdot g) = \deg(f) + \deg(g) \geq \deg(f) > 0$ for every nonzero $g(x)$. On the other hand, if $\deg(f) = 0$, so that $f(x) = a$ for some $a \neq 0$ in F, then the inverse of $f(x)$ is $g(x) = a^{-1}$, also in $F[x]$.

The remaining properties of an integral domain (the commutative, associative, and distributive properties) can be verified directly, and are left as Exercise 2. □

Since $F[x]$ is an integral domain, we can consider definitions and properties of divisibility in $F[x]$. We saw in Proposition C.43 that the units in $F[x]$ are polynomials of degree zero, that is, nonzero constant polynomials. Elements $f(x)$ and $g(x)$ of $F[x]$ are associates if $g(x)$ is a nonzero constant multiple of $f(x)$. Every nonzero polynomial has a unique monic associate. A polynomial $f(x)$ with $\deg(f) > 0$ is irreducible in $F[x]$ if it is impossible to write $f(x) = g(x) \cdot h(x)$ with $0 < \deg(g), \deg(h) < \deg(f)$. Note that a polynomial of degree one must be irreducible in $F[x]$. The following theorem is useful for considering questions of divisiblity in a ring of polynomials over a field.

THEOREM C.44 (Division Algorithm for Polynomials). *Let $f(x)$ and $g(x)$ be polynomials in $F[x]$ for some field F, with $g(x)$ not equal to the zero polynomial. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$, with $\deg(r) < \deg(g)$ or $r(x) = 0$, so that $f(x) = g(x)q(x) + r(x)$.*

We omit the proof of this theorem. In practice, we can apply this algorithm through the process of long division. We illustrate the idea with an example.

EXAMPLE. Let $f(x) = 3x^3 + 4x + 2$ and $g(x) = 2x + 3$ in $\mathbb{F}_5[x]$. In the division process, we first look for a *monomial* expression that we can multiply by the leading term of $g(x)$ to make it equal to the leading term of $f(x)$. Since $2^{-1} = 3$ and $3 \cdot 3 = 4$ in $\mathbb{F}_5$, we find that $4x^2$ has this property. Note that

$$f(x) - g(x) \cdot 4x^2 = (3x^3 + 4x + 2) - (3x^3 + 2x^2) = 3x^2 + 4x + 2.$$

Now we repeat this process with this new polynomial in place of $f(x)$. We find that

$$(3x^2 + 4x + 2) - g(x) \cdot 4x = (3x^2 + 4x + 2) - (3x^2 + 2x) = 2x + 2.$$

Finally,

$$(2x + 2) - g(x) \cdot 1 = (2x + 2) - (2x + 3) = 4.$$

The resulting term now has smaller degree than that of $g(x)$. Combining these equations, we find that

$$\begin{aligned} f(x) = g(x) \cdot 4x^2 + (3x^2 + 4x + 2) &= g(x) \cdot 4x^2 + g(x) \cdot 4x + (2x + 2) \\ &= g(x) \cdot 4x^2 + g(x) \cdot 4x + g(x) \cdot 1 + 4 = g(x)(4x^2 + 4x + 1) + 4 \end{aligned}$$

and conclude that $q(x) = 4x^2 + 4x + 1$ and $r(x) = 4$. ◊

The following corollary of the division algorithm is useful for establishing divisibility statements.

COROLLARY C.45. *Let c be an element of some field F, and let $f(x)$ be an element of $F[x]$. Then $g(x) = x - c$ divides $f(x)$ if and only if $f(c) = 0$.*

PROOF. By the division algorithm, we can write $f(x) = (x-c)q(x)+r(x)$ for some polynomial $r(x)$ with $\deg(r) < \deg(g)$ or $r(x) = 0$. Since $\deg(g) = 1$, then $r(x) = a$ is a constant polynomial in either case. But now notice that $f(c) = (c - c)q(c) + r(c) = a$. In particular, $r(c) = 0 = r(x)$ if and only if $f(x) = (x - c)q(x)$, that is, $x - c$ divides $f(x)$. □

EXAMPLE. Let $f(x) = x^2 + 1$ in $\mathbb{F}_3[x]$. If $f(x)$ is not irreducible in $\mathbb{F}_3[x]$, it must factor as a product of two linear (degree one) polynomials. Multiplying by units if necessary, we may assume that any such factor is monic, say of the form $g(x) = x - c$ for some c in $\mathbb{F}_3$. But since $f(0) = 1$, $f(1) = 2$, and $f(2) = 2$ in $\mathbb{F}_3$, Corollary C.45 shows that no such factor exists. So $f(x) = x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$. ◊

EXAMPLE. If $f(x) = x^2 + 1$ in $\mathbb{F}_5[x]$, we find that $f(2) = 0$. Applying the division algorithm, we can confirm that $f(x) = (x - 2)(x - 3)$, so that $f(x)$ is not irreducible in $\mathbb{F}_5[x]$. ◊

The division algorithm shows that $F[x]$ is a Euclidean domain—specifically, if we define a function $\phi : F[x] \to \mathbb{N}$ by $\phi(0) = 0$ and $\phi(f(x)) = 2^{\deg(f)}$ when $f(x) \neq 0$, we find that ϕ is a Euclidean function. By Theorems C.29 and C.32, $F[x]$ is also a principal ideal domain and a unique factorization domain.

Factor Rings as Extension Fields. We now demonstrate how we can use an irreducible polynomial in $\mathbb{F}_p[x]$ to construct a finite extension field of $\mathbb{F}_p$. Let $g(x)$ be irreducible in $\mathbb{F}_p[x]$ and consider the ideal $A = \langle g(x) \rangle$. (We can assume that $g(x)$ is monic, since it can be replaced by any of its associates.) Then A is maximal among principal ideals of $\mathbb{F}_p[x]$ by Theorem C.36. But since every ideal of $\mathbb{F}_p[x]$ is principal, it follows that A is a maximal ideal of $\mathbb{F}_p[x]$. Therefore, the factor ring $\mathbb{F}_p[x]/A$ is a field. The following proposition compiles some properties of fields of this type.

PROPOSITION C.46. *Let $g(x)$ be an irreducible polynomial of degree $k > 1$ in $\mathbb{F}_p[x]$ for some prime number p. Let $A = \langle g(x) \rangle$, and write the factor ring $\mathbb{F}_p[x]/A$ as E. Then E has the following properties.*

1. *Every element of E can be written uniquely as $r(x) + A$ where $\deg(r) < k$ or $r(x) = 0$.*
2. *The set of elements $\{a + A \mid a \in \mathbb{F}_p\}$ (that is, where $r(x) = a$ is a constant polynomial) forms a subfield of E with the same properties as $\mathbb{F}_p$.*
3. *If $v = x + A$, then $g(v) = 0$.*

PROOF. (1) By definition, the typical element of $\mathbb{F}_p[x]/A$ has the form $f(x) + A$ where $f(x)$ is in $\mathbb{F}_p[x]$. Using the division algorithm, we can write $f(x) = g(x)q(x) + r(x)$ with $\deg(r) < \deg(g)$ or $r(x) = 0$. But then since $f(x) - r(x)$ is an element of $A = \langle g(x) \rangle$, we have that $f(x) + A = r(x) + A$. On the other hand, if $r(x)$ and $s(x)$ are distinct polynomials with degree smaller than k, then $r(x) + A \neq s(x) + A$, since the degree of $r(x) - s(x)$ is smaller than k but every nonzero element of A has degree at least k. So every element of $\mathbb{F}_p[x]/A$ can be written *uniquely* as $r(x) + A$.

(2) The sum and product of two constant polynomials is a constant polynomial, as is the negative of any constant polynomial and inverse of any nonzero constant polynomial. So $\{a + A \mid a \in \mathbb{F}_p\}$ is a subfield of $\mathbb{F}_p[x]/A$. Identifying $a + A$ with a, we find that this subfield has all the properties of $\mathbb{F}_p$.

(3) Let $g(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$. If we identify each coefficient a_i with the coset $a_i + A$, as in part (2), then we can say that

$$g(x + A) = (x + A)^k + (a_{k-1} + A)(x + A)^{k-1} + \cdots + (a_1 + A)(x + A) + (a_0 + A).$$

But then by repeated application of the definition of addition and multiplication in a factor ring, we find that

$$g(x + A) = (x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0) + A = g(x) + A = 0 + A,$$

the final equation using the fact that $g(x)$ is an element of A. We can interpret this equation as $g(v) = 0$, where $v = x + A$ in E. □

To summarize this proposition, if $g(x)$ is irreducible in $\mathbb{F}_p[x]$ with $\deg(g) = k$, and $A = \langle g(x) \rangle$, then $E = \mathbb{F}_p[x]/A$ has p^k elements, since there are p choices for each of the k coefficients of $x^0, x^1, \ldots, x^{k-1}$ in $r(x)$. We can view $\mathbb{F}_p$ as a subfield of E, that is, E as an extension field of $\mathbb{F}_p$. The field E contains a root $v = x + A$ of the polynomial $g(x)$. We can write the typical element of E as

$$\begin{aligned} r(x) + A &= (a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1}) + A \\ &= (a_0 + A) + (a_1 + A)(x + A) + (a_2 + A)(x + A)^2 + \cdots + (a_{k-1} + A)(x + A)^{k-1} \\ &= a_0 + a_1 v + a_2 v^2 + \cdots + a_{k-1}v^{k-1}. \end{aligned}$$

That is,

$$E = \{a_0 + a_1 v + a_2 v^2 + \cdots + a_{k-1}v^{k-1} \mid a_i \in \mathbb{F}_p \text{ and } g(v) = 0\}.$$

The fact that $g(v) = 0$ allows us to calculate products and write inverses in this form, as we illustrate in the following example.

EXAMPLE. We saw that $g(x) = x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$. So if $A = \langle g(x) \rangle$, then $E = \mathbb{F}_3[x]/A$ is a field with $3^2 = 9$ elements,

$$E = \{a + bv \mid a, b \in \mathbb{F}_3\} = \{0, 1, 2, v, 1 + v, 2 + v, 2v, 1 + 2v, 2 + 2v\},$$

where v satisfies $v^2 + 1 = 0$, so $v^2 = -1 = 2$. For example,

$$(1 + 2v)(2 + v) = (1 \cdot 2) + (1 \cdot 1 + 2 \cdot 2)v + (2 \cdot 1)v^2 = 2 + 2v + 2(2) = 2v,$$

with all coefficient calculations carried out in $\mathbb{F}_3$. Likewise, $(1+2v)^{-1}$ is an element $a+bv$ that satisfies

$$1 = (1+2v)(a+bv) = a + (b+2a)v + 2bv^2 = a + (2a+b)v + 2b(2) = (a+b) + (2a+b)v.$$

This equation can hold only if $a+b = 1$ and $2a+b = 0$. The latter equation implies that $b = -2a = a$, so then the first equation becomes $a + a = 1$. So $a = 2 = b$, and $(1+2v)^{-1} = 2 + 2v$. ♢

This example illustrates that if $g(x)$ is a polynomial in $F[x]$ for some field F, then we can construct an extension field of F in which $g(x)$ has a root. By repeating this process, it is likewise possible to construct an extension field E of F so that $g(x)$ factors completely into linear terms in $E[x]$. We will assume that the smallest field in which this occurs is uniquely determined by F and by $g(x)$. (More precisely, any two such fields are isomorphic.) We refer to this field E as the *splitting field* of $g(x)$ over F.

Properties of Finite Fields. We have seen that if F is a finite field, then the number of elements in F is p^k where p is a prime number and k is a positive integer. We conclude this section by showing that a field with this number of elements does exist and is essentially unique, and we describe certain properties of this field.

LEMMA C.47. *Let F be a finite field of characteristic p. Then $(a+b)^p = a^p + b^p$ for every a and b in F. The function $\phi : F \to F$ defined by $\phi(x) = x^p$ is an automorphism of F, that is, an isomorphism between F and itself.*

PROOF. As a consequence of the distributive property, one can establish the *Binomial Theorem* in every commutative ring R, that is, the equation

$$(a+b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2}a^{n-2}b^2 + \cdots + b^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i,$$

for all a and b in R and every positive integer n, where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$. When $n = p$ is prime, then p divides $\binom{p}{i}$ for $0 < i < p$. In a field F of characteristic p, this means that all terms in this sum are zero except for the first and last. That is, $(a+b)^p = a^p + b^p$. Since it is also true that $(ab)^p = a^p b^p$ in F, by the commutative property of multiplication, then the function $\phi : F \to F$ defined by $\phi(x) = x^p$ is a ring homomorphism. This function is injective, since if $\phi(x) = x^p = y^p = \phi(y)$, then $x^p - y^p = (x-y)^p = 0$. (Here we use the fact that $(-1)^p = -1$ if p is odd, while $-1 = 1$ in a field of characteristic $p = 2$.) But this implies that $x = y$, since otherwise $x - y$ has an inverse in F, and we would be forced to conclude that $1 = 0$ in F. Finally, since F is finite, a injective function $\phi : F \to F$ must also be surjective. So ϕ is an automorphism of F. □

THEOREM C.48. *If p is a prime number and k is a positive integer, then there is a field containing p^k elements. Any two such fields are isomorphic.*

PROOF. Let $n = p^k$ and consider the polynomial $g(x) = x^n - x$ in $\mathbb{F}_p[x]$. As noted above, there is a smallest extension field E of $\mathbb{F}_p$ so that $g(x)$ factors completely in $E[x]$. In this case, $g(x)$ has n roots in E. (There are no repeated roots of $g(x)$, since no element can satisfy both $g(x) = 0$ and $g'(x) = 0$. In fact, $g'(x) = nx^{n-1} - 1 = p^k x^{n-1} - 1$ has no roots in a field with characteristic p.) But we can show as follows that the subset F of E consisting of those n roots is a subfield of E, in which case $F = E$.

(1) 0 is an element of F since $0^n = 0$.
(2) 1 is an element of F since $1^n = 1$.
(3) If a is in F, then $(-a)^n = (-1)^n a^n = -a$ so that $-a$ is in F.
(4) If $a \neq 0$ is in F, then $(a^{-1})^n = (a^n)^{-1} = a^{-1}$ so that a^{-1} is in F.

(5) If a and b are in F, then $(ab)^n = a^n b^n = ab$ so that ab is in F.
(6) If a and b are in F, then $(a+b)^n = (a+b)^{p^k} = ((a+b)^p)^{p^{k-1}} = (a+b)^{p^{k-1}} = a+b$ by repeated application of Lemma C.47. So $a+b$ is in F.

(Note that in statement (3), $(-1)^n = -1$ if n is odd. If $n = 2^k$, then $(-1)^n = 1$, but $1 = -1$ in a field of characteristic 2.)

So a field F with p^k elements exists. Now suppose that K is some other field with $n = p^k$ elements. Since $K^\times$ is a group with $n-1$ elements, we know that $a^{n-1} = 1$ for every $a \neq 0$ in K. But then $a^n = a$ if $a \neq 0$. It is also true that $0^n = 0$. So every element of K is a root of $g(x) = x^n - x$, and no smaller field can have this property. Thus K is a splitting field of $g(x)$ over $\mathbb{F}_p$, and must be isomorphic to the field F above. □

Example. In a previous example, we saw that

$$E = \mathbb{F}_3[x]/\langle x^2+1\rangle = \{a+bv \mid a,b \in \mathbb{F}_3 \text{ and } v^2 = -1 = 2\}$$

is a field with $3^2 = 9$ elements. Since $g(x) = x^2+x+2$ is also irreducible in $\mathbb{F}_3[x]$, then

$$K = \mathbb{F}_3[x]/\langle x^2+x+2\rangle = \{a+bw \mid a,b \in \mathbb{F}_3 \text{ and } w^2 = -w-2 = 1+2w\}$$

is another field with nine elements. To illustrate that K is isomorphic to E, we begin by noting that E contains a root of $g(x)$. If $x = a+bv$, then

$$x^2+x+2 = (a+bv)^2+(a+bv)+2 = ((a^2+2b^2)+2abv)+(a+bv)+2 = (a^2+2b^2+a+2)+(2ab+b)v = 0$$

implies that $a^2+2b^2+a+2 = 0$ and $2ab+b = (2a+1)b = 0$. If $b = 0$, then the first equation implies that $a^2+a+2 = 0$, but this is impossible for a in $\mathbb{F}_3$. So $2a+1 = 0$, that is, $a = 1$, and then $2b^2 = 2$, implying that $b = \pm 1$. Thus $1+v$ and $1+2v$ are two elements of E that satisfy $x^2+1 = 0$. The function $\phi : K \to E$ defined by $\phi(a+bw) = a+b(1+v) = (a+b)+bv$ is an isomorphism, as one can verify directly. ♢

We note some additional properties of finite fields, after the following preliminary observation.

Lemma C.49. *Let $f(x)$ be polynomial of degree n in $F[x]$ for some field F. Then there are no more than n elements a in F so that $f(a) = 0$.*

Proof. We use induction on the degree n of $f(x)$. If $n = 0$, then $f(x)$ is a nonzero constant polynomial, so there are no elements a in F with $f(a) = 0$. So now let n be a positive integer, and suppose that for every polynomial of degree $k < n$, there are no more than k roots of that polynomial in F. Then let $f(x)$ be a polynomial of degree n in $F[x]$. If f has no roots in F, then we are done, so suppose instead that a is an element of F so that $f(a) = 0$. The division algorithm implies that we can write $f(x) = (x-a)g(x) + r(x)$ where either $r(x)$ has degree zero or $r(x)$ is itself the zero polynomial. In either case, $r(x) = c$ is a constant polynomial. But now $0 = f(a) = (a-a)g(a) + r(a) = c$. So $f(x) = (x-a)g(x)$, and $\deg(g) = n-1$. If $f(b) = (b-a)g(b) = 0$, then either $b = a$ or b is a root of $g(x)$. (Here we use the fact that $b-a$ and $g(b)$ are elements of the field F, which is also an integral domain.) By the inductive hypothesis, $g(x)$ has no more than $n-1$ roots in F. Those roots, together with a, are the only possible roots of $f(x)$. So $f(x)$ has no more than n roots in F. The result follows by induction. □

Theorem C.50. *Let F be a finite field of characteristic p, so that F contains a subfield isomorphic to $\mathbb{F}_p$. If v is an element of F, then $v^p = v$ if and only if v is in $\mathbb{F}_p$.*

Proof. First note as follows that if v is an element of $\mathbb{F}_p$, then $v^p = v$. If $v = 0$, then $0^p = 0$. If $v \neq 0$, then v is an element of a group, $\mathbb{F}_p^\times$, of order $p-1$, so that $v^{p-1} = 1$ and then $v^p = v$. So the polynomial $x^p - x$ has p roots in $\mathbb{F}_p$, and so in every extension field F of $\mathbb{F}_p$. This is the maximum number of roots possible, and thus $v^p \neq v$ if v is an element of F not in the subfield $\mathbb{F}_p$. □

THEOREM C.51. *Let F be a finite field of characteristic p, so that F contains a subfield isomorphic to $\mathbb{F}_p$. Let $g(x)$ be a polynomial with coefficients in $\mathbb{F}_p$, and suppose that v is an element of F for which $g(v) = 0$. Then $g(v^p) = 0$ also.*

PROOF. Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with each a_i in $\mathbb{F}_p$, and suppose that $g(v) = 0$ for some v in F. Let $\phi : F \to F$ be the automorphism of F defined by $\phi(x) = x^p$, as in Lemma C.47, and note that $\phi(a) = a$ for every a in $\mathbb{F}_p$ by Theorem C.50. Applying ϕ to both sides of the equation $0 = a_n v^n + a_{n-1}v^{n-1} + \cdots + a_1 v + a_0$, we find that

$$0 = \phi(0) = \phi(a_n v^n + a_{n-1}v^{n-1} + \cdots + a_1 v + a_0) = a_n(\phi(v))^n + a_{n-1}(\phi(v))^{n-1} + \cdots a_1\phi(v) + a_0,$$

using the fact that ϕ is a homomorphism. But then $\phi(v) = v^p$ is a root of $g(x)$, as we wanted to show. □

THEOREM C.52. *Let F be a finite field. Then the group $F^\times$ of nonzero elements in F is cyclic.*

PROOF. Let t be maximum order of all the elements of $F^\times$. Since $F^\times$ is a finite abelian group, then $x^t = 1$ for all elements of $F^\times$ by Lemma C.11. But then every element of $F^\times$ is a root of the polynomial $f(x) = x^t - 1$. Lemma C.49 shows that this is impossible unless t is the number of elements in $F^\times$. So $F^\times$ contains at least one element of order $t = |F^\times|$, and is thus a cyclic group. □

Exercises on Finite Fields.

1. Show that if F is a field of characteristic p with unity element 1, then $f : \mathbb{F}_p \to F$ defined by $f(a) = a \cdot 1$ is a well-defined, injective ring homomorphism.
2. Verify that polynomial addition and multiplication are commutative and associative operations, and that multiplication is distributive over addition.
3. Verify that $g(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, list the elements in the factor ring $E = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$, and compile addition and multiplication tables for E.
4. Repeat Exercise 3 for $g(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$.
5. Verify that $g(x) = x^2 + 1$ is irreducible in $\mathbb{F}_7[x]$, and describe the addition and multiplication operations in the field $E = \mathbb{F}_7[x]/\langle x^2 + 1\rangle$. Show that $h(x) = x^2 + 2x + 2$ is irreducible in $\mathbb{Z}_7[x]$, but that $h(x)$ has two roots in E.