

Chapter 2

Basic Number Theory

2.1 The Ring of Integers

The theory of numbers is concerned with the properties of the **integers**, that is, the class of whole numbers and zero, $0, \pm 1, \pm 2, \dots$. We will denote the class of integers by \mathbb{Z} . The positive integers, $1, 2, 3, \dots$ are called the **natural numbers**, which we will denote by \mathbb{N} . We will assume that the reader is familiar with the basic arithmetic properties of \mathbb{Z} and in this section we will look at the abstract algebraic properties of the integers and what makes \mathbb{Z} unique as an algebraic structure.

Recall that a **ring** R is a set with two binary operations, addition, denoted by $+$, and multiplication denoted by \cdot or just by juxtaposition, defined on it satisfying the following six axioms:

1. Addition is commutative: $a + b = b + a$ for each pair a, b in R .
2. Addition is associative: $a + (b + c) = (a + b) + c$ for $a, b, c \in R$.
3. There exists an additive identity, denoted by 0 , such that $a + 0 = a$ for each $a \in R$.
4. For each $a \in R$ there exists an additive inverse denoted $-a$, such that $a + (-a) = 0$.
5. Multiplication is associative: $a(bc) = (ab)c$ for $a, b, c \in R$.
6. Multiplication is distributive over addition: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for $a, b, c \in R$.

If in addition R satisfies

7. Multiplication is commutative: $ab = ba$ for each pair a, b in R

then R is a **commutative ring**, while if R satisfies

8. There exists a multiplicative identity denoted by 1 (not equal to 0) such that $a \cdot 1 = 1 \cdot a = a$ for each a in R

then R is a **ring with an identity**. A **commutative ring with identity** satisfies 1 through 8.

A **field** K is a commutative ring with an identity in which every nonzero element has a multiplicative inverse, that is, for each $a \in K$ with $a \neq 0$ there exists an element $b \in K$ such that $ab = ba = 1$. In this case the set $K^* = K \setminus \{0\}$ forms an abelian group with respect to the multiplication in K . K^* is called the **multiplicative group** of K .

A ring can be considered as the most basic algebraic structure in which addition, subtraction, and multiplication can be done. In any ring the equation $x + b = c$ can always be solved. Further a field can be considered as the most basic algebraic structure in which addition, subtraction, multiplication, and division can be done. Hence in any field, the equation $ax + b = c$ with $a \neq 0$ can always be solved.

Combining this definition with our knowledge of \mathbb{Z} we get that

Lemma 2.1.1 *The integers \mathbb{Z} form a commutative ring with identity.*

There are many examples of such rings (see Exercises), so to define \mathbb{Z} uniquely we must introduce certain other properties. If two nonzero integers are multiplied together then the result is nonzero. This is not always true in a ring. For example, consider the set of functions defined on the interval $[0, 1]$. Under ordinary multiplication and addition, these form a ring (see Exercises) with the zero element being the function which is identically zero. Now let $f(x)$ be zero on $[0, \frac{1}{2}]$ and nonzero elsewhere and let $g(x)$ be zero on $[\frac{1}{2}, 1]$ and nonzero elsewhere. Then $f(x) \cdot g(x) = 0$ but neither is the zero function. We define an **integral domain** to be a commutative ring R with an identity and with the property that if $ab = 0$ with $a, b \in R$ then either $a = 0$ or $b = 0$. Two nonzero elements which multiply together to get zero are called **zero divisors** and hence an integral domain is a commutative ring with an identity and no zero divisors. Therefore, \mathbb{Z} is an integral domain.

The integers are also ordered, that is, we can compare any two integers. We abstract this idea in the following manner. We say that an integral domain D is an **ordered integral domain** if there exists a distinguished set D^+ , called the **set of positive elements**, with the properties that

- (1) The set D^+ is closed under addition and multiplication.
- (2) If $x \in D$ then exactly one of the following is true
 - (a) $x = 0$
 - (b) $x \in D^+$
 - (c) $-x \in D^+$.

In any ordered integral domain D we can order the elements in the standard way. If $x, y \in D$ then $x < y$ means that $(y - x) \in D^+$. With this ordering D^+ can clearly be identified with those $x \in D$ such that $x > 0$. We then get

Lemma 2.1.2 *If D is an ordered integral domain then*

- (1) $x < y$ and $y < z$ imply $x < z$.
- (2) If $x, y \in D$ then exactly one of the following holds:

$$x = y \text{ or } x < y \text{ or } y < x.$$

We thus have that the integers are an ordered integral domain. Their uniqueness as such a structure depends on two additional properties of \mathbb{Z} which are equivalent.

The Inductive Property Let S be a subset of the natural numbers \mathbb{N} . Suppose $1 \in S$ and S has the property that if $n \in S$ then $(n + 1) \in S$. Then $S = \mathbb{N}$.

The Well-Ordering Property Let S be a nonempty subset of the natural numbers \mathbb{N} . Then S has a least element.

Lemma 2.1.3 The inductive property is equivalent to the well-ordering property.

Proof To prove this we must assume first the inductive property and show that the well-ordering property holds and then vice versa. Suppose the inductive property holds and let S be a nonempty subset of \mathbb{N} . We must show that S has a least element. Let T be the set

$$T = \{x \in \mathbb{N}; x \leq s, \forall s \in S\}.$$

Now $1 \in T$ since $S \subset \mathbb{N}$. If whenever $x \in T$ it would follow that $(x + 1) \in T$ then by the inductive property $T = \mathbb{N}$ but then S would be empty contradicting that S is nonempty. Therefore, there exists an a with $a \in T$ and $(a + 1) \notin T$. We claim that a is the least element of S . Now $a \leq s$ for all $s \in S$ since $a \in T$. If $a \notin S$ then every $s \in S$ would also satisfy $(a + 1) \leq s$. This would imply that $(a + 1) \in T$ a contradiction. Therefore, $a \in S$ and $a \leq s$ for all $s \in S$ and hence a is the least element. Therefore, the inductive property implies the well-ordering property.

Conversely, suppose that the well-ordering property holds and suppose $1 \in S$ and whenever $n \in S$ it follows that $(n + 1) \in S$. We must show that $S = \mathbb{N}$. If $S \neq \mathbb{N}$ then $\mathbb{N} \setminus S$ is a nonempty subset of \mathbb{N} . Therefore, it must have a least element n . Hence $(n - 1) \in S$. But then $(n - 1) + 1 = n \in S$, also which is a contradiction. Therefore, $\mathbb{N} \setminus S$ is empty and $S = \mathbb{N}$. \square

The inductive property is of course the basis for **inductive proofs** which play a big role in the theory of numbers. To remind the reader, in an inductive proof we want to prove statements $\mathcal{P}(n)$ which depend on positive integers. In the induction we show that $\mathcal{P}(1)$ is true, then show that the truth of $\mathcal{P}(n + 1)$ depends upon the truth of $\mathcal{P}(n)$. From the inductive property $\mathcal{P}(n)$ is then true for all positive integers n . We give an example which has an ancient history in number theory.

Example 2.1.1 Show that $1 + 2 + \cdots + n = \frac{(n)(n+1)}{2}$

Here for $n = 1$ we have $1 = \frac{(1)(2)}{2} = 1$. So its true for $n = 1$. Assume that the statement is true for $n = k$, that is

$$1 + 2 + \cdots + k = \frac{k(k + 1)}{2}$$

and consider $n = k + 1$.

$$1 + 2 + \cdots + k + (k + 1) = (1 + 2 + \cdots + k) + (k + 1) = \frac{k(k + 1)}{2} + (k + 1) = \frac{(k + 1)(k + 2)}{2}$$

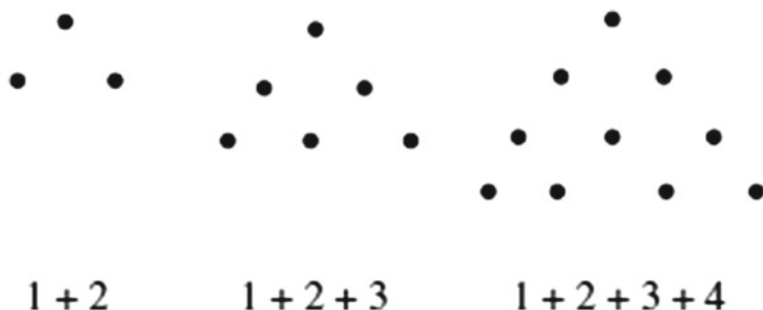


Fig. 2.1 Triangular Numbers

Hence the statement is true for $n = k + 1$ and hence true by induction for all $n \in \mathbb{N}$.
The series of integers

$$1, 1 + 2 = 3, 1 + 2 + 3 = 6, 1 + 2 + 3 + 4 = 10, \dots$$

are called the **triangular numbers** since they are the sums of dots placed in triangular form as in Figure 2.1. These numbers were studied by the Pythagoreans in Greece in 500 B.C.

The inductive property is enough to characterize the integers among ordered integral domains up to **isomorphism**. Recall that if R and S are rings, a function $f : R \rightarrow S$ is a **homomorphism** if it satisfies:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$ for $r_1, r_2 \in R$.
2. $f(r_1 r_2) = f(r_1) f(r_2)$ for $r_1, r_2 \in R$.

If f is also a bijection, then f is an **isomorphism**, and R and S are **isomorphic**. Isomorphic algebraic structures are essentially algebraically the same. We have the following theorem.

Theorem 2.1.1 *Let R be an ordered integral domain which satisfies the inductive property (replacing \mathbb{N} by the set of positive elements in R). Then R is isomorphic to \mathbb{Z} .*

We outline a proof in the exercises.

2.2 Divisibility, Primes, and Composites

The starting point for the theory of numbers is **divisibility**.

Definition 2.2.1 *If a, b are integers we say that a **divides** b , or that a is a **factor** or **divisor** of b , if there exists an integer q such that $b = aq$. We denote this by $a|b$.*

is then a **multiple** of a . If $b > 1$ is an integer whose only factors are $\pm 1, \pm b$ then b is a **prime**, otherwise $b > 1$ is **composite**.

The following properties of divisibility are straightforward consequences of the definition:

Theorem 2.2.1 (1) $a|b \implies a|bc$ for any integer c .

(2) $a|b$ and $b|c$ imply $a|c$.

(3) $a|b$ and $a|c$ imply that $a|(bx + cy)$ for any integers x, y .

(4) $a|b$ and $b|a$ imply that $a = \pm b$.

(5) If $a|b$ and $a > 0, b > 0$ then $a \leq b$.

(6) $a|b$ if and only if $ca|cb$ for any integer $c \neq 0$.

(7) $a|0$ for all $a \in \mathbb{Z}$ and $0|a$ only for $a = 0$.

(8) $a|\pm 1$ only for $a = \pm 1$.

(9) $a_1|b_1$ and $a_2|b_2$ imply that $a_1a_2|b_1b_2$.

Proof We prove (2) and leave the remaining parts to the exercises.

Suppose $a|b$ and $b|c$. Then there exist x, y such that $b = ax$ and $c = by$. But then $c = axy = a(xy)$ and therefore $a|c$. \square

If b, c, x, y are integers then an integer $bx + cy$ is called a **linear combination** of b, c . Thus part (3) of Theorem 2.2.1 says that if a is a **common divisor** of b, c then a divides any linear combination of b and c .

Further, note that if $b > 1$ is a composite then there exists $x > 0$ and $y > 0$ such that $b = xy$ and from part (5) we must have $1 < x < b, 1 < y < b$.

In ordinary arithmetic, given a, b we can always attempt to divide a into b . The next theorem, called the **division algorithm**, says that if $a > 0$ either a will divide b or the **remainder** of the division of b by a will be less than a .

Theorem 2.2.2 (Division Algorithm) Given integers a, b with $a > 0$ then there exist unique integers q and r such that $b = qa + r$ where either $r = 0$ or $0 < r < a$.

One may think of q and r as the **quotient** and **remainder**, respectively, when dividing b by a .

Proof Given a, b with $a > 0$ consider the set

$$S = \{b - qa \geq 0; q \in \mathbb{Z}\}.$$

If $b > 0$ then $b + a > 0$ and the sum is in S . If $b \leq 0$ then there exists a $q > 0$ with $-qa < b$. Then $b + qa > 0$ and is in S . Therefore, in either case S is nonempty. Hence S is a nonempty subset of $\mathbb{N} \cup \{0\}$ and therefore has a least element r . If $r \neq 0$ we must show that $0 < r < a$. Suppose $r \geq a$, then $r = a + x$ with $x \geq 0$ and $x < r$ since $a > 0$. Then $b - qa = r = a + x \implies b - (q + 1)a = x$. This means that $x \in S$. Since $x < r$ this contradicts the minimality of r which is a contradiction. Therefore, if $r \neq 0$ it follows that $0 < r < a$.

The only thing left is to show the uniqueness of q and r . Suppose $b = q_1a + r_1$ also. By the construction above r_1 must also be the minimal element of S . Hence $r_1 \leq r$ and $r \leq r_1$ so $r = r_1$. Now

$$b - qa = b - q_1a \implies (q_1 - q)a = 0$$

but since $a > 0$ it follows that $q_1 - q = 0$ so that $q = q_1$. \square

The next ideas that are necessary are the concepts of **greatest common divisor** and **least common multiple**.

Definition 2.2.2 Given nonzero integers a, b their **greatest common divisor** or **GCD** $d > 0$ is a positive integer which is a common divisor, that is, $d|a$ and $d|b$, and if d_1 is any other common divisor then $d_1|d$. We denote the greatest common divisor of a, b by either $\gcd(a, b)$ or (a, b) .

The next result says that given any nonzero integers they do have a greatest common divisor and it is unique.

Theorem 2.2.3 Given nonzero integers a, b their GCD exists, is unique, and can be characterized as the least positive linear combination of a and b .

Proof Given nonzero a, b consider the set

$$S = \{ax + by > 0; x, y \in \mathbb{Z}\}$$

Now $a^2 + b^2 > 0$ so S is a nonempty subset of \mathbb{N} and hence has a least element $d > 0$. We show that d is the GCD.

First, we must show that d is a common divisor. Now $d = ax + by$ and is the least such positive linear combination. By the division algorithm $a = qd + r$ with $0 \leq r < d$. Suppose $r \neq 0$. Then $r = a - qd = a - q(ax + by) = (1 - qx)a - qby > 0$. Hence r is a positive linear combination of a and b and therefore is in S . But then $r < d$ contradicting the minimality of d in S . It follows that $r = 0$ and so $a = qd$ and $d|a$. An identical argument shows that $d|b$ and so d is a common divisor of a and b . Let d_1 be any other common divisor of a and b . Then d_1 divides any linear combination of a and b and so $d_1|d$. Therefore, d is the GCD of a and b .

Finally, we must show that d is unique. Suppose d_1 is another GCD of a and b . Then $d_1 > 0$ and d_1 is a common divisor of a, b . Then $d_1|d$ since d is a GCD. Identically $d|d_1$ since d_1 is a GCD. Therefore, $d = \pm d_1$ and then $d = d_1$ since they are both positive. \square

We note that as a consequence of Theorem 2.2.3 that if a, b, k are nonzero integers then the equation $ax + by = k$ has integer solutions x, y if and only if (a, b) divides k .

If $(a, b) = 1$ then we say that a, b are **relatively prime** or **coprime**. It follows that a and b are relatively prime if and only if 1 is expressible as a linear combination of a and b . We need the following three results:

Lemma 2.2.1 *If $d = (a, b)$ then $a = a_1d$ and $b = b_1d$ with $(a_1, b_1) = 1$.*

Proof If $d = (a, b)$ then $d|a$ and $d|b$. Hence $a = a_1d$ and $b = b_1d$. We have

$$d = ax + by = a_1dx + b_1dy.$$

Dividing both sides of the equation by d we obtain

$$1 = a_1x + b_1y.$$

Therefore, $(a_1, b_1) = 1$. □

Lemma 2.2.2 *For any integer c we have that $(a, b) = (a, b + ac)$.*

Proof Suppose $(a, b) = d$ and $(a, b + ac) = d_1$. Now d is the least positive linear combination of a and b . Suppose $d = ax + by$. d_1 is a linear combination of $a, b + ac$ so that

$$d_1 = ar + (b + ac)s = a(cs + r) + bs.$$

Hence d_1 is also a linear combination of a and b and therefore $d_1 \geq d$. On the other hand, $d_1|a$ and $d_1|(b + ac)$ and so $d_1|b$. Therefore, $d_1|d$ so $d_1 \leq d$. Combining these we must have $d_1 = d$. □

From this we easily see that $(a, b) = a$ if a, b are nonzero integers with $a|b$.

The next result, called the **Euclidean algorithm**, provides a technique for both finding the GCD of two integers and expressing the GCD as a linear combinations.

Theorem 2.2.4 (The Euclidean Algorithm) *Given integers b and $a > 0$ with $a \nmid b$ form the repeated divisions*

$$b = q_1a + r_1, 0 < r_1 < a$$

$$a = q_2r_1 + r_2, 0 < r_2 < r_1$$

...

$$r_{n-2} = q_nr_{n-1} + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1}r_n.$$

The last nonzero remainder r_n is the GCD of a, b . Further r_n can be expressed as a linear combination of a and b by successively eliminating the r_i 's in the intermediate equations.

Proof In taking the successive divisions as outlined in the statement of the theorem each remainder r_i gets strictly smaller and still nonnegative. Hence it must finally

end with a zero remainder. Therefore, there is a last nonzero remainder r_n . We must show that this is the GCD.

Now from Lemma 2.2.2, the GCD satisfies

$$(a, b) = (a, b - q_1a) = (a, r_1) = (r_1, a - q_2r_1) = (r_1, r_2).$$

Continuing in this manner we have then that $(a, b) = (r_{n-1}, r_n) = r_n$ since r_n divides r_{n-1} . This shows that r_n is the GCD.

To express r_n as a linear combination of a and b notice first that

$$r_n = r_{n-2} - q_nr_{n-1}.$$

Substituting this in the immediately preceding division we get

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) = (1 + q_nq_{n-1})r_{n-2} - q_nr_{n-3}.$$

Doing this successively, we ultimately express r_n as a linear combination of a and b . \square

EXAMPLE 2.2.1 Find the GCD of 270 and 2412 and express it as a linear combination of 270 and 2412.

We apply the Euclidean algorithm

$$2412 = (8)(270) + 252$$

$$270 = (1)(252) + 18$$

$$252 = (14)(18)$$

Therefore, the last nonzero remainder is 18 which is the GCD. We now must express 18 as a linear combination of 270 and 2412.

From the first equation

$$252 = 2412 - (8)(270)$$

which gives in the second equation

$$270 = (2412 - (8)(270)) + 18 \implies 18 = (-1)(2412) + (9)(270)$$

which is the desired linear combination.

Now suppose that $d = (a, b)$ where $a, b \in \mathbb{Z}$ and $a \neq 0, b \neq 0$. Then we note that given one integer solution of the equation

$$ax + by = d$$

we can easily obtain all solutions.

Suppose without loss of generality that $d = 1$, that is, a, b are relatively prime. If not we can divide through by $d > 1$. Suppose that x_1, y_1 and x_2, y_2 are two integer solutions of the equation $ax + by = 1$, that is,

$$ax_1 + by_1 = 1$$

$$ax_2 + by_2 = 1.$$

Then

$$a(x_1 - x_2) = -b(y_1 - y_2).$$

Since $(a, b) = 1$ we get from Lemma 2.2.3 that $b|(x_1 - x_2)$ and hence $x_2 = x_1 + bt$ for some $t \in \mathbb{Z}$. Substituting back into the equations, we then get

$$ax_1 + by_1 = a(x_1 + bt) + by_2 \implies by_1 = abt + by_2.$$

Therefore, $y_2 = y_1 - at$. Hence all solutions are given by

$$x_2 = x_1 + bt$$

$$y_2 = y_1 - at$$

for some $t \in \mathbb{Z}$.

The final idea of this section is that of a **least common multiple**.

Definition 2.2.3 Given nonzero integers a, b their **least common multiple** or **LCM** $m > 0$ is an positive integer which is a common multiple, that is, $a|m$ and $b|m$, and if m_1 is any other common multiple then $m|m_1$. We denote the least common multiple of a, b by either $\text{lcm}(a, b)$ or $[a, b]$.

As for GCD's given any nonzero integers they do have a least common multiple and it is unique. First, we need the following result known as **Euclid's Lemma**. In the next section, we will use a special case of this applied to primes. We note that this special case is traditionally also called Euclid's lemma.

Lemma 2.2.3 (Euclid's Lemma) Suppose $a|bc$ and $(a, b) = 1$, then $a|c$.

Proof Suppose $(a, b) = 1$ then 1 is expressible as a linear combination of a and b . That is,

$$ax + by = 1.$$

Multiply by c , so that

$$acx + bcy = c.$$

Now $a|a$ and $a|bc$ so a divides the linear combination $acx + bcy$ and hence $a|c$. \square

Theorem 2.2.5 *Given nonzero integers a, b their LCM exists and is unique. Further we have*

$$(a, b)[a, b] = ab.$$

Proof Let $d = (a, b)$ and let $m = |\frac{ab}{d}|$. We show that m is the LCM. Now $a = a_1d, b = b_1d$ with $(a_1, b_1) = 1$. Then $m = a_1b_1d$. Since $a = a_1d, m = b_1a$ so $a|m$. Identically, $b|m$ so m is a common multiple. Now let m_1 be another common multiple so that $m_1 = ax = by$. We then get

$$a_1dx = b_1dy \implies a_1x = b_1y \implies a_1|b_1y.$$

But $(a_1, b_1) = 1$ so from Lemma 2.2.3 $a_1|y$. Hence $y = a_1z$. It follows then that

$$m_1 = b_1d(a_1z) = a_1b_1dz = mz$$

and hence $m|m_1$. Therefore, m is an LCM.

The uniqueness follows in the same manner as the uniqueness of GCD's. Suppose m_1 is another LCM, then $m|m_1$ and $m_1|m$ so $m = \pm m_1$ and since they are both positive $m = m_1$. \square

EXAMPLE 2.2.2 Find the LCM of 270 and 2412.

From Example 2.2.1, we found that $(270, 2412) = 18$. Therefore,

$$[270, 2412] = \frac{(270)(2412)}{(270, 2412)} = \frac{(270)(2412)}{18} = 36180.$$

2.3 The Fundamental Theorem of Arithmetic

In this section, we prove the fundamental theorem of arithmetic which is really the most basic number theoretic result. This result says that any integer $n > 1$ can be decomposed into prime factors in essentially a unique manner. First, we show that there always exists such a decomposition into prime factors.

Lemma 2.3.1 *Any integer $n > 1$ can be expressed as a product of primes, perhaps with only one factor.*

Proof The proof is by induction. $n = 2$ is prime so its true at the lowest level. Suppose that every integer $2 \leq k < n$ can be decomposed into prime factors, we must show that n then also has a prime factorization.

If n is prime then we are done. Suppose then that n is composite. Hence $n = m_1m_2$ with $1 < m_1 < n, 1 < m_2 < n$. By the inductive hypothesis both m_1 and m_2 can be expressed as products of primes. Therefore, n can also use the primes from m_1 and m_2 , completing the proof. \square

Before we continue to the fundamental theorem, we mention that this result can be used to prove that the set of primes is infinite. The proof we give goes back to Euclid and is quite straightforward. In the next chapter, we will present a whole collection of proofs, some quite complicated also show that the primes are an infinite set. Each of these other proofs will shed more light however on the nature of the integers.

Theorem 2.3.1 *There are infinitely many primes.*

Proof Suppose that there are only finitely many primes p_1, \dots, p_n . Each of these is positive so we can form the positive integer

$$N = p_1 p_2 \cdots p_n + 1.$$

From Lemma 2.3.1, N has a prime decomposition. In particular, there is a prime p which divides N . Then

$$p | (p_1 p_2 \cdots p_n + 1).$$

Since the only primes are assumed p_1, p_2, \dots, p_n it follows that $p = p_i$ for some $i = 1, \dots, n$. But then $p | p_1 p_2 \cdots p_i \cdots p_n$ so p cannot divide $p_1 \cdots p_n + 1$ which is a contradiction. Therefore, p is not one of the given primes showing that the list of primes must be endless. \square

A variation of Euclid's argument gives the following proof of Theorem 2.3.1. Suppose there are only finitely many primes p_1, \dots, p_n . Certainly $n \geq 2$. Let $P = \{p_1, \dots, p_n\}$. Divide P into two disjoint nonempty subsets P_1, P_2 . Now consider the number $m = q_1 + q_2$ where q_1 is a product of primes from P_1 and q_2 is a product of primes from P_2 . Let p be a prime divisor of m . Since $p \in P$ it follows that p divides either q_1 or q_2 but not both. But then p does not divide m a contradiction. Therefore, p is not one of the given primes and the number of primes must be infinite.

Although there are infinitely many primes, a glance at the list of primes, shows that they appear to become scarcer as the integers get larger. If we let

$$\pi(x) = \text{number of primes} \leq x$$

a basic question is what is the asymptotic behavior of this function. This question is the basis of the prime number theorem which will be discussed in Chapter 4. However, it is easy to show that there are arbitrarily large spaces or gaps within the set of primes.

Theorem 2.3.2 *Given any positive integer k there exists k consecutive composite integers.*

Proof Consider the sequence

$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k + 1.$$

Suppose n is an integer with $2 \leq n \leq k+1$. Then $n | ((k+1)! + n)$. Hence each of the integers in the above sequence is composite. \square

To show the uniqueness of the prime decomposition we need Euclid's Lemma, from the previous section, applied to primes.

Lemma 2.3.2 (Euclid's Lemma) *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

Proof Suppose $p|ab$. If p does not divide a then clearly a and p must be relatively prime, that is, $(a, p) = 1$. Then from Lemma 2.2.3, $p|b$. \square

We now state and prove the **fundamental theorem of arithmetic**.

Theorem 2.3.3 (The Fundamental Theorem of Arithmetic) *Given any integer $n \neq 0$ there is a factorization*

$$n = cp_1p_2 \cdots p_k$$

where $c = \pm 1$ and p_1, \dots, p_n are primes. Further this factorization is unique up to the ordering of the factors.

Proof We assume that $n \geq 1$. If $n \leq -1$ we use $c = -1$ and the proof is the same. We define the product of no primes, that is, when $k = 0$, to be 1. Then the statement certainly holds for $n = 1$ with $k = 0$. Now suppose $n > 1$. From Lemma 2.3.1, n has a prime decomposition

$$n = p_1p_2 \cdots p_m.$$

We must show that this is unique up to the ordering of the factors. Suppose then that n has another such factorization $n = q_1q_2 \cdots q_k$ with the q_i all prime. We must show that $m = k$ and that the primes are the same. Now we have

$$n = p_1p_2 \cdots p_m = q_1 \cdots q_k$$

Assume that $k \geq m$. Then it follows that $p_1|q_1q_2 \cdots q_k$. From Lemma 2.3.2, then we must have that $p_1|q_i$ for some i . But q_i is prime and $p_1 > 1$ so it follows that $p_1 = q_i$. Therefore, we can eliminate p_1 and q_i from both sides of the factorization to obtain

$$p_2 \cdots p_m = q_1 \cdots q_{i-1}q_{i+1} \cdots q_k.$$

Continuing in this manner, we can eliminate all the p_i from the left side of the factorization to obtain

$$1 = q_{i_1} \cdots q_{i_t}, \text{ with } t = k - m$$

If q_{i_1}, \dots, q_{i_t} were primes this would be impossible. Therefore, $m = k$ and each prime p_i was included in the primes q_1, \dots, q_m and vice versa. Therefore, the factorizations differ only in the order of the factors, proving the theorem. \square

For any positive integer $n > 1$ we can combine all the same primes to write

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \text{ with } p_1 < p_2 < \cdots < p_k.$$

This is called the **standard prime decomposition**. Note that given any two positive integers a, b we can always write the prime decomposition with the **same** primes by allowing a zero exponent.

There are several easy consequences of the fundamental theorem.

Theorem 2.3.4 *Let a, b be positive integers > 1 . Suppose*

$$a = p_1^{e_1} \cdots p_k^{e_k}$$

$$b = p_1^{f_1} \cdots p_k^{f_k}$$

where we include zero exponents for noncommon primes. Then

$$(a, b) = p_1^{\min(e_1, f_1)} \cdot p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

$$[a, b] = p_1^{\max(e_1, f_1)} \cdot p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

Corollary 2.3.1 *Let a, b be positive integers > 1 , then $(a, b)[a, b] = ab$.*

We leave the proofs to the exercises but give an example.

EXAMPLE 2.3.1 Find the standard prime decompositions of 270 and 2412 and use them to find the GCD and LCM.

Recall that we found the GCD and LCM of these numbers in the previous section using the Euclidean algorithm. We note that in general it is very difficult as the size gets larger to determine the actual prime decomposition or even whether it is a prime or not. We will discuss primality testing in Chapter 5.

To find the prime decomposition we factor and then continue refactoring until there are only prime factors.

$$270 = (27)(10) = 3^3 \cdot 2 \cdot 5 = 2 \cdot 3^3 \cdot 5$$

which is the standard prime decomposition of 270.

$$2412 = 4 \cdot 603 = 4 \cdot 3 \cdot 201 = 4 \cdot 3 \cdot 3 \cdot 67 = 2^2 \cdot 3^2 \cdot 67$$

which is the standard prime decomposition of 2412. Hence we have

$$270 = 2 \cdot 3^3 \cdot 5 \cdot 67^0$$

$$2412 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 67$$

$$\implies (a, b) = 2 \cdot 3^2 \cdot 5^0 \cdot 67^0 = 2 \cdot 3^2 = 18$$

and

$$[a, b] = 2^2 \cdot 3^3 \cdot 5 \cdot 67 = 36180.$$

Note that the fundamental theorem of arithmetic can be extended to the rational numbers. Suppose $r = \frac{a}{b}$ with $a > 0$, $b \neq 0$ is a positive rational. Then

$$r = \frac{p_1^{e_1} \cdots p_k^{e_k}}{p_1^{f_1} \cdots p_k^{f_k}} = p_1^{e_1 - f_1} \cdots p_k^{e_k - f_k}.$$

Therefore, any positive rational has a standard prime decomposition

$$p_1^{t_1} \cdots p_k^{t_k} \text{ where } t_1, \dots, t_k \text{ are integers.}$$

So, for example,

$$\frac{15}{49} = 3 \cdot 5 \cdot 7^{-2}.$$

This has the following interesting consequence.

Lemma 2.3.3 *If a is an integer which is not a perfect n th power then the n th root of a is irrational.*

Proof This result says, for example, that if an integer is not a perfect square then its square root is irrational. The fact that the square root of 2 is irrational was known to the Greeks.

Suppose b is an integer with standard prime decomposition

$$b = p_1^{e_1} \cdots p_k^{e_k}.$$

Then

$$b^n = p_1^{ne_1} \cdots p_k^{ne_k}$$

and this must be the standard prime decomposition for b^n . It follows that an integer a is an n th power if and only if it has a standard prime decomposition

$$a = q_1^{f_1} \cdots q_t^{f_t} \text{ with } n \mid f_i \text{ for every } i.$$

Suppose a is not an n th power then

$$a = q_1^{f_1} \cdots q_t^{f_t}$$

where n does not divide f_i for some i . Taking the n th root

$$a^{1/n} = q_1^{f_1/n} \cdots q_i^{f_i/n} \cdots q_t^{f_t/n}$$

But f_i/n is not an integer so $a^{1/n}$ cannot be rational by the extension of fundamental theorem to rationals. \square

While induction and least well-ordering characterize the integers, unique factorization into primes does not. We close this section with a brief further discussion of unique factorization.

The concept of divisor and factor can be extended to any ring. $a|b$ is a ring R if there is a $c \in R$ with $b = ac$. We will restrict ourselves to integral domains. A **unit** in an integral domain is an element e with a multiplicative inverse. This means that there is an element e_1 in R with $ee_1 = 1$. Thus the only units in \mathbb{Z} are ± 1 . Two elements r, r_1 of an integral domain are **associates** if $r = er_1$ for some unit e . A **prime** in a general integral domain is an element whose only divisors are associates of itself or units. With these definitions, we can talk about factorization into primes.

We say that an integral domain D is a **unique factorization domain** or **UFD** if for each $d \in D$ then either $d = 0$, d is a unit or d has a factorization into primes which is unique up to ordering and unit factors. This means that if

$$r = p_1 \cdots p_m = q_1 \cdots q_k$$

then $m = k$ and each p_i is an associate of some q_j .

The fundamental theorem of arithmetic in more general algebraic language says that the integers \mathbb{Z} are a unique factorization domain. However, they are far from being the only one. In the exercises, we outline a proof of the following.

Theorem 2.3.5 *Let F be a field and $F[x]$ the ring of polynomials in one variable over F . Then $F[x]$ is a UFD.*

This theorem is actually a special case of something even more general. An integral domain D is called a **Euclidean domain** if there exists a function $N : D \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ satisfying:

For each $a, b \in D$, $a \neq 0$ there exists $q, r \in D$ such that

$$b = aq + r \text{ and either } r = 0 \text{ or } r \neq 0 \text{ and } N(r) < N(a).$$

Theorem 2.3.6 *Any Euclidean domain is a UFD.*

The proof of this essentially mimics the proof for the integers. See the exercises.

The **Gaussian integers** $\mathbb{Z}[i]$ are the complex numbers $a + bi$ where a, b are integers.

Lemma 2.3.4 *The integer \mathbb{Z} , the Gaussian integers $\mathbb{Z}[i]$, and the ring of polynomials $F[x]$ over a field F are all Euclidean domains.*

Corollary 2.3.2 *$\mathbb{Z}[i]$ and $F[x]$ with F , a field, are UFDs.*

Proofs of these results will be given in Chapter 6.

2.4 Congruences and Modular Arithmetic

Gauss based much of his number theoretical investigations around the theory of congruences. As we will see a **congruence** is just a statement about divisibility put into a more formal framework. In this section and the remainder of the chapter, we will consider congruences and in particular the solution of polynomial congruences. First, we give the basic definitions and properties.

2.4.1 Basic Theory of Congruences

Definition 2.4.1 Suppose m is a positive integer. If x, y are integers such that $m|(x - y)$ we say that x is **congruent to y modulo m** and denote this by $x \equiv y \pmod{m}$. If m does not divide $x - y$ then x and y are **incongruent modulo m** .

If $x \equiv y \pmod{m}$ then y is called a **residue** of x modulo m . Given $x \in \mathbb{Z}$ the set of integers $\{y \in \mathbb{Z}; x \equiv y \pmod{m}\}$ is called the **residue class** for x modulo m . We denote this by $[x]$. Notice that $x \equiv 0 \pmod{m}$ is equivalent to $m|x$. We first show that the residue classes partition \mathbb{Z} , that is, each integer falls in one and only one residue class.

Theorem 2.4.1 Given $m > 0$ then congruence modulo m is an equivalence relation on the integers. Therefore, the residue classes partition the integers.

Proof Recall that a relation \sim on a set S is an **equivalence relation** if it is **reflexive**, that is, $s \sim s$ for all $s \in S$; **symmetric**, that is, if $s_1 \sim s_2$ then $s_2 \sim s_1$; and **transitive**, that is, if $s_1 \sim s_2$ and $s_2 \sim s_3$ then $s_1 \sim s_3$. If \sim is an equivalence relation then the equivalence classes $[s] = \{s_1 \in S; s_1 \sim s\}$ partition S .

Consider $\equiv \pmod{m}$ on \mathbb{Z} . Given $x \in \mathbb{Z}$, $x - x = 0 = 0 \cdot m$ so $m|(x - x)$ and $x \equiv x \pmod{m}$. Therefore, $\equiv \pmod{m}$ is reflexive.

Suppose $x \equiv y \pmod{m}$ then $m|(x - y) \implies x - y = am$ for some $a \in \mathbb{Z}$. Then $y - x = -am$ so $m|(y - x)$ and $y \equiv x \pmod{m}$. Therefore, $\equiv \pmod{m}$ is symmetric.

Finally suppose $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$. Then $x - y = a_1m$ and $y - z = a_2m$. But then $x - z = (x - y) + (y - z) = a_1m + a_2m = (a_1 + a_2)m$. Therefore, $m|(x - z)$ and $x \equiv z \pmod{m}$. Therefore, $\equiv \pmod{m}$ is transitive and the theorem is proved. \square

Hence given $m > 0$ every integer falls into one and only one residue class. We now show that there are exactly m residue classes modulo m .

Theorem 2.4.2 Given $m > 0$ there exist exactly m residue classes. In particular,

$$[0], [1], \dots, [m - 1]$$

gives a complete set of residue classes.

Proof We show that given $x \in \mathbb{Z}$, x must be congruent modulo m to one of $0, 1, 2, \dots, m-1$. Further none of these are congruent modulo m . As a consequence

$$[0], [1], \dots, [m-1]$$

give a complete set of residue classes modulo m and hence there are m of them.

To see these assertions suppose $x \in \mathbb{Z}$. By the division algorithm, we have

$$x = qm + r \text{ where } 0 \leq r < m$$

This implies that $r = x - qm$ or in terms of congruences that $x \equiv r \pmod{m}$. Therefore, x is congruent to one of the sets $\{0, 1, 2, \dots, m-1\}$.

Suppose $0 \leq r_1 < r_2 < m$. Then $m \nmid r_2 - r_1$ so r_1 and r_2 are incongruent modulo m . Therefore, every integer is congruent to one and only one of $0, 1, \dots, m-1$, and hence $[0], [1], \dots, [m-1]$ give a complete set of residue classes modulo m . \square

There are many sets of complete residue classes modulo m . In particular, a set of m integers x_1, x_2, \dots, x_m will comprise a **complete residue system** modulo m if $x_i \not\equiv x_j \pmod{m}$ unless $i = j$. Given one complete residue system, it is easy to get another.

Lemma 2.4.1 *If $\{x_1, \dots, x_m\}$ form a complete residue system modulo m and $(a, m) = 1$ then $\{ax_1, \dots, ax_m\}$ also comprise a complete residue system.*

Proof Suppose $ax_i \equiv ax_j \pmod{m}$. Then $m \mid a(x_i - x_j)$. Since $(a, m) = 1$ then by Euclid's lemma $m \mid (x_i - x_j)$ and hence $x_i \equiv x_j \pmod{m}$. \square

Finally, we will need the following:

Lemma 2.4.2 *If $x \equiv y \pmod{m}$ then $(x, m) = (y, m)$.*

Proof Suppose $x - y = am$ then any common divisor of x and m is also a common divisor of y . From this the result is immediate. \square

2.4.2 The Ring of Integers Mod N

Perhaps the easiest way to handle results on congruences is to place them in the framework of abstract algebra. To do this we construct, for each $n > 0$ a ring, called the **ring of integers modulo n** . We will follow this approach. However we note, that although this approach simplifies and clarifies many of the proofs, historically purely number theoretical proofs were given. Often these purely number theoretical proofs inspired the algebraic proofs.

To construct this ring, we first need the following:

Lemma 2.4.3 *If $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then*

1. $a + c \equiv b + d \pmod n$
2. $ac \equiv bd \pmod n$

Proof Suppose $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a - b = q_1n$ and $c - d = q_2n$ for some integers q_1, q_2 . This implies that $(a + c) - (b + d) = (q_1 + q_2)n$ or that $n \mid ((a + c) - (b + d))$. Therefore, $a + c \equiv b + d \pmod n$.

We leave the proof of (2) to the exercises. \square

We now define operations on the set of residue classes.

Definition 2.4.2 *Consider a complete residue system x_1, \dots, x_n modulo n . On the set of residue classes $[x_1], \dots, [x_n]$ define*

1. $[x_i] + [x_j] = [x_i + x_j]$
2. $[x_i][x_j] = [x_i x_j]$

Theorem 2.4.3 *Given a positive integer $n > 0$, the set of residue classes forms a commutative ring with an identity under the operations defined in Definition 2.4.2. This is called the **ring of integers modulo n** and is denoted by \mathbb{Z}_n . The zero element is $[0]$ and the identity element is $[1]$.*

Proof Notice that from Lemma 2.4.3, it follows that these operations are well-defined on the set of residue classes, that is, if we take two different representatives for a residue class, the operations are still the same.

To show \mathbb{Z}_n is a commutative ring with an identity we must show that it satisfies, relative to the defined operations, all the ring properties. Basically, \mathbb{Z}_n inherits these properties from \mathbb{Z} . We show commutativity of addition and leave the other properties to the exercises.

Suppose $[a], [b] \in \mathbb{Z}_n$. Then

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

where $[a + b] = [b + a]$ since addition is commutative in \mathbb{Z} . \square

This theorem is actually a special case of a general result in abstract algebra. In the ring of integers \mathbb{Z} the set of multiples of an integer n forms an ideal (see [A] for terminology) which is usually denoted $n\mathbb{Z}$. The ring \mathbb{Z}_n is the **quotient ring** of \mathbb{Z} modulo the ideal $n\mathbb{Z}$, that is, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

We usually consider \mathbb{Z}_n as consisting of $0, 1, \dots, n - 1$ with addition and multiplication **modulo n** . When there is no confusion we will denote the element $[a]$ in \mathbb{Z}_n just as a . Below we give the addition and multiplication table modulo 5, that is, in \mathbb{Z}_5 .

EXAMPLE 2.4.2.1 Addition and Multiplication Tables for \mathbb{Z}_5

+	0	1	2	3	4	.	0	1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

Notice, for example, that modulo 5, $3 \cdot 4 = 12 \equiv 2 \pmod{5}$ so that in \mathbb{Z}_5 , $3 \cdot 4 = 2$. Similarly, $4 + 2 = 6 \equiv 1 \pmod{5}$ so in \mathbb{Z}_5 , $4 + 2 = 1$.

The question arises as to when the commutative ring \mathbb{Z}_n is an integral domain and when is \mathbb{Z}_n a field. The answer is when n is a prime and only when n is a prime.

Theorem 2.4.4 (1) \mathbb{Z}_n is an integral domain if and only if n is a prime.

(2) \mathbb{Z}_n is a field if and only if n is a prime.

Proof Since \mathbb{Z}_n is a commutative ring with an identity for any n it will be an integral domain if and only if it has no zero divisors.

Suppose first that n is a prime and suppose that $ab = 0$ in \mathbb{Z}_n . Then in \mathbb{Z} we have

$$ab \equiv 0 \pmod{n} \implies n|ab.$$

Since n is prime, by Euclid's lemma $n|a$ or $n|b$. In terms of congruences then

$$a \equiv 0 \pmod{n} \implies a = 0 \text{ in } \mathbb{Z}_n \text{ or } b \equiv 0 \pmod{n} \implies b = 0 \text{ in } \mathbb{Z}_n$$

Therefore, \mathbb{Z}_n is an integral domain if n is prime.

Suppose n is not prime. Then $n = m_1 m_2$ with $1 < m_1 < n$, $1 < m_2 < n$. Then $n \nmid m_1$, $n \nmid m_2$ but $n|m_1 m_2$. Translating this into \mathbb{Z}_n , we have

$$m_1 m_2 = 0 \text{ but } m_1 \neq 0 \text{ and } m_2 \neq 0.$$

Therefore, \mathbb{Z}_n is not an integral domain if n is not prime. These prove part (1).

Since a field is an integral domain, \mathbb{Z}_n cannot be a field unless n is prime. To complete part (2), we must show that if n is prime then \mathbb{Z}_n is a field. Suppose n is prime, since \mathbb{Z}_n is a commutative ring with identity to show that it's a field we must show that each nonzero element has a multiplicative inverse.

Suppose $a \in \mathbb{Z}_n$, $a \neq 0$. Then in \mathbb{Z} we have $n \nmid a$ and hence since n is prime $(a, n) = 1$. Therefore, in \mathbb{Z} there exists x, y such that $ax + ny = 1$. In terms of congruences this says that

$$ax \equiv 1 \pmod{n}$$

or in \mathbb{Z}_n ,

$$ax = 1.$$

Therefore, a has an inverse in \mathbb{Z}_n and hence \mathbb{Z}_n is a field. □

The proof of the last theorem actually indicates a method to find the multiplicative inverse of an element modulo a prime. Suppose n is a prime and $a \neq 0$ in \mathbb{Z}_n . Use the Euclidean algorithm in \mathbb{Z} to express 1 as a linear combination of a and n , that is,

$$ax + ny = 1.$$

The residue class for x will be the multiplicative inverse of a .

EXAMPLE 2.4.2.2 Find 6^{-1} in \mathbb{Z}_{11} .

Using the Euclidean algorithm

$$11 = 1 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$\implies 1 = 6 - (1 \cdot 5) = 6 - (1 \cdot (11 - 1 \cdot 6)) \implies 1 = 2 \cdot 6 - 1 \cdot 11.$$

Therefore, the inverse of 6 modulo 11 is 2, that is, in \mathbb{Z}_{11} , $6^{-1} = 2$.

EXAMPLE 2.4.2.3 Solve the linear equation

$$6x + 3 = 1$$

in \mathbb{Z}_{11} .

Using purely formal field algebra, the solution is

$$x = 6^{-1}(1 - 3).$$

In \mathbb{Z}_{11} we have

$$1 - 3 = -2 = 9 \text{ and } 6^{-1} = 2 \implies x = 2 \cdot 9 = 18 = 7.$$

Therefore, the solution in \mathbb{Z}_{11} is $x = 7$. A quick check shows that

$$6 \cdot 7 + 3 = 42 + 3 = 45 = 1 \text{ in } \mathbb{Z}_{11}.$$

A linear equation in \mathbb{Z}_{11} is called a **linear congruence** modulo 11. We will discuss solutions of such congruences in Section 2.5.

The fact that \mathbb{Z}_p is a field for p a prime leads to the following nice result known as **Wilson's theorem**.

Theorem 2.4.5 (*Wilson's Theorem*) *If p is a prime then*

$$(p - 1)! \equiv -1 \text{ mod } p.$$

Proof Now $(p-1)! = (p-1)(p-2) \cdots 1$. Since \mathbb{Z}_p is a field each $x \in \{1, 2, \dots, p-1\}$ has a multiplicative inverse modulo p . Further suppose $x = x^{-1}$ in \mathbb{Z}_p . Then $x^2 = 1$ which implies $(x-1)(x+1) = 0$ in \mathbb{Z}_p and hence either $x = 1$ or $x = -1$ since \mathbb{Z}_p is an integral domain. Therefore, in \mathbb{Z}_p only 1, -1 are their own multiplicative inverses. Further $-1 = p-1$ since $p-1 \equiv -1 \pmod{p}$.

Hence in the product $(p-1)(p-2) \cdots 1$ considered in the field \mathbb{Z}_p each element is paired up with its distinct multiplicative inverse except 1 and $p-1$. Further the product of each with its inverse is 1. Therefore, in \mathbb{Z}_p we have $(p-1)(p-2) \cdots 1 = p-1$. Written as a congruence then

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

□

The converse of Wilson's theorem is also true, that is, if $(n-1)! \equiv -1 \pmod{n}$, then n must be a prime.

Theorem 2.4.6 *If $n > 1$ is a natural number and*

$$(n-1)! \equiv -1 \pmod{n}$$

then n is a prime.

Proof Suppose $(n-1)! \equiv -1 \pmod{n}$. If n were composite then $n = mk$ with $1 < m < n-1$ and $1 < k < n-1$. If $m \neq k$ then both m and k are included in $(n-1)!$. It follows that $(n-1)!$ is divisible by n so that $(n-1)! \equiv 0 \pmod{n}$ contradicting the assertion that $(n-1)! \equiv -1 \pmod{n}$. If $m = k \neq 2$ then $(n-1)! \equiv 0 \pmod{m}$ which is not congruent to $-1 \pmod{m}$. Therefore, n must be prime. If $m = k = 2$ then $n = 4$ and $(n-1)! = 6$ which is not congruent to $-1 \pmod{4}$. □

2.4.3 Units and the Euler Phi Function

In a field F every nonzero element has a multiplicative inverse. If R is a commutative ring with an identity, not necessarily a field, then a **unit** is any element with a multiplicative inverse. In this case its inverse is also a unit. For example, in the integers \mathbb{Z} the only units are ± 1 . The set of units in a commutative ring with identity form an abelian group under ring multiplication called the **unit group** of R . Recall that a **group** G is a set with one operation which is associative, has an identity for that operation, and such that each element has an inverse with respect to this operation. If the operation is also commutative then G is an **abelian group**.

Lemma 2.4.4 *If R is a commutative ring with an identity then the set of units in R form an abelian group under ring multiplication. This is called the **unit group** of R denoted $U(R)$.*

Proof The commutativity and associativity of $U(R)$ follow from the ring properties. The identity of $U(R)$ is the multiplicative identity of R while the ring multiplicative inverse for each unit is the group inverse. We must show that $U(R)$ is closed under ring multiplication. If $a \in R$ is a unit we denote its multiplicative inverse by a^{-1} . Now suppose $a, b \in U(R)$. Then a^{-1}, b^{-1} exist. It follows that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$

Hence ab has an inverse, namely $b^{-1}a^{-1}$ ($= a^{-1}b^{-1}$ in a commutative ring) and hence ab is also a unit. Therefore, $U(R)$ is closed under ring multiplication. \square

The proof of Theorem 2.4.4 actually provides a method to classify the units in any \mathbb{Z}_n .

Lemma 2.4.5 $a \in \mathbb{Z}_n$ is a unit if and only if $(a, n) = 1$.

Proof Suppose $(a, n) = 1$. Then there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. This implies that $ax \equiv 1 \pmod{n}$ which in turn implies that $ax = 1$ in \mathbb{Z}_n and therefore a is a unit.

Conversely, suppose a is a unit in \mathbb{Z}_n . Then there is an $x \in \mathbb{Z}_n$ with $ax = 1$. In terms of congruence then

$$ax \equiv 1 \pmod{n} \implies n \mid (ax - 1) \implies ax - 1 = ny \implies ax - ny = 1.$$

Therefore, 1 is a linear combination of a and n and so $(a, n) = 1$. \square

If a is a unit in \mathbb{Z}_n then a linear equation

$$ax + b = c$$

can always be solved with a unique solution given by $x = a^{-1}(c - b)$. Determining this solution is the same technique as in \mathbb{Z}_p with p a prime. If a is not a unit the situation is more complicated. We will consider this case in Section 2.5.

EXAMPLE 2.4.3.1

Solve $5x + 4 = 2$ in \mathbb{Z}_6 .

Since $(5, 6) = 1$, 5 is a unit in \mathbb{Z}_6 . Therefore, $x = 5^{-1}(2 - 4)$. Now $2 - 4 = -2 = 4$ in \mathbb{Z}_6 . Further $5 = -1$ so $5^{-1} = -1^{-1} = -1$. Then we have

$$x = 5^{-1}(2 - 4) = -1(4) = -4 = 2$$

Thus the unique solution in \mathbb{Z}_6 is $x = 2$.

Since an element a is a unit in \mathbb{Z}_n if and only if $(a, n) = 1$ it follows that the number of units in \mathbb{Z}_n is equal to the number of positive integers less than or equal to n and relatively prime to n . This number is given by the **Euler Phi Function**, our first look at a number theoretical function.

Definition 2.4.3 For any $n > 0$,

$\phi(n) =$ number of integers less than or equal to n and relatively prime to n .

EXAMPLE 2.4.3.2

$\phi(6) = 2$ since among 1, 2, 3, 4, 5, 6 only 1, 5 are relatively prime to 6.

The following is immediate from our characterization of units:

Lemma 2.4.6 The number of units in \mathbb{Z}_n , which is the order of the unit group $U(\mathbb{Z}_n)$, is $\phi(n)$.

Definition 2.4.4 Given $n > 0$ a **reduced residue system modulo n** is a set of integers x_1, \dots, x_k such that each x_i is relatively prime to n , $x_i \not\equiv x_j \pmod{n}$ unless $i = j$ and if $(x, n) = 1$ for some integer x then $x \equiv x_i \pmod{n}$ for some i .

Hence a reduced residue system is a complete collection of representatives of those residue classes of integers relatively prime to n . Hence it is a complete collection of units (up to congruence modulo n) in \mathbb{Z}_n . It follows that any reduced residue system modulo n has $\phi(n)$ elements.

EXAMPLE 2.4.3.3

A reduced residue system modulo 6 would be $\{1, 5\}$.

We now develop a formula for $\phi(n)$. As is the theme of this book, we first determine a formula for prime powers and then paste back together via the fundamental theorem of arithmetic.

Lemma 2.4.7 For any prime p and $m > 0$,

$$\phi(p^m) = p^m - p^{m-1} = p^m \left(1 - \frac{1}{p}\right).$$

Proof Recall that if $1 \leq a \leq p^m$ then either $a = p^k$ for some $k < m$ or $(a, p) = 1$. It follows that the positive integers less than p^m which are not relatively prime to p^m are precisely the multiples of p , that is, $p, 2p, 3p, \dots, p^{m-1}p$. All other positive $a < p^m$ are relatively prime to p^m . Hence the number of positive integers less than p^m and relatively prime to p^m is

$$p^m - p^{m-1}.$$

□

Lemma 2.4.8 If $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.

Proof Let $R_a = \{x_1, \dots, x_{\phi(a)}\}$ be a reduced residue system modulo a , $R_b = \{y_1, \dots, y_{\phi(b)}\}$ be a reduced residue system modulo b , and let

$$S = \{ay_i + bx_j; i = 1, \dots, \phi(b), j = 1, \dots, \phi(a)\}.$$

We claim that S is a reduced residue system modulo ab . Since S has $\phi(a)\phi(b)$ elements it will follow that $\phi(ab) = \phi(a)\phi(b)$.

To show that S is a reduced residue system modulo ab we must show three things: first, each $x \in S$ is relatively prime to ab ; second, the elements of S are distinct; and finally, given any integer n with $(n, ab) = 1$ then $n \equiv s \pmod{ab}$ for some $s \in S$.

Let $x = ay_i + bx_j$. Then since $(x_j, a) = 1$ and $(a, b) = 1$ it follows that $(x, a) = 1$. Analogously, $(x, b) = 1$. Since x is relatively prime to both a and b we have $(x, ab) = 1$. This shows that each element of S is relatively prime to ab .

Next suppose that

$$ay_i + bx_j \equiv ay_k + bx_l \pmod{ab}.$$

Then

$$ab \mid ((ay_i + bx_j) - (ay_k + bx_l)) \implies ay_i \equiv ay_k \pmod{b}.$$

Since $(a, b) = 1$ it follows that $y_i \equiv y_k \pmod{b}$. But then $y_i = y_k$ since R_b is a reduced residue system. Similarly, $x_j = x_l$. This shows that the elements of S are distinct modulo ab .

Finally, suppose $(n, ab) = 1$. Since $(a, b) = 1$ there exist x, y with $ax + by = 1$. Then

$$anx + bny = n.$$

Since $(x, b) = 1$ and $(n, b) = 1$ it follows that $(nx, b) = 1$. Therefore, there is an s_i with $nx = s_i + tb$. In the same manner $(ny, a) = 1$ and so there is an r_j with $ny = r_j + ua$. Then

$$\begin{aligned} a(s_i + tb) + b(r_j + ua) = n &\implies n = as_i + br_j + (t + u)ab \\ &\implies n \equiv as_i + br_j \pmod{ab} \end{aligned}$$

and we are done. □

We now give the general formula for $\phi(n)$.

Theorem 2.4.7 Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) = n \prod_i (1 - 1/p_i).$$

Proof From the previous lemma, we have

$$\begin{aligned} \phi(n) &= \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) \\ &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \end{aligned}$$

$$\begin{aligned}
&= p_1^{e_1}(1 - 1/p_1) \cdots p_k^{e_k}(1 - 1/p_k) = p_1^{e_1} \cdots p_k^{e_k} \cdot (1 - 1/p_1) \cdots (1 - 1/p_k) \\
&= n \prod_i (1 - 1/p_i).
\end{aligned}$$

□

EXAMPLE 2.4.3.4Determine $\phi(126)$. Now

$$126 = 2 \cdot 3^2 \cdot 7 \implies \phi(126) = \phi(2)\phi(3^2)\phi(7) = (1)(3^2 - 3)(6) = 36.$$

Hence there are 36 units in \mathbb{Z}_{126} .

An interesting result with many generalizations which we will look at later is the following.

Theorem 2.4.8 For $n > 1$ and for $d \geq 1$

$$\sum_{d|n} \phi(d) = n.$$

Proof As before we first prove the theorem for prime powers and then paste together via the fundamental theorem of arithmetic.

Suppose that $n = p^e$ for p a prime. Then the divisors of n are $1, p, p^2, \dots, p^e$, so

$$\sum_{d|n} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^e) = 1 + (p-1) + (p^2 - p) + \cdots + (p^e - p^{e-1}).$$

Notice that this sum telescopes, that is, $1 + (p-1) = p$, $p + (p^2 - p) = p^2$ and so on. Hence the sum is just p^e and the result is proved for n a prime power.

We now do an induction on the number of distinct prime factors of n . The above argument shows that the result is true if n has only one distinct prime factor. Assume that the result is true whenever an integer has less than k distinct prime factors and suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ has k distinct prime factors. Then $n = p^e c$ where $p = p_1$, $e = e_1$ and c has fewer than k distinct prime factors. By the inductive hypothesis,

$$\sum_{d|c} \phi(d) = c.$$

Since $(c, p) = 1$ the divisors of n are all of the form $p^\alpha d_1$ where $d_1|c$ and $\alpha = 0, 1, \dots, e$. It follows that

$$\sum_{d|n} \phi(d) = \sum_{d_1|c} \phi(c) + \sum_{d_1|c} \phi(pd_1) + \cdots + \sum_{d_1|c} \phi(p^e d_1)$$

Since $(d_1, p^\alpha) = 1$ for any divisor of c this sum equals

$$\begin{aligned}
&= \sum_{d_1|c} \phi(c) + \sum_{d_1|c} \phi(p)\phi(d_1) + \cdots + \sum_{d_1|c} \phi(p^e)\phi(d_1) \\
&= \sum_{d_1|c} \phi(c) + (p-1) \sum_{d_1|c} \phi(d_1) + \cdots + (p^e - p^{e-1}) \sum_{d_1|c} \phi(d_1) \\
&= c + (p-1)c + (p^2 - p)c + \cdots + (p^e - p^{e-1})c
\end{aligned}$$

As in the case of prime powers this sum telescopes giving a final result

$$= p^e c = n.$$

□

EXAMPLE 2.4.3.5

Consider $n = 10$. The divisors are 1, 2, 5, 10. Then $\phi(1) = 1$, $\phi(2) = 1$, $\phi(5) = 4$, $\phi(10) = 4$. Then

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10.$$

2.4.4 Fermat's Little Theorem and the Order of an Element

For any positive integer n the unit group $U(\mathbb{Z}_n)$ is a finite abelian group. Recall that in any group G each element $g \in G$ generates a **cyclic subgroup** consisting of all the distinct powers of g . If this cyclic subgroup is finite of order m then m is called the **order** of the element g . Equivalently, the order of an element $g \in G$ can be described as the least positive power m such that $g^m = 1$. If no such power exists then g has infinite order. We denote the order of the group G by $|G|$ and the order of $g \in G$ by $|g|$. If the whole group G is finite then each element clearly has finite order. We will apply these ideas to the unit group $U(\mathbb{Z}_n)$ but first we recall some further facts about finite groups.

Theorem 2.4.9 (*Lagrange's Theorem*) Suppose G is a finite group of order n . Then the order of any subgroup divides n . In particular, the order of any element divides the order of the group.

If $g \in G$ with $|G| = n$ then from Lagrange's theorem above there is an m with $g^m = 1$ and $m|n$. Hence $n = mk$ and so $g^n = g^{mk} = (g^m)^k = 1^k = 1$. Hence in any finite group, we have the following:

Corollary 2.4.1 If G is a finite group of order n and $g \in G$ then $g^n = 1$.

Theorem 2.4.10 Let G be a finite abelian group with $|G| = n$ then

1. if $g_1, g_2 \in G$ with $|g_1| = a$, $|g_2| = b$ then $(g_1 g_2)^{lcm(a,b)} = 1$,

2. if $g_1, g_2 \in G$ with $|g_1| = a, |g_2| = b$ and $(a, b) = 1$ then $|g_1 g_2| = ab$,
3. if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of n then

$$G = H_1 \times H_2 \times \cdots \times H_k$$

where $|H_i| = p_i^{e_i}$.

The third part of the last theorem is part of the **Fundamental Theorem for Finitely Generated Abelian Groups** which plays the same role in abelian group theory as the fundamental theorem of arithmetic does in number theory.

With these facts in hand, consider a unit $a \in \mathbb{Z}_n$. Then $a \in U(\mathbb{Z}_n)$ and hence a has a **multiplicative order**, that is, there is an integer m with $a^m = 1$ in \mathbb{Z}_n . In terms of congruences this means that $a^m \equiv 1 \pmod n$. If $a \in \mathbb{Z}_n$ is not a unit then there cannot exist a power $m \geq 1$ such that $a^m \equiv 1 \pmod n$ for if such an m existed then a^{m-1} would be an inverse for a .

Lemma 2.4.9 *Given $n > 0$ then for an integer a there exists an integer m such that $a^m \equiv 1 \pmod n$ if and only if $(a, n) = 1$ or equivalently a is a unit in \mathbb{Z}_n .*

Definition 2.4.5 *If $(a, n) = 1$ then the **order** of a modulo n is the least positive power m such that $a^m \equiv 1 \pmod n$. We will write $\text{order}(a)$ or alternatively $|a|$ or $|a|$ for the order of a . Equivalently, the order of a is the order of a considered as an element of the unit group $U(\mathbb{Z}_n)$.*

Since the order of $U(\mathbb{Z}_n) = \phi(n)$ we immediately get that the order of any element modulo n must divide $\phi(n)$.

Lemma 2.4.10 *If $(a, n) = 1$ then $\text{order}(a) | \phi(n)$.*

Applying Corollary 2.4.1 to the unit group $U(\mathbb{Z}_n)$ we get the following result, known as **Euler's theorem**.

Theorem 2.4.11 (*Euler's Theorem*) *If $(a, n) = 1$ then*

$$a^{\phi(n)} \equiv 1 \pmod n.$$

If $n = p$ a prime then any integer $a \not\equiv 0 \pmod p$ is a unit in \mathbb{Z}_p . Further $\phi(p) = p - 1$, and hence we obtain the next corollary which is called **Fermat's theorem**. (This is often called **Fermat's Little theorem** to distinguish it from the result on $x^n + y^n = z^n$.)

Corollary 2.4.2 *If p is a prime and $p \nmid a$ then*

$$a^{p-1} \equiv 1 \pmod p.$$

If $(a, n) = 1$ and the order of a is exactly $\phi(n)$ then a is called a **primitive root** modulo n . In this case, the unit group is cyclic with a as a generator. For $n = p$ a prime there is always a primitive root.

Theorem 2.4.12 *For a prime p there is always an element a of order $\phi(p) = p - 1$, that is, a primitive root. Equivalently, the unit group of \mathbb{Z}_p is always cyclic.*

Proof Since every nonzero element in \mathbb{Z}_p is a unit, the unit group $U(\mathbb{Z}_p)$ is precisely the multiplicative group of the field \mathbb{Z}_p . The fact that $U(\mathbb{Z}_p)$ is cyclic follows from the following more general result whose proof is also given. \square

Theorem 2.4.13 *Let F be a field. Then any finite subgroup of the multiplicative group of F must be cyclic.*

Proof Suppose $G \subset F$ is a finite multiplicative subgroup of the multiplicative group of F . Suppose $|G| = n$. As has been our general mode of approaching results we will prove it for n a power of a prime and then paste the result together via the fundamental theorem of arithmetic.

Suppose $n = p^k$ for some k . Then the order of any element in G is p^α with $\alpha \leq k$. Suppose the maximal order is p^t with $t < k$. Then the lcm of the orders is p^t . It follows that for every $g \in G$ we have $g^{p^t} = 1$. Therefore, every $g \in G$ is a root of the polynomial equation

$$x^{p^t} - 1 = 0.$$

However, over a field a polynomial cannot have more roots than its degree. Since G has $n = p^k$ elements and $p^t < p^k$, this is a contradiction. Therefore, the maximal order must be $p^k = n$. Therefore, G has an element of order $n = p^k$ and hence this element generates G and G must be cyclic.

We now do an induction on the number of distinct prime factors in $n = |G|$. The above argument handles the case where there is only one distinct prime factor. Assume the result is true if the order of G has less than k distinct prime factors. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$. Then $n = p^e c$ where c has less than k distinct prime factors. Since G is a finite abelian group with

$$|G| = n = p^e c \implies G = H \times K \text{ with } |H| = p^e, |K| = c.$$

By the inductive hypothesis, H and K are both cyclic so H has an element h of order p^e and K has an element k of order c . Since $(p^e, c) = 1$ the element hk has order $p^e c = n$ completing the proof. \square

EXAMPLE 2.4.4.1 Determine a primitive root modulo 7.

This is equivalent to finding a generator for the multiplicative group of \mathbb{Z}_7 . The nonzero elements are 1, 2, 3, 4, 5, 6 and we are looking for an element of order 6.

The table below list these elements and their orders

x	1	2	3	4	5	6
$ x $	1	3	6	3	6	2

Therefore, there are two primitive roots 3 and 5 modulo 7. To see how these were determined powers were taken modulo 7 until a value of 1 was obtained. For example,

$$3^2 = 9 = 2, 3^3 = 2 \cdot 3 = 6, 3^4 = 3 \cdot 6 = 18 = 4, 3^5 = 3 \cdot 4 = 12 = 5,$$

$$3^6 = 3 \cdot 5 = 15 = 1$$

EXAMPLE 2.4.4.2 Show that there is no primitive root modulo 15.

The units in \mathbb{Z}_{15} are $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Since $\phi(15) = 8$ we must show that there is no element of order 8. The table below gives the units and their respective orders.

x	1	2	4	7	8	11	13	14
$ x $	1	4	2	4	4	2	4	2

Therefore, there is no element of order 8.

Modulo a prime, there is always a primitive root but other integers can have primitive roots also. The fundamental result describing when an integer will have a primitive root is the following. We outline the proof in the exercises.

Theorem 2.4.14 *An integer n will have a primitive root modulo n if and only if*

$$n = 2, 4, p^k, 2p^k,$$

where p is a prime.

The order of an element, especially Fermat's theorem, provides a method for **primality testing**. Primality testing refers to determining for a given integer n whether it is prime or not. The simplest primality test is the following. If n were composite then $n = m_1 m_2$ with $1 < m_1 < n$, $1 < m_2 < n$. At least one of these factors must be $\leq \sqrt{n}$. Therefore, check all the integers less than or equal to the \sqrt{n} . If none of these divides n then n is prime. This can be improved using the fundamental theorem of arithmetic. If n has a divisor $\leq \sqrt{n}$ then it has a prime divisor $\leq \sqrt{n}$. It follows that in the above divisibility check, only the primes $\leq \sqrt{n}$ need be checked.

While this method always works it is often impractical for large n and other methods must be employed to see if a number is prime. By Fermat's theorem, if n were prime and $a < n$ then $a^{n-1} \equiv 1 \pmod{n}$. If a number a is found where this is not true then a cannot be prime. We give a trivial example.

EXAMPLE 2.4.4.3 Determine if 77 is prime.

If 77 were prime then $2^{76} \equiv 1 \pmod{77}$. Now

$$2^{76} = 2^{38 \cdot 2} = 4^{38}.$$

Now we do computations mod 77

$$\begin{aligned}
4^3 = 64 = -13 &\implies 4^6 = 169 = 15 \implies 4^{12} = 225 = 71 = -6 \\
\implies 4^{36} = (-6)^3 = -216 = -62 &\implies 4^{38} = 4^2(-62) = -992 = -68 \neq 1.
\end{aligned}$$

Therefore, 77 is not prime.

This method can determine if a number n is **not** prime however it cannot determine if it is prime. There are numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ is true for all $(a, n) = 1$ but n is not prime. These are called **pseudoprimes**. We will discuss primality testing further and in more detail in Chapter 5.

2.4.5 On Cyclic Groups

In the previous sections, we used some material from abstract algebra to prove results in number theory. Here we briefly reverse the procedure to use some number theory to develop and prove other ideas from algebra. After we do this we will turn the tables back again and use this algebra to give another proof of Theorem 2.4.8 on the Euler phi function.

Recall that a cyclic group G is a group with a single generator say g . We denote a cyclic group G with generator g by $\langle g \rangle$. The group G then consists of all the powers of g , that is, $G = \{1, g^{\pm 1}, g^{\pm 2}, \dots\}$. If G is finite of order n then $g^n = 1$ and n is the least positive integer x such that $g^x = 1$. It is then clear that if $g^m = 1$ for some power m it must follow that $m \equiv 0 \pmod{n}$, and if $g^k = g^l$ then $k \equiv l \pmod{n}$.

Let $H = (\mathbb{Z}_n, +)$ denote the additive subgroup of \mathbb{Z}_n . Then H is cyclic of order n with generator 1. If $G = \langle g \rangle$ is also cyclic of order n then since multiplication of group elements is done via addition of exponents, it is fairly straightforward that the homomorphism $f : G \rightarrow (\mathbb{Z}_n, +)$ given by $g \rightarrow 1$ is actually an isomorphism (see the exercises). Further if $G = \langle g \rangle$ is cyclic of infinite order then $g \rightarrow 1$ gives an isomorphism from G to the additive group of \mathbb{Z} .

Lemma 2.4.11 (1) If G is a finite cyclic group of order n then G is isomorphic to $(\mathbb{Z}_n, +)$. In particular all finite cyclic groups of a given order are isomorphic.

(2) If G is an infinite cyclic group then G is isomorphic to $(\mathbb{Z}, +)$.

Cyclic groups are abelian and hence their subgroups are also abelian. However as an almost direct consequence of the division algorithm, we get that any subgroup of a cyclic group must be cyclic.

Lemma 2.4.12 Let G be a cyclic group. Then any subgroup of G is also cyclic.

Proof Suppose $G = \langle g \rangle$ and $H \subset G$ is a subgroup. Since G consists of powers of g , H also consists of certain powers of g . Let k be the least positive integer such that $g^k \in H$. We show that $H = \langle g^k \rangle$, that is, H is the cyclic subgroup generated by g^k . This is clearly equivalent to showing that every $h \in H$ must be a power of g^k .

Suppose $g^t \in H$. We may assume that $t > 0$ and that $t > k$ since k is the least positive integer such that $g^k \in H$. If $t < 0$ work with $-t$. By the division algorithm, we then have

$$t = qk + r \text{ with } r = 0 \text{ or } 0 < r < k.$$

If $r \neq 0$ then $0 < r < k$ and $r = t - k$. Hence $g^r = g^{t-k} = g^t g^{-k}$. Now $g^t \in H$ and $g^k \in H$ and since H is a subgroup it follows that $g^{t-k} \in H$. But then $g^r \in H$ which is a contradiction since $0 < r < k$ and k is the least power of g in H . Therefore, $r = 0$ and $t = qk$. We then have

$$g^t = g^{qk} = (g^k)^q$$

completing the proof. \square

Each element of a cyclic group G generates its own cyclic subgroup. The question is when does this cyclic subgroup coincide with all of G . In particular, which powers g^k are generators of G . The answer is purely number theoretic.

Lemma 2.4.13 (1) Let $G = \langle g \rangle$ be a finite cyclic group of order n . Then g^k with $k > 0$ is a generator of G if and only if $(k, n) = 1$, that is, k and n are relatively prime.

(2) If $G = \langle g \rangle$ is an infinite cyclic group then g, g^{-1} are the only generators.

Proof Suppose first that $G = \langle g \rangle$ is finite cyclic of order n and suppose that $(k, n) = 1$. Then there exists integers x, y such that $kx + ny = 1$. It follows then that

$$g = g^1 = g^{kx+ny} = g^{kx} g^{ny} = (g^k)^x (g^n)^y.$$

But $g^n = 1$ so $(g^n)^y = 1$ and therefore

$$g = (g^k)^x.$$

Therefore, g is a power of g^k and hence every power of g is also a power of g^k . The whole group g then consists of powers of g^k and hence g^k is a generator for G .

Conversely, suppose that g^k is also a generator for G . Then there exists a power x such that $g = (g^k)^x = g^{kx}$. Hence $kx \equiv 1 \pmod{n}$ and so k is a unit mod n which implies from the last section that $(k, n) = 1$.

Suppose next that $G = \langle g \rangle$ is infinite cyclic. Then there is no power of g which is the identity. Suppose g^k is also a generator with $k > 1$. Then there exists a power x such that $g = (g^k)^x = g^{kx}$. But this implies that $g^{kx-1} = 1$ contradicting that no power of g is the identity. Hence $k = 1$. \square

Recall that $\phi(n)$ denotes the number of positive integers less than n which are relatively prime to n . This is then the number of generators of a cyclic group of order n .

Corollary 2.4.3 *Let G be a finite cyclic group of order n . Then there are $\phi(n)$ generators for G .*

By Lagrange's theorem (Theorem 2.4.9) for any finite group the order of a subgroup divides the order of a group, that is, if $|G| = n$ and $|H| = d$ with H a subgroup of G then $d|n$. However, the converse in general is not true, that is, if $|G| = n$ and $d|n$ there need not be a subgroup of order d . Further if there is a subgroup of order d there may or may not be other subgroups of order d . For a finite cyclic group G of order n however there is for each $d|n$ a **unique** subgroup of order d .

Theorem 2.4.15 *Let G be a finite cyclic group of order n . Then for each $d|n$ with $d \geq 1$ there exists a unique subgroup H of order d .*

Proof Let $G = \langle g \rangle$ and $|G| = n$. Suppose $d|n$, then $n = kd$. Consider the element g^k . Then $(g^k)^d = g^{kd} = g^n = 1$. Further if $0 < t < d$ then $0 < kt < kd$ so $kt \not\equiv 0 \pmod{n}$ and hence $g^{kt} = (g^k)^t \neq 1$. Therefore, d is the least power of g^k which is the identity and hence g^k has order d and generates a cyclic subgroup of order d . We must show that this is unique.

Suppose $H = \langle g^t \rangle$ is another cyclic subgroup of order d (recall that all subgroups of G are also cyclic). We may assume that $t > 0$ and we show that g^t is a power of g^k and hence the subgroups coincide. The proof is essentially the same as the proof of Lemma 2.4.12.

Since H has order d we have $g^{td} = 1$ which implies that $td \equiv 0 \pmod{n}$. Since $n = kd$ it follows that $t > k$. Apply the division algorithm

$$t = qk + r \text{ with } 0 \leq r < k.$$

If $r \neq 0$ then $0 < r < k$ and $r = t - qk$. Then

$$r = t - qk \implies rd = td - qkd \equiv 0 \pmod{n}.$$

Hence $n|rd$ which is impossible since $rd < kd = n$. Therefore, $r = 0$ and $t = qk$. From this

$$g^t = g^{qk} = (g^k)^q.$$

Therefore, g^t is a power of g^k and $H = \langle g^k \rangle$. □

We now use this result to give an alternate proof of Theorem 2.4.8.

Theorem 2.4.16 *For $n > 1$ and for $d \geq 1$*

$$\sum_{d|n} \phi(d) = n.$$

Proof Consider a cyclic group G of order n . For each $d|n$, $d \geq 1$ there is a unique cyclic subgroup H of order d . H then has $\phi(d)$ generators. Each element in G

generates its own cyclic subgroup H_1 , say of order d and hence must be included in the $\phi(d)$ generators of H_1 . Therefore,

$$\sum_{d|n} \phi(d) = \text{sum of the numbers of generators of the cyclic subgroups of } G.$$

But this must be the whole group and hence this sum is n . □

2.5 The Solution of Polynomial Congruences Modulo m

We are interested in solving **polynomial congruences** mod m . That is, solving polynomial equations

$$f(x) \equiv 0 \pmod{m}$$

where $f(x)$ is a nonzero polynomial with coefficients in \mathbb{Z}_m , the ring of integers modulo m . Typical examples might be

$$4x^2 + 3x - 2 \equiv 0 \pmod{12} \text{ or } 4x + 5 \equiv 0 \pmod{7}.$$

Of course the solution of such congruences is given in terms of residue classes for if $x \equiv y \pmod{m}$ then $f(x) \equiv f(y) \pmod{m}$. Hence if x is a solution to a polynomial congruence then so is every integer congruent to its modulo m .

As has been our general procedure, we will reduce the solution of polynomial congruences to the solution modulo primes and then try to paste general solutions back together via the fundamental theorem of arithmetic. Suppose then that m has the prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and that x_0 is a solution of $f(x) \equiv 0 \pmod{m}$. Then x_0 is also a solution of $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for $i = 1, \dots, k$. Then for each $i = 1, \dots, k$ there is a y_i with $x_0 \equiv y_i \pmod{p_i^{e_i}}$. Conversely, suppose we are given y_i with $f(y_i) \equiv 0 \pmod{p_i^{e_i}}$ for $i = 1, \dots, k$ then there is a technique based on what is called the **Chinese remainder theorem**, which we will discuss shortly, to piece these y_i together to get a solution x_0 of $f(x) \equiv 0 \pmod{m}$.

As a first step, we will describe the solution of linear congruences and the Chinese remainder theorem and then move on to higher degree congruences.

2.5.1 Linear Congruences and the Chinese Remainder Theorem

A **linear congruence** is of the form $ax + b \equiv 0 \pmod{m}$ where $a \not\equiv 0 \pmod{m}$. In this section, we will consider solutions of linear congruences.

Before proceeding further, we note that solving a polynomial congruence

$$f(x) \equiv 0 \pmod{m}$$

is essentially equivalent to solving a polynomial equation

$$f(x) = 0$$

in the modular ring \mathbb{Z}_m . The solutions of the congruence are precisely the congruence classes modulo m .

For example, the congruence

$$2x \equiv 4 \pmod{5}$$

is equivalent to the equation

$$2x = 4$$

in \mathbb{Z}_5 . The unique solution in \mathbb{Z}_5 is $x = 2$, so that the solution of the congruence is $x \equiv 2 \pmod{5}$. We will move freely between the two approaches to solving congruences, using \equiv for congruence mod m and $=$ for equality in \mathbb{Z}_m .

Now we consider the linear congruence $ax + b \equiv 0 \pmod{m}$ where a is noncongruent to $0 \pmod{m}$. For $m = p$, p a prime, the solution is immediate and it is unique. Since \mathbb{Z}_p is a field and $a \neq 0$ the element a has an inverse. Therefore, the solution in \mathbb{Z}_p is

$$x = a^{-1}(-b)$$

and any solution x_0 must be of the form $x_0 \equiv a^{-1}(-b) \pmod{p}$.

EXAMPLE 2.5.1.1 Solve $3x + 4 \equiv 0 \pmod{7}$.

From the formal field properties, the solution is $x = 3^{-1} \cdot (-4)$. In \mathbb{Z}_7 we have $-4 = 3$ and since $3 \cdot 5 \equiv 1 \pmod{7}$ it follows that $3^{-1} = 5$. Therefore, the solution is $x = 5 \cdot 3 = 15 \equiv 1 \pmod{7}$.

Essentially the same method works if m is not prime but $(a, m) = 1$. In this case a is a unit in \mathbb{Z}_m and the unique solution is $x = a^{-1}(-b)$. Consider the same equation as in Example 2.5.1.1 but modulo 8, that is

$$3x + 4 \equiv 0 \pmod{8} \implies x \equiv 3^{-1} \cdot (-4) \pmod{8}.$$

However, modulo 8 we have $-4 = 4$ and $3^{-1} = 3$ so the solution is $x = 4 \cdot 3 = 12 = 4 \pmod{8}$.

If $(a, m) \neq 1$ the situation becomes more complicated. We have the following theorem which describes the solutions and provides a technique for finding all solutions.

Theorem 2.5.1 Consider $ax + b \equiv 0 \pmod{m}$ with $(a, m) = d > 1$. Then the congruence is solvable if and only if $d|b$. In this case there are exactly d solutions that are given by

$$x = x_0 + \frac{tm}{d}, t = 0, 1, \dots, d-1$$

where x_0 is any solution of the reduced equation

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}}.$$

Proof Let $d = (a, m)$. If x_0 is a solution then $b \equiv -ax_0 \pmod{m}$ or $b = -ax_0 + tm$ for some t . Therefore, $d|b$. Hence if d does not divide b there is no solution.

Suppose then that $d|b$. Then $(\frac{a}{d}, \frac{m}{d}) = 1$ and the reduced congruence

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}}$$

has a unique solution $(\pmod{\frac{m}{d}})$ say x_0 . But then x_0 is also a solution \pmod{m} of the original congruence. Any integer x congruent to x_0 modulo $\frac{m}{d}$ and hence of the form $x = x_0 + \frac{tm}{d}$ is also a solution to the reduced congruence. However only d of these are incongruent modulo m . It is easy to check that each of $x = x_0 + \frac{tm}{d}$, $t = 0, 1, \dots, d-1$ are incongruent modulo m . \square

The problem of solving a linear congruence is then reduced to finding a single solution of a congruence of the form $ax \equiv b \pmod{m}$ with $(a, m) = 1$. The solution is then $x \equiv a^{-1}b$ where a^{-1} is the inverse of $a \pmod{m}$. As explained in Section 2.4.3 this can be found using the Euclidean algorithm.

EXAMPLE 2.5.1.2 Solve $26x + 81 \equiv 0 \pmod{245}$

We apply the Euclidean algorithm to both determine if $(26, 245) = 1$ and if so to find the inverse of $26 \pmod{245}$

$$245 = (9)(26) + 11$$

$$26 = (2)(11) + 4$$

$$11 = (2)(4) + 3$$

$$4 = (1)(3) + 1.$$

Therefore, $(245, 26) = 1$. Working backward, we express 1 as a linear combination of 26 and 245

$$1 = 4 - (1)(3) = 4 - (11 - (2)(4)) = (3)(4) - (1)(11) = \dots = (66)(26) - (7)(245)$$

Hence modulo 245 we have $66 \cdot 26 = 1$ and $26^{-1} = 66$. Therefore, the solution is

$$x = (26^{-1})(-81) \implies x = (66)(164) = 10824 \equiv 44 \pmod{245}.$$

EXAMPLE 2.5.1.3 Solve $78x + 243 \equiv 0 \pmod{735}$.

Using the Euclidean algorithm, we find that $(78, 735) = 3$ and $3|243$. The reduced congruence is

$$\frac{78}{3}x + \frac{243}{3} = 0 \pmod{\frac{735}{3}} \implies 26x + 81 \equiv 0 \pmod{245}.$$

From the previous example, the solution to the reduced congruence is $x_0 = 44$ with $d = 3$. The solutions then mod 735 would be

$$\begin{aligned} x_0 + \frac{tm}{d}, t = 0, 1, \dots, d-1 &\implies x = 44 + \frac{735t}{3}, t = 0, 1, 2 \\ &\implies x \equiv 44, 289, 534 \pmod{735} \end{aligned}$$

The methods above provide techniques for solving linear congruences. Systems of linear congruences are handled by the next result which is called the **Chinese remainder theorem**.

Theorem 2.5.2 (*Chinese Remainder Theorem*) Suppose that m_1, m_2, \dots, m_k are k positive integers that are relatively prime in pairs. If a_1, \dots, a_k are any integers then the simultaneous congruences

$$x \equiv a_i \pmod{m_i}, i = 1, \dots, k$$

have a common solution which is unique modulo $m_1 m_2 \cdots m_k$.

Proof The proof we give not only provides a verification but also provides a technique for finding the common solution.

Let $m = m_1 m_2 \cdots m_k$. Since the m_i are relatively prime in pairs we have $(\frac{m}{m_i}, m_i) = 1$. Therefore, there is a solution x_i to the reduced congruence

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}.$$

Further for x_i we clearly have

$$\frac{m}{m_j} x_i \equiv 0 \pmod{m_i} \text{ if } i \neq j.$$

Now let

$$x_0 = \sum_{i=1}^k \frac{m}{m_i} x_i a_i.$$

We claim that x_0 is a solution to the simultaneous congruences and that it is unique modulo m .

Now

$$x_0 = \sum_{i=1}^k \frac{m}{m_i} x_i a_i \equiv \frac{m}{m_j} x_j a_j \pmod{m_j}$$

since $\frac{m}{m_i} x_i \equiv 0 \pmod{m_j}$ if $i \neq j$. It follows then that

$$x_0 \equiv \frac{m}{m_j} x_j a_j \pmod{m_j} \equiv a_j \pmod{m_j}$$

since $\frac{m}{m_j} x_j \equiv 1 \pmod{m_j}$. Therefore, x_0 is a common solution. We must show the uniqueness part.

If x_1 is another common solution then $x_1 \equiv x_0 \pmod{m_i}$ for $i = 1, \dots, k$. Therefore, $x_1 \equiv x_0 \pmod{m}$.

We note that if the integers m_i are not relatively prime in pairs there may be no solution to the simultaneous congruences. \square

EXAMPLE 2.5.1.4 Solve the simultaneous congruences

$$x \equiv 6 \pmod{13}$$

$$x \equiv 9 \pmod{45}$$

$$x \equiv 12 \pmod{17}.$$

Here $m_1 = 13, m_2 = 45, m_3 = 17$ so $m = 13 \cdot 45 \cdot 17$. We first solve

$$(17)(45)x \equiv 1 \pmod{13} \implies x \equiv 6$$

$$(13)(17)x \equiv 1 \pmod{45} \implies x \equiv 11$$

$$(13)(45)x \equiv 1 \pmod{17} \implies x \equiv 5.$$

To see how these solutions are found let us look at the second one:

$$(13)(17) \equiv 1 \pmod{45} \implies 221x \equiv 1 \pmod{45} \implies 41x \equiv 1 \pmod{45}$$

since $221 \equiv 41 \pmod{45}$. We now use the Euclidean algorithm;

$$45 = 1 \cdot 41 + 4, 41 = 10 \cdot 4 + 1 \implies 1 = (11)(41) - (10)(45) \implies 41^{-1} \equiv 11 \pmod{45}.$$

Therefore using these solutions, the common solution is

$$\begin{aligned} x_0 &= \frac{13 \cdot 45 \cdot 17}{13} (6)(6) + \frac{13 \cdot 45 \cdot 17}{45} (11)(9) + \frac{13 \cdot 45 \cdot 17}{17} (5)(12) = \\ &\implies x_0 = 27540 + 21879 + 35100 = 84519 \equiv 4959 \pmod{9945} \\ &\implies x_0 = 4959. \end{aligned}$$

The Chinese Remainder can also be used to piece together the solution of a single linear congruence.

EXAMPLE 2.5.1.5 Solve $5x + 7 \equiv 0 \pmod{468}$.

Now $(468, 5) = 1$ so the solution is $x \equiv 5^{-1}(-7) \pmod{468}$. The prime decomposition of $468 = 2^2 3^2 13$. Therefore, the solution can be considered as the simultaneous solution of

$$x \equiv 5^{-1}(-7) \pmod{2^2} \implies x \equiv 1 \pmod{4}$$

$$x \equiv 5^{-1}(-7) \pmod{3^2} \implies x \equiv 4 \pmod{9}$$

$$x \equiv 5^{-1}(-7) \pmod{13} \implies x \equiv 9 \pmod{13}.$$

Letting $m_1 = 4, m_2 = 9, m_3 = 13$, and $m = 468$, then as before we first solve

$$(9)(13)x \equiv 1 \pmod{4} \implies x \equiv 1 \pmod{4}$$

$$(4)(13)x \equiv 1 \pmod{9} \implies x \equiv 4 \pmod{9}$$

$$(4)(9)x \equiv 1 \pmod{13} \implies x \equiv 4 \pmod{13}$$

The common solution is

$$\begin{aligned} x_0 &= (9)(13)(1)(1) + (4)(13)(4)(4) + (4)(9)(9)(4) \equiv 10201 \pmod{468} \\ &\implies x_0 = 373. \end{aligned}$$

In the previous sections, we noted that for any natural number n , the additive group of \mathbb{Z}_n and the group of units of \mathbb{Z}_n are finite abelian groups. As an easy consequence of the Chinese remainder theorem, we have the following result.

Theorem 2.5.3 *For any natural number m let $(\mathbb{Z}_m, +)$ denote the additive group of \mathbb{Z}_m and let $U(\mathbb{Z}_m)$ be the group of units of \mathbb{Z}_m . Let $n = n_1 n_2 \cdots n_k$ be a factorization*

of n with pairwise relatively prime factors. Then

$$(\mathbb{Z}_n, +) \cong (\mathbb{Z}_{n_1}, +) \times (\mathbb{Z}_{n_2}, +) \times \cdots \times (\mathbb{Z}_{n_k}, +)$$

$$U(\mathbb{Z}_n) = U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_k}).$$

We leave the proof to the exercises.

2.5.2 Higher Degree Congruences

Now that we have handled linear congruences, we turn to the problem of solving higher degree polynomial congruences

$$f(x) \equiv 0 \pmod{m} \quad (2.5.3)$$

where $f(x)$ is a nonconstant integral polynomial of degree $k > 1$. Suppose that

$$f(x) = a_0 + a_1x + \cdots + a_kx^k \text{ and } g(x) = b_0 + b_1x + \cdots + b_kx^k$$

where $a_i \equiv b_i \pmod{m}$ for $i = 1, \dots, k$. Then $f(c) \equiv g(c) \pmod{m}$ for any integer c and hence the roots of $f(x)$ modulo m are the same as those of $g(x)$ modulo m . Therefore, we may assume that in (2.5.2.1) the polynomial $f(x)$ is actually a polynomial with coefficients in \mathbb{Z}_m .

As remarked earlier if m has the prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and x_0 is a solution of $f(x) \equiv 0 \pmod{m}$, then x_0 is also a solution of $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for $i = 1, \dots, k$. Then for each $i = 1, \dots, k$ there is y_i with $x_0 \equiv y_i \pmod{p_i^{e_i}}$. Conversely, suppose we are given y_i with $f(y_i) \equiv 0 \pmod{p_i^{e_i}}$ for $i = 1, \dots, k$ then the Chinese remainder theorem can be used to patch these y_i together to get a solution x_0 of $f(x) \equiv 0 \pmod{m}$. Specifically,

$$x_0 = \sum_{i=1}^k \frac{m}{p_i^{e_i}} z_i y_i$$

would give a solution where the z_i are determined so that $\frac{m}{p_i^{e_i}} z_i \equiv 1 \pmod{p_i^{e_i}}$.

EXAMPLE 2.5.2.1 Solve $x^2 + 7x + 4 \equiv 0 \pmod{33}$.

Since $33 = 3 \cdot 11$ we consider $x^2 + 7x + 4 \equiv 0 \pmod{3}$ and $x^2 + 7x + 4 \pmod{11}$. First,

$$x^2 + 7x + 4 \equiv 0 \pmod{3} \implies x^2 + x + 1 \equiv 0 \pmod{3} \implies x \equiv 1 \pmod{3}.$$

and this is the only solution. Notice that in \mathbb{Z}_3 we have $(x+2)^2 = x^2 + x + 1$. Now modulo 11 we have

$$x^2 + 7x + 4 = 0 \implies x^2 - 4x + 4 = 0 \implies (x - 2)^2 = 0 \implies x = 2$$

is the only solution. Therefore, a solution modulo 33 would be given by the solution of the pair of congruences

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{11}.$$

Now $11y \equiv 1 \pmod{3} \implies y = 2$ and $3y \equiv 1 \pmod{11} \implies y = 4$ so by the Chinese remainder theorem the solution modulo 33 is

$$x = (11)(2)(1) + (3)(4)(2) = 46 \equiv 13 \pmod{33}$$

Hence we have reduced the problem of solving polynomial congruences to the problem of solving modulo prime powers. From the algorithm using the Chinese remainder theorem, we can further give the total number of solutions. If $f(x)$ is a polynomial with coefficients in \mathbb{Z}_m we let $N_f(m)$ denote the number of solutions of $f(x) = 0 \pmod{m}$. Then

Theorem 2.5.4 *If $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime decomposition of m then $N_f(m) = N_f(p_1^{e_1}) N_f(p_2^{e_2}) \cdots N_f(p_k^{e_k})$.*

The simplest case of solving modulo a prime power p^α is of course when $\alpha = 1$. Then we are attempting to find solutions within \mathbb{Z}_p . Recalling that if p is a prime then \mathbb{Z}_p is a field we can use certain basic properties of equations over fields to further simplify the problem. First recalling that in a field, a polynomial of degree n can have at most n distinct roots we get:

Theorem 2.5.5 *The polynomial congruence $f(x) \equiv 0 \pmod{p}$, p prime, has at most k solutions if the degree of $f(x)$ is k .*

Recall that from Fermat's theorem $x^p = x$ for any $x \in \mathbb{Z}_p$. This implies that every element of \mathbb{Z}_p is a root of the polynomial $x^p - x$. Suppose that $f(x)$ is a polynomial of degree higher than p over \mathbb{Z}_p . Using the division algorithm for polynomials, we then have

$$f(x) = q(x)(x^p - x) + g(x) \text{ where } g(x) = 0 \text{ or } \deg(g(x)) < p.$$

Since every element of \mathbb{Z}_p is a solution of $x^p - x$ it follows that the solutions of $f(x) = 0$ are precisely the solutions of $g(x) = 0$. Hence we can always reduce a polynomial congruence modulo p to a congruence of degree less than p .

Theorem 2.5.6 *If $f(x)$ has degree higher than p , p prime, then there exists a polynomial $h(x)$ of degree less than p such that the solutions of $f(x) \equiv 0 \pmod{p}$ are exactly the solutions of $h(x) \equiv 0 \pmod{p}$.*

There is no general method to solve a polynomial congruence modulo a prime p . However for degree 2 and p an odd prime the quadratic formula holds. First, some more definitions.

Definition 2.5.1 If $(a, m) = 1$ and $x^2 \equiv a \pmod{m}$ has a solution then a is called a **quadratic residue** mod m . If $x^2 \equiv a \pmod{m}$ has no solution then a is a **quadratic nonresidue**.

We will talk more about quadratic and nonquadratic residues in the next section. However, modulo a prime, we get something special. $x^2 - a$ is a quadratic polynomial and hence in a field it can have at most two solutions. Therefore,

Lemma 2.5.1 Given $(a, p) = 1$ with p a prime. Suppose a is a quadratic residue mod p and $x_0^2 \equiv a \pmod{p}$. Then $-x_0$ is the only other solution and if p is odd, x_0 and $-x_0$ are distinct.

If a is a quadratic residue mod p let \sqrt{a} denote one of the two solutions to $x^2 \equiv a \pmod{p}$. We then obtain the quadratic formula modulo any odd prime.

Theorem 2.5.7 If p is an odd prime then the solutions to the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ with $a \not\equiv 0 \pmod{p}$, are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In particular, if $b^2 - 4ac$ is a quadratic nonresidue mod p then $ax^2 + bx + c \equiv 0 \pmod{p}$ has no solutions mod p .

Proof The development of the quadratic formula is solely dependent on the field properties and so can be carried out purely symbolically in \mathbb{Z}_p . Suppose

$$ax^2 + bx + c \equiv 0 \pmod{p} \text{ then } x^2 + \frac{b}{a}x = -\frac{c}{a}.$$

Completing the square on the left side in the usual manner gives

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a}$$

where $\frac{b^2}{4a^2}$ is defined since $4 \not\equiv 0$ and $a^2 \not\equiv 0$ in \mathbb{Z}_p (since p was odd). Then

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \implies x + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

where the squareroot has the meaning described above. Finally,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

EXAMPLE 2.5.2.2 Solve $3x^2 + 5x + 1 \equiv 0 \pmod{7}$.

First, we divide through by 3. Since $3 \cdot 5 = 1$ in \mathbb{Z}_7 then $3^{-1} = 5$ and so

$$3x^2 + 5x + 1 = 0 \implies x^2 + 25x + 5 = 0 \implies x^2 + 4x + 5 = 0.$$

Applying the quadratic formula

$$x = \frac{-4 \pm \sqrt{16 - 4(1)(5)}}{2} = \frac{3 \pm \sqrt{-4}}{2} = \frac{3 \pm \sqrt{3}}{2}.$$

Now 3 is a quadratic nonresidue mod 7 so the original congruence has no solutions modulo 7.

For prime power moduli p^α with $\alpha > 1$ the general idea is to first find solutions mod p , if possible, and then move, using the found solutions iteratively to solutions mod p^2 , then solutions mod p^3 , and so on. There is an algorithm, to handle this iterative procedure. We will not discuss this but refer the reader to [NZ] or [N] for more on this.

2.6 Quadratic Reciprocity

We close this chapter on basic number theory with a discussion of a famous result due originally to Gauss, called the **law of quadratic reciprocity**. There are now dozens of proofs of this result in print and the result has far ranging implications well beyond what might be expected. Further there are generalizations to algebraic number theory as well as applications to problems involving sums of squares.

Recall from the last section that if $x^2 \equiv a \pmod{n}$ has a solution then a is called a **quadratic residue** mod n . If $n = p$, an odd prime, then there are exactly two solutions mod p . Suppose that p, q are distinct odd primes. Then p might be, or might not be, a quadratic residue mod q . Similarly q might be, or might not be, a quadratic residue mod p . At first glance, there might seem to be no relationship between these two questions. Gauss discovered that there is a quite strong relationship and this is the quadratic reciprocity law. In particular, if either of p or q is congruent to 1 mod 4 then either both of $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ are solvable or both are nonsolvable. If both p and q are congruent to 3 mod 4 then one is solvable and the other is not. Before we state the theorem precisely, we introduce some terminology and machinery.

First, we give a criterion for an integer to be a quadratic residue modulo an odd prime.

Lemma 2.6.1 *If p is an odd prime and $(a, p) = 1$ then a is a quadratic residue mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If a is a quadratic nonresidue then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Proof Suppose $(a, p) = 1$. We do the computations in the field \mathbb{Z}_p . Since $a \neq 0$ then from Fermat's theorem $a^{p-1} = 1$ in \mathbb{Z}_p . This implies that $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = 0$ in \mathbb{Z}_p . Since \mathbb{Z}_p is a field it has no zero divisors and this implies that either $a^{\frac{p-1}{2}} = 1$ or $a^{\frac{p-1}{2}} = -1$. Hence either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We show that in the former case and only in the former case is a a quadratic residue.

Suppose that $x^2 = a$ has a solution say x_0 in \mathbb{Z}_p . Then

$$a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} = 1.$$

It follows further that if $a^{\frac{p-1}{2}} = -1$ there can be no solution.

Conversely, suppose $a^{\frac{p-1}{2}} = 1$. Since the multiplicative group of \mathbb{Z}_p is cyclic (see the last section) it follows that there is a $g \in \mathbb{Z}_p$ which generates this cyclic group and $a = g^t$ for some t . Hence $g^{\frac{t(p-1)}{2}} = 1$. However, the order of the multiplicative group of \mathbb{Z}_p is $p - 1$ and therefore this implies that

$$\frac{t(p-1)}{2} \equiv 0 \pmod{p-1}.$$

Therefore, t must be even $t = 2k$. Hence $a = g^{2k} = (g^k)^2$ and there is a solution to $x^2 = a$. \square

To express the quadratic reciprocity law in a succinct manner, we introduce the **Legendre symbol**.

Definition 2.6.1 *If p is an odd prime and $(a, p) = 1$ then the **Legendre symbol** (a/p) is defined by*

1. $(a/p) = 1$ if a is a quadratic residue mod p .
2. $(a/p) = -1$ if a is a quadratic nonresidue mod p .

Thus the value of the Legendre symbol distinguishes quadratic residues from quadratic nonresidues. The next lemma establishes the basic properties of (a/p) .

Lemma 2.6.2 *If p is an odd prime and $(a, p) = (b, p) = 1$ then*

1. $(a^2/p) = 1$,
2. If $a \equiv b \pmod{p}$ then $(a/p) = (b/p)$,
3. $(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}$,
4. $(ab/p) = (a/p)(b/p)$.

Proof Parts (1) and (2) are immediate from the definition of the Legendre symbol. Part (3) is a direct consequence of Lemma 2.6.1.

To see part (4) notice that $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$ and use part (3). \square

From part (4) of this last lemma, we see that to compute (a/p) we can use the prime factorization of a and then restrict to (q/p) where q is a prime distinct from p . The quadratic reciprocity law will allow us to compute this for odd primes and we will give a separate result for $(2/p)$. After proving the quadratic reciprocity law, we will give examples on how to do this. We now give the theorem.

Theorem 2.6.1 (Law of Quadratic Reciprocity) *If p, q are distinct odd primes then*

$$(p/q)(q/p) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Alternatively if p, q are distinct odd primes then

(1) *If at least one of p, q is congruent to 1 mod 4 then*

$$x^2 \equiv q \pmod{p} \text{ and } x^2 \equiv p \pmod{q}$$

are either both solvable or both unsolvable.

(2) *If both p and q are congruent to 3 mod 4 then one of*

$$x^2 \equiv q \pmod{p} \text{ and } x^2 \equiv p \pmod{q}$$

is solvable and the other is unsolvable.

Proof The proof we give is based on two lemmas due to Gauss and then a nice geometric argument due to Eisenstein.

Let p, q be distinct odd primes and set $h = \frac{p-1}{2}$. Consider the set

$$R = \{-h, \dots, -2, -1, 1, 2, \dots, h\}.$$

This is reduced residue system mod p and hence every integer a relatively prime to p , that is, with $(a, p) = 1$, is congruent to exactly one element of R . Let

$$S = \{q, 2q, \dots, hq\}.$$

Since $(p, q) = 1$ any two elements of S are incongruent mod p and therefore each element of S is congruent to exactly one element of R . We first need the following lemma.

Lemma 2.6.3 *If n is the number of elements of S congruent mod p to negative elements of R then $(q/p) = (-1)^n$.*

Proof (Lemma 2.6.3) Suppose a_1, \dots, a_n are the negative elements of R congruent to elements of S and b_1, \dots, b_m with $m + n = h$ the positive elements congruent to the remaining elements of S . The product of the elements of S is $h!q^h$ so

$$h!q^h \equiv a_1 \cdots a_n b_1 \cdots b_m \pmod{p}.$$

Since any two elements of S are incongruent modulo p we cannot have $-a_i = b_j$ for some i, j , for if so then $a_i + b_j = 0 \equiv mq + nq \pmod{p}$ which would imply that $p \mid (m+n)q$ which is impossible since $m, n \leq \frac{p-1}{2}$. Therefore, $-a_1, \dots, -a_n, b_1, \dots, b_m$ give h distinct positive integers all less than or equal to h . Hence

$$\{-a_1, \dots, -a_n, b_1, \dots, b_m\} = \{1, \dots, h\}.$$

It follows that

$$(-1)^n a_1 \cdots a_n b_1 \cdots b_m = h! \implies (-1)^n h! q^h \equiv h! \pmod{p}.$$

However $(h!, p) = 1$ then

$$(-1)^n q^h \equiv 1 \pmod{p} \implies q^h = q^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

From Lemma 2.6.2, we have

$$(q/p) \equiv q^{\frac{p-1}{2}} \pmod{p} \implies (q/p) \equiv (-1)^n \pmod{p}.$$

□

We are now going to count (q/p) in a different way. Let $[x]$ denote the greatest integer less than or equal to x . Notice that if $a, b \in \mathbb{Z}$ and $a = qb + r$ with $0 \leq r < b$ then $[\frac{a}{b}] = q$ and so $a = [\frac{a}{b}]b + r$. Consider now the sum

$$M = \sum_{i=1}^h [\frac{iq}{p}].$$

M is called a **Gauss sum**. The next lemma ties this Gauss sum to (q/p) .

Lemma 2.6.4 *Let p, q be distinct odd primes and let M be defined as above. Then*

$$(q/p) = (-1)^M.$$

Proof As explained above for each i we have

$$iq = [\frac{iq}{p}]p + r_i, 0 < r_i < p.$$

Let R be as in Lemma 2.6.3. If iq is congruent to a negative element a_i of R then $r_i = p + a_i$ while if iq is congruent to a positive element b_i then $r_i = b_i$. Then

$$\sum_{i=1}^h iq = p \sum_{i=1}^h \left[\frac{iq}{p} \right] + \sum_{i=1}^n (a_i + p) + \sum_{i=1}^m b_i.$$

Further

$$\sum_{i=1}^h i = \frac{h(h+1)}{2} = \frac{p^2-1}{8}.$$

Let $P = \frac{p^2-1}{8}$ and plugging back into our sum over $\{iq\}$ we get

$$\sum_{i=1}^h iq = Pq = pM + np + \sum_{i=1}^n a_i + \sum_{i=1}^m b_i.$$

However as we saw in the proof of Lemma 2.6.3,

$$\{-a_1, \dots, -a_n, b_1, \dots, b_m\} = \{1, \dots, h\} \implies -\sum_{i=1}^n a_i + \sum_{i=1}^m b_i = P.$$

Then

$$Pq = pM + np + P + 2 \sum_{i=1}^n a_i \implies P(q-1) = (M+n)p + 2 \sum_{i=1}^n a_i.$$

Since q is odd $q-1 \equiv 0 \pmod{2}$ and hence if we take the last sum mod 2 we get that

$$M+n \equiv 0 \pmod{2}$$

which implies that M, n are both even or both odd. It follows that $(-1)^M = (-1)^n$. From Lemma 2.6.3 we have $(q/p) = (-1)^n$ and hence $(q/p) = (-1)^M$ proving the second lemma. \square

We now interchange the roles of p and q . Let $k = \frac{q-1}{2}$ and let N be the Gauss sum for q ,

$$N = \sum_{i=1}^k \left[\frac{ip}{q} \right].$$

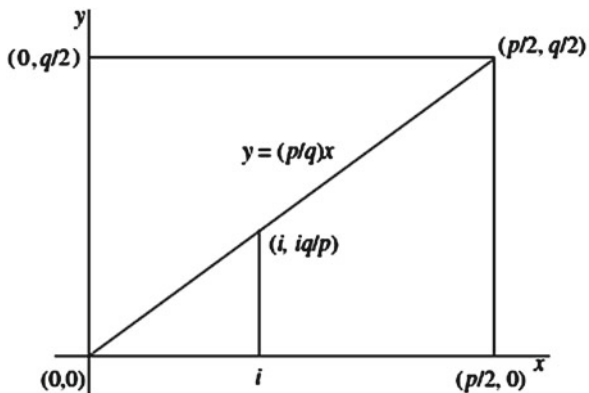
Therefore from Lemma 2.6.4 applied to q , we have $(p/q) = (-1)^N$. Hence

$$(p/q)(q/p) = (-1)^M(-1)^N = (-1)^{M+N}.$$

We will show that

$$M+N = hk = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \quad 2.6.1$$

Fig. 2.2 Geometric argument for Quadratic Reciprocity



which will prove the quadratic reciprocity law.

To show (2.6.1) we will use a lovely geometric argument. Consider the lattice points, that is, points with integer coordinates, within the rectangle with corners at

$$(0, 0), \left(\frac{p}{2}, 0\right), \left(\frac{p}{2}, \frac{q}{2}\right), \left(0, \frac{q}{2}\right)$$

as pictured in Figure 2.2.

Let T be the total number of lattice points within the rectangle. We will compute T in two different ways. First, notice that $T = hk$ since $\lfloor \frac{p}{2} \rfloor = h$ and $\lfloor \frac{q}{2} \rfloor = k$.

Now consider the number below the diagonal. Since the equation of the diagonal is $y = \frac{q}{p}x$ there are no lattice points on the diagonal. For an integer i , the vertical line $x = i$ hits the diagonal at the point $(i, \frac{qi}{p})$ and hence the number of lattice points along the line $x = i$ and below the diagonal is $\lfloor \frac{iq}{p} \rfloor$. It follows that the total number of lattice points below the diagonal is

$$\sum_{i=1}^h \left\lfloor \frac{iq}{p} \right\rfloor = M.$$

An analogous argument shows that the total number of lattice points above the diagonal is N . Therefore, $T = M + N$. Hence

$$M + N = hk$$

and the quadratic reciprocity law is proved.

Before giving some examples we note that by modifying slightly the proof of Lemma 2.6.3 we get the following which allows us to compute $(2/p)$ for any odd prime p .

Theorem 2.6.2 *If p is an odd prime, then*

1. $(-1/p) = (-1)^{\frac{p-1}{2}}$ and
2. $(2/p) = (-1)^{\frac{p^2-1}{8}}$.

Proof The first part (1) follows directly from Lemmas 2.6.1 and 2.6.2 taking $a = -1$.

For (2), although we assumed that q was an odd prime in both Lemmas 2.6.3 and 2.6.4 the construction of the sets R and S and the Gauss sum M only required that $(q, p) = 1$. Now let $q = 2$. Then from the definition of the Gauss sum $M = 0$. Hence $\frac{p^2-1}{8} \equiv n \pmod{p}$. Then $(2/p) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$. \square

With the quadratic reciprocity law and Theorem 2.6.2 it is relatively easy to compute (a/p) for any a .

EXAMPLE 2.6.1 Determine $(870/7)$.

The prime factorization of 870 is $870 = 2 \cdot 3 \cdot 5 \cdot 29$. Then

$$(870/7) = (2/7)(3/7)(5/7)(29/7).$$

First,

$$(2/7) = (-1)^{\frac{49-1}{8}} = (-1)^6 = 1$$

$$(3/7) = -(7/3) \text{ since both are congruent to } 3 \pmod{4}$$

$$(7/3) = (1/3) = 1 \implies (3/7) = -1$$

$$(5/7) = (7/5) \text{ since } 5 \equiv 1 \pmod{4}$$

$$(7/5) = (2/5) = (-1)^{\frac{24}{8}} = -1 \implies (5/7) = -1.$$

Finally,

$$(29/7) = (1/7) = 1.$$

Putting these all together

$$(870/7) = (2/7)(3/7)(5/7)(29/7) = (1)(-1)(-1)(1) = 1$$

and hence 870 is a quadratic residue mod 7.

This was just an illustration. For a small prime like 7 it would be easier to reduce mod 7 and do it directly.

$$870 \equiv 2 \pmod{7} \implies (870/7) = (2/7) = 1.$$

2.7 Exercises

2.1 Verify that the following are rings. Indicate which are commutative and which have identities. Which are integral domains?

- (a) The set of rational numbers.
- (b) The set of continuous functions on a closed interval $[a, b]$ under ordinary addition and multiplication of functions.
- (c) The set of 2×2 matrices with integral entries.
- (d) The set $n\mathbb{Z}$ consisting of all integers which are multiples of the fixed integer n .

2.2 (a) Show that in an ordered ring nonzero squares must be positive. Conclude that in an ordered ring with identity the multiplicative identity must be positive.

(b) Show that the complex numbers under the ordinary operations cannot be ordered.

2.3 Show that any ordered ring must be infinite. (Hint: Suppose $a > 0$ then $a + a > 0$, $a + a + a > 0$ and continue).

2.4 Prove by induction that there are 2^n subsets of a finite set with n elements.

2.5 Prove that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

2.6 Let R be an ordered integral domain which satisfies the inductive property. Prove that R is isomorphic to \mathbb{Z} .

(Hint: Let 1 be the multiplicative identity in R . Define $2 \cdot 1 = 1 + 1$ and inductively $n \cdot 1 = (n - 1) \cdot 1 + 1$ in R . Define

$$\bar{R} = \{n \cdot 1 \in R; n \in \mathbb{Z}\}$$

and let $f : \mathbb{Z} \rightarrow R$ by $f(n) = n \cdot 1$. Show first that f is an isomorphism from \mathbb{Z} to \bar{R} . Then use the inductive property in R to show that \bar{R} is all of R .)

2.7 Prove the remaining parts of Theorem 2.2.1.

2.8 Find the GCD and LCM of the following pairs of integers and then express the GCD as a linear combination

- (a) 78 and 30,
- (b) 175 and 35,
- (c) 380 and 127.

2.9 Prove that if $a = qb + r$ then $(a, b) = (b, r)$.

2.10 Prove that if $d = (a, b)$ then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

2.11 Show that if $(a, b) = c$ then $(a^2, b^2) = c^2$. (Hint: The easiest method is to use the fundamental theorem of arithmetic.)

2.12 Redo Problem 2.8 using the prime decomposition of each integer.

2.13 Show that an integer is divisible by 3 if and only if the sum of its digits (in decimal expansion) is divisible by 3. (Hint: Write out the decimal expansion and take everything modulo 3.)

2.14 Let F be a field and let $F[x]$ denote the ring of polynomials over F . Prove that if $f(x), g(x) \in F[x]$ with $g(x) \neq 0$ then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x), \quad r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$

This is the division algorithm for polynomials. (Hint: Model the proof on the proof for the integers.)

2.15 Suppose $p(x)$ is a polynomial over F and $p(r) = 0$. Show that $p(x) = (x - r)h(x)$ where $h(x)$ is another polynomial of degree one less. (Use the division algorithm.)

2.16 Let $g(x), f(x) \in F[x]$. Then their **greatest common divisor** or **GCD** is the monic polynomial $d(x)$ (leading coefficient 1) such that $d(x)$ divides both $f(x)$ and $g(x)$ and if $d_1(x)$ is any other common divisor of $g(x)$ and $f(x)$ the $d_1(x)$ divides $d(x)$. Show that the GCD of two polynomials exists and is the monic polynomial of least degree which can be expressed as a linear combination of $f(x)$ and $g(x)$. That is,

$$d(x) = h(x)f(x) + k(x)g(x)$$

and $d(x)$ has the least degree of any linear combination of this form. (Hint: Again model the proof on the proof for the integers.)

2.17 Prove Euclid's lemma for polynomials, that is, if $d(x)$ divides $f(x)g(x)$ and $(d(x), g(x)) = 1$ then $d(x)$ divides $f(x)$.

2.18 A polynomial $p(x)$ of positive degree over a field F is a **prime polynomial** or **irreducible polynomial** if it cannot be expressed as a product of two polynomials of positive degree over F . Prove that any nonconstant polynomial $f(x) \in F[x]$, where F is a field can be decomposed as a product of prime polynomials. Further this decomposition is unique except for ordering and unit factors. This is the **unique factorization theorem** for polynomial rings over fields. (Hint: Again model the proof on the proof of the fundamental theorem of arithmetic.)

2.19 Suppose $p(x)$ is a polynomial over F and the degree of $p(x)$ is n . Prove that $p(x)$ can have at most n distinct roots over F .

2.20 Mimic the results in Problems 2.14 through 2.18 for general Euclidean domains (see the definition on p. 21) and then use this to prove Theorem 2.3.6.

2.21 Show that the Gaussian integers $\mathbb{Z}[i]$ are Euclidean domain with $N(a+bi) = a^2 + b^2$. This shows that the Gaussian integers are a unique factorization domain.

2.22 Prove part (c) of Theorem 2.6.2: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

2.23 Verify the remaining ring properties to show that for any positive integer n , \mathbb{Z}_n is a commutative ring with an identity.

2.24 Find the multiplicative inverse if it exists

- (a) of 13 in \mathbb{Z}_{47} ,
- (b) of 17 in \mathbb{Z}_{22} ,
- (c) of 6 in \mathbb{Z}_{30} .

2.25 Solve the linear congruences

- (a) $4x + 6 = 2$ in \mathbb{Z}_7 ,
- (b) $5x + 9 = 12$ in \mathbb{Z}_{47} ,
- (c) $3x + 18 = 27$ in \mathbb{Z}_{40} .

2.26 Find $\phi(n)$ for

- (a) $n = 17$,
- (b) $n = 526$,
- (c) $n = 138$.

2.27 Determine the units and write down the group table for the unit group $U(\mathbb{Z}_n)$ for

- (a) \mathbb{Z}_{12} ,
- (b) \mathbb{Z}_{26} .

2.28 Verify Theorem 2.4.8 for

- (a) $n = 26$,
- (b) $n = 88$.

2.29 Prove Theorem 2.5.3, that is, for any natural number m let $(\mathbb{Z}_m, +)$ denote the additive group of \mathbb{Z}_m and let $U(\mathbb{Z}_m)$ be the group of units of \mathbb{Z}_m . Let $n = n_1 n_2 \cdots n_k$ be a factorization of n with pairwise relatively prime factors. Then

$$(\mathbb{Z}_n, +) \cong (\mathbb{Z}_{n_1}, +) \times (\mathbb{Z}_{n_2}, +) \times \cdots \times (\mathbb{Z}_{n_k}, +)$$

$$U(\mathbb{Z}_n) = U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_k}).$$

2.30 Prove that if an integer is congruent to 2 modulo 3 then it must have a prime factor congruent to 2 modulo 3.

2.31 Prove that if p is an odd prime then there exist positive integers x, y such that $p = x^2 - y^2$.

2.32 Prove that if bc is a perfect square for integers b, c and $(b, c) = 1$ then both b and c are perfect squares.

2.33 Determine a primitive root modulo 11.

2.34 We outline a proof of Theorem 2.4.14: An integer n will have a primitive root modulo n if and only if

$$n = 2, 4, p^k, 2p^k$$

where p is a prime.

(a) Show that if $(m, n) = 1$ with $m > 2, n > 2$ then there is no primitive root modulo mn .

(b) Show that there is no primitive root modulo 2^k for $k > 2$.

(c) Prove that if p is an odd prime then there exists a primitive root $a \bmod p$ such that a^{p-1} is not congruent to 1 modulo p^2 . (Hint: Let a be a primitive root mod p . Then $a + p$ is also a primitive root. Show that either a or $(a + p)$ satisfies the result.)

(d) Prove that there exists a primitive root modulo p^k for any $k \geq 2$. (Hint: Let a be the primitive root mod p from part (c). Then this is a primitive root mod p^k for any $k \geq 2$.)

(e) Prove that if a is a primitive root mod p^k then, if a is odd, a is also a primitive root mod $2p^k$. If a is even then $a + p^k$ is a primitive root modulo $2p^k$.

2.35 Use the primality test based on Fermat's theorem to show that 1053 is not prime.

2.36 If $m > 2$ show that $\phi(m)$ is even.

2.37 Prove that $\phi(n^2) = n\phi(n)$ for any positive integer n .

2.38 Prove that if $n \geq 2$ then

$$\sum_{(m,n)=1, 0 < m < n} m = \frac{n\phi(n)}{2}.$$

2.39 Prove that if n has k distinct odd factors then $2^k | \phi(n)$.

Number Theory

An Introduction via the Density of Primes

Fine, B.; Rosenberger, G.

2016, XIII, 413 p. 12 illus., 1 illus. in color., Hardcover

ISBN: 978-3-319-43873-3

A product of Birkhäuser Basel