Chapter 2
The Integers and Modular Arithmetic

In this chapter, we begin with a discussion of mathematical induction. Next, we examine a number of properties of the integers, with an emphasis on divisibility and prime factorization. We conclude by introducing modular arithmetic.

2.1 Induction and Well Ordering

We begin with an important property of the set of natural numbers.

Property 2.1 (Well Ordering Axiom). If S is a nonempty set of positive integers, then S has a smallest element.

This seems so obvious, but it is actually a rather special property of $\mathbb{N}$. Indeed, $\mathbb{Z}$ has no smallest element; neither, for that matter, does the set of positive real numbers.

There is an equivalent form of the Well Ordering Axiom that is especially useful. To state it, we need a definition. A **proposition** is a statement that is either true or false. For instance, "Ottawa is the capital of Canada" is a true proposition, and "There are only finitely many even integers" is a false one. We avoid statements having no truth value, such as "This statement is false" as well as statements that are a matter of opinion, such as "*Xena: Warrior Princess* was a great television program"[1]. What we would like to do is define a sequence of propositions, $P(1)$, $P(2)$, $P(3)$ and so on, and prove that all of them are true at once. This is where induction comes in.

Theorem 2.1 (Principle of Mathematical Induction). *Suppose that, for each positive integer n, we have a proposition $P(n)$. Further suppose that*

[1] Of course, any reasonable person would agree with this statement, but in principle, it is a matter of opinion.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_2

1. $P(1)$ *is true; and*
2. *for each* $n \in \mathbb{N}$, *if* $P(n)$ *is true, then so is* $P(n+1)$.

Then $P(n)$ *is true for every positive integer* n.

Proof. Suppose the theorem is false, and let S be the set of all positive integers n such that $P(n)$ is false. Then S is a nonempty subset of $\mathbb{N}$. By the Well Ordering Axiom, S has a smallest element k. Now, we are assuming that $P(1)$ is true, so $k > 1$. Then $k-1 \notin S$, and hence $P(k-1)$ is true. By our assumption, $P(k)$ is true as well, giving us a contradiction and completing the proof. □

Induction is a powerful tool! We can prove infinitely many propositions in just two steps. Here is a simple example.

Example 2.1. We claim that for every positive integer n, we have

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

We proceed by induction. For each $n \in \mathbb{N}$, the proposition $P(n)$ is the statement

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

First, we must prove $P(1)$. But it states that

$$1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6},$$

which is obvious. Now, we assume $P(n)$ and prove $P(n+1)$. But

$$1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2,$$

by our inductive hypothesis, $P(n)$. Simplifying, we have

$$\begin{aligned} 1^2 + 2^2 + \cdots + (n+1)^2 &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}. \end{aligned}$$

But this is precisely $P(n+1)$. Thus, the proof is complete.

There is another result that we can prove by induction, and which we will need later. A bit of notation is required. For any positive integer n, we define $n!$ (read "n factorial") via $n! = n(n-1)(n-2)\cdots(2)(1)$. Also, $0! = 1$. If n and k are integers, with $n \geq k \geq 0$, then we define $\binom{n}{k}$ (read "n choose k") via $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Example 2.2. We have $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ and $\binom{6}{2} = \frac{6!}{4!2!} = \frac{720}{24 \cdot 2} = 15$.

Theorem 2.2 (Binomial Theorem). *Let a and b be real numbers and n a positive integer. Then*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n.$$

Proof. Let us proceed by induction on n. When $n = 1$, both sides of the equation are $a + b$, so there is nothing to do. Assume the result for n, and prove it for $n + 1$. But

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n(a+b)\\ &= \left(a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n\right)(a+b),\end{aligned}$$

by our inductive hypothesis.

When we expand this product, we obtain a sum of terms consisting of a coefficient multiplied by $a^{n+1-k}b^k$, where $0 \leq k \leq n+1$. The coefficients of a^{n+1} and b^{n+1} are clearly 1, whereas if $0 < k < n+1$, then the coefficient of $a^{n+1-k}b^k$ is $\binom{n}{k} + \binom{n}{k-1}$, since these terms arise from $(\binom{n}{k}a^{n-k}b^k)a$ and $(\binom{n}{k-1}a^{n-(k-1)}b^{k-1})b$. However,

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k+1)!(k-1)!}\\ &= \frac{n!(n-k+1) + n!k}{(n-k+1)!k!}\\ &= \binom{n+1}{k}.\end{aligned}$$

That is,

$$(a+b)^{n+1} = a^{n+1} + \binom{n+1}{1}a^nb + \cdots + \binom{n+1}{n}ab^n + b^{n+1},$$

and the proof is complete. □

Sometimes, a slightly different form of induction is required.

Theorem 2.3 (Strong Induction). *Suppose that, for each positive integer n, we have a proposition $P(n)$. Further suppose that*

1. *$P(1)$ is true; and*
2. *for each integer $n > 1$, if $P(k)$ is true for every $k < n$, then $P(n)$ is true.*

Then $P(n)$ is true for every positive integer n.

Proof. Suppose that the theorem is false, and let S be the set of positive integers n such that $P(n)$ is false. Then S is a nonempty subset of $\mathbb{N}$. By the Well Ordering Axiom, it has a smallest element j. As $P(1)$ is true, $j > 1$. But then by the minimality of j, we see that $P(k)$ is true whenever $k < j$. Thus, $P(j)$ is true, giving us a contradiction. □

As before, we must prove the first proposition. But after that, instead of just assuming that the previous case is true, we assume that all prior cases are true. This can give us more to work with.

Example 2.3. Define a sequence via $a_1 = 1$, $a_2 = 3$, $a_3 = 7$ and, for each $n \geq 4$, $a_n = a_{n-1} + a_{n-2} + a_{n-3}$. We claim that $a_n < 2^n$ for all $n \in \mathbb{N}$. We need strong induction here, because when we consider a_n, we require information not just about a_{n-1}, but about the terms before it as well. When $n = 1$, there is nothing to do. Assume that $n > 1$ and that the claim is true for smaller values of n. If $n = 2$ or 3, again, the result is obvious, so assume that $n \geq 4$. Then $a_n = a_{n-1} + a_{n-2} + a_{n-3} < 2^{n-1} + 2^{n-2} + 2^{n-3}$, by our inductive hypothesis. However, $2^{n-1} + 2^{n-2} + 2^{n-3} = 7 \cdot 2^{n-3} < 2^n$. We are done.

Exercises

2.1. Show that for every positive integer n,

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

2.2. Show that for every positive integer n,

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

2.3. Show that for every positive integer n, the following two identities hold.

1.
$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

2.
$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0$$

2.4. In the plane $\mathbb{R}^2$, let us draw n lines, no two of which are parallel and no three of which meet at a point. Into how many regions do they divide the plane?

2.5. Show that for all integers $n \geq 2$, we have

1. $(1+a)^n > 1 + na$, for all positive real numbers a; and
2. $\sqrt[n]{n} < 2 - \frac{1}{n}$.

2.6. Show that $\binom{2n}{n}$ is less than 4^{n-1} for all positive integers $n \geq 5$.

2.7. We define the Fibonacci sequence via $f_1 = f_2 = 1$, and if $n > 2$, then $f_n = f_{n-1} + f_{n-2}$. Show that, for every positive integer n, $f_n \leq (7/4)^{n-1}$.

2.8. With f_n as in the preceding exercise, show that for every positive integer n,

$$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

2.9. A bar of chocolate is a rectangular array consisting of r rows and c columns of unit square chocolate pieces, with thin lines separating the rows and columns. A single action consists of taking one bar, and breaking it along a line separating two rows or two columns, producing two smaller bars. Show that it will take precisely $rc - 1$ such actions to turn the bar into rc square pieces. (This can be done using strong induction, or with no induction at all.)

2.10. Show that for every positive integer n, there exist a positive integer k, and integers $a_i \in \{0, 1\}$, such that $n = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + \cdots + 2^k a_k$.

2.2 Divisibility

The following theorem simply formalizes the usual division process in the integers.

Theorem 2.4 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.*

Proof. We will prove the existence of q and r first, and then worry about their uniqueness. Let $S = \{a - bt : t \in \mathbb{Z}, a - bt \geq 0\}$. If $0 \in S$, then $a - bq = 0$ for some $q \in \mathbb{Z}$, and hence $a = bq + 0$, as desired. Therefore, we may assume that $S \subseteq \mathbb{N}$. We claim that S is nonempty. Let $t = -|a|$. Then $a - bt = a + |a|b$. If $a \geq 0$, then $a + |a|b \geq 0$, since $b > 0$. If $a < 0$, then $a + |a|b = a(1 - b)$. But $a < 0$ and since $b \geq 1$, we have $1 - b \leq 0$. Thus, $a(1 - b) \geq 0$. Either way, the claim is proved.

In view of the Well Ordering Axiom, S has a least element, say $r = a - bq$. By definition, $r \geq 0$. If $r \geq b$, then $0 \leq r - b < r$, but also $r - b = a - bq - b = a - b(q + 1)$, and therefore $a - b(q + 1)$ is a smaller element of S than r, contradicting the choice of r. Thus, $a = bq + r$, with $0 \leq r < b$.

As to uniqueness, suppose that $a = bq_1 + r_1 = bq_2 + r_2$, with $q_i, r_i \in \mathbb{Z}$ and $0 \leq r_i < b$. Then $b(q_1 - q_2) = r_2 - r_1$. In particular, $b|q_1 - q_2| = |r_2 - r_1|$. If $q_1 \neq q_2$, then $b|q_1 - q_2| \geq b$. But $0 \leq r_1, r_2 < b$, so $|r_2 - r_1| < b$, which is impossible. Therefore, $q_1 = q_2$. But then $r_1 = r_2$ as well. □

We call q and r in the preceding theorem the **quotient** and **remainder** respectively.

Example 2.4. Using $b = 5$, we have $68 = 5(13) + 3$ and $-21 = 5(-5) + 4$.

The case in which the remainder is 0 is of particular interest.

Definition 2.1. Let a and b be integers. We say that a **divides** b (or b is a **multiple** of a) if there exists an integer c such that $b = ac$. In this case, we write $a|b$.

Example 2.5. As $84 = 6(14)$ and $84 = -3(-28)$, we write $6|84$ and $-3|84$. On the other hand, $10 \nmid 84$.

Here are a few basic properties of divisibility, the proofs of which are left as Exercise 2.14.

Lemma 2.1. *Let $a, b, c \in \mathbb{Z}$. Then*

1. *if $a|b$ and $b|c$, then $a|c$;*
2. *if $a|b$ and $b \neq 0$, then $a \leq |b|$; and*
3. *if $a|b$ and $a|c$, then $a|(bu + cv)$ for any $u, v \in \mathbb{Z}$.*

Definition 2.2. Let a and b be integers, not both 0. Then the **greatest common divisor** (or **gcd**) of a and b, written (a, b), is the largest positive integer g such that $g|a$ and $g|b$.

Example 2.6. We have $(60, 170) = 10$ and $(42, -55) = 1$.

Note that the gcd must always exist. As 1 divides everything, a and b must have a common divisor. Also, by Lemma 2.1, if $a \neq 0$, then $(a, b) \leq |a|$. Thus, only the numbers from 1 to $|a|$ need to be considered. We specifically exclude the case $a = b = 0$, since everything divides 0.

Let us mention a couple of easy facts about gcds.

Lemma 2.2. *Take any integers a and b with $a \neq 0$. Then*

1. *$(a, b) = (-a, b)$; and*
2. *$(a, 0) = |a|$.*

Proof. (1) Any divisor of a also divides $-a$, and vice versa.

(2) Clearly $|a|$ divides both a and 0, and Lemma 2.1 shows that no larger integer can do so. □

One particular case is important.

Definition 2.3. Let $a, b \in \mathbb{Z}$, not both 0. Then we say that a and b are **relatively prime** if $(a, b) = 1$.

Example 2.7. By Example 2.6, 60 and 170 are not relatively prime, but 42 and -55 are.

Why is the gcd so significant? The following theorem gives us an idea.

Theorem 2.5. *Let a and b be integers, not both* 0. *Then there exist $u, v \in \mathbb{Z}$ such that $(a, b) = au + bv$. Furthermore, (a, b) is the smallest positive integer that can be written in this way.*

Proof. Let $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. Clearly $S \subseteq \mathbb{N}$. Without loss of generality, we may assume that $a \neq 0$. Then $a^2 + b(0) = a^2 \in S$, and hence S is not empty. By the Well Ordering Axiom, S has a least element, say $g = au + bv$. We claim that $g = (a, b)$. This will complete the proof.

Suppose that $c|a$ and $c|b$. By Lemma 2.1, $c|g$ and, hence, $c \leq g$. It remains only to show that g divides both a and b. Using the division algorithm, write $a = gq + r$, where q and r are integers and $0 \leq r < g$. Then

$$r = a - gq = a - (au + bv)q = a(1 - uq) + b(-vq).$$

Thus, if $r > 0$, then $r \in S$. But $r < g$, contradicting the minimality of g. Therefore, $r = 0$ and $g|a$. By the same argument, $g|b$. □

The following is an immediate consequence.

Corollary 2.1. *Let $a, b \in \mathbb{Z}$, not both* 0. *Then a and b are relatively prime if and only if there exist integers u and v such that $au + bv = 1$.*

We can now prove a couple of useful results for relatively prime numbers.

Corollary 2.2. *Let $a, b, c \in \mathbb{Z}$ with a and b not both* 0. *If $(a, b) = 1$ and $a|bc$, then $a|c$.*

Proof. By the preceding corollary, we may write $au + bv = 1$, for some u, $v \in \mathbb{Z}$. Then $acu + bcv = c$. But $a|a$ and $a|bc$ hence, by Lemma 2.1, $a|(acu + bcv) = c$. □

Corollary 2.3. *Let $a, b \in \mathbb{Z}$, not both* 0. *If a and b are relatively prime, and for some integer n, we have $a|n$ and $b|n$, then $ab|n$.*

Proof. See Exercise 2.18. □

Be careful not to apply the last two corollaries if a and b are not relatively prime! For instance, $6|4 \cdot 3$, but $6 \nmid 4$ and $6 \nmid 3$. Also, $4|12$ and $6|12$ but $24 \nmid 12$.

What we have not yet discussed is how to find (a, b) and the numbers u and v from Theorem 2.5. We could certainly list the common divisors of a and b and see which one is largest, but if the numbers are large, this would be rather time-consuming. It would also give us no insight into finding u and v. Happily, there is a better way. The following technique is attributed to the ancient Greek mathematician Euclid.

Theorem 2.6 (Euclidean Algorithm). *Let a and b be integers, with b positive. If $b|a$, then $(a, b) = b$. Otherwise, apply the division algorithm repeatedly. Let*

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k \\ r_{k-1} &= r_kq_{k+1} + 0, \end{aligned}$$

where $q_i, r_i \in \mathbb{Z}$ for all i and $0 < r_k < r_{k-1} < \cdots < r_1 < b$. Then $(a, b) = r_k$.

Proof. If $b|a$, then b is a common divisor of a and b. In view of Lemma 2.1, it is the largest possible common divisor. Assume that $b \nmid a$. Note that we will only apply the division algorithm finitely many times, as each $r_{i+1} < r_i$, and all are positive. Suppose that $c|a$ and $c|b$. By Lemma 2.1, $c|(a - bq_1) = r_1$. Thus, every common divisor of a and b is also a common divisor of b and r_1. But if $d|b$ and $d|r_1$, then $d|(bq_1 + r_1) = a$. That is, the common divisors of a and b are precisely the same as those of b and r_1. In particular, $(a, b) = (b, r_1)$. But by exactly the same argument,

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_k, 0) = r_k,$$

by Lemma 2.2. □

We do require b to be positive in the Euclidean algorithm, but we can use the fact that $(a, b) = (-a, b)$ if neither a nor b is positive.

In fact, the Euclidean algorithm is doubly useful, because if we start with the penultimate equation and work our way backwards, we can find integers u and v such that $(a, b) = au + bv$. Indeed, we have

$$(a, b) = r_k = r_{k-2}(1) + r_{k-1}(-q_k),$$

and so (a, b) is a multiple of r_{k-2} plus a multiple of r_{k-1}. But then

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$$

and substitution yields

$$(a, b) = r_{k-2}(1) + (r_{k-3} - r_{k-2}q_{k-1})(-q_k) = r_{k-2}(1 + q_{k-1}q_k) + r_{k-3}(-q_k).$$

That is, (a, b) is a multiple of r_{k-3} plus a multiple of r_{k-2}. Eventually, we will write it in the desired form.

Example 2.8. Let $a = 45$ and $b = 33$. Applying the Euclidean algorithm, we have

$$\begin{aligned} 45 &= 33(1) + 12 \\ 33 &= 12(2) + 9 \\ 12 &= 9(1) + 3 \\ 9 &= 3(3) + 0. \end{aligned}$$

Thus, $(a, b) = 3$. Let us find u and v such that $au + bv = 3$. We have

$$\begin{aligned} 3 &= 12(1) + 9(-1) \\ &= 12(1) + (33(1) + 12(-2))(-1) \\ &= 12(3) + 33(-1) \\ &= (45(1) + 33(-1))(3) + 33(-1) \\ &= 45(3) + 33(-4). \end{aligned}$$

That is, $(a, b) = 3a - 4b$.

Exercises

2.11. In each case, use the Euclidean algorithm to find (a, b).

1. $a = 57, b = 20$
2. $a = 117, b = 51$

2.12. For each of the two parts of the preceding problem, find integers u and v such that $(a, b) = au + bv$.

2.13. Let a and b be integers such that $a|b$ and $b|a$. Show that $a \in \{b, -b\}$.

2.14. Prove Lemma 2.1.

2.15. Show that if a, b and c are positive integers, with $(a, b) = 1$, and $c|a$, then $(c, b) = 1$.

2.16. Show that $n^5 - n$ is divisible by 5 for every positive integer n.

2.17. Let a and n be positive integers. Show that there exists an integer u such that $n|(au - 1)$ if and only if a and n are relatively prime.

2.18. Let $a, b \in \mathbb{Z}$, not both 0. If a and b are relatively prime, and for some integer n, we have $a|n$ and $b|n$, show that $ab|n$.

2.19. Take f_n as in Exercise 2.7. Show that $3|f_n$ if and only if $4|n$.

2.20. Take f_n as in Exercise 2.7. Show that $4|f_n$ if and only if $6|n$.

2.3 Prime Factorization

Prime numbers will have a special importance throughout the course.

Definition 2.4. A natural number $p > 1$ is said to be **prime** if its only positive divisors are 1 and p. Otherwise, it is **composite**.

Note that 1 is neither prime nor composite.

Example 2.9. The first few primes are 2, 3, 5, 7, 11, 13, 17, ...

An equivalent way of defining a prime number is given in the following result due to Euclid.

Theorem 2.7 (Euclid's Lemma). *Let $p > 1$ be a positive integer. Then the following are equivalent:*

1. *p is prime; and*
2. *if a and b are integers such that $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose that p is prime and $p|ab$. Now, $(p, a)|p$, so $(p, a) = 1$ or p. If $(p, a) = p$, then since $(p, a)|a$, we have $p|a$. Otherwise, by Corollary 2.1, there exist integers u and v such that $pu + av = 1$. But then $pbu + abv = b$. Now, $p|p$ and $p|ab$, so by Lemma 2.1, $p|b$.

On the other hand, if p is composite, then let $p = cd$, where $1 < c, d < p$. In this case, $p|cd$, but by Lemma 2.1, $p \nmid c$ and $p \nmid d$. □

Corollary 2.4. *Let p be a prime number and $a_1, \dots, a_n \in \mathbb{Z}$. If $p|a_1a_2\cdots a_n$, then $p|a_i$, for some i.*

Proof. Exercise 2.24. □

In fact, every positive integer larger than 1 can be written as a product of primes, called its **prime factorization**.

Theorem 2.8 (Fundamental Theorem of Arithmetic). *If $a \in \mathbb{N}$ and $a > 1$, then there exist primes $p_1, \dots, p_n$ (not necessarily distinct) such that $a = p_1p_2\cdots p_n$. Furthermore, this product is unique up to order. That is, if $a = q_1q_2\cdots q_m$, for some primes q_i, then $m = n$ and, after rearranging the primes, $p_i = q_i$ for all i.*

Proof. Let us prove the existence of the prime factorization and then handle the uniqueness. We will prove the result by strong induction on a. We are excluding the case $a = 1$, so start with $a = 2$. There is nothing to do here, since 2 is prime. Thus, let $a > 2$ and assume that the theorem is true for smaller numbers. If a is prime, there is nothing to do. Otherwise, we can write $a = bc$, with $1 < b, c < a$. But then by our inductive hypothesis, b and c are both products of primes, and hence a is a product of primes.

Now let us prove the uniqueness. Suppose that

$$a = p_1 \cdots p_n = q_1 \cdots q_m,$$

for some primes p_i and q_i. Without loss of generality, say $n \leq m$. Now, $p_1 | a$. Thus, by Corollary 2.4, $p_1 | q_i$, for some i. Rearranging the primes as needed, we may assume that $p_1 | q_1$. But q_1 is prime, so $p_1 = 1$ or q_1. As 1 is not prime, $p_1 = q_1$. Cancelling p_1 and q_1 from the two sides of our equation, we have

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Now do the same for p_2 and repeat. We find that, after rearranging, $p_i = q_i$, $1 \leq i \leq n$. If $m = n$, we are done. Otherwise, we are left with $1 = q_{n+1} \cdots q_m$. But then $q_m | 1$, which is impossible, as $q_m > 1$. □

Example 2.10. We can write $1400 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7$, and there is no other way to write 1400 as a product of primes, except by rearranging (for instance, $2 \cdot 5 \cdot 7 \cdot 2 \cdot 2 \cdot 5$).

Note that this gives us one good reason not to consider 1 as a prime: we would have to abandon uniqueness, as we could multiply by 1 as many times as we wanted.

We can use the existence of prime factors to prove a handy fact.

Corollary 2.5. *Let a, b and n be integers, with $n \neq 0$. If $(a, n) = (b, n) = 1$, then $(ab, n) = 1$.*

Proof. If $(ab, n) > 1$, then by Theorem 2.8, there exists a prime p dividing (ab, n). Since $p | ab$, Theorem 2.7 tells us that $p | a$ or $p | b$. But $p | n$ as well; thus, $(a, n) \geq p$ or $(b, n) \geq p$. Either way, we have a contradiction. □

Exercises

2.21. Factor each of the following numbers into a product of primes: 3528, 30030 and 220000.

2.22. Show that for every prime $p > 3$, there exists a positive integer k such that $p = 6k + 1$ or $p = 6k - 1$.

2.23. Let p be a prime and n an integer. Show that either $p | n$ or $(p, n) = 1$.

2.24. Use induction to prove Corollary 2.4.

2.25. Let $p_1, \ldots, p_k$ be any primes. Show that for each i, $p_i \nmid (p_1 p_2 \cdots p_k + 1)$.

2.26. Use the preceding exercise to show that there are infinitely many primes.

2.27. Let p be a prime and $a, n \in \mathbb{N}$. Suppose that $p | a^n$. Show that $p^n | a^n$.

2.28. Let $p_1, \ldots, p_k$ be distinct primes, and let m_i, n_i be nonnegative integers. Find the gcd of $p_1^{m_1} \cdots p_k^{m_k}$ and $p_1^{n_1} \cdots p_k^{n_k}$.

2.4 Properties of the Integers

This section may seem a tad underwhelming. Indeed, there are no proofs at all and we will not really learn any new facts about the integers. The whole point is to establish some terminology that we will see many times in different settings. While our discussion will take place in $\mathbb{Z}$, it is worth noting that we could just as easily use $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

First, we observe that $\mathbb{Z}$ is **closed** under addition and multiplication. That is,

$$a + b, ab \in \mathbb{Z}$$

for all $a, b \in \mathbb{Z}$.

Next, addition and multiplication on $\mathbb{Z}$ are both **associative**. This means that

$$(a + b) + c = a + (b + c) \text{ and } (ab)c = a(bc)$$

for all $a, b, c \in \mathbb{Z}$. In particular, we can write $a + b + c$ and abc without fear of ambiguity.

Furthermore, addition and multiplication are both **commutative** on $\mathbb{Z}$. In other words,

$$a + b = b + a \text{ and } ab = ba$$

for all $a, b \in \mathbb{Z}$.

We also have the **distributive law**. Specifically,

$$a(b + c) = ab + ac$$

for all $a, b, c \in \mathbb{Z}$.

The numbers 0 and 1 are rather special. We call 0 the **additive identity** for $\mathbb{Z}$ and 1 the **multiplicative identity**. This is because

$$a + 0 = a \text{ and } a \cdot 1 = a$$

for all $a \in \mathbb{Z}$.

Finally, if $a \in \mathbb{Z}$, then $-a$ is its **additive inverse**. This means that

$$a + (-a) = 0.$$

It is important to note that we do not have **multiplicative inverses** for all integers; that is, if $a \in \mathbb{Z}$, it does not follow that there exists a $b \in \mathbb{Z}$ such that $ab = 1$. In fact, this only happens if a is 1 or -1. (The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are a bit different on this last point. Every element other than 0 has a multiplicative inverse in these sets. For instance, in $\mathbb{Q}$, the multiplicative inverse of $\frac{2}{9}$ is $\frac{9}{2}$.)

Exercises

2.29. For each of the following binary operations on $\mathbb{Z}$, decide if it is commutative; that is, do we have $a * b = b * a$ for all $a, b \in \mathbb{Z}$?

1. $a * b = ab + 1$
2. $a * b = a + b + ab$
3. $a * b = a$

2.30. For each part of the preceding exercise, are the operations associative? That is, do we have $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathbb{Z}$?

2.31. For parts (1) and (2) from Exercise 2.29, decide if $*$ has an identity; that is, does there exist an $e \in \mathbb{Z}$ such that $a * e = e * a = a$ for all $a \in \mathbb{Z}$?

2.32. Define a binary operation $*$ on $\mathbb{Q}$ via $a * b = a + b - ab$. Find an identity e; that is, find $e \in \mathbb{Q}$ such that $a * e = e * a = a$ for all $a \in \mathbb{Q}$. Then decide which elements of $\mathbb{Q}$ have inverses. That is, determine for which $b \in \mathbb{Q}$ there exists a $c \in \mathbb{Q}$ such that $b * c = c * b = e$.

2.5 Modular Arithmetic

When we perform modular arithmetic, we choose an integer $n \geq 2$ and then for any integer a, we concern ourselves only with the remainder when a is divided by n. As the only possible remainders are $0, 1, 2, \ldots, n-1$, these are the only numbers to worry about.

Definition 2.5. Let $n \geq 2$ be an integer. If $a, b \in \mathbb{Z}$, then we say that a is **congruent** to b **modulo** n, and write $a \equiv b \pmod{n}$, if $n | (a - b)$; that is, if a and b have the same remainder when divided by n.

Example 2.11. As $8 | (53 - 21)$, we have $53 \equiv 21 \pmod{8}$. Putting this another way, 53 and 21 both have remainder 5 when divided by 8. We reduce to the remainder and write $53 \equiv 5 \pmod{8}$ and $21 \equiv 5 \pmod{8}$.

We add and multiply modulo n in the usual way, simply reducing to the remainder.

Example 2.12. We observe that

$$5 + 8 \equiv 1 \pmod{12} \text{ and } 5 \cdot 8 \equiv 4 \pmod{12}.$$

Of course, we should be a bit careful here. For instance, since $5 \equiv 17 \pmod{12}$, we had better make sure that $5 + 8 \equiv 17 + 8 \pmod{12}$. This is certainly the case, but it will help if we express things in terms of equivalence classes.

Theorem 2.9. *Let $n \geq 2$ be an integer. Then $a \equiv b \pmod{n}$ is an equivalence relation on $\mathbb{Z}$. The equivalence class of a consists of all integers having the same remainder as a when divided by n.*

Proof. Reflexivity: We have $n|0 = a - a$, so $a \equiv a \pmod{n}$. Symmetry: Suppose that $a \equiv b \pmod{n}$. Then $n|(a-b)$, and hence $n| - (a-b) = b - a$. Thus, $b \equiv a \pmod{n}$. Transitivity: Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n|(a-b)$ and $n|(b-c)$. Hence, $n|((a-b)+(b-c)) = a - c$. That is, $a \equiv c \pmod{n}$. The statement about the equivalence classes follows from the definition. □

Definition 2.6. Let $n \geq 2$ be an integer. The set of **integers modulo** n, denoted $\mathbb{Z}_n$, is the set of all equivalence classes of $\mathbb{Z}$ with respect to the equivalence relation $a \equiv b \pmod{n}$. We call these the **congruence classes** modulo n. Specifically, $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Example 2.13. The elements of $\mathbb{Z}_4$ are [0], [1], [2] and [3], where

$$\begin{aligned}
[0] &= \{\ldots, -, 8, -4, 0, 4, 8, \ldots\} \\
[1] &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
[2] &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
[3] &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}.
\end{aligned}$$

As usual, in dealing with equivalence classes, the choice of the representative of the class is not unique. For instance, in the above example, we could just as easily have written $[-5]$ or [7] instead of [3]. It is, however, customary to reduce final answers in $\mathbb{Z}_n$ to the form $[a]$, where $0 \leq a < n$.

We can now define addition and multiplication on $\mathbb{Z}_n$. These work in the obvious way. Specifically,

$$\begin{aligned}
[a] + [b] &= [a+b] \\
[a][b] &= [ab].
\end{aligned}$$

Example 2.14. In $\mathbb{Z}_7$, we have $[5] + [2] = [7] = [0]$ and $[5][3] = [15] = [1]$.

Theorem 2.10. *For any integer $n \geq 2$, addition and multiplication on $\mathbb{Z}_n$ are well-defined.*

Proof. Suppose that $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2).$$

Since $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$, we see that $n|((a_1 + b_1) - (a_2 + b_2))$. That is, $[a_1 + b_1] = [a_2 + b_2]$, so addition is well-defined. Also,

$$a_1b_1 - a_2b_2 = (a_1b_1 - a_1b_2) + (a_1b_2 - a_2b_2) = a_1(b_1 - b_2) + (a_1 - a_2)b_2.$$

Since $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$, we find that $n|(a_1b_1 - a_2b_2)$. That is, $[a_1b_1] = [a_2b_2]$, and multiplication is well-defined. □

Let us discuss a few properties of addition and multiplication in $\mathbb{Z}_n$. These should be compared with the properties of $\mathbb{Z}$ mentioned in Section 2.4.

Theorem 2.11. *Let $n \geq 2$ be an integer, and take any $[a], [b], [c] \in \mathbb{Z}_n$. Then*

1. $[a] + [b] \in \mathbb{Z}_n$ *(closure under addition);*
2. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ *(associativity);*
3. $[a] + [b] = [b] + [a]$ *(commutativity);*
4. $[a] + [0] = [a]$ *(additive identity); and*
5. $[a] + [-a] = [0]$ *(additive inverse).*

Proof. (1) is clear from the definition. The other parts all work because they work in $\mathbb{Z}$. For instance, $[a] + [b] = [a + b] = [b + a] = [b] + [a]$, proving (3). The remaining parts are left as Exercise 2.35. □

And now, some properties of multiplication.

Theorem 2.12. *Let $n \geq 2$ be an integer, and $[a], [b], [c] \in \mathbb{Z}_n$. Then*

1. $[a][b] \in \mathbb{Z}_n$ *(closure under multiplication);*
2. $[a]([b][c]) = ([a][b])[c]$ *(associativity);*
3. $[a][b] = [b][a]$ *(commutativity);*
4. $[a]([b] + [c]) = [a][b] + [a][c]$ *(distributive law); and*
5. $[a][1] = [a]$ *(multiplicative identity).*

Proof. (1) follows from the definition, and the other parts are true because they are true in $\mathbb{Z}$. For instance,

$$\begin{aligned}[a]([b] + [c]) &= [a][b + c] = [a(b + c)] \\ &= [ab + ac] = [ab] + [ac] = [a][b] + [a][c],\end{aligned}$$

proving (4). The rest is left as Exercise 2.36. □

As in $\mathbb{Z}$, we do not necessarily have multiplicative inverses. For instance, in $\mathbb{Z}_{14}$, we find that $[5][3] = [1]$, but there is no integer a such that $[6][a] = [1]$. However, $\mathbb{Z}_5$ behaves more like $\mathbb{Q}$; indeed, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_5$ such that $[a][b] = [1]$. More on this later!

It is worth mentioning that $\mathbb{Z}_n$ does not behave exactly like $\mathbb{Z}$. For instance, in $\mathbb{Z}$, we are used to the fact that if $ab = 0$, then $a = 0$ or $b = 0$. But in $\mathbb{Z}_{12}$, we have $[4][9] = [0]$. We are also accustomed to cancellation in $\mathbb{Z}$; that is, if $ab = ac$, and $a \neq 0$, then $b = c$. Not necessarily true in $\mathbb{Z}_n$! For example, in $\mathbb{Z}_{12}$, we have $[2][3] = [2][9]$, but $[2] \neq [0]$ and $[3] \neq [9]$. So we must be careful with our assumptions.

And now, having acquainted ourselves with $\mathbb{Z}_n$, we are going to make a change in notation. It is rather cumbersome to have to write $[a]$ or $[a] + [b]$ all the time. Therefore, when working in $\mathbb{Z}_n$, we will normally simply write a or $a + b$, as long as the context is clear. We will include the equivalence class brackets if they are needed for greater clarity.

Example 2.15. When working in $\mathbb{Z}_{10}$, we simply write $3 + 8 = 1$ and $3 \cdot 8 = 4$.

We need to prove one last property of modular arithmetic, which dates back to ancient China.

Theorem 2.13 (Chinese Remainder Theorem). *Let $n_1, \dots, n_k$ be positive integers, all larger than 1, such that $(n_i, n_j) = 1$ whenever $i \neq j$. If $a_1, \dots, a_k \in \mathbb{Z}$, then there exists an integer b such that $b \equiv a_i \pmod{n_i}$ for all i. Furthermore, if $c \equiv a_i \pmod{n_i}$ for all i, then $b \equiv c \pmod{n_1 n_2 \cdots n_k}$.*

Proof. For each i, let d_i be the product of all of the n_j except for n_i; that is, $d_i = \frac{n_1 n_2 \cdots n_k}{n_i}$. Since $(n_i, n_j) = 1$ when $i \neq j$, Corollary 2.5 shows us that $(n_i, d_i) = 1$. By Corollary 2.1, there exist integers u_i and v_i such that $n_i u_i + d_i v_i = 1$. Thus, $d_i v_i \equiv 1 \pmod{n_i}$. Let

$$b = d_1 v_1 a_1 + d_2 v_2 a_2 + \cdots + d_k v_k a_k.$$

Then since $n_i | d_j$ if $i \neq j$, we have

$$b \equiv d_i v_i a_i \equiv a_i \pmod{n_i},$$

for all i, as required.

Finally, if $c \equiv a_i \pmod{n_i}$ for all i as well, then $b \equiv c \pmod{n_i}$ for all i; that is, $n_i | (b - c)$ for all i. By Corollary 2.3, $n_1 n_2 \cdots n_k | (b - c)$. □

Example 2.16. Let us solve the congruences $b \equiv 3 \pmod 5$, $b \equiv 4 \pmod{11}$ and $b \equiv 6 \pmod{14}$. We have $d_1 = 154$, $d_2 = 70$ and $d_3 = 55$. Solving $5u_1 + 154v_1 = 1$ using the Euclidean algorithm, we get $u_1 = 31$, $v_1 = -1$. When we solve $11u_2 + 70v_2 = 1$, we get $u_2 = -19$, $v_2 = 3$. Finally, a solution to $14u_3 + 55v_3 = 1$ is $u_3 = 4$, $v_3 = -1$. Therefore, $b = 154(-1)(3) + 70(3)(4) + 55(-1)(6) = 48$. Thus, the solution is $b \equiv 48 \pmod{770}$.

Exercises

2.33. Perform each calculation in $\mathbb{Z}_7$. The final answer should be a nonnegative integer no larger than 6.

1. $2 - 3 \cdot 4$
2. $(4 \cdot 5)^{25}$

2.34. Perform each calculation in $\mathbb{Z}_{15}$. The final answer should be a nonnegative integer no larger than 14.

1. $5 \cdot 11 - 3 \cdot 4$
2. 2^{82}

2.35. Complete the proof of Theorem 2.11.

2.36. Complete the proof of Theorem 2.12.

2.37. For each nonzero element $a \in \mathbb{Z}_{20}$, decide if there is a nonzero $b \in \mathbb{Z}_{20}$ such that $ab = 0$ in $\mathbb{Z}_{20}$. If so, provide such an element b.

2.38. For each element $a \in \mathbb{Z}_{20}$, decide if there exists a $b \in \mathbb{Z}_{20}$ such that $ab = 1$ in $\mathbb{Z}_{20}$. If so, provide such an element b.

2.39. Show that if p is prime, then there are at most two elements $a \in \mathbb{Z}_p$ such that $a^2 = 1$ in $\mathbb{Z}_p$. Find an example of a composite p where there are more than two solutions.

2.40. Let a and b be integers. Show that if $a \equiv b \pmod{p}$ for every prime p, then $a = b$.

2.41. Find $a \in \mathbb{Z}$ such that $a \equiv 2 \pmod{3}$, $a \equiv 4 \pmod{7}$ and $a \equiv 3 \pmod{10}$ simultaneously.

2.42. Find $a \in \mathbb{Z}$ such that $a \equiv 3 \pmod{8}$, $a \equiv 4 \pmod{11}$ and $a \equiv 7 \pmod{15}$ simultaneously.