CHAPTER 4: EXPLORING $\mathbb{Z}$

MATH 378, CSUSM. SPRING 2009. AITKEN

1. Introduction

In this chapter we continue the study of the ring $\mathbb{Z}$. We begin with absolute values. The absolute value function $\mathbb{Z} \to \mathbb{N}$ is the identity when restricted to $\mathbb{N}$. The fundamental law $|ab| = |a| \cdot |b|$ shows that this function is compatible with products. Equally important is the fact that it is not always compatible with sums.

Next we consider induction. In previous chapters we used only a limited form of induction where the base case is zero and where we have to prove a statement n when assuming it for $n-1$. In practice we sometimes want the base case to start at another integer (positive or negative). Also, sometimes we want to be able to prove the case n not from the assumption that it holds for $n-1$, but under the stronger assumption that it holds for all suitable integers less than n. These variants are developed in this chapter.[1] Unlike the earlier principle of induction, these new forms of induction will not be the basis of new axioms, but will be proved to be valid from previous results.

A major theme of this chapter is divisibility. We consider division b/a, but at first only in the case where $a \mid b$ (and where $a \neq 0$). This is followed by a more general conception of division captured by the important Quotient-Remainder Theorem, which introduces the basic concepts of quotient and remainder. We use the Quotient-Remainder Theorem to prove a few things about least common multiples (LCMs). We also briefly discuss the analogous idea of greatest common divisors (GCDs). We then consider prime numbers and relatively prime pairs, and prove a few basic results including the principle, valid for prime p, that

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

From these topics, there are three other topics that naturally follow (i) the fact that every $n > 1$ is the product of primes (part of the Fundamental Theorem of Arithmetic), (ii) the fact that the set of prime numbers is infinite, and (iii) the fact that, for any fixed base $B > 1$, every integer has a unique base B representation. The only difficulty with these topics is that they involve finite products $\prod a_i$ and sums $\sum a_i$. We have yet to consider such

Date: April 7, 2009.

[1] We won't consider all forms of induction. For example, *transfinite induction* will not be covered in these notes. This is a type of induction concerning collections of transfinite ordinals instead of just $\mathbb{N}$ or subsets of $\mathbb{Z}$.

products and sums and justify their basic laws. These concepts also require the concept of a finite sequence $a_1, \ldots, a_k$.

A large part of the chapter will be used to justify the basic laws for finite sums and products, but before this is done there will be a section where we discuss informal proofs of the three facts (i), (ii), (iii) mentioned above (concerning primes and base B representations), and where we discuss what properties of products $\prod a_i$ and sums $\sum a_i$ are required for their proofs. In subsequent sections the necessary theory of finite sequences, finite sums, and finite products is developed. The official proofs of (i), (ii), and (iii) are given in later sections. Optional sections follow which discuss $\prod a_i$ and $\sum a_i$ further.

Only part of the Fundamental Theorem of Arithmetic is proved in this Chapter. The full version of the Fundamental Theorem of Arithmetic will be deferred to a future chapter where we will prove it both for $\mathbb{Z}$ and for polynomial rings.

2. Absolute Values

Definition 1. The *absolute value* $|a|$ of $a \in \mathbb{Z}$ is defined as follows.

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

The following is an easy consequence of the definition and the fact, from Chapter 3, that $a < 0$ if and only if $-a > 0$.

Theorem 1. *If $a \in \mathbb{Z}$ then $|a| \geq 0$. Furthermore, for $n \in \mathbb{N}$,*

$$|a| = n \iff a = n \text{ or } a = -n.$$

In particular (since $-0 = 0$), $|a| = 0$ if and only if $a = 0$.

Remark 1. Since $|a| \geq 0$, the rule $x \mapsto |x|$ defines a function $\mathbb{Z} \to \mathbb{N}$. If $a \in \mathbb{N}$ then $|a| = a$ so the restriction from $\mathbb{Z}$ to $\mathbb{N}$ of $x \mapsto |x|$ is the identity function.

Exercise 1. Use the last statement of Theorem 1 to show that $|a| \geq 1$ if and only if $a \neq 0$.

Absolute value is compatible with multiplication.

Theorem 2. *If $a, b \in \mathbb{Z}$ then*

$$|ab| = |a| \cdot |b|.$$

Exercise 2. Prove this theorem. Hint: if either a or b is zero, the result is easy. Divide the remaining proof into four cases. In the cases where $a < 0$, write $a = -m$ for $m \in \mathbb{N}$. In the cases where $b < 0$, write $b = -n$ for $n \in \mathbb{N}$.

Informal Exercise 3. Absolute value is less compatible with addition. Give examples where $|a + b| = |a| + |b|$ holds, and give examples where it fails.

Theorem 3. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then $|a| \leq n$ if and only if $-n \leq a \leq n$. Similarly, $|a| < n$ if and only if $-n < a < n$.*

Proof. Suppose $|a| \leq n$. Let $m = |a|$. So $0 \leq m \leq n$. By Theorem 1, either $a = m$ or $a = -m$. In the first case $0 \leq a \leq n$. In the second case $0 \leq -a$ and $-a \leq n$, which implies $0 \geq a$ and $a \geq -n$ by results of Chapter 3. In either case $-n \leq a \leq n$.

Now suppose $-n \leq a \leq n$. If $a \geq 0$ then $|a| = a$ so $|a| \leq n$. If $a < 0$ then observe that $-n \leq a$ implies $-a \leq n$ by a result of Chapter 3. Thus $|a| \leq n$ in this case as well.

The proof for $<$ is similar. □

Theorem 4. *Let $x, y, n \in \mathbb{Z}$. If $0 \leq x < n$ and $0 \leq y < n$ then $|x - y| \leq n$.*

Proof. We have $-y \leq 0$ (Chapter 3), so $x + (-y) \leq x + 0 < n + 0$. Thus $x - y < n$ by mixed transitivity.

We also have $-n < -y$ (Chapter 3). So $0 + (-n) < 0 + (-y) \leq x + (-y)$. Thus $-n < x - y$ by mixed transitivity.

By Theorem 3, $|x - y| < n$. □

3. Induction Variants

In Chapter 1, the axiom of induction was introduced. This axiom allows us to prove a statement for all natural numbers provided we know the statement is true for 0, and provided we have an argument that its truth for n implies its truth for $n + 1$. Obviously this is not the only valid form of induction. For example, one can choose to start at other integers than 0, and adjust the conclusion accordingly. There is also a variant called "strong induction" that is easier to use when the n and $n + 1$ cases are not clearly connected. Here, in the inductive step, you get to assume that the statement holds of *all* integers from the base to $n - 1$, and then you try to prove that it hold for n. This allows you to use a stronger hypothesis than regular induction, which in turn makes it easier to prove desired results.

Since these variant forms of induction were not included in the axioms, we need to prove they are valid before we can use them. This is the purpose of this section.

In Chapter 3 translation functions were used to show the following: *Let S be a non-empty subset of $\mathbb{Z}$. If S has a lower bound than it has a minimum, and if S has an upper bound than it has a maximum.* We use this result to to justify the variant forms of induction.[2]

Theorem 5 (Base b induction)**.** *Let b be an integer, and S a subset of $\mathbb{Z}$ such that (i) $b \in S$ and (ii) $n \in S \Rightarrow n + 1 \in S$ for arbitrary integers $n \geq b$. Then*

$$\{x \in \mathbb{Z} \mid x \geq b\} \subseteq S.$$

[2]Warning: "base" here is used in a different sense then at the end of the chapter where we discuss base B representations of an integer.

Proof. Consider the set E of exceptions. In other words, let E be the set of all integers $x \geq b$ not in S. We wish to show that E is empty. So suppose that E is not empty.

Observe that E has lower bound b, but $b \notin E$ (by assumption (i)). So, by the above mentioned property (from Chapter 3), E must have a minimum $m > b$. Let $a = m - 1$. There are no integers between a and $m = a+1$, so $a \geq b$. Also, a cannot be an exception since m is the minimum of E and a is less than m. In other words, $a \in S$. By assumption, $a \in S \Rightarrow a+1 \in S$. Thus $m = a + 1$ is in S, a contradiction. □

Here is a finite version of the above:

Theorem 6. *Let b and c be integers with $b \leq c$, and let S be a subset of integers such that (i) $b \in S$ and (ii) $n \in S \Rightarrow n+1 \in S$ for all $b \leq n < c$. Then*

$$\{b, \ldots, c\} \subseteq S.$$

Exercise 4. Modify the proof of Theorem 5 to prove the above.

Finally, one sometimes needs the following form of induction:

Theorem 7 (Strong induction)**.** *Let $b \in \mathbb{Z}$ and $S \subseteq \mathbb{Z}$. Suppose $b \in S$ and*

$$\{b, \ldots, n-1\} \subseteq S \implies n \in S \qquad \forall\, n > b.$$

Then

$$\{x \in \mathbb{Z} \mid x \geq b\} \subseteq S.$$

Proof. Let E be the set of all integers $x \geq b$ not in S. We wish to show that E is empty. So suppose that E is not empty.

Observe that E has lower bound b. So E must have a minimum m. Since $b \notin E$ we have $m > b$. Since m is the minimum, $\{b, \ldots, m-1\} \subseteq S$. By assumption, however, $\{b, \ldots, m-1\} \subseteq S \;\Rightarrow\; m \in S$. This means $m \in S$, a contradiction. □

Remark 2. Recall that if $c < b$ we defined $\{b, \ldots, c\}$ to be the empty set. With that in mind, observe that the hypothesis in the above theorem can be restated as

$$\{b, \ldots, n-1\} \subseteq S \implies n \in S \qquad \forall\, n \geq b$$

with $n \geq b$ replacing $n > b$. If $n = b$ this becomes $\varnothing \subseteq S \implies b \in S$. Since $\varnothing \subseteq S$ is always true, this is logically equivalent to $b \in S$. So there is no reason to explicitly require $b \in S$ if we require the implication for all $n \geq b$ and not just $n > b$.

4. Divisibility and Division

In previous chapters we have discussed addition, subtraction, multiplication, and even exponentiation. We have covered almost all of basic arithmetic, except we have avoided the delicate topic of division. We start with divisibility

Definition 2. Let $d \in \mathbb{Z}$. An integer of the form cd with $c \in \mathbb{Z}$, is called a *multiple* of d. If $b = cd$ is a multiple of d, then we also say that d *divides* b. In this case we call d a *divisor* of b, and we write $d \mid b$.

In other words, given $b, d \in \mathbb{N}$, the statement $d \mid b$ hold if and only if there exists a $c \in \mathbb{Z}$ such that $b = cd$.

Warning. The term *divides* refers to a relation: it is either true or false when applied to two integers. It does not produce a number.

The relation $\mid$ is written with a vertical stroke, and should not be confused with / (Definition 3) which produces a number. There is a relationship between these two ideas. In fact, $a|b$ if and only if b/a is an integer. Note that the order is reversed! (Here we assume $a \neq 0$).

Exercise 5. Prove the following simple consequences of the definition.

Theorem 8. *Suppose $a, b \in \mathbb{Z}$.*
(i) $a \mid a$.
(ii) $1 \mid a$.
(iii) $a \mid ab$.
(iv) $a \mid 0$.

Exercise 6. So $a \mid 0$ for all $a \in \mathbb{Z}$. Show, however, that $0 \nmid a$ for all $a \neq 0$.

Exercise 7. Prove the following. Show that the divisibility relation is also reflexive, but not symmetric.

Theorem 9. *The divisibility relation is transitive: for all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Exercise 8. Prove the following.

Theorem 10. *Suppose $a, b, d \in \mathbb{Z}$ with $a \neq 0$. Then $d \,|\, b$ if and only if $ad \mid ab$.*

Exercise 9. Prove the following theorem and its corollary.

Theorem 11. *Suppose $a, b, c, u, v \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ua + vb$.*

Corollary 12. *Suppose that $c \mid a$ and $c \mid b$ where $a, b, c \in \mathbb{Z}$. Then c divides the sum and difference of a and b.*

Theorem 13. *Let $d, a \in \mathbb{Z}$. If $d \mid a$ where $a \neq 0$, then $|d| \leq |a|$.*

Proof. By definition, $a = cd$ for some $c \in \mathbb{Z}$. Claim: $c \neq 0$. To see this, observe that if $c = 0$ then $a = 0$, a contradiction.

By Exercise 1, $|c| \geq 1$. Now multiply both sides of the inequality $1 \leq |c|$ by $|d|$. By Theorem 2, we get

$$|d| \leq |c||d| = |cd| = |a|.$$

□

Exercise 10. Show that the only divisors of 1 are ± 1. Show that the only divisors of 2 are ± 1 and ± 2. Hint: see Theorem 1.

Exercise 11. Show that the set of divisors of a non-zero integer a is finite. Hint: apply Theorem 3 to $n = |a|$. Is $\{-n, \ldots, n\}$ finite?

Exercise 12. Prove the following. (Treat zero cases separately).

Corollary 14. *If $a \mid b$ and $b \mid a$ then $|a| = |b|$.*

Remark 3. The above results hint at the fact that the sign of the integers does not affect divisibility. The following lemma and corollaries illustrates this. Thus it is traditional to focus on the positive divisors only.[3]

Lemma 15. *Let $a, b \in \mathbb{Z}$. If $a \mid b$ then $-a \mid b$, $a \mid -b$, and $-a \mid -b$.*

Corollary 16. *Let $a, b \in \mathbb{Z}$. Then*

$$a \mid b \iff |a| \mid b \iff a \mid |b| \iff |a| \mid |b|.$$

In particular $a \mid |a|$ and $|a| \mid a$ (since $a \mid a$).

Corollary 17. *Let $b \in \mathbb{Z}$. Then b and $-b$ have the same divisors.*

Corollary 18. *Let $b \in \mathbb{Z}$. Then $d \mid b$ if and only if $-d \mid b$.*

We now define division, but only in the case where $a \mid b$. The general case must wait until we introduce the rational numbers $\mathbb{Q}$.

Definition 3 (Division)**.** Suppose $a, b \in \mathbb{Z}$ are such that $a \mid b$ and $a \neq 0$. Then b/a is defined to be the integer $c \in \mathbb{Z}$ such that $ac = b$. (This integer exists since $a \mid b$. You will show it is unique.)

Exercise 13. For the above definition to be valid, the element c must be unique. Show the uniqueness.

Remark 4. Division is analogous to subtraction. Subtraction, which is defined in terms of addition, is only partially defined in $\mathbb{N}$, but becomes totally defined in the ring $\mathbb{Z}$. Similarly division, which is defined in terms of multiplication, is only partially defined in $\mathbb{Z}$, but becomes almost totally defined in the field $\mathbb{Q}$. Division is never totally defined: you cannot divide by zero.

It is sometimes handy to restate a definition as a theorem. Obviously for such theorems the proof is a simple appeal to the definition, and does not usually need to be written out. We now restate the definition of division:

Theorem 19 (Basic law of division)**.** *Suppose $a, b, c \in \mathbb{Z}$ are such that $a \mid b$ and $a \neq 0$. Then $b/a = c$ if and only if $b = ac$.*

Exercise 14. Prove the following four theorems with the basic law of division.

Theorem 20. *Let $a \in \mathbb{Z}$ be non-zero. Then $a/a = 1$ and $0/a = 0$.*

Theorem 21. *Suppose $a, b \in \mathbb{Z}$ are such that $a \neq 0$ and $a \mid b$. Then $b = a \cdot (b/a)$.*

[3] The proofs of the next few results are left to you the reader. In general, some of the easier results will not be proved. You the reader, should supply the proofs. It is fine to do this in your head if the proof is simple enough.

Theorem 22. *Suppose $a, b, c \in \mathbb{Z}$ are non-zero integers such that a and b divide c. Then $c/a = b$ if and only if $c/b = a$.*

Theorem 23. *Suppose $a, b \in \mathbb{Z}$ where $b \neq 0$ Then $ab/b = a$.*

5. The Quotient-Remainder Theorem

Suppose $a \neq 0$ and a possibly does not divide b. Then we do not consider a simple quotient b/a. Instead we get a both quotient and a *remainder*. If $a \mid b$ then the remainder is 0. These ideas are based on the following:

Theorem 24 (Quotient-Remainder)**.** *Let $a, b \in \mathbb{Z}$ be such that $a \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ such that*

$$b = qa + r \qquad \textit{and} \qquad 0 \leq r < |a|.$$

Definition 4. The integers q and r above are called the *quotient* and *remainder* of dividing b by a.

The strategy of the proof is to define q to be such that qa is the largest multiple of a that is less than b. We need a lemma that shows that there is a largest multiple.

Lemma 25. *Suppose $a, b \in \mathbb{Z}$ are such that $a \neq 0$. Then there is a largest multiple of a that is less than or equal to b.*

Proof. Let S be the set of multiples of a that are less than or equal to b. By a result of Chapter 3, if S is non-empty and has an upper bound, then it has a maximum. Obviously b is an upper bound. So we only need to show that S is non-empty.

If $b \geq 0$ then $0 \in S$, so we are done. So assume $b < 0$. Since $a \neq 0$, we have $|a| \geq 1$ (Exercise 1). Multiplying both sides of $|a| \geq 1$ by b gives $|a| \cdot b \leq b$. Since a divides $|a|$ we have a divides $|a| \cdot b$ (transitivity). In particular, $|a| \cdot b \in S$. □

We now prove the existence of q and r in Theorem 24.

Proof of existence. Let qa be the largest multiple of a such that $qa \leq b$. This exists by the previous lemma. Let $r \stackrel{\text{def}}{=} b + (-qa)$. By adding qa to both sides we get $qa + r = b$ as desired.

We still need to show that $0 \leq r < |a|$. Since $qa \leq b$, we have

$$qa + (-qa) \leq b + (-qa).$$

In other words, $0 \leq r$. So we must only show $r < |a|$.

Suppose otherwise that $r \geq |a|$. Then $r + (-|a|) \geq |a| + (-|a|)$. In other words $r - |a| \geq 0$. So

$$b = qa + r = qa + |a| + (r - |a|) \geq qa + |a|.$$

However, $qa + |a| > qa$, and a divides $qa + |a|$ by Theorem 11. This contradicts the choice of qa as the maximum multiple of a less than or equal to b. □

Proof of uniqueness. Suppose $b = qa + r = q'a + r'$ where $0 \le r < |a|$ and $0 \le r' < |a|$. Then, using laws from Chapter 3,

$$r - r' = (b + (-qa)) - (b + (-q'a)) = (q' - q)a.$$

By Theorem 4, $|r - r'| < |a|$. By Theorem 2,

$$|r - r'| = |q' - q| \cdot |a|.$$

So $|q' - q| \cdot |a| < |a|$. This means $|q' - q| < 1$ (Chapter 1). Since $|q' - q|$ is an integer, we have $|q' - q| = 0$. So $q' - q = 0$ (Theorem 1). Thus $q' = q$. Also, since $r - r' = (q' - q)a$, we have $r - r' = 0$. So $r' = r$. □

Definition 5. Let $b, a \in \mathbb{Z}$ where $a \neq 0$. Then $\mathrm{Rem}(b, a)$ is defined to be the remainder when dividing b by a.

Exercise 15. Prove the following:

Theorem 26. *Let $a, b \in \mathbb{Z}$ where $a \neq 0$, Then*

$$\mathrm{Rem}(b, a) = 0 \iff a \mid b.$$

If $\mathrm{Rem}(b, a) = 0$ then b/a is the quotient (as defined in Definition 4).

Informal Exercise 16. Find the quotient and remainder of dividing 20 by 9. Find the quotient and remainder of dividing -30 by 7.

Informal Exercise 17. What is $\mathrm{Rem}(109, 7)$, $\mathrm{Rem}(-109, 7)$, $\mathrm{Rem}(-70, 7)$?

6. GCDs and LCMs

Definition 6. Suppose that $a, b \in \mathbb{Z}$. Then a *common divisor* is an integer d such that $d \mid a$ and $d \mid b$. A *common multiple* is an integer m that is both a multiple of a and a multiple of b. In other words, $a \mid m$ and $b \mid m$.

Informal Exercise 18. Final all the common divisors of -8 and 12 (even the negative divisors). Find four common multiples of -8 and 12.

Theorem 27. *Let a, b be integers, not both zero. Then a and b have a greatest common divisor. This divisor is also called the GCD of a and b, and is written $\gcd(a, b)$.*

Proof. Let S be the set of common divisors. We know that $1 \in S$, so S is not empty. Without loss of generality, suppose $a \neq 0$. By Theorem 13, all elements $x \in S$ satisfy $x \le |a|$. Thus S has an upper bound. By a result of Chapter 3, S has a maximum. □

Informal Exercise 19. Find two positive integers a and b whose GCD is 1. Find two distinct positive integers a and b, both greater than 1, whose GCD is just a.

Theorem 28. *Let a, b be non-zero integers. Then a and b have a least common positive multiple. This multiple is usually called the least common multiple, or the LCM, of a and b.*

Proof. Let S be the set of positive common multiples. Since $|ab| \in S$, S is not empty. By the well-ordering property of $\mathbb{N}$, the set S has a minimum. □

Informal Exercise 20. Find two positive integers a and b whose LCM is ab. Find two distinct positive integers a and b whose LCM is not ab.

Exercise 21. Prove the following.

Theorem 29 (Linear Combination)**.** *Let $a, b, u, v \in \mathbb{Z}$. Every common divisor of a and b divides $ua + vb$. In particular,* $\gcd(a, b) \mid ua + vb$.

The following is sometimes handy:

Lemma 30. *Let b, a be integers where $a \neq 0$. Then any common divisor of b and a also divides* $\mathrm{Rem}(b, a)$*. In particular,* $\gcd(b, a) \mid \mathrm{Rem}(b, a)$.

Proof. We have that $b = qa + r$ where q is the quotient and r is the remainder. Thus $\mathrm{Rem}(b, a) = (1)b + (-q)a$. By Theorem 29, any common divisor of b and a divides $\mathrm{Rem}(b, a)$. □

It is easy to see that any multiple of the LCM is a common multiple, the following gives a converse.

Theorem 31. *Let a, b be non-zero integers, and let m be the LCM. Then any common multiple of a and b is a multiple of m.*

Proof. Let c be a common multiple of a and b. Observe that a is a common divisor of c and m. Thus a is a common divisor of $\mathrm{Rem}(c, m)$ by Lemma 30. Likewise b is a common divisor of $\mathrm{Rem}(c, m)$. Thus $\mathrm{Rem}(c, m)$ is a common multiple of a and b. But $\mathrm{Rem}(c, m) < m$ (Quotient-Remainder theorem), and m is the least common positive multiple. Thus $\mathrm{Rem}(c, m) = 0$ which implies that c is a multiple of m. □

7. Prime numbers and relatively prime pairs

Definition 7 (Prime Number)**.** A *prime number* (or a *prime*) is an integer p such that (i) $p > 1$, and (ii) the only postive divisors of p are 1 and p.

Exercise 22. Show that 2 and 3 are prime, but that 4 is not. You may use the facts $\{1, \ldots, 2\} = \{1, 2\}$ and $\{1, \ldots, 3\} = \{1, 2, 3\}$. You may also use the facts $3 = 2 + 1$, $4 = 2 \cdot 2$, and $1 < 2 < 4$. (These facts are all easily provable using the results of Chapters 1 and 2). Hint: use Theorem 13.

The following is a great illustration of the usefulness of strong induction. Regular induction is not as easy to use here since knowing that n has a prime divisor does not help us to show that $n + 1$ has a prime divisor.

Theorem 32. *Let $n \geq 2$ be an integer. Then n has at least one prime divisor.*

Proof. Let S be the set of all integers $x \geq 2$ such that x has a prime divisor. Observe that S contains all prime numbers since $p \mid p$ for all such p. In particular $2 \in S$. Now suppose that $n > 2$ and that we have established $\{2, \ldots, n-1\} \subseteq S$. If n is prime we have $n \in S$, so consider the case where n is not prime. Then n has a positive divisor d where $d \neq 1$ and $d \neq n$. By Theorem 13 this implies that $1 < d < n$. So $d \in S$. Thus d has a prime divisor p. Since $p \mid d$ and $d \mid n$, we have $p \mid n$ by transitivity. So $n \in S$.

By the principle of strong induction (Theorem 7), all integers $n \geq 2$ are in S. So any such n has a prime divisor. □

Definition 8 (Relatively Prime)**.** Let $a, b \in \mathbb{Z}$. We say that a and b are *relatively prime* if 1 is the only positive common divisor of a and b. In other words, a and b are relatively prime if and only if $\gcd(a, b) = 1$.

Remark 5. Observe that being prime is a property of one integer, while being relatively prime is a property of a pair of integers.

Theorem 33. *If $p, q \in \mathbb{N}$ are distinct prime numbers, then p and q are relatively prime. More generally, if p is a prime and $p \nmid a$ where $a \in \mathbb{Z}$ then p and a are relatively prime.*

Exercise 23. Prove the above theorem.

Exercise 24. Show that 3 and 4 are relatively prime. Hint: $4 = 3 + 1$, so what is $\mathrm{Rem}(4, 3)$?

Theorem 34. *Suppose that $a, b \in \mathbb{Z}$ are non-zero and relatively prime. Then the LCM of a and b is $|ab|$.*

Proof. Let m be the LCM of a and b. Since $|ab|$ is a common multiple of a and b, we have $mq = |ab|$ for some $q \in \mathbb{Z}$ (Theorem 31).

Since a and b are non-zero, the same is true of ab. Thus $|ab|$ is positive. Also m is positive. Thus q must be positive (the other cases lead to contradictions). Also $mq' = ab$ where $q' = q$ or $q' = -q$.

Claim: $q \mid a$. To see this, write $m = kb$ (m is a multiple of b). So $ab = q'm = q'(kb) = (q'k)b$. By the cancellation law for multiplication (Chapter 3), $a = q'k$. Thus $q' \mid a$. Hence $q \mid a$ (Lemma 15).

Likewise, $q \mid b$. Thus q is a common positive divisor of a and b. Since a and b are relatively prime, $q = 1$. So $m = |ab|$. □

Theorem 35. *Suppose that $a, b, c \in \mathbb{Z}$, and that a and b are relatively prime. If $a \mid c$ and $b \mid c$ then $ab \mid c$.*

Proof. If $a = 0$ then we must have $c = 0$ since c is a multiple of a. Since $0 \mid 0$ we are done. Likewise if $b = 0$ then $c = 0$, and we are done. So we can now assume a and b are non-zero.

By Theorem 34 the LCM of a and b is $|ab|$. In particular $|ab| \mid c$ by Theorem 31. The result follows from Corollary 16. □

Informal Exercise 25. Give two examples of the above theorem for specific a, b, c. Now give two counter-examples if we drop the requirement that a and b be relatively prime.

Here is an important fact about prime numbers:

Theorem 36. *Let $a, b \in \mathbb{Z}$, and p a prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$ we are done, so we will assume that $p \nmid a$. By Theorem 33, p and a are relatively prime. Observe that $a \mid ab$ (def. of divisibility) and $p \mid ab$ (assumption), so $ap \mid ab$ by Theorem 35. By Theorem 10, $p \mid b$ as desired (note $a \neq 0$ since $p \nmid a$). □

Informal Exercise 26. Give two examples of the above theorem for specific a, b, p. Now give two counter-examples if we drop the requirement that p be prime.

Definition 9. A *composite number* is a positive integer n such that $n = ab$ for some $a, b \in \mathbb{N}$ with $1 < a < n$ and $1 < b < n$.

Remark 6. Some sources may allow some negative integers to be classified as composite as well, but our definition is adequate for most situations.

Theorem 37. *Let $n \in \mathbb{Z}$. Suppose $n > 1$. Then exactly one of the following occurs: (i) n is prime, or (ii) n is composite.*

Proof. It is clear that both cannot occur: if $n = ab$ with $1 < a < n$ then a is a divisor of n not equal to 1 or n, so n is not a prime.

Now we will show that at least one of the two cases occurs. If n is prime we are done. Otherwise, by the negating the definition of prime, we see that there is a positive divisor a of n such that $a \neq 1$ and $a \neq n$. So $1 < a < n$ (Theorem 13). Since $a \mid n$, there is a $b \in \mathbb{Z}$ such that $ab = n$. Since a and n are positive, b must be as well (the other possibilities lead to contradictions).

The assumptions $b = 1$ or $b = n$ lead to contradictions. Also b is a positive divisor of n. Thus $1 < b < n$ (Theorem 13). Thus n is composite as desired. □

Exercise 27. Show that, in the above proof, the assumption $b = 1$ leads to a contradiction. Show that $b = n$ also leads to a contradiction.

8. Important consequences (Informal)

The results developed in the above sections give us a powerful set of tools to explore the integers. We will conclude the chapter by using these tools to prove three important results: (i) every integer $n \geq 2$ can be factored into prime numbers, (ii) the set of prime numbers is an infinite set, and (iii) given a base $B > 1$ every integer has a unique base B representation. We have the tools to prove many more results about $\mathbb{Z}$, but the exploration of advanced properties of $\mathbb{Z}$ is in the purview of a branch of mathematics called *number theory* and goes beyond the scope of this chapter.

In this section we give sketches of the proofs of the three results (i), (ii), and (iii) mentioned above. The sketches are informal and utilize facts about summation and genera finite products that have not been developed yet. In the next few sections, we will formally develop the needed background on sequences, summation, and products. The chapter ends with the formal proofs of the three featured results. (Followed by few optional sections).

We begin with the statement that *every* $n \geq 2$ *can be written as the product of primes.* In other words,

$$n = \prod_{i=1}^{k} p_i$$

for some finite sequence $p_1, \ldots, p_k$ of prime numbers.

This result has a quick proof using strong induction. Let S be the set of integers $x \geq 2$ which can be written as a product of primes. Obviously all primes are in S (use $k = 1$ and $p_1 = n$). In particular, we have the base case: $2 \in S$ since 2 is a prime. Now we wish to show $n \in S$ assuming that $\{2, \ldots, n-1\} \subseteq S$. Given such an $n > 2$, let p be a prime divisor of n, and write $n = pm$. We know such p exists by Theorem 32. If $m = 1$ we are done: n is prime. If $m > 1$ then $m \in \{2, \ldots, n-1\}$. Thus $m \in S$, and so m is the product of primes (inductive hypothesis and definition of S):

$$m = \prod_{i=1}^{k} p_i.$$

So, if p_{k+1} is defined to be p then

$$n = \prod_{i=1}^{k} p_i \cdot p = \prod_{i=1}^{k+1} p_i$$

as desired. By the principle of strong induction, S contains all $n \geq 2$.

The second result is that *the set of prime numbers is infinite.* The proof very old: it can be found in Euclid's *Elements of Geometry.* It proceeds by contradiction: suppose the set S of primes is finite. Then we can list all the primes in a finite sequence $p_1, \ldots, p_k$. Let

$$n = 1 + \prod_{i=1}^{k} p_i.$$

By Theorem 32, there is a prime p dividing n. Since $p_1, \ldots, p_k$ lists all primes, $p = p_i$ for some i. Observe that

$$n - 1 = \prod_{i=1}^{k} p_i,$$

so $p = p_i$ divides $n - 1$. Since p divides n and $n - 1$, it must divide the difference. The difference is 1, a contradiction since 1 has no prime divisors.

The third result is that, given a base $B > 1$, *every positive integer* n *can be written uniquely in the form*

$$\sum_{i=0}^{k} d_i B^i$$

where k is a non-negative integer, and where $d_0, \ldots, d_k$ is a finite sequence with each $d_i \in \{0, \ldots, B-1\}$ where $d_k \neq 0$. The sequence is called the *base B representation of n*.

The proof is by strong induction. Fix $B > 1$ and let S be the set of all positive integers with unique base B representation. First we observe that S contains all integers n where $1 \leq n < B$. To see existence, let $k = 0$ and $d_0 = n$. To see uniqueness, observe that k must be zero, otherwise the sum has value B or more. Since $k = 0$, we must have $d_0 = n$. In particular, we have the base case $1 \in S$.

Now we wish to show $n \in S$ assuming that $\{2, \ldots, n-1\} \subseteq S$. By the above argument, we can assume $n \geq B$. By the Quotient-Remainder Theorem, $n = qB + r$ for some q and r with $r \in \{0, \ldots, B-1\}$. Since $1 \leq q < n$, we have $q \in S$. So

$$q = \sum_{i=0}^{l} e_i B^i$$

for unique l and unique $e_i \in \{0, \ldots, B-1\}$ with $e_l \neq 0$. Thus

$$n = qB + r = B \sum_{i=0}^{l} e_i B^i + r = \sum_{i=0}^{l} e_i B^{i+1} + r = \sum_{i=1}^{l+1} e_{i-1} B^i + r.$$

Let $k = l + 1$, let $d_i = e_{i-1}$ if $1 \leq i \leq k$, and let $d_0 = r$. This choice gives existence. The uniqueness follows from the uniqueness of the base B representation of q and the uniqueness of the remainder r. So $n \in S$. By the principle of strong induction, S contains all $n \geq 1$.

Observe that the above proofs make use of three key concepts that have not been developed yet: finite sequences $(a_1, \ldots, a_k)$, summations (using $\sum$), and general finite products (using $\prod$). So before we can give formal proofs for the above results, we need to develop these three concepts. This is the purpose of the next three sections.

9. Sequences

Functions provide a common framework for much of mathematics, and a surprising number of mathematical objects and concepts are actually just functions. For example, addition is thought of as a binary operator. In other words, addition is a function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Other binary operations, such as multiplication and subtraction are also thought of as functions. Successor is such a basic function that it was incorporated into our axioms. We interpreted iteration as composing a function with itself a certain number of times. In Chapter 2 we even interpreted the counting process as a bijective function $\{1, \ldots, n\} \to S$.

In this section we use functions to interpret another basic concept: the sequence. We begin with finite sequences.

Definition 10. Let S be a set. A *finite sequence* with values in S is a function $\{m, \ldots, n\} \to S$. Here m and n are integers with $m \leq n$.

Remark 7. If c is such a finite sequence, we usually write $c(i)$ as c_i. As with other kinds of functions, we often define a sequence by giving a rule expressed in terms of a generic element i in the domain. For instance, we might say something like "$c_i = 2^i + 1 \in \mathbb{N}$ where $i = 0, \dots, 5$" which means that we are defining the sequence c as the function $\{0, \dots, 5\} \to \mathbb{N}$ given by the rule $i \mapsto 2^i + 1$. The variable i used here to define our sequence can be replaced by any other unused variable. So the above sequence could just as well be defined as $c_j = 2^j + 1 \in \mathbb{N}$ where $j = 0, \dots, 5$. A variable (such as i above) that can be replaced by any other undeclared variable (such as j above) is called a *bound* or *dummy variable*.

The image of a particular i is called the *ith term of the sequence*, or the *ith value*, and i is called the *index*. The domain $\{m, \dots, n\}$ is called the *index set*, and the codomain is called the *value set*.

Remark 8. We often denote a finite sequence with the notation $(c_i)_{i=m,\dots n}$, or just (c_i) if there is no need to describe the domain. In other words we just indicate the generic ith term inside parentheses. For instance, the sequence in the previous remark can be written $(2^i + 1)_{i=0,\dots,5}$. Again, i here is a bound or dummy variable. So

$$(2^i + 1)_{i=m,\dots,n} = (2^k + 1)_{k=m,\dots,n}.$$

There are actually a variety of ways to denote sequences. For instance, we could write $(c_m, \dots, c_n)$ or even $c_m, \dots, c_n$. Other notation may be employed, but always keep in mind that, regardless of how we denote it, the sequence is just a function.

We often define sequences in terms of other sequences. So the sequence $(3a_i + 4)_{i=m,\dots,n}$ denotes a sequence $(c_i)_{i=m,\dots,n}$ where $c_i = 3a_i + 4$ and where (a_i) is a previously given sequence. Similarly $(3B_{2i+1})$ denotes a sequence defined in terms of another sequence (B_i). Here, only some of the terms (the odd terms) of (B_i) are used. The ith term of the new sequence uses the $2i + 1$st term of another sequence (B_i).

The sequence $(b_{i+k})_{i=m-k,\dots,n-k}$ is not equal to $(b_i)_{i=m,\dots,n}$ even though they have the same values in the same order. The reason is that sequences are functions, and two functions with differing domains are not equal. The one sequence is called a *shift* of the other.

Now we describe infinite sequences. These are important in analysis, and will be considered later in connection with the real numbers.

Definition 11. If $n \in \mathbb{Z}$ then let $\{n, n + 1, \dots\}$ denote $\{x \in \mathbb{Z} \mid x \geq n\}$.

Definition 12. An *infinite sequence* in S is a function $\{n, n + 1, \dots\} \to S$ where $n \in \mathbb{Z}$.

Remark 9. Notational conventions described in the definition of finite sequences will be extended to infinite sequences in the obvious way. For example, $(a_i)_{i=1,2,\dots}$ denotes a sequence with domain or index set $\{1, 2, \dots\}$. We can also write $(a_i)_{i\geq 1}$ or $(a_1, a_2, \dots)$ to denote such an infinite sequence.

Informal Exercise 28. Consider the values $5, 10, 17, 26, 37$. Define a sequence with these values. What is the domain? What is the index set? What is the value set? Write a shifted sequence with the same values. Extend the original sequence to an infinite sequence.

10. Summation

Informally,

$$\sum_{i=m}^{n} b_i$$

denotes the sum $b_m + b_{m+1} + \ldots + b_n$. For example, if we have a sequence with terms $c_1, c_2, c_3, c_4 \in \mathbb{Z}$, then

$$\sum_{i=1}^{4} c_i = c_1 + c_2 + c_3 + c_4.$$

The summation notation can be used for any sequence (b_i) with values b_i in a ring or additive group U. More generally, it can be used for sequences with values in any set U possessing a binary operation called $+$. The formal definition takes the following recursive form:

Definition 13. Let (b_i) be a finite or infinite sequence. Suppose each $b_i \in \mathbb{Z}$ or, more generally, each $b_i \in U$ where U is a set possessing a binary operation called $+$. If $\{m, \ldots, n\}$ is in the domain of (b_i) where $m \le n$, then

$$\sum_{i=m}^{n} b_i$$

is defined by the following recursive definition: if $n = m$ then

$$\sum_{i=m}^{m} b_i \stackrel{\text{def}}{=} b_m.$$

If $n > m$ then write $n = k + 1$ where $k \ge m$ and use the following:

$$\sum_{i=m}^{k+1} b_i \stackrel{\text{def}}{=} \left(\sum_{i=m}^{k} b_i \right) + b_{k+1}.$$

Remark 10. In the final (optional) sections of Chapter 1 we saw that such recursive definitions can be justified using the Iteration Axiom (now a theorem). We further discuss the validity of this definition in the optional Section 16 at the end of this chapter.

Remark 11. The variable i in the above definition is a dummy variable and is not an essential part of the definition. It can be replaced by any other variable not currently in use. So, for instance,

$$\sum_{i=m}^{n} b_i = \sum_{u=m}^{n} b_u.$$

Remark 12. It is important to allow U to be any set with an additive binary operation. This allows us to use the summation idea for all the number systems of the course (including $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) without redeveloping it for each special case. Most of the number systems are rings, but $\mathbb{N}$ is not, so we do not want to restrict ourselves only to rings.

One consequence of the definition is that the summation will be an element of U if all the terms are in U (assuming $+$ is a binary operation on U which means that U is closed under addition). For example, if each $b_i \in \mathbb{N}$ then $\sum b_i \in \mathbb{N}$. Likewise, if each b_i is a positive integer then so is $\sum b_i$, and if each $b_i \in \mathbb{Z}$ is divisible by $d \in \mathbb{Z}$ then so is $\sum b_i$. This is because the set of positive integers and the set of multiples of d are sets closed under addition, and so can be chosen as U.

Exercise 29. Use the above definition to show that

$$\sum_{i=1}^{1} a_i = a_1, \quad \sum_{i=1}^{2} a_i = a_1 + a_2, \quad \sum_{i=1}^{3} a_i = (a_1 + a_2) + a_3,$$

and

$$\sum_{i=1}^{4} a_i = \big((a_1 + a_2) + a_3\big) + a_4$$

Theorem 38 (General Distributive Law)**.** *Let R be a ring.*[4] *Let c be a constant and let (b_i) be a sequence such that $c \in R$ and each $b_i \in R$. Suppose that the domain of (b_i) contains $\{m, \ldots, n\}$ where $m \le n$. Then*

$$c \sum_{i=m}^{n} b_i \; = \; \sum_{i=m}^{n} c\, b_i.$$

Proof. We will use the form of induction in Theorem 6. Let S be the set of integers $k \in \{m, \ldots, n\}$ such that

$$c \sum_{i=m}^{k} b_i \; = \; \sum_{i=m}^{k} c\, b_i$$

holds.

First we need to show that $m \in S$ (base case). In this case

$$c \left(\sum_{i=m}^{m} b_i \right) = c(b_m)$$

and

$$\sum_{i=m}^{m} (c\, b_i) = (c\, b_m)$$

by Definition 13 (case where $n = m$). Thus $m \in S$.

[4]Or at least assume R is a set with binary addition and multiplication operations for which the left distributive law holds.

Now assume that $k \in S$ with $m \le k < n$. We wish to show $k+1 \in S$. Observe that

$$\begin{aligned} c\left(\sum_{i=m}^{k+1} b_i\right) &= c\left(\left(\sum_{i=m}^{k} b_i\right) + b_{k+1}\right) \quad \text{(Def. 13)} \\ &= c\left(\sum_{i=m}^{k} b_i\right) + c\,b_{k+1} \quad \text{(Distr. Law)} \\ &= \left(\sum_{i=m}^{k} c\,b_i\right) + c\,b_{k+1} \quad \text{(Since } k \in S) \\ &= \sum_{i=m}^{k+1} c\,b_i \qquad \text{(Def. 13)} \end{aligned}$$

Thus $k+1 \in S$.

By Induction (Theorem 6) we have $\{m, \ldots, n\} \subseteq S$. In particular $n \in S$. The theorem follows. □

Remark 13. If R is a non-commutative ring, then we would want a general right distributive law. Its proof is essentially the same.

Exercise 30. Show that the usual distributive law is just the special case of the above theorem where $m = 1$ and $n = 2$.

For $R = \mathbb{Z}$, or for R any commutative ring, we have a general commutative law. Since the proof and statement are a bit complicated, and since we do not need it in what follows, this is discussed in an optional section below. Informally it states that $\sum a_i$ is preserved when we permute the terms of the sequence (a_i). The following is also a type of commutative law:

Theorem 39. *Let R be a ring.*[5] *Suppose that (b_i) and (c_i) are two sequences in R, and suppose the domains of (b_i) and (c_i) both contain $\{m, \ldots, n\}$ where $m \le n$. Then*

$$\sum_{i=m}^{n} (b_i + c_i) \;=\; \sum_{i=m}^{n} b_i + \sum_{i=m}^{n} c_i.$$

Exercise 31. Prove the above theorem.

Theorem 40. *Suppose $m \le n$ where $m, n \in \mathbb{Z}$. Then*

$$\sum_{i=m}^{n} 0 = 0.$$

(Here the summation is in $\mathbb{Z}$ or in any set U with an addition operation that possesses an additive identity 0.)

Exercise 32. Prove the above theorem.

[5]Or at least assume R is a set with a binary addition that is commutative and associative.

Theorem 41. *Suppose (b_i) is a sequence in $\mathbb{Z}$ (or in any additive abelian group). Suppose the domain of (b_i) contains $\{m, \ldots, n\}$ where $m \le n$. Then*

$$-\sum_{i=m}^{n} b_i \;=\; \sum_{i=m}^{n} (-b_i)$$

Proof. By Theorem 39 and Theorem 40

$$\sum_{i=m}^{n} b_i + \sum_{i=m}^{n} (-b_i) = \sum_{i=m}^{n} \big(b_i + (-b_i)\big) = \sum_{i=m}^{n} 0 = 0.$$

Now add $-\sum b_i$ to both sides. □

Theorem 42 (General Associative Law)**.** *Let (b_i) be a sequence in a ring R, or more generally in a set U with an associative binary operation called $+$. Suppose $l, m, n \in \mathbb{Z}$ satisfy $l \le m-1$ and $m \le n$. If the domain of (b_i) contains $\{l, \ldots, n\}$, then*

$$\sum_{i=l}^{n} b_i \;=\; \sum_{i=l}^{m-1} b_i \;+\; \sum_{i=m}^{n} b_i.$$

Proof. We will use the form of induction of Theorem 6. Let S be the set of all integers k such that $m \le k \le n$ and

$$\sum_{i=l}^{k} b_i \;=\; \sum_{i=l}^{m-1} b_i \;+\; \sum_{i=m}^{k} b_i.$$

First we need to show that $m \in S$ (base case). In this case

$$\sum_{i=l}^{m} b_i \;=\; \sum_{i=l}^{m-1} b_i + b_m \;=\; \sum_{i=l}^{m-1} b_i + \sum_{i=m}^{m} b_i$$

using Definition 13. Thus $m \in S$.

Now assume that $k \in S$ with $m \le k < n$. We must show $k+1 \in S$. Observe that

$$\begin{aligned}
\sum_{i=l}^{k+1} b_i &= \left(\sum_{i=l}^{k} b_i\right) + b_{k+1} && \text{(Def. 13)} \\
&= \left(\sum_{i=l}^{m-1} b_i + \sum_{i=m}^{k} b_i\right) + b_{k+1} && \text{(Since } k \in S\text{. Ind. Hyp.)} \\
&= \sum_{i=l}^{m-1} b_i + \left(\sum_{i=m}^{k} b_i + b_{k+1}\right) && \text{(Assoc. Law)} \\
&= \sum_{i=l}^{m-1} b_i + \sum_{i=m}^{k+1} b_i && \text{(Def. 13).}
\end{aligned}$$

Thus $k+1 \in S$.

By Induction (Theorem 6) we have $\{m, \ldots, n\} \subseteq S$. In particular $n \in S$. The theorem follows. $\square$

Exercise 33. Show that the general associative law for the case where $l = 1$, $m = 2$, and $n = 4$ is

$$\big((a_1 + a_2) + a_3\big) + a_4 = a_1 + \big((a_2 + a_3) + a_4\big)$$

Exercise 34. Show that the usual associative law is given by the case where $l = 1, m = 2, n = 3$.

Remark 14. As the above exercises illustrate, this theorem is called the *general associative law* because it allows you to move parentheses. For instance, the default placement of (outer) parentheses of $a_1 + a_2 + a_3 + a_4 + a_5$ is $(a_1 + a_2 + a_3 + a_4) + a_5$, but the above theorem allows you to equate this with, for instance, $(a_1 + a_2) + (a_3 + a_4 + a_5)$ or even $a_1 + (a_2 + a_3 + a_4 + a_5)$. Of course, one can use this law to regroup the subgroupings as well. So, for instance, it implies

$$(((a_1 + a_2) + a_3) + a_4) + a_5 = a_1 + \big(a_2 + ((a_3 + a_4) + a_5)\big).$$

To see this, step by step, observe

$$\begin{aligned}
(((a_1 + a_2) + a_3) + a_4) + a_5 &= \sum_{i=1}^{5} a_i \qquad \text{(Def. 13)} \\
&= \sum_{i=1}^{1} a_i + \sum_{i=2}^{5} a_i \qquad \text{(Thm. 42)} \\
&= a_1 + \left(\sum_{i=2}^{2} a_i + \sum_{i=3}^{5} a_i \right) \qquad \text{(Thm 42)} \\
&= a_1 + (a_2 + ((a_3 + a_4) + a_5)) \qquad \text{(Def. 13)}
\end{aligned}$$

Remark 15. The general associative law allows you to move the parentheses around, but it does not allow you to reorder the a_i. For that you need general commutative law discussed in the later (optional) Section 15.

There is one more summation law that we will need:

Theorem 43. *Suppose that (b_i) is a sequence with values in a set U with binary operation $+$. Suppose $m, n, k \in \mathbb{Z}$ are such that $m \le n$ and such that the domain of (b_i) contains $\{m, \ldots, n\}$. Then*

$$\sum_{i=m}^{n} b_i = \sum_{i=m+k}^{n+k} b_{i-k}.$$

Proof. First observe that the function $i \mapsto b_{i-k}$ has domain containing the set $\{m + k, \ldots, n + k\}$, so $\sum_{i=m+k}^{n+k} b_{i-k}$ is defined. This is due to the fact that $m + k \le i \le n + k$ implies $m \le i - k \le n$.

The proof will use the form of induction in Theorem 6. Let S be the set of all integers of the form $l \in \{m, \ldots, n\}$ such that

$$\sum_{i=m}^{l} b_i = \sum_{i=m+k}^{l+k} b_{i-k}.$$

First we need to show that $m \in S$ (base case). In this case

$$\sum_{i=m}^{m} b_i \;=\; b_m \;=\; b_{(m+k)-k} \;=\; \sum_{i=m+k}^{m+k} b_{i-k}$$

by Definition 13. Thus $m \in S$.

Now assume that $l \in S$ with $m \le l < n$. We need to show $m+1 \in S$. Observe that

$$\begin{aligned} \sum_{i=m}^{l+1} b_i &= \left(\sum_{i=m}^{l} b_i\right) + b_{l+1} && \text{(Def. 13)} \\ &= \left(\sum_{i=m+k}^{l+k} b_{i-k}\right) + b_{((l+1)+k)-k} && \text{(Since } l \in S\text{)} \\ &= \sum_{i=m+k}^{(l+1)+k} b_{i-k} && \text{(Def. 13)} \end{aligned}$$

Thus $l+1 \in S$.

By Induction (Theorem 6) we have $\{m, \ldots, n\} \subseteq S$. In particular $n \in S$. The theorem follows. □

11. General Finite Products

Informally, the general finite product

$$\prod_{i=m}^{n} b_i$$

denotes the product $b_m \cdot b_{m+1} \cdots b_n$. For example, if we have a sequence with terms $b_1, b_2, b_3 \in \mathbb{Z}$ then

$$\prod_{i=1}^{3} b_i = b_1 \cdot b_2 \cdot b_3.$$

The finite product can be defined for sequences (b_i) with values in any set U that possesses a binary operation that is written multiplicatively.

The concept of a general finite product is similar to that of a finite sum discussed in the previous section. In fact, the difference in some of the proofs is purely notational. Even the definition is very similar:

Definition 14. Let (b_i) be a sequence with values in a ring U or, more generally, a set possessing a binary operation written with multiplicative notation. If $\{m, \ldots, n\}$ is in the domain of (b_i), then

$$\prod_{i=m}^{n} b_i$$

is defined by the following recursive definition: if $n = m$ then

$$\prod_{i=m}^{m} b_i \stackrel{\text{def}}{=} b_m.$$

If $n > m$ then write $n = k + 1$ where $k \geq m$ and use the following:

$$\prod_{i=m}^{k+1} b_i \stackrel{\text{def}}{=} \left(\prod_{i=m}^{k} b_i \right) \cdot b_{k+1}.$$

Remark 16. In the final (optional) sections of Chapter 1 we saw that this type of recursive definition can be justified using iteration. We discuss the validity of Definition 13 (summation) in optional Section 16 later in this chapter, and this discussion applies, after minor notational changes, to Definition 14 (products) as well.

As with summation, it is important to allow U to be any set with a binary operation that is written multiplicatively. In particular, if U is any set that is closed under a multiplication operation, then the general finite product will have value in U if all the terms are in U. For example, if all the terms b_i are positive integers, then so is the general finite product $\prod b_i$. This is seen by choosing, in this example, the set U to be the set of positive integers.

Remark 17. The variable i in the above definition is a dummy variable, and can be replaced by any variable not currently in use. So, for instance,

$$\prod_{i=m}^{n} b_i = \prod_{w=m}^{n} b_w.$$

Exercise 35. Suppose $(a_i)_{i=1,\ldots,4}$ is a sequence in a ring R. Use the above definition to show that

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{2} a_i = a_1 \cdot a_2, \quad \prod_{i=1}^{3} a_i = (a_1 \cdot a_2) \cdot a_3,$$

and

$$\prod_{i=1}^{4} a_i = \big((a_1 \cdot a_2) \cdot a_3 \big) \cdot a_4$$

Theorem 44 (General Associative Law)**.** *Suppose U is a ring, or at least a set with an associative binary operation written in multiplicative notation.*

Let (b_i) be a sequence in U. Suppose $l, m, n \in \mathbb{Z}$ satisfy $l \le m-1$ and $m \le n$. If the domain of (b_i) contains $\{l, \ldots, n\}$, then

$$\prod_{i=l}^{n} b_i \;=\; \prod_{i=l}^{m-1} b_i \;\cdot\; \prod_{i=m}^{n} b_i.$$

Proof. Adapt the proof of Theorem 42. □

Exercise 36. Show that the usual associative law is given by the case where $l = 1, m = 2, n = 3$.

Exercise 37. Describe the associative law for the case where $l = 1$, $m = 3$, and $n = 5$.

Now we consider divisibility properties of general finite products. First we prove a special case as a lemma:

Lemma 45. *Suppose (a_j) is a sequence with values in a ring R and with domain containing $\{m, \ldots, n\}$ where $m \le n$. Then, for some $b \in R$,*

$$\prod_{j=m}^{n} a_j = a_m \cdot b.$$

Proof. If $n = m$ then $\prod_{j=m}^{m} a_j = a_m$ (Def. 14), so let $b = 1$.

If $m < n$ then

$$\begin{aligned} \prod_{j=m}^{n} a_j &= \prod_{j=m}^{m} a_j \cdot \prod_{j=m+1}^{n} a_j && \text{(Thm. 44, Gen. Assoc.)} \\ &= a_m \cdot \prod_{j=m+1}^{n} a_j && \text{(Definition 14).} \end{aligned}$$

□

Theorem 46. *Suppose (a_j) is a sequence with values in $\mathbb{Z}$ and with domain containing $\{m, \ldots, n\}$ where $m \le n$. Then, for each $i \in \{m, \ldots, n\}$,*

$$a_i \quad \textit{divides} \quad \prod_{j=m}^{n} a_j.$$

Proof. The case $i = m$ is covered by the previous lemma. So assume that $m < i \le n$. Then

$$\begin{aligned}
\prod_{j=m}^{n} a_j &= \prod_{j=m}^{i-1} a_j \cdot \prod_{j=i}^{n} a_j \qquad \text{(Thm. 44, Gen. Assoc.)} \\
&= \prod_{j=m}^{i-1} a_j \cdot (a_i \cdot b) \quad \text{for some } b \in \mathbb{Z} \qquad \text{(Lem. 45)} \\
&= (a_i \cdot b) \cdot \prod_{j=m}^{i-1} a_j \qquad \text{(Comm. Law)} \\
&= a_i \left(b \cdot \prod_{j=m}^{i-1} a_j \right) \qquad \text{(Assoc. Law).}
\end{aligned}$$

So a_i divides the product. □

Theorem 47. *Let R be a commutative ring.*[6] *Suppose that (b_i) and (c_i) are two sequences in R. Suppose the domains of (b_i) and (c_i) both contain $\{m, \ldots, n\}$ where $m \le n$. Then*

$$\prod_{i=m}^{n} (b_i \, c_i) \; = \; \prod_{i=m}^{n} b_i \cdot \prod_{i=m}^{n} c_i.$$

Proof. Adapt the proof of Theorem 39. □

Theorem 48. *Suppose $m \le n$ where $m, n \in \mathbb{Z}$. Then*

$$\prod_{i=m}^{n} 1 = 1.$$

(Here the product is in a ring U or in any set U with a multiplication operation that possesses an multiplicative identity 1.)

Theorem 49. *Suppose that (b_i) is a sequence with values in a set U with binary operation written multiplicatively. Suppose $m, n, k \in \mathbb{Z}$ are such that $m \le n$ and such that the domain of (b_i) contains $\{m, \ldots, n\}$. Then*

$$\prod_{i=m}^{n} b_i = \prod_{i=m+k}^{n+k} b_{i-k}.$$

Proof. Adapt the proof of Theorem 43. □

We end this section with a lemma we will need later.

---

[6] Or at least assume R is a set with a binary multiplication that is commutative and associative.

Lemma 50. *Let (a_i) and (b_i) be sequences with values in a set U and with domain containing $\{m, \ldots, n\}$. Suppose $a_i = b_i$ for all i with $m \le i \le n$ (they can differ for other i). If U has an additive binary operation then*

$$\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} b_i \ ,$$

and if U has a multiplicative binary operation then

$$\prod_{i=m}^{n} a_i = \prod_{i=m}^{n} b_i \ .$$

Proof. Use the form of induction of Theorem 6. □

12. Prime Factorization

Now that we have developed the concepts of summation and general finite products, we can return to the topics mentioned in Section 8. We begin with prime factorizations.

Theorem 51. *Let n be an integer with $n \ge 2$. Then there is a sequence of primes numbers $(p_i)_{i=1,\ldots,k}$ such that*

$$n = \prod_{i=1}^{k} p_i.$$

Proof. Let S be the set of integers $n \ge 2$ with such a prime sequence. Observe that if p is a prime then $p \in S$. To see this, let $p_1 = p$ and $k = 1$. then $\prod_{i=1}^{1} p_1 = p$ by Definition 14.

We will use strong induction to show that every n with $n \ge 2$ is in S. The base case $2 \in S$ has already been shown since 2 is a prime. Now we assume $\{2, \ldots, n-1\} \subseteq S$ with the goal of showing $n \in S$.

By Theorem 32, there is a prime p with $p \mid n$. So write $n = pm$ for some $m \in \mathbb{Z}$. Since n and p are positive, m cannot be zero or negative. Thus m is positive. If $m = 1$ then n is a prime, and $n \in S$ as observed above.

Now suppose $m > 1$. Thus $m \ge 2$. Since $p > 1$ we get $mp > m$, so $m < n$. This means $m \in S$ by the inductive hypothesis. So there is a sequence $(p_i)_{i=1,\ldots,k}$ of primes with $m = \prod_{i=1}^{k} p_i$. Define a new sequence $(p'_i)_{i=1,\ldots,k+1}$ of primes by the rule $p'_i = p_i$ if $1 \le i \le k$, and $p'_{k+1} = p$. Thus, using Lemma 50 and Definition 14,

$$n = mp = \left(\prod_{i=1}^{k} p_i \right) \cdot p = \left(\prod_{i=1}^{k} p'_i \right) \cdot p'_{k+1} = \prod_{i=1}^{k+1} p'_i.$$

Hence $n \in S$.

By the principle of strong induction (Theorem 7), S contains all $n \ge 2$. □

Informal Exercise 38. Illustrate Theorem 51 for the integers 12, 20, 5, and 84. For $n = 12$ find three different sequences that work.

Remark 18. The above theorem is part of what is know as the *fundamental theorem of arithmetic*. The full version of this theorem also asserts that the sequence of primes for a given n is essentially unique. More precisely, that two sequences for the same n have the same prime values and every prime value occurs the same number of times in both sequences. Another way to say this is that the terms of once sequence can be obtained by permuting the terms of the other. We will wait until a future chapter to prove the full theorem where we prove it for both integers and for polynomials.

13. Infinitude of Primes

Now we give a formal proof of Euclid's classic theorem.

Theorem 52. *Let $\mathcal{P}$ be the set of prime numbers. Then $\mathcal{P}$ is infinite.*

Proof. Suppose otherwise, suppose that $\mathcal{P}$ is finite. Then there is a bijection $\{1, \ldots, k\} \to \mathcal{P}$ for some k. This bijection can be thought of as a sequence (p_i) with domain $\{1, \ldots, k\}$ and with values that give all the primes (by definition of sequence, Def 10). Let

$$n = 1 + \prod_{i=1}^{k} p_i.$$

By Theorem 32, there is a prime p dividing n. Since p is a prime, $p = p_i$ for some $1 \leq i \leq k$. Observe that

$$n - 1 = \prod_{i=1}^{k} p_i,$$

so $p = p_i$ divides $n - 1$ (Theorem 46). Since p divides n and $n - 1$, it must divide the difference (Corollary 12). The difference is 1. Thus $p \leq 1$ (Theorem 13). This gives a contradiction. $\square$

Informal Exercise 39. Modify the above proof as follows. Suppose $\mathcal{P}$ is finite. Then $\mathcal{P}$ must have a maximum (Chapter 2). Let q be the maximum prime. Let $n = 1 + q!$, and derive a contradiction.

14. Base B representations of integers

Let $B > 1$ be a fixed integer, called the *base*. The standard in most of the world today is $B = 10$. However, $B = 2, B = 8$, and $B = 16$ are common in computer science. The Babylonians instituted $B = 60$, a choice that still survives in our use of minutes and seconds.

To develop base B in general is no harder than to develop a specific base such as 10, so we will develop the general theory.[7]

[7] The above discussion is informal: we have not defined $10, 16$, or 60 yet.

Remark 19. In a sense, base systems are a luxury, not a necessity. With 0 and σ we can, with enough patience, denote any natural number. Likewise, with $0, 1$ and $+$ we can denote any natural number. For instance, ignoring parentheses, we can denote sixteen as

$$1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1,$$

but it is much more efficient to write '16'.

Definition 15. Let $B > 1$ be a fixed base. A *base B representation* of an integer $n > 0$ is a sequence $(d_i)_{i=1,\ldots,k}$ in $\mathbb{Z}$ with each $0 \le d_i < B$ such that

$$n = \sum_{i=0}^{k} d_i B^i$$

such that $d_k \neq 0$. The number d_i is called the *i-th digit* of n.

Remark 20. We often choose specific symbols (numerals) for the numbers in the set $\{1, \ldots, B-1\}$. These symbols are often also called *digits*.[8] We abbreviate $\sum_{i=0}^{k} d_i B^i$ by listing such symbols for the d_i in order (decreasing the index i as you go from left to right). For example, in base 8 we we can use $[7, 4, 4, 0]$, or simply $[7440]$, to denote

$$7 \cdot 8^3 + 4 \cdot 8^2 + 4 \cdot 8^1 + 0 \cdot 8^0.$$

Exercise 40. Show that a base B representation of B itself is given by the sequence $(d_i)_{i=0,\ldots,1}$ where $d_0 = 0$ and $d_1 = 1$. In other words, we can write B as $[1, 0]$ or $[10]$.

Definition 16. Let *ten* be $9 + 1$ (recall, we have defined 9 in Chapter 1). By the above exercise, ten can be written $[10]$ in base ten.

Definition 17. We will use square brackets around the digits in any base except base ten. In base ten we will usually write the digits without brackets in the usual way. Thus, if $B = 5$ we write $[4, 3, 1]$ or $[431]$ for $4B^2 + 3B + 1$, but if B is ten, we write $4B^2 + 3B + 1$ simply as 431.

In particular, 10 refers to ten. So $10 = 9 + 1$. In general, however, $[10]$ or $[1, 0]$ refers to B where B is the base being used.

In base ten, or in any base, we can separate digits by commas for convenience. Thus 20138 or $20,138$ both represent

$$2 \cdot 10^4 + 0 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10 + 8.$$

Definition 18. If B is not clear from context, we can write B in base 10 as a superscript following the base B representation. Thus

$$[24]_5 = 2 \cdot 5 + 4, \qquad [24]_{16} = 2 \cdot 16 + 4$$

where the right-hand sides are in base 10.

---

[8] The word *digit* comes from Latin *digitus* meaning 'finger'. So really the term *digit* is most appropriate to base ten. We use it for other bases where we imagine an alien or mythical being with B fingers. Homer Simpson would be be a good choice for $B = 8$.

Definition 19. When working in base $B > 10$, one needs symbols for digits up to B. Define $a = 9+1, b = a+1, c = b+1, d = c+1, e = d+1$, and $f = e+1$. Other digits can be defined if needed.[9]

Informal Exercise 41. Using symbols $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f$ write 1219 in base $B = 16$. Write 1219 in base 4. Write 512 in base 12. Write your answers out in summation and short form. Example:

$$603 = 2B^2 + 5B + b \qquad \text{and} \qquad 603 = [25b]_{16}$$

in base $B = 16$.

The key theorem of this section is that every positive integer has a unique base B representation. This shows that base B representation gives a way of representing positive integers, and gives a way of determining if two such integers are distinct. By using '0' and negation '$-$' we can denote all integers uniquely.

Theorem 53. *Let $B > 1$. Then every positive integer has a unique base B representation.*

Before the proof, we give a few lemmas.

Lemma 54. *Suppose (d_i) be a sequence of natural numbers whose domain contains $\{0, \ldots, k\}$ where $k \geq 0$. If $d_k \neq 0$ and B is a positive integer then*

$$\sum_{i=0}^{k} d_i B^i > 0.$$

Proof. If $k = 0$ the result is clear since $d_0 B^0 = d_0$, so assume $k > 0$. By Definition 13,

$$\sum_{i=0}^{k} d_i B^i = \sum_{i=0}^{k-1} d_i B^i + d_k B^k.$$

By the results of Chapter 1, each term $d_i B^i$ is in $\mathbb{N}$. Let $U = \mathbb{N}$. By Definition 13, $\sum_{i=0}^{k-1} d_i B^i$ is in $U = \mathbb{N}$ since $+$ is a binary operation on $\mathbb{N}$ (See Remark 12). Since d_k and B^k are positive by results of Chapter 1, $d_k B^k$ is positive. Thus

$$\sum_{i=0}^{k} d_i B^i = \sum_{i=0}^{k-1} d_i B^i + d_k B^k \geq 0 + d_k B^k > 0.$$

$\square$

[9]In base 60 the custom is to use base 10 to denote the digits up to 59 instead of making up new symbols. So $[34, 2, 17]_{60}$ is the number $34 \cdot 60^2 + 2 \cdot 60 + 17$. Observe that commas must be used to separate digits to avoid confusion.

Lemma 55. *Let (d_i) be a sequence of integers whose domain contains $\{0, \dots, k\}$ with $k > 0$. Let B be a positive integer. Then*

$$\sum_{i=0}^{k} d_i B^i = B\left(\sum_{i=1}^{k} d_i B^{i-1}\right) + d_0 = B\left(\sum_{i=0}^{k-1} d_{i+1} B^i\right) + d_0.$$

If $0 \le d_0 \le B-1$, then d_0 is the remainder and $\sum_{i=1}^{k} d_i B^{i-1} = \sum_{i=0}^{k-1} d_{i+1} B^i$ is the quotient when we divide $\sum_{i=0}^{k} d_i B^i$ by B.

Proof. (Sketch) Use the general assoc. law (Thm. 42) to separate d_0 from the rest of the terms. Use the general distributive law (Thm. 38) to factor out a B. Use the theorem on shifting the sequence (Thm. 43) to justify the equation $\sum_{i=1}^{k} d_i B^{i-1} = \sum_{i=0}^{k-1} d_{i+1} B^i$. Also use basic laws of Ch. 1. For the final statement, use the Quotient-Remainder Theorem (Thm. 24). □

Lemma 56. *Suppose B and n are positive integers where $n < B$. Let $d_0 = n$. Then the sequence (d_i) with domain $\{0\}$ is the unique base B representation of n.*

Proof. By definition of summation (Def. 13),

$$\sum_{i=0}^{0} d_i B^i = d_0 B^0 = d_0 = n.$$

We conclude that (d_i) is indeed a base B representation.

Suppose (d_i') is another base B representation with domain $\{0, \dots, k'\}$. When we divide n by B we have remainder $r = n$ and quotient $q = 0$ since $n = 0 \cdot B + n$ and $0 \le n < B$. By Lemma 55, applied to (d_i') we get that the remainder is d_0'. Thus $d_0' = n = d_0$. If $k' > 0$ then the quotient is $\sum_{i=0}^{k'-1} d_{i+1}' B^i$ by Lemma 55, and is positive by Lemma 54. This contradicts that the quotient is 0. So $k' = 0$. Thus (d_i) and (d_i') are the same sequence, giving uniqueness. □

Proof of Main Theorem (Thm. 53). (Strong Induction). Let S be the set of all positive integers with unique base B expansions. Our goal is to show B includes all positive integers. The base case, $1 \in B$, is covered by Lemma 56.

Now we wish to show $n \in S$ assuming that $\{1, \dots, n-1\} \subseteq S$. If $n < B$ then $n \in S$ by Lemma 56. So we can assume $n \ge B$. By the Quotient-Remainder Theorem, $n = qB + r$ for some q and r with $r \in \{0, \dots, B-1\}$.

Claim: $1 \le q$. Suppose otherwise. If $q = 0$, then $n = qB + r = r$, contrarily to the assumption $n \ge B$. If $q < 0$, then $qB < 0$. This gives $qB + r < r$ contrary to the assumption $n \ge B$. Thus $q \ge 1$.

Since $B > 1$ we get $q < qB \le qB + r$. Thus $q < n$. Since $1 \le q < n$ we have $q \in S$ (inductive hypothesis). So q has a unique base B representation (e_i). Thus (e_i) has domain $\{0, \dots, l\}$ for some l, and

$$q = \sum_{i=0}^{l} e_i B^i$$

where $e_l \neq 0$ and $0 \leq e_i < B$ for all $i \in \{0, \ldots, l\}$. This gives

$$\begin{aligned} n &= qB + r \\ &= B \sum_{i=0}^{l} e_i B^i + r \\ &= \sum_{i=0}^{l} e_i B^{i+1} + r \qquad \text{(General Distr.)} \\ &= r + \sum_{i=1}^{l+1} e_{i-1} B^i \qquad \text{(Thm. 43)} \\ &= \sum_{i=0}^{k} d_i B^i. \qquad \text{(General Assoc., see below for } d_i\text{)} \end{aligned}$$

In the last equation, we set $k = l + 1$, and we define (d_i) by the rule $d_0 = r$ and $d_i = e_{i-1}$ for $i \in \{1, \ldots, l+1\}$. So (d_i) is a sequence with domain $\{0, \ldots, k\}$. Since $e_l \neq 0$ we have $d_k \neq 0$. Likewise, $0 \leq d_i < B$. Thus (d_i) is a base B representation of n. So existence holds for n.

We need to show uniqueness. Suppose (d'_i) is another base B representation with domain $\{0, \ldots, k'\}$. If $k' = 0$ then $n = d'_0$, but $n \geq B$, a contradiction. So we can assume $k' > 0$. By Lemma 55, the remainder is d'_0. But d_0 was defined to be the remainder. Thus $d_0 = d'_0$. By Lemma 55, the quotient q is $\sum_{i=0}^{k'-1} d'_{i+1} B^i$. Earlier we determined that $q \in S$, and defined (e_i) as the unique base B representation of q. So

$$q = \sum_{i=0}^{k'-1} d'_{i+1} B^i = \sum_{i=0}^{l} e_i B^i.$$

By uniqueness (since $q \in S$), $l = k' - 1$ and $d'_{i+1} = e_i$ for $i \in \{0, \ldots, l\}$. This means that $k' = l + 1$ and $d'_i = e_{i-1}$ for all $i \in \{1, \ldots, k'\}$. But $k = l + 1$ and $d_i = e_{i-1}$ for all $i \in \{1, \ldots, k\}$. So $k = k'$ and $d_i = d'_i$ for all $i \in \{1, \ldots, k\}$. Uniqueness follows for n. We conclude that $n \in S$.

By the principle of strong induction, S contains all positive integers. The result follows. □

Remark 21. Suppose that you have made an addition table for $n + m$ for all $n, m \in \{0, \ldots, B - 1\}$ (and proved the table is valid). Then you can perform any base B addition using the laws we have proved. Likewise, if you have made an multiplication table for $n \cdot m$ for all $n, m \in \{0, \ldots, B - 1\}$ (and proved it is valid), then you can perform any base B multiplication using the basic laws of arithmetic. The algorithms you were taught in grade school are just a notational short-cut for the more rigorous use of the laws of arithmetic.

For example, suppose you want to add 108 and 17 in a rigorous manner. Suppose your table, which you suppose was derived earlier using rigorous methods from Chapter 1, shows that $8 + 7 = 15$ and $1 + 1 = 2$. Then, using only results from Chapter 1 and this information from the table (and combining several steps into some of the step),

$$\begin{aligned} 108 + 17 &= ((1 \cdot 10^2 + 0 \cdot 10^1) + 8 \cdot 10^0) + (1 \cdot 10 + 7 \cdot 10^0) \\ &= (10^2 + 8) + (10 + 7) = (10^2 + 10) + (8 + 7) \\ &= (10^2 + 10) + 15 = (10^2 + 1 \cdot 10) + (1 \cdot 10 + 5) \\ &= (10^2 + (1 \cdot 10 + 1 \cdot 10)) + 5 = (10^2 + (1 + 1) \cdot 10^1) + 5 \\ &= (1 \cdot 10^2 + 2 \cdot 10^1) + 5 \cdot 10^0 = 125. \end{aligned}$$

Observe how we "carried the 1". This is a simple example, but in principle any addition and multiplication can be carried out rigorously by a careful use of the laws from Chapter 1. One could attempt to prove (at least informally) that the algorithms that are taught in grade school will always work, and can always be translated to a formal proof.

Informal Exercise 42. Make an addition table for $n + m$ for all $n, m \in \{0, \ldots, 7\}$ for base 8. Use the basic laws of Chapter 1 (distributive, etc.) to find a base 8 representation of $[2, 7, 3]_8 + [7, 3, 1]_8$. (You can use the associative and commutative laws freely, drop parentheses, and you can skip steps using these laws. Be sure to write $[2, 7, 3]_8$ as $2 \cdot 8^2 + 7 \cdot 8 + 3$, and so on.)

Informal Exercise 43. Using the techniques of chapter 1, one could easily make an addition table for $n + m$ for all $n, m \in \{0, \ldots, 9\}$, and prove it to be valid. Do not do this, but assume that someone has done this. Suppose also that you do not yet know how to add larger numbers. Use the basic laws of Chapter 1 to determine $1094 + 329$. Do this by expanding 329 as $3 \cdot 10^2 + 2 \cdot 10 + 9$, and expanding 1094 in a similar manner. (You can use the associative and commutative laws freely, drop parentheses, and skip steps using these laws.)

Informal Exercise 44. Using the techniques of chapter 1, one could easily make an multiplication table for nm for all $n, m \in \{0, \ldots, 9\}$, and prove it to be valid. Do not do this, but assume that someone has done this. Suppose also that you do not yet know how to multiply larger numbers. Use the basic laws of Chapter 1 to determine $17 \cdot 15$. Do this by expanding 17 as $1 \cdot 10 + 7$, and expanding 15 in a similar manner. (You can use the associative and commutative laws freely, drop parentheses, and skip steps using these laws.)

You should be able to see the connection between the above exercises and the traditional algorithms for addition and multiplication.

15. Further properties of summation and products (Optional)

Informally, the general associative law allows us to move parentheses. See Remark 14 for an illustration. This means that in situations where this rule applies, there is no real need to use parentheses, and in everyday mathematics parentheses are dropped. We will do so in future chapters, but for definiteness let us agree to the following convention.

Definition 20. If $a, b, c \in U$ where U is a set with a binary operation $+$, then $a+b+c$ is defined to be $\sum_{i=1}^{3} u_i$ where (u_i) is the sequence defined by $u_1 = a$, $u_2 = b$, $u_3 = c$. As we saw above, this means $a+b+c$ is officially defined to be $(a+b)+c$.

If $a, b, c \in U$ where U is a set with a binary operation written mutliplicatively, then abc is defined to be $\prod_{i=1}^{3} u_i$ where (u_i) is the sequence defined by $u_1 = a$, $u_2 = b$, $u_3 = c$.

We extend this to more than three terms. So $a+b+c+d$ is $\sum_{i=1}^{4} u_i$ for the corresponding sequence (u_i). So $a+b+c+d = ((a+b)+c)+d$.

In essence, we are adopting a left association rule for addition and multiplication: the two leftmost terms are bound together first. In most situations, for example in rings such as $\mathbb{Z}$, addition and multiplication are associative, so a right association rule gives the same result, but we choose the left association rule as our official default. We will adopt a left association rule for functional composition as well. For example, $f \circ g \circ h$ is officially $(f \circ g) \circ h$. However, function composition is associative, so one can prove a general associativity law for composition as well.

The general commutative law states that the value of a summation or finite product does not change if we permute the terms of the sequence. This is different from the general associative law that only allows us to move parentheses. We now state and prove this law. First a definition.

Definition 21. A *permutation* of a set S is simply a bijection $S \to S$. Suppose $S = \{m, \ldots, n\}$ where $m \leq n$, and suppose (a_i) is a sequence whose domain contains S. Then a permutation of the sequence (a_i) on the domain $\{m, \ldots, n\}$ is defined to be the sequence defined by the rule $i \mapsto a_{\sigma(i)}$ for some permutation σ of S. This new sequence has domain $\{m, \ldots, n\}$ and is written $(a_{\sigma i})$.

Example 1. Let (a_i) be the sequence defined by $a_1 = 3$, $a_2 = 11$, and $a_3 = 12$. Suppose σ is the permutation of $\{1, 2, 3\}$ defined by $1 \mapsto 2$, $2 \mapsto 3$, and $3 \mapsto 1$. Then $(a_{\sigma i})$ is the sequence (b_i) where $b_1 = 11$, $b_2 = 12$, and $b_3 = 3$.

Definition 22. Suppose $a \in S$ where S is a set. A permutation σ of S is said to *fix* a if $\sigma(a) = a$.

Remark 22. Let $a, b \in S$ where S is a set. In Chapter 2 we defined a bijection $S \to S$, written $\tau_{(ab)}$, with the property that $a \mapsto b$, $b \mapsto a$, and σ fixes all other $x \in S$. This kind of permutation is called a *transposition*. It is the simplest type of permutation, aside from the identity map. In Chapter 2, we proved that a transposition has inverse equal to itself.

Theorem 57 (General Commutative Law)**.** *Suppose (a_i) is a sequence with domain containing $\{m, \ldots, n\}$ where $m \leq n$ and suppose σ is a permutation* *of* $\{m, \ldots, n\}$. *If* U *is a set with an associative and commutative binary operation written as* $+$ *then*

$$\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} a_{\sigma i}.$$

If U *is a set with an associative and commutative binary operation written multiplicatively then*

$$\prod_{i=m}^{n} a_i = \prod_{i=m}^{n} a_{\sigma i}.$$

Example 2. If σ is defined by the rule $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. Then, under the assumptions of the above theorem, we get

$$a_1 + a_2 + a_3 = a_2 + a_3 + a_1 \qquad a_1\, a_2\, a_3 = a_2\, a_3\, a_1.$$

Before considering the proof of Theorem 57, we consider a few lemmas. The first is important for facilitating the inductive step.

Lemma 58. *Suppose* $m, n \in \mathbb{Z}$ *with* $m < n$, *and suppose* $S = \{m, \ldots, n\}$. *If* σ *is a permutation of* S *with* $\sigma(n) \neq n$ *then* σ *is of the form* $\alpha \circ \tau_{(n-1\ n)} \circ \beta$ *where* α *and* β *are both permutations of* S *fixing* n.

Proof. Let $c = \sigma(n)$, let $\alpha = \tau_{(c\ n-1)}$, and let $\beta = \tau_{(n-1\ n)} \circ \alpha \circ \sigma$. Since α is a transpositions, $\alpha^{-1} = \alpha$. Similarly for $\tau_{(n-1\ n)}$. Thus

$$\begin{aligned} \alpha \circ \tau_{(n-1\ n)} \circ \beta &= \alpha \circ \tau_{(n-1\ n)} \circ \big(\tau_{(n-1\ n)} \circ \alpha \circ \sigma\big) \\ &= \alpha \circ \alpha \circ \sigma \\ &= \sigma. \end{aligned}$$

By definition of transposition, α fixes n. This implies that

$$\beta(n) = \big(\tau_{(n-1\ n)} \circ \alpha \circ \sigma\big)(n) = \big(\tau_{(n-1\ n)} \circ \alpha\big)(c) = \tau_{(n-1\ n)}(n-1) = n,$$

so β fixes n as well. □

The following lemma allows you to switch the order of the last two terms of a summation. It is an important step on the way to the more general commutative law.

Lemma 59. *Let* (a_i) *be a sequence whose domain contains* $\{m, \ldots, n\}$ *with* $m < n$. *Suppose the values of* (a_i) *are in a set possessing an associative and commutative binary operation* $+$. *Let* $\tau = \tau_{(n\ n-1)}$ *be the transposition switching the last two elments of* $\{m, \ldots, n\}$. *Then*

$$\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} a_{\tau i}.$$

Proof. If $n = m + 1$ then

$$\sum_{i=m}^{n} a_i = a_m + a_n, \qquad \sum_{i=m}^{n} a_{\tau(i)} = a_{\tau(m)} + a_{\tau(n)} = a_n + a_m,$$

so the result follows from the commutative law. If $m + 1 < n$ then

$$\begin{aligned}
\sum_{i=m}^{n} a_i &= \sum_{i=m}^{n-1} a_i + a_n && \text{(Def. 13)}\\
&= \left(\sum_{i=m}^{n-2} a_i + a_{n-1}\right) + a_n && \text{(Def. 13 again)}\\
&= \sum_{i=m}^{n-2} a_i + (a_n + a_{n-1}) && \text{(Assoc, Comm. Law)}\\
&= \sum_{i=m}^{n-2} a_i + \big(a_{\tau(n-1)} + a_{\tau(n)}\big) && \text{(Def. of } \tau)\\
&= \sum_{i=m}^{n-2} a_{\tau i} + \big(a_{\tau(n-1)} + a_{\tau(n)}\big) && \text{(Lemma 50)}
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\sum_{i=m}^{n} a_{\tau i} &= \sum_{i=m}^{n-1} a_{\tau i} + a_{\tau(n)} && \text{(Def. 13)}\\
&= \left(\sum_{i=m}^{n-2} a_{\tau i} + a_{\tau(n-1)}\right) + a_{\tau(n)} && \text{(Def. 13 again)}\\
&= \sum_{i=m}^{n-2} a_{\tau i} + \big(a_{\tau(n-1)} + a_{\tau(n)}\big) && \text{(Assoc. Law).}
\end{aligned}$$

The result follows. □

Proof of Theorem 57, General Commutativity. (Proof by induction on the variable $k = n - m$). Let S be the set of all $k \in \mathbb{N}$ such that the theorem holds under the extra assumption that $n = m + k$. If $k = 0$ then the equations of the theorem are both just $a_m = a_m$. Thus $0 \in S$.

Suppose that $k \in S$. We wish to show that $k + 1 \in S$. We will only prove the equation for $\sum$ since the proof for $\prod$ is analogous. With this in mind, suppose that $n = m + (k + 1)$, that (a_i) is a sequence with domain containing $\{m, \dots, n\}$, that σ is a permutation of $\{m, \dots, n\}$, and that U is a set with an associative and commutative binary operation written as $+$.

First we consider the case where $\sigma(n) = n$. Since σ is injective, $\sigma(x) \neq n$ if $x < n$. So we can restrict σ to $\{m, \dots, n-1\}$ to get a permutation σ'. By the inductive hypothesis ($k \in S$),

$$\sum_{i=m}^{n-1} a_i = \sum_{i=m}^{n-1} a_{\sigma' i} = \sum_{i=m}^{n-1} a_{\sigma i}.$$

where the right hand equation follows from Lemma 50. Thus

$$\begin{aligned}
\sum_{i=m}^{n} a_i &= \sum_{i=m}^{n-1} a_i + a_n \qquad \text{(Def. 13)}\\
&= \sum_{i=m}^{n-1} a_i + a_{\sigma(n)} \qquad \text{(Assumption)}\\
&= \sum_{i=m}^{n-1} a_{\sigma i} + a_{\sigma(n)} \qquad \text{(See above)}\\
&= \sum_{i=m}^{n} a_{\sigma i} \qquad \text{(Def. 13).}
\end{aligned}$$

Thus the result follows for all such σ (including α and β below).

Finally, consider the case where $\sigma(n) \neq n$. By Lemma 58, we can write σ as $\alpha \circ \tau \circ \beta$ where α and β are both permutations of $\{m, \ldots, n\}$ fixing n and where $\tau = \tau_{(n-1\ n)}$. For all i in the domain, let $b_i = a_{\alpha i}$, let $c_i = b_{\tau i}$, and let $d_i = c_{\beta i}$. Observe that $d_i = a_{\sigma i}$ since $\sigma = \alpha \circ \tau \circ \beta$. So

$$\begin{aligned}
\sum_{i=m}^{n} a_i &= \sum_{i=m}^{n} b_i \qquad \text{(Previous case applied to } \alpha)\\
&= \sum_{i=m}^{n} c_i \qquad \text{(Lemma 59)}\\
&= \sum_{i=m}^{n} d_i \qquad \text{(Previous case applied to } \beta)\\
&= \sum_{i=m}^{n} a_{\sigma i} \qquad \text{(Def. of } d_i).
\end{aligned}$$

Thus the result follows in this case as well. By the Induction Axiom, $S = \mathbb{N}$. Therefore, the result holds for all $n \geq m$. $\square$

16. Summation via Iteration (Optional)

In Definition 13 summation is defined using a recursive definition, and the final (optional) sections of Chapter 1 describe why such definitions are valid. The purpose of this section is to explicitly show that our recursive definition of summation is valid by describing the definition from the point of view of iteration. Everything in this section applies, with minor notational modifications, to general finite products as well.

Let (c_i) be a sequence in U where U is a set possessing a binary operation called $+$. Let $m \in \mathbb{Z}$ be a fixed element in the domain of the sequence (c_i). In what follows we iterate a function $H\colon U \times \mathbb{Z} \to U \times \mathbb{Z}$ whose purpose is to add terms to a previous sum. This function is defined as follows:

$$H(x,j) = \begin{cases} (\, x + c_{j+1}\, ,\, j+1\,) & \text{if } j+1 \text{ is in the domain of } (c_i) \\ (\, x\, ,\, j+1\,) & \text{otherwise} \end{cases}$$

The next lemma shows how the second coordinate changes as we iterate H.

Lemma 60. *Let H^k be the kth iterate of H where $k \in \mathbb{N}$. Then the second coordinate of $H^k(x,j)$ is $j+k$.*

Proof. (sketch) Use induction on k. $\square$

The sequence (F_k) constructed below is the key to our definition of summation.

Theorem 61. *Let U be a set possessing a binary operation called $+$. Let (c_i) be a sequence of elements of U, and let $m \in \mathbb{Z}$ be in the domain of (c_i). Then there is a unique infinite sequence $F : \mathbb{N} \to U$ such that (i) $F_0 = c_m$, and (ii) for all $k \in \mathbb{N}$*

$$F_{k+1} = \begin{cases} F_k + c_{m+(k+1)} & \textit{if } m+(k+1) \textit{ is in the domain of } (c_i) \\ F_k & \textit{otherwise} \end{cases}$$

Proof. Uniqueness can be proved by induction. We leave this to the reader.

For existence, let $H\colon U \times \mathbb{Z} \to U \times \mathbb{Z}$ be as above. Define F_k to be the first coordinate of $H^k(c_m, m)$. Since $H^0 = id$, we have $F_0 = c_m$.

Next we verify the equation for F_{k+1}. By definition of F_k and by Lemma 60

$$H^k(c_m, m) = (F_k\, ,\ m+k).$$

So

$$H^{k+1}(c_m, m) = H(H^k(c_m, m)) = H(F_k, m+k).$$

If $(m+k)+1$ is in the domain of (c_i) then

$$H^{k+1}(c_m, m) = H(F_k, m+k) = \big(F_k + c_{(m+k)+1}, (m+k)+1\big).$$

Thus $F_{k+1} = F_k + c_{m+(k+1)}$. If $(m+k)+1$ is not in the domain of (c_i) then

$$H^{k+1}(c_m, m) = H(F_k, m+k) = \big(F_k, (m+k)+1\big).$$

Thus $F_{k+1} = F_k$. $\square$

Definition 23. Suppose (c_i) is a sequence with values a set U set possessing a binary operation called $+$. Suppose also that $\{m, \ldots, n\}$ is in the domain of (b_i) where $m \le n$. Let i be a variable (any unused variable will do). Let (F_j) be as in the above theorem (for our choice of (c_i) and m). Then

$$\sum_{i=m}^{n} c_i \ \stackrel{\text{def}}{=}\ F_{n-m}.$$

Remark 23. Note that the same value is defined regardless of what variable is used. Here we use i, but we can replacing with any other unused variable. For instance,

$$\sum_{i=m}^{n} c_i = \sum_{t=m}^{n} c_t.$$

Remark 24. Observe that if m is in the domain of (c_i) then

$$\sum_{i=m}^{m} c_i = F_0 = c_m.$$

and, if $\{m, \ldots, n+1\}$ is in the domain of (c_i) where $n \geq m$,

$$\sum_{i=m}^{n+1} c_i = F_{(n-m)+1} = F_{n-m} + c_{n+1} = \left(\sum_{i=m}^{n} c_i \right) + c_{n+1}.$$

From these equations it is easily proved (by induction) that Definition 13 and Definition 23 give the same value for the summation.

17. Some Formulas (Optional)

If n is a positive integer, define $n!$ as

$$n! \stackrel{\text{def}}{=} \prod_{k=1}^{n} k.$$

You can use methods from this Chapter to prove that $1! = 1$ and that $(n+1)! = (n+1)\, n!$. You can also prove that $1 \leq k \leq n$ implies $k \mid n!$.

Define $0! = 1$ as a special case. In general, you can consider 1 as the product of zero terms (in $\mathbb{Z}$ or any ring R), and 0 as the sum of zero terms (in $\mathbb{Z}$ or any additive group). This allows us to include 1 in the set of natural numbers that can be written as the product of (zero or more) primes.

If n and m are natural number, n^m was defined in Chapter 1. One can prove, by induction, that if $m \geq 1$ then

$$n^m = \prod_{i=1}^{m} n_i$$

where $n_i = n$ for all $i \in \{1, \ldots, m\}$. The right-hand side makes sense even for negative n. We will explore exponentiation further, even for negative m, in future chapters.