CHAPTER 4 SUMMARY: EXPLORING $\mathbb{Z}$

MATH 422, CSUSM. SPRING 2009. AITKEN

1. Introduction

This is an abridged form of Chapter 4 from the number systems course (Math 378). It will be used as the first unit for number theory (Math 422).

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.

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

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

Next we consider properties of finite sums $\sum a_i$ and products and $\prod a_i$.

We end this summary with three basic theorems: (i) every $n > 1$ is the product of primes (part of the Fundamental Theorem of Arithmetic), (ii) the set of prime numbers is infinite, and (iii) for any fixed base $B > 1$, every integer has a unique base B representation.

Date: January 20, 2009.

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.

Absolute value is compatible with multiplication.

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

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

Exercise 1. 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 $-n < a < n$.*

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

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.

Theorem 5 (Base step 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*

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

Here is a finite version of the above:

Theorem 6. *Let b and c be integers with $b \le c$, 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 $b \le n < c$. Then*

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

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*

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

Then

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

Proof. Let E be the set of all integers $x \ge b$ 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, $\{b, \dots, m-1\} \subseteq S$. By assumption, however, $\{b, \dots, m-1\} \subseteq S \Rightarrow m \in S$. This means $m \in S$, a contradiction. □

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

$$\{b, \dots, n-1\} \subseteq S \implies n \in S \qquad \forall\, n \ge b$$

with $n \ge b$ 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 $n \ge b$ 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 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 $d \mid b$.

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 $a \ne 0$).

Exercise 2. 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 3. So $a \mid 0$ for all $a \in \mathbb{Z}$. Show, however, that $0 \nmid a$ for all $a \neq 0$.

Exercise 4. 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 5. 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 6. 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 $|d| \leq |a|$.*

Exercise 7. 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 8. 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?

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.

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 9. 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 $b = ac$.*

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 $b = a \cdot (b/a)$.*

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 $|a| \geq 1$. 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 $r \overset{\text{def}}{=} b + (-qa)$. 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 $0 \leq r < |a|$ and $0 \leq r' < |a|$. Then,

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

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

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

So $|q' - q| \cdot |a| < |a|$. This means $|q' - q| < 1$. 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 $\operatorname{Rem}(b, a)$ is defined to be the remainder when dividing b by a.

Exercise 10. Prove the following:

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

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

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

Exercise 11. Find the quotient and remainder of dividing 20 by 9. Find the quotient and remainder of dividing -30 by 7.

Exercise 12. What is $\operatorname{Rem}(109, 7)$, $\operatorname{Rem}(-109, 7)$, $\operatorname{Rem}(-70, 7)$?

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 $b \mid m$.

Exercise 13. 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 $x \leq |a|$. Thus S has an upper bound. By a result of Chapter 3, S has a maximum. □

Exercise 14. 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. □

Exercise 15. 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 16. 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 17. 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 18. Prove the above theorem.

Exercise 19. 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. □

Exercise 20. 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 $p \nmid a$). □

Exercise 21. 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 22. Show that, in the above proof, the assumption $b = 1$ leads to a contradiction. Show that $b = n$ also leads to a contradiction.

8. Summation

We use the notation

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

to denote 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 an associative binary operation called $+$. The formal definition takes the following recursive form:

Remark 7. The variable i in the above definition is a bound variable (also called a "dummy variable") which means that 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 8. It is important to allow U to be any set with an additive binary operation. This allows us to use the summation notation in a wide variety of settings (including $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Theorem 38 (General Distributive Law)**.** *Let R be a ring.*[1] *Let c be a constant and let $(b_m, \ldots, b_n)$ be a sequence such that $c \in R$ and each $b_i \in R$. Then*

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

Exercise 23. Show that the usual distributive law is just the special case of the above theorem where $m = 1$ and $n = 2$.

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

Theorem 39. *Let R be a ring.*[2] *Suppose that $(b_m, \dots, b_n)$ and $(c_m, \dots, c_n)$ are two sequences in R,. Then*

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

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

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

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

Theorem 41. *Suppose $(b_m, \dots, b_n)$ is a sequence in $\mathbb{Z}$ (or in any additive abelian group). Then*

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

Theorem 42 (General Associative Law)**.** *Let $(b_l, \dots, b_n)$ 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 $l \leq m-1$ and $m \leq n$.*

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

Theorem 43. *Suppose that $(b_m, \dots, b_n)$ is a sequence with values in a set U with binary operation $+$. Then*

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

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 10. A *permutation* of a set S is simply a bijection $S \to S$. Suppose $S = \{m, \dots, n\}$ where $m \leq n$, and suppose $(a_m, \dots, a_n)$ is a sequence. Then a permutation of the sequence $(a_m, \dots, a_n)$ is defined to be the sequence defined by the rule $i \mapsto a_{\sigma(i)}$ for some permutation σ of S. This new sequence 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 $b_3 = 3$.

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

Theorem 44 (General Commutative Law)**.** *Suppose $(a_m, \ldots, a_n)$ where $m \le n$ 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*

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

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

$$a_1 + a_2 + a_3 = a_2 + a_3 + a_1.$$

9. General Finite Products

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 most of the statements and their proofs is purely notational.

We use the notation

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

to denote 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 an associative binary operation that is written multiplicatively.

Theorem 45 (General Associative Law)**.** *Suppose U is a ring, or at least a set with an associative binary operation written in multiplicative notation. Let $(b_l, \ldots, b_n)$ be a finite sequence in U. Suppose $l, m, n \in \mathbb{Z}$ satisfy the inequalities $l \le m - 1$ and $m \le n$. Then*

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

Now we consider divisibility properties of general finite products.

Theorem 46. *Suppose $(a_m, \ldots, a_n)$ is a sequence with values in $\mathbb{Z}$. Then, for each $i \in \{m, \ldots, n\}$,*

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

Theorem 47. *Let R be a commutative ring.*[3] *Suppose that $(b_m, \ldots, b_n)$ and $(c_m, \ldots, c_n)$ are two sequences in R. Then*

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

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 $(b_m, \ldots, b_n)$ is a sequence with values in a set U with a binary operation written multiplicatively. Then*

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

Theorem 50 (General Commutative Law)**.** *Suppose $(a_m, \ldots, a_n)$ where $m \le n$ and suppose σ is a permutation of $\{m, \ldots, n\}$. 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 3. If n is a positive integer, define $n!$ as

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

With the above laws once can prove that $1! = 1$ and that $(n+1)! = (n+1)\, n!$. One can also prove that $1 \le k \le n$ 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.

10. Prime Factorization

We now show that every $n \ge 2$ has a prime factorization. We will use strong induction in the proof.

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

Theorem 51. *Let n be an integer with $n \geq 2$. Then there is a finite sequence of primes numbers $(p_1, \ldots, p_k)$ such that*

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

Proof. Let S be the set of integers $n \geq 2$ for which there is such a sequence of primes whose product is n. Observe that if p is a prime then $p \in S$. To see this, let $p_1 = p$ and $k = 1$. then $\prod_{i=1}^{1} p_1 = p$, so this sequence with one term suffices.

We will now use strong induction to show that every n with $n \geq 2$ is in S. The base case $2 \in S$ has already been shown since 2 is a prime.

Now, as is usual in strong induction, 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 $n = pm$ 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. Otherwise, $m \geq 2$. We also have $m < n$ since $p > 1$. Hence $m \in S$ by the inductive hypothesis. So there is a sequence $(p_i)_{i=1,\ldots,k}$ of primes with

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

Let $p_{k+1} = p$. So

$$\prod_{i=1}^{k+1} p_i = \prod_{i=1}^{k} p_i \cdot \prod_{i=k+1}^{k+1} p_i = \left(\prod_{i=1}^{k} p_i\right) \cdot p_{k+1} = mp = n$$

Hence $n \in S$. By t

he principle of strong induction, $S = \{n \mid n \geq 2\}$. The result follows from our definition of S. □

Exercise 24. Illustrate Theorem 51 for the integers 12, 20, 5, and 84. For $n = 12$ find three different sequences that work.

Remark 9. 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 one sequence can be obtained by permuting the terms of the other. We will see this later.

11. Infinitude of Primes

Now we give a proof of Euclid's classic theorem that there are an infinite number of primes.

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

Proof. Suppose otherwise that $\mathcal{P}$ is finite. By the definition of finite (Chapter 2) this means there is a bijection $\{1, \ldots, k\} \to \mathcal{P}$ for some k. In other words, there is a sequence $(p_1, \ldots, p_k)$ whose values give all elements of $\mathcal{P}$.

Let

$$N \overset{\text{def}}{=} 1 + \prod_{i=1}^{k} p_i.$$

By Theorem 32, there is a prime p dividing N. Since p is a prime, $p = p_i$ for some $1 \leq i \leq k$. Thus p divides $\prod_{i=1}^{k} p_i$ (Theorem 46).

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 sum (Corollary 12) which is 1. Thus $p \leq 1$ (Theorem 13). This contradicts the fact that all primes are greater than one. □

12. Base B representations of integers

We conclude with the following result: given a base $B > 1$ every positive integer has a unique base B representation.

Definition 11. Let $B > 1$ be a fixed base. A *base B representation* of an integer $n > 0$ is a sequence $(d_0, \ldots, d_k)$ where each $0 \leq d_i < B$ but $d_k \neq 0$, and where

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

The number d_i is called the *i-th digit* of n.

Example 4. The base 8 (or 'octal') representation of 3872 is $d_0 = 0$, $d_1 = 4$, $d_2 = 4$, $d_3 = 7$

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

Traditionally this would be written as $(7, 4, 4, 0)$, or even $(7440)_8$.

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

Proof. 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 $d_0 = n$. Thus all $n \in S$.

In particular, we have the base case $1 \in S$ of strong induction.

Now we wish to show $n \in S$ assuming that $\{1, \ldots, n-1\} \subseteq S$. By the above argument, we have $n \in S$ if $n < B$, so we focus on the case $n \geq B$.

By the Quotient-Remainder Theorem, $n = qB + r$ for some q and r with $r \in \{0, \ldots, B-1\}$. Since $1 \le q < n$, we have $q \in S$ by hypothesis. 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 $1 \le i \le k$, 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. In particular, if there is another base B representation

$$n = \sum_{i=0}^{k'} d'_{i-1} B^i$$

then clearly $k' > 0$ since $n \ge B$, and

$$n = B \sum_{i=1}^{k'} d'_i B^{i-1} + d'_0.$$

So the remainder, when dividing n by B, is d'_0 and the quotient is

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

By uniqueness of remainder and quotient, $r = d'_0$ and

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

From the assumption that $q \in S$, and the uniqueness of remainder, we get that the representation agrees with the earlier representation. Thus $n \in S$.

By the principle of strong induction, $S = \{n \mid n \ge 1\}$. The result follows from our definition of S. □