CHAPTER 5: MODULAR ARITHMETIC

LECTURE NOTES FOR MATH 378 (CSUSM, SPRING 2009). WAYNE AITKEN

1. Introduction

In this chapter we will consider congruence $\equiv$ modulo m, and explore the associated arithmetic called *modular arithmetic*. This will lead us to the system $\mathbb{Z}_m$ where m is a positive integer. Unlike other number systems, $\mathbb{Z}_m$ is finite: it has m elements. We will define an addition and multiplication operation on $\mathbb{Z}_m$, and show that they have many of the same properties that one finds in other number systems. In fact, we will prove that $\mathbb{Z}_m$ has enough arithmetic properties to be a commutative ring.

We will determine which elements of $\mathbb{Z}_m$ have multiplicative inverses. These will be called the *units* of $\mathbb{Z}_m$. The set of units forms an abelian group. When $m = p$ is a prime, we will show further that every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse. This will show that $\mathbb{Z}_p$ is a *field*. We will sometimes write $\mathbb{F}_p$ for $\mathbb{Z}_p$ to indicate that we are indicating a field with p elements. We will consider fields in general.

We will end with a discussion of negative exponents for units, and show that such exponentiation satisfies the usual properties.

2. Congruence modulo m

Let m be a fixed positive integer. We call m the *modulus*.

Definition 1. If $a, b \in \mathbb{Z}$ are such that $\mathrm{Rem}(a, m) = \mathrm{Rem}(b, m)$, then we say that a and b are *congruent* modulo m and write

$$a \equiv b \mod m \qquad \text{or} \qquad a \equiv_m b.$$

Remark 1. Recall that whenever the word *if* is used to define a new concept, it really means, from a logical point of view, *if and only if.* The above gives an example of this. The definition stipulates that

$$\mathrm{Rem}(a, m) = \mathrm{Rem}(b, m) \iff a \equiv b \bmod m \iff a \equiv_m b.$$

Remark 2. The abbreviation "mod m" is short for "modulo m", which in Latin means "using modulus m".

Theorem 1. *Fix m. Then $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.*

Exercise 1. Prove the above.

Date: March 21, 2009.

A very common use of congruences is to assert $a \equiv r \bmod m$ where r is the remainder $\mathrm{Rem}(a, m)$. This is supported in the following theorem. For example, one would commonly say $7 \equiv 2 \bmod 5$. However, this is not the only valid use of congruences. One could also say that $7 \equiv 17 \bmod 5$, or $7 \equiv 7 \bmod 5$, or even $7 \equiv -13 \bmod 5$.

Theorem 2. *If $a, m \in \mathbb{Z}$ with $m > 0$ then*

$$a \equiv \mathrm{Rem}(a, m) \mod m.$$

Lemma 3. *If $0 \le c < m$ then $\mathrm{Rem}(c, m) = c$.*

Proof of Lemma. Since $c = 0 \cdot m + c$ and $0 \le c < m$, the Quotient-Remainder Theorem (Ch. 4) forces c to be the remainder $\mathrm{Rem}(c, m)$. □

Proof of Theorem. Let $r = \mathrm{Rem}(a, m)$. Since $0 \le r < m$ we have $r = \mathrm{Rem}(r, m)$ by the above lemma. Thus $\mathrm{Rem}(a, m) = \mathrm{Rem}(r, m)$. By definition of congruence, $a \equiv_m r$. □

Since congruence is reflexive, an equality can always be converted to a congruence. The following says that for small integers, a congruence can be converted to an equality.

Theorem 4. *Suppose $a, b, m \in \mathbb{N}$. Suppose also that $0 \le a < m$ and $0 \le b < m$. Then*

$$a \equiv_m b \iff a = b.$$

Proof. Assume $a \equiv_m b$. Thus $\mathrm{Rem}(a, m) = \mathrm{Rem}(b, m)$ by Definition 1. By Lemma 3, $\mathrm{Rem}(a, m) = a$ and $\mathrm{Rem}(b, m) = b$. Thus $a = b$.

The other direction follows from the fact that $\equiv_m$ is reflexive (congruence is an equivalence relation). □

Corollary 5. *Suppose $a, m \in \mathbb{Z}$ with $m > 0$. Then there is exactly one $b \in \{0, \dots, m-1\}$ such that*

$$a \equiv b \mod m.$$

Exercise 2. Justify the above corollary. Hint: use Theorems 2 and 4.

The following is another characterization of congruence. It is often chosen as the definition of congruence in number theory books.

Theorem 6. *Let $a, b \in \mathbb{Z}$. Let m be a positive integer. Then*

$$a \equiv_m b \iff m \mid (a - b).$$

Proof. Suppose $a \equiv b$ modulo m. Then a and b have the same remainder (but perhaps different quotients). So we have $a = qm + r$ and $b = q'm + r$ for some $q, q' \in \mathbb{Z}$. Thus

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

This implies that $m \mid (a - b)$.

Suppose $m \mid (a - b)$. So $a - b = cm$ for some $c \in \mathbb{Z}$. Thus $a = b + cm$. Apply the Quotient Remainder Theorem (Ch. 4) to b giving us $b = qm + r$ with $0 \le r < m$. Thus

$$a = b + cm = (qm + r) + cm = (q + c)m + r.$$

Since $0 \le r < m$, this implies that the quotient and remainder for a divided by m are $q + c$ and r respectively. In particular, a and b have the same remainder r. Thus $a \equiv b \bmod m$. □

Exercise 3. Use the above theorem to show that $a \equiv b$ modulo 1 is always true (for all $a, b \in \mathbb{Z}$).

3. Modular Arithmetic

The first rule of modular arithmetic allows you to add a constant to both sides of a congruence.

Theorem 7. *Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$.*

$$a \equiv b \mod m \implies a + c \equiv b + c \mod m.$$

Proof. By Theorem 6, $m \mid (a - b)$. But

$$(a + c) - (b + c) = a + c + (-b) + (-c) = a - b.$$

So $m \mid \big((a + c) - (b + c)\big)$. The conclusion follows from Theorem 6. □

Using the above twice gives the following

Theorem 8. *Let $a, b, a', b', m \in \mathbb{Z}$ with $m > 0$.*

$$a \equiv_m a' \quad \text{and} \quad b \equiv_m b' \quad \implies \quad a + b \equiv_m a' + b'.$$

Proof. By Theorem 7, we can add a to both sides of $b \equiv_m b'$:

$$a + b \equiv a + b' \mod m$$

By Theorem 7 again, we can add b' to both sides of $a \equiv_m a'$:

$$a + b' \equiv a' + b' \mod m$$

Now use transitivity. □

Informal Exercise 4. Illustrate Theorems 8 and 10 with several examples.

Not only can you add constants to congruences, you can multiply constants to congruences.

Theorem 9. *Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$.*

$$a \equiv_m b \implies ac \equiv_m bc.$$

Exercise 5. Use Theorem 6 to prove the above.

Theorem 10. *Let $a, b, a', b', m \in \mathbb{Z}$ with $m > 0$.*

$$a \equiv_m a' \quad \text{and} \quad b \equiv_m b' \quad \implies \quad ab \equiv_m a'b'.$$

Exercise 6. Prove the above. Hint: see Theorem 8 for ideas.

Exercise 7. Let $a, b, m, n \in \mathbb{Z}$ where $n \geq 0$ and $m > 0$. Prove, by induction, that if $a \equiv_m b$, then $a^n \equiv_m b^n$.

Informal Exercise 8. Use congruences to show that adding 52 hours to a clock is the same as adding 4 to a clock.

Informal Exercise 9. Ignoring the effect of leap years, consecutive birthdays differ by 365 days. Suppose this is so, where the first of the consecutive birthdays occurs on a Friday. Use congruences to show that the second of the consecutive birthdays must be on a Saturday.

Exercise 10. Suppose that $a, m \in \mathbb{Z}$ with $m > 0$. Show that you can freely add or subtract m in a congruence:

$$a \equiv a + m \equiv a - m \mod m.$$

For instance, if you are given $a = -6$ and $m = 8$, you could add 8 and conclude $-6 \equiv 2$ modulo 8.

Exercise 11. Suppose that $a, k, m \in \mathbb{Z}$ with $m > 0$. Suppose $d \mid m$ where $d > 0$. Show that if $a \equiv_m b$ then $a \equiv_d b$. Hint: use Theorem 6.

4. Application to finding remainders

In this section we give quick ways to find remainders when we divide by various small integers. The technique is based on writing a number in base 10, but it generalizes easily to other bases.

Exercise 12. Show that

$$10^n \equiv 1^n \equiv 1 \mod 9$$

and

$$10^n \equiv 1 \mod 3.$$

for all $n \in \mathbb{N}$.

Informal Exercise 13. Let s be the sum of the digits of a number $n \in \mathbb{N}$ written in base 10. Show that

$$n \equiv s \mod 9$$

and

$$n \equiv s \mod 3.$$

Informal Exercise 14. Use the sum of the digits method to find Rem(3783, 9) and Rem(12345, 3). What is the closest number to 45,991 that is divisible by 9?

Informal Exercise 15. Derive your own procedure for finding $\text{Rem}(n, 7)$ where $n \in \mathbb{N}$ has up to three digits. Hint: work with 10^k modulo 7 for $k = 0, 1, 2$. Use this procedure to find Rem(249, 7) and Rem(723, 7).

Exercise 16. Prove (without induction) that

$$B^n \equiv 0 \mod B$$

for all positive integers B and n. Hint: write n as $m+1$.

Informal Exercise 17. Show that if n is a natural number, and m is the last digit of n written in base B, then $n \equiv m \bmod B$. What is a quick way to find the remainder of $n \in \mathbb{N}$ when you divide by 10? what is $\mathrm{Rem}(12329392912012, 10)$? What is the remainder of $[1000000000003574]_{16}$ when you divide by 16?

Exercise 18. Show that $10^n \equiv (-1)^n \bmod 11$. Hint: use Exercise 7.

Informal Exercise 19. Let $n \in \mathbb{N}$, and write n in base 10 as

$$n = \sum_{i=0}^{k} d_i 10^i.$$

Show that

$$n \equiv \sum_{i=0}^{k} (-1)^i d_i \mod 11.$$

Use this to find the remainder of $156,347$ when dividing by 11.

Informal Exercise 20. Observe that $4 \mid 10^2$. Show that to find $\mathrm{Rem}(n, 4)$, you just need to replace $n \in \mathbb{N}$ with the number formed from the last two digits of n. Show that if d_1 and d_0 are the last two digits, then $n \equiv 2d_1 + d_0 \bmod 4$.

Informal Exercise 21. How many digits do you need to consider when calculating $\mathrm{Rem}(n, 8)$? Explain why.

Informal Exercise 22. How many digits do you need to consider when calculating $\mathrm{Rem}(n, 5)$ or $\mathrm{Rem}(n, 2)$? Explain why.

Informal Exercise 23. Find the remainder of 337 when dividing by $2, 3, 4, 5, 7, 9, 10$, and 11 using the techniques in this section.

Informal Exercise 24. Give short cuts for finding the remainder of the number $[100010453000001]_8$ when dividing by $7, 8$ or 9.

5. Even and Odd

By Corollary 5, if $a \in \mathbb{Z}$ then exactly one of the following can occur:

$$a \equiv 0 \mod 2 \qquad \text{or} \qquad a \equiv 1 \mod 2.$$

Definition 2. If $a \equiv 0 \bmod 2$ then a is called an *even* integer.
If $a \equiv 1 \bmod 2$ then a is called an *odd* integers.

Theorem 11. *An even integer plus an even integer is even. An odd integer plus an odd integer is even. An even integer plus an odd integer is odd. An even integer times an even integer is even. An odd integer times an odd integer is odd. An even integer times an odd integer is even.*

Proof. We consider the case of two odd integers. The other cases are left to the reader. If $a, b \in \mathbb{Z}$ are odd then by Theorem 8

$$a + b \equiv 1 + 1 \equiv 2 \equiv 0 \mod 2,$$

so $a + b$ is even. Also, by Theorem 10,

$$ab \equiv 1 \cdot 1 \equiv 1 \mod 2$$

so ab is odd. □

Exercise 25. Prove the other cases in the above theorem.

6. The finite ring $\mathbb{Z}_m$.

Since $\equiv_m$ is an equivalence relation, we can consider the equivalence classes under this relation. The set of equivalence classes $\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ will be shown to be a ring (after we define a suitable $+$ and $\cdot$).

At first one might think that this ring $\mathbb{Z}_m$ is infinite since, for each $a \in \mathbb{Z}$, we can form the equivalence class $[a]$. However, due to the properties of $\equiv_m$, the number of elements in $\mathbb{Z}_m$ is just m.

Definition 3. Fix a positive integer m, and consider the equivalence relation $\equiv_m$ defined above. If $a \in \mathbb{Z}$, then let $[a]$ denote the equivalence class containing a under this relation. In other words, $[a] = \{x \in \mathbb{Z} \mid x \equiv_m a\}$. Define

$$\mathbb{Z}_m = \big\{[a] \mid a \in \mathbb{Z}\big\}.$$

We call $\mathbb{Z}_m$ the set of *integers modulo m*. We often write $\overline{a}$ for $[a]$. We also write $[a]_m$ when we want to be clear about the modulus.

Informal Exercise 26. Describe the set $[5]$ if $m = 1$. Show that $[5] = [-1]$ in this case.

Informal Exercise 27. Describe the set $[5]$ if $m = 2$. Show that $[5]$ consists of the odd integers.

Informal Exercise 28. Describe the set $[5]$ if $m = 3$. Show that $[5] = [2]$.

Informal Exercise 29. Describe the sets $[0], [1]$, and $[2]$ if $m = 3$.

Theorem 12. *Let m be a positive integer and $a, b \in \mathbb{Z}$. Then*

$$a \equiv_m b \iff [a] = [b].$$

Proof. This is a general fact about equivalence classes (from set theory). □

Corollary 13. *Let m be a positive integer and $a, b \in \mathbb{Z}$. Then*

$$[a]_m = [b]_m \iff \mathrm{Rem}(a, m) = \mathrm{Rem}(b, m) \iff m \mid (a - b)$$

Proof. These conditions are all equivalent to $a \equiv_m b$ by earlier results. □

The following shows that when working in $\mathbb{Z}_m$ we can always limit ourselves to $[b]$ with $0 \le b < m$.

Theorem 14. *Suppose $[a] \in \mathbb{Z}_m$ where m is a positive integer. Then there is exactly one $b \in \{0, \ldots, m-1\}$ such that $[a] = [b]$.*

Proof. Combine Corollary 5 with Theorem 12. □

Corollary 15. *Let m be a positive integer. The rule $x \mapsto [x]$ defines a bijection $f : \{0, \ldots, m-1\} \to \mathbb{Z}_m$.*

Proof. We show that f is injective and surjective. Suppose $f(x) = f(y)$ where $x, y \in \{0, \ldots, m-1\}$. Then $[x] = [y]$. So $x \equiv y$ modulo m by Theorem 12. Therefore, $x = y$ by Theorem 4

Now we show f is surjective. Let $[a] \in \mathbb{Z}_m$ be an arbitrary element. We must find something in the domain that maps to $[a]$. By Theorem 14 there is a unique $b \in \{0, \ldots, m-1\}$ such that $[a] = [b]$. Thus $f(b) = [a]$. So f is surjective. □

Corollary 16. *Let m be a positive integer. The set $\mathbb{Z}_m$ has m elements.*

Proof. The above corollary gives a bijection $\{0, \ldots, m-1\} \to \mathbb{Z}_m$. However, $\{0, \ldots, m-1\}$ has m elements (Chapter 3). Thus $\mathbb{Z}_m$ has m elements (Chapter 2). □

Now we consider addition and multiplication in $\mathbb{Z}_m$.

Informal Exercise 30. Show that $[3] + [7] = [1]$ in $\mathbb{Z}_9$ using the following definition of addition (and Theorem 12). Hint: first show $[3] + [7] = [10]$.

Definition 4. Let m be a positive integer. Suppose $[a], [b] \in \mathbb{Z}_m$. Then $[a] + [b]$ is defined to be $[a + b]$ where addition inside [ ] is as in Chapter 3. This defines a binary operation

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m.$$

Since this definition involves equivalence classes, and since there are several ways to denote the same class, we need to show that the definition of addition is well-defined. This is done in the following lemma.

Lemma 17. *Let m be a positive integer. If $[a] = [a']$ and $[b] = [b']$ in $\mathbb{Z}_m$ then*

$$[a] + [b] = [a'] + [b'].$$

Proof. By Theorem 12, $a \equiv_m a'$ and $b \equiv_m b'$. Then $a + b \equiv_m a' + b'$ by Theorem 8. So, by Theorem 12, $[a + b] = [a' + b']$. □

Many of the properties of addition for $\mathbb{Z}$ also apply to $\mathbb{Z}_m$. For example, we prove the commutative law.

Theorem 18. *Let $[a], [b] \in \mathbb{Z}_m$ where m is a positive integer. Then*

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

Proof. Observe

$$\begin{aligned}[a]+[b] &= [a+b] \qquad &&\text{(Def. of addition in } \mathbb{Z}_m)\\ &= [b+a] &&\text{(Comm. Law for + in } \mathbb{Z}\text{: Ch. 3)}\\ &= [b]+[a] &&\text{(Def. of addition in } \mathbb{Z}_m).\end{aligned}$$

□

Exercise 31. Prove the associative law of addition for $\mathbb{Z}_m$.

Now we turn our attention to multiplication.

Informal Exercise 32. Show that $[3]\cdot[7]=[3]$ in $\mathbb{Z}_9$ using the following definition of multiplication (and Theorem 12 or Corollary 13).

Definition 5. Let m be a positive integer. Suppose $[a],[b]\in\mathbb{Z}_m$. Then $[a]\cdot[b]$ is defined to be $[ab]$, where multiplication inside [ ] is as in Chapter 3. This defines a binary operation

$$\cdot : \mathbb{Z}_m\times\mathbb{Z}_m\to\mathbb{Z}_m.$$

As with the definition of addition on $\mathbb{Z}_m$, we need to show that this definition is well-defined. This is done in the following lemma.

Lemma 19. *Let m be a positive integer. If $[a]=[a']$ and $[b]=[b']$ in $\mathbb{Z}_m$ then*

$$[a]\cdot[b]=[a']\cdot[b'].$$

Proof. Combine Theorem 12 with Theorem 10. □

Exercise 33. Let $[a],[b]\in\mathbb{Z}_m$ where m is a positive integer. Then show

$$[a]\cdot[b]=[b]\cdot[a].$$

Now we come to the key theorem of the section.

Theorem 20. *Let m be a positive integer. Then $\mathbb{Z}_m$ is a commutative ring with additive identity $[0]$ and multiplicative identity $[1]$. The additive inverse of $[a]$ is $[-a]$.*

Exercise 34. Prove the above theorem. Hint: some pieces have been done in earlier theorems and exercises. For example, if you want to show $[0]$ is the additive identity, you only need to show $[a]+[0]=[a]$ since $[0]+[a]=[a]+[0]$ from an earlier theorem.

Exercise 35. Show that the additive inverse of $[a]\in\mathbb{Z}_m$ is $[m-a]$. Show that $\overline{2}$ is the additive inverse of $\overline{3}$ in $\mathbb{Z}_5$.

Remark 3. Since the additive inverse of $[a]$ is $[-a]$ you can write

$$-[a]=[-a]$$

where the first $-$ signifies inverse in $\mathbb{Z}_m$, and the second $-$ signifies inverse in $\mathbb{Z}$.

Remark 4. Using the notation $\overline{a}$ for $[a]$ we can write the above definitions and results as

$$\overline{a+b} = \overline{a} + \overline{b} \qquad \overline{ab} = \overline{a}\,\overline{b} \qquad -\overline{a} = \overline{-a} = \overline{m-a}.$$

The additive identity is $\overline{0}$. The multiplicative identity is $\overline{1}$.

Remark 5. In any ring, 0 customarily denotes the additive identity. So we can write

$$0 = [0] = \overline{0}$$

where the left 0 is the identity in $\mathbb{Z}_m$ and the middle and right 0 is the identity in $\mathbb{Z}$. Likewise, 1 can denote the multiplicative identity in any ring:

$$1 = [1] = \overline{1}$$

where the left 1 is the identity in $\mathbb{Z}_m$ and the middle and right 1 is the identity in $\mathbb{Z}$.

Informal Exercise 36. Make addition and multiplication tables for $\mathbb{Z}_m$ for $m = 1, 2, 3, 4, 5, 6$. Your answers should be in the form $\overline{a}$ where $0 \le a < m$, but to save time you do not have to write bars over the answer: if you write '3', everyone will know that you actually mean $\overline{3}$. Hint: use the commutative law to save time.

Exercise 37. Suppose m is a positive integer, and that $m = ab$ where a and b are positive and less than m (in other words, suppose that m is composite). Show that $\mathbb{Z}_m$ is not an integral domain.

Later, we will show that $\mathbb{Z}_p$ is an integral domain if p is a prime number.

7. Units in a ring

Every element in a ring has an additive inverse, but only some elements have multiplicative inverses. Any element with a multiplicative inverse is called a *unit*. Recall that we assume all rings have a multiplicative identity.

Definition 6. Let R be a ring with multiplicative identity 1. If $a, b \in R$ are such that $ab = ba = 1$ then we say that a and b are multiplicative inverses. We write $b = a^{-1}$ and $a = b^{-1}$ to indicate that b is the inverse of a and a is the inverse of b. If R is commutative, we only need to check $ab = 1$.

An element $a \in R$ is called a *unit* if it has an inverse. The set of units is written $R^\times$:

$$R^\times \overset{\text{def}}{=} \{u \in R \mid u \text{ is a unit}\}.$$

Observe that $R^\times$ is a subset of R.

Warning. The above use of the superscript -1 is different than its use in iteration.

Informal Exercise 38. What are the units of $\mathbb{Z}$? In other words, what is $\mathbb{Z}^\times$?

Informal Exercise 39. Make a multiplication table for $\mathbb{Z}_9$. Use it to find $\mathbb{Z}_9^\times$. List all the inverses of all the units. To save time, you do not have to use bars or brackets in the tables. Hint: remember how to find remainders modulo 9, and use the fact that multiplication is commutative.

Informal Exercise 40. Are $\mathbb{Z}^\times$ and $\mathbb{Z}_9^\times$ closed under addition?

Exercise 41. Let a be an element of a ring R. Show that if a is a unit, then its multiplicative inverse is unique.

Exercise 42. Show that 1 and -1 are units in any ring R. Show that if R is a ring with $0 \neq 1$ then 0 is not a unit. (Most rings have $0 \neq 1$. The *trivial ring* is an exception: it has only one element so all elements are equal).

Exercise 43. Show that if u is a unit in a ring R then so is u^{-1}, and that

$$\left(u^{-1}\right)^{-1} = u.$$

Here is the main theorem of this section. It tells us which elements of $\mathbb{Z}_m$ are units.

Theorem 21. *Let $\overline{a} \in \mathbb{Z}_m$ where m is a positive integer. Then $\overline{a}$ is a unit if and only if a and m are relatively prime.*

Proof. Suppose that $\overline{a}$ is a unit. This means that there is a $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod m$. In other words, m divides $ab - 1$. In particular, $ab - 1 = mc$ for some $c \in \mathbb{Z}$. So $ab - cm = 1$. Any common divisor of a and m must divide the linear combination $ab - cm = 1$ (Section 6 of Chapter 4). Thus the only positive common divisor of a and m is 1. This means that a and m are relatively prime.

Now suppose that a and m are relatively prime. Consider the function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ defined by the rule $x \mapsto \overline{a}x$. We first show that f is injective. Suppose $f\left(\overline{b}\right) = f\left(\overline{c}\right)$. Then $\overline{a}\ \overline{b} = \overline{a}\ \overline{c}$. In other words, $ab \equiv_m ac$. This means that m divides $ab - ac = a(b - c)$. Clearly a also divides $a(b - c)$. Since a and m are relatively prime, we have $am \mid a(b-c)$ (Section 7, Ch. 4). Thus $m \mid (b - c)$. This means that $b \equiv_m c$, so $\overline{b} = \overline{c}$.

We conclude that f is injective. Since f is injective, and maps a finite set to itself, it must also be surjective (Chapter 2). Thus there is an element $\overline{b}$ such that $f\left(\ \overline{b}\ \right) = \overline{1}$. By definition of f, we have $\overline{a}\ \overline{b} = \overline{1}$. So $\overline{a}$ is a unit. □

Informal Exercise 44. Use the above theorem to identify $\mathbb{Z}_m^\times$ for $m = 1$ to $m = 12$. Make multiplication tables for $\mathbb{Z}_m^\times$ for $m = 1, 2, 3, 4, 5, 7, 8, 10, 12$. (To save time, you do not have to use bars or brackets in the tables.)

As the tables from the above exercise show, the set $\mathbb{Z}_m$ is closed under multiplication:

Lemma 22. *If $a, b \in R^\times$ are units in a ring R, then ab is a unit. Furthermore, $(ab)^{-1} = b^{-1}a^{-1}$. If R is commutative then $(ab)^{-1} = a^{-1}b^{-1}$*

Proof. (sketch) First show $b^{-1}a^{-1}$ is the inverse of ab. So the inverse of ab exists. In other words, ab is a unit. □

This lemma implies that for $R^\times$ multiplication gives a binary operation

$$R^\times \times R^\times \to R^\times.$$

Multiplication is associative since R is a ring, and $R^\times$ is a subset of R. Since 1 is a unit in any ring, there is an identity for this operation. Furthermore, if $u \in R^\times$ then clearly $u^{-1} \in R^\times$ (see Exercise 43). Thus every element of $R^\times$ has an inverse in $R^\times$. Thus we get the following:

Theorem 23. *If R is a ring, then the units $R^\times$ form a group under multiplication. If R is a commutative ring, then $R^\times$ is an abelian group.*

8. The field $\mathbb{F}_p$

In this section we will see that every non-zero element of $\mathbb{Z}_p$ is a unit when p is a prime. Commutative rings with this property are very important, and are called *fields*. Because $\mathbb{Z}_p$ is a field we sometimes write $\mathbb{F}_p$ for $\mathbb{Z}_p$. Since every field is an integral domain, $\mathbb{Z}_p$ is also an integral domain. We saw above that $\mathbb{Z}_m$ is not an integral domain if m is composite.

Theorem 24. *If p is a prime, then every non-zero element of $\mathbb{Z}_p$ is a unit.*

Proof. Let $\overline{a} \in \mathbb{Z}_p$ be non-zero. Observe that a is not a multiple of p (otherwise $a \equiv_p 0$, a contradiction). Since $p \nmid a$ and since p is a prime, a and p are relatively prime (Chapter 4). By Theorem 21, $\overline{a}$ is a unit. □

Definition 7. A *field* is a commutative ring F such that (i) $0 \neq 1$, and (ii) every non-zero element is a unit.

Remark 6. The conditions (i) and (ii) in the above definition can be folded into one condition: $x \in F$ is a unit if and only if $x \neq 0$.

Remark 7. Fields are extremely important in mathematics. The number systems $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. In a field you can make use of all four basic algebraic operations $+, -, \times, \div$, with the only restriction that you cannot divide by zero since zero is not a unit.

Theorem 25. *If p is a prime then $\mathbb{Z}_p$ is a field.*

Proof. Observe that (i) $\overline{0} \neq \overline{1}$ since $p > 1$. In addition, (ii) every non-zero element of $\mathbb{Z}_p$ is a unit by Theorem 24. □

Definition 8. If p is a prime, then $\mathbb{F}_p$ as another name for $\mathbb{Z}_p$. The field $\mathbb{F}_p$ is an example of a finite field.

Remark 8. Every field is an integral domain, but not all integral domains are fields. We leave the verification of these facts to the reader.

9. Exponentiation

In Chapter 1 we used the idea of repeated multiplication to define exponentiation. This idea can be extended to any ring R. For units, we can extend this idea and define exponentiation for negative exponents. Exponentiation in a general ring satisfies familiar rules such as $a^{m+n} = a^m a^n$. We have seen similar rules in the context of iteration. In fact, we will use the rules for iteration to prove the analogous rules for exponentiation.

In this section we will consider exponentiation for general elements in a ring. In the next section we will consider exponentiation of units.

Definition 9 (Exponentiation in rings)**.** Suppose R is a ring and $a \in R$. Let $M_a : R \to R$ be defined by the rule $x \mapsto xa$. If $n \in \mathbb{N}$ then

$$a^n \stackrel{\text{def}}{=} M_a^n(1).$$

Our strategy for studying exponentiation is to find identities between M_a. This approach is very similar to that used in Chapter 3 when we studied the translation function A_a. In what follows, let R be a ring.

Lemma 26. *Let $a \in R$. Then $M_a^0 = id$ and $M_a^1 = M_a$.*

Proof. These are basic properties of iteration (Chapter 1). □

Corollary 27. *Let $a \in R$. Then $a^0 = 1$ and $a^1 = a$.*

Proof. Apply M_a^0 and M_a^1 to 1. The above lemma gives the result. □

Lemma 28. *Let $a, b \in R$. Then $M_a \circ M_b = M_{ba}$.*

Proof. For any $x \in R$,

$$M_a \circ M_b(x) = M_a\big(M_b(x)\big) = M_a(xb) = (xb)a = x(ba) = M_{ba}(x).$$

The conclusion follows. □

Lemma 29. *Let $a, b \in R$. Suppose $ab = ba$ (which holds, for example, if R is a commutative ring). Then M_a and M_b commute.*

Proof. This follows from the above lemma since $M_{ab} = M_{ba}$. □

Lemma 30. *Consider the iteration M_a^n where $a \in R$ and $n \in \mathbb{N}$. Then there is an element $c \in R$ such that $M_a^n = M_c$.*

Proof. Fix $a \in R$. Let S be the set of $n \in \mathbb{N}$ such that the conclusion holds. Observe that $0 \in S_a$ since $M_a^0 = id = M_1$.

Suppose that $n \in S_a$. This means $M_a^n = M_b$ for some $b \in R$. Thus

$$M_a^{n+1} = M_a \circ M_a^n = M_a \circ M_b = M_{ba}. \qquad \text{(Lemma 28)}$$

Thus $n + 1 \in S_a$.

By induction, $S_a = \mathbb{N}$. The result follows. □

The following is very useful for deriving identities.

Lemma 31. *If $n \in \mathbb{N}$ and $a \in R$ then $M_a^n = M_{a^n}$.*

Proof. By Lemma 30, $M_a^n = M_c$ for some $c \in R$. Apply M_a^n and M_c to 1:

$$a^n \overset{\text{def}}{=} M_a^n(1) = M_c(1) = 1 \cdot c = c.$$

Thus $c = a^n$. But, $M_a^n = M_c$. So $M_a^n = M_{a^n}$ □

Lemma 32. *Let $a, b \in R$. If $M_a = M_b$ then $a = b$.*

Proof. Suppose $M_a = M_b$. Then $M_a(1) = M_b(1)$. But $M_a(1) = 1 \cdot a = a$ and $M_b(1) = 1 \cdot b = b$ □

We know from Chapter 2 that iteration satisfies the law $f^{m+n} = f^m \circ f^n$ for $m, n \in \mathbb{N}$. We use this fact in the following.

Theorem 33. *Let $a \in R$ where R is a ring, and let $m, n \in \mathbb{N}$. Then*

$$a^{m+n} = a^m a^n.$$

Proof. Observe that

$$\begin{aligned} M_{a^{m+n}} &= M_a^{m+n} && \text{(Lemma 31)} \\ &= M_a^{n+m} && \text{(Comm. Law, Ch. 1)} \\ &= M_a^n \circ M_a^m && (f^{m+n} = f^m \circ f^n, \text{ Ch. 2}) \\ &= M_{a^n} \circ M_{a^m} && \text{(Lemma 31)} \\ &= M_{a^m a^n} && \text{(Lemma 28)} \end{aligned}$$

Thus $a^{m+n} = a^m a^n$ by Lemma 32. □

Theorem 34. *Consider $0 \in R$. If n is a positive integer then*

$$0^n = 0.$$

Proof. Write n as $m + 1$. Then, using the previous theorem,

$$0^n = 0^{m+1} = 0^m 0^1 = 0^m 0 = 0.$$

□

We know from Chapter 2 that iteration of functions satisfies the law $(f^m)^n = f^{mn}$ for all $m, n \in \mathbb{N}$. We use this fact in the following.

Theorem 35. *Let $a \in R$ and $m, n \in \mathbb{N}$. Then*

$$(a^m)^n = a^{mn}.$$

Proof. Start with $M_{a^m} = M_a^m$ (Lemma 31). Then

$$\begin{aligned} (M_{a^m})^n &= \left(M_a^m\right)^n && \text{(Iterate same funct.)} \\ &= M_a^{mn} && \text{(Ch. 2: } (f^m)^n = f^{mn}) \end{aligned}$$

Apply both sides to 1:

$$(a^m)^n \overset{\text{def}}{=} (M_{a^m})^n(1) = M_a^{mn}(1) \overset{\text{def}}{=} a^{mn}.$$

□

We know from Chapter 3 that if $f : S \to S$ and $g : S \to S$ commute (for some set S) then we have $(f \circ g)^n = f^n \circ g^n$ for all $n \in \mathbb{N}$. We use this fact in the following.

Theorem 36. *Let $a, b \in R$ and $n \in \mathbb{N}$. Suppose $ab = ba$ (which is true, for example, if R is a commutative ring). Then*

$$(ab)^n = a^n b^n.$$

Proof. By Lemma 29, M_a and M_b commute. So

$$\begin{aligned}\big(M_{ab}\big)^n &= \big(M_b \circ M_a\big)^n && \text{(Lemma 28)}\\ &= M_b^n \circ M_a^n && \text{(Ch. 3: } (f \circ g)^n = f^n \circ g^n)\\ &= M_{b^n} \circ M_{a^n} && \text{(Lemma 31)}\\ &= M_{a^n b^n} && \text{(Lemma 28)}\end{aligned}$$

Apply both sides to 1:

$$(ab)^n \overset{\text{def}}{=} \big(M_{ab}\big)^n(1) = M_{a^n b^n}(1) = a^n b^n.$$

□

Exponentiation can also be thought of in terms of finite products:

Theorem 37. *Let $a \in R$ where R is a ring. If n is a positive integer then*

$$a^n = \prod_{i=1}^{n} a_i$$

where $(a_i)_{i=1,\ldots,n}$ is the constant sequence defined by the rule $a_i = a$ for all $i \in \{1, \ldots, n\}$.

Proof. (Sketch) This can be proved by induction. The details are left to the reader. □

Remark 9. If $a \in \mathbb{Z}$ then the definition of a^n given in this section agrees with the definition of Chapter 1 whenever $a \geq 0$. To see this, compare the two definitions and observe that $\mu_a(x) = M_a(x)$ for all $x \geq 0$. By induction, it follows that $\mu_a^n = M_a^n$ for all $n \in \mathbb{N}$. In particular, $\mu_a^n(1) = M_a^n(1)$.

10. Exponentiation of Units

If a is a unit in a ring R, then we can define a^u for negative $u \in \mathbb{Z}$. In what follows let R be a ring.

Lemma 38. *If $a \in R$ is a unit then M_a has an inverse function and*

$$(M_a)^{-1} = M_{a^{-1}}.$$

Proof. We know $M_a \circ M_{a^{-1}} = M_1$ by Lemma 28. But $M_1 = id$ by definition of M_a. Likewise $M_{a^{-1}} \circ M_a = id$. The conclusion follows. □

Corollary 39. *If $a \in R$ is a unit then M_a is a bijection, and M_a^u is defined for all $u \in \mathbb{Z}$.*

Now we can define a^u for all $u \in \mathbb{Z}$, even for negative u.

Definition 10. Suppose $a \in R$ is a unit and $u \in \mathbb{Z}$. Then

$$a^u \overset{\text{def}}{=} M_a^u(1).$$

Recall from Chapter 3 that if $f : S \to S$ is the identity function, then $f^u = id$ for all $u \in \mathbb{Z}$. This is used below.

Theorem 40. *Let* 1 *be the multiplicative identity of a ring* R*. If* $u \in \mathbb{Z}$ *then*

$$1^u = 1.$$

Proof. Observe that M_1 is the identity. Then M_1^u is the identity (Ch. 3). Thus $1^u = M_1^u(1) = id(1) = 1$. □

Informal Exercise 45. Find a^{-2} for all non-zero $a \in \mathbb{F}_7$. How do these compare to a^4?

The following generalizes Lemma 30.

Lemma 41. *Consider the iteration* M_a^u *where* $a \in R$ *and* $u \in \mathbb{Z}$*. Then there is an element* $c \in R$ *such that* $M_a^u = M_c$*.*

Proof. If $u \geq 0$ this follows from Lemma 41.

Now assume $u < 0$, so $u = -n$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned} M_a^u &= M_a^{-n} && \text{(Rewrite)} \\ &= \left(M_a^{-1}\right)^n && \text{(Ch. 3: } f^{uv} = (f^u)^v\text{)} \\ &= \left(M_{a^{-1}}\right)^n && \text{(Lemma 38)} \\ &= M_{a^{-1}}^n && \text{(Rewrite)} \\ &= M_{(a^{-1})^n} && \text{(Lemma 31)} \end{aligned}$$

Thus $M_a^u = M_c$ where $c = \left(a^{-1}\right)^n$. □

The following generalizes Lemma 31.

Lemma 42. *Let* $a \in R$ *be a unit. If* $u \in \mathbb{Z}$ *then* $M_a^u = M_{a^u}$*.*

Proof. (Sketch) This is similar to the proof of Lemma 31, but adapted from natural numbers to integers. □

The following generalizes Theorem 33.

Theorem 43. *Suppose* $a \in R$ *is a unit and that* $u, v \in \mathbb{Z}$*. Then*

$$a^{u+v} = a^u a^v.$$

Proof. This is similar to the proof of Theorem 33, but adapted from natural numbers to integers. □

The following generalizes Theorem 35.

Theorem 44. *Suppose* $a \in R$ *is a unit and that* $u, v \in \mathbb{Z}$*. Then*

$$(a^u)^v = a^{uv}.$$

Proof. This is similar to the proof of Theorem 35, but adapted from natural numbers to integers. □

The following generalizes Theorem 36.

Theorem 45. *Let $a, b \in R$ be units, and let $u \in \mathbb{Z}$. If $ab = ba$ then*

$$(ab)^u = a^u b^u.$$

Proof. This is similar to the proof of Theorem 36, but adapted from natural numbers to integers. □

Theorem 46. *If $a \in R$ is a unit and $u \in \mathbb{Z}$ then a^u is also a unit.*

Proof. By Theorem 43, $a^u \cdot a^{-u} = a^0$ and $a^{-u} \cdot a^u = a^0$. By Corollary 27, $a^0 = 1$. The result follows. □

Appendix: miscellaneous comments

The theory of exponentiation can be developed for groups as well. There is both an additive and a multiplicative version.