CHAPTER 5 SUMMARY: MODULAR ARITHMETIC

MATH 422, CSUSM. SPRING 2009. AITKEN

1. Introduction

This is an abridged form of Chapter 5 from the number systems course (Math 378). It will be used as part of the first unit for number theory (Math 422).

We will consider congruence $\equiv$ modulo m, and explore the associated arithmetic called *modular arithmetic*. This will lead us to the finite ring $\mathbb{Z}_m$ where m is a positive integer. 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. Hence, we will sometimes write $\mathbb{F}_p$ for $\mathbb{Z}_p$. We will briefly discuss fields in general.

We will end with a discussion of negative exponents for units and how 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 $\text{Rem}(a, m) = \text{Rem}(b, m)$, 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. The definition stipulates that

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

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.

A very common use of congruences is to assert $a \equiv r \bmod m$ where r is the remainder $\text{Rem}(a, m)$. 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 $7 \equiv -13 \bmod 5$.

Date: January 30, 2009.

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

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

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

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

Proof of Theorem. Let $r = \text{Rem}(a, m)$. Since $0 \leq r < m$ we have $r = \text{Rem}(r, m)$ by the above lemma. Thus $\text{Rem}(a, m) = \text{Rem}(r, m)$. 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 $0 \leq a < m$ and $0 \leq b < m$. Then*

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

Proof. Assume $a \equiv_m b$. Thus $\text{Rem}(a, m) = \text{Rem}(b, m)$ by Definition 1. By Lemma 3, $\text{Rem}(a, m) = a$ and $\text{Rem}(b, m) = b$. 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 $b \in \{0, \ldots, m-1\}$ 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 sometimes chosen as the definition of congruence by other authors.

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 $a \equiv b \bmod m$. 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 $0 \leq r < m$. Thus

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

Since $0 \leq r < m$, 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. Observe that $a \equiv b \bmod 1$ 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. □

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

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

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. □

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 4. Use Theorem 6 to prove the above.

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

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

Exercise 5. Prove the above. Hint: see Theorem 8 for ideas.

Exercise 6. Illustrate the above by several examples.

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 $a^n \equiv_m b^n$.

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

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 $a, k, m \in \mathbb{Z}$ with $m > 0$. Show that

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

For instance, if you are give $a = -10$ and $m = 8$, you could add 16 and conclude $-10 \equiv_8 6$.

Exercise 11. Suppose that $a, k, m \in \mathbb{Z}$ with $m > 0$. Suppose $d \mid m$ where $d > 0$. Show that if $a \equiv_m b \implies a \equiv_d b$. 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 $n \in \mathbb{N}$.

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

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

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

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 $k = 0, 1, 2$.

Exercise 16. Use the previous exercise to find $\text{Rem}(249, 7)$.

Exercise 17. Prove (without induction) that

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

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

Exercise 18. Show that if n is a natural number, and m is the last digit (i.e. the B^0 place digit d_0) digit of n written in base B, then $n \equiv m \bmod B$.

Exercise 19. What is a quick way to find the remainder of $n \in \mathbb{N}$ when you divide by 10?

Exercise 20. What is the remainder of $[100003574]_{16}$ when you divide by 16? Here $[100003574]_{16}$ is a number written in base 16 where the digits are listed from most significant ($d_8 = 1$) to least significant ($d_0 = 4$).

Exercise 21. Show that $10^n \equiv (-1)^n \bmod 11$. Hint: use Exercise 7.

Exercise 22. Let $n \in \mathbb{N}$, and write n in base 10 as

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

Show that

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

Exercise 23. Use the above to find the remainder of $156,347$ when dividing by 11.

Exercise 24. Observe that $4 \mid 10^2$. Show that to find $\text{Rem}(n, 4)$, you just need to replace $n \in \mathbb{N}$ with the number formed from the last two digits of 4. Show that if d_1 and d_0 are the last two digits, then $n \equiv 2d_1 + d_0 \mod 4$.

Exercise 25. How many digits do you need to consider when calculating $\text{Rem}(n, 8)$? Explain why.

Exercise 26. How many digits do you need to consider when calculating $\text{Rem}(n, 5)$ or $\text{Rem}(n, 2)$? Explain why.

Exercise 27. Find the remainder of 337 when dividing by $2, 3, 4, 5, 7, 9, 10$, and 11 using the techniques in this section.

Exercise 28. What is the remainder of the number $[100010453000001]_8$, written in base 8, when dividing by $7, 8$ or 9. (Do this without converting to base 10).

5. Even and Odd

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

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

In the first case, where $a \equiv 0 \bmod 2$, the integer a is even. In the second case, where $a \equiv 1 \bmod 2$, the integer a is odd.

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 29. 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 $\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ is a ring (after we define a suitable $+$ and $\cdot$).

Definition 2. 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.

Exercise 30. Describe the set $[5]$ if $m = 1$. Show that $[5] = [-1]$ in this case.

Exercise 31. Describe the set $[5]$ if $m = 2$. Show that $[5]$ consists of the odd integers.

Exercise 32. Describe the set $[5]$ if $m = 3$. Show that $[5] = [2]$.

Exercise 33. 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. □

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 $0 \leq b < m$. This means $\mathbb{Z}_m$ is actually finite.

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 $x \mapsto \overline{x}$ defines a bijection $f : \{0, \ldots, m-1\} \to \mathbb{Z}_m$.*

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

Proof. Corollary 15 describes a bijection $\{0, \ldots, m-1\} \to \mathbb{Z}_m$. Since $\{0, \ldots, m-1\}$ has m elements, the set $\mathbb{Z}_m$ has m elements. □

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

Exercise 34. 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 3. 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 the addition in $\mathbb{Z}$. 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 (or Cor. 13), $[a + b] = [a' + b']$. □

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

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

□

Exercise 35. Prove the associative law of addition for $\mathbb{Z}_m$.

Now we turn our attention to multiplication.

Exercise 36. Show that $[3] \cdot [7] = [3]$ in $\mathbb{Z}_9$ using the following definition of multiplication (and Theorem 12 or Corollary 13).

Definition 4. 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 $\mathbb{Z}$. 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 37. 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 38. 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 39. 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 $\mathbb{Z}$.

In fact we can drop the bars in general if it is clear from context that we are working in $\mathbb{Z}_m$ (and not $\mathbb{Z}$). So '3' can be used to refer to $\overline{3} \in \mathbb{Z}_5$ if it is clear from context that we are working in $\mathbb{Z}_5$. Similarly, if it is clear that we are working in $\mathbb{Z}_9$, we can write equations such as '$3 + 7 = 1$'.

Exercise 40. Make addition and multiplication tables for $\mathbb{Z}_m$ where $m = 1, 2, 3, 4, 5, 6$. (So there are twelve tables you have to make). Your answers should be in the form $\overline{a}$ where $0 \leq a < m$, but to save time you do not have to write bars over the answer (as discussed in the above remark). Hint: use the commutative law to save time.

Exercise 41. 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 5. 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 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 $R^\times$:

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

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

Exercise 42. What are the units of $\mathbb{Z}$? In other words, what is $\mathbb{Z}^\times$?

Exercise 43. Make a multiplication table for $\mathbb{Z}_9$. Use it to find $\mathbb{Z}_9^\times$. List all the inverses of all the units. Hint: remember how to find remainders modulo 9, and use the fact that multiplication is commutative.

Exercise 44. Are $\mathbb{Z}^\times$ and $\mathbb{Z}_9^\times$ closed under addition? Under multiplication?

Exercise 45. Let a be an element of a ring R. Show that if a is a unit, then its multiplicative inverse is unique.

Exercise 46. 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 47. 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 $ab - cm = 1$. 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 $ab - ac = a(b-c)$. By the following lemma, $m \mid (b-c)$. 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. □

Lemma 22. *Suppose a and m are relatively prime integers. If $m \mid ax$ where x is an integer, then $m \mid x$.*

Proof. Observe that a and m both divide ax. Thus ax is a common multiple of a and x. From a result of Chapter 4, the least common multiple of a and m is $|am|$ since a and m are relatively prime. From another result of Chapter 4, the LCM divides any common multiple. Thus $am \mid ax$. This implies $m \mid x$ if $a \neq 0$.

In the special case where $a = 0$, then m must be 1 and the result follows trivially. □

Remark 6. Once we have Bezout's identity, we can give a shorter proof of the above theorem which doesn't use the lemma.

Exercise 48. 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 $m = 1, 2, 3, 4, 5, 7, 8, 10, 12$.

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

Lemma 23. *If $a, b \in R^\times$ are units in a ring R, then ab is a unit.*

Proof. The inverse of ab exists. In fact, it is just $b^{-1}a^{-1}$. (If R is commutative, we can write $a^{-1}b^{-1}$ instead). □

This lemma implies that for $R^\times$ multiplication is 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 47). Thus every element of $R^\times$ has an inverse in $R^\times$. Thus we get the following:

Theorem 24. *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 25. *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 6. A *field* is a commutative ring such that (i) $0 \neq 1$, and (ii) every non-zero element is a unit.

Remark 7. The conditions (i) and (ii) in the above definition can be folded into one condition: x is a unit if and only if $x \neq 0$.

Remark 8. Fields are extremely important in mathematics. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

Theorem 26. *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 25. □

Definition 7. 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 9. Every field is an integral domain, but not all fields are integral domains.

9. Exponentiation

Exponentiation can be defined in $\mathbb{Z}_n$. In fact, exponentiation can be defined in any ring R. If $a \in R$ and $n \in \mathbb{N}$ then a^n can be defined as repeated multiplication.[1] Of course, a^0 is defined to be $1 \in R$. If u is a negative integer, then a^u is only defined if a is a unit in R. In this case, we can define a^u as the nth power of the inverse a^{-1} where $n = |u|$.

Here we list the properties of exponentiation.

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

Theorem 28. *Let $a \in R$ where R is a ring, and let $m, n \in \mathbb{N}$. Then*

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

Theorem 29. *Consider $0 \in R$. If n is a positive integer then*

$$0^n = 0.$$

Theorem 30. *Let $a \in R$ and $m, n \in \mathbb{N}$. Then*

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

[1]Warning: we do not claim that a^b can be defined in any ring R where $a, b \in R$. In what follows the exponent will always be an integer.

Theorem 31. *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*

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

Theorem 32. *Let 1 be the multiplicative identity of a ring R. If $u \in \mathbb{Z}$ then*

$$1^u = 1.$$

Theorem 33. *Suppose $a \in R$ is a unit and that $u, v \in \mathbb{Z}$. Then*

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

Theorem 34. *Suppose $a \in R$ is a unit and that $u, v \in \mathbb{Z}$. Then*

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

Theorem 35. *Let $a, b \in R$ be units, and let $u \in \mathbb{Z}$. If $ab = ba$ then*

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

Theorem 36. *If $a \in R$ is a unit and $u \in \mathbb{Z}$ then a^u is also a unit. Its inverse is a^{-u}.*