## 6.2 Modular Arithmetic

Every reader is familiar with arithmetic from the time they are three or four years old. It is the study of numbers and various ways in which we can combine them, such as through addition and subtraction, multiplication and division. Since even before they were in grade school, every reader knew that adding 2 and 2 together gives us 4, and can make that calculation now without almost any thinking. And even if the answer is not immediately obvious, every college student (at least in Penn), knows how to add together much larger numbers, such as 4,378,123 and 5,621,877. This is classical arithmetic, and it turns up in countless applications in our everyday lives.

The reader is also likely familiar with another kind of arithmetic, even if we don't always think of it as such. If it is 4 o'clock now, what will the time be in 25 hours? If we didn't know from watches and clocks, we would probably have answered 29 o'clock. But we are familiar with watches, clocks, and the standard conventions of time-keeping, and so every reader would probably have answered the answer with 5 o'clock. How can we add 25 to 4 and end up with 5? The reason is that in this system 25 o'clock is the same as 1 o'clock, 26 is the same as 2, and so forth. In many time-keeping systems, we don't even use numbers larger than 12, and instead use a.m. and p.m. (from the Latin *ante meridiem* and *post meridiem*) to denote the earlier and latter halves of a 24-hour period. Such systems, that "wrap around" after hitting some limit, are called **modular arithmetic systems**, and play an important role both in theoretical and applied mathematics.

Modular arithmetic motivates many questions that don't arise when studying classic arithmetic. For example, in classic arithmetic, adding a positive number $a$ to another number $b$ always produces a number larger than $b$. In modular arithmetic this is not always so. For example, if it is now 4 o'clock and we "add" 23 hours, the time will then be 3 o'clock, which doesn't appear to be larger than 4 o'clock. In fact, it is no longer clear whether it makes sense at all to discuss "larger" and "smaller" in such systems.

Here is another question. Suppose it is now 2 o'clock and we wait for 1 hour and then write down the time. We then wait another hour and mark the time, and repeat this until we eventually mark 2 o'clock again, at which point we stop. It is clear that when we stop, we will have marked down every hour. If we do the same thing but instead wait 2 or 3 hours in between each marking there will be certain hours which we never mark, such as 7 o'clock. But if we wait 5 hours between each marking, then we will eventually mark every hour. This raises the question, for which waiting intervals between marks can we ensure that we will eventually mark every hour?

While this particular example may seem contrived, it should motivate us think, if even momentarily, about modular arithmetic systems and the ways in which they are similar to and different from the classical arithmetic with which we are familiar. The next several sections will investigate these systems which have a finite number of numbers, and in which numbers "wrap around" after going too high.

The central definition in studying modular arithmetic systems establishes a relationship between pairs of numbers with respect to a special number $m$ called the *modulus*:

**Definition 25.** *Two integers $a$ and $b$ are* **congruent modulo** *$m$ if they differ by an integer multiple of $m$, i.e., $b - a = km$ for some $k \in \mathbb{Z}$. This equivalence is written $a \equiv b \pmod{m}$.*

Although this definition looks somewhat technical, the idea is very simple. For some fixed integer $m$, two numbers are roughly the same if they differ by multiples of $m$. In a sense, this definition generalizes previous discussions of odd and even numbers. In previous sections, we proved theorems such as the square of an even number is even and the square of odd number is odd. As far as even and odds numbers go, and as far as these theorems are concerned, there is no difference between 17 and 2073, as both are odd and behave the same under squaring. In a similar manner, in modular arithmetic, there is no difference between a pair of numbers that differ by the modulus $m$, which could be 2 or could be 15,485,863. In arithmetic mod 7, for example, there is no difference between 1, 8, and 15, as they all differ from one another by multiples of 7. Likewise, 22, 701 and -6 also differ from all of these numbers by multiples of 7, and are hence congruent.

**Example 1.** Every number is congruent to itself for any modulus; that is, $a \equiv a \pmod{m}$ for any $a, m \in \mathbb{Z}$. The reason for this is that $a - a = 0$, which is a multiple of $m$, since $0 = 0 \times m$ for any $m$. It might seem a bit silly, but is a consequence of the way in which we defined congruence.

**Example 2.** Every number is congruent to any other number mod 1; that is, $a \equiv b \pmod{1}$ for any $a, b \in \mathbb{Z}$. The reason for this is that $b - a$, is a multiple of 1 for any $a$ and $b$. Again, this might seem a bit silly, but is a consequence of the way in which we defined congruence.

**Example 3.** Any even numbers are congruent to one another mod 2; likewise, any odd numbers are congruent to one another mod 2. For example, we have $12 \equiv 3132 \pmod{2}$ and $-7 \equiv 19 \pmod{3}$. This is because any pair of even numbers differ from one another by a multiple of 2. Likewise, any pair of odd numbers differ from one another by a multiple of 2.

**Example 4.** The numbers 31 and 46 are congruent mod 3 because they differ by a multiple of 3. We can write this as $31 \equiv 46 \pmod{3}$. Since the difference between 31 and 46 is 15, then these numbers also differ by a multiple of 5; i.e., $31 \equiv 46 \pmod{5}$.

**Example 5.** By the definition of congruence, every pair of integers $a$ and $b$ are congruent mod 1, since any pair of integers differ by a multiple of 1. In symbols, for all integers $a$ and $b$, we have $a \equiv b \pmod{1}$.

**Example 6.** In general it is not true that $a \equiv -a \pmod{m}$, unless $m = 2$ or else $a$ is a multiple of 2. For example, it is not true that $7 \equiv -7 \pmod{3}$, since the difference between 7 and -7 is 14, which is not a multiple of 3.

**Rules of Modular Arithmetic**

After considering the basic definition of modular arithmetic, we next consider some of its basic properties. It turns out that modular arithmetic follows many of the same rules of classical arithmetic, thus making it very easy to work with. In order to highlight what is going on, we try to compare and contrast modular arithmetic to classical arithmetic.

Suppose we have two numbers $a$ and $b$:

$$\begin{aligned} a &= 5 \\ b &= 8. \end{aligned}$$

We all know that in classical arithmetic we can combine these equations to obtain:

$$a + b = 5 + 8 = 13.$$

More generally, if we have

$$\begin{aligned} a &= c \\ b &= d, \end{aligned}$$

then we can combine them in many different ways, to obtain:

$$\begin{aligned} a + b &= c + d, \\ a - b &= c - d, \\ a \times b &= c \times d. \end{aligned}$$

Pause to think about this statement, and make sure it aligns with what you know. Of course these are only several ways of combining these equations, and every reader can think of several others. All of the above are "rules" of classical arithmetic. What we would like to do now is consider whether similar rules apply to modular arithmetic as well.

Suppose we have the following two congruence relations:

$$\begin{aligned} a &\equiv b \pmod{m} \\ c &\equiv d \pmod{m}. \end{aligned}$$

Are we able to combine these to obtain

$$\begin{aligned} a + b &\equiv c + d \pmod{m}, \\ a - b &\equiv c - d \pmod{m}, \\ a \times b &\equiv c \times d \pmod{m}? \end{aligned}$$

That is, do the rules that govern how we can combine equations in classical arithmetic also govern the ways in which we combine statements in modular arithmetic? In what follows we prove that indeed many of the rules *do* carry over – the rules of modular arithmetic will be familiar to us.

**Addition**

The first rule we consider is that associated with addition. Suppose we have two congruence relations: $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. In other words, $a$ and $b$ are congruent and $c$ and $d$ are congruent, both mod $m$. We can add the left sides of these congruent relations, add the right sides, and the results will again be congruent. In symbols,

**Theorem 15.**

$$\begin{aligned} \textit{If} \qquad a &\equiv b \pmod{m} \qquad \textit{and} \\ c &\equiv d \pmod{m}, \qquad \textit{then} \\ a+c &\equiv b+d \pmod{m}. \end{aligned}$$

Proving this result involves nothing more than applying the definition of congruence and some basic algebraic manipulation.

*Proof.* By the definition of congruence (Definition 25) we know that $a$ and $b$ differ by some multiple of $m$, i.e.,

$$b - a = km \tag{64}$$

for some $k \in \mathbb{Z}$. Likewise we know that $c$ and $d$ also differ by some multiple of $m$, i.e.,

$$d - c = jm \tag{65}$$

for some $j \in \mathbb{Z}$. Note that we use $j$ instead of $k$ since the multiple of $m$ by which $c$ and $d$ differ might be different from the multiple by which $a$ and $b$ differ. Next we add these two equations together:

$$(b - a) + (d - c) = km + jm. \tag{66}$$

We can rewrite this equation as

$$(b + d) - (a + c) = (j + k)m. \tag{67}$$

By the definition of congruence modulo $m$, this is the same as saying that $a + c$ is congruent to $b + d$ modulo $m$, since $a + c$ and $b + d$ differ by an integer multiple $(j + k)$ of $m$. In symbols, we have:

$$a + c \equiv b + d \pmod{m}, \tag{68}$$

as desired. □

A similar proof can be used to show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$.

These two results allow us to treat all numbers that are congruent modulo $m$ as identical when adding and subtracting numbers. If we know that $a \equiv 3 \pmod{7}$ and $b \equiv 4 \pmod{7}$, then we can know that $a + b \equiv 7 \equiv 0 \pmod{7}$. This is true whether $a$ is 10 or 703, and whether $b$ is 7004, 10000, or 7,000,004. What $a$ and $b$ actually are does not matter if we only want to determine whether $a + b$ is congruent to 0 or not.

**Multiplication**

After understanding how addition and subtraction work in modular arithmetic, we turn our attention to understanding multiplication. In classical arithmetic, if $a = 2$ and $b = 5$, then of course $a \times b = 2 \times 5 = 10$. Does a similar relationship also hold in modular arithmetic? In particular, if we know that $a \equiv 2 \pmod{m}$ and $b \equiv 5 \pmod{m}$, do we know that $a \times b \equiv 2 \times 5 \pmod{m}$?

The following theorem answers this question affirmatively.

**Theorem 16.**

$$\begin{array}{rrcll} \textit{If} & a & \equiv & b \pmod{m} & \textit{and} \\ & c & \equiv & d \pmod{m}, & \textit{then} \\ & a \times c & \equiv & b \times d \pmod{m}. & \end{array}$$

*Proof.* By the definition of congruence we know that $a$ and $b$ differ by a multiple of $m$, as do $c$ and $d$:

$$\begin{aligned} b - a &= jm \\ d - c &= km \end{aligned}$$

for some $j, k \in \mathbb{Z}$. Note that we use distinct multiples $j$ and $k$ for the two equations, since $a$ and $b$ might differ by one multiple of $m$, and $c$ and $d$ might differ by another multiple of $m$.

To prove the desired result, we rearrange the equations:

$$\begin{aligned} b &= jm + a \\ d &= km + c \end{aligned}$$

We multiply both sides by each other to obtain

$$\begin{aligned} bd &= (jm + a)(km + c) \\ &= jkm^2 + jmc + kma + ac \\ &= (jkm + jc + ka)m + ac. \end{aligned}$$

We then subtract $ac$ from both sides to obtain

$$bd - ac = (jkm + jc + ka)m.$$

Since $(jkm + jc + ka)m$ is an integer multiple of $m$, then $ac$ and $bd$ differ by an integer multiple of $m$, and so by definition are congruent mod $m$. □

**Example 1.** If we know that $a \equiv 3 \pmod{7}$ and we know that $b \equiv 4 \pmod{7}$, then we can determine that $ab \equiv 12 \equiv 5 \pmod{7}$. This is true whether $a$ is 10, 703, or 7,000,003 and whether $b$ is 7004 or 10000. In any of these cases, the product $ab$ will be congruent to 5 modulo 7.

**Example 2.** How can we simplify $20 \times 21$ in arithmetic modulo 19? We first note that $20 \equiv 1 \pmod{19}$ and also that $21 \equiv 2 \pmod{19}$. Theorem 16 tells us that we can combine these equations to obtain $20 \times 21 \equiv 1 \times 2 \equiv 2 \pmod{19}$.

**Example 3.** Can we simplify $17^{753}$ in arithmetic modulo 9? We first note that $17 \equiv -1 \pmod{9}$, because 17 and -1 differ by a multiple of 9. Theorem 16 allows us to then combine this congruence relation as many times as we would like. In particular, by combining 753 copies, we obtain $17^{753} \equiv (-1)^{753} \pmod{9}$. Since $(-1)^n = -1$ for any odd integer $n$, we have $17^{753} \equiv -1 \pmod{9}$. Finally, if we would like to have a simple, positive answer, then we can add 9 to obtain a final answer of 8.

Theorems 15 and 16 show us that we can treat all numbers that are congruent modulo $m$ as the same, in addition and in multiplication operations. Division is much more complicated, and will not be discussed.

### Remainders

We take a moment to draw out a connection to division with remainders, an idea we considered briefly in Section 4.1. In particular, back in elementary school we learned about a way of dividing integers by other integers that entirely avoids decimals and fractions. In particular, suppose we divide 7 by 4. In third, fourth, or fifth grade, we learned that we can write this as 1, remainder 3. That is, 4 can 1 time "into" 7, leaving over 3. As we got older, we learned that we could also write the answer as 1.75 or 1¾, but we still occasionally deal with situations in which discussing fractions would be silly. If we have 52 playing cards and 5 players, a dealer could give each player 10 cards and then be left with 2 cards. It makes little sense to say that the dealer should give each player 10.2, or 10 and a fifth, cards.

What is the connection of modular arithmetic to division with remainders? Suppose that we divide some integer $a$ by another integer $m$. Notice that the "remainder" is always congruent to $a$ modulo $m$. For example, suppose we divide 1031 by 19. We obtain 54, remainder 5. This tells us that 5 is congruent to 1031 modulo 19. Likewise, since the remainder of 7381/57 is 28, we know that $28 \equiv 7381 \pmod{57}$.

Why is the remainder after division always congruent to the number we are dividing? One way to think about this is by considering how we can find a remainder without actually doing any division. Suppose we want to know the remainder of 11 after dividing by 3. We can subtract 3 over and over until we obtain a number that is smaller than 3: 11, 8, 5, and eventually 2. Each time we subtract 3, we are realizing that 3 can "go into" 11 one more time; whatever is left at the end is the remainder. At the same time, we got from the original number to the remainder by jumps of 3, so of course the difference between 11 and 2 is divisible by 3, making 11 and 2 congruent. The same idea works for dividing any number $a$ with any other number $m$.

**Standard Representation**

We have by now seen that in arithmetic modulo $m$, there is no difference between writing 1, $1+m$, $1+2m$, and so forth, at least as far as addition, subtraction, and multiplication are concerned. For this reason, writing $4+11 \equiv 15 \pmod{13}$ is "just as correct" as writing $4+11 \equiv 2 \pmod{13}$, and "just as correct" as writing $4+11 \equiv -11 \pmod{13}$. As far as arithmetic modulo 13 is concerned, 2, 15, and -11 are exactly the same number. However, in some applications it is convenient to agree upon a standard way to represent numbers. What is a good way to do this? Which of $\{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}$ should we consider the standard representative?

You have likely encountered a similar problem back in your days learning about trigonometric functions. A teacher may have asked you what is the inverse sine of $-1$, i.e., $\sin^{-1}(-1)$. You may have correctly answered $270°$. Or you may have correctly answered $-90°$. In fact, any number that can be written $270° + n360°$, for any integer $n \in \mathbb{Z}$, would also be equally correct. But if each student wrote a different number on an exam, it could take a long time to determine whether or not every answer is correct. Is $1500°$ a correct solution? Is $1530°$? For this reason, we might specify that we looking for a correct answer between $0°$ and $360°$, or else between $-180°$ and $180°$, since there is exactly one correct answer in each of these ranges.

In the same way, when working in arithmetic modulo 41, the numbers $\{\ldots, -29, 12, 53, 94, 135, \ldots\}$ are all the same, yet we might hope to specify one of them to be the standard representation of them. Indeed, in arithmetic modulo $m$, we refer to the numbers $\{0, 1, 2, \ldots, m-1\}$ as the **standard representations** of the integers. If numbers are always represented in this standard form, determining whether or not two numbers are congruent is as easy as looking at whether the numbers are equal. Notice also that this set of numbers is also the set of possible remainders after dividing a number by $m$.

**Example 1.** Suppose we want to know the remainder of $17 \times 18$ when it is divided by 19. We can do this in two different ways. First, we can multiply the two numbers directly and obtain 306; some calculation will show that 306 is congruent to 2 modulo 19. Alternatively, we know that $17 \equiv -2 \pmod{19}$ and $18 \equiv -1 \pmod{19}$. Multiplying both sides we see that $17 \times 18 \equiv (-2) \times (-1) \equiv 2 \pmod{19}$.

**Example 2.** Suppose we want to determine the standard form of $17^2$ in mod 19 arithmetic. One way in which we can do this is by considering the square of 17, which is 289, divide that by 19 and then take the remainder. However, since we know that $17 \equiv -2 \pmod{19}$, we can multiply this congruence equation by itself to obtain $17^2 \equiv -2^2 \equiv 4 \pmod{19}$. We can easily verify that the remainder of 289, when divided by 17, is indeed 4.

**Example 3.** Suppose we want to determine the standard form of $18^{489391312}$ in mod 19 arithmetic. We should first notice that in mod 19 arithmetic, 18 is congruent to $-1$, and so $18^{489391312} \equiv (-1)^{489391312} \pmod{19}$. It is relatively

easy to see that if $n$ is odd then $(-1)^n = -1$, and if $n$ is even then $(-1)^n = 1$. Since 489391312 is even, $18^{489391312} \equiv 1 \pmod{19}$.

### Dividing by 9

We can use the rules of modular addition and multiplication to prove a theorem you may have once seen. Suppose we have a number, for example 2,383,623, and want to know whether it is divisible by 9. Is there an easy way to figure this out without doing "long division"? You may have learned the following trick: add up the digits of the number (e..g., $2 + 3 + 8 + 3 + 6 + 2 + 3 = 27$). If this sum is divisible by 9, then so is the original number; if the sum is not divisible by 9, then neither is the original number. Is this just a miraculous trick, or is it something that we can prove should work?

The rules of modular addition and multiplication (Theorems 15 and 16 above) can help us prove this beautiful result. Let's begin by proving a simpler result about the remainders we get when we divide powers of 10 by 9. In particular, the remainder is always 1.

**Lemma 17.** *For any natural number $n$, we have $10^n \equiv 1 \pmod{9}$.*

*Proof.* Recall that if we have two congruences: $a \equiv b$ and $c \equiv d \pmod{m}$, then we can combine them to form a new congruence relation: $ac \equiv bd \pmod{m}$. Since $10 \equiv 1 \pmod{9}$, then we can combine the equation with itself to obtain $100 = 10 \times 10 \equiv 1 \times 1 \equiv 1 \pmod{9}$. We can indeed combine this equation with itself as many times as we want (e.g., $n$ times), and therefore have $10^n \equiv 1^n \equiv 1 \pmod{9}$ for any natural number $n$. □

Next, let's consider what happens when we divide numbers such as 300, 5000, and 2,000,000 by 9. What are the remainders? Theorem 16 can help us see that the remainders are 3, 5, and 2 in these examples. To see why this is so, notice that each of these numbers can be written as the product of an integer and a power of 10: $300 = 3 \cdot 10^2$, $5000 = 5 \cdot 10^3$, and $2{,}000{,}000 = 2 \cdot 10^6$. This leads us to the following theorem.

**Lemma 18.** *For any natural numbers $c$ and $n$, we have $c \cdot 10^n \equiv c \pmod{9}$.*

*Proof.* Recall that if we have two congruences: $a \equiv b$ and $c \equiv d \pmod{m}$, then we can combine them to form a new congruence relation: $ac \equiv bd \pmod{m}$. Since $c \equiv c$ and $10^n \equiv 1 \pmod{9}$ for any $n$, then we can combine the equations to obtain $c \cdot 10^n \equiv c \cdot 1 \equiv c \pmod{9}$. □

This now leads us to our central theorem:

**Theorem 19.** *A number is divisible by 9 if and only if the sum of its digits (written in base 10) is divisible by 9.*

*Proof.* In base 10, every number can be written as a sum of ones, tens, hundreds, thousands, and so forth. For example, $5776 = 5000+700+70+6$. More generally, we can write this as $n = c_0 + c_1 10^1 + c_2 10^2 + c_3 10^3 + \ldots$, where the $c_i$ variables

are the numbers of ones, tens, hundreds, thousands, and so forth. According to Lemma 18, for each of the $c_i$ we have $c_i \cdot 10^n \equiv c_i \pmod 9$. Using Theorem 15, we can combine the congruence relations

$$\begin{aligned} c_0 &\equiv c_0 \pmod 9, \\ c_1 &\equiv c_1 10^1 \pmod 9, \\ c_2 &\equiv c_2 10^2 \pmod 9, \\ c_3 &\equiv c_2 10^3 \pmod 9, \\ &\dots \\ c_n &\equiv c_2 10^n \pmod 9, \end{aligned}$$

to give us

$$c_0 + c_1 10^1 + c_2 10^2 + \dots c_n 10^n \equiv c_0 + c_1 + c_2 + \dots c_n \pmod 9 \tag{69}$$

In other words, a number $n$ is congruent to the sum of its digits in mod 9. If a number is divisible by 9, i.e., $n \equiv 0 \pmod 9$, then so is the sum of its digits. $\square$