

Note 7: Modular Arithmetic

CS 70, Summer 2024

1 Number Theory

1.1 Division

Before we begin our exploration of modular arithmetic, we recap some previous results in number theory and develop some new ones.

We begin with the following definition.

Definition 1. For two integers $a, b \in \mathbb{Z}$, we say that a divides b if there exists some integer $k \in \mathbb{Z}$ such that

$$b = ak.$$

We write this as “ $a \mid b$.”

This is a quite reasonable definition of one number dividing another—if a divides b , then we can write b as the product of a and some integer.

Example 1. Determine which of the following are true.

- (a) $1 \mid 4$.
- (b) $3 \mid 4$.
- (c) $2 \mid 0$.
- (d) $0 \mid 2$.
- (e) $0 \mid 0$.

Let’s work through each of the parts.

- (a) We can see that it is indeed true that $1 \mid 4$ since $4 = 1 \cdot 4$. In fact, for any $a \in \mathbb{Z}$, we have that $1 \mid a$.
- (b) We do not have $3 \mid 4$. We can’t write $4 = 3k$ for $k \in \mathbb{Z}$. In particular the integer multiples of 3 are $\{3k : k \in \mathbb{Z}\} = \{\dots, -3, 0, 3, 6, 9, \dots\}$. This doesn’t include 4.
- (c) $2 \mid 0$ is true since we can write $0 = 2 \cdot 0$. We can extend this to say that $a \mid 0$ for any $a \in \mathbb{Z}$.
- (d) $0 \nmid 2$. Note that $0 \cdot k = 0$ for any $k \in \mathbb{Z}$, so we cannot have that $2 = 0 \cdot k$. So for any nonzero integer $a \in \mathbb{Z} \setminus \{0\}$, we have that $0 \nmid a$.
- (e) This last one is true, since $0 = 0 \cdot k$ for any $k \in \mathbb{Z}$. So $0 \mid 0$.

Now that we have a better idea of what it means for two numbers to divide one another, let’s prove a small but useful lemma about divisibility.

Lemma 1. Suppose that for integers $a, b, d \in \mathbb{Z}$, we have that $d \mid a$ and $d \mid b$. Then for any integers $x, y \in \mathbb{Z}$, we have that $d \mid (ax + by)$.

That is, if d divides both a and b , then d divides any sum of integer multiples of a and b .

Proof. Directly. Suppose that $d \mid a$ and $d \mid b$. We must show that $d \mid (ax + by)$, i.e., find some integer ℓ such that $ax + by = d\ell$.

By definition, there exist integers $k, j \in \mathbb{Z}$ such that $a = dk$ and $b = dj$. Then

$$ax + by = dkx + d jy = d(kx + jy),$$

where $\ell = kx + jy \in \mathbb{Z}$ since it is created by multiplying and adding integers. So we have that $ax + by = d\ell$ for some $\ell \in \mathbb{Z}$. By the definition of divisibility, we have that $d \mid (ax + by)$.

1.2 Greatest Common Divisors

This brings us to the idea of a **greatest common divisor**.

Definition 2. For any two integers $a, b \in \mathbb{Z}$, we say that the *greatest common divisor* of a and b is the greatest $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$. We write $d = \gcd(a, b) = \gcd(b, a)$. We define as convention that $\gcd(0, 0) = 0$.

More formally, we say that $d = \gcd(a, b)$ if the following are true.

- (1) d is a *common divisor* of a and b : $d \mid a$ and $d \mid b$.
- (2) For any other common divisor c of a and b , we have that $c \leq d$.

This definition is quite reasonable. It's exactly what we'd expect of something that we call the "greatest common divisor." Let's look at some examples.

Example 2. Find $\gcd(4, 18)$.

To find $\gcd(4, 18)$, we'll check all possible divisors of 4 and 18 to see each is a common divisor. Then we'll simply take the largest one. The possible divisors are 0, 1, 2, 3, and 4; we don't need to consider any integers past 4 since a divisor is necessarily less than the dividend. We get the following.

$0 \nmid 4$	$0 \nmid 18$
$1 \mid 4$	$1 \mid 18$
$2 \mid 4$	$2 \mid 18$
$3 \nmid 4$	$3 \nmid 18$
$4 \mid 4$	$4 \nmid 18$.

The common divisors of 4 and 18 are 1 and 2. Thus the greatest common divisor is 2. That is, $\gcd(4, 18) = 2$.

Example 3. Show that for any natural number $n \in \mathbb{N}$, $\gcd(n, 0) = n$.

Note that the greatest any divisor of n can be is n itself. So if we are able to show that n is a common divisor of both n and 0 we are done.

We can confirm that $n \mid n$ since $n = n \cdot 1$ and $n \mid 0$ since $0 = n \cdot 0$. Therefore $\gcd(n, 0) = n$. This fact will act as a "base case" for all of our gcd algorithms.

Finding the greatest common divisor was rather annoying. To find $\gcd(4, 18)$, we had to check whether every natural number divided both 4 and 18. We'll try to develop some number theory that allows us to quickly compute gcds.

Let's try and prove the following fact about the greatest common divisor of two integers.

Lemma 2. For any integers $a, b \in \mathbb{Z}$, we have that $\gcd(a, b) = \gcd(a - b, b)$.

Proof. We will show that a and b have the same common divisors as $a - b$ and b . Therefore they must also have the same greatest common divisor.

Suppose that $d \mid a$ and $d \mid b$. We then already have that $d \mid b$, so it remains to show that $d \mid (a - b)$. By **Lemma 1**, we have that $d \mid (a(1) + b(-1))$. In other words, $d \mid (a - b)$.

Now suppose that $d \mid b$ and $d \mid (b - a)$. We then already have that $d \mid b$, so it remains to show that $d \mid a$. Again by **Lemma 1**, we have that $d \mid ((b - a)(-1) + b(1))$. In other words, $d \mid a$.

This is very useful, since it allows us to simplify gcd problems into ones that are easier to work with.

Example 4. Use **Lemma 2** to find $\gcd(24, 18)$ and $\gcd(3, 13)$.

By the lemma and the fact that $\gcd(a, b) = \gcd(b, a)$ we have that

$$\begin{aligned}\gcd(24, 18) &= \gcd(24 - 18, 18) = \gcd(6, 18) \\ &= \gcd(6, 18 - 6) = \gcd(6, 12) \\ &= \gcd(6, 12 - 6) = \gcd(6, 6) \\ &= \gcd(6 - 6, 6) = \gcd(0, 6) \\ &= 6.\end{aligned}$$

The same algorithm yields

$$\begin{aligned}\gcd(3, 13) &= \gcd(3, 13 - 3) = \gcd(3, 10) \\ &= \gcd(3, 10 - 3) = \gcd(3, 7) \\ &= \gcd(3, 7 - 3) = \gcd(3, 4) \\ &= \gcd(3, 4 - 3) = \gcd(3, 1) \\ &= \gcd(3 - 1, 1) = \gcd(2, 1) \\ &= \gcd(2 - 1, 1) = \gcd(1, 1) \\ &= \gcd(1 - 1, 1) = \gcd(0, 1) \\ &= 1.\end{aligned}$$

That's much faster than finding all the common divisors and taking the largest. However, it feels like there's still some area for tightening up this algorithm—what if instead of removing just copy of a in each of step, we removed as many as possible? That would allow us to shortcut from $\gcd(18, 6)$ to $\gcd(0, 6)$ by removing all three 6s in one step. Similarly, if we had instead removed all four 3s in one go, we could have gone straight from $\gcd(3, 13)$ to $\gcd(3, 1)$. And then we could have gone straight to $\gcd(0, 1)$ by removing as many 1s as possible.

In all of these “shortcuts,” by removing as many copies of a as we can from b , we're left the remainder of b when dividing by a . Towards this end, we prove the following theorem, known as the **division algorithm**.

Theorem 1. Division algorithm. For any integer $a \in \mathbb{Z}$ and divisor $d \in \mathbb{Z}^+$, there are unique integers $q, r \in \mathbb{Z}$ such that $0 \leq r < d$ and

$$a = qd + r.$$

We call r the *remainder* of a when dividing by d , and write $r = a \bmod d$.

This is a somewhat complicated way of saying that a can be written as some integer multiple of d with a remainder of $r < d$.

Proof. We first show that such q and r exist. Intuitively, we can get the remainder of a when dividing by d by repeatedly subtracting off d and stopping right before we hit the negative numbers. That way

we've removed as many ds from a as we can, and whatever is left is the remainder. So let's define the following set:

$$S = \{a - dk : k \in \mathbb{Z} \wedge a - dk \geq 0\}.$$

That is, S consists of the nonnegative differences you get by repeatedly subtracting d off from a .

We claim that $S \neq \emptyset$. We can consider two cases: either $a \geq 0$ or $a < 0$.

- (1) $a \geq 0$. Then we can pick $k = 0$ to get $a = a - d \cdot 0 \geq 0$. So $a \in S$.
- (2) $a < 0$. Then we can pick $k = a$ to get $a - da = a(1 - d)$. Then $a < 0$ by assumption and $1 - d \leq 0$ since d is a positive integer. So $a - da = a(1 - d) \geq 0$. Therefore $a - da \in S$.

In either case, there's at least one element in S . So S is a non-empty subset of the natural numbers. By the well-ordering principle, let $r \in S$ be the smallest element of S . This r is precisely the remainder we're looking for.

Since $r \in S$, we have that $r \geq 0$ and that $r = a - dq$ for some $q \in \mathbb{Z}$. We claim that $r < d$. Suppose for contradiction that $r \geq d$. Then $r - d \geq 0$ and

$$r - d = a - dq - d = a - d(q + 1).$$

So $r - d \in S$. But then, since $d > 0$, $r - d < r$. This is a contradiction, since r was supposed to be the smallest element of S . Our assumption that $r \geq d$ must be incorrect. So we have that $r < d$, as desired.

So $r = a - dq$, with $0 \leq r < d$. Some rearranging gets us $a = dq + r$, so we have shown that such q and r exist.

To show that these q and r are unique, consider two pairs q_1, r_1 and q_2, r_2 such that $a = dq_1 + r_1$ and $a = dq_2 + r_2$. We will show that we must have that $r_1 = r_2$ and $q_1 = q_2$.

Suppose without loss of generality that $r_2 \geq r_1$. Then $r_2 - r_1 = d(q_1 - q_2) \geq 0$. So $r_2 - r_1$ is some multiple of d ; that is, $r_2 - r_1 = d\ell$ for some $\ell \in \mathbb{Z}$. Note that $\ell \geq 0$ since $r_2 - r_1 \geq 0$ and $d > 0$.

But since $r_2, r_1 < d$, it must be that $r_2 - r_1 < d$. So we cannot have $\ell \geq 1$, since that would make $r_2 - r_1 \geq d$. So it must be that $\ell = 0$ and therefore $r_2 - r_1 = d \cdot 0 = 0$. So $r_2 = r_1$.

Then

$$q_1 = \frac{a - r_1}{d} = \frac{a - r_2}{d} = q_2.$$

So we have shown that any division of a by d yields identical qs and rs ; therefore q and r are unique.

We can use the division algorithm in combination with the following fact to derive a new algorithm for computing the gcd.

Lemma 3. For any integers $a, b \in \mathbb{Z}$, we have that $\gcd(a, b) = \gcd(b, a \bmod b)$. That is, writing $a = bq + r$ by the division algorithm, we have that $\gcd(a, b) = \gcd(b, r)$.

Proof. Left as an exercise.

Let's see this in action.

Example 5. Use **Lemma 3** to find $\gcd(29, 17)$.

To find this gcd, we'll repeatedly apply the division algorithm. We'll highlight the arguments to the gcd algorithm in bold and leave the q coefficients from the division algorithm unbolded.

$$\begin{aligned}
\gcd(29, 17) &= \gcd(17, 12) & 29 &= 1 \times 17 + 12 \\
&= \gcd(12, 5) & 17 &= 1 \times 12 + 5 \\
&= \gcd(5, 2) & 12 &= 2 \times 5 + 2 \\
&= \gcd(2, 1) & 5 &= 2 \times 2 + 1 \\
&= \gcd(1, 0) & 2 &= 2 \times 1 + 0 \\
&= 1.
\end{aligned}$$

This method for finding the gcd is known as the **Euclidean algorithm**. Let's try to write it down formally.

Algorithm 1. *Euclidean algorithm.* For any two natural numbers $a, b \in \mathbb{N}$, suppose without loss of generality that $a \geq b$. Then the following algorithm computes $\gcd(a, b)$.

```

gcd(a, b):
  if b = 0 then
    return a
  else
    return gcd(b, a mod b)

```

Note that this algorithm is recursive. Recursive algorithms lend themselves quite well to analysis by induction. Let's prove that our algorithm actually works.

Theorem 2. The Euclidean algorithm, **Algorithm 1**, works.

Proof. By strong induction on $b \geq 0$, the smaller of the two inputs. We prove that $\gcd(a, b) = \gcd(a, b)$ for all $a \geq b$.

Base case. $b = 0$. When $\gcd(a, 0)$ runs, the first if-statement means that the algorithm will output a . Therefore $\gcd(a, 0) = a = \gcd(a, 0)$.

Induction case.

Induction hypothesis. Suppose that for some $b \in \mathbb{N}$, the claim holds for all natural numbers up to b . That is, for all $k \leq b$, the $\gcd(a, k) = \gcd(a, k)$ for any $a \geq k$.

Induction step. Now we must show that the \gcd algorithm correctly compute $\gcd(a, b + 1)$ for any $a \geq b + 1$.

Let $a \geq b + 1$ and consider $\gcd(a, b + 1)$. The algorithm returns $\gcd(b + 1, a \bmod (b + 1))$, where $a \bmod (b + 1) \leq b$ by the division algorithm (**Theorem 1**). Therefore we can apply the induction hypothesis.

$$\begin{aligned}
\gcd(a, b + 1) &= \gcd(b + 1, a \bmod (b + 1)) && \text{by \textbf{Algorithm 1}} \\
&= \gcd(b + 1, a \bmod (b + 1)) && \text{by the induction hypothesis} \\
&= \gcd(a, b + 1). && \text{by \textbf{Lemma 3}}
\end{aligned}$$

So the algorithm returns $\gcd(a, b + 1)$, as desired.

1.3 Diophantine Equations

We wrap up our exploration of number theory by examining *linear Diophantine equations*. These are equations of the form

$$ax + by = c,$$

where $a, b, c \in \mathbb{Z}$ are known integers and $x, y \in \mathbb{Z}$ are unknown integers for which we are trying to solve. Do such equations always have solutions? If a solution exists, is it unique? Let's consider some examples.

Example 6. Show that $1 = 4x + 2y$ has no integer solutions $x, y \in \mathbb{Z}$.

Let's suppose for contradiction that there is an integer solution $x, y \in \mathbb{Z}$. Then we have that

$$1 = 4x + 2y = 2(2x + y) \iff 2x + y = \frac{1}{2}.$$

But $2x + y$ is an integer since x and y are integers. This is a contradiction, so there must not be a solution.

Example 7. Show that $2 = 4x + 2y$ has infinitely many integer solutions $x, y \in \mathbb{Z}$.

We have that

$$2 = 4x + 2y = 2(2x + y) \iff 1 = 2x + y$$

By trial and error, $x = 1$ and $y = -1$ is a solution. So is $x = 2, y = -3$. In fact, for any $x \in \mathbb{Z}$, we can pick $y = 1 - 2x$. So any $k \in \mathbb{Z}$, the pair $x = k, y = 1 - 2k$ is a solution to the equation. Therefore there are infinitely many solutions.

The following famous lemma will help us to characterize when solutions exist.

Lemma 4. *Bezout's identity.* For any integers $a, b \in \mathbb{Z}$, there exist integers $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

That is, we can always write the greatest common divisor of a and b as the sum of two integer multiples of a and b .

Proof. Left as an exercise.

We'll use Bezout's identity to prove when linear Diophantine equations have solutions.

Theorem 3. *Linear Diophantine equations.* For $a, b, c \in \mathbb{Z}$, let $d = \gcd(a, b)$. Then $ax + by = c$ has integer solutions $x, y \in \mathbb{Z}$ if and only if $d \mid c$.

Proof. (\implies) For the forwards direction, suppose that $ax + by = c$ has integer solutions $x, y \in \mathbb{Z}$. By **Lemma 1**, since $d \mid a$ and $d \mid b$, we have that $d \mid (ax + by)$. So $d \mid c$.

(\impliedby) Now for the backwards direction, suppose that $d \mid c$. Then $c = dk$ for some $k \in \mathbb{Z}$. Moreover, by Bezout's identity, we have that there exist $u, v \in \mathbb{Z}$ such that

$$au + bv = d.$$

Scale the equation by k to get that

$$a(ku) + b(kv) = dk = c.$$

So $ku, kv \in \mathbb{Z}$ are integer solutions to $ax + by = c$.

Theorem 3 shows that solutions only exist when $\gcd(a, b) \mid c$.

Concep Check 1. Confirm that **Theorem 3** implies that **Example 6** has no solutions and that **Example 7** has solutions.

So how can we find these integers x and y ? The proof of **Theorem 3** is not very constructive. We can do it by working backwards through our output from the Euclidean algorithm.

Example 8. Use the calculation from **Example 5** to find x and y such that $29x + 17y = 1$.

Note that in **Example 5**, we wrote each remainder in terms of the previous and next remainders, e.g. $17 = 1 \times 12 + 5$, where here **12** is the remainder from the previous step and **5** is the new remainder. We'll flip each of the equations and successively apply the previous equations to eventually get our last remainder of $1 = \gcd(29, 17)$ in terms of **29** and **17**.

Let's start by flipping the equations. The last equation is grayed out since we won't be using it.

$$\begin{array}{ll}
 \gcd(29, 17) = \gcd(17, 12) & \mathbf{12} = 29 - 1 \times 17 \quad (1) \\
 = \gcd(12, 5) & \mathbf{5} = 17 - 1 \times 12 \quad (2) \\
 = \gcd(5, 2) & \mathbf{2} = 12 - 2 \times 5 \quad (3) \\
 = \gcd(2, 1) & \mathbf{1} = 5 - 2 \times 2 \quad (4) \\
 = \gcd(1, 0) & \mathbf{0} = 2 - 2 \times 1 \\
 = 1. &
 \end{array}$$

Equation (4) tells us that $1 = 5 - 2 \times 2$. But using equation (3), we can express **2** in terms of **5** and **12**; and then using equation (2), we can write **5** in terms of **12** and **17**. Finally, using equation (1), we can write **12** in terms of **17** and **29**. Once we've reached this point, everything in terms of **17** and **29**, and we'll have a solution to our question.

Let's see it in action.

$$\begin{array}{ll}
 \mathbf{1} = 5 - 2 \times 2 & \text{by (4)} \\
 = 5 - 2 \times (12 - 2 \times 5) & \text{by (3)} \\
 = 5 \times 5 - 2 \times 12 & \\
 = 5 \times (17 - 1 \times 12) - 2 \times 12 & \text{by (2)} \\
 = 5 \times 17 - 7 \times 12 & \\
 = 5 \times 17 - 7 \times (29 - 1 \times 17) & \text{by (1)} \\
 = 12 \times 17 - 7 \times 29. &
 \end{array}$$

This process of working backwards through the equations from the Euclidean algorithm is known as the **extended Euclidean algorithm**.

So we have that $x = 12$ and $y = -7$ are integer solutions to the Diophantine equation $17x + 29y = 1$.

We will not prove it here, but it is a true fact that whenever a linear Diophantine equation has one solution, it has infinitely many.

Concept Check 2. Confirm that for any $k \in \mathbb{Z}$, $x = 12 + 29k$ and $y = -7 - 17k$ are integer solutions to $17x + 29y = 1$.

Concept Check 3. Suppose that $x, y \in \mathbb{Z}$ are integer solutions to the Diophantine equation $ax + by = c$. Use x and y to construct infinitely many more integer solutions.

2 Modular Arithmetic

In many settings, arithmetic is done over a fixed, finite range of numbers. Such settings are especially common in the computer sciences, since computers cannot do exact arithmetic over the real numbers—they

don't have infinite precision. **Modular arithmetic** is a system of arithmetic which limits the available numbers to a discrete range and wraps around when any operations try to leave that range. For example, you may have seen on a computer an integer overflow error, wherein a large positive integer result is instead computed to be a very large negative integer. That kind of wrap around is precisely what modular arithmetic is all about—it's how computers do math.

The cyclical way in which humans measure time lends itself quite nicely to modular arithmetic—the hours of the day have a cycle of 24 hours; the days of the week have a cycle of 7 days; the weeks of the year have a cycle of 52 weeks, and so on. When calculating times with respect to these cycles, we automatically use modular arithmetic.

For example, if it's the second day of the week today (Monday), then in 13 days, it'll be the first day of the week (Sunday). We can think of that as $2 + 13 = 15 = 2(7) + 1$. That remainder of 1 is what tells us it'll be Sunday. In fact, if we're especially savvy, we might just work with remainders: 13 has a remainder of 6, so we can say that it'll be $2 + 6 = 8 = 1(7) + 1$. If we're even more savvy, we might say that 13 is one fewer than a multiple of 7, so $2 + (-1) = 1$.

Example 9. Let's work in military time. Suppose it is currently the 10:00. What time will it be in 14 hours? In 25 hours? In 82 hours?

Since we're working with time, we're working with just the numbers 0 through 23. So we need to think about each number's remainder when divided by 24.

For 14 hours, that's $10 + 14 = 24 = 1(24)$. So it'll be 0:00.

For 25 hours, that's $10 + 25 = 35 = 1(24) + 11$. So it'll be 11:00. We could also first reduce 25 to its remainder when divided by 24, which is 1, and then do the arithmetic: $10 + 1 = 11$.

The remainder of 82 when divided by 24 is 10. So that's $10 + 10 = 20$, or 20:00.

We call the positive integer with respect to which we take our remainder the **modulus**. For military time, we're doing arithmetic with respect to a modulus of 24. As we saw in the division algorithm, we will define $x \bmod m$, said " x modulo m ," to be the remainder when the integer x is divided by the modulus m .

2.1 Modular Equivalences

We saw earlier that 82 was "like" 10 when working with a modulus of 24, since they have the same remainder when divided by 24. Since we don't want to write $82 = 10$, since that looks like nonsense, we'll instead define a new notion of equality which only cares about the remainders with respect to a modulus.

Definition 3. For any integers $a, b \in \mathbb{Z}$ and any modulus $m \in \mathbb{Z}^+$, we say that a is *congruent to b modulo m* if $m \mid (a - b)$. We write this as

$$a \equiv b \pmod{m}$$

That is, we would say that 82 is congruent to 10 modulo 24, and we would write $82 \equiv 10 \pmod{24}$. However, this definition doesn't seem to be saying the same thing as what we were—that 82 and 10 have the same remainder when divided by 24.

In fact, these two notions are equivalent—but it's often easier to work with this definition. Let's prove that these two ideas of equality with respect to a modulus are actually the same.

Theorem 4. For any integers $a, b \in \mathbb{Z}$ and any modulus $m \in \mathbb{Z}^+$, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

That is, a is congruent to b modulo m if and only if a and b have the same remainder when divided by m .

Proof. By the division algorithm, let

$$\begin{aligned} a &= qm + r \\ b &= sm + t \end{aligned}$$

for integers $q, s \in \mathbb{Z}$ and remainders $r, t \in \{0, \dots, m-1\}$.

(\Leftarrow) Suppose that $r = a \bmod m = b \bmod m = t$. Then

$$a - b = qm + r - (sm + t) = m(q - s) + (r - t) = m(q - s).$$

By definition, $m \mid (a - b)$, so $a \equiv b \pmod{m}$.

(\Rightarrow) Suppose that $a \equiv b \pmod{m}$, that is, that $m \mid (a - b)$. Therefore $m \mid (m(q - s) + (r - t))$, so there is some integer $k \in \mathbb{Z}$ such that

$$m(q - s) + (r - t) = mk.$$

Then

$$r - t = m(k - q + s),$$

so there is an integer $\ell = m(k - q + s) \in \mathbb{Z}$ such that $r - t = m\ell$. However, since $0 \leq r, t < m$, we have that $-m < r - t < m$. We cannot have $\ell \leq -1$, since that would mean $r - t \leq -m$; nor can we have $\ell \geq 1$, since that would mean $r - t \geq m$. So it must be that $\ell = 0$. Therefore $r - t = m \cdot 0 = 0$, so $r = t$. That is, $a \bmod m = b \bmod m$, as desired.

We get a quite useful corollary out of this theorem.

Corollary 1. For any integers $a, b \in \mathbb{Z}$ and any modulus $m \in \mathbb{Z}^+$, $a \equiv b \pmod{m}$ if and only if there exists some integer $k \in \mathbb{Z}$ such that $a = km + b$.

That is, two numbers are equivalent with respect to a modulus if they differ by some multiple of that modulus.

Proof. (\Rightarrow) Let $a = jm + r$ for some $j \in \mathbb{Z}$ and $r \in \{0, \dots, m-1\}$ by the division algorithm. Since $a \equiv b \pmod{m}$, by **Theorem 4**, we must have that $b = \ell m + r$ for some $\ell \in \mathbb{Z}$. Then $r = b - \ell m$, so we can write

$$a = jm + r = jm + (b - \ell m) = (j - \ell)m + b.$$

So we have an integer $k = j - \ell \in \mathbb{Z}$ such that $a = km + b$, as desired.

(\Leftarrow) Suppose that $a = km + b$. Then $b - a = km$, so $m \mid (b - a)$. Therefore $a \equiv b \pmod{m}$.

A note on notation. As we have seen, the notation $r = a \bmod m$ refers to the remainder of a when divided by m . This differs from $b \equiv a \pmod{m}$, which says that b and a are equivalent modulo m . The distinction is that $a \bmod m$ refers to the smallest nonnegative integer which is equivalent to a modulo m . We will always have that $a \bmod m \in \{0, \dots, m-1\}$. For example, a statement like $5 = 7 \bmod 2$ is false, but a statement like $5 \equiv 7 \pmod{2}$ is true.

2.2 Modular Addition and Subtraction

Addition with respect to a modulus works just the way we've been doing it so far. But now that we have a well-defined notion of equality with respect to a modulus, let's prove that we can do what we've been doing.

Theorem 5. *Modular addition.* For any integers $a, b, c, d \in \mathbb{Z}$ and any modulus $m \in \mathbb{Z}^+$, suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $a + c \equiv b + d \pmod{m}$.

Proof. By **Corollary 1**, we have that there are integers $j, k \in \mathbb{Z}$ such that $a = km + b$ and $c = jm + d$. Then

$$(a + c) = km + b + jm + d = (k + j)m + (b + d).$$

That is, $a + c$ is $b + d$ more than some multiple of m . Again by **Corollary 1**, this means that $a + c \equiv b + d \pmod{m}$.

Let's do some examples.

Example 10. Evaluate each of the following expressions.

- (a) $(43 + 65) \pmod{6}$.
- (b) $(84 + 204 + 193 + 14323) \pmod{2}$.
- (c) $(44 + 123 + 104) \pmod{10}$.

Note that we're being asked to find the remainders. For each modulus m , our answer needs to be in the range $\{0, \dots, m - 1\}$.

- (a) Note that $43 = 6(7) + 1$, so $43 \equiv 1 \pmod{6}$. Similarly, $65 = 6(10) + 5$, so $65 \equiv 5 \pmod{6}$. Then by **Theorem 5**, $43 + 65 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{6}$. Our final answer is 0.
- (b) When working with a modulus of 2, any even number is 0 and any odd number is 1. So $84 + 204 + 193 + 14323 \equiv 0 + 0 + 1 + 1 \equiv 2 \equiv 0 \pmod{2}$. Our final answer is 0.
- (c) When working with a modulus of 10, the remainder is just the ones digit. So $44 + 123 + 104 \equiv 4 + 3 + 4 \equiv 11 \equiv 1 \pmod{10}$. Our final answer is 1.

What about subtraction with respect to a modulus? For example, what would $(3 - 6) \pmod{4}$ be? The intuition is that it should wrap around the other way: -3 is just $4 - 3 = 1$. This is exactly the right idea.

Corollary 2. *Modular subtraction.* For any integer $a \in \mathbb{Z}$ and modulus $m \in \mathbb{Z}^+$, $-a \equiv m - a \pmod{m}$.

Proof. $m - a - (-a) = m = m \cdot 1$. So $m \mid (m - a - (-a))$; therefore $-a \equiv m - a \pmod{m}$.

This calls for a few more examples.

Example 11. Evaluate each of the following expressions.

- (a) $-4 \pmod{9}$.
- (b) $(43 - 65) \pmod{6}$.
- (c) $(123 - 423 + 14) \pmod{10}$.

We apply **Corollary 2**.

- (a) $-4 \equiv 9 - 4 \equiv 5 \pmod{9}$. The answer is 5.
- (b) From **Example 10**, $43 \equiv 1$ and $65 \equiv 5$. Then $-65 \equiv 6 - 5 \equiv 1$, so $43 - 65 \equiv 1 + 1 \equiv 2 \pmod{6}$. The answer is 2.

- (c) $123 \equiv 3 \pmod{10}$, $423 \equiv 3 \pmod{10}$, and $14 \equiv 4 \pmod{10}$. Therefore $123 - 423 + 14 \equiv 3 - 3 + 4 \equiv 4 \pmod{10}$. The answer is 4. Note that since $123 - 423 + 14$ is negative, this is *not* the ones digit of the result. Rather, the ones digit is $10 - 4 = 6$.

2.3 Modular Multiplication

Multiplication with respect to a modulus works just the way you'd expect. Let's prove it.

Theorem 6. *Modular multiplication.* For any integers $a, b, c, d \in \mathbb{Z}$ and any modulus $m \in \mathbb{Z}^+$, suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $ac \equiv bd \pmod{m}$.

Proof. By **Corollary 1**, we have that there are integers $j, k \in \mathbb{Z}$ such that $a = km + b$ and $c = jm + d$. Then

$$\begin{aligned} ac &= (km + b)(jm + d) \\ &= kjm^2 + kmd + jmb + bd \\ &= (kjm + kd + jb)m + bd. \end{aligned}$$

So ac is bd more than some multiple of m . By **Corollary 1**, this means that $ac \equiv bd \pmod{m}$.

The other typical properties of arithmetic with numbers (association, commutation, distribution) all hold as well—we won't prove that.

Let's practice this with some examples.

Example 12. Evaluate each of the following expressions.

- (a) $(65 \cdot 43) \pmod{6}$.
- (b) $(103 \cdot 2034 \cdot 493) \pmod{10}$.
- (c) $(34 \cdot (24 - 32)) \pmod{3}$.

- (a) As we have seen in **Example 11**, $65 \equiv -1 \pmod{6}$ and $43 \equiv 1 \pmod{6}$. So $65(43) \equiv (-1)(1) \equiv -1 \equiv 5 \pmod{6}$. The answer is 5.

- (b) $103 \equiv 3 \pmod{10}$, $2034 \equiv 4 \pmod{10}$, and $493 \equiv 3 \pmod{10}$. Therefore

$$103 \cdot 2034 \cdot 493 \equiv 3 \cdot 4 \cdot 3 \equiv 12 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \pmod{10}.$$

The answer is 6.

- (c) $34 \equiv 1 \pmod{3}$, $24 \equiv 0 \pmod{3}$, and $32 \equiv -1 \pmod{3}$. So

$$(34 \cdot (24 - 32)) \equiv 1 \cdot (0 - (-1)) \equiv 1 \pmod{3}.$$

The answer is 1.

Let's use these properties to prove some number-theoretic results.

Example 13. Prove that for any $n \in \mathbb{Z}$, we have that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

To prove the statement, we will consider the four possible remainders when dividing n by 4.

- (1) $n \equiv 0 \pmod{4}$. Then $n^2 \equiv 0^2 \equiv 0 \pmod{4}$.
- (2) $n \equiv 1 \pmod{4}$. Then $n^2 \equiv 1^2 \equiv 1 \pmod{4}$.

(3) $n \equiv 2 \pmod{4}$. Then $n^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod{4}$.

(4) $n \equiv 3 \pmod{4}$. Then $n^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod{4}$.

In each case, we got that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$, as desired.

Example 14. Suppose $m = 4k + 3$ for some $k \in \mathbb{Z}$. Then m cannot be written as the sum of the squares of two integers.

We'll use contradiction, since assuming that m is the sum of two squares gives us something to work with. Suppose that for integers $a, b \in \mathbb{Z}$, that $m = a^2 + b^2$. Using **Example 13**, we split into cases based on the parity of a^2 and b^2 modulo 4.

(1) $a^2 \equiv b^2 \equiv 0 \pmod{4}$. Then $m \equiv 0 + 0 \equiv 0 \pmod{4}$.

(2) $a^2 \equiv 0 \pmod{4}, b^2 \equiv 1 \pmod{4}$. Then $m \equiv 0 + 1 \equiv 1 \pmod{4}$.

(3) $a^2 \equiv 1 \pmod{4}, b^2 \equiv 0 \pmod{4}$. Then $m \equiv 1 + 0 \equiv 1 \pmod{4}$.

(4) $a^2 \equiv b^2 \equiv 1 \pmod{4}$. Then $m \equiv 1 + 1 \equiv 2 \pmod{4}$.

Base on our cases, either $m \equiv 0 \pmod{4}$, $m \equiv 1 \pmod{4}$, or $m \equiv 2 \pmod{4}$. However, since $m = 4k + 3$, $m \equiv 4k + 3 \equiv 3 \pmod{4}$. This is a contradiction, so it must not be possible to write $m = a^2 + b^2$ as we had assumed.

2.4 Modular Division

Understanding division with respect to a modulus requires some more thought. Typically, when we divide two integers, we usually get a non-integer ratio like $3/2$. What would dividing numbers look like over something like $\{0, \dots, m-1\}$?

We'll do something similar to what we did with modular addition and modular subtraction. That is, we just defined modular subtraction by a as adding $m - a$. We'll try and do something similar here: we'll define modular division by a as multiplying by some other number, which we call the **multiplicative inverse** of a modulo m .

What should this number be? Over something like the real numbers, we know that dividing by a is the same thing as multiplying by $1/a$. Note that $a \cdot 1/a = 1$. This is precisely how we'll define modular division.

Definition 4. *Modular inverses.* For any integer $a \in \mathbb{Z}$ and modulus $m \in \mathbb{Z}^+$, if there exists an $x \in \mathbb{Z}$ such that

$$ax \equiv 1 \pmod{m},$$

we say that x is an *inverse of a modulo m* . We write $x \equiv a^{-1} \pmod{m}$.

We use $a^{-1} \pmod{m}$ to refer to smallest nonnegative inverse of a modulo m .

Why is this a natural way to define the multiplicative inverse of a modulo m ? Let's imagine we were trying to solve the equation $2x \equiv 3 \pmod{5}$. Our inclination is to divide both sides by 2; while we can't do that, we can multiply both sides by $2^{-1} \pmod{5}$:

$$2^{-1} \cdot 2x \equiv 2^{-1} \cdot 3 \pmod{5}.$$

Then, by **Definition 4**, $2^{-1} \cdot 2 \equiv 1 \pmod{5}$, so

$$x \equiv 2^{-1} \cdot 3 \pmod{5}.$$

Let's do some examples.

Example 15. Solve the following.

- (a) Find $2^{-1} \bmod 5$.
- (b) Solve the equation $2x \equiv 3 \pmod{5}$ for x , up to modular equivalence.
- (c) Prove that 2 has no inverse modulo 4.

(a) By trial and error, $2 \cdot 3 \equiv 6 \equiv 1 \pmod{5}$. So $2^{-1} \equiv 3 \pmod{5}$. That is, $3 = 2^{-1} \bmod 5$.

(b) We can multiply both sides by $3 = 2^{-1} \bmod 5$.

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 6x &\equiv 9 \pmod{5} \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

As we hoped, multiplying by the inverse turned $2x$ into just x . Therefore $x \equiv 4 \pmod{5}$ solves the equation.

(c) For any $n \in \mathbb{Z}$, we have that $n \bmod 4 \in \{0, 1, 2, 3\}$. Let's consider the four cases.

- (1) $n \equiv 0 \pmod{4}$. Then $2n \equiv 2 \cdot 0 \equiv 0 \pmod{4}$.
- (2) $n \equiv 1 \pmod{4}$. Then $2n \equiv 2 \cdot 1 \equiv 2 \pmod{4}$.
- (3) $n \equiv 2 \pmod{4}$. Then $2n \equiv 2 \cdot 2 \equiv 4 \equiv 0 \pmod{4}$.
- (4) $n \equiv 3 \pmod{4}$. Then $2n \equiv 2 \cdot 3 \equiv 6 \equiv 2 \pmod{4}$.

In each of the four cases, $2n \bmod 4 \in \{0, 2\}$. That is, there is no $n \in \mathbb{Z}$ such that $2n \equiv 1 \pmod{4}$. So no inverse exists.

We saw in the last part of **Example 15** that inverses don't always exist. In particular, we weren't able to find an inverse for 2 modulo 4 because they shared factors in common—so they have overlapping cycles that never differ by one. In fact, if two numbers don't share any factors in common—that is, if their greatest common divisor is 1—we are guaranteed that an inverse exists. We have a special name for such numbers whose greatest common divisor is 1.

Definition 5. *Coprime numbers.* For any integers $a, b \in \mathbb{Z}$, we say that a and b are **coprime** or that they are **relatively prime** if $\gcd(a, b) = 1$.

Our shiny new definition allows us to describe when multiplicative inverses exist.

Theorem 7. For any integer $a \in \mathbb{Z}$ and modulus $m \in \mathbb{Z}^+$, a has a unique multiplicative inverse modulo m if and only if a and m are coprime.

Proof. We show that an inverse exists if a and m are coprime. The reverse direction, as well as the uniqueness, are left as an exercise.

(\Leftarrow) Suppose that $\gcd(a, m) = 1$. By Bezout's identity (**Lemma 4**), we have integers $x, y \in \mathbb{Z}$ such that

$$ax + my = 1.$$

Taking this equation with respect to the modulus m , we get that

$$\begin{aligned} ax + my &\equiv 1 \pmod{m} \\ ax + 0 &\equiv 1 \pmod{m} \\ ax &\equiv 1 \pmod{m}. \end{aligned}$$

Therefore $x \equiv a^{-1} \pmod{m}$.

This theorem gives us a way to find modular inverses—using the extended Euclidean algorithm. As we saw in **Section 1.3**, the extended Euclidean algorithm allows us to find the coefficients $x, y \in \mathbb{Z}$ which satisfy Bezout's identity.

We saw in **Example 8** that $12 \times 17 - 7 \times 29 = 1$. Taking this equation modulo 29 gets

$$12 \cdot 17 - 7 \cdot 29 \equiv 12 \cdot 17 \equiv 1 \pmod{29},$$

so $12 \equiv 17^{-1} \pmod{29}$. Similarly, taking the equation modulo 17 gets

$$12 \cdot 17 - 7 \cdot 29 \equiv -7 \cdot 29 \equiv 1 \pmod{17},$$

so the multiplicative inverse of $12 \equiv 29 \pmod{17}$ is $-7 \equiv 10 \pmod{17}$. That is, $12^{-1} \pmod{17} = 10$.

2.5 Modular Exponentiation

Just like addition, subtraction, multiplication, and division, we can also define exponentiation with respect to a modulus. We will define it recursively.

Definition 6. *Modular exponentiation.* For any integer $a \in \mathbb{Z}$, modulus $m \in \mathbb{Z}^+$, and exponent $n \in \mathbb{N}$, we define the modular exponential a^n modulo m with the following recursion.

- $a^0 \equiv 1 \pmod{m}$.
- $a^{n+1} \equiv a^n \cdot a \pmod{m}$.

We define $a^{-n} \equiv (a^{-1})^n \pmod{m}$.

This definition of exponentiation with respect to a modulus works just the way we expect exponentiation to work, since, just like regular exponentiation, this repeated multiplication.

Theorem 8. *Modular exponentiation.* For any natural numbers $n, k \in \mathbb{N}$, integers $a, b \in \mathbb{Z}$, and modulus $m \in \mathbb{Z}^+$, the following are true.

- (1) $a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$.
- (2) $a^{n+k} \equiv a^n a^k \pmod{m}$.
- (3) $a^n b^n \equiv (ab)^n \pmod{m}$.
- (4) $(a^n)^k \equiv a^{nk} \pmod{m}$.
- (5) $a^{n-k} \equiv a^n a^{-k} \pmod{m}$.
- (6) $(a^{-n})^k \equiv a^{-nk} \pmod{m}$.

Proof. Because modular exponentiation is defined through recursion, it lends itself well to proof by induction. All of these can be shown through induction. We will show (2) and (6). The rest are left as exercises.

For (2), we use proof by induction on n . That is, for each $n \in \mathbb{N}$ we prove that for all $k \in \mathbb{N}$ we have that $a^{n+k} \equiv a^n a^k$.

Base case. $n = 0$. Then for any $k \in \mathbb{N}$, we have that $a^{0+k} \equiv a^k \equiv 1 \cdot a^k \equiv a^0 a^k \pmod{m}$, as desired.

Induction case.

Induction hypothesis. For some $n \in \mathbb{N}$, suppose that for all $j \leq n$, for any $\ell \in \mathbb{N}$ we have that

$$a^{j+\ell} \equiv a^j a^\ell \pmod{m}.$$

Induction step. For any $k \in \mathbb{N}$, consider $a^{(n+1)+k}$. We have that

$$\begin{aligned} a^{(n+1)+k} &\equiv a^{(n+k)+1} \\ &\equiv a^{n+k} a^1 && \text{by the induction hypothesis with } j=1, \ell=n+k \\ &\equiv a^n a^k a^1 && \text{by the induction hypothesis with } j=n, \ell=k \\ &\equiv a^n a^1 a^k \\ &\equiv a^{n+1} a^k. && \text{by the induction hypothesis with } j=n, k=1 \end{aligned}$$

By the principle of mathematical induction, we have shown that for all $n \in \mathbb{N}$, for any $k \in \mathbb{N}$, $a^{n+k} \equiv a^n a^k \pmod{m}$.

For (3), we can use induction in much the same way we would in (4). However, a quicker proof just uses the result from (4):

$$(a^{-n})^k \equiv ((a^{-1})^n)^k \stackrel{(4)}{\equiv} (a^{-1})^{nk} \equiv a^{-nk}.$$

Rules (2), (3), and (4) can be seen as consequences of the corresponding real number equalities. For example, since $a^{n+k} = a^n a^k$ for $a \in \mathbb{R}$, the same equality is maintained in modular arithmetic.

Let's see some examples.

Example 16. Evaluate each of the following expressions.

(a) $1039403^4 \pmod{10}$.

(b) $(-4)^3 \pmod{3}$.

(c) $(43^3)^{-2} \pmod{5}$.

We'll simplify these expressions using **Theorem 8**.

(a) We have that $1039403 \equiv 3 \pmod{10}$. So $1039403^4 \equiv 3^4 \equiv 81 \equiv 1 \pmod{10}$. Our answer is 1.

(b) $-4 \equiv 3 - 4 \equiv -1 \equiv 3 - 1 \equiv 2 \pmod{3}$. So $(-4)^3 \equiv 2^3 \equiv 8 \equiv 2 \pmod{3}$.

(c) $43 \equiv 3 \pmod{5}$, so $(43^3)^{-2} \equiv 43^{-6} \equiv 3^{-6} \equiv (3^{-1})^6 \pmod{5}$.

Then $3^{-1} \equiv 2 \pmod{5}$ since $3 \cdot 2 \equiv 6 \equiv 1 \pmod{5}$, so $(3^{-1})^6 \equiv 2^6 \equiv 64 \equiv 4 \pmod{5}$.

There's one key place where modular exponentiation differs from our typical exponentiation on the real numbers. Over the real numbers, we have that if $n = k$, then $a^n = a^k$ —however this is no longer true with modular exponentiation.

Example 17. Suppose that $n \equiv k \pmod{m}$. Find a counterexample which shows that it is not necessarily the case that $a^n \equiv a^k \pmod{m}$.

Let's find an integer $a \in \mathbb{Z}$, two exponents $n, m \in \mathbb{N}$, and a modulus $m \in \mathbb{Z}^+$ such that the $n \equiv k \pmod{m}$ but $a^n \not\equiv a^k \pmod{m}$.

We can't use $a = 1$, since its powers are all 1. So we'll use $a = 2$. Then $n = 1$ and $k = 4$ are equivalent modulo $m = 3$. That is, $1 \equiv 4 \pmod{3}$. Then $2^1 \equiv 2 \pmod{3}$, but $2^4 \equiv 16 \equiv 1 \pmod{3}$. So we have our counterexample.

In general, we can use (1) from **Theorem 8** and simplifying with respect to our modulus to prevent our modular exponentials from blowing up too quickly, which makes computation of large exponentials more tractable.

For example, to compute $3^6 \pmod{5}$, we may do the following:

$$\begin{aligned} 3^6 &\equiv 3 \cdot 3 \cdot 3^4 \equiv 9 \cdot 3^4 \equiv 4 \cdot 3^4 \pmod{5} \\ &\equiv 4 \cdot 3 \cdot 3^3 \equiv 12 \cdot 3^3 \equiv 2 \cdot 3^3 \pmod{5} \\ &\equiv 2 \cdot 3 \cdot 3^2 \equiv 6 \cdot 3^2 \equiv 1 \cdot 3^2 \pmod{5} \\ &\equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod{5}. \end{aligned}$$

However, this can take many iterations—especially for large exponents—since each iteration decrements the exponent we’re dealing with by one.

For a faster algorithm, we can use the following observation which allows us to multiplicatively reduce exponents.

For any $n \in \mathbb{N}$, if $n = 2k$, then $a^n = a^{2k} = a^k a^k$. If instead $n = 2k + 1$, then $a^n = a^{2k+1} = a^k a^k a$. Notice that rather than decrementing the exponent n by 1, we’re dividing it by 2.

This motivates us to create the following **repeat squaring algorithm**.

Algorithm 2. *Repeat squaring.* For any integer $a \in \mathbb{Z}$, exponent $n \in \mathbb{N}$, and modulus $m \in \mathbb{Z}^+$, the following algorithm computes $a^n \pmod{m}$.

```
exp(a, n, m):
  if n = 0 then
    return 1
  else if n ≡ 0 (mod 2) then
    a_k ← exp(a, n/2, m)
    return (a_k · a_k) mod m
  else
    a_k ← exp(a, (n - 1)/2, m)
    return (a_k · a_k · a) mod m
```

Let’s see this algorithm in action.

Example 18. Use the repeat squaring algorithm to find $10^{20} \pmod{7}$.

Since $10 \equiv 3 \pmod{7}$, we know that $10^{20} \equiv 3^{20} \pmod{7}$. So we can instead find $3^{20} \pmod{7}$.

Using the algorithm, we get the following decomposition.

$$\begin{aligned} 3^{20} &\equiv (3^{10})^2 \pmod{7} \\ 3^{10} &\equiv (3^5)^2 \pmod{7} \\ 3^5 &\equiv (3^2)^2 \cdot 3 \pmod{7} \\ 3^2 &\equiv (3^1)^2 \pmod{7} \\ 3^1 &\equiv (3^0)^2 \cdot 3 \pmod{7} \\ 3^0 &\equiv 1 \pmod{7}. \end{aligned}$$

Starting from the bottom and working our way up, we get

$$\begin{aligned} 3^0 &\equiv 1 \pmod{7} \\ 3^1 &\equiv (3^0)^2 \cdot 3 \equiv 1^2 \cdot 3 \equiv 3 \pmod{7} \\ 3^2 &\equiv (3^1)^2 \equiv (3)^2 \equiv 9 \equiv 2 \pmod{7} \\ 3^5 &\equiv (3^2)^2 \cdot 3 \equiv (2)^2 \cdot 3 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \pmod{7} \\ 3^{10} &\equiv (3^5)^2 \equiv (5)^2 \equiv 4 \pmod{7} \\ 3^{20} &\equiv (3^{10})^2 \equiv (4)^2 \equiv 16 \equiv 2 \pmod{7}. \end{aligned}$$

That is, $10^{20} \bmod 7 = 2$.

A similar approach does the repeat squaring first, and then decomposes our exponential into the repeat squares second. That is, we can first evaluate 3^1 , $3^2 = (3^1)^2$, $3^4 = (3^2)^2$, and so on, as follows.

$$\begin{aligned} 3^1 &\equiv 3 & (\bmod 7) \\ 3^2 &\equiv (3^1)^2 \equiv (3)^2 \equiv 9 \equiv 2 & (\bmod 7) \\ 3^4 &\equiv (3^2)^2 \cdot 2^3 \equiv 4 & (\bmod 7) \\ 3^8 &\equiv (3^4)^2 \equiv (4)^2 \equiv 16 \equiv 2 & (\bmod 7) \\ 3^{16} &\equiv (3^8)^2 \equiv (2)^2 \equiv 4 & (\bmod 7). \end{aligned}$$

Once we have the repeat squares, we can then find a decomposition of our exponential in terms of the repeat squares. In this case, we can use the decomposition $3^{20} = 3^{16} \cdot 3^4$.

$$3^{20} \equiv 3^{16} \cdot 3^4 \equiv 4 \cdot 4 \equiv 16 \equiv 2 \pmod{7}.$$

3 Fermat's Little Theorem

Our investigation into modular exponentiation leads quite nicely into a spectacular result about modular exponentials known as **Fermat's little theorem**.

Let's consider two sequences. The first is just the integers modulo 5:

$$1, 2, 3, 4.$$

The second is the remainders of multiples of 2 modulo 5:

$$1 \times 2 \bmod 5, \quad 2 \times 2 \bmod 5, \quad 3 \times 2 \bmod 5, \quad 4 \times 2 \bmod 5.$$

Note that if we evaluate each term in the second sequence, we get the sequence

$$2, 4, 1, 3,$$

which is the same as our first sequence, but in a different order. Therefore if we multiply our first sequence together, we should get the same thing as if we multiply the second sequence together:

$$\begin{aligned} 1 \times 2 \times 3 \times 4 &\equiv 2 \times 4 \times 1 \times 3 & (\bmod 5) \\ 1 \times 2 \times 3 \times 4 &\equiv (1 \times 2) \times (2 \times 2) \times (3 \times 2) \times (4 \times 2) & (\bmod 5) \\ 24 &\equiv 24 \times 2^4 & (\bmod 5) \\ 4 &\equiv 4 \times 2^4 & (\bmod 5). \end{aligned}$$

If we multiply each side by $4 = 4^{-1} \bmod 5$, we get

$$2^4 \equiv 2^{5-1} \equiv 1 \pmod{5}.$$

This result is a specific instance of Fermat's little theorem.

Theorem 9. *Fermat's little theorem.* For any prime p and any $a \in \{1, \dots, p-1\}$, we have that

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem is quite useful for simplifying modular exponents when we're working with a prime modulus. For example, we could work through **Example 18** much more quickly, without using the repeat squaring

algorithm at all.

$$\begin{aligned}
10^{20} &\equiv 3^{20} \pmod{7} \\
&\equiv (3^6)^3 \cdot 3^2 \pmod{7} \\
&\equiv 1^3 \cdot 9 \pmod{7} && \text{by Fermat's little theorem} \\
&\equiv 2 \pmod{7}.
\end{aligned}$$

Before we can prove this theorem, we'll need to prove a few quick results.

Lemma 5. For any $a \in \mathbb{Z}$ and modulus $m \in \mathbb{Z}^+$ such that a and m are coprime, the numbers

$$0 \bmod m, \quad a \bmod m, \quad 2a \bmod m, \quad 3a \bmod m, \quad \dots, \quad (m-1)a \bmod m$$

are all distinct.

Proof. Suppose for contradiction that the numbers are not distinct; that is, suppose that there are repeats in the sequence. In particular, suppose that for some $j, k \in \{0, \dots, m-1\}$ with $j \neq k$, we have that $ja \bmod m = ka \bmod m$.

By **Theorem 4**, this means that $ja \equiv ka \pmod{m}$. Since a and m are coprime, $a^{-1} \bmod m$ exists and therefore

$$\begin{aligned}
ja &\equiv ka \pmod{m} \\
jaa^{-1} &\equiv kaa^{-1} \pmod{m} \\
j &\equiv k \pmod{m}.
\end{aligned}$$

Therefore $m \mid (j - k)$, so there exists $\ell \in \mathbb{Z}$ such that $j - k = \ell m$. However, since $0 \leq j, k < m$, we have that $-m < j - k < m$. We cannot have that $\ell \geq 1$ since then $j - k = \ell m \geq m$; likewise, we cannot have $\ell \leq -1$, since then $j - k = \ell m \leq -m$. It must be that $\ell = 0$. So $j - k = 0 \cdot m = 0$, which means that $j = k$.

This contradicts our assumption that $j \neq k$. So our assumption that there were repeats must be false. That is, the numbers must all be distinct.

Here's a slightly more straightforward result.

Lemma 6. For any prime p and integer $a \in \mathbb{Z}$, if $a \not\equiv 0 \pmod{p}$, then we have that $\gcd(a, p) = 1$. That is, if a is not a multiple of p , then $\gcd(a, p) = 1$.

Proof. By definition, since p is a prime, its only divisors are 1 and p . So the greatest common divisor can only be 1 or p . We can see that $1 \mid a$, so 1 is a common divisor.

Now suppose for contradiction that $p \mid a$. Then $a = kp$ for some $k \in \mathbb{Z}$, so a is a multiple of p . But then $a \equiv 0 \pmod{p}$, which is a contradiction. Therefore $p \nmid a$, so p is not a common divisor of a and p .

Therefore the greatest common divisor is 1. That is, $\gcd(a, p) = 1$.

Now we are ready to prove Fermat's little theorem.

Theorem 10. *Fermat's little theorem.* For any prime p and any $a \not\equiv 0 \pmod{p}$, we have that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Let $S = \{1, \dots, p-1\}$ be the set of nonzero integers modulo p . Consider the sequence of numbers

$$a \bmod p, \quad 2a \bmod p, \quad \dots, \quad (p-1)a \bmod p.$$

Note that since these numbers are remainders modulo p , each term is in the set $\{0, 1, \dots, p-1\}$.

By **Lemma 6**, $\gcd(a, p) = 1$. Therefore, by **Lemma 5**, these numbers are all distinct. Moreover, we claim that none of them are zero. By **Lemma 5**, the numbers

$$0 \bmod p, \quad a \bmod p, \quad \dots, \quad (p-1)a \bmod p.$$

are all distinct. In particular, the last $p-1$ terms, which are exactly the terms in our sequence, are all distinct from $0 = 0 \bmod p$. Therefore none of the terms in our sequence are zero. So each term is in the set $\{1, \dots, p-1\} = S$.

Since each of the $p-1$ terms in our sequence are distinct and in $\{1, \dots, p-1\}$, they must include each element of S exactly once. Suppose for contradiction that they did not. That is, suppose that some element of S occurs more than once or never occurs in the sequence.

- (1) Some element of S occurs more than once in the sequence. Then the terms in the sequence are not distinct.
- (2) Some element of S never occurs in the sequence. Then only $p-1-1 = p-2$ elements occur in the sequence. But there are $p-1 < p-2$ terms in our sequence, so by the pigeonhole principle, some element of S must then occur twice. But then all the terms in the sequence are not distinct.

So the only option is that every element of S occurs exactly once in the sequence. That is, the numbers in S and the numbers in the sequence are exactly the same.

Consider the product of all numbers in S , modulo p .

$$1 \cdot 2 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv (p-1)! \pmod{p}.$$

If we instead take the product of all numbers in the sequence, modulo p , we get

$$a \cdot 2a \cdot \dots \cdot (p-a)a \cdot (p-1)a \equiv a^{p-1}(p-1)! \pmod{p}.$$

Since S and the sequence have the same elements, this product of our sequence must be equal to our earlier product of S .

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Finally, since p is prime, each of $1, 2, \dots, p-1$ is coprime with p by **Lemma 6**, and hence has an inverse modulo p . So $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$ has an inverse since $1, 2, \dots, p-1$ all have inverses. That is,

$$(p-1)!^{-1} \equiv 1^{-1} \times 2^{-1} \times \dots \times (p-1)^{-1} \pmod{p}.$$

Therefore

$$\begin{aligned} a^{p-1}(p-1)! &\equiv (p-1)! && \pmod{p} \\ a^{p-1}(p-1)!((p-1)!)^{-1} &\equiv (p-1)!((p-1)!)^{-1} && \pmod{p} \\ a^{p-1} &\equiv 1 && \pmod{p}. \end{aligned}$$

The following corollary follows immediately from Fermat's little theorem.

Corollary 3. For any prime p and any $a \in \{0, 1, \dots, p-1\}$, we have that

$$a^p \equiv a \pmod{p}.$$

Proof. Left as an exercise.

4 The Chinese Remainder Theorem

In **Section 2.1**, we were introduced to the idea of linear congruences: equations of the form

$$ax \equiv b \pmod{m}$$

for $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, and an unknown $x \in \mathbb{Z}$ which we wish to solve for. We saw in **Section 2.4** how we can use the idea of modular inverses to solve such equations.

If a and m are coprime, then a^{-1} exists and is unique modulo m . Moreover, it can be found using the extended Euclidean algorithm. Therefore, when a and m are coprime, all solutions are given by

$$x \equiv a^{-1}b \pmod{m}.$$

4.1 Systems of Two Linear Congruences

A natural next step from linear congruences is to consider systems of linear congruences.

Example 19. Show that the following system of congruences has no solutions.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{4}. \end{aligned}$$

The first equation requires that x is even; that is, that $x = 2k$ for some $k \in \mathbb{Z}$. The second equation requires that x is one more than a multiple of 4. That is, that $x = 4j + 1$. However, this means that $x = 2(2j) + 1$, so x must be odd. This contradicts the fact that x is even, so no such x can exist.

The following theorem provides a sufficient condition for a system of two linear congruences to have a solution.

Theorem 11. For $m, n \in \mathbb{Z}^+$ relatively prime and $a, b \in \mathbb{Z}$, the system

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a solution, and it is unique modulo mn .

Proof. We tackle the existence of a solution first. We will construct $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} u &\equiv 1 \pmod{m} & u &\equiv 0 \pmod{n} \\ v &\equiv 0 \pmod{m} & v &\equiv 1 \pmod{n}. \end{aligned}$$

We can think of u and v like “switches” which activate (become 1) when the right modulus is being used. That is, u is a switch for m , and v is a switch for n .

Then $x = au + bv$ is a solution to the system, since

$$\begin{aligned} x &\equiv au + bv \equiv a \cdot 1 + b \cdot 0 \equiv a \pmod{m} \\ x &\equiv au + bv \equiv a \cdot 0 + b \cdot 1 \equiv b \pmod{n}. \end{aligned}$$

So let's find out what u and v have to be. The constraint $u \equiv 0 \pmod{n}$ means that u is a multiple of n . That is, for $k \in \mathbb{Z}$, $u = kn$. Now we apply the other constraint, which requires that

$$u \equiv kn \equiv 1 \pmod{m}.$$

By definition, this means that any $k \equiv n^{-1} \pmod{m}$ will work, where n^{-1} exists modulo m since $\gcd(m, n) = 1$. In particular, we'll use $k = n^{-1} \pmod{m}$.

A similar argument holds for v . Since $v \equiv 0 \pmod{m}$, we must have $j \in \mathbb{Z}$ such that $v = jm$. And then, since $v \equiv jm \equiv 1 \pmod{n}$, we have that $j = m^{-1} \pmod{n}$ works. Again, this inverse exists since $\gcd(m, n) = 1$.

Therefore

$$\begin{aligned} u &= (n^{-1} \pmod{m}) \cdot n \\ v &= (m^{-1} \pmod{n}) \cdot m \end{aligned}$$

works. In particular, our solution is

$$x = a \cdot (n^{-1} \pmod{m}) \cdot n + b \cdot (m^{-1} \pmod{n}) \cdot m.$$

Let's confirm again that this solution works.

$$\begin{aligned} x &\equiv a \cdot (n^{-1} \pmod{m}) \cdot n + b \cdot (m^{-1} \pmod{n}) \cdot m \pmod{m} \\ &\equiv a \cdot n^{-1} \cdot n + b \cdot (m^{-1} \pmod{n}) \cdot 0 \pmod{m} \\ &\equiv a \cdot 1 + b \cdot 0 \pmod{m} \\ &\equiv a \pmod{m}. \\ x &\equiv a \cdot (n^{-1} \pmod{m}) \cdot n + b \cdot (m^{-1} \pmod{n}) \cdot m \pmod{n} \\ &\equiv a \cdot (n^{-1} \pmod{m}) \cdot 0 + b \cdot m^{-1} \cdot m \pmod{n} \\ &\equiv a \cdot 0 + b \cdot 1 \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

We have that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, as desired.

To show that the solution is unique modulo mn , suppose that x and y are two solutions to the system of equations. That is,

$$\begin{array}{ll} x \equiv a \pmod{m} & \text{and} \quad y \equiv a \pmod{m} \\ x \equiv b \pmod{n} & y \equiv b \pmod{n}. \end{array}$$

Therefore

$$\begin{aligned} x &\equiv y \pmod{m} \\ x &\equiv y \pmod{n}. \end{aligned}$$

This means that $m \mid (x - y)$ and $n \mid (x - y)$. Since n and m are relatively prime, this means that $nm \mid (x - y)$; we use this fact without proving it. That is,

$$x \equiv y \pmod{mn}.$$

We have shown that any two solutions are equivalent modulo mn .

Concept Check 4. Prove the unjustified step of the uniqueness proof in **Theorem 11**. That is, prove that for $a, b \in \mathbb{Z}$ coprime and $c \in \mathbb{Z}$, if $a \mid c$ and $b \mid c$, then $ab \mid c$.

The following example allows us to see that this actually works.

Example 20. Find the smallest odd natural number x which is two more than a multiple of three.

By simply thinking about this, we can see that $x = 5$ works. Let's confirm that the method constructed in **Theorem 11** works as well.

The example says that x is odd, which means that $x \equiv 1 \pmod{2}$ and that x is two more than a multiple of three, which means that $x \equiv 2 \pmod{3}$. That's our system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3}. \end{aligned}$$

We need to construct the switches u and v . By **Theorem 11**,

$$\begin{aligned} u &= (3^{-1} \pmod{2}) \cdot 3 = 1 \cdot 3 = 3 \\ v &= (2^{-1} \pmod{3}) \cdot 2 = 2 \cdot 2 = 4. \end{aligned}$$

Therefore the solution as presented by **Theorem 11** is

$$x = 1 \cdot 3 + 2 \cdot 4 = 11.$$

That's a little strange—we got that $x = 5$ was the solution. But $x = 11$ also works. And if we think about it, $x = 17$ also works, or $x = 23$. All these solutions differ by $6 = 2 \cdot 3$. This is the uniqueness part of **Theorem 11**, which tells us that all solutions are equivalent modulo $2 \cdot 3 = 6$.

However, the example asks us for the smallest positive number. So $x = 5$ is our answer.

4.2 General Systems of Linear Congruences

Now we extend to systems of arbitrarily many linear congruences. The **Chinese remainder theorem**, named after the Chinese mathematician Sunzi who first stated the theorem sometime between the 3rd and 5th centuries CE, provides a sufficient condition for such systems to have a solution.

Theorem 12. *The Chinese remainder theorem.* For $m_1, \dots, m_n \in \mathbb{Z}^+$ pairwise coprime and any $a_1, \dots, a_n \in \mathbb{Z}$, the following system of $n \in \mathbb{N}^+$ equations has a unique solution modulo $m_1 \cdot \dots \cdot m_n$.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

Here, “pairwise coprime” means that $\gcd(m_i, m_j) = 1$ for any $i, j \in \{1, \dots, n\}$ with $i \neq j$.

Proof. The proof follows the proof of **Theorem 11** quite closely. We will construct switches s_1, \dots, s_n such that

$$\begin{array}{ccccccc} s_1 &\equiv 1 &\pmod{m_1} & s_1 &\equiv 0 &\pmod{m_2} & \dots & s_1 &\equiv 0 &\pmod{m_n} \\ s_2 &\equiv 0 &\pmod{m_1} & s_2 &\equiv 1 &\pmod{m_2} & \dots & s_2 &\equiv 0 &\pmod{m_n} \\ &\vdots & & &\vdots & & & &\vdots & \\ s_n &\equiv 0 &\pmod{m_1} & s_n &\equiv 0 &\pmod{m_2} & \dots & s_n &\equiv 1 &\pmod{m_n}. \end{array}$$

That is, for any $i, j \in \{1, \dots, n\}$ with $i \neq j$, the switch s_i activates under modulus m_i and deactivates under any other modulus m_j :

$$s_i \equiv 1 \pmod{m_i} \quad s_i \equiv 0 \pmod{m_j}.$$

Then we can construct a solution as

$$x = a_1 s_1 + \dots + a_n s_n = \sum_{i=1}^n a_i s_i.$$

To construct switch s_i , we require that $s_i \equiv 0 \pmod{m_j}$ for any $j \neq i$; that is, s_i must be a multiple of every modulus m_j except for m_i .

Towards this end, let $M = m_1 \cdot \dots \cdot m_n$ be the product of all the moduli and let $M_i = M/m_i$ be the product of all the moduli except for m_i . Then M_i is a multiple of each modulus m_j except for m_i by construction. We will use $s_i = kM_i$ so that for any $j \neq i$,

$$s_i \equiv kM_i \equiv 0 \pmod{m_j}.$$

We also require that $s_i \equiv 1 \pmod{m_i}$. This means that

$$kM_i \equiv 1 \pmod{m_i},$$

or, equivalently, that $k \equiv M_i^{-1} \pmod{m_i}$. We will without proof assume that this inverse exists modulo m_i ; in particular, we will use $k = M_i^{-1} \pmod{m_i}$.

Therefore, for each $i \in \{1, \dots, n\}$, we construct switch s_i as

$$s_i = (M_i^{-1} \pmod{m_i}) \cdot M_i.$$

Let us confirm that this yields a solution. For any $i \in \{1, \dots, n\}$,

$$\begin{aligned} x &\equiv \sum_{i=1}^n a_i s_i && \pmod{m_i} \\ &\equiv a_i s_i + \sum_{j \neq i}^n a_j s_j && \pmod{m_i} \\ &\equiv a_i \cdot (M_i^{-1} \pmod{m_i}) \cdot M_i + \sum_{j \neq i} a_j \cdot (M_j^{-1} \pmod{m_j}) \cdot M_j && \pmod{m_i} \\ &\equiv a_i \cdot M_i^{-1} \cdot M_i + \sum_{j \neq i} a_j \cdot (M_j^{-1} \pmod{m_j}) \cdot M_j && \pmod{m_i} \\ &\equiv a_i \cdot 1 + \sum_{j \neq i} a_j \cdot 0 && \pmod{m_i} \\ &\equiv a_i. \end{aligned}$$

So x solves the system of congruences.

To prove that the solution is unique modulo M , consider any two solutions x and y . Since they both solve the system, we have that

$$\begin{aligned} x &\equiv y \pmod{m_1} \\ &\vdots \\ x &\equiv y \pmod{m_n}. \end{aligned}$$

So $m_1 \mid (x - y), \dots, m_n \mid (x - y)$. Since they are pairwise coprime, this means that their product M also divides $x - y$. That is, $M \mid (x - y)$; we use this fact without proof. So $x \equiv y \pmod{M}$. Any two solutions are congruent modulo M .

The following example illustrates an application of the Chinese remainder theorem.

Example 21. Find the smallest integer solution to the following system.

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 3 \pmod{5} \\x &\equiv 2 \pmod{7}.\end{aligned}$$

We first compute M_1 , M_2 , and M_3 .

$$M_1 = 5 \cdot 7 = 35$$

$$M_2 = 3 \cdot 7 = 21$$

$$M_3 = 3 \cdot 5 = 15.$$

Next, we compute the inverses $M_1^{-1} \bmod m_1$, $M_2^{-1} \bmod m_2$, and $M_3^{-1} \bmod m_3$.

$$M_1^{-1} \bmod m_1 = 35^{-1} \bmod 3 = 2^{-1} \bmod 3 = 2$$

$$M_2^{-1} \bmod m_2 = 21^{-1} \bmod 5 = 1^{-1} \bmod 5 = 1$$

$$M_3^{-1} \bmod m_3 = 15^{-1} \bmod 7 = 1^{-1} \bmod 7 = 1.$$

In our penultimate step, we construct the switches s_1 , s_2 , and s_3 .

$$s_1 = (M_1^{-1} \bmod m_1) \cdot M_1 = 2 \cdot 35 = 70$$

$$s_2 = (M_2^{-1} \bmod m_2) \cdot M_2 = 1 \cdot 21 = 21$$

$$s_3 = (M_3^{-1} \bmod m_3) \cdot M_3 = 1 \cdot 15 = 15.$$

Finally, we construct a solution x .

$$x = a_1 s_1 + a_2 s_2 + a_3 s_3 = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233.$$

However, the question asks for the smallest positive integer solution. Is our answer here the smallest positive solution? By the Chinese remainder theorem (**Theorem 12**), all solutions are congruent modulo $m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$. So we can take the remainder of our solution modulo 105 to get the smallest positive solution.

$$233 \bmod 105 = 23.$$

Our answer is 23. Let's check that this actually solves the equations.

$$23 \equiv 2 \pmod{3} \quad \text{since } 23 = 7(3) + 2$$

$$23 \equiv 3 \pmod{5} \quad \text{since } 23 = 4(5) + 3$$

$$23 \equiv 2 \pmod{7} \quad \text{since } 23 = 3(7) + 2.$$

Concept Check 5. Find the smallest positive integer solution to the following system of equations.

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 4 \pmod{5}.$$