1. Divisibility in modular arithmetic

In this chapter, we’ll discuss division. Division is more difficult than addition, subtraction, and multiplication. We want to see when we can make sense of a fraction \( \frac{a}{b} \) (mod \( m \)). Further, when we can make sense of \( \frac{a}{b} \), we want to see how to compute \( \frac{a}{b} \).

1.1. Introduction to Division. We would like to say that \( \frac{a}{b} \equiv x \) (mod \( m \)) if \( b \cdot x \equiv a \) (mod \( m \)). The idea is that if \( b \cdot x \equiv a \) (mod \( m \)), and we divide each side by \( b \), we should get:

\[
\frac{b}{b} \cdot x \equiv \frac{a}{b} \pmod{m}.
\]

If \( \frac{b}{b} \equiv 1 \) (mod \( m \)), this gives:

\[
1 \cdot x \equiv \frac{a}{b} \pmod{m}.
\]

\[
x \equiv \frac{a}{b} \pmod{m}.
\]

As we’ll see in this Unit, this only works when \( b \) and \( m \) are relatively prime. We’ll see why division is more subtle than it appears, and learn to compute \( \frac{a}{b} \) (mod \( m \)) when \( b \) and \( m \) are relatively prime. For now, we’ll keep the following idea:

If \( \frac{a}{b} \equiv x \) (mod \( m \)), then

\[
a \equiv b \cdot x \pmod{m}.
\]

**EXAMPLE:** \( \frac{2}{3} \equiv 4 \) (mod 5), so \( 2 \equiv 3 \cdot 4 \) (mod 5).

You can check for yourself that \( 2 \equiv 3 \cdot 4 \) (mod 5).

1.2. Reciprocals. The easiest way to think about the fraction \( \frac{a}{b} \) is to first understand the fraction \( \frac{1}{b} \). Once we have understood \( \frac{1}{b} \) (mod \( m \)), then we will set \( \frac{a}{b} \equiv a \cdot \frac{1}{b} \) (mod \( m \)).

We say \( a \equiv \frac{1}{b} \) (mod \( m \)) if \( b \cdot a \equiv 1 \) (mod \( m \)).

**EXAMPLE:** Compute \( \frac{1}{3} \) (mod 5).

To answer this, let’s take a look at the mod 5 multiplication table from Unit 11:
We look for a mod 5 number \( x \) so that \( 3 \cdot x \equiv 1 \) (mod 5). If we look in the 3-row, we find 1 in the 2-column. This means that \( 3 \cdot 2 \equiv 1 \) (mod 5), so \( 2 \equiv \frac{1}{3} \) (mod 5).

Similarly, \( \frac{1}{4} \equiv 4 \) (mod 5), since \( 4 \cdot 4 \equiv 1 \) (mod 5), and similarly, \( \frac{1}{1} \equiv 1 \) (mod 5), and \( \frac{1}{2} \equiv 3 \) (mod 5). Note that \( \frac{1}{0} \) does not exist mod 5, since we cannot find a mod 5 number \( x \) so that \( 0 \cdot x \equiv 1 \) (mod 5).

Let’s try the same issue mod 6.

Find \( \frac{1}{5} \) (mod 6).

To solve this, we can take a look at the mod 6 multiplication table from Unit 11:

\[
\begin{array}{c|cccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 \\
2 & 0 & 2 & 4 & 0 & 2 & 4 \\
3 & 0 & 3 & 0 & 3 & 0 & 3 \\
4 & 0 & 4 & 2 & 0 & 4 & 2 \\
5 & 0 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

We find 1 in the 5-row and 5-column, which means that \( 5 \cdot 5 \equiv 1 \) (mod 6), so \( 5 \equiv \frac{1}{5} \) (mod 6).

How about \( \frac{1}{2} \) (mod 6)? If you look in the 2-row, there is no 1. This means there is no mod 6 number \( x \) so that \( 2 \cdot x \equiv 1 \) (mod 6). This means that \( \frac{1}{2} \) does not exist mod 6. Similarly, since there is no 1 in the 0, 3, or 4 columns, \( \frac{1}{0}, \frac{1}{3}, \) and \( \frac{1}{4} \) also do not exist. As you may expect, \( \frac{1}{1} \equiv 1 \) (mod 6).

We just saw that \( \frac{1}{a} \) (mod 6) exists when \( a = 1 \) or 5, and does not exist when \( a = 0, 2, 3, \) or 4. Note that 1 and 5 are relatively prime to 6, while 0, 2, 3 and 4 are not relatively prime to 6. This suggests the following result.

**Theorem 1.1.** \( \frac{1}{a} \) (mod \( m \)) exists exactly when \( a \) and \( m \) are relatively prime.
Let’s see why this works in an example where \( m = 21 \). The number \( a = 16 \) is relatively prime to 21, which is another way of saying that \( \gcd(16, 21) = 1 \). Following the method of Unit 7, we can use the reverse Euclidean algorithm to write 1 as a combination of 16 and 21. Explicitly,

\[
21 = 1 \cdot 16 + 5 \\
16 = 3 \cdot 5 + 1
\]

When we reverse these steps as in Unit 7, we find:

\[
1 = 16 - 3 \cdot 5 \\
1 = 16 - 3 \cdot (21 - 16) = 4 \cdot 16 - 3 \cdot 21
\]

so

\[
1 = 4 \cdot 16 - 3 \cdot 21.
\]

Let’s interpret this identity mod 21. It says:

\[
1 \equiv 4 \cdot 16 - 3 \cdot 21 \pmod{21},
\]

so

\[
1 \equiv 4 \cdot 16 \pmod{21}.
\]

In general, if \( \gcd(a, m) = 1 \), then by using the method of Unit 7, there are integers \( x \) and \( y \) so that \( a \cdot x + m \cdot y = 1 \). Then

\[
1 \equiv a \cdot x + m \cdot y \equiv a \cdot x + m \cdot 0 \equiv a \cdot x \pmod{m}.
\]

Thus,

\[
1 \equiv a \cdot x \pmod{m} \text{ and } \frac{1}{a} \equiv x \pmod{m}.
\]

We can also see in an example why \( \frac{1}{a} \pmod{m} \) does not exist if \( \gcd(a, m) \) is not 1.

Let’s try this with \( a = 6 \) and \( m = 21 \). If \( \frac{1}{6} \equiv x \pmod{21} \), then \( 6 \cdot x \equiv 1 \pmod{21} \).

But this means that 21 divides \( 1 - 6 \cdot x \), so also 3 divides \( 1 - 6 \cdot x \). Since 3 divides \( 1 - 6 \cdot x \), \( 1 - 6 \cdot x \equiv 0 \pmod{3} \), so \( 1 \equiv 6 \cdot x \pmod{3} \). But this cannot happen, since 6 \( \equiv 0 \pmod{3} \) because 6 \( \equiv 0 \pmod{3} \), so we would get the absurd statement \( 1 \equiv 0 \pmod{3} \). This shows that \( \frac{1}{6} \pmod{21} \) cannot exist. A similar argument implies that \( \frac{1}{a} \pmod{m} \) does not exist if \( \gcd(a, m) \) is not 1.

### 1.3. Computing reciprocals

If you are asked to compute \( \frac{1}{a} \pmod{m} \), you can solve the problem as follows.

**STEP 1:** Compute \( \gcd(a, m) \). If the answer is not 1, then \( \frac{1}{a} \pmod{m} \) does not exist by Theorem 1.1 of the last section. Say that the reciprocal does not exist, and move on to the next problem.
STEP 2: If \( \gcd(a, m) = 1 \), then use the reverse Euclidean algorithm from Unit 7 to find integers \( x \) and \( y \) so that \( a \cdot x + m \cdot y = 1 \). Then \( a \cdot x \equiv 1 \pmod{m} \), and \( x \equiv \frac{1}{a} \pmod{m} \).

In this section, we’ll work out some examples of this.

PROBLEM: Compute \( \frac{1}{5} \pmod{26} \).

To solve this, note that \( \gcd(5, 26) = 1 \), so \( \frac{1}{5} \) exists. Now do the Euclidean algorithm for 26 and 5:

\[
26 = 5 \cdot 5 + 1
\]

and use this to write 1 as a combination of 5 and 26:

\[
1 = 1 \cdot 26 - 5 \cdot 5.
\]

Interpret this as a mod 26 equality, to get:

\[
1 \equiv 1 \cdot 26 - 5 \cdot 5 \equiv -5 \cdot 5 \pmod{26},
\]

since clearly \( 1 \cdot 26 \equiv 0 \pmod{26} \). So

\[
1 \equiv -5 \cdot 5 \pmod{26},
\]

and we get:

\[
\frac{1}{5} \equiv -5 \equiv 21 \pmod{26}, \quad \text{and} \quad \frac{1}{5} \equiv 21 \pmod{26}
\]

solves the problem.

PROBLEM: Compute \( \frac{1}{17} \pmod{60} \).

You can check that \( \gcd(17, 60) = 1 \). Now use the Euclidean algorithm to write 1 as a combination of 17 and 60. The steps are:

\[
60 = 3 \cdot 17 + 9
\]

\[
17 = 9 + 8
\]

\[
9 = 8 + 1, \quad \text{so} \quad 1 = 9 - 8
\]

\[
1 = 9 - (17 - 9) = 2 \cdot 9 - 17
\]

\[
1 = 2 \cdot (60 - 3 \cdot 17) - 17 = 2 \cdot 60 - 7 \cdot 17
\]

so

\[
1 = 2 \cdot 60 - 7 \cdot 17.
\]

Consider this mod 60, which gives

\[
1 \equiv -7 \cdot 17 \pmod{60}, \quad \text{so} \quad \frac{1}{17} \equiv -7 \equiv 53 \pmod{60}.
\]

So \( \frac{1}{17} \equiv 53 \pmod{60} \). You can check this with a calculator by verifying that \( 17 \cdot 53 \equiv 1 \pmod{60} \), i.e., 60 divides \( 17 \cdot 53 \) with remainder 1.

PROBLEM: Compute \( \frac{1}{201} \pmod{340} \) and \( \frac{1}{17} \pmod{340} \).

Since \( \gcd(17, 340) = 17 \), 17 and 340 are not relatively prime, so \( \frac{1}{17} \pmod{340} \) does not exist. The following steps show that \( \gcd(201, 340) = 1 \):

\[
340 = 201 + 139
\]
\[201 = 139 + 62\]
\[139 = 2 \cdot 62 + 15\]
\[62 = 4 \cdot 15 + 2\]
\[15 = 7 \cdot 2 + 1,\]
and then if we use the reverse Euclidean algorithm, we get:
\[1 = 15 - 7 \cdot 2 = 15 - 7 \cdot (62 - 4 \cdot 15) = 29 \cdot 15 - 7 \cdot 62\]
\[1 = 29 \cdot (139 - 2 \cdot 62) - 7 \cdot 62 = 29 \cdot 139 - 65 \cdot 62\]
\[1 = 29 \cdot 139 - 65 \cdot (201 - 139) = 94 \cdot 139 - 65 \cdot 201\]
\[1 = 94 \cdot (340 - 201) - 65 \cdot 201 = 94 \cdot 340 - 159 \cdot 201,\]
so
\[1 = 94 \cdot 340 - 159 \cdot 201.\]
We consider this mod 340, and get:
\[1 \equiv -159 \cdot 201 \pmod{340},\]
so
\[\frac{1}{201} \equiv -159 \equiv 181 \pmod{340}.\]
So \(\frac{1}{201} \equiv 181 \pmod{340}\) is our final answer. This problem takes quite a bit of work, but if you are systematic and careful, this problem is not difficult.

1.4. Division. We are now ready to discuss \(\frac{a}{b} \pmod{m}\).

CASE 1: If \(\gcd(b, m)\) does not equal 1, then \(\frac{a}{b} \pmod{m}\) does not exist.

CASE 2: If \(\gcd(b, m) = 1\), then \(\frac{a}{b} = a \cdot \frac{1}{b} \pmod{m}\).

In CASE 2, we can compute \(\frac{1}{b} \pmod{m}\) following the method of the previous section, and multiply that number by \(a\) to get \(\frac{a}{b} \pmod{m}\).

EXAMPLE: Compute \(\frac{3}{4} \pmod{9}\)

To compute this, first check that \(\gcd(4, 9) = 1\), so \(\frac{3}{4} \pmod{9}\) exists. Now calculate \(\frac{1}{4} \pmod{9}\). To do this, use the Euclidean algorithm to find:
\[9 = 2 \cdot 4 + 1,\]
which implies that:
\[1 = 9 - 2 \cdot 4,\]
so
\[1 \equiv -2 \pmod{9},\]
and
\[\frac{1}{4} \equiv -2 \pmod{9}.\]
Since \(-2 \equiv 7 \pmod{9}\), \(\frac{1}{4} \equiv 7 \pmod{9}\).

So \(\frac{3}{4} \equiv 3 \cdot \frac{1}{4} \equiv 3 \cdot 7 \equiv 21 \equiv 3 \pmod{9}\), so \(\frac{3}{4} \equiv 3 \pmod{9}\).

EXAMPLE: Compute \(\frac{5}{6} \pmod{21}\).

We compute \(\gcd(6, 21) = 3\), so 6 and 21 are not relatively prime. This means that \(\frac{5}{6} \pmod{21}\) does not exist.
EXAMPLE: Compute \( \frac{3}{17} \pmod{60} \).

Since \( \gcd(17, 60) = 1 \), the fraction \( \frac{3}{17} \pmod{60} \) exists. In the last section, we compute \( \frac{1}{17} \equiv 53 \pmod{60} \), so
\[
\frac{3}{17} \equiv 3 \cdot \frac{1}{17} \equiv 3 \cdot 53 \equiv 159 \equiv 39 \pmod{60}, \quad \text{so} \quad \frac{3}{17} \equiv 39 \pmod{60}.
\]

CHECKING CALCULATIONS: If \( \frac{a}{b} \equiv c \pmod{m} \), then \( \gcd(b, m) = 1 \), and by multiplying each side by \( b \), we get:
\[
\frac{a}{b} \cdot b \equiv b \cdot c \pmod{m}.
\]
But
\[
\frac{a}{b} \cdot b \equiv a \cdot \frac{1}{b} \cdot b \equiv a \cdot \frac{b}{b} \equiv a \cdot 1 \equiv a \pmod{m}.
\]
We conclude: \( \frac{a}{b} \equiv c \pmod{m} \) implies that \( a \equiv b \cdot c \pmod{m} \).

We can use this last observation to check our calculations. For example, to check that our computation \( \frac{3}{17} \equiv 39 \pmod{60} \) from the last example is correct, we can check that \( 3 \equiv 17 \cdot 39 \pmod{60} \). If you check on your calculator, you will find that \( 17 \cdot 39 \equiv 663 \equiv 3 \pmod{60} \), which verifies that our calculation is correct.

WEIRDNESS WITH MODULAR ARITHMETIC FRACTIONS: There are some strange things that happen with fractions in modular arithmetic.

PROBLEM: Compute \( \frac{1}{3} \pmod{10} \). Compute \( \frac{2}{6} \pmod{10} \).

To solve the first problem, since \( \gcd(3, 10) = 1 \), \( \frac{1}{3} \pmod{10} \) exists. Using the reverse Euclidean algorithm, we get \( 1 \equiv 10 - 3 \cdot 3 \pmod{10} \), so
\[
1 \equiv -3 \cdot 3 \pmod{10} \quad \text{and} \quad \frac{1}{3} \equiv -3 \equiv 7 \pmod{10}, \quad \text{so} \quad \frac{1}{3} \equiv 7 \pmod{10}.
\]

On the other hand, \( \frac{2}{6} \pmod{10} \) does not exist since \( \gcd(6, 10) = 2 \) is not 1. So we have the counterintuitive situation that \( \frac{1}{3} \) exists, but \( \frac{2}{6} \) does not exist in mod 10 arithmetic. Especially, \( \frac{1}{3} \) does not equal \( \frac{2}{6} \) in mod 10 arithmetic.

To explain this, we can refer to the motivation at the beginning of Section 1.1. We said that \( x \equiv \frac{a}{b} \pmod{m} \) should mean that \( b \cdot x \equiv a \pmod{m} \). The idea is that if \( b \cdot x \equiv a \pmod{m} \), then if we divide each side by \( b \), we should get:
\[
x \equiv \frac{a}{b} \pmod{m}.
\]

Let’s try this with \( b = 6 \), \( a = 2 \), and \( m = 10 \). Then you can easily check that:
\[
6 \cdot 2 \equiv 2 \pmod{10}.
\]
If we could divide each side by 6, we would get:
\[
2 \equiv \frac{2}{6} \pmod{10}.
\]
On the other hand, we can also check that:
6 \cdot 7 \equiv 2 \pmod{10}. If we divide each side by 6, we would get:
7 \equiv \frac{2}{6} \pmod{10}.

So putting these two cases together, we find:
2 \equiv \frac{2}{6} \equiv 7 \pmod{10}, so
2 \equiv 7 \pmod{10}, and this is clearly wrong, since 10 does not divide 2 \cdot 7.
The main issue is that dividing by 6 in mod 10 arithmetic, would be the same thing
as multiplying by \frac{1}{6} \pmod{10}, and we saw earlier that \frac{1}{6} \pmod{10} does not exist
in Theorem 1.1 since 6 and 10 are not relatively prime. In other words, \frac{1}{6} \pmod{10}
does not exist because there is no number x such that 6 \cdot x \equiv 1 \pmod{10}. Indeed,
6 \cdot x - 1 must be an odd number, so it cannot be a multiple of 10. Another way of
thinking about this is to say that we can’t divide by 6 mod 10 for the same reason
that we can’t divide by 0 in usual arithmetic.

We can summarize this discussion:
(1) If gcd(b, m) = 1, then \frac{a}{b} \pmod{m} exists. Further, \frac{a}{b} \equiv a \pmod{m}, i.e., x \equiv \frac{a}{b} \pmod{m}
is the only solution to b \cdot x \equiv a \pmod{m}.

EXAMPLE: \frac{2}{3} \equiv 10 \pmod{14}.

To see this, note first that gcd(3, 14) = 1, and then note that \frac{1}{3} \equiv 5 \pmod{14}, so
\frac{2}{3} \equiv 2 \cdot \frac{1}{3} \equiv 2 \cdot 5 \equiv 10 \pmod{14}.

Further, x \equiv \frac{2}{3} \equiv 10 \pmod{14} is a solution to 3 \cdot x \equiv 2 \pmod{14} since 3 \cdot 10 \equiv 2
(\pmod{14}). On the other hand, if 3 \cdot x \equiv 2 \pmod{14}, we can multiply each side by
\frac{1}{3} \equiv 5 to obtain:
5 \cdot 3 \cdot x \equiv 5 \cdot 2 \equiv 10 \pmod{14}.
Since 5 \cdot 3 \equiv 1 \pmod{14}, this means that
x \equiv 1 \cdot x \equiv 5 \cdot 3 \cdot x \equiv 10 \pmod{14},
so if x is a solution to 3 \cdot x \equiv 2 \pmod{14}, then x \equiv 2 \pmod{14}.

(2) If gcd(b, m) is not 1, then \frac{a}{b} \pmod{m} does not exist. Either
(A) there is no solution to b \cdot x \equiv a \pmod{m} or
(B) There is more than one solution to b \cdot x \equiv a \pmod{m}.

For example, if we let m = 14 and b = 4 so gcd(4, 14) = 2, then there is no solution to:
4 \cdot x \equiv 3 \pmod{14}. If there were a solution, then 4 \cdot x - 3 \equiv 0 \pmod{14}, so 14 divides
4 \cdot x - 3. But 4 \cdot x - 3 is odd because 4 \cdot x is even and 3 is odd, so 14 cannot divide
an odd number.

For an example of (B), consider the equation
4 \cdot x \equiv 6 \pmod{14}. The reader can check easily that \( x \equiv 5 \pmod{14} \) and \( x \equiv 12 \pmod{14} \) are both solutions, since \( 4 \cdot 5 \equiv 20 \equiv 6 \pmod{14} \) and \( 4 \cdot 12 \equiv 6 \pmod{14} \). This means that \( \frac{6}{4} \pmod{14} \) does not exist, because it would have two values.

EXERCISES:

1. Compute the following reciprocals in modular arithmetic, or explain why the reciprocal does not exist:
   (a) \( \frac{1}{11} \pmod{14} \)
   (b) \( \frac{1}{8} \pmod{14} \)
   (c) \( \frac{1}{3} \pmod{7} \)
   (d) \( \frac{1}{6} \pmod{7} \)
   (e) \( \frac{1}{7} \pmod{7} \)

2. Compute the following reciprocals in modular arithmetic, or explain why the reciprocal does not exist:
   (a) \( \frac{1}{13} \pmod{43} \)
   (b) \( \frac{1}{42} \pmod{43} \)
   (c) \( \frac{1}{-1} \pmod{43} \)
   (d) \( \frac{1}{17} \pmod{42} \)
   (e) \( \frac{1}{35} \pmod{42} \)

3. Compute the following reciprocals in modular arithmetic:
   (a) \( \frac{1}{123} \pmod{503} \)
   (b) \( \frac{1}{423} \pmod{2311} \)

4. Compute the following fractions in modular arithmetic, or explain why they do not exist:
   (a) \( \frac{5}{8} \pmod{13} \)
   (b) \( \frac{5}{13} \pmod{43} \)
   (c) \( \frac{5}{24} \pmod{42} \)
   (d) \( \frac{7}{8} \pmod{102013452} \)
   (e) \( \frac{7}{423} \pmod{2311} \)
(5) Find all mod 22 numbers \( x \) so that \( 3 \cdot x \equiv 4 \pmod{22} \). Find all mod 22 numbers \( x \) so that \( 6 \cdot x \equiv 8 \pmod{22} \). Does the fraction \( \frac{4}{3} \pmod{22} \) exist?

Does the fraction \( \frac{8}{6} \pmod{22} \) exist?

(6) Find a mod 60 number \( x \) so that \( 31 \cdot x \equiv 5 \pmod{60} \).

(7) A security guard drives past an ATM at exactly 5 minutes after the start of each hour (i.e., at 1:05, 2:05, 3:05 and so on). A robber wearing a mask comes to the ATM every 31 minutes starting at 1:31. When does the security guard first arrive at the ATM at the same time as the robber? (hint: use the last problem. Also, the security guard and robber never have to sleep).