Math 3527 (Number Theory 1)

Lecture #8 of 38 $\sim$ January 26, 2026

Residue Classes + Modular Arithmetic

- Residue Classes Modulo m
- Modular Arithmetic
- Units in $\mathbb{Z}/m\mathbb{Z}$

This material represents §2.1.2-§2.1.4 from the course notes.

Recall, I

Recall our discussion of congruences last week:

Definition

If m is a modulus, we say $a \equiv b$ (modulo m) when m divides $b - a$.

Proposition (Properties of Congruences)

For any modulus $m > 0$ and any integers a, b, c, d, we have

1. $a \equiv a \pmod{m}$.
2. $a \equiv b \pmod{m}$ *if and only if* $b \equiv a \pmod{m}$.
3. *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.
4. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$.
5. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$.

Recall, II

We also introduced residue classes:

Definition

If a is an integer, the residue class of a modulo m is the set $\overline{a} = \{b \in \mathbb{Z} : a \equiv b (\text{mod } m)\}$ *of integers congruent to a modulo m.*

- More explicitly, $\overline{a} = \{\ldots, a-3m, a-2m, a-m, a, a+m, a+2m, a+3m, \ldots\}$.
- It is very important to remember that residue classes are *sets* of integers: they are not themselves numbers. (Yet.)

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\ldots, -6, -2, 2, 6, 10, 14, \ldots\}$.

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\ldots, -6, -2, 2, 6, 10, 14, \ldots\}$.
- The residue class of 2 modulo 5 is the set $\{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$.

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\dots, -6, -2, 2, 6, 10, 14, \dots\}$.
- The residue class of 2 modulo 5 is the set $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.
- The residue class of 11 modulo 19 is the set $\{\dots,\ -27,\ -8, 11,\ 30,\ 49,\ 68,\ ,\dots\}$.

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\dots, -6, -2, 2, 6, 10, 14, \dots\}$.
- The residue class of 2 modulo 5 is the set $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.
- The residue class of 11 modulo 19 is the set $\{\dots,\ -27,\ -8, 11,\ 30,\ 49,\ 68,\ ,\dots\}$.
- The residue class of 0 modulo 2 is the set $\{\dots, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$ of even integers.

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\dots, -6, -2, 2, 6, 10, 14, \dots\}$.
- The residue class of 2 modulo 5 is the set $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.
- The residue class of 11 modulo 19 is the set $\{\dots,\ -27,\ -8, 11,\ 30,\ 49,\ 68,\ ,\dots\}$.
- The residue class of 0 modulo 2 is the set $\{\dots, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$ of even integers.
- The residue class of 1 modulo 2 is the set $\{\dots, -5, -3, -1, 1, 3, 5, 7, 9, \dots\}$ of odd integers.

Examples

Here are some examples of residue classes for different moduli m:

- The residue class of 2 modulo 4 is the set $\{\ldots, -6, -2, 2, 6, 10, 14, \ldots\}$.
- The residue class of 2 modulo 5 is the set $\{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$.
- The residue class of 11 modulo 19 is the set $\{\ldots,\ -27,\ -8, 11,\ 30,\ 49,\ 68,\ ,\ldots\}$.
- The residue class of 0 modulo 2 is the set $\{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$ of even integers.
- The residue class of 1 modulo 2 is the set $\{\ldots, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}$ of odd integers.
- More generally, the residue class of 0 modulo m is the set $\{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ of multiples of m.

Examples Mod 3

Last time, we identified three different residue classes modulo 3:

- Zeroth, $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.
- First, $\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$.
- Second, $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.

If you write out other residue classes modulo 3, you'll discover they just end up duplicating one of these three:

Examples Mod 3

Last time, we identified three different residue classes modulo 3:

- Zeroth, $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.
- First, $\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$.
- Second, $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.

If you write out other residue classes modulo 3, you'll discover they just end up duplicating one of these three:

- Try $\overline{4} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\} = \overline{1}$.
- Or $\overline{5} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\} = \overline{2}$.
- Or $\overline{10} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\} = \overline{1}$ also.

It seems that there are really only three different residue classes modulo 3, each of which has many different names. What pattern do the names have?

Properties of Residue Classes, I

Let's prove some properties of residue classes:

Proposition (Properties of Residue Classes)

Let $m > 0$ be a modulus. Then

1. *If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.*
2. *Two residue classes modulo m are either disjoint or identical.*
3. *There are exactly m distinct residue classes modulo m, given by $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.*

Properties of Residue Classes: II

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

Let's strategize first.

- Note that this is an if-and-only-if statement, so we need to prove both directions: "if $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$" and the converse "if $\overline{a} = \overline{b}$ then $a \equiv b \pmod{m}$".
- Note also that the statement $\overline{a} = \overline{b}$ is an equality of sets.
- To show that, we need to show each set is a subset of the other.

Properties of Residue Classes; III

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

Proof: [Forward] If $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$.

- So, suppose $a \equiv b \pmod{m}$. [Goal: Show that $\overline{a} \subseteq \overline{b}$.]
- So suppose $x \in \overline{a}$, which is to say, $x \equiv a \pmod{m}$.

Properties of Residue Classes; III

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

Proof: [Forward] If $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$.

- So, suppose $a \equiv b \pmod{m}$. [Goal: Show that $\overline{a} \subseteq \overline{b}$.]
- So suppose $x \in \overline{a}$, which is to say, $x \equiv a \pmod{m}$.
- Now because $x \equiv a \pmod{m}$ and $a \equiv b \pmod{m}$, by our properties of congruences we can conclude that $x \equiv b \pmod{m}$, and therefore $x \in \overline{b}$ as claimed.

Properties of Residue Classes; III

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

Proof: [Forward] If $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$.

- So, suppose $a \equiv b \pmod{m}$. [Goal: Show that $\overline{a} \subseteq \overline{b}$.]
- So suppose $x \in \overline{a}$, which is to say, $x \equiv a \pmod{m}$.
- Now because $x \equiv a \pmod{m}$ and $a \equiv b \pmod{m}$, by our properties of congruences we can conclude that $x \equiv b \pmod{m}$, and therefore $x \in \overline{b}$ as claimed.
- We still have to show that $\overline{b} \subseteq \overline{a}$. In fact, the argument is exactly the same, just with a and b swapped. (Write it out if you like!)

Properties of Residue Classes. IV

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

<u>Proof</u>: [Reverse] If $\overline{a} = \overline{b}$ then $a \equiv b \pmod{m}$.

- Now suppose $\overline{a} = \overline{b}$.

Properties of Residue Classes. IV

1. If a and b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod{m}$ if and only if $\overline{a} = \overline{b}$.

Proof: [Reverse] If $\overline{a} = \overline{b}$ then $a \equiv b \pmod{m}$.

- Now suppose $\overline{a} = \overline{b}$.
- Since $a \in \overline{a}$, by definition, that means $a \in \overline{b}$ too.
- But $\overline{b}$ is just the set of integers congruent to b modulo m.
- So that means a is congruent to b modulo m, as desired.

Properties of Residue Classes! V

2. Two residue classes modulo m are either disjoint or identical.

Proof:

- Suppose that $\overline{a}$ and $\overline{b}$ are residue classes modulo m.
- If $\overline{a} \cap \overline{b} = \emptyset$ then we are immediately done, so suppose $\overline{a} \cap \overline{b}$ is nonempty. [To show: $\overline{a} = \overline{b}$.]

Properties of Residue Classes! V

2. Two residue classes modulo m are either disjoint or identical.

Proof:

- Suppose that $\overline{a}$ and $\overline{b}$ are residue classes modulo m.
- If $\overline{a} \cap \overline{b} = \emptyset$ then we are immediately done, so suppose $\overline{a} \cap \overline{b}$ is nonempty. [To show: $\overline{a} = \overline{b}$.]
- Since $\overline{a} \cap \overline{b}$ is nonempty, the intersection contains some element x.
- Since $x \in \overline{a}$ that means $a \equiv x \pmod{m}$, and since $x \in \overline{b}$ that means $b \equiv x \pmod{m}$.
- So by congruence properties, we see that $a \equiv b \pmod{m}$.
- But now, by (1) from earlier, that implies $\overline{a} = \overline{b}$, as desired.

Properties of Residue Classes? VII

3. There are exactly m distinct residue classes modulo m, given by $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.

Proof:

- Notice that these are the possible remainders when we divide an integer by m.

Properties of Residue Classes? VII

3. There are exactly m distinct residue classes modulo m, given by $\overline{0}, \overline{1}, \dots, \overline{m-1}$.

Proof:

- Notice that these are the possible remainders when we divide an integer by m.
- So: by the division algorithm, for any integer a there exists a unique r with $0 \leq r < m$ such that $a = qm + r$ with $q \in \mathbb{Z}$.
- But now $a = qm + r$ tells us that $a \equiv r \pmod{m}$, which by (1) says $\overline{a} = \overline{r}$.
- But the possible values of r are the m integers 0, 1, ... , $m - 1$, and r is unique.
- Thus, any residue class $\overline{a}$ modulo m is equal to precisely one of the residue classes $\overline{0}, \overline{1}, \dots, \overline{m-1}$, as claimed!

Properties of Residue Classes – VIII

Definition

The collection of residue classes modulo m is denoted $\mathbb{Z}/m\mathbb{Z}$ (read as "$\mathbb{Z}$ modulo $m\mathbb{Z}$").

- Remark: Many other authors denote this collection of residue classes modulo m as $\mathbb{Z}_m$.[1] We will avoid this notation and exclusively use $\mathbb{Z}/m\mathbb{Z}$ (or its shorthand $\mathbb{Z}/m$), since $\mathbb{Z}_m$ is used elsewhere in algebra and number theory for a different object.
- By the properties we just proved, $\mathbb{Z}/m\mathbb{Z}$ contains exactly m elements: namely, $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.

[1] Feel free, if you see other people writing the integers modulo m this way, to tell them that I, Prof. Dummit, specifically said you should tell them they're using the wrong notation.

Arithmetic With Residue Classes, I

Our goal now is to describe how to define arithmetic operations on the residue classes modulo m.

Definition

The addition operation in $\mathbb{Z}/m\mathbb{Z}$ is defined as $\overline{a} + \overline{b} = \overline{a+b}$, and the multiplication operation is defined as $\overline{a} \cdot \overline{b} = \overline{ab}$.

- Notationally, the operations look very natural: we just add (or multiply) the corresponding numbers under the bars.
- But the notation is hiding a lot of complexity: remember, $\overline{a}$ is a *set*, not a number.

Arithmetic With Residue Classes, II

Let's illustrate with an example: take modulus $m = 4$, so that our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- The definition on the last slide says, for example, that we should define $\overline{1} + \overline{1} = \overline{2}$. Seems reasonable, right?

Arithmetic With Residue Classes, II

Let's illustrate with an example: take modulus $m = 4$, so that our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- The definition on the last slide says, for example, that we should define $\overline{1} + \overline{1} = \overline{2}$. Seems reasonable, right?
- Okay, so then what should $\overline{1} + \overline{3}$ be? By definition, that's... $\overline{4}$.
- But $\overline{4}$ isn't one of our residue classes.

Arithmetic With Residue Classes, II

Let's illustrate with an example: take modulus $m = 4$, so that our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- The definition on the last slide says, for example, that we should define $\overline{1} + \overline{1} = \overline{2}$. Seems reasonable, right?
- Okay, so then what should $\overline{1} + \overline{3}$ be? By definition, that's... $\overline{4}$.
- But $\overline{4}$ isn't one of our residue classes.
- Except, yes, it actually is, because it's just $\overline{0}$ by another name. So we have $\overline{1} + \overline{3} = \overline{0}$.

Arithmetic With Residue Classes, III

Let's continue with $m = 4$ and residue classes $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- We just decided that $\overline{1} + \overline{3} = \overline{0}$.
- Okay, now: what is $\overline{5} + \overline{11}$? (Remember, these are perfectly good residue classes modulo 4!)

Arithmetic With Residue Classes, III

Let's continue with $m = 4$ and residue classes $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- We just decided that $\overline{1} + \overline{3} = \overline{0}$.
- Okay, now: what is $\overline{5} + \overline{11}$? (Remember, these are perfectly good residue classes modulo 4!)
- The definition says the sum should be $\overline{16}$.
- But wait: $\overline{5}$ is equal to $\overline{1}$, and $\overline{3}$ is equal to $\overline{11}$. So the sum $\overline{5} + \overline{11}$ is just the sum $\overline{1} + \overline{3}$ in disguise.
- But that means the result should come out the same, namely, $\overline{0}$. Does it?

Arithmetic With Residue Classes, III

Let's continue with $m = 4$ and residue classes $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$.

- We just decided that $\overline{1} + \overline{3} = \overline{0}$.
- Okay, now: what is $\overline{5} + \overline{11}$? (Remember, these are perfectly good residue classes modulo 4!)
- The definition says the sum should be $\overline{16}$.
- But wait: $\overline{5}$ is equal to $\overline{1}$, and $\overline{3}$ is equal to $\overline{11}$. So the sum $\overline{5} + \overline{11}$ is just the sum $\overline{1} + \overline{3}$ in disguise.
- But that means the result should come out the same, namely, $\overline{0}$. Does it?
- Yes, luckily for us, $\overline{16}$ is also just another name for $\overline{0}$, so everything is still okay.

Arithmetic With Residue Classes, IV

To illustrate, compare to what happens if we just take some random sets of integers, instead of residue classes.

- Suppose for example we have sets
  $A = \{\dots, 1, 3, 5, 6, 9, \dots\}$
  $B = \{\dots, 0, 4, 7, 10, 12, \dots\}$
  $C = \{\dots, 2, 8, 11, 13, \dots\}$
  and we define $\overline{a}$ to be the set (A, B, or C) that a is an element of. Then for example $\overline{1} = A$ while $\overline{2} = C$.

Now suppose we try to "define" $\overline{a} + \overline{b} = \overline{a + b}$.

Arithmetic With Residue Classes, IV

To illustrate, compare to what happens if we just take some random sets of integers, instead of residue classes.

- Suppose for example we have sets
  $A = \{\ldots, 1, 3, 5, 6, 9, \ldots\}$
  $B = \{\ldots, 0, 4, 7, 10, 12, \ldots\}$
  $C = \{\ldots, 2, 8, 11, 13, \ldots\}$
  and we define $\overline{a}$ to be the set (A, B, or C) that a is an element of. Then for example $\overline{1} = A$ while $\overline{2} = C$.

Now suppose we try to "define" $\overline{a} + \overline{b} = \overline{a+b}$.

- For example, we would have $\overline{1} + \overline{3} = \overline{4}$, and also $\overline{1} + \overline{5} = \overline{6}$.
- But in terms of the sets, these are contradictory statements, since they say $A + A = B$ and $A + A = A$ respectively.
- This is very bad, because it means the operations don't make any sense!

Arithmetic With Residue Classes, V

Luckily for us, we will never run into this problem using the addition and multiplication operations on residue classes. But we need to *justify* that fact!

- We need to show that our addition and multiplication operations on residue classes are "well defined": that the definitions make sense and are unambiguous.
- Otherwise, we haven't given a valid definition.

The potential ambiguity in our definition comes from the fact that each residue class has many different names: we need to show that no matter which name we use, the result comes out the same.

Arithmetic With Residue Classes, VI

The key properties that make everything work are that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

- Why? Imagine we want to compute $\overline{a} + \overline{c}$ modulo m.
- No matter which element b in the residue class of a and which element d in the residue class of c we take, the properties above dictate that the sum $b + d$ will lie in the same residue class as $a + c$, and the product bd will lie in the same residue class as ac.
- So we never have to worry about an "inconsistency".

Let's formalize all of this.

Arithmetic With Residue Classes, VII

Proposition (Modular Arithmetic, Part 1)

Let m be a modulus. Then the addition and multiplication operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ are well defined on the set $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m.

Arithmetic With Residue Classes, VII

Proposition (Modular Arithmetic, Part 1)

Let m be a modulus. Then the addition and multiplication operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ are well defined on the set $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m.

Proof:

- First, consider the task of computing $\overline{a} + \overline{c}$.
- If $\overline{b} = \overline{a}$ and $\overline{d} = \overline{c}$, then we need to verify $\overline{b} + \overline{d}$ has the same definition as $\overline{a} + \overline{c}$.

Arithmetic With Residue Classes, VII

Proposition (Modular Arithmetic, Part 1)

Let m be a modulus. Then the addition and multiplication operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ are well defined on the set $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m.

Proof:

- First, consider the task of computing $\overline{a} + \overline{c}$.
- If $\overline{b} = \overline{a}$ and $\overline{d} = \overline{c}$, then we need to verify $\overline{b} + \overline{d}$ has the same definition as $\overline{a} + \overline{c}$.
- By our properties, these say $a \equiv b$ and $c \equiv d \pmod{m}$ which imply $a + c \equiv b + d \pmod{m}$, hence $\overline{a+c} = \overline{b+d}$.
- But since $\overline{a} + \overline{c} = \overline{a+c}$ and $\overline{b} + \overline{d} = \overline{b+d}$, the results agree!
- So addition is well defined. The same argument works for multiplication.

Now we can actually do arithmetic with residue classes!

Modular Arithmetic – I

Let's do a few examples of calculations modulo 6. Our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

- What is $\overline{2} + \overline{3}$?

Modular Arithmetic – I

Let's do a few examples of calculations modulo 6. Our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

- What is $\overline{2} + \overline{3}$? Just add: it's $\overline{5}$.
- What is $\overline{2} + \overline{4}$?

Modular Arithmetic – I

Let's do a few examples of calculations modulo 6. Our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

- What is $\overline{2} + \overline{3}$? Just add: it's $\overline{5}$.
- What is $\overline{2} + \overline{4}$? Adding gives $\overline{2} + \overline{4} = \overline{6}$. And remember, $\overline{6} = \overline{0}$.
- So we have $\overline{2} + \overline{4} = \overline{0}$.
- What is $\overline{2} \cdot \overline{2}$?

Modular Arithmetic – I

Let's do a few examples of calculations modulo 6. Our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

- What is $\overline{2}+\overline{3}$? Just add: it's $\overline{5}$.
- What is $\overline{2}+\overline{4}$? Adding gives $\overline{2}+\overline{4}=\overline{6}$. And remember, $\overline{6}=\overline{0}$.
- So we have $\overline{2}+\overline{4}=\overline{0}$.
- What is $\overline{2}\cdot\overline{2}$? Just multiply: it's $\overline{4}$.
- What is $\overline{4}\cdot\overline{5}$?

Modular Arithmetic – I

Let's do a few examples of calculations modulo 6. Our residue classes are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

- What is $\overline{2}+\overline{3}$? Just add: it's $\overline{5}$.
- What is $\overline{2}+\overline{4}$? Adding gives $\overline{2}+\overline{4}=\overline{6}$. And remember, $\overline{6}=\overline{0}$.
- So we have $\overline{2}+\overline{4}=\overline{0}$.
- What is $\overline{2}\cdot\overline{2}$? Just multiply: it's $\overline{4}$.
- What is $\overline{4}\cdot\overline{5}$? Multiplying gives $\overline{4}\cdot\overline{5}=\overline{20}$, and remember, $\overline{20}=\overline{2}$, because 2 is the remainder when we divide 20 by 6.
- So we have $\overline{4}\cdot\overline{5}=\overline{2}$.

In fact, because there are only six different residue classes to add and multiply, we can just write out the entire addition and multiplication tables modulo 6.

Modular Arithmetic — II

Here's the addition table modulo 6:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Modular Arithmetic — III

Here's the multiplication table modulo 6:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Modular Arithmetic —— IV

Here are the two tables modulo 5:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Modular Arithmetic —— V

In general, how can we fill in these tables efficiently? (Imagine that you had some homework problems asking you to fill in these kinds of tables....)

- The idea is just to replace the result of each calculation with its remainder when we divide by m. (We usually call that "reducing modulo m".)
- The reason this works is because if $a = qm + r$ then $a \equiv r \pmod{m}$ and therefore $\overline{a} = \overline{r}$.
- So, for example, to find $\overline{7} \cdot \overline{11} \pmod{20}$, we compute $7 \cdot 11 = 77$ and then reduce modulo 20: since $77 = 3 \cdot 20 + 17$, the remainder is 17, so $\overline{7} \cdot \overline{11} = \overline{77} = \overline{17}$.

Modular Arithmetic ——— VI

In fact, arithmetic modulo m is commonly described by ignoring residue classes entirely and only working with the integers 0 through $m-1$, with the result of every computation "reduced modulo m" to obtain a result lying in this range.

- So why don't we just do it that way? Many reasons.

Modular Arithmetic —— VI

In fact, arithmetic modulo m is commonly described by ignoring residue classes entirely and only working with the integers 0 through $m-1$, with the result of every computation "reduced modulo m" to obtain a result lying in this range.

- So why don't we just do it that way? Many reasons.
- First, it's cumbersome and inelegant.
- Second, many basic properties of arithmetic are no longer true, or (at least) have to be modified substantially.
- Third, this approach doesn't generalize very well to other settings of interest. And so, once you enter those settings, you have to redo everything again (properly) with residue classes.
- And finally, residue classes extend quite well to more general settings where we may not have such an obvious set of "representatives" for the classes like $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.

Modular Arithmetic ——— VII

In many programming languages "a mod m", frequently denoted "$a\%m$", is defined to be a *function* returning the corresponding remainder in the interval $[0, m-1]$.

- With this definition, it is *not* true that $(a+b)\%m = (a\%m) + (b\%m)$, nor is it true that $ab\%m = (a\%m) \cdot (b\%m)$.

Modular Arithmetic ——— VII

In many programming languages "a mod m", frequently denoted "$a\%m$", is defined to be a *function* returning the corresponding remainder in the interval $[0, m-1]$.

- With this definition, it is *not* true that $(a+b)\%m = (a\%m) + (b\%m)$, nor is it true that $ab\%m = (a\%m) \cdot (b\%m)$.
- The reason is that because the sum and product may each exceed m, we may have to reduce again at the end.
- To obtain actually true statements, one needs to write something like $ab\%m = [(a\%m) \cdot (b\%m)]\%m$. (Ugh.)

That's why the best viewpoint is to work with residue classes: then the statement $\overline{a} \cdot \overline{b} = \overline{ab}$ is perfectly acceptable.

- It is also good to get used to thinking about equalities of residue classes directly, rather than falling back to the idea of reducing all terms to their residues $\{0, 1, \ldots, m-1\}$.

$\mathbb{Z}/m\mathbb{Z}$ Is A Ring, I

These addition and multiplication operations make $\mathbb{Z}/m\mathbb{Z}$ into a commutative ring with 1:

Proposition (Modular Arithmetic, Part 2)

For any modulus m and any residue classes $\overline{a}$, $\overline{b}$, $\overline{c}$, we have

[R1] $+$ is associative: $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

[R2] $+$ is commutative: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

[R3] $\overline{0}$ is an additive identity: $\overline{a} + \overline{0} = \overline{a}$.

[R4] $\overline{a}$ has an additive inverse $-\overline{a}$ with $\overline{a} + (-\overline{a}) = \overline{0}$.

[R5] $\cdot$ is associative: $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

[R6] $\cdot$ is commutative: $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.

[R7] $\cdot$ distributes over $+$: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

[R8] $\overline{1}$ is a multiplicative identity: $\overline{1} \cdot \overline{a} = \overline{a}$.

$\mathbb{Z}/m\mathbb{Z}$ Is A Ring, II

The proofs are all very similar so I'll just do [R1].

[R1] $+$ is associative: $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

$\mathbb{Z}/m\mathbb{Z}$ Is A Ring, II

The proofs are all very similar so I'll just do [R1].

[R1] $+$ is associative: $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

Proof:

- By definition of residue class addition, we have $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b + c} = \overline{a + (b + c)}$ and also $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c}$.

$\mathbb{Z}/m\mathbb{Z}$ Is A Ring, II

The proofs are all very similar so I'll just do [R1].

[R1] $+$ is associative: $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

Proof:

- By definition of residue class addition, we have $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b + c} = \overline{a + (b + c)}$ and also $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c}$.
- But $a + (b + c) = (a + b) + c$ by the associative property [I1] of the integers.
- Thus, the associated residue classes $\overline{a + (b + c)}$ and $\overline{(a + b) + c}$ are also equal.

The other properties [R2]-[R8] follow in a very similar way from the analogous properties [I2]-[I8] of the integers.

Units in $\mathbb{Z}/m\mathbb{Z}$, I

Last lecture we also introduced the notion of a unit in a commutative ring with 1, which is simply an element r with a multiplicative inverse r^{-1}, where $r \cdot r^{-1} = 1 = r^{-1} \cdot r$. Naturally, some residue classes are units.

- Example: With modulus $m = 10$, observe that $\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$, so $\overline{3}$ and $\overline{7}$ are multiplicative inverses modulo 10.

Units in $\mathbb{Z}/m\mathbb{Z}$, I

Last lecture we also introduced the notion of a unit in a commutative ring with 1, which is simply an element r with a multiplicative inverse r^{-1}, where $r \cdot r^{-1} = 1 = r^{-1} \cdot r$. Naturally, some residue classes are units.

- Example: With modulus $m = 10$, observe that $\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$, so $\overline{3}$ and $\overline{7}$ are multiplicative inverses modulo 10.

- Example: With modulus $m = 9$, observe that $\overline{2} \cdot \overline{5} = \overline{10} = \overline{1}$, so $\overline{2}$ and $\overline{5}$ are multiplicative inverses modulo 9.

Units in $\mathbb{Z}/m\mathbb{Z}$, I

Last lecture we also introduced the notion of a unit in a commutative ring with 1, which is simply an element r with a multiplicative inverse r^{-1}, where $r \cdot r^{-1} = 1 = r^{-1} \cdot r$. Naturally, some residue classes are units.

- Example: With modulus $m = 10$, observe that $\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$, so $\overline{3}$ and $\overline{7}$ are multiplicative inverses modulo 10.

- Example: With modulus $m = 9$, observe that $\overline{2} \cdot \overline{5} = \overline{10} = \overline{1}$, so $\overline{2}$ and $\overline{5}$ are multiplicative inverses modulo 9.

We can identify the invertible residue classes modulo m using the multiplication table: simply check the row for $\overline{a}$ to see if it has an entry $\overline{1}$ in it. If it does, then the corresponding column label is the inverse $\overline{a}^{-1}$, since $\overline{a}^{-1} \cdot \overline{a} = \overline{1}$.

Units in $\mathbb{Z}/m\mathbb{Z}$, II

Which residue classes are units modulo 6, and what are their inverses?

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Units in $\mathbb{Z}/m\mathbb{Z}$, II

Which residue classes are units modulo 6, and what are their inverses?

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

We can see that only $\overline{1}$ and $\overline{5}$ are invertible, and each one is its own inverse: $\overline{1} \cdot \overline{1} = \overline{1}$ and $\overline{5} \cdot \overline{5} = \overline{1}$.

Units in $\mathbb{Z}/m\mathbb{Z}$, III

Which residue classes are units modulo 5, and what are their inverses?

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Units in $\mathbb{Z}/m\mathbb{Z}$, III

Which residue classes are units modulo 5, and what are their inverses?

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

We can see that all of $\overline{1}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$ are invertible: specifically, $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{2} \cdot \overline{3} = \overline{1}$, and $\overline{4} \cdot \overline{4} = \overline{1}$.

So $\overline{1}$ and $\overline{4}$ are their own inverses, while $\overline{2}$ and $\overline{3}$ are each other's inverses.

Units in $\mathbb{Z}/m\mathbb{Z}$, IV

Here's a table of some more invertible residue classes and their inverses for small moduli m:

Modulus	Invertible residue classes, and their inverses
$m = 2$	$\overline{1}^{-1} = \overline{1}$
$m = 3$	$\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{2}$
$m = 4$	$\overline{1}^{-1} = \overline{1}$, $\overline{3}^{-1} = \overline{3}$
$m = 5$	$\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$
$m = 6$	$\overline{1}^{-1} = \overline{1}$, $\overline{5}^{-1} = \overline{5}$
$m = 9$	$\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{5}$, $\overline{4}^{-1} = \overline{7}$, $\overline{5}^{-1} = \overline{2}$, $\overline{7}^{-1} = \overline{4}$, $\overline{8}^{-1} = \overline{8}$
$m = 10$	$\overline{1}^{-1} = \overline{1}$, $\overline{3}^{-1} = \overline{7}$, $\overline{7}^{-1} = \overline{3}$, $\overline{9}^{-1} = \overline{9}$

(7, 8 are skipped because they're on the HW.) See any patterns?

Units in $\mathbb{Z}/m\mathbb{Z}$, V

Here's a table of the invertible and non-invertible residue classes for small moduli m:

Modulus	Invertible	Non-Invertible
$m = 2$	$\overline{1}$	$\overline{0}$
$m = 3$	$\overline{1}, \overline{2}$	$\overline{0}$
$m = 4$	$\overline{1}, \overline{3}$	$\overline{0}, \overline{2}$
$m = 5$	$\overline{1}, \overline{2}, \overline{3}, \overline{4}$	$\overline{0}$
$m = 6$	$\overline{1}, \overline{5}$	$\overline{0}, \overline{2}, \overline{3}, \overline{4}$
$m = 9$	$\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$	$\overline{0}, \overline{3}, \overline{6}$
$m = 10$	$\overline{1}, \overline{3}, \overline{7}, \overline{9}$	$\overline{0}, \overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}$

Can you identify a rule for when a residue class is invertible?

Units in $\mathbb{Z}/m\mathbb{Z}$, V

Here's a table of the invertible and non-invertible residue classes for small moduli m:

Modulus	Invertible	Non-Invertible
$m = 2$	$\overline{1}$	$\overline{0}$
$m = 3$	$\overline{1}$, $\overline{2}$	$\overline{0}$
$m = 4$	$\overline{1}$, $\overline{3}$	$\overline{0}$, $\overline{2}$
$m = 5$	$\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$	$\overline{0}$
$m = 6$	$\overline{1}$, $\overline{5}$	$\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{4}$
$m = 9$	$\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$, $\overline{8}$	$\overline{0}$, $\overline{3}$, $\overline{6}$
$m = 10$	$\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$	$\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{8}$

Can you identify a rule for when a residue class is invertible?
It seems like the invertible residue classes are the ones relatively prime to the modulus.

Units in $\mathbb{Z}/m\mathbb{Z}$, VI

In fact, this is true:

Proposition (Invertible Elements Modulo m)

If m is a modulus, then the residue class $\overline{a}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$, meaning that there exists some residue class $\overline{x}$ with $\overline{x} \cdot \overline{a} = \overline{1}$, if and only if a and m are relatively prime.

We will prove this result next time.

Units in $\mathbb{Z}/m\mathbb{Z}$, VI

In fact, this is true:

Proposition (Invertible Elements Modulo m)

If m is a modulus, then the residue class $\overline{a}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$, meaning that there exists some residue class $\overline{x}$ with $\overline{x} \cdot \overline{a} = \overline{1}$, if and only if a and m are relatively prime.

We will prove this result next time. But here is a nice corollary:

Corollary

The ring $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number.

Proof (of corollary): By definition, $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if every nonzero residue class is a unit. By the proposition, that occurs if and only if each of $1, 2, \ldots, p-1$ are relatively prime to p. But this is readily seen to be equivalent to saying p is prime.

Summary

We described the addition and multiplication operations on residue classes, and showed that they are well defined.

We discussed the ring structure of $\mathbb{Z}/m\mathbb{Z}$.

We discussed units in $\mathbb{Z}/m\mathbb{Z}$.

Next lecture: More units, zero divisors, and powers in $\mathbb{Z}/m\mathbb{Z}$.