Math 1365 (Intensive Mathematical Reasoning)

Lecture #14 of 35 $\sim$ October 11, 2023

Modular Congruences + Residue Classes

- Congruences Modulo m
- Residue Classes

This material represents §2.5.1-§2.5.2 from the course notes.

Note: Midterm 1 covers up through §2.4, meaning that today's material will NOT appear on Midterm 1.

Modular Congruences Intro, I

In various situations, we naturally group together certain kinds of integers in ways that respect laws of arithmetic.

- For example, if we group the integers together into "even" and "odd", then as you worked out carefully on the homework,

$$\begin{aligned} \text{even} + \text{even} &= \text{even} \\ \text{even} + \text{odd} &= \text{odd} \\ \text{odd} + \text{even} &= \text{odd} \\ \text{odd} + \text{odd} &= \text{even} \end{aligned}$$

Modular Congruences Intro, I

In various situations, we naturally group together certain kinds of integers in ways that respect laws of arithmetic.

- For example, if we group the integers together into "even" and "odd", then as you worked out carefully on the homework,

$$\begin{aligned} \text{even} + \text{even} &= \text{even} \\ \text{even} + \text{odd} &= \text{odd} \\ \text{odd} + \text{even} &= \text{odd} \\ \text{odd} + \text{odd} &= \text{even} \end{aligned}$$

- These rules are true regardless of which specific even and odd numbers we add together.
- We have a similar phenomenon with multiplication (odd times odd is odd, and even times anything is even).

Modular Congruences Intro, II

As another example, consider the fact that 9 hours after 4 o'clock, it is 1 o'clock, despite the fact that $9 + 4 = 13$, not 1.

Modular Congruences Intro, II

As another example, consider the fact that 9 hours after 4 o'clock, it is 1 o'clock, despite the fact that $9 + 4 = 13$, not 1.

- Similarly, 6 hours after 11 o'clock, it is 5 o'clock, even though $6 + 11 = 17$ rather than 5.
- The point is that in general, we identify times that are 12 hours apart and view them as equivalent, at least as far as the clock is concerned.
- In fact, this is exactly the same thing we do when we condense integers down to "even" and "odd", except with even and odd we identify integers that differ by a multiple of 2, rather than identifying times that differ by a multiple of 12 hours.

Let's formalize this idea.

Modular Congruences, I

Let's formalize this idea:

Definition

If m is a positive integer and m divides $b-a$, we say that a and b are <u>congruent modulo</u> <u>m</u> (or <u>equivalent modulo</u> <u>m</u>), and write "$a \equiv b$ (modulo m)".

The statement $a \equiv b \pmod{m}$ can be thought of as saying "a and b are equal, up to adding or subtracting a multiple of m".

- <u>Notation</u>: As shorthand we usually write "$a \equiv b \pmod{m}$", or even just "$a \equiv b$" when the modulus m is clear from the context.
- Observe that if $m|(b-a)$, then $(-m)|(b-a)$ as well, so we do not lose anything by assuming that the modulus m is positive.

Modular Congruences, II

<u>Examples</u>: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m | (b - a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.
4. We have $-3 \equiv 3 \pmod{6}$, as 6 divides $3 - (-3) = 6$.

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m | (b - a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.
4. We have $-3 \equiv 3 \pmod{6}$, as 6 divides $3 - (-3) = 6$.
5. We have $2 \not\equiv 7 \pmod{3}$, as 3 does not divide $7 - 2 = 5$.

More Examples:

1. Is $4 \equiv 19 \pmod{5}$?

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.
4. We have $-3 \equiv 3 \pmod{6}$, as 6 divides $3 - (-3) = 6$.
5. We have $2 \not\equiv 7 \pmod{3}$, as 3 does not divide $7 - 2 = 5$.

More Examples:

1. Is $4 \equiv 19 \pmod{5}$? Yes, since $5|(19-4)$.
2. Is $0 \equiv 30 \pmod{6}$?

Modular Congruences, II

<u>Examples</u>: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.
4. We have $-3 \equiv 3 \pmod{6}$, as 6 divides $3 - (-3) = 6$.
5. We have $2 \not\equiv 7 \pmod{3}$, as 3 does not divide $7 - 2 = 5$.

<u>More Examples</u>:

1. Is $4 \equiv 19 \pmod{5}$? Yes, since $5|(19 - 4)$.
2. Is $0 \equiv 30 \pmod{6}$? Yes, since $6|(30 - 0)$.
3. Is $0 \equiv 30 \pmod{7}$?

Modular Congruences, II

Examples: Remember $a \equiv b \pmod{m}$ means $m|(b-a)$.

1. We have $3 \equiv 9 \pmod{6}$, as 6 divides $9 - 3 = 6$.
2. We have $-2 \equiv 28 \pmod{5}$, as 5 divides $28 - (-2) = 30$.
3. We have $0 \equiv -666 \pmod{3}$, as 3 divides $-666 - 0 = -666$.
4. We have $-3 \equiv 3 \pmod{6}$, as 6 divides $3 - (-3) = 6$.
5. We have $2 \not\equiv 7 \pmod{3}$, as 3 does not divide $7 - 2 = 5$.

More Examples:

1. Is $4 \equiv 19 \pmod{5}$? Yes, since $5|(19-4)$.
2. Is $0 \equiv 30 \pmod{6}$? Yes, since $6|(30-0)$.
3. Is $0 \equiv 30 \pmod{7}$? No, since $7 \nmid (30-0)$.

Modular Congruences, III

Modular congruences share a number of properties with equalities:

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* $ac \equiv bd \pmod{m}$.
6. *If* $a \equiv b \pmod{m}$, *then* $ac \equiv bc \pmod{mc}$ *for any* $c > 0$.
7. *If* $d|m$, *then* $a \equiv b \pmod{m}$ *implies* $a \equiv b \pmod{d}$.

Modular Congruences, IV

1. $a \equiv a \pmod{m}$.

Proof:

Modular Congruences, IV

1. $a \equiv a \pmod{m}$.

Proof:

- By definition, $a \equiv a \pmod{m}$ is equivalent to $m | (a - a)$.
- But this just says $m | 0$, and that is true! (Because $0 = 0 \cdot m$.)

---

2. $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.

Proof:

Modular Congruences, IV

1. $a \equiv a \pmod{m}$.

Proof:

- By definition, $a \equiv a \pmod{m}$ is equivalent to $m|(a-a)$.
- But this just says $m|0$, and that is true! (Because $0 = 0 \cdot m$.)

---

2. $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.

Proof:

- First suppose $a \equiv b \pmod{m}$.
- Then $m|(b-a)$, so $b - a = km$ for some k.
- Then $a - b = (-k)m$, so $m|(a-b)$, meaning $b \equiv a \pmod{m}$.
- The converse follows in the same way.

Modular Congruences, V

3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof:

Modular Congruences, V

3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof:

- Suppose $a \equiv b$ and $b \equiv c \pmod{m}$.
- Then $m|(b-a)$ and $m|(c-b)$.
- Then m also divides the sum $(c-b)+(b-a)=c-a$.
- But that means $a \equiv c \pmod{m}$, as required.

---

4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.

Proof:

Modular Congruences, V

3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof:

- Suppose $a \equiv b$ and $b \equiv c \pmod{m}$.
- Then $m|(b-a)$ and $m|(c-b)$.
- Then m also divides the sum $(c-b)+(b-a) = c-a$.
- But that means $a \equiv c \pmod{m}$, as required.

---

4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.

Proof:

- Suppose $a \equiv b$ and $c \equiv d \pmod{m}$.
- Then $m|(b-a)$ and $m|(d-c)$.
- Then m also divides $(d-c)+(b-a) = (b+d)-(a+c)$.
- But that means $a+c \equiv b+d \pmod{m}$, as required.

Modular Congruences, VI

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Modular Congruences, VI

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

- Suppose $a \equiv b$ and $c \equiv d \pmod{m}$.
- Then $m|(b-a)$ and $m|(d-c)$.
- Then m also divides $d(b-a)$ and $a(d-c)$ and thus also divides their sum, $d(b-a)+a(d-c) = (bd-ad)+(ad-ac) = bd-ac$. But that means $ac \equiv bd \pmod{m}$, as required.

Modular Congruences, VI

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

- Suppose $a \equiv b$ and $c \equiv d \pmod{m}$.
- Then $m|(b-a)$ and $m|(d-c)$.
- Then m also divides $d(b-a)$ and $a(d-c)$ and thus also divides their sum, $d(b-a)+a(d-c)=(bd-ad)+(ad-ac)=bd-ac$. But that means $ac \equiv bd \pmod{m}$, as required.

---

6. If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.
7. If $d|m$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.

Proofs: Homework 6. (Due a week after the midterm.)

Modular Congruences, VII

Let me draw your attention in particular to the first five of these properties, where the modulus is m in all situations:

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

Modular Congruences, VII

Let me draw your attention in particular to the first five of these properties, where the modulus is m in all situations:

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

Notice that these all become very familiar properties of equality if we replace the congruence sign $\equiv$ with an equals sign $=$.

- The point: these properties tell us that congruence mod m behaves a lot like a "weaker" version of equality.
- Also, congruence behaves well with respect to the arithmetic operations $+$ and $\cdot$.

Residue Classes, I

The motivation for talking about congruences is our observation from earlier that we can do arithmetic with the words "even" and "odd" that mirrors the arithmetic of the integers.

- Notice that the even integers are the integers congruent to 0 modulo 2, while the odd integers are the integers congruent to 1 modulo 2.
- In the same way, "1 o'clock" is shorthand for a set of times that includes 1, 13, 25, and in general, all the times congruent to 1 modulo 12.

So let's examine more generally the set consisting of all integers congruent to a particular integer a modulo m.

Residue Classes, II

Definition

If a is an integer, the residue class of a modulo m, denoted $\overline{a}$, is the collection of all integers congruent to a modulo m.

Remark: The residue class $\overline{a}$ depends on the modulus m. It is just an unfortunate aspect of the notation that m is not included, and needs to be known from context.

- Let's write out what the elements in the residue class $\overline{a}$ are.
- Since $a \equiv b \pmod{m}$ precisely when $m|(b-a)$ precisely when there exists an integer k with $b - a = km$, we see that $\overline{a} = \{a + km,\ k \in \mathbb{Z}\}$.
- More explicitly, $\overline{a} = \{\dots, a-3m, a-2m, a-m, a, a+m, a+2m, a+3m, \dots\}$.

Residue Classes, III

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

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

Residue Classes, III

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 $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.

Residue Classes, III

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 $\{\dots,\ -27,\ -8, 11,\ 30,\ 49,\ 68,\ ,\dots\}$.

Residue Classes, III

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.

Residue Classes, III

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.

Residue Classes, III

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.
- More generally, the residue class of 0 modulo m is the set $\{\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots\}$ of multiples of m.

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

- Here's one: $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

- Here's one: $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.
- Another: $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

- Here's one: $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.
- Another: $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.
- Another: $\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$.

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

- Here's one: $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.
- Another: $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.
- Another: $\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$.
- Another: $\overline{3} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.

Notice anything interesting here?

Residue Classes, IV

Let's examine residue classes modulo 3 more closely:

- Here's one: $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.
- Another: $\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.
- Another: $\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$.
- Another: $\overline{3} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$.

Notice anything interesting here?

- In fact, the residue class $\overline{3}$ is *exactly the same* as the residue class $\overline{0}$ modulo 3.
- Remember, the residue classes $\overline{0}$ and $\overline{3}$ are sets, and these two sets (as you can see) have exactly the same elements in them.

Residue Classes, V

So far we found 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, $\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$.

We saw that $\overline{3}$ turned out the same as $\overline{0}$. Can you identify any other residue classes modulo 3? Are they the same as the ones listed above, or can you find new ones?

Residue Classes, V

So far we found three different residue classes modulo 3:

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

We saw that $\overline{3}$ turned out the same as $\overline{0}$. Can you identify any other residue classes modulo 3? Are they the same as the ones listed above, or can you find new ones?

- Try $\overline{4} = \{\dots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \dots\} = \overline{1}$.
- Or $\overline{5} = \{\dots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \dots\} = \overline{2}$.
- How about $\overline{11} = \{\dots, -4, -1, 2, 5, 8, 11, 14, 17, 20, 23, \dots\}$? No, in fact, that's the same as $\overline{2}$.

Residue Classes, VI

If you tried to find some other residue classes modulo 3, you'll discover they just end up duplicating one of the three we already found: $\overline{0}$, $\overline{1}$, $\overline{2}$.

- So it seems that there are really only three different residue classes modulo 3, each of which has lots of different names. What pattern do the names have?
- For instance, $\overline{0}$ is the same as $\overline{3}$ and also the same as $\overline{6}$ and $\overline{-3}$ and ....

Residue Classes, VI

If you tried to find some other residue classes modulo 3, you'll discover they just end up duplicating one of the three we already found: $\overline{0}$, $\overline{1}$, $\overline{2}$.

- So it seems that there are really only three different residue classes modulo 3, each of which has lots of different names. What pattern do the names have?
- For instance, $\overline{0}$ is the same as $\overline{3}$ and also the same as $\overline{6}$ and $\overline{-3}$ and ....
- It seems pretty clear that when we write out $\overline{0} = \{\dots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \dots\}$, if we take the residue class of any element in $\overline{0}$ (e.g., -6), that residue class is just equal to $\overline{0}$ again (i.e., $\overline{-6} = \overline{0}$).

Residue Classes, VII

In fact, all of these observations hold in general:

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 $\overline{0}, \overline{1}, \dots, \overline{m-1}$.*

We will prove these properties next time.

Winding Down, I

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 on the previous slide, $\mathbb{Z}/m\mathbb{Z}$ contains exactly m elements: namely, $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.

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

Winding Down, II

We will continue our discussion of residue class arithmetic a week from today.

- Next class will be devoted to exam review. I will present the solutions to some of the problems on the review sheet, and also take requests for other problems that people would like to see the solutions to.
- Monday's class will be the midterm exam (it is still in person, in the regular classroom). Please try to arrive at least 5 minutes early to class so everyone can get settled and the exam can start promptly.

Summary

We introduced congruences modulo m and established some basic properties of congruences.

We defined residue classes modulo m and established some of their basic properties.

Next lecture: Review for midterm 1.