Math 1365 (Intensive Mathematical Reasoning)

Lecture #15 of 35 $\sim$ October 18, 2023

Residue Classes + Modular Arithmetic

- Properties of Residue Classes
- Modular Arithmetic

This material represents §2.5.2-§2.5.3 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 $\overline{a} = \{b \in \mathbb{Z} : a \equiv b (mod\ m)\}$ 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.

Residue classes can have many different names.

- For instance, the residue class
  $\overline{0} = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$
  is exactly the same set as the residue class
  $\overline{m} = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$.

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

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. How do we prove an equality of sets?

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. How do we prove an equality of sets?
- We need to show each set is a subset of the other. So in fact we have a few things to do here.

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

- So, suppose $a \equiv b \pmod{m}$. Let's first show that $\overline{a} \subseteq \overline{b}$.
- So suppose $x \in \overline{a}$. [Goal: show that $x \in \overline{b}$.]

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

- So, suppose $a \equiv b \pmod{m}$. Let's first show that $\overline{a} \subseteq \overline{b}$.
- So suppose $x \in \overline{a}$. [Goal: show that $x \in \overline{b}$.]
- Now, $x \in \overline{a}$ says that $x \equiv a \pmod{m}$.
- 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: [To show] If $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$.

- So, suppose $a \equiv b \pmod{m}$. Let's first show that $\overline{a} \subseteq \overline{b}$.
- So suppose $x \in \overline{a}$. [Goal: show that $x \in \overline{b}$.]
- Now, $x \in \overline{a}$ says that $x \equiv a \pmod{m}$.
- 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 $\overline{a} = \overline{b}$.

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

- 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: If $\overline{a} = \overline{b}$ then $a \equiv b \pmod{m}$.

- 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.

Let's strategize first.

- Explicit statement: if $\overline{a}$ and $\overline{b}$ are two residue classes modulo m, then either $\overline{a} \cap \overline{b}$ is empty, or $\overline{a} = \overline{b}$.
- How can we prove this?

Properties of Residue Classes! V

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

Let's strategize first.

- Explicit statement: if $\overline{a}$ and $\overline{b}$ are two residue classes modulo m, then either $\overline{a} \cap \overline{b}$ is empty, or $\overline{a} = \overline{b}$.
- How can we prove this?
- Well, if $\overline{a} \cap \overline{b}$ is empty then we are immediately done.
- So, we only need to worry about the case where $\overline{a} \cap \overline{b}$ is nonempty: we would need to show that $\overline{a} = \overline{b}$ in that situation.
- So to prove the desired statement, we could show that if $\overline{a} \cap \overline{b}$ is nonempty, then $\overline{a} = \overline{b}$.
- Finally, how could we show that $\overline{a} = \overline{b}$?

Properties of Residue Classes! V

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

Let's strategize first.

- Explicit statement: if $\overline{a}$ and $\overline{b}$ are two residue classes modulo m, then either $\overline{a} \cap \overline{b}$ is empty, or $\overline{a} = \overline{b}$.
- How can we prove this?
- Well, if $\overline{a} \cap \overline{b}$ is empty then we are immediately done.
- So, we only need to worry about the case where $\overline{a} \cap \overline{b}$ is nonempty: we would need to show that $\overline{a} = \overline{b}$ in that situation.
- So to prove the desired statement, we could show that if $\overline{a} \cap \overline{b}$ is nonempty, then $\overline{a} = \overline{b}$.
- Finally, how could we show that $\overline{a} = \overline{b}$? Look back at what we just proved: $\overline{a} = \overline{b}$ is equivalent to $a \equiv b \pmod{m}$.

Properties of Residue Classes? VI

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

Proof:

- Suppose that $\overline{a}$ and $\overline{b}$ are two 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? VI

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

Proof:

- Suppose that $\overline{a}$ and $\overline{b}$ are two 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 $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{m-1}$.

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

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 $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$, 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, $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{m-1}$.

[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.

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 me illustrate with an example. Let's 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 me illustrate with an example. Let's 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 me illustrate with an example. Let's 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 a minute: $\overline{5}$ 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 a minute: $\overline{5}$ 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
  $A = \{\ldots, 1, 3, 5, 6, 9, \ldots\}$
  $B = \{\ldots, 0, 4, 7, 10, 12, \ldots\}$
  $C = \{\ldots, 2, 8, 11, 13, \ldots\}$
  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" $\overline{a} + \overline{b} = \overline{a + b}$.

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!

- What we need to show is that our addition and multiplication operations on residue classes are what we call "well defined": that the definitions make sense and are unambiguous.
- Otherwise, we haven't given a valid definition. (Why not? Because mathematical statements must be propositions that have an unambiguous truth value.)

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 are these properties important?
- 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, $\overline{20} = \overline{4}$, because 4 is the remainder when we divide 20 by 6.
- So we have $\overline{4} \cdot \overline{5} = \overline{4}$.

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 $\{0, 1, \ldots, m-1\}$.

Properties of Modular Arithmetic, I

Most laws of arithmetic in $\mathbb{Z}$ extend to $\mathbb{Z}/m\mathbb{Z}$:

Proposition (Modular Arithmetic, Part 2)

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

1. *$+$ is associative:* $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.
2. *$+$ is commutative:* $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.
3. *$\overline{0}$ is an additive identity:* $\overline{a} + \overline{0} = \overline{a}$.
4. *$\overline{a}$ has an additive inverse $-\overline{a}$ with* $\overline{a} + (-\overline{a}) = \overline{0}$.
5. *$\cdot$ is associative:* $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.
6. *$\cdot$ is commutative:* $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.
7. *$\cdot$ distributes over $+$:* $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.
8. *$\overline{1}$ is a multiplicative identity:* $\overline{1} \cdot \overline{a} = \overline{a}$.

Properties of Modular Arithmetic, II

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

Properties of Modular Arithmetic, II

1. $+$ 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 $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c}$.

Properties of Modular Arithmetic, II

1. $+$ 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 (2)-(8) follow in a very similar way from the analogous properties [I2]-[I8] of the integers. (You get to do some of them yourself on Homework 6!)

Summary

We established some properties of residue classes modulo m.

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

We worked through some examples of residue class arithmetic.

Next lecture: Properties of modular arithmetic, inverses.