Math 1365 (Intensive Mathematical Reasoning)

Lecture #17 of 35 $\sim$ October 19, 2023

Modular Arithmetic + Modular Inverses

- Modular Cancellation
- Modular Inverses

This material represents §2.5.2 from the course notes.

Recall, I

Recall that we proved some properties of residue classes yesterday:

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.

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

Recall, II

We also constructed addition and multiplication operations on residue classes, and showed they were well defined and obey most of the familiar laws of arithmetic:

Definition

Let m be a modulus and $\mathbb{Z}/m\mathbb{Z}$ be the collection of residue classes modulo m. Then we have well-defined addition and multiplication operations on $\mathbb{Z}/m\mathbb{Z}$, defined as $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ respectively.

These operations possess various properties of arithmetic: specifically, $+$ and $\cdot$ are associative and commutative, the element $\overline{0}$ is an additive identity and $\overline{1}$ is a multiplicative identity, every residue class $\overline{a}$ has an additive inverse $\overline{-a}$, and $+$ distributes over $\cdot$.

Cancellation Mod m, I

As we just saw, the arithmetic in $\mathbb{Z}/m\mathbb{Z}$ shares many properties with the arithmetic in $\mathbb{Z}$. However, there are some very important differences.

- For example, if a, b, c are integers with $ab = ac$ and $a \neq 0$, then we can "cancel" a from both sides to conclude that $b = c$.

Cancellation Mod m, I

As we just saw, the arithmetic in $\mathbb{Z}/m\mathbb{Z}$ shares many properties with the arithmetic in $\mathbb{Z}$. However, there are some very important differences.

- For example, if a, b, c are integers with $ab = ac$ and $a \neq 0$, then we can "cancel" a from both sides to conclude that $b = c$.
- However, this does not always work in $\mathbb{Z}/m\mathbb{Z}$!
- For example, $\overline{2} \cdot \overline{1} = \overline{2} \cdot \overline{4}$ modulo 6, but $\overline{1} \neq \overline{4}$ modulo 6: we cannot cancel the factor $\overline{2}$.
- Likewise, $\overline{6} \cdot \overline{3} = \overline{6} \cdot \overline{6}$ modulo 9, but $\overline{3} \neq \overline{6}$ modulo 9.

Cancellation Mod m, II

Why does cancellation work in $\mathbb{Z}$ but not in $\mathbb{Z}/m\mathbb{Z}$?

- First let's examine why cancellation *does* work for integers (i.e., why $ab = ac$ and $a \neq 0$ imply $b = c$).

Cancellation Mod m, II

Why does cancellation work in $\mathbb{Z}$ but not in $\mathbb{Z}/m\mathbb{Z}$?

- First let's examine why cancellation *does* work for integers (i.e., why $ab = ac$ and $a \neq 0$ imply $b = c$).
- If $ab = ac$, then we can rearrange and factor using the distributive law to see that $a(b - c) = 0$.
- Then we use the property that if two integers have product 0, at least one of them must be zero: thus either $a = 0$ or $b - c = 0$. But since $a \neq 0$ that means $b - c = 0$, so $b = c$.

Now, which of these steps are still valid in $\mathbb{Z}/m\mathbb{Z}$?

Cancellation Mod m, II

Why does cancellation work in $\mathbb{Z}$ but not in $\mathbb{Z}/m\mathbb{Z}$?

- First let's examine why cancellation *does* work for integers (i.e., why $ab = ac$ and $a \neq 0$ imply $b = c$).
- If $ab = ac$, then we can rearrange and factor using the distributive law to see that $a(b - c) = 0$.
- Then we use the property that if two integers have product 0, at least one of them must be zero: thus either $a = 0$ or $b - c = 0$. But since $a \neq 0$ that means $b - c = 0$, so $b = c$.

Now, which of these steps are still valid in $\mathbb{Z}/m\mathbb{Z}$?

- If $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ then we can still rearrange and factor to see that $\overline{a}(\overline{b} - \overline{c}) = \overline{0}$.
- And the last step is also valid: if we knew $\overline{a} = \overline{0}$ or $\overline{b} - \overline{c} = \overline{0}$ then since $\overline{a} \neq \overline{0}$ that would say $\overline{b} - \overline{c} = \overline{0}$ and so $\overline{b} = \overline{c}$.
- But now, is it true that if two residue classes have product $\overline{0}$, then one or the other must be zero?

Cancellation Mod m, III

Is it true that if two residue classes have product $\overline{0}$, then one or the other must be zero? Let's look at multiplication modulo 4:

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

Can you identify any nonzero residue classes whose product is $\overline{0}$?

Cancellation Mod m, III

Is it true that if two residue classes have product $\overline{0}$, then one or the other must be zero? Let's look at multiplication modulo 4:

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

Can you identify any nonzero residue classes whose product is $\overline{0}$?
Yes: we can do $\overline{2} \cdot \overline{2} = \overline{0}$.

Cancellation Mod m, IV

How about modulo 6? Can you find two nonzero residue classes with product $\overline{0}$?

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

Cancellation Mod m, IV

How about modulo 6? Can you find two nonzero residue classes with product $\overline{0}$?

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

Sure: we have $\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{2} = \overline{0}$, and also $\overline{3} \cdot \overline{4} = \overline{4} \cdot \overline{3} = \overline{0}$.

Cancellation Mod m, V

How about modulo 5?

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

Cancellation Mod m, V

How about modulo 5?

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

Here there aren't any nonzero residue classes whose product is $\overline{0}$: the only way to get a product of $\overline{0}$ modulo 5 is to have at least one term be equal to $\overline{0}$.

Cancellation Mod m, VI

So it seems like for some moduli m, there exist nonzero residue classes whose product is $\overline{0}$ mod m, while for other m there are no such residue classes.

- Perhaps it might be the case that *some* residue classes $\overline{a}$ can be cancelled modulo m: in other words, have the property that $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ implies $\overline{b} = \overline{c}$.
- For instance, $\overline{a} = \overline{1}$ has this property (though it's rather trivial).
- Our question above then boils down to asking this: which residue classes are "cancellable"?

Cancellation and Inverses, I

Let's instead think about real numbers for a moment. If we had an equation of the form $ab = ac$ and $a \neq 0$, we could simply divide both sides by a to get $b = c$.

- What this actually means is to multiply both sides of $ab = ac$ by the multiplicative inverse a^{-1} of a: the number with $a^{-1} \cdot a = 1$.

Does the same thing work with residue classes?

Cancellation and Inverses, I

Let's instead think about real numbers for a moment. If we had an equation of the form $ab = ac$ and $a \neq 0$, we could simply divide both sides by a to get $b = c$.

- What this actually means is to multiply both sides of $ab = ac$ by the multiplicative inverse a^{-1} of a: the number with $a^{-1} \cdot a = 1$.

Does the same thing work with residue classes? First we need to define what it means to have a multiplicative inverse:

Definition

Let m be a modulus and $\overline{a}$ be a residue class modulo m. If the residue class $\overline{x}$ has the property that $\overline{x} \cdot \overline{a} = \overline{1}$, we say that $\overline{x}$ is a <u>multiplicative inverse</u> of $\overline{a}$, and we say $\overline{a}$ itself is <u>invertible</u>.

Cancellation and Inverses, II

Here are some examples of invertible residue classes:

- 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.

Cancellation and Inverses, II

Here are some examples of invertible residue classes:

- 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.

- 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.

Cancellation and Inverses, II

Here are some examples of invertible residue classes:

- 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.

- 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.

- With modulus $m = 31$, observe that $\overline{7} \cdot \overline{9} = \overline{63} = \overline{1}$ (since $63 - 1 = 62 = 2 \cdot 31$), so $\overline{7}$ and $\overline{9}$ are multiplicative inverses modulo 31.

Cancellation and Inverses, III

We claim that if $\overline{a}$ is invertible, then $\overline{a}$ has cancellation:

Proposition (Cancellation With Inverses)

Let m be a modulus and $\overline{a}$ be a residue class modulo m that has a multiplicative inverse $\overline{x}$ modulo m. Then $\overline{a}$ has multiplicative cancellation: if $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$, then $\overline{b} = \overline{c}$.

Cancellation and Inverses, III

We claim that if $\overline{a}$ is invertible, then $\overline{a}$ has cancellation:

Proposition (Cancellation With Inverses)

Let m be a modulus and $\overline{a}$ be a residue class modulo m that has a multiplicative inverse $\overline{x}$ modulo m. Then $\overline{a}$ has multiplicative cancellation: if $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$, then $\overline{b} = \overline{c}$.

Proof:

- Suppose $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$.
- Multiply both sides by $\overline{x}$ to obtain $\overline{x} \cdot \overline{a} \cdot \overline{b} = \overline{x} \cdot \overline{a} \cdot \overline{c}$.
- But since $\overline{x} \cdot \overline{a} = \overline{1}$, we can simplify each side of the equation to get $\overline{1} \cdot \overline{b} = \overline{1} \cdot \overline{c}$, hence $\overline{b} = \overline{c}$.

Cancellation and Inverses, IV

We can identify the invertible residue classes modulo m using the multiplication table.

- Specifically, to decide whether $\overline{a}$ is invertible, 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 $\overline{x}$, since $\overline{x} \cdot \overline{a} = \overline{1}$.
- Otherwise, if there is no $\overline{1}$, then $\overline{a}$ is not invertible modulo m.

Cancellation and Inverses, V

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

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

Cancellation and Inverses, V

Which residue classes are invertible 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 $\overline{5} \cdot \overline{5} = \overline{1}$.

Cancellation and Inverses, VI

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

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

Cancellation and Inverses, VI

Which residue classes are invertible 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.

Cancellation and Inverses, VII

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

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

Notice any patterns?

Cancellation and Inverses, VIII

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

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

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

Cancellation and Inverses, VIII

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

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

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, while the non-invertible residue classes have a gcd with the modulus that's bigger than 1.

Cancellation and Inverses, IX

In fact, this is true:

Proposition (Invertible Elements Modulo m)

If m is a modulus, then the residue class $\overline{a}$ has a multiplicative inverse 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.

Cancellation and Inverses, IX

In fact, this is true:

Proposition (Invertible Elements Modulo m)

If m is a modulus, then the residue class $\overline{a}$ has a multiplicative inverse 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.

To prove this result, we will need the characterization of when two integers are relatively prime that was proven a few weeks ago during our discussion of gcds:

- The integers a and m are relatively prime if and only if there exist integers x and y with $xa + yb = 1$.

Note also that the statement is an if-and-only-if, so we have two directions to show.

Cancellation and Inverses, X

1. If a and m are relatively prime, then $\overline{a}$ is invertible modulo m.

Proof:

Cancellation and Inverses, X

1. If a and m are relatively prime, then $\overline{a}$ is invertible modulo m.

<u>Proof</u>:

- First suppose that a and m are relatively prime.
- Then by our facts about gcds, there exist integers x and y such that $xa + ym = 1$.
- But since $1 - xa = ym$ we see that $m | (1 - xa)$ and therefore $xa \equiv 1 \pmod{m}$.
- But this in turn means that $\overline{x} \cdot \overline{a} = \overline{xa} = \overline{1}$. Therefore, $\overline{a}$ has a multiplicative inverse (namely, $\overline{x}$).

Cancellation and Inverses, XI

2. If $\overline{a}$ is invertible modulo m, then a and m are relatively prime.

Proof:

Cancellation and Inverses, XI

2. If $\overline{a}$ is invertible modulo m, then a and m are relatively prime.

Proof:

- Suppose that $\overline{a}$ is invertible modulo m: then there exists $\overline{x}$ such that $\overline{x} \cdot \overline{a} = \overline{1}$.
- Equivalently, that says $\overline{xa} = \overline{1}$, which is the same as saying $xa \equiv 1 \pmod{m}$.
- By definition of congruence, this says there exists an integer y such that $1 - xa = ym$, or equivalently, $xa + ym = 1$.
- But by our property of gcds again, this implies a and m are relatively prime, as claimed.

Notice in fact that this second part of the proof is pretty much exactly the same as the first part, just in reverse order. (If you like, you can work out how to rephrase the whole proof as a chain of equivalences.)

Cancellation and Inverses, XII

So, the result we just proved shows that $\overline{a}$ has a multiplicative inverse modulo m if and only if a is relatively prime to m.

- But in fact, the proof actually tells us a bit more: it even tells us how to *find* the multiplicative inverse.

[1] How convenient that someone made you learn how to work those coefficients out already!

Cancellation and Inverses, XII

So, the result we just proved shows that $\overline{a}$ has a multiplicative inverse modulo m if and only if a is relatively prime to m.

- But in fact, the proof actually tells us a bit more: it even tells us how to *find* the multiplicative inverse.
- Specifically, we just have to calculate the integers x and y such that $xa + ym = 1$, and then the multiplicative inverse of $\overline{a}$ is simply $\overline{x}$.
- And of course, you surely remember how to find those coefficients x and y: just use the Euclidean algorithm![1]

[1] How convenient that someone made you learn how to work those coefficients out already!

Cancellation and Inverses, XIII

Example: Find the multiplicative inverse of $\overline{5}$ modulo 11.

Cancellation and Inverses, XIII

<u>Example</u>: Find the multiplicative inverse of $\overline{5}$ modulo 11.

- We do the Euclidean algorithm on 5 and 11:

$$\begin{aligned} 11 &= 2 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 \end{aligned}$$

- Since the last nonzero remainder is 1, the gcd is 1. (That's good, otherwise $\overline{5}$ wouldn't be invertible mod 11!)
- Now we solve for the remainders:

$$1 = 11 - 2 \cdot 5$$

- So because $11 - 2 \cdot 5 = 1$, this means $(-2) \cdot 5 \equiv 1 \pmod{1}$, and so $\overline{-2} \cdot \overline{5} = \overline{1}$.
- So the multiplicative inverse of $\overline{5}$ modulo 1 is $\boxed{\overline{-2} = \overline{9}}$.

Cancellation and Inverses, XIV

Example: Find the multiplicative inverse of $\overline{19}$ modulo 44.

Cancellation and Inverses, XIV

Example: Find the multiplicative inverse of $\overline{19}$ modulo 44.

- We do the Euclidean algorithm on 19 and 44:

$$\begin{aligned} 44 &= 2 \cdot 19 + 6 \\ 19 &= 3 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 \end{aligned}$$

- Since the last nonzero remainder is 1, the gcd is 1. Now we solve for the remainders:

$$\begin{aligned} 6 &= 44 - 2 \cdot 19 \\ 1 &= 19 - 3 \cdot 6 = 19 - 3 \cdot (44 - 2 \cdot 19) = 7 \cdot 19 - 3 \cdot 44 \end{aligned}$$

- So because $7 \cdot 19 - 3 \cdot 44 = 1$, this means $7 \cdot 19 \equiv 1 \pmod{44}$, and so $\overline{7} \cdot \overline{19} = \overline{1}$.
- So the multiplicative inverse of $\overline{19}$ modulo 44 is $\boxed{\overline{7}}$.

Cancellation and Inverses, XV

Now, back to our other question, which was about cancellation.

- Specifically, we saw that we can do cancellation of a residue class modulo m precisely when that residue class is invertible.
- Obviously, $\overline{0}$ is never invertible (since anything times $\overline{0}$ is $\overline{0}$).
- But when will all the other residue classes be invertible?

Cancellation and Inverses, XV

Now, back to our other question, which was about cancellation.

- Specifically, we saw that we can do cancellation of a residue class modulo m precisely when that residue class is invertible.
- Obviously, $\overline{0}$ is never invertible (since anything times $\overline{0}$ is $\overline{0}$).
- But when will all the other residue classes be invertible?
- We saw that happen with $m = 2$, $m = 3$, and $m = 5$, for instance, but not for $m = 4$ or $m = 6$.)
- In other words, when are all of $1, 2, 3, \ldots, m - 1$ relatively prime to m?

Cancellation and Inverses, XV

Now, back to our other question, which was about cancellation.

- Specifically, we saw that we can do cancellation of a residue class modulo m precisely when that residue class is invertible.
- Obviously, $\overline{0}$ is never invertible (since anything times $\overline{0}$ is $\overline{0}$).
- But when will all the other residue classes be invertible?
- We saw that happen with $m = 2$, $m = 3$, and $m = 5$, for instance, but not for $m = 4$ or $m = 6$.)
- In other words, when are all of $1, 2, 3, \ldots, m - 1$ relatively prime to m?
- As suggested by the examples, that happens precisely when m is prime!

Cancellation and Inverses, XVI

Corollary

Every nonzero residue class in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse if and only if p is a prime number.

Proof:

Cancellation and Inverses, XVI

Corollary

Every nonzero residue class in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse if and only if p is a prime number.

Proof:

- If p is prime, then p is relatively prime to each of 1, 2, ... , $p-1$, so all of the nonzero residue classes modulo p are invertible by our previous result.
- Inversely, if n is composite, say $n = ab$ with $1 < a, b < n$, then $\gcd(a, n) = a > 1$, and so $\overline{a}$ is not invertible modulo n.

Cancellation and Inverses, XVII

This corollary states that when p is prime, $\mathbb{Z}/p\mathbb{Z}$ has the structure of the algebraic object called a field.

- To summarize: a field is a set F together with two binary operations of addition $(+)$ and multiplication $(\cdot)$ both of which are associative and commutative and where $\cdot$ distributes over $+$, that also possesses an additive identity 0 and a multiplicative identity $1 \neq 0$, and where every element has an additive inverse and every nonzero element has a multiplicative inverse.
- Some familiar examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
- We will discuss fields a little bit more at the end of the semester.

Wrap-Up

This marks the end of our discussion of modular arithmetic, but I would like to mention a few places it shows up.

- Modular arithmetic is foundational in mathematics, particularly for algebra, number theory, and topology.
- In CS, modular arithmetic is deeply enmeshed in many algorithms, particularly in cryptography. Most current cryptosystems (e.g., RSA, AES, and elliptic-curve cryptography) use modular arithmetic in a central way. You'll see a few pieces of some of that on Homework 6.
- Modular arithmetic also arises naturally in chemistry (in the study of molecular symmetries), music theory (in the study of tuning systems), economics and game theory (in the study of fair division problems), and the visual arts (in the study of various artistic designs).

Summary

We discussed cancellation modulo m and what it means for a residue class to have a multiplicative inverse.

We characterized the invertible residue classes and showed how to use the Euclidean algorithm to calculate modular inverses.

Next lecture: Relations, equivalence relations (start §3).