Math 321: Modular Arithmetic

Kameryn J Williams

University of Hawaiʻi at Mānoa

Fall 2020

A break from proof strategies

We've been talking about strategies for proofs. There's still more to learn here, but let's take a break to apply what we've learned.

Specifically, we're going to look at modular arithmetic.

A break from proof strategies

We've been talking about strategies for proofs. There's still more to learn here, but let's take a break to apply what we've learned.

Specifically, we're going to look at modular arithmetic.

The idea: fix a number n. Then do addition, multiplication, and so on where you only care about the remainder where you divide by n.

For example:

$$1 + 1 \equiv 0 \mod 2$$

is another way to express that the sum of two odd numbers is even. Modular arithmetic lets us generalize this kind of thinking.

A warmup: let's prove this makes sense

Let's prove that if you do integer division with remainder you always get a unique answer.

Theorem

Let n, d be integers with $d > 0$. Then there are unique integers q and r so that $n = qd + r$ with $0 \leq r < d$. We call q the quotient and r the remainder. You could instead write this as:

$$\frac{n}{d} = q + \frac{r}{d}$$

(In fact this is also true if $d < 0$.)

A warmup: let's prove this makes sense

Let's prove that if you do integer division with remainder you always get a unique answer.

Theorem

Let n, d be integers with $d > 0$. Then there are unique integers q and r so that $n = qd + r$ with $0 \leq r < d$. We call q the quotient and r the remainder. You could instead write this as:

$$\frac{n}{d} = q + \frac{r}{d}$$

(In fact this is also true if $d < 0$.)

The strategy: let q be the largest integer so that $qd \leq n$, then let $r = n - qd$. This uniquely determines q and r. Check that this works.

Proving you can do integer division with remainder

Proof.

First, let us see that the set X of integers x so that $xd \leq n$ is bounded from above. This can be seen just by noting that if $x > n$ then $xd > n \cdot 1 = n$, so every number in X is $\leq n$. Because X is a set of integers which is bounded above, it has a largest element, call it q. And because $qd \leq n$ there is an integer $r \geq 0$ so that $qd + r = n$. Note that q and r are uniquely determined.

It remains only to check that $r < d$. Suppose toward a contradiction that $r \geq d$. Then we get that $qd + d = (q+1)d < qd + r = n$. So $q + 1 \in X$, contradicting that q is the largest element of X. $\square$

Defining modular arithmetic

Let a, b be integers and n be a positive integer. Say that a and b are equivalent modulo n, written

$$a \equiv b \mod n,$$

if a and b have the same remainder when divided by n.

Defining modular arithmetic

Let a, b be integers and n be a positive integer. Say that a and b are equivalent modulo n, written

$$a \equiv b \mod n,$$

if a and b have the same remainder when divided by n.

We could equivalently define that $a \equiv b \mod n$ if $b - a$ is a multiple of n.

Defining modular arithmetic

Let a, b be integers and n be a positive integer. Say that a and b are equivalent modulo n, written

$$a \equiv b \mod n,$$

if a and b have the same remainder when divided by n.

We could equivalently define that $a \equiv b \mod n$ if $b - a$ is a multiple of n.

Why? Because if $a = q_a n + r$ and $b = q_b n + r$ then $b - a = (q_b - q_a)n$.

An example

Problem

It is currently 7:00. What time will it be in 8 hours?

An example

Problem

It is currently 7:00. What time will it be in 8 hours?

Answer.

$$7 + 8 = 15 \equiv 3 \mod 12,$$

so it will be 3:00. $\square$

Arithmetic mod n

Proposition

Suppose $a_0 \equiv a_1 \mod n$ *and* $b_0 \equiv b_1 \mod n$. *Then:*

1. $a_0 + b_0 \equiv a_1 + b_1 \mod n$;
2. $a_0 - b_0 \equiv a_1 - b_1 \mod n$; *and*
3. $a_0 \cdot b_0 \equiv a_1 \cdot b_1 \mod n$.

This proposition says that if we do modular arithmetic, then all that matters is the remainder: If two numbers have the same remainder, then you can substitute one for the other and get the same answer.

Let's check the + case

Suppose $a_0 \equiv a_1 \mod n$ and $b_0 \equiv b_1 \mod n$. We want to see that $a_0 + b_0 \equiv a_1 + b_1 \mod n$. By definition, we know that $(a_1 - a_0) = k_a n$ and $(b_1 - b_0) = k_b n$. Now look at

$$\begin{aligned}(a_1 + b_1) - (a_0 + b_0) &= (a_1 - a_0) + (b_1 - b_0) \\ &= k_a n + k_b n \\ &= (k_a + k_b) n.\end{aligned}$$

That is, we have seen that $a_0 + b_0 \equiv a_1 + b_1 \mod n$.

Let's check the + case

Suppose $a_0 \equiv a_1 \mod n$ and $b_0 \equiv b_1 \mod n$. We want to see that $a_0 + b_0 \equiv a_1 + b_1 \mod n$. By definition, we know that $(a_1 - a_0) = k_a n$ and $(b_1 - b_0) = k_b n$. Now look at

$$\begin{aligned}(a_1 + b_1) - (a_0 + b_0) &= (a_1 - a_0) + (b_1 - b_0) \\ &= k_a n + k_b n \\ &= (k_a + k_b) n.\end{aligned}$$

That is, we have seen that $a_0 + b_0 \equiv a_1 + b_1 \mod n$.

You can show the subtraction and multiplication case by a similar argument.

What about division?

In $\mathbb{Z}$, in general you cannot divide any two (nonzero) numbers. (Or rather, you can divide but it'll take you outside of $\mathbb{Z}$.) So it doesn't make sense to try to define modular arithmetic with division by looking at what a/b is modulo n.

What about division?

In $\mathbb{Z}$, in general you cannot divide any two (nonzero) numbers. (Or rather, you can divide but it'll take you outside of $\mathbb{Z}$.) So it doesn't make sense to try to define modular arithmetic with division by looking at what a/b is modulo n.

But there is an alternate way to think about division. Saying that $\frac{a}{b} = c$ is just saying that $a = bc$. That is, we can define division just in terms of multiplication.

What about division?

In $\mathbb{Z}$, in general you cannot divide any two (nonzero) numbers. (Or rather, you can divide but it'll take you outside of $\mathbb{Z}$.) So it doesn't make sense to try to define modular arithmetic with division by looking at what a/b is modulo n.

But there is an alternate way to think about division. Saying that $\frac{a}{b} = c$ is just saying that $a = bc$. That is, we can define division just in terms of multiplication.

Can we do this with modular multiplication? That is, if we have a and b when can we find c so that $a \equiv bc \mod n$?

What about division?

In $\mathbb{Z}$, in general you cannot divide any two (nonzero) numbers. (Or rather, you can divide but it'll take you outside of $\mathbb{Z}$.) So it doesn't make sense to try to define modular arithmetic with division by looking at what a/b is modulo n.

But there is an alternate way to think about division. Saying that $\frac{a}{b} = c$ is just saying that $a = bc$. That is, we can define division just in terms of multiplication.

Can we do this with modular multiplication? That is, if we have a and b when can we find c so that $a \equiv bc \mod n$?

Let's note that we can reduce the problem to asking: given b when can we find c so that $1 \equiv bc \mod n$? If we can do it for 1, then multiplying both sides by a gives it us for a. So to know whether we can divide by b what we need to know is whether b has a multiplicative inverse.

What about division?

Let's look at the example $n = 5$. We can write out the full multiplication table modulo 5:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

In each nonzero row a 1 appears, so every nonzero number has a multiplicative inverse modulo 5.

What about modular division?

Next let's look at the example $n = 6$. We can write out the full multiplication table modulo 6:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Only the rows for 1 and 5 have a 1 in them, so only 1 and 5 have a multiplicative inverse modulo 6.

What's the general pattern for modular division?

What's the general pattern for modular division?

Theorem

Let $a < n$ be a nonzero natural number. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
In particular, if n is prime then all non zero $a < n$ have multiplicative inverses modulo n.

What's the general pattern for modular division?

Theorem

Let $a < n$ be a nonzero natural number. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
In particular, if n is prime then all non zero $a < n$ have multiplicative inverses modulo n.

We will see why this is true another time :)