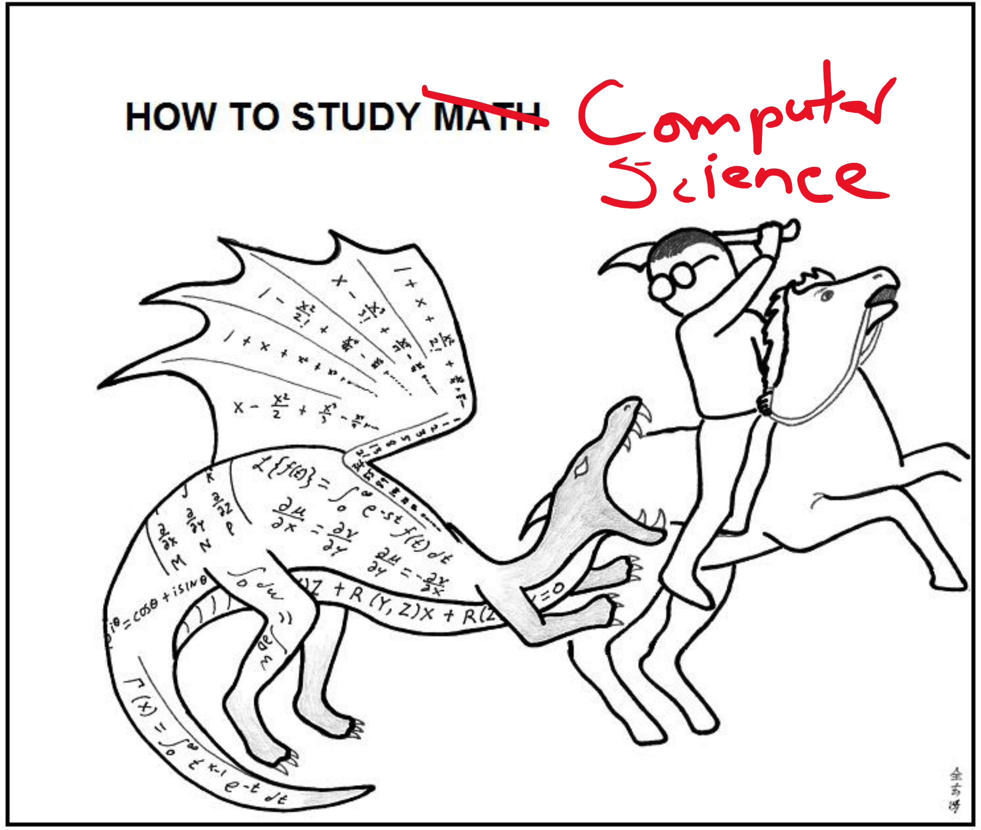


Don't just read it; fight it!

--- Paul R. Halmos

https://abstrusegoose.com/353

Number Theory

CSE 311 Autumn 2023
Lecture 12

Announcements

Don't forget CC11 (from Friday).

CC11 and CC12 (today's CC) are due Wednesday morning.

"How do I get started?"

↳ planning to record

OH tonight
CSE 403
6PM

Plan for this week (number theory)

Monday: Definitions, our first number theory proof.

Wednesday: A new kind of proof (proof by contradiction)

Thursday (in section): An algorithm to find greatest common divisors (and some extra information)

Friday: Another proof; why you should care about the algorithm from section; a few fun facts about number theory in CS.

Goal: learn enough number thy to (somewhat) understand RSA encryption

Divides

$x|y$

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

$4 \nmid 2$ $\quad 2(-1) = -2$

Which of these are true?

$2 \cdot \boxed{2} = 4$ $\quad 2|4$ ✓

$4 \cdot \boxed{} \neq 2$ $\quad 4|2$ ✗

$2|-2$ ✓

$5 \cdot \boxed{0} = 0$ $\quad 5|0$ ✓

$0|5$ ✗

$1|5$ ✓

Divides

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Which of these are true?

$2\|4$	True	$4\|2$	False	$2\|-2$	True
$5\|0$	True	$0\|5$	False	$1\|5$	True

A useful theorem

$\frac{a}{d}$

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d} > \mathbf{0}$
There exist ***unique*** integers q, r with $0 \leq r < d$
Such that $a = dq + r$

Remember when non integers were still secret, you did division like this?

d q r

$$\begin{array}{r} 4\ \text{R}5 \\ 7\overline{)33} \\ \underline{28} \\ 5 \end{array}$$

a q r

q is the "quotient"
r is the "remainder"

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d} > \mathbf{0}$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

The q is the result of `a/d` (integer division) in Java

The r is the result of `a%d` in Java

That's slightly a lie, r is always non-negative, Java's % operator sometimes gives a negative number.

Terminology

You might have called the % operator in Java "mod"

We're going to use the word "mod" to mean a closely related, but different thing.

Java's % is an operator (like + or ·) you give it two numbers, it produces a number.

The word "mod" in this class, refers to a set of rules

Modular Arithmetic

“arithmetic mod 12” is familiar to you. You do it with clocks.

$10+3=1$

What’s 3 hours after 10 o’clock?

1 o’clock. You hit 12 and then “wrapped around”

“13 and 1 are the same, mod 12” “-11 and 1 are the same, mod 12”

We don’t just want to do math for clocks – what about if we need to talk about parity (even vs. odd) or ignore higher-order-bits (mod by 16, for example)

Modular Arithmetic

~~$13 = 1$~~ $25 \% 12 = 1$

To say "the same" we don't want to use = … that means the normal =

$1 \equiv 13 \pmod{12}$

We'll write $13 \equiv 1 \pmod{12}$

≡ because "equivalent" is "like equal," and the "modulus" we're using in parentheses at the end so we don't forget it.

$25 \equiv 13 \pmod{12}$

(we'll also say "congruent mod 12")

The notation here is bad. We all agree it's bad. Most people still use it.

$13 \equiv_{12} 1$ would have been better. "mod 12" is giving you information about the ≡ symbol, it's not operating on 1.

$25 \equiv 1 \pmod{12}$

$13 \% 12 = 1$

Modular Arithmetic

$a \equiv b \pmod{n}$

We need a definition! We can't just say "it's like a clock"

Pause what do you expect the definition to be?

Is it related to % ? |

$a \% n = b \% n$

Modular Arithmetic

We need a definition! We can't just say "it's like a clock"

Pause what do you expect the definition to be?

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Huh?

Long Pause

It’s easy to read something with a bunch of symbols and say “yep, those are symbols.” and keep going

STOP Go Back.

You have to *fight* the symbols they’re probably trying to pull a fast one on you.

Same goes for when I’m presenting a proof – you shouldn’t just believe me – I’m wrong all the time!

You should be *trying* to do the proof with me. Where do you think we’re going next?

Why?

$27 \equiv 15 \pmod{12}$

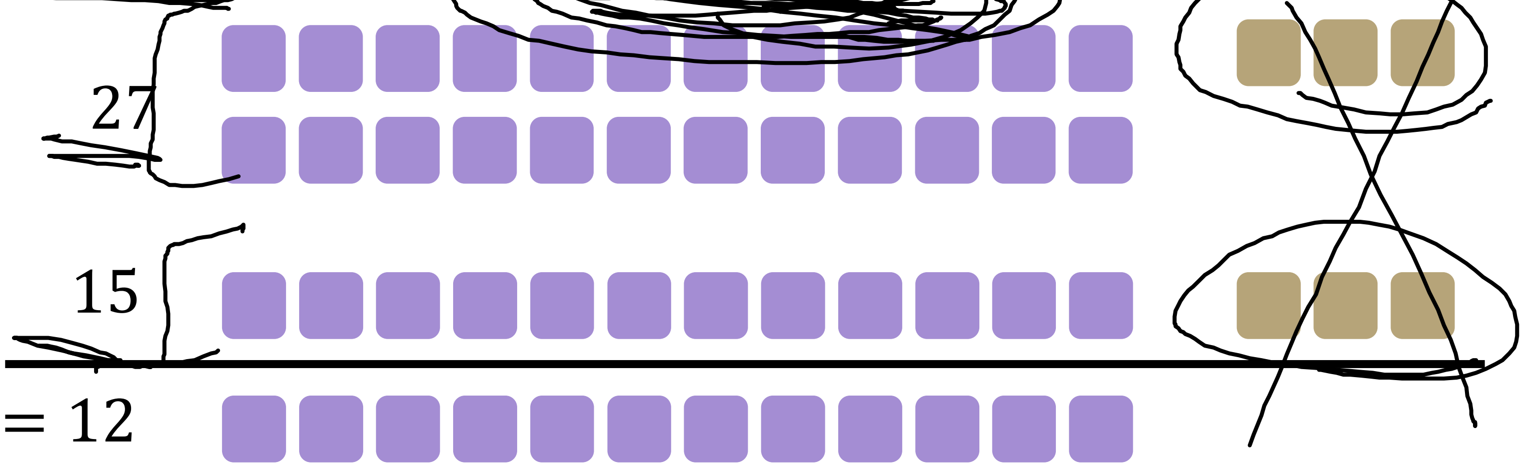
$27 \% 12 = 15 \% 12$

We'll post an optional (15-minute-ish) video ~~soon with why.~~

Here's the short version:

$n \mid (a-b)$

It really is equivalent to "what we expected"
`a%n=b%n` if and only if $n|(b-a)$



When you subtract, the remainders cancel. What you're left with is a multiple of 12.

The divides version is much easier to use in proofs…

Claim: for all $a, b, c, n \in \mathbb{Z}, n > 0$: $a \equiv b \pmod{n} \rightarrow a + c \equiv b + c \pmod{n}$

$\forall a \forall b \forall c \forall n ([n > 0 \wedge a \equiv b \pmod{n}] \rightarrow a + c \equiv b + c \pmod{n})$

Before we start, we must know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b\ (mod\ n)$ if and only if $n|(b - a)$

Pollev.com/robbie

Claim: $a, b, c, n \in \mathbb{Z}, n > 0$: $a \equiv b \pmod{n} \rightarrow a + c \equiv b + c \pmod{n}$

$n \mid (b-a)$

$n \mid (b-a+c-c)$

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$, and suppose $a \equiv b \pmod{n}$.

$\rightarrow n \mid b-a$

$\exists k \; (nk = b-a)$

$(n\_\_\_ = (b+c)-(a+c))$

$n \mid (b+c)-(a+c)$

$a + c \equiv b + c \pmod{n}$

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.

We say $a \equiv b \ (mod\ n)$ if and only if $n|(b-a)$

A proof

$nk = b - a$

$nk + c = b - a + c \Rightarrow nk = b - a + c - c$

$b + c - a - c$

Claim: $a, b, c, n \in \mathbb{Z}, n > 0$: $a \equiv b \pmod{n} \rightarrow a + c \equiv b + c \pmod{n}$

$(b+c) - (a+c)$

Proof:

$nz = b - a$

Let a, b, c, n be arbitrary integers with $n > 0$,
and suppose $a \equiv b (\mathrm{mod}\, n)$.

By definition of mod, $\mathrm{n}|(b - a)$

$+c \;\; -c$

By definition of divides, $nk = (b - a)$ for some integer k.

$(b+c) - (a+c)$

Adding and subtracting c, we have $nk = ([b + c] - [\mathrm{a} + \mathrm{c}])$.

Since k is an integer $n|([b + c] - [a + c])$

By definition of mod, $a + c \equiv b + c \pmod{n}$

You Try!

Claim: for all $a, b, c, n \in \mathbb{Z}, n > 0$: If $a \equiv b \ (mod\ n)$ then $ac \equiv bc \ (mod\ n)$

Before we start we must know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Claim: for all $a, b, c, n \in \mathbb{Z}, n > 0$: If $a \equiv b \ (mod\ n)$ then $ac \equiv bc \ (mod\ n)$

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$
and suppose $a \equiv b (mod\ n)$.

$ac \equiv bc \ (mod\ n)$

Claim: for all $a, b, c, n \in \mathbb{Z}, n > 0$: If $a \equiv b\ (mod\ n)$ then $ac \equiv bc\ (mod\ n)$

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$
and suppose $a \equiv b(mod\ n)$.

By definition of mod $n|(b-a)$

By definition of divides, $nk = b - a$ for some integer k

Multiplying both sides by c, we have $n(ck) = bc - ac$.

Since c and k are integers, $n|(bc - ac)$ by definition of divides.

So, $ac \equiv bc\ (mod\ n)$, by the definition of mod.

Don't lose your intuition!

Let's check that we understand "intuitively" what mod means:

$x \equiv 0 \pmod{2}$

"x is even" Note that negative (even) x values also make this true.

$-1 \equiv 19 \pmod{5}$

This is true! They both have remainder 4 when divided by 5.

$y \equiv 2 \pmod{7}$

This is true as long as $y = 2 + 7k$ for some integer k

Proof by Contrapositive

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrary integers, and suppose $a \nmid (bc)$.

Then there is not an integer z such that $az = bc$

…

So $a \nmid b$ or $a \nmid c$

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrar ... $c)$.

Then there is not an

…

So $a \nmid b$ or $a \nmid c$

There has to be a better way!

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

There has to be a better way!

If only there were some equivalent implication…

One where we could negate everything…

Take the contrapositive of the statement:

For all integers, a, b, c: Show if $a|b$ and $a|c$ then $a|(bc)$.

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

Therefore $a|bc$

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

By definition of divides, $ax = b$ and $ay = c$ for integers x and y.

Multiplying the two equations, we get $axay = bc$

Since a, x, y are all integers, xay is an integer. Applying the definition of divides, we have $a|bc$.

Signs you might want to use proof by contrapositive

1. The hypothesis of the implication you're proving has a "not" in it (that you think is making things difficult)

2. The target of the implication you're proving has an "or" or "not" in it.

3. You get halfway through the proof and you can't "get ahold of" what you're trying to show.

You're working with a "not equal" instead of an "equals" or "every thing doesn't have this property" instead of "some thing does have that property"

Logical Ordering

Logical Ordering

When doing a proof, we often work from both sides…

But we have to be careful!

When you read from top to bottom, every step has to follow only from what's **before** it, not after it.

Suppose our target is q and I know $q \to p$ and $r \to q$.

What can I put as a "new target?"

Logical Ordering

So why have all our prior steps been ok backward?

They’ve all been either:

A definition (which is always an “if and only if”)

An algebra step that is an “if and only if”

Even if your steps are “if and only if” you still have to put everything in order – start from your assumptions, and only assert something once it can be shown.

A bad proof

Claim: if x is positive then $x + 5 = -x - 5$.

$x + 5 = -x - 5$

$|x + 5| = |-x - 5|$

$|x + 5| = |-(x + 5)|$

$|x + 5| = |x + 5|$

$0 = 0$

This claim is **false –** if you're trying to do algebra, you need to start with an equation you know (say $x = x$ or $2 = 2$ or $0 = 0$) and expand to the equation you want.

More Mod proofs

More proofs

Show that if $a \equiv b (mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Step 1: What do the words mean?

Step 2: What does the statement as a whole say?

Step 3: Where do we start?

Step 4: What's our target?

Step 5: Now prove it.

Another Proof

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$ac \equiv bd(mod\ n)$

Another Proof

Show that if $a \equiv b (mod\, n)$ and $c \equiv d\ (mod\, n)$ then $ac \equiv bd\ (mod\, n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b (mod\, n)$ and $c \equiv d\ (mod\, n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd (mod\, n)$

Another Proof

Show that if $a \equiv b (mod\, n)$ and $c \equiv d\ (mod\, n)$ then $ac \equiv bd\ (mod\, n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b (mod\, n)$ and $c \equiv d\ (mod\, n)$.

$n|(b - a)$ and $n|(d - c)$ by definition of mod.

$nk = (b - a)$ and $nj = (d - c)$ for integers j, k by definition of divides.

$nknj = (d - c)(b - a)$ by multiplying the two equations

$nknj = (bd - bc - ad + ac)$

…

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd (mod\, n)$

Another Proof

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$nknj = (d-c)(b-a)$ by multiplying the two equations

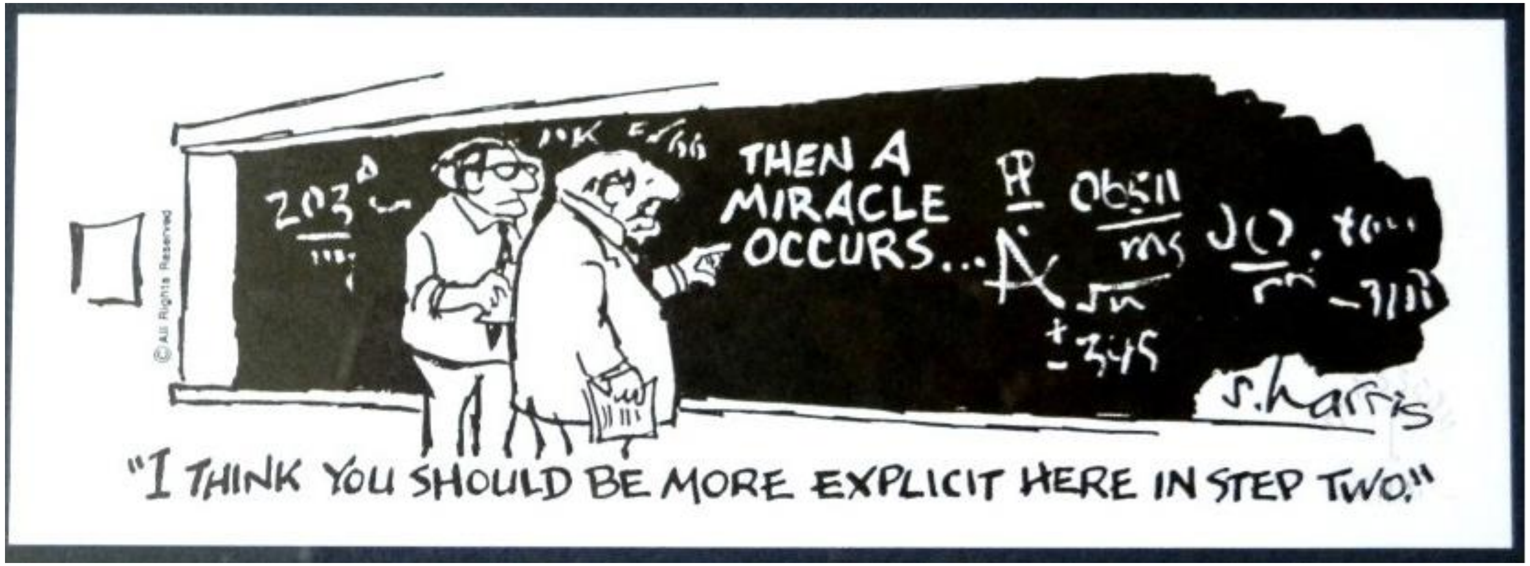
$nknj = (bd - bc - ad + ac)$

And then a miracle occurs

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\ n)$



Uh-Oh

We hit (what looks like) a dead end.

But how did I know we hit a dead end? Because I knew exactly where we needed to go. If you didn't, you'd have been staring at that for ages trying to figure out the magic step.

(or worse, assumed you lost a minus sign somewhere, and just "fixed" it….)

Let's try again. This time, let's **separate** b from a and d from c before combining.

Another Approach

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$b = nk + a, d = nj + c$

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\ n)$

Another Approach

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b - a)$ and $n|(d - c)$ by definition of mod.

$nk = (b - a)$ and $nj = (d - c)$ for integers j, k by definition of divides.

$b = nk + a, d = nj + c$,

$bd = (nk + a)(nj + c) = n^2kj + anj + cnk + ac$

$bd - ac = n^2kj + anj + cnk = n(nkj + aj + ck)$

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\ n)$

Another Approach

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

Isolating,b and d, we have: $b = nk + a, d = nj + c$

Multiplying the equations, and factoring, $bd = (nk+a)(nj+c) = n^2kj + anj + cnk + ac$

Rearranging, and facoring out n: $bd - ac = n^2kj + anj + cnk = n(nkj + aj + ck)$

Since all of $n, j, k, a,$ and c are integers, we have that $bd - ac$ is n times an integer, so

$n|(bd - ac)$, and by definition of mod

$ac \equiv bd(mod\ n)$

Extra Practice

Warm-up

Show that if $a \equiv b(mod\ n)$ then $b \equiv a\ (mod\ n)$.

Now that we've proven this, we aren't going to care whether you write $n|(b-a)$ or $n|(a-b)$ when you write the definition.

We can't remember the right order either.

Warm-up

Show that if $a \equiv b(mod\ n)$ then $b \equiv a\ (mod\ n)$.

Let a, b be arbitrary integers and let n be an arbitrary integer > 0, and suppose $a \equiv b(mod\ n)$.

By definition of equivalence mod n, $n|(b - a)$. By definition of divides, $nk = b - a$ for some integer k. Multiplying by -1, we get

$$n(-k) = a - b$$

Since k was an integer, so is $-k$. Thus $n|(a - b)$, and by definition of mod, $b \equiv a(mod\ n)$.

Extra Practice!

Warm up

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b-a)$

Show that $a \equiv b \ (mod\ n)$ if and only if $b \equiv a(mod\ n)$

Show that $a\%n$=$(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d} > \mathbf{0}$
There exist *unique* integers q, r with $0 \leq r < d$ Such that $a = dq + r$

Warm up

Show that $a \equiv b\ (mod\ n)$ if and only if $b \equiv a(mod\ n)$

$a \equiv b(mod\ n) \leftrightarrow n|(b-a) \leftrightarrow nk = b - a(\text{for } k \in \mathbb{Z}) \leftrightarrow$

$n(-k) = a - b(\text{for } -\mathrm{k} \in \mathbb{Z}) \leftrightarrow n|(a-b) \leftrightarrow b \equiv a(mod\ n)$

Show that $a\%n$=$(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

By definition of %, $a = qn + (a\%n)$ for some integer q. Subtracting n,

$a - n = (q-1)n + (a\%n)$. Observe that $q-1$ is an integer, and that this is the form of the division theorem for $(a-n)\%n$. Since the division theorem guarantees a unique integer, $(a-n)\%n = (a\%n)$

% and Mod

Other resources use mod to mean an operation (takes in an integer, outputs an integer). We will not in this course. mod only describes $\equiv$. It's not "just on the right hand side"

Define $a\%b$ to be "the r you get from the division theorem"
i.e. the integer r such that $0 \leq r < d$ and $a = bq + r$ for some integer q.

This is the "mod function"

I claim $a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$.

How do we show and if-and-only-if?

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$a\%n = (b - nk)\%n = b\%n$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$n|b-a$ so $nk = b - a$ for some integer k. (by definitions of mod and divides).

So $a = b - nk$

Taking each side $\%n$ we get:

$a\%n = (b - nk)\%n = b\%n$

Where the last equality follows from k being an integer and doing k applications of the identity we proved in the warm-up.

$a\%n = b\%n$ if and only if $a \equiv b (mod\ n)$

Show the forward direction:

If $a\%n = b\%n$ then $a \equiv b(mod\ n)$.

This proof is a bit different than the other direction.

Remember to work from top and bottom!!

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b\ (mod\ n)$ if and only if $n|(b - a)$

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d} > \mathbf{0}$
There exist *unique* integers q, r with $0 \leq r < d$ Such that $a = dq + r$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Forward direction:

Suppose $a\%n = b\%n$.

By definition of $\%, a = kn + (a\%n)$ and $b = jn + (b\%n)$ for integers k, j

Isolating $a\%n$ we have $a\%n = a - kn$. Since $a\%n = b\%n$, we can plug into the second equation to get: $b = jn + (a - kn)$

Rearranging, we have $b - a = (j - k)n$. Since k, j are integers we have $n|(b - a)$.

By definition of mod we have $a \equiv b(mod\ n)$.