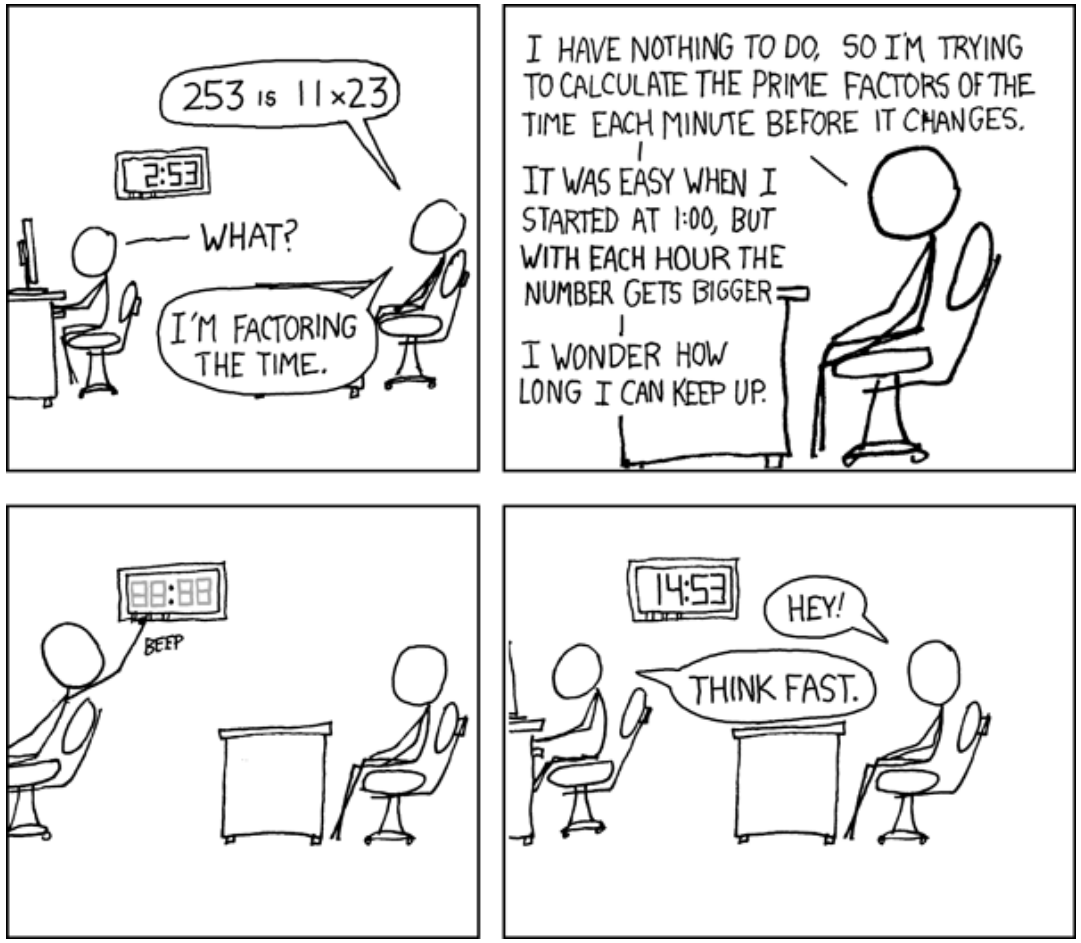


xkcd.com/247

More Number Theory

CSE 311 Spring 2022
Lecture 12

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!

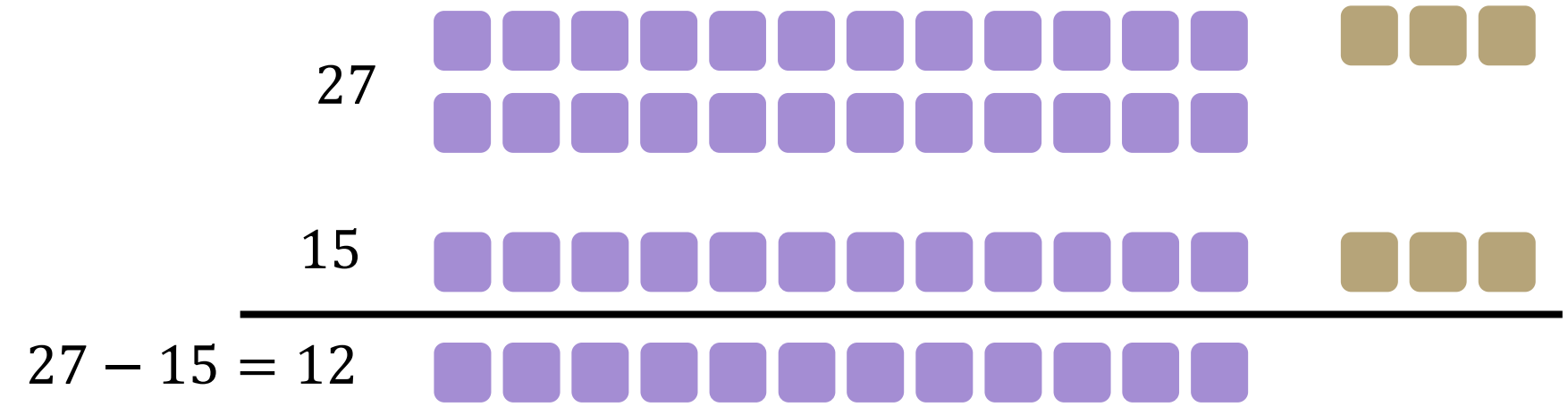
You should be *trying* to do the proof with me. Where do you think we're going next?

Why?

We'll post an optional (15-minute-ish) video over the weekend with why.

Here's the short version:

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

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.

Pollev.com/uwcse311

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

Proof:

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

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

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

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

Proof:

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

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

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

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

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, $b \equiv a(mod\ n)$.

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 $a \nmid c$.

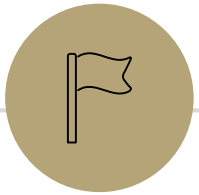
We argue by contrapositive.

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 $a|bc$.



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

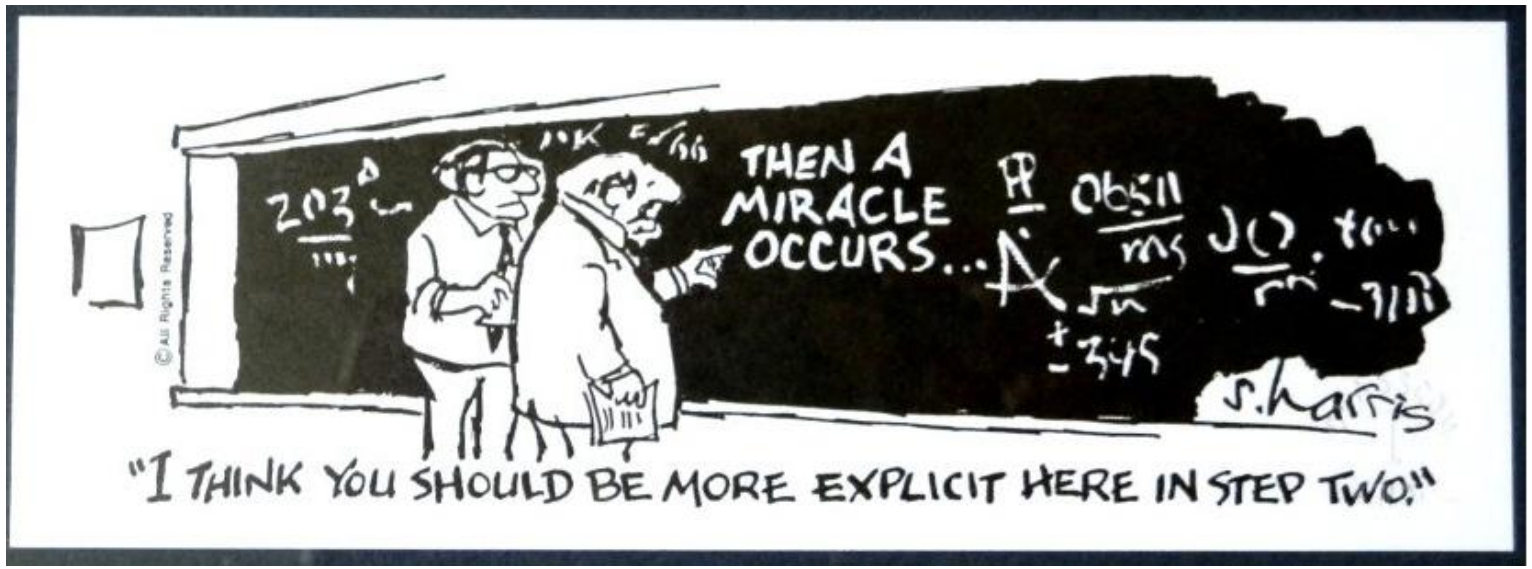
$nknj = (bd - bc - ad + ac)$

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

$ac \equiv bd(mod\ n)$

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 $x + 5 = -x - 5$.

$x + 5 = -x - 5$

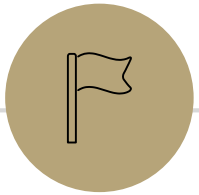
$|x + 5| = |-x - 5|$

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

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

$0 = 0$

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.



Divisors and Primes

Primes and FTA

Prime

An integer $p > 1$ is prime iff its only positive divisors are 1 and p. Otherwise it is "composite"

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization.

GCD and LCM

Greatest Common Divisor

The Greatest Common Divisor of a and b (gcd(a,b)) is the largest integer c such that $c|a$ and $c|b$

Least Common Multiple

The Least Common Multiple of a and b (lcm(a,b)) is the smallest positive integer c such that $a|c$ and $b|c$.

Try a few values…

gcd(100,125)

gcd(17,49)

gcd(17,34)

gcd(13,0)

lcm(7,11)

lcm(6,10)