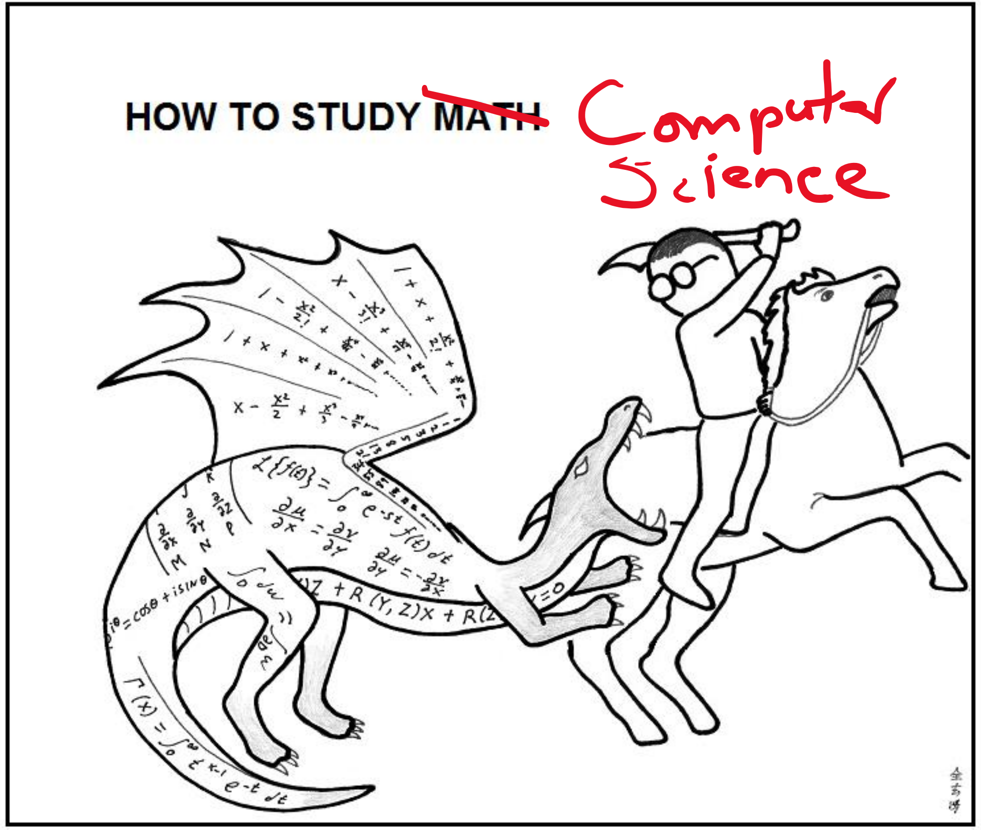


Don't just read it; fight it!

--- *Paul R. Halmos*

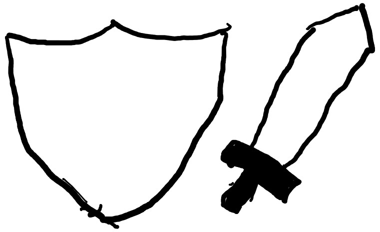
https://abstrusegoose.com/353

Warm-up

Let $S = \mathcal{P}(\{a,b,c\})$

- Is $\emptyset \in S$? ✓
- Is $\emptyset \subseteq S$? ✓
- Is $\{\{a\}\} \in S$? ✗
- Is $\{\{a\}\} \subseteq S$? ✓

$S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$



Number Theory

CSE 311 Autumn 2020

Lecture 11

Announcements

Lots of folks sounded concerned about English proofs in sections.

THAT'S NORMAL

English proofs aren't easy the first few times (or the next few times…sometimes not even after a decade…)

Keep asking questions!

Don't expect breakout room activities to be "easy."

If you know the right answer immediately, you won't learn much by doing it.

Last Time

Went reaaaaaaaaaaaaal fast…so we could practice proofs in section and slowly today.

We’ll keep practicing in the background.

Two More Set Operations

Given a set, let's talk about it's powerset.

$\mathcal{P}(A) = \{\mathrm{X} : \mathrm{X} \text{ is a subset of } A\}$

The powerset of A is the **set** of all subsets of A.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

Two More Set Operations

$A \times B = \{(a,b) : a \in A \land b \in B\}$

the set of all ordered pairs of A and B

Called "the Cartesian product" of A and B.

$\mathbb{R} \times \mathbb{R}$ is the "real plane" ordered pairs of real numbers.

$(x, f(x))$

$\{1,2\} \times \{1,2,3\} = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$

$A \times B \times C = \{(a,b,c) : a \in A \land b \in B \land c \in C\}$

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?

$2\|4$ ✓	$4\|2$ ✗	$2\|-2$ ✓
$2 \cdot 2 = 4$	$4 \cdot \frac{1}{2} = 2$	$2 \cdot -1 = -2$
$5\|0$ ✓	$0\|5$ ✗	$1\|5$ ✓
$5 \cdot 0 = 0$	$0 \cdot \_ = 5$	$1 \cdot 5 = 5$

Why Number Theory?

Applicable in Computer Science

“hash functions” (you’ll see them in 332) commonly use modular arithmetic
Much of classical cryptography is based on prime numbers.

More importantly, a great playground for writing English proofs.

A useful theorem

"is an element of"

integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

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 $a = dq + r$

$\frac{a}{d} = q$

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

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

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

Unique

The Division Theorem

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

"unique" means "only one"….but be careful with how this word is used.

r is unique, **given** a, d. – it still depends on a, d but once you've chosen a and d

$\forall \; \exists$

"unique" is not saying $\cancel{\exists r \forall a, d}\ \ P(a, d, r)$
It's saying $\forall a, d \exists r [P(a, d, r) \wedge [P(a, d, x) \rightarrow x = r]]$

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$
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.

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 a different number of "hours"?

Modular Arithmetic

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

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

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

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? $a \equiv b \pmod{n}$

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?

So, why?

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 $n |\ (b - a)$

What does it mean to be "the same in clock math"

If I divide by 12 then I get the same remainder.

Another try

$a \% n = b \% n$

Equivalence in modular arithmetic (correct, but bad)

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 the r guaranteed by the division theorem is equal for a/n and b/n

$r_a = r_b$

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 $a = dq + r$

$\frac{a}{d} = q$ with rem. r

Another Try

Equivalence in modular arithmetic (correct, but bad)

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 the r guaranteed by the division theorem is equal for a/n and b/n

This is a perfectly good definition. No one uses it.

Let's say you want to prove $a \equiv b \pmod{n} \rightarrow a + c \equiv b + c \pmod{n}$

So, uhh, who wants to divide $a + c$ by n and figure out what the remainder is?

a%n = b%n

(a+c)%n ⇝ (a%n + c%n) ~~%n~~

Once More, with feeling

Equivalence in modular arithmetic (correct, but bad)

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 the r guaranteed by the division theorem is equal for a/n and b/n

How do humans check if numbers are equivalent?

You subtract 12 as soon as the number gets too big, and make sure you end up with the same number (i.e. r)

So a is $r + 12k$ for some integer k and b is $r + 12j$ for some integer j

So b $- a = \cancel{r} + 12j - (\cancel{r} + 12k) = 12(j - k)$

$12 \mid (b-a)$

Now I see it

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 $n|(b-a)$

So, is it actually better?

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

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

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.

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

Proof:

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

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

$n \mid (b-a)$

$nk = b-a$ $\quad k \in \mathbb{Z}$.

$nk = b+c-a-c$

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

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

$a + c \equiv b + c \,(\text{mod } n)$

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

Proof:

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

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 $n|(b - a)$

Fill out the poll everywhere for Activity Credit!
Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 22333

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

$n \mid (b-a)$

$nk = b-a$ $k \in \mathbb{Z}$

$n\,kc = bc - ac$ $kc \in \mathbb{Z}$ ✓

$n \mid (bc - ac)$

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

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