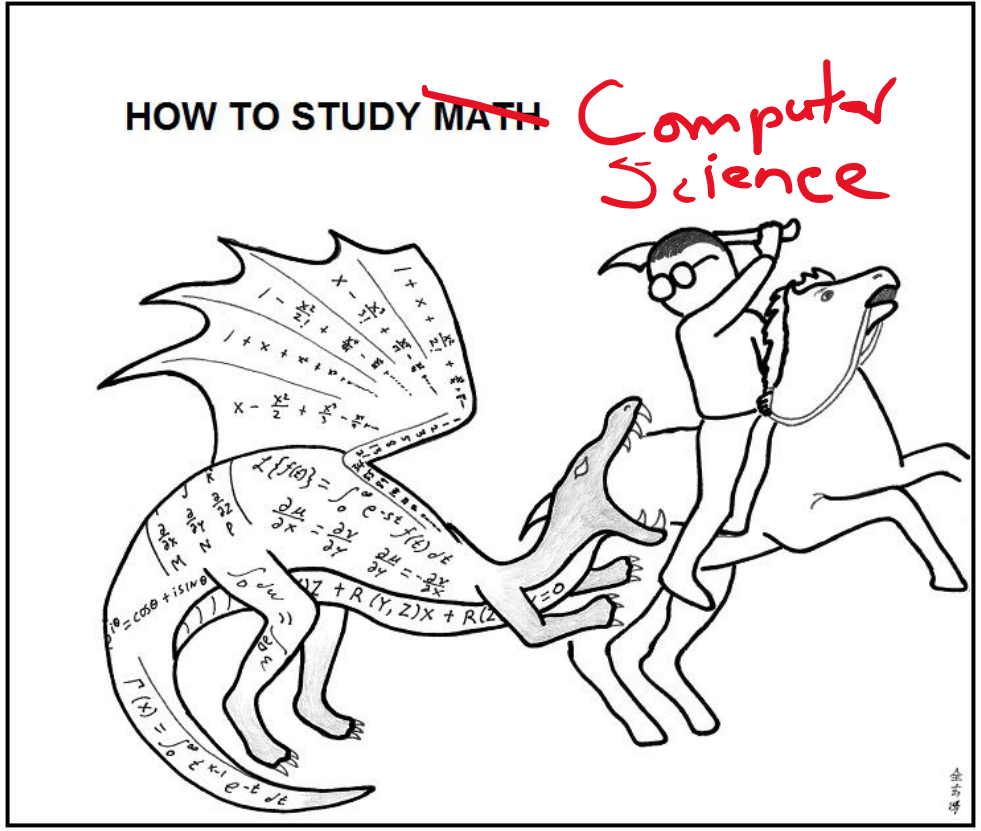


New slides posted ~2 minutes ago

Don't just read it; fight it!

--- Paul R. Halmos

https://abstrusegoose.com/353

Number Theory

CSE 311 Winter 2022
Lecture 11

Announcements

Set proofs (and English proofs in general) were a struggle in many sections yesterday.

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 section problems or breakout room activities to be "easy."

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

Announcements

We've only gotten a few responses to the office hour preferences

google form

If you have preferences about OH please fill it out tonight (otherwise we'll assume you don't care whether OH are in-person or on zoom).

Also has a spot to share questions/concerns.

We'll be in-person for lectures and sections going forward (unless we hear otherwise from the university).

Lectures still will be recorded, sections still will have "replacement videos"

Last Time/This Time

Went reaaaaaaaaaaaaal fast through sets…so we could practice proofs in section and have time for number theory today.

We'll keep practicing in the background.

Today we're starting on Number Theory

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.

Divides

Divides

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

$x | y$

Which of these are true?

$2|4$ — yes, true

$2 \cdot z = 4$

$4|2$ — false

$4 \cdot \frac{1}{2} = 2$

$2|-2$ — true

$5|0$ — true

$5 \cdot z = 0$

$0|5$ — false

$0 \cdot ? = 5$

$1|5$ — true

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 $a = dq + r$

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

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

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

$$33 = 4 \cdot 7 + 5$$
$$a = q \cdot d + r$$

$$15\overline{)733}$$

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

"unique" is not saying $\exists r \forall a, d \quad P(a, d, r)$
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 $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
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 to talk about parity (even vs. odd) or ignore lower-order-bits (mod by 16, for example)

Modular Arithmetic

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

We'll write $13 \equiv 1 (\mathbf{mod}\ 12)$

≡ 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"

$a \equiv b \pmod{n}$

Pause what do you expect the definition to be?

Is it related to % ?

$a \% n = b$

$a \% n = b \% n$

$a + kn = b + rn$ for some k, r

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?

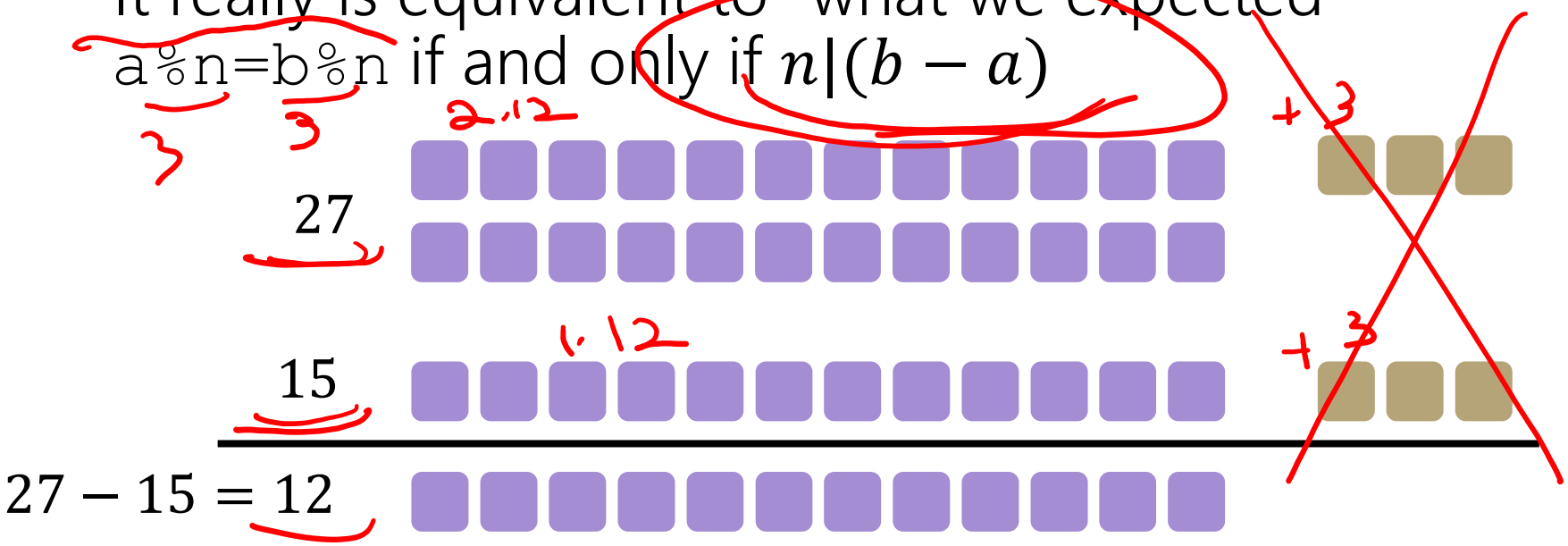
Why?

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

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.

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

fun defn of $\equiv \pmod n$, $n \mid b-a$

fun defn of $\mid$,
thus an int k, $nk = b-a$

$nk = a+c-[b+c]$

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

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

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

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

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

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

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

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:

$x \equiv 0 \pmod 2$

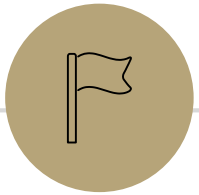
"x is even" Note that negative (even) x values also make this true.

$-1 \equiv 19 \pmod 5$

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.

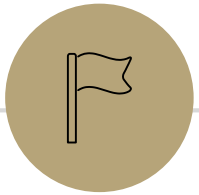
Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

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 $a|bc$, which is what we wanted to show.

Since a, b, c were arbitrary, our original claim holds for all integers.



Extra Set Practice

Extra Set Practice

Show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Proof:
Firse, we'll show: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
Let x be an arbitrary element of$A \cup (B \cap C)$.
Then by definition of ∪,∩ we have:
$x \in A \vee (x \in B \wedge x \in C)$
Applying the distributive law, we get
$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
Applying the definition of union, we have:
$x \in (A \cup B)$ and $x \in (A \cup C)$
By definition of intersection we have $x \in (A \cup B) \cap (A \cup C)$.
So $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Now we show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$
Let x be an arbitrary element of $(A \cup B) \cap (A \cup C)$.
By definition of intersection and union, $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
Applying the distributive law, we have $x \in A \vee (x \ \in B \wedge x \in C)$
Applying the definitions of union and intersection, we have $x \in A \cup (B \cap C)$
So $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
Combining the two directions, since both sets are subsets of each other, we have $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Extra Set Practice

Suppose $A \subseteq B$. Show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let A, B be arbitrary sets such that $A \subseteq B$.

Let X be an arbitrary element of $\mathcal{P}(A)$.

By definition of powerset, $X \subseteq A$.

Since $X \subseteq A$, every element of X is also in A. And since $A \subseteq B$, we also have that every element of X is also in B.

Thus $X \in \mathcal{P}(B)$ by definition of powerset.

Since an arbitrary element of $\mathcal{P}(A)$ is also in $\mathcal{P}(B)$, we have $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Extra Set Practice

Disprove: If $A \subseteq (B \cup C)$ then $A \subseteq B$ or $A \subseteq C$

Consider $A = \{1,2,3\}, B = \{1,2\}, C = \{3,4\}$.

$B \cup C = \{1,2,3,4\}$ so we do have $A \subseteq (B \cup C)$, but $A \nsubseteq B$ and $A \nsubseteq C$.

When you disprove a ∀, you're just providing a counterexample (you're showing ∃) – your proof won't have "let x be an arbitrary element of A."