CSE 311 Section 4

English Proofs & Set Theory

Administrivia

Announcements & Reminders

- HW2
  - If you think something was graded incorrectly, submit a regrade request!

- HW3 was due yesterday 1/24 @ 11:59PM on Gradescope
  - Use late days if you need them!

- HW4
  - Due Friday 1/31 @ 11:59pm

References

- Helpful reference sheets can be found on the course website!
  - https://courses.cs.washington.edu/courses/cse311/23wi/resources/
- How to LaTeX (found on Assignments page of website):
  - https://courses.cs.washington.edu/courses/cse311/23wi/assignments/HowToLaTeX.pdf
- Set Reference Sheet
  - https://courses.cs.washington.edu/courses/cse311/23wi/resources/reference-sets.pdf
- Number Theory Reference Sheet
  - https://courses.cs.washington.edu/courses/cse311/23wi/resources/reference-number-theory.pdf
- Plus more!

English Proofs

Writing a Proof (symbolically or in English)

- Don’t just jump right in!

1. Look at the **claim**, and make sure you know:
   - What every word in the claim means
   - What the claim as a whole means
2. Translate the claim in predicate logic.
3. Next, write down the **Proof Skeleton**:
   - Where to **start**
   - What your **target** is
   -
4. Then once you know what claim you are proving and your starting point and ending point, you can finally write the proof!

Helpful Tips for English Proofs

- Start by introducing your assumptions
  - Introduce variables with "let"
    - "Let x be an arbitrary prime number…"
  - Introduce assumptions with "suppose"
    - "Suppose that $y \in A \land y \notin B$…"

- When you supply a value for an existence proof, use "Consider"
  - "Consider $x = 2$…"

- **ALWAYS** state what type your variable is (integer, set, etc.)

- Universal Quantifier means variable must be arbitrary

- Existential Quantifier means variable can be specific

Divisibility

Problem 1

(a) Identify the statements that are true for divides

(i) 1 | 3

(ii) 3 | 1

(iii) 2 | 2018

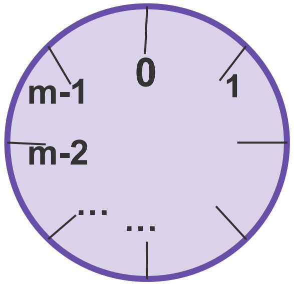
(iv) -2 | 12

(v) 1 * 2 * 3 * 4 | 1 * 2 * 3 * 4 * 5

Mod

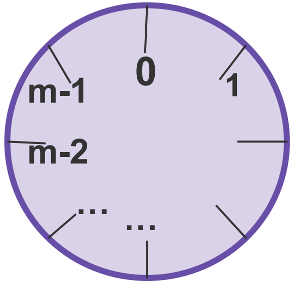
$a \equiv b \pmod{m}$

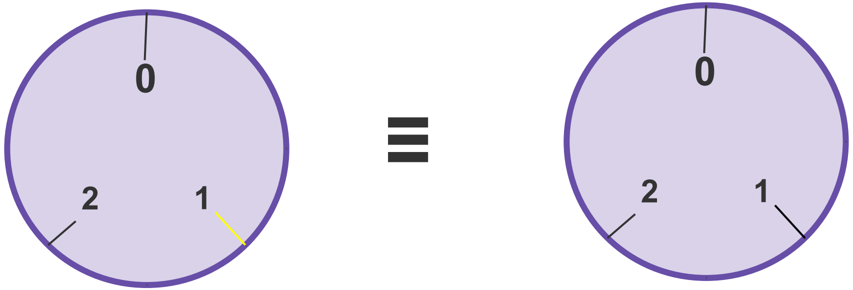
Imagine a clock with m numbers



a ≡ b (mod m)

Imagine a clock with m numbers

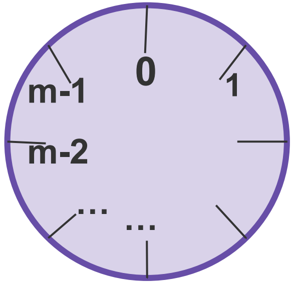


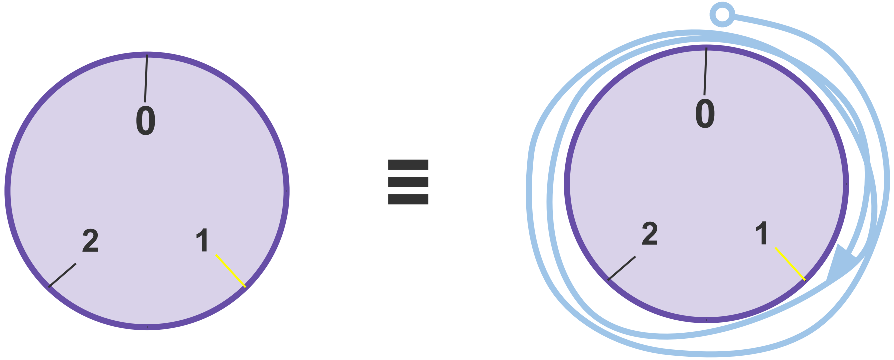


1 (mod 3) **VS** 10 (mod 3)

a ≡ b (mod m)

Imagine a clock with m numbers

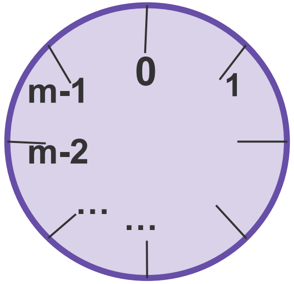


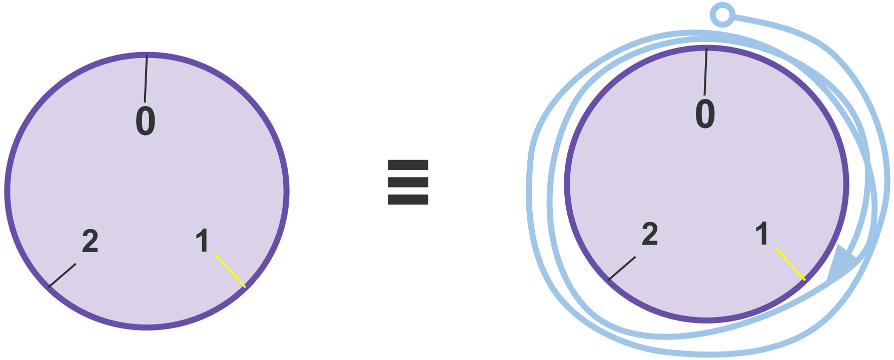


1 (mod 3) **VS** 10 (mod 3)

a ≡ b (mod m)

Imagine a clock with m numbers



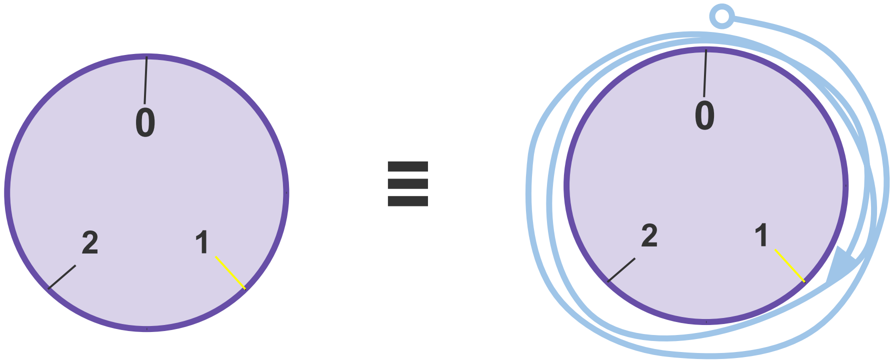


1 (mod 3) **VS** 10 (mod 3)

So we can say that **a ≡ b (mod m)** where a and b are in the same position in the mod clock

Divides

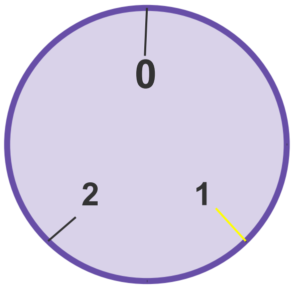
What if we “unroll” this clock?



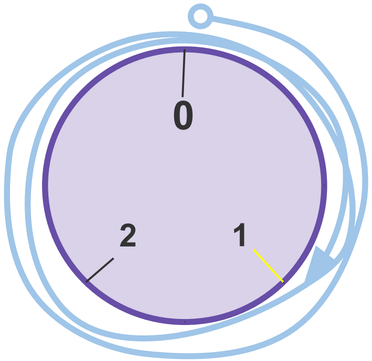
1 (mod 3) **VS** 10 (mod 3)

Divides

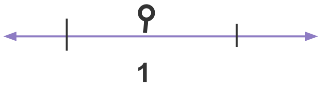
What if we “unroll” this clock?



≡

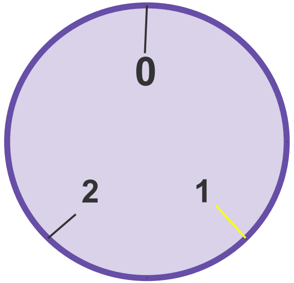


1 (mod 3) **VS** 10 (mod 3)

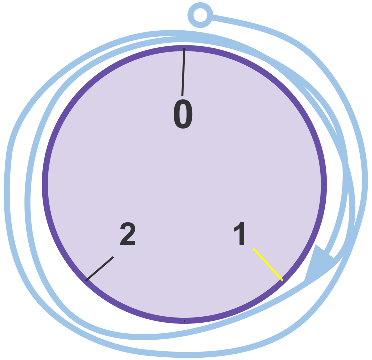


Divides

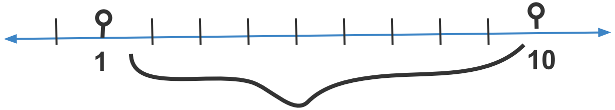
What if we “unroll” this clock?



≡



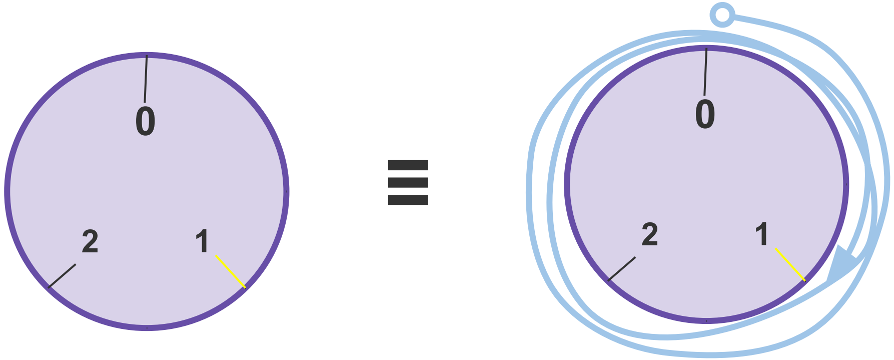
1 (mod 3) **VS** 10 (mod 3)



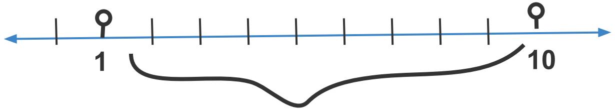
Anything interesting?

Divides

What if we "unroll" this clock?



1 (mod 3) **VS** 10 (mod 3)



(10-1) = 9

9 ÷ 3 = 3 so 3 | 9

Anything interesting?

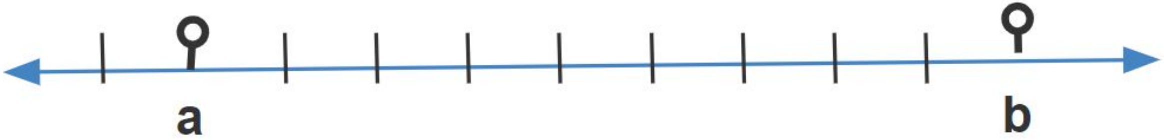
$3 \nmid 10$ and $3 \nmid 1$ BUT $3|9$

So m divides the <u>difference</u> between a and b

Formalizing Mod and Divides

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 $n|(b-a)$



n | (b-a)

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod{3}$

(ii) $0 \equiv 9000 \pmod{9}$

(iii) $44 \equiv 13 \pmod{7}$

(iv) $-58 \equiv 707 \pmod{5}$

(v) $58 \equiv 707 \pmod{5}$

Proving Divisibility

“Unwrapping”

a ≡ b (mod n) ⟷ n|(b-a) ⟷ (b-a) = n * k

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 $n|(b - a)$

Problem 3

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Problem 3

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(1) Understand what this claim means
(2) Write your start and end goal
(3) Write the skeleton
(4) Fill in the skeleton

Proof By Cases

Problem 5: Fair and Square

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(1) Understand what this claim means
(2) Write your start and end goal
(3) Write the skeleton
(4) Fill in the skeleton

Proofs by Contrapositive

Some claims are hard to prove directly!

- Sometimes you will run into claims that, because of the way they are structured, will be time consuming or difficult to prove.
- Recall in lecture, you attempted to prove that if the square of an integer is even, the integer must also be even.
- It was problematic to prove this because you had to deal with square roots.

Luckily, we can manipulate implications to put them into a form that is easier to solve!!

Why does Proof by Contrapositive work?

Consider the following truth table:

P	Q	$\neg P$	$\neg Q$	$P \to Q$	$\neg Q \to \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Note that, when the assignments of P and Q are such that $P \to Q$ is true, the assignments of their negation's *must also be such* that $\neg Q \to \neg P$ is also true. They are logically equivalent statements! (You can also do a four-step chain of equivalence to show this.)

Problem 6

For any integer j, if 3j+1 is even, then j is odd

(a) Write the predicate logic of this claim

Odd(x) := x is Odd

Even(x) := x is Even

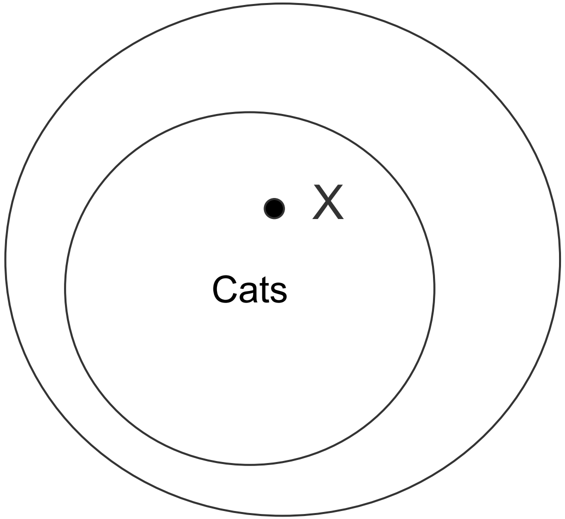
(b) Write the contrapositive of this claim

Problem 6

(c) Determine which claim is easier to prove, then prove it!

Side Note: What exactly *is* arbitrary?

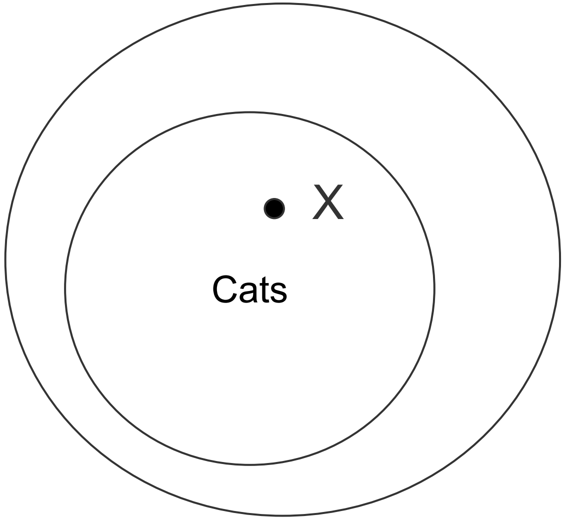
Domain: Animals



- Arbitrary is a word we use to describe an unspecified member of our domain. You can think of it as simultaneously being *any* and *all* members.
- When we attempt to prove universal claims, we must prove them with arbitrary variables. This is how we can know a claim holds for all members of the domain.

Side Note: What exactly *is* arbitrary?

Domain: Animals



- Consider the following claim: $\forall x[Cat(x) \rightarrow CuteInHolidaySweater(x)]$
- We would go about proving this claim by first defining x to be an *arbitrary cat.*
- If we can show that x does in fact look cute in a holiday sweater, this would mean that we have shown that *all members of the domain Cats* must also look cute in a holiday sweater.
- In other words, we have proven a relationship between the *property* of being a cat and the *property* of looking cute in a holiday sweater.

Side Note: What exactly *is* arbitrary?

An arbitrary cat, X

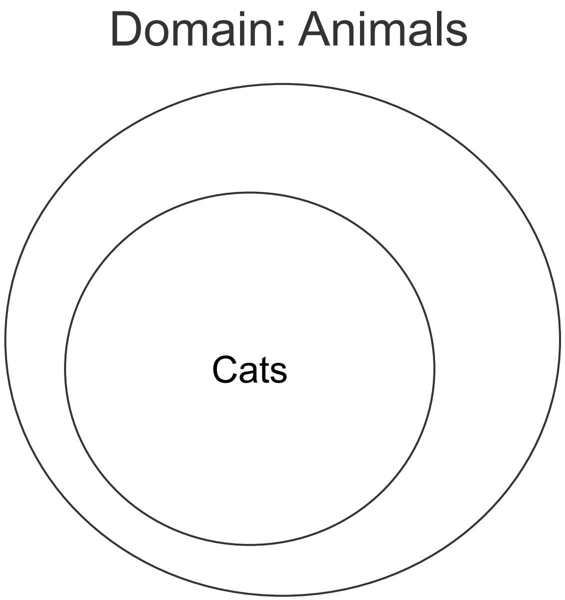
- X is an arbitrary cat, and X looks cute in a holiday sweater. So we know that for any element of our domain X, if it is a cat, then it must also look cute in a holiday sweater.

Side Note: What exactly *is* arbitrary?

More arbitrary cats

- We can pull as many elements from our domain as we like, in order for a universal claim to be true, it must be true for all of them.
- Claim proven!
- But what about existential claims?

Side Note: What exactly *is* arbitrary?



- Consider the following claim: $\exists x[Cat(x) \land DrinksBoba(x)]$
- Note that this is an existential claim. All we have to do is show that *at least one* example member of our domain fulfills these criteria in order for the claim to hold.
- Proving existentials is easier than proving universals, you simply furnish an example!

Side Note: What exactly *is* arbitrary?

A specific animal, Bagel

- When furnishing examples for an existential claim, we usually say “Consider… blank.”
- So, consider the following member of our domain, Bagel.
- Bagel is a cat, and Bagel drinks boba.
- This is enough information for us to know that the existential claim $\exists x[Cat(x) \wedge DrinksBoba(x)]$ holds. It *does not* have to extend to all other members of the domain, though it can.

That’s All Folks

Brought to you by Aruna & Cade’s suffering