

# CSE 311 Section 4

**English Proofs, Divisibility/Modulo, and  
Inference Proofs**

# Administrivia



# Announcements & Reminders

- HW2
  - If you think something was graded incorrectly, submit a regrade request!
- HW3 due yesterday 10/16 @ 11:59PM on Gradescope
  - Use late days if you need them!
- HW4
  - Due Wednesday 10/23 @ 11:59pm

# References

- Helpful reference sheets can be found on the course website!
  - <https://courses.cs.washington.edu/courses/cse311/24au/resources/>
- How to LaTeX (found on Assignments page of website):
  - <https://courses.cs.washington.edu/courses/cse311/24au/assignments/HowToLaTeX.pdf>
- Set Reference Sheet
  - <https://courses.cs.washington.edu/courses/cse311/24au/resources/reference-sets.pdf>
- Number Theory Reference Sheet
  - <https://courses.cs.washington.edu/courses/cse311/24au/resources/reference-number-theory.pdf>
- Plus more!

# English Proofs



# Writing a Proof (symbolically or in English)

- Don't just jump right in!
- Look at the **claim**, and make sure you know:
  - What every word in the claim means
  - What the claim as a whole means
- Translate the claim in predicate logic.
- Next, write down the **Proof Skeleton**:
  - Where to start
  - What your target is
- 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  $y \in A \wedge y \notin B...$ ”
- 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

## Problem 2 – Just the Setup

For each of these statements,

- Translate the sentence into predicate logic.
  - Write the first few sentences and last few sentences of the English proof.
- 
- a) The product of an even integer and an odd integer is even.
  - b) There is an integer  $x$  such that  $x^2 > 10$  and  $3x$  is even.
  - c) For every integer  $n$ , there is a prime number  $p$  greater than  $n$ .
  - d) If  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$  for any sets  $A, B, C$ .

Work on parts (b) and (c) with the people around you, and then we'll go over it together!



## Problem 2 – Just the Setup

b) There is an integer  $x$  such that  $x^2 > 10$  and  $3x$  is even.

## Problem 2 – Just the Setup

c) For every integer  $n$ , there is a prime number  $p$  greater than  $n$ .

# Divisibility & Modulus



# Some Definitions

- Divides:
  - For  $a, b \in \mathbb{Z}$ :  $a \mid b$  iff  $\exists(k \in \mathbb{Z}) b = ka$
  - For integers  $a$  and  $b$ , we say  $a$  divides  $b$  if and only if there exists an integer  $k$  such that  $b = ka$
- Congruence Modulo:
  - For  $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$ :  $a \equiv b \pmod{m}$  iff  $m \mid (b - a)$
  - For integers  $a$  and  $b$  and positive integer  $m$ , we say  $a$  is congruent to  $b$  modulo  $m$  if and only if  $m$  divides  $b - a$

# Problem 1 – Divisibility

(a) Circle the statements below that are true. Recall that for  $a, b \in \mathbb{Z}$ :  $a|b$  if and only if  $\exists k \in \mathbb{Z}$  such that  $b = ka$ .

(i)  $1 \mid 3$

(ii)  $3 \mid 1$

(iii)  $2 \mid 2018$

(iv)  $-2 \mid 12$

(v)  $1 \cdot 2 \cdot 3 \cdot 4 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

# Problem 1 – Divisibility

(b) Circle the statements below that are true. Recall that for  $a, b, m \in \mathbb{Z}$  and  $m > 0$ :  $a \equiv b \pmod{m}$  if and only if  $m \mid (a - b)$ .

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

# Inference Proofs



# Inference Proofs

- New way of doing proofs:
  - Write down all the facts we know (givens)
  - Combine the things we know to derive new facts
  - Continue until what we want to show is a fact
- **Modus Ponens**
  - $[(p \rightarrow q) \wedge p] \rightarrow q \equiv T$
  - If you have an implication and its hypothesis as facts, you can get the conclusion
- **Direct Proof Rule**
  - Assume  $x$  and then eventually get  $y$ , you can conclude that  $x \rightarrow y$



## Problem 10 - Formal Spoofs

For each of the following proofs, determine why the proof is incorrect. Then, consider whether the conclusion of the proof is true or not. If it is true, state how the proof could be fixed. If it is false, give a counterexample.

(a) Show that  $\exists z \forall x P(x, z)$  follows from  $\forall x \exists y P(x, y)$

(b) Show that  $\exists z (P(z) \wedge Q(z))$  follows from  $\forall x P(x)$  and  $\exists y Q(y)$

Let's do part a

## Problem 10 – Formal Spoofs

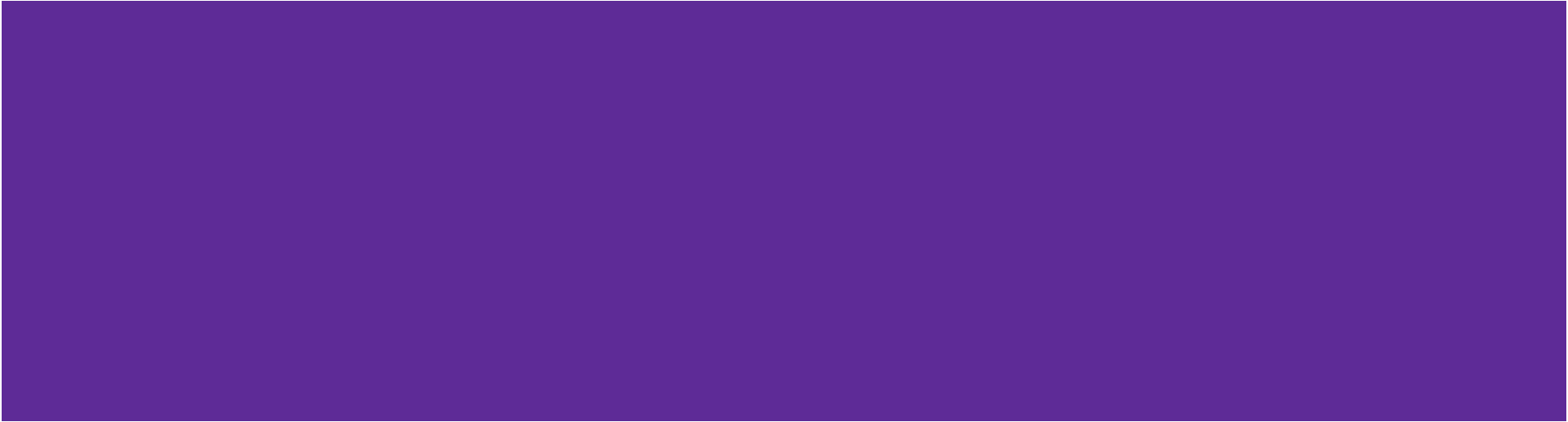
(a) Show that  $\exists z \forall x P(x, z)$  follows from  $\forall x \exists y P(x, y)$

1.  $\forall x \exists y P(x, y)$  [Given]
2.  $\forall x P(x, c)$  [ $\exists$  Elim: 1, c special]
3.  $\exists z \forall x P(x, z)$  [ $\exists$  Intro: 2]

## Problem 12 – A Formal Proof in Predicate Logic

Prove  $\exists x (P(x) \vee R(x))$  from  $\forall x (P(x) \vee Q(x))$  and  $\forall y (\neg Q(y) \vee R(y))$

# Bonus: Modular Arithmetic



## Problem 3 – Modular Arithmetic

- a) Prove that if  $a \mid b$  and  $b \mid a$ , where  $a$  and  $b$  are integers, then  $a = b$  or  $a = -b$ .
  
- b) Prove that if  $n \mid m$ , where  $n$  and  $m$  are integers greater than 1, and if  $a \equiv b \pmod{m}$ , where  $a$  and  $b$  are integers, then  $a \equiv b \pmod{n}$ .

Lets walk through part (a) together.

## Problem 3 – Modular Arithmetic

- b) Prove that if  $n \mid m$ , where  $n$  and  $m$  are integers greater than 1, and if  $a \equiv b \pmod{m}$ , where  $a$  and  $b$  are integers, then  $a \equiv b \pmod{n}$ .

# Inference Proof Example

Given  $((p \rightarrow q) \wedge (q \rightarrow r))$ , show that  $(p \rightarrow r)$

1.  $((p \rightarrow q) \wedge (q \rightarrow r))$

Given

2.  $p \rightarrow q$

Eliminate  $\wedge$ : 1

3.  $q \rightarrow r$

Eliminate  $\wedge$ : 1

4.1  $p$

Assumption

4.2  $q$

Modus Ponens: 4.1, 2

4.3  $r$

Modus Ponens: 4.2, 3

5.  $p \rightarrow r$

Direct Proof Rule

# **That's All, Folks!**

**Thanks for coming to section this week!**  
**Any questions?**