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

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

$\exists x[\text{GreaterThan10}(x^2) \wedge \text{Even}(3x)]$

Problem 2 – Just the Setup

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

$\exists x[\text{GreaterThan10}(x^2) \wedge \text{Even}(3x)]$

Consider $x = 6$.

. . . .

Problem 2 – Just the Setup

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

$\exists x[\text{GreaterThan10}(x^2) \wedge \text{Even}(3x)]$

Consider $x = 6$.

. . . .

Then there exists some integer k such that $3 \cdot 6 = 2k$.

Problem 2 – Just the Setup

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

$\exists x[\text{GreaterThan10}(x^2) \wedge \text{Even}(3x)]$

Consider $x = 6$.
. . . .
Then there exists some integer k such that $3 \cdot 6 = 2k$.
So $6^2 > 10$ and $3 \cdot 6$ is even.
Hence, 6 is the desired x.

Problem 2 – Just the Setup

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

Problem 2 – Just the Setup

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

$\forall x \exists y [\text{Prime}(y) \wedge \text{GreaterThan}(y, x)]$

Problem 2 – Just the Setup

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

$\forall x \exists y [\text{Prime}(y) \wedge \text{GreaterThan}(y, x)]$

Let x be an arbitrary integer.

Problem 2 – Just the Setup

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

$\forall x \exists y [\text{Prime}(y) \wedge \text{GreaterThan}(y, x)]$

Let x be an arbitrary integer.
Consider $y = p$ (this p is a specific prime)
. . . .

Problem 2 – Just the Setup

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

$\forall x \exists y [\text{Prime}(y) \wedge \text{GreaterThan}(y, x)]$

Let x be an arbitrary integer.
Consider $y = p$ (this p is a specific prime)
. . . .
So p is prime and $p > x$.
Since x was arbitrary, we have that every integer has a prime number that is greater than it.

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

(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) $1 \mid 3$ True

(ii) $3 \mid 1$ False

(iii) $2 \mid 2018$ True

(iv) $-2 \mid 12$ True

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

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

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) $-3 \equiv 3 \pmod{3}$ True

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

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

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

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

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 $\exists z\big(P(z) \wedge Q(z)\big)$ 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.	$\forall x\, P(x, c)$	[∃ Elim: 1, c special]
3.	$\exists z \forall x\, P(x, z)$	[∃ Intro: 2]

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

Mistake on line 2, an inference rule is used on a subexpression. When we apply something like the ∃ Elim rule, the ∃ must be at the start of the expression and outside all other parts of the statement

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

Mistake on line 2, an inference rule is used on a subexpression. When we apply something like the ∃ Elim rule, the ∃ must be at the start of the expression and outside all other parts of the statement

The conclusion is false, it's basically saying we can interchange the order of ∀ and ∃ quantifiers. Let the domain of discourse be integers and define $P(x, y)$ to be $x < y$. Then the hypothesis is true: for every integer, there is a larger integer. However, the conclusion is false: there is no integer that is larger than every other integer. Hence, there can be no correct proof that the conclusion follows from the hypothesis.

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 $\forall y\ (\neg Q(y) \vee R(y))$

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]

?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]

?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]

?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]
6.	$\neg\neg P(a) \vee Q(a)$	[Double Negation: 3]

?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]
6.	$\neg\neg P(a) \vee Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \rightarrow Q(a)$	[Law of implication: 5]

?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\,(\neg Q(y) \vee R(y))$

1. $\forall x\,(P(x) \vee Q(x))$ [Given]
2. $\forall y\,(\neg Q(y) \vee R(y))$ [Given]
3. $P(a) \vee Q(a)$ [Elim ∀: 1]
4. $\neg Q(a) \vee R(a)$ [Elim ∀: 2]
5. $Q(a) \rightarrow R(a)$ [Law of implication: 4]
6. $\neg\neg P(a) \vee Q(a)$ [Double Negation: 3]
7. $\neg P(a) \rightarrow Q(a)$ [Law of implication: 5]

    8.1. $\neg P(a)$ [Assumption]

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 $\forall y\,(\neg Q(y) \vee R(y))$

1. $\forall x\,(P(x) \vee Q(x))$ [Given]
2. $\forall y\,(\neg Q(y) \vee R(y))$ [Given]
3. $P(a) \vee Q(a)$ [Elim ∀: 1]
4. $\neg Q(a) \vee R(a)$ [Elim ∀: 2]
5. $Q(a) \rightarrow R(a)$ [Law of implication: 4]
6. $\neg\neg P(a) \vee Q(a)$ [Double Negation: 3]
7. $\neg P(a) \rightarrow Q(a)$ [Law of implication: 5]
    - 8.1. $\neg P(a)$ [Assumption]
    - 8.2. $Q(a)$ [Modus Ponens: 8.1, 7]

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 $\forall y\ (\neg Q(y) \vee R(y))$

1. $\forall x\ (P(x) \vee Q(x))$ [Given]
2. $\forall y\ (\neg Q(y) \vee R(y))$ [Given]
3. $P(a) \vee Q(a)$ [Elim ∀: 1]
4. $\neg Q(a) \vee R(a)$ [Elim ∀: 2]
5. $Q(a) \rightarrow R(a)$ [Law of implication: 4]
6. $\neg\neg P(a) \vee Q(a)$ [Double Negation: 3]
7. $\neg P(a) \rightarrow Q(a)$ [Law of implication: 5]
    - 8.1. $\neg P(a)$ [Assumption]
    - 8.2. $Q(a)$ [Modus Ponens: 8.1, 7]
    - 8.3. $R(a)$ [Modus Ponens: 8.2, 5]

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 $\forall y\,(\neg Q(y) \vee R(y))$

1. $\forall x\,(P(x) \vee Q(x))$ [Given]
2. $\forall y\,(\neg Q(y) \vee R(y))$ [Given]
3. $P(a) \vee Q(a)$ [Elim ∀: 1]
4. $\neg Q(a) \vee R(a)$ [Elim ∀: 2]
5. $Q(a) \rightarrow R(a)$ [Law of implication: 4]
6. $\neg\neg P(a) \vee Q(a)$ [Double Negation: 3]
7. $\neg P(a) \rightarrow Q(a)$ [Law of implication: 5]
    - 8.1. $\neg P(a)$ [Assumption]
    - 8.2. $Q(a)$ [Modus Ponens: 8.1, 7]
    - 8.3. $R(a)$ [Modus Ponens: 8.2, 5]
8. $\neg P(a) \rightarrow R(a)$ [Direct Proof]

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]
6.	$\neg\neg P(a) \vee Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \rightarrow Q(a)$	[Law of implication: 5]
8.	$\neg P(a) \rightarrow R(a)$	[Direct Proof: 4]
9.	$\neg\neg P(a) \vee R(a)$	[Law of implication: 8]
?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\ (\neg Q(y) \vee R(y))$

1.	$\forall x\ (P(x) \vee Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]
6.	$\neg\neg P(a) \vee Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \rightarrow Q(a)$	[Law of implication: 5]
8.	$\neg P(a) \rightarrow R(a)$	[Direct Proof: 4]
9.	$\neg\neg P(a) \vee R(a)$	[Law of implication: 8]
10.	$P(a) \vee R(a)$	[Double Negation: 9]
?.	$\exists x\ (P(x) \vee R(x))$	???

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 $\forall y\,(\neg Q(y) \vee R(y))$

1.	$\forall x\,(P(x) \vee Q(x))$	[Given]
2.	$\forall y\,(\neg Q(y) \vee R(y))$	[Given]
3.	$P(a) \vee Q(a)$	[Elim ∀: 1]
4.	$\neg Q(a) \vee R(a)$	[Elim ∀: 2]
5.	$Q(a) \rightarrow R(a)$	[Law of implication: 4]
6.	$\neg\neg P(a) \vee Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \rightarrow Q(a)$	[Law of implication: 5]
8.	$\neg P(a) \rightarrow R(a)$	[Direct Proof: 4]
9.	$\neg\neg P(a) \vee R(a)$	[Law of implication: 8]
10.	$P(a) \vee R(a)$	[Double Negation: 9]
11.	$\exists x\,(P(x) \vee R(x))$	[Intro ∃: 10]

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

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

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

…

Therefore, it follows that $a = -b$ or $a = b$.

Start with your proof skeleton!

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 $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka$, $a = jb$ for some integers k, j.

…

Therefore, it follows that $a = -b$ or $a = b$.

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 $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0, b \neq 0$ and $b = ka, a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
…

Therefore, it follows that $a = -b$ or $a = b$.

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 $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka$, $a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$.

…

Therefore, it follows that $a = -b$ or $a = b$.

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 $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka$, $a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$.
Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$.

Therefore, it follows that $a = -b$ or $a = b$.

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

Now try part (b) with the people around you, and then we'll go over it 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 $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

…

Therefore, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

…

… we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

NOTE: we don't know what C will look like yet, just that there is SOME integer here!

…

… we have $b - a = nC$.

Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.

…

… we have $b - a = nC$.

Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
…
… we have $b - a = nC$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
… we have $b - a = nC$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
Equivalently, we have $b - a = n(-kj)$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

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

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
Equivalently, we have $b - a = n(-kj)$.
Because $-kj$ is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Inference Proof Example

Given $((p \to q) \land (q \to r))$, show that $(p \to r)$

1.	$((p \to q) \land (q \to r))$	Given
2.	$p \to q$	Eliminate ∧: 1
3.	$q \to r$	Eliminate ∧: 1
	4.1 p	Assumption
	4.2 q	Modus Ponens: 4.1, 2
	4.3 r	Modus Ponens: 4.2, 3
5.	$p \to r$	Direct Proof Rule

That's All, Folks!

Thanks for coming to section this week!
Any questions?