Pre-class quiz #9 is due Monday November 9\textsuperscript{th} at 19:00
- Epp, 5\textsuperscript{th} or 4\textsuperscript{th} edition: 12.2, pages 791 to 795.
- Epp, 3\textsuperscript{rd} edition: 12.2, pages 745 to 747, 752 to 754
- Rosen, 6\textsuperscript{th} edition: 12.2 pages 796 to 798, 12.3
- Rosen, 7\textsuperscript{th} edition: 13.2 pages 858 to 861, 13.3

Pre-class quiz #10 is tentatively due Monday November 16\textsuperscript{th} at 19:00.
- Textbook sections:
  - Epp, 5\textsuperscript{th} or 4\textsuperscript{th} edition: 5.1 to 5.4
  - Epp, 3\textsuperscript{rd} edition: 4.1 to 4.4
  - Rosen, 6\textsuperscript{th} edition: 4.1, 4.2
  - Rosen, 7\textsuperscript{th} edition: 5.1, 5.2

By the start of class, you should be able to, for each proof strategy below:
- Identify the form of statement the strategy can prove.
- Sketch the structure of a proof that uses the strategy.

**Strategies:**
- constructive/non-constructive proofs of existence
- generalizing from the generic particular
- direct proof (antecedent assumption)
Module 8: Proof Techniques (part 1)

- Strategies (continued):
  - indirect proofs by contrapositive and contradiction
  - proof by cases.

Module 8: Proof Techniques (part 1)

- Quiz 8 open-ended question: when should you switch strategies?
  - When you are stuck.
  - When the proof is going around in circles.
  - When the proof is getting too messy.
  - When it is taking too long.
  - Through experience (how do you get that?)

Module 8: Proof Techniques (part 1)

- CPSC 121: the BIG questions:
  - How can we convince ourselves that an algorithm does what it's supposed to do?
    - We need to prove its correctness.
  - How do we determine whether or not one algorithm is better than another one?
    - Sometimes, we need a proof to convince someone that the number of steps of our algorithm is what we claim it is.

Module 8: Proof Techniques (part 1)

- By the end of this module, you should be able to:
  - Devise and attempt multiple different, appropriate proof strategies for a given theorem, including
    - all those listed in the "pre-class" learning goals
    - logical equivalences,
    - rules of inference,
    - universal modus ponens/tollens,
  - For theorems requiring only simple insights beyond strategic choices or for which the insight is given/hinted, additionally prove the theorem.
Module 8: Proof Techniques (part 1)

- Module Summary
  - Techniques for **direct proofs**.
    - Existential quantifiers.
    - Universal quantifiers.
    - Dealing with nested quantifiers.
    - Indirect proofs: contrapositive and contradiction
    - Choosing a proof strategy
  - Additional Examples

Module 8.1: Direct Proofs

- Direct Proofs:
  - We start with some facts (premises, hypotheses)
    - They are known or assumed to be true.
  - We move **one** step at a time towards the conclusion.
  - There are two general forms of statements:
    - Those that start with an existential quantifier.
    - Those that start with a universal quantifier.
  - We use different techniques for them.

Module 8.1.1: Direct Proofs (existential)

- **Form 1**: \( \exists x \in D, P(x) \)

- To prove this statement is true, we must
  - Find a value of \( x \) (a “witness”) for which \( P(x) \) holds.
  - So the proof will look like this:
    - Choose \( x = \text{<some value in } D\)>
    - Verify that the \( x \) we chose satisfies the predicate.

- Example: there is a prime number \( x \) such that \( 3^x + 2 \) is not prime.

- How do we translate **There is a prime number \( x \) such that \( 3^x + 2 \) is not prime** into predicate logic?
  - a) \( \forall x \in \mathbb{Z}^+, \text{Prime}(x) \land \neg \text{Prime}(3^x + 2) \)
  - b) \( \exists x \in \mathbb{Z}^+, \text{Prime}(x) \land \neg \text{Prime}(3^x + 2) \)
  - c) \( \forall x \in \mathbb{Z}^+, \text{Prime}(x) \rightarrow \neg \text{Prime}(3^x + 2) \)
  - d) \( \exists x \in \mathbb{Z}^+, \text{Prime}(x) \rightarrow \neg \text{Prime}(3^x + 2) \)
  - e) \( \forall x \in P, \neg \text{Prime}(3^x + 2) \) where \( P \) is the set of all primes
Module 8.1.1: Direct Proofs (existential)

- So the proof goes as follows:
  Proof:
  Choose \( x = \) 
  It is prime because its only factors are 1 and 
  Now \( 3^x + 2 = \) and 
  Hence \( 3^x + 2 \) is not prime.
  QED.

Worksheet problem 1

Theorem: There are perfect squares and perfect cubes larger than 1 that are also Fibonacci numbers.

Module 8.1.2: Direct Proofs (universal)

- Form 2: \( \forall x \in D, P(x) \)
  To prove this statement is true, we must
  - Show that \( P(x) \) holds no matter how we choose \( x \).
  - So the proof will look like this:
    Consider an unspecified element \( x \) of \( D \)
    Verify that the predicate \( P \) holds for this \( x \).
    Note: the only assumption we can make about \( x \) is the fact that it belongs to \( D \). So we can only use properties common to all elements of \( D \).
Example: every non-anonymous Racket function is at least 12 characters long.

The proof goes as follows:

Proof:
Consider an unspecified Racket function \( f \)
This function

Therefore \( f \) is at least 12 characters long.

QED

Terminology: the following statements all mean the same thing:

- Consider an unspecified element \( x \) of \( D \)
- Without loss of generality consider a valid element \( x \) of \( D \).
- Suppose \( x \) is a particular but arbitrarily chosen element of \( D \).
- Let \( x \) be an arbitrary element of \( D \).
- Let \( x \) be any element of \( D \).

Why can we write Assume that \( P(x) \) is true?

- Because these are the only cases where \( Q(x) \) matters.
- Because \( P(x) \) is preceded by a universal quantifier.
- Because we know that \( P(x) \) is true.
- Both (a) and (c)
- Both (b) and (c)
Module 8.1.2: Direct Proofs (universal)

- Example: prove that
  \( \forall n \in \mathbb{N}, \ n \geq 1024 \rightarrow 10n \leq n\log_2 n \)
- Proof:
  Consider an unspecified natural number \( n \).
  Assume that \( n \geq 1024 \).
  Then ...

Module 8.1.1: Direct Proofs (existential)

Worksheet problems 2 and 3

Theorem: Squares of odd integers are congruent to 1 modulo 4.

Theorem: For all subsets \( A, B, C \) of an arbitrary universal set \( U \), \( A \subseteq C \rightarrow A \subseteq B \cup C \)

Module 8.1.2: Direct Proofs (universal)

- Other interesting techniques for direct proofs 😊
  - Proof by intimidation
  - Proof by lack of space (Fermat's favorite!)
  - Proof by authority
  - Proof by never-ending revision

- For the full list, see:

Module 8: Proof Techniques (part 1)

- Module Summary
  - Techniques for direct proofs.
    - Existential quantifiers.
    - Universal quantifiers.
  - Dealing with nested quantifiers.
  - Indirect proofs: contrapositive and contradiction
  - Choosing a proof strategy
  - Additional Examples
Module 8.2: Dealing with nested quantifiers

- How do we deal with theorems that involve multiple quantifiers?
  - Start the proof from the outermost quantifier.
  - Work our way inwards.

Example 1:
- For any two distinct real numbers, there is a third real number that is larger than one but smaller than the other.
- Written using predicate logic:

The proof goes as follows:

Proof:
Consider two unspecified real numbers \( x \) and \( y \).
Assume without loss of generality that \( x < y \).
Choose \( z = \)
Now prove that \( x < z < y \).

Example 2:
- For every positive integer \( n \), there is a prime \( p \) that is larger than \( n \).
- Written using predicate logic:

The proof goes as follows:

Proof:
Consider an unspecified positive integer \( n \).
Choose \( p \) as follows:
Now prove that \( p > n \) and that \( p \) is prime.
Details (part 1)

How do we choose \( p \)?

First we compute \( x = n! + 1 \) (where \( n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n \)).

By the fundamental theorem of arithmetic, \( x \) can be written as a product of primes:

\[ x = p_1 \cdot p_2 \cdot \ldots \cdot p_t \]

We use any one of these as \( p \) (say \( p_1 \)). The integer \( p \) is a prime by definition.

Details (part 2).

Now we need to prove that \( p > n \).

Which of the following should we prove?

a) \( \forall i \in \mathbb{Z}^+, i \leq n \rightarrow i \) divides \( n! \)

b) \( \exists i \in \mathbb{Z}^+, i \leq n \land i \) does not divide \( x \)

c) \( \forall i \in \mathbb{Z}^+, i \leq p \rightarrow i \) does not divide \( x \)

d) \( \forall i \in \mathbb{Z}^+, (i > 1 \land i \leq n) \rightarrow i \) does not divide \( x \)

e) None of the above.

Details (part 3).

Now the proof:

Pick an unspecified integer \( 2 \leq i \leq n \).

Observe that

\[
\frac{x}{i} = \frac{n! + 1}{i} = \frac{n!}{i} + \frac{1}{i} = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (i-1) \cdot (i+1) \cdot \ldots \cdot n + \frac{1}{i}
\]

Since \( 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (i-1) \cdot (i+1) \cdot \ldots \cdot n \) is an integer, but \( 1/i \) is not an integer, this means that \( x/i \) is not an integer.

Hence \( i \) does not divide \( x \).

Therefore no integer from \( 2 \) to \( n \) is a factor of \( x \). Since \( p \) is a factor of \( x \), this means that \( p > n \).

Worksheet problems 4 and 5

Theorem: Every positive, odd integer is the difference between two perfect squares.

\[ n^2 + 3n + 5 \in O(n^2) \]

Recall: \( f \in O(g) \) if \( \exists c \in \mathbb{R}^+, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \rightarrow f(n) \leq cg(n). \)
Module 8: Proof Techniques (part 1)

- Module Summary
  - Techniques for direct proofs.
    - Existential quantifiers.
    - Universal quantifiers.
  - Dealing with nested quantifiers.
  - Indirect proofs: contrapositive and contradiction
  - Choosing a proof strategy
  - Additional Examples

Module 8.3: Indirect Proofs

- Consider the following theorem:
  If the square of a positive integer $n$ is even, then $n$ is even.

- How can we prove this?
  - Let's try a direct proof.

  Consider an unspecified integer $n$.
  Assume that $n^2$ is even.
  So $n^2 = 2k$ for some (positive) integer $k$.
  Hence $n = \sqrt{2k}$.
  Then what?

- What is the relationship between
  If a positive integer $n$ is odd, then its square is odd.
  and
  If the square of a positive integer $n$ is even, then $n$ is even.
  and hence

  Therefore $n^2$ is odd.
### Module 8.3: Indirect Proofs

- **We would normally write the proof of the original theorem like this:**

  **Proof:** we will prove the contrapositive, that is, that if a positive integer \( n \) is odd, then its square is odd. Consider an unspecified positive integer \( n \).

  ...

- **Another proof technique:** *Proofs by contradiction.*

  - **To prove:**
    
    Premise 1
    
    ...  
    
    Premise \( n \)
    
    \( \therefore \) Conclusion

  - We assume Premise 1, ..., Premise \( n \), \( \sim \)Conclusion and then derive a contradiction (\( p \land \sim p \), \( x \) is odd \( \land \) \( x \) is even, \( x < 5 \land x > 10 \), etc).

  - We then conclude that Conclusion is true.

### Module 8.3: Indirect Proofs

- **Why are proofs by contradiction a valid proof technique?**
  - We proved

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \land \) \( \sim \)Conclusion \( \rightarrow \) F

  - This is only true if

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \land \) \( \sim \)Conclusion \( \equiv \) F

  - If

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \equiv \) F

    then

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \rightarrow \) Conclusion

    is true.

  - Otherwise

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \equiv \) T

    but

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \land \) \( \sim \)Conclusion \( \equiv \) F

    therefore

    \( \sim \)Conclusion \( \equiv \) F which means that Conclusion \( \equiv \) T

    and so

    Premise 1 \( \land \) ... \( \land \) Premise \( n \) \( \rightarrow \) Conclusion

    is true.
Module 8.3: Indirect Proofs

- Example:
  Not every CPSC 121 student got an above average grade on midterm 1.
- What are:
  - The premise(s)?
  - The negated conclusion?
- Let us prove this theorem together.

Module 8.1.1: Direct Proofs (existential)

Worksheet problems 6 and 7

**Theorem:** For all real numbers \( x \) and \( y \), if \( x \) is a rational number, and \( y \) is an irrational number, then \( x+y \) is irrational.

**Theorem:** There do not exist two positive integers \( x \) and \( y \) such that \( x^2 - 3xy - 10y^2 = 9 \).

Module 8: Proof Techniques (part 1)

**Module Summary**
- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- Dealing with nested quantifiers.
- Indirect proofs: contrapositive and contradiction
- Choosing a proof strategy
- Additional Examples

Module 8.4: Choosing a proof strategy

- How should you tackle a proof?
  - Try the simpler methods first:
    - Witness proofs (if applicable).
    - Direct proofs.
    - Indirect proof using the contrapositive.
    - Proof by contradiction.
  - If you don't know if the theorem is true:
    - Alternate between trying to prove and disprove it.
    - Use a failed attempt at one to help with the other.
Module 8.4: Choosing a proof strategy

How should you tackle a proof (continued)?

- If you get stuck, try looking backwards from the conclusion you want.
  - But don't forget the argument must eventually be written from the premises to the conclusion (not the other way around).
- Try to derive all new facts you can derive from the premises without worrying about whether or not they will help.
- If you are really stuck, ask for help!

Module 8: Proof Techniques (part 1)

- Module Summary
  - Techniques for direct proofs.
    - Existential quantifiers.
    - Universal quantifiers.
  - Dealing with nested quantifiers.
  - Indirect proofs: contrapositive and contradiction
  - Additional Examples

Module 8.5: Additional examples

- Additional theorems you might wish to prove:
  - Prove that for every positive integer $x$, either $\sqrt{x}$ is an integer, or it is irrational.
  - Prove that any circuit consisting of NOT, OR, AND and XOR gates can be implemented using only NOR gates.
Module 8.5: Additional examples

- Additional theorems you might wish to prove:
  - Prove that if \( a, b \) and \( c \) are integers, and \( a^2 + b^2 = c^2 \), then at least one of \( a \) and \( b \) is even. Hint: use a proof by contradiction, and show that \( 4 \) divides both \( c^2 \) and \( c^2 - 2 \).
  - Prove that there is a positive integer \( c \) such that \( x + y \leq c \cdot \max\{ x, y \} \) for every pair of positive integers \( x \) and \( y \).