"Yes, yes, I know that, Sidney... everybody knows that!... But look: Four wrongs squared, minus two wrongs to the fourth power, divided by this formula, do make a right."

cozy cs.

\[ 13 - 1 \]

\[ \frac{A, A \rightarrow B}{... B} \]
Last class: Inference Rules for Quantifiers

** c is a NEW name.
List all dependencies for c.

dependencies:
other named arbitrary constants in $\exists x \ P(x)$

```
Intro $\exists$  
\[ P(c) \text{ for some } c \] 
\[ \therefore \exists x \ P(x) \]

Elim $\forall$  
\[ \forall x \ P(x) \] 
\[ \therefore P(a) \text{ (for any } a) \]
```

```
Elim $\exists$  
\[ \exists x \ P(x) \] 
\[ \therefore P(c) \text{ for some special }* \ast \ast \ c \]

Intro $\forall$  
\[ \exists x \ P(x) \] 
\[ \therefore \forall x \ P(x) \]
```


dependencies: other named arbitrary constants in $\exists x \ P(x)$

* in the domain of P. No other name in P depends on a.
Prove “The sum of two odd numbers is even.”

Let \( x \) and \( y \) be arbitrary integers.

Suppose that both are odd.

Then, we have \( x = 2a+1 \) for some integer \( a \) and \( y = 2b+1 \) for some integer \( b \).

Their sum is \( x+y = \ldots = 2(a+b+1) \)

so \( x+y \) is, by definition, even.

Since \( x \) and \( y \) were arbitrary, the sum of two odd integers is even.
Prove “The sum of two odd numbers is even.”

Proof: Let \( x \) and \( y \) be arbitrary integers.

Suppose that both are odd. Then, we have \( x = 2a + 1 \) for some integer \( a \) and \( y = 2b + 1 \) for some integer \( b \). Their sum is \( x + y = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1) \), so \( x + y \) is, by definition, even.

Since \( x \) and \( y \) were arbitrary, the sum of any two odd integers is even. 

\[
\forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))
\]
A real number $x$ is *rational* iff there exist integers $a$ and $b$ with $b \neq 0$ such that $x = a/b$.

\[ \text{Rational}(x) := \exists a \exists b \left( \left( \text{Integer}(a) \land \text{Integer}(b) \right) \land \left( x = a/b \right) \land b \neq 0 \right) \]
Rationality

Predicate Definitions

\[
\text{Rational}(x) := \exists a \ \exists b \ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))
\]

Prove: “The product of two rationals is rational.”

Formally, prove \( \forall x \ \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \)

\[
\text{Let } x \text{ and } y \text{ be arbitrary real numbers.}
\]

\[
\text{Assume } x \text{ and } y \text{ are rational.}
\]

\[
\therefore xy \text{ is rational.}
\]

\[
\text{Since } x \text{ and } y \text{ are arbitrary real numbers, this proves the statement.}
\]
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let \( x \) and \( y \) be arbitrary reals.
Suppose \( x \) and \( y \) are rational.

Thus, \( xy \) is rational.

Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. \( \square \)

\[ \forall x \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \]
Rationality

Proof: “The product of two rationals is rational.”

Proof: Let \( x \) and \( y \) be arbitrary rationals.

Thus, \( xy \) is rational.

Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. ■

\[ \forall x \, \forall y \, ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \]
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let x and y be arbitrary rationals. Then, x = a/b for some integers a, b, where b\(\neq 0\), and y = c/d for some integers c, d, where d\(\neq 0\).

Thus, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

\(\forall x \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy))\)
Prove: “The product of two rationals is rational.”

Proof: Let $x$ and $y$ be arbitrary rationals. Then, $x = a/b$ for some integers $a$, $b$, where $b \neq 0$, and $y = c/d$ for some integers $c$, $d$, where $d \neq 0$.

By definition, then, $xy$ is rational. Since $x$ and $y$ were arbitrary, we have shown that the product of any two rationals is rational. ■

$\forall x \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy))$
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let x and y be arbitrary rationals. Then, x = a/b for some integers a, b, where b ≠ 0, and y = c/d for some integers c, d, where d ≠ 0. Multiplying, we get that xy = (a/b)(c/d) = (ac)/(bd).

By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. □

∀x ∀y ((Rational(x) ∧ Rational(y)) → Rational(xy))
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let \( x \) and \( y \) be arbitrary rationals.
Then, \( x = a/b \) for some integers \( a, b \), where \( b \neq 0 \), and \( y = c/d \) for some integers \( c, d \), where \( d \neq 0 \).
Multiplying, we get that \( xy = (a/b)(c/d) = (ac)/(bd) \).
\( ac \) and \( bd \) are integers. Also, since \( b \neq 0 \) and \( d \neq 0 \) we have \( bd \neq 0 \). By definition, then, \( xy \) is rational.
Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. 

\[ \forall x \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \]
English Proofs

- **High-level language lets us work more quickly**
  - should not be necessary to spill out every detail
  - examples so far
    - skipping Intro ∧ and Elim ∧ (and hence, Commutativity and Associativity)
    - skipping Double Negation
    - not stating existence claims (immediately apply Elim ∃ to name the object)
    - not stating that the implication has been proven ("Suppose X... Thus, Y." says it already)
  - (list will grow over time)

- **English proof is correct if the reader is convinced they could translate it into a formal proof**
  - the reader is the “compiler” for English proofs
Proof Strategies
Proof Strategies: Counterexamples

To prove \( \neg \forall x \ P(x) \), prove \( \exists \neg P(x) \):

- Equivalent by De Morgan’s Law
- All we need to do that is find an \( x \) where \( P(x) \) is false
- This example is called a counterexample to \( \forall x \ P(x) \).

e.g. Prove “Not every prime number is odd”

Proof: 2 is a prime that is not odd — a counterexample to the claim that every prime number is odd.

An English proof does not need to cite De Morgan’s law.
Proof Strategies: Proof by Contrapositive

If we assume \( \neg q \) and derive \( \neg p \), then we have proven \( \neg q \rightarrow \neg p \), which is equivalent to proving \( p \rightarrow q \).

1. **Assumption**
   - \( \neg q \)

   ... 

1.3. \( \neg p \)

1. \( \neg q \rightarrow \neg p \) Direct Proof
2. \( p \rightarrow q \) Contrapositive: 1
Proof Strategies: Proof by Contrapositive

If we assume \( \neg q \) and derive \( \neg p \), then we have proven \( \neg q \rightarrow \neg p \), which is equivalent to proving \( p \rightarrow q \).

We will prove the contrapositive.

Suppose \( \neg q \).

\[ 1.1. \quad \neg q \quad \text{Assumption} \]

\[ 1.3. \quad \neg p \]

Thus, \( \neg p \).

\[ 1. \quad \neg q \rightarrow \neg p \quad \text{Direct Proof} \]

\[ 2. \quad p \rightarrow q \quad \text{Contrapositive: 1} \]
Proof by Contradiction: One way to prove $p$

If we assume $\neg p$ and derive $F$ (a contradiction), then we have proven $p$.

1. $\neg p$ Assumption
   
   ... 

1.3. $F$

1. $\neg p \rightarrow F$ Direct Proof
2. $\neg \neg p \lor F$ Law of Implication: 1
3. $p \lor F$ Double Negation: 2
4. $p$ Identity: 3
Proof Strategies: Proof by Contradiction

If we assume \( \neg p \) and derive \( F \) (a contradiction), then we have proven \( p \).

We will argue by contradiction.

Suppose \( \neg p \).  

\[ 1.1. \quad \neg p \quad \text{Assumption} \]

\[ 1.3. \quad F \]

1. \( \neg p \rightarrow F \)  \quad \text{Direct Proof}
2. \( \neg
\neg p \lor F \)  \quad \text{Law of Implication: 1}
3. \( p \lor F \)  \quad \text{Double Negation: 2}
4. \( p \)  \quad \text{Identity: 3}

Often, we will infer \( \neg R \), where \( R \) is a prior fact.
Putting these together, we have \( R \land \neg R \equiv F \).
Prove: “No integer is both even and odd.”

Formally, prove $\neg \exists x \ (\text{Even}(x) \land \text{Odd}(x))$

Proof: We will argue by contradiction.
Prove: “No integer is both even and odd.”

Formally, prove \( \neg \exists x (\text{Even}(x) \land \text{Odd}(x)) \)

Proof: We will argue by contradiction.

Suppose that \( x \) is an integer that is both even and odd.

This is a contradiction. ■
Even and Odd

Prove: “No integer is both even and odd.”

Formally, prove \( \neg \exists x (\text{Even}(x) \land \text{Odd}(x)) \)

Proof: We will argue by contradiction.
Suppose that \( x \) is an integer that is both even and odd. Then, \( x=2a \) for some integer \( a \), and \( x=2b+1 \) for some integer \( b \).

This is a contradiction. ■
Prove: “No integer is both even and odd.”

Formally, prove $\neg \exists x (\text{Even}(x) \land \text{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that $x$ is an integer that is both even and odd. Then, $x=2a$ for some integer $a$, and $x=2b+1$ for some integer $b$. This means $2a=x=2b+1$ and hence $2a-2b=1$ and so $a-b=\frac{1}{2}$. But $a-b$ is an integer while $\frac{1}{2}$ is not, so they cannot be equal. This is a contradiction. ■

Formally, we’ve shown $\text{Integer}(\frac{1}{2}) \land \neg \text{Integer}(\frac{1}{2}) \equiv F.$
Proof by Cases

On Homework 3, Task 1 you are asked to show:

- Given \( p \to r \) and \( \neg p \to r \) derive \( r \)
- Given \( p \lor q, p \to r \) and \( q \to r \) derive \( r \)

This will mean that...

If we prove \( p \to r \) and \( \neg p \to r \) then we have proven \( r \).

If we prove \( p \lor q, p \to r \) and \( q \to r \) then we have proven \( r \).
Strategies

• Simple proof strategies already do a lot
  – counter examples
  – proof by contrapositive
  – proof by contradiction
  – proof by cases

• Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)
Applications of Predicate Logic

- Remainder of the course will use predicate logic to prove important properties of interesting objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

- Encode domain knowledge in predicate definitions
- Then apply predicate logic to infer useful results

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>( \text{Even}(x) \equiv \exists y \ (x = 2 \cdot y) )</td>
</tr>
<tr>
<td></td>
<td>( \text{Odd}(x) \equiv \exists y \ (x = 2 \cdot y + 1) )</td>
</tr>
</tbody>
</table>
Number Theory
Number Theory (and applications to computing)

• Branch of Mathematics with direct relevance to computing

• Many significant applications
  – Cryptography & Security ✔
  – Data Structures
  – Distributed Systems

• Important toolkit
Modular Arithmetic

- Arithmetic over a finite domain
- Almost all computation is over a finite domain
I'm ALIVE!

```java
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println("I will be alive for at least "+
                         SEC_IN_YEAR * 101 + " seconds."
        );
    }
}
```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println("I will be alive for at least "+
                        SEC_IN_YEAR * 101 + " seconds.");
    }
}

---jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

---jGRASP: operation complete.
Divisibility

Definition: “b divides a”

For $a, b$ with $b \neq 0$:

$b \mid a \iff \exists q (a = qb)$

Check Your Understanding. Which of the following are true?

- $5 \mid 1$
- $25 \mid 5$
- $5 \mid 0$
- $3 \mid 2$
- $1 \mid 5$
- $5 \mid 25$
- $0 \mid 5$
- $2 \mid 3$

$\square = \text{True}$

$\times = \text{False}$
Divisibility

Definition: “b divides a”

For $a, b$ with $b \neq 0$:

$b \mid a \iff \exists q (a = qb)$

Check Your Understanding. Which of the following are true?

<table>
<thead>
<tr>
<th>5</th>
<th>1</th>
<th>25</th>
<th>5</th>
<th>5</th>
<th>0</th>
<th>3</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>1 iff 1 = 5k</td>
<td>25</td>
<td>5 iff 5 = 25k</td>
<td>5</td>
<td>0 iff 0 = 5k</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>5 iff 5 = 1k</td>
<td>5</td>
<td>25 iff 25 = 5k</td>
<td>0</td>
<td>5 iff 5 = 0k</td>
<td>2</td>
</tr>
</tbody>
</table>

Domain of Discourse
Integers
For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b | a$, then, by definition, we have $a = qb$ for some $q$. The number $q$ is called the **quotient**.

Dividing both sides by $b$, we can write this as

$$\frac{a}{b} = q$$

(We want to stick to integers, though, so we’ll write $a = qb$.)
Recall: Elementary School Division

For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b \nmid a$, then we end up with a remainder $r$ with $0 < r < b$. Now,

\[
\frac{a}{b} = q \quad \text{we have} \quad \frac{a}{b} = q + \frac{r}{b}
\]

Multiplying both sides by $b$ gives us

\[a = qb + r\]

(A bit nicer since it has no fractions.)
Recall: Elementary School Division

For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b \mid a$, then we have $a = q b$ for some $q$.  
If $b \not\mid a$, then we have $a = q b + r$ for some $q, r$ with $0 < r < b$.

In general, we have $a = q b + r$ for some $q, r$ with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.  

0 1 2 3
**Division Theorem**

<table>
<thead>
<tr>
<th>Division Theorem</th>
<th>$-3 = \boxed{-2 \cdot 2 + 1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>For $a, b$ with $b &gt; 0$</td>
<td>there exist <em>unique</em> integers $q, r$ with $0 \leq r &lt; b$ such that $a = qb + r$.</td>
</tr>
</tbody>
</table>

To put it another way, if we divide $b$ into $a$, we get a unique quotient $q = a \div b$ and non-negative remainder $r = a \mod b$.

Note: $r \geq 0$ even if $a < 0$. Not quite the same as $a \% b$. 

Domain of Discourse

Integers
To put it another way, if we divide $b$ into $a$, we get a unique quotient $q = a \text{ div } b$ and non-negative remainder $r = a \text{ mod } b$.
**div and mod**

\[ x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7) \]