CSE 311: Foundations of Computing

Topic 2: Proofs

Logical Inference

- So far, we've considered:
  - how to understand and *express* things using propositional and predicate logic
  - how to *compute* using Propositional logic (circuits)
  - how to show that different ways of expressing or computing them are *equivalent* to each other

- Logic also has methods that let us *infer* implied properties from ones that we know
  - equivalence is a small part of this

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	
T	F	T	
F	T	F	
F	F	F	

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	T
T	F	T	T
F	T	F	
F	F	F	

Given that A is true, we see that B is also true.

$$A \Rightarrow B$$

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	T
T	F	T	T
F	T	F	?
F	F	F	?

When we zoom out, what have we proven?

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	*q*	A(*p*,*q*)	B(*p*,*q*)	A → B
T	T	T	T	T
T	F	T	T	T
F	T	F	T	T
F	F	F	F	T

When we zoom out, what have we proven?

$$(A \rightarrow B) \equiv \mathbf{T}$$

New Perspective

Equivalences

$A \equiv B$ and $(A \leftrightarrow B) \equiv T$ are the same

Inference

$A \Rightarrow B$ and $(A \rightarrow B) \equiv T$ are the same

Proofs

- Start with given facts (hypotheses)
- Use rules of inference to extend set of facts
- Result is proved when it is included in the set

An inference rule: *Modus Ponens*

- If A and $A \rightarrow B$ are both true, then B must be true
- Write this rule as $\dfrac{A \;;\; A \rightarrow B}{\therefore\ B}$
- Given:
  - If it is Friday, then you have a 311 lecture today.
  - It is Friday.
- Therefore, by Modus Ponens:
  - You have a 311 lecture today.

My First Proof!

Show that r follows from p, $p \rightarrow q$, and $q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	$q \rightarrow r$	Given
4.		
5.		

Modus Ponens $\dfrac{A \; ; \; A \rightarrow B}{\therefore \; B}$

My First Proof!

Show that r follows from p, $p \rightarrow q$, and $q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	$q \rightarrow r$	Given
4.	q	MP: 1, 2
5.	r	MP: 4, 3

Modus Ponens $\dfrac{A \; ; \; A \rightarrow B}{\therefore \; B}$

Proofs can use equivalences too

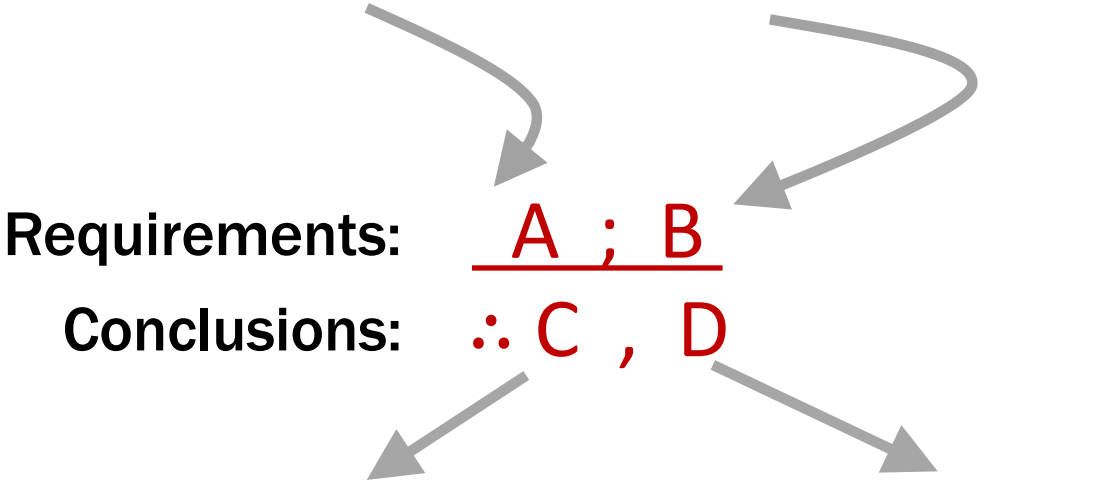
Show that ¬p follows from p → q and ¬q

1.	$p \rightarrow q$	Given
2.	$\neg q$	Given
3.	$\neg q \rightarrow \neg p$	Contrapositive: 1
4.	$\neg p$	MP: 2, 3

Modus Ponens $\dfrac{A \; ; \; A \rightarrow B}{\therefore \; B}$

Inference Rules

If A is true and B is true ....

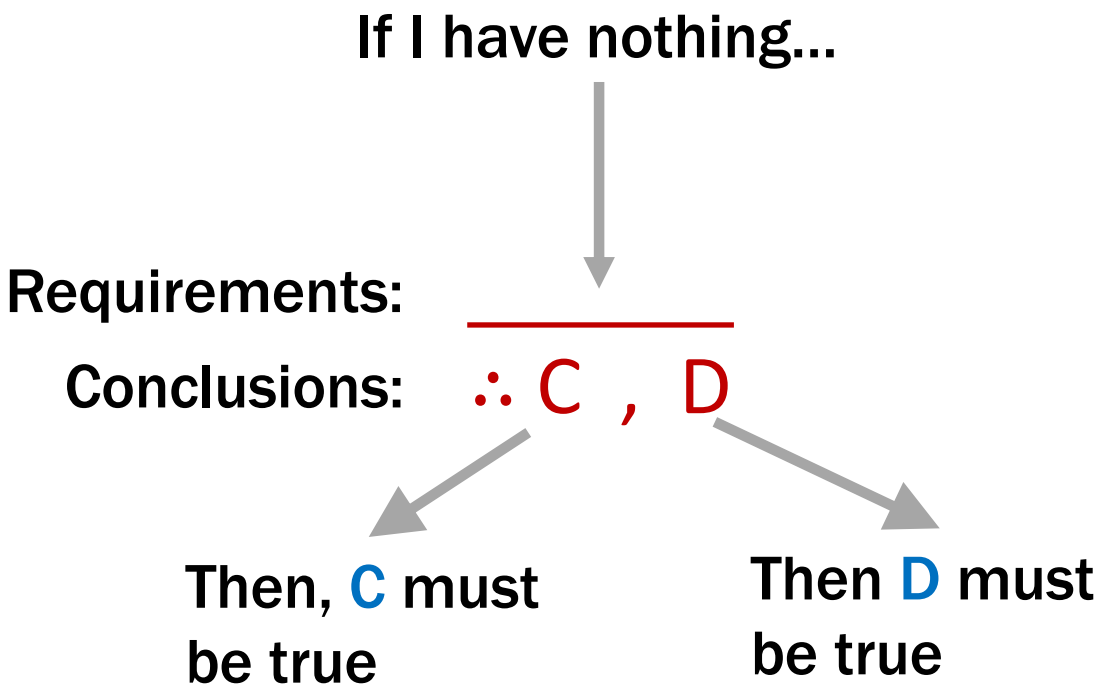


Example (Modus Ponens):

$$\frac{A \;;\; A \rightarrow B}{\therefore \quad B}$$

If I have A and $A \rightarrow B$ both true, Then B must be true.

Axioms: Special inference rules



Example (Excluded Middle):

$$\frac{}{\therefore\ A \vee \neg A}$$

$A \vee \neg A$ must be true.

Simple Propositional Inference Rules

Two inference rules per binary connective, one to eliminate it and one to introduce it

Elim $\wedge$

$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro $\wedge$

$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim $\vee$

$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro $\vee$

$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Proofs

Show that r follows from $p, p \to q,$ and $p \wedge q \to r$

How To Start:

We have givens, find the ones that go together and use them. Now, treat new things as givens, and repeat.

$$\frac{A \;;\; A \to B}{\therefore\ B}$$

$$\frac{A \wedge B}{\therefore\ A,\ B}$$

$$\frac{A \;;\; B}{\therefore\ A \wedge B}$$

Proofs

Show that r follows from $p, p \to q,$ and $p \wedge q \to r$

1.	p	Given
2.	$p \to q$	Given
3.	$p \wedge q \to r$	Given

$$\frac{A \;;\; A \to B}{\therefore\ B}$$

$$\frac{A \wedge B}{\therefore\ A,\ B}$$

$$\frac{A \;;\; B}{\therefore\ A \wedge B}$$

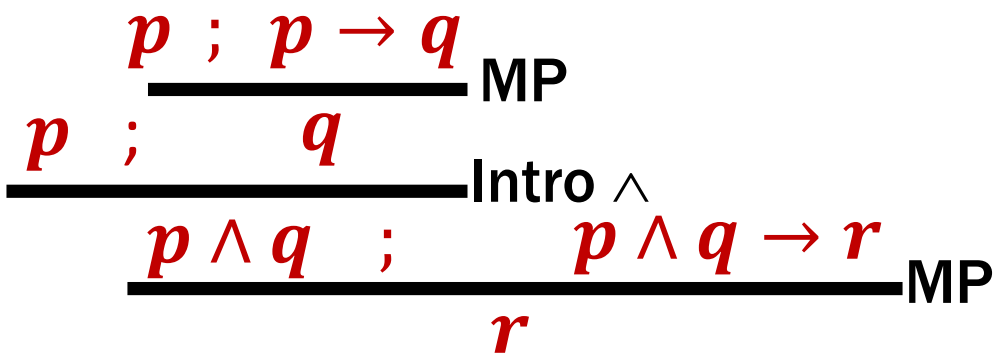
Proofs

Show that r follows from $p, p \rightarrow q,$ and $p \wedge q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	$p \wedge q \rightarrow r$	Given
4.	q	MP: 1, 2
5.	$p \wedge q$	Intro $\wedge$: 1, 4
6.	r	MP: 5, 3

Proofs

Show that r follows from $p, p \rightarrow q$, and $p \wedge q \rightarrow r$



Proofs

Show that r follows from $p, p \to q$, and $p \wedge q \to r$

1.	p	Given
2.	$p \to q$	Given
3.	q	MP: 1, 2
4.	$p \wedge q$	Intro $\wedge$: 1, 3
5.	$p \wedge q \to r$	Given
6.	r	MP: 4, 5

Two visuals of the same proof. We will use the right one, but if the bottom one helps you think about it, that's great!

$$\dfrac{\dfrac{p \quad ; \quad \dfrac{p \quad ; \quad p \to q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro}\,\wedge \quad ; \quad p \wedge q \to r}{r}\,\text{MP}$$

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given

First: Write down givens and goal

20. $\neg r$?

Idea: Work backwards!

Proofs

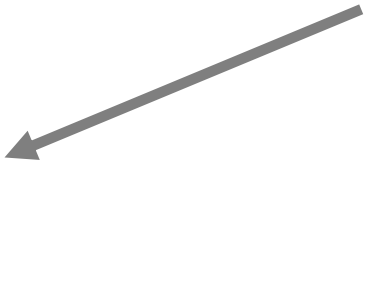
Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given

Idea: Work backwards!

We want to eventually get $\neg r$. How?

- We can use $q \rightarrow \neg r$ to get there.
- The justification between 2 and 20 looks like "elim →" which is MP.



20. $\neg r$ MP: 2, ?

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given

Idea: Work backwards!

We want to eventually get $\neg r$. How?

- Now, we have a new "hole"
- We need to prove q...
  - Notice that at this point, if we prove q, we've proven $\neg r$...

19.	q	?
20.	$\neg r$	MP: 2, 19

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
19.	q	?
20.	$\neg r$	MP: 2, 19

This looks like or-elimination.

Elim ∨ $\dfrac{A \vee B \; ; \; \neg A}{\therefore B}$

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given

18.	$\neg\neg s$	
19.	q	∨ Elim: 3, 18
20.	$\neg r$	MP: 2, 19

$\neg\neg s$ doesn't show up in the givens but s does and we can use equivalences

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	?
18.	$\neg\neg s$	Double Negation: 17
19.	q	Elim ∨: 3, 18
20.	$\neg r$	MP: 2, 19

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	Elim ∧: 1
18.	$\neg\neg s$	Double Negation: 17
19.	q	Elim ∨: 3, 18
20.	$\neg r$	MP: 2, 19

No holes left! We just need to clean up a bit.

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
4.	s	Elim ∧: 1
5.	$\neg\neg s$	Double Negation: 4
6.	q	Elim ∨: 3, 5
7.	$\neg r$	MP: 2, 6

Important: Applications of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.

  e.g. $(p \rightarrow r) \vee q \equiv (\neg p \vee r) \vee q$

- Inference rules only can be applied to whole formulas (not correct otherwise).

  e.g. 1. $p \rightarrow r$ given

  ~~2. $(p \vee q) \rightarrow r$ intro $\vee$ from 1.~~

  Does not follow! e.g . p=F, q=T, r=F

Recall: Propositional Inference Rules

Two inference rules per binary connective, one to eliminate it and one to introduce it

Elim $\wedge$

$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro $\wedge$

$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim $\vee$

$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro $\vee$

$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Not like other rules

To Prove An Implication: $A \rightarrow B$

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

- We use the direct proof rule
- The "pre-requisite" $A \Rightarrow B$ for the direct proof rule is a **proof** that "**Assuming** A, we can prove B."
- **The direct proof rule:**

  If you have such a proof, then you can conclude that $A \rightarrow B$ is true

Proofs using the direct proof rule

Show that p $\rightarrow$ r follows from q and (p $\wedge$ q) $\rightarrow$ r

1. q Given
2. $(p \wedge q) \rightarrow r$ Given
   - 3.1. p Assumption
   - 3.2.
   - 3.3. r ??
3. $p \rightarrow r$ Direct Proof

This is a proof of $p \rightarrow r$

If we know p is true...
Then, we've shown
r is true

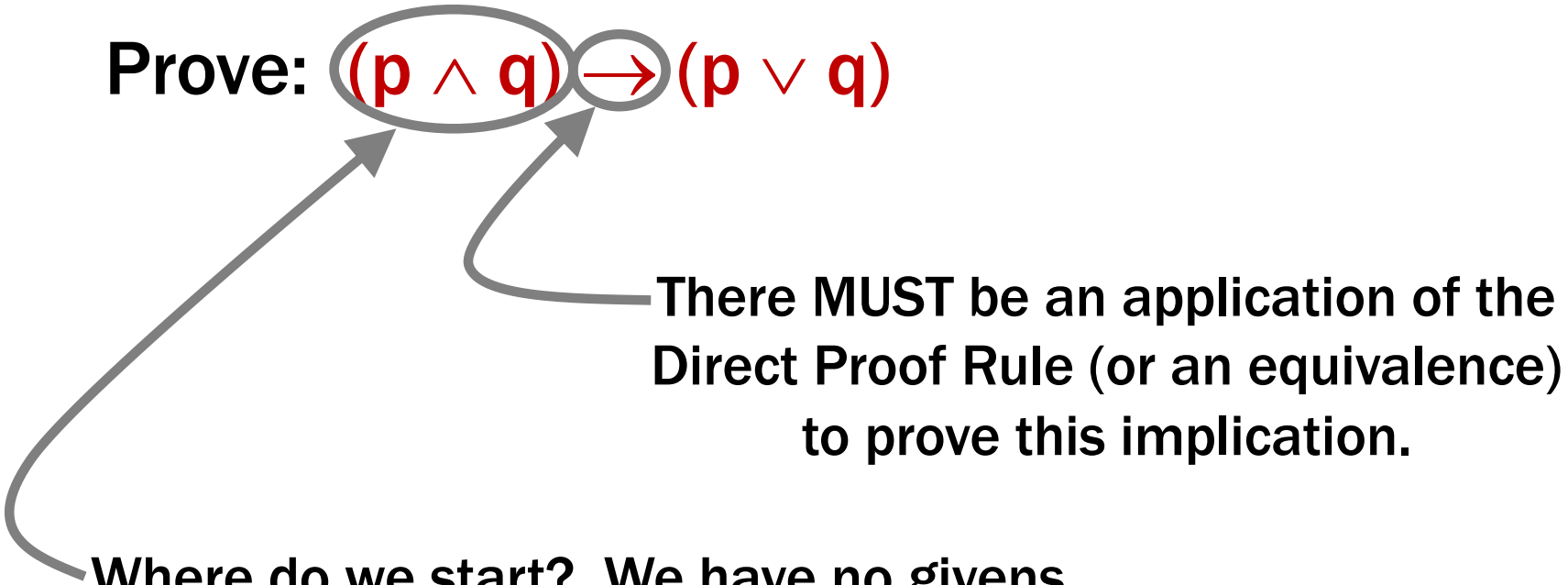
Proofs using the direct proof rule

Show that p $\rightarrow$ r follows from q and (p $\wedge$ q) $\rightarrow$ r

1. q Given
2. $(p \wedge q) \rightarrow r$ Given
    - 3.1. p Assumption
    - 3.2. $p \wedge q$ Intro $\wedge$: 1, 3.1
    - 3.3. r MP: 2, 3.2
3. $p \rightarrow r$ Direct Proof

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$



Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1. $p \wedge q$ Assumption

1.9. $p \vee q$??

1. $(p \wedge q) \rightarrow (p \vee q)$ Direct Proof

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.2.	p	Elim $\wedge$: 1.1
1.3.	$p \vee q$	Intro $\vee$: 1.2
1.	$(p \wedge q) \rightarrow (p \vee q)$	Direct Proof

Our General Proof Strategy

1. Use **introduction** rules to see how you would build **up** the formula you want to prove from pieces of what is given

2. Use **elimination** rules to break **down** the given formulas to get the pieces you need to do 1.

3. Write the proof beginning with what you figured out for 2 followed by 1.

Our General Proof Strategy

1. $p \to q$ Given
2. p Given

...

?. $(p \vee r) \wedge q$?

Use **elimination** rules to move **down**

Our General Proof Strategy

1. $p \to q$	Given
2. p	Given
3. q	MP: 2, 1
…	
?. $(p \vee r) \wedge q$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $p \to q$ Given
2. p Given
3. q MP: 2, 1

Use **elimination** rules to move **down**

...

?. $p \vee r$

?. q

?. $(p \vee r) \wedge q$ Intro $\wedge$

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $p \rightarrow q$ Given
2. p Given

...

?. $p \vee r$ Intro $\vee$??

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro $\vee$ (**must** wait until you know which one is true)

Our General Proof Strategy

1. $p \to q$	Given	
2. p	Given	
…		
?. r	?	
?. $p \vee r$	Intro ∨	

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ (**must** wait until you know which one is true)

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1. $(p \rightarrow q) \wedge (q \rightarrow r)$ Assumption

1.? $p \rightarrow r$

1. $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ Direct Proof

Example

Prove: $((p \to q) \wedge (q \to r)) \to (p \to r)$

1.1.	$(p \to q) \wedge (q \to r)$	Assumption
1.2.	$p \to q$	Elim ∧: 1.1
1.3.	$q \to r$	Elim ∧: 1.1

1.? $p \to r$

1. $\big((p \to q) \wedge (q \to r)\big) \to (p \to r)$ Direct Proof

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1. $(p \rightarrow q) \wedge (q \rightarrow r)$ Assumption

1.2. $p \rightarrow q$ Elim ∧: 1.1

1.3. $q \rightarrow r$ Elim ∧: 1.1

1.4.1. p Assumption

1.4.? r

1.4. $p \rightarrow r$ Direct Proof

1. $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ Direct Proof

Example

Prove: $((p \to q) \wedge (q \to r)) \to (p \to r)$

1.1.	$(p \to q) \wedge (q \to r)$	Assumption
1.2.	$p \to q$	Elim ∧: 1.1
1.3.	$q \to r$	Elim ∧: 1.1
1.4.1.	p	Assumption
1.4.2.	q	MP: 1.2, 1.4.1
1.4.3.	r	MP: 1.3, 1.4.2
1.4.	$p \to r$	Direct Proof
1.	$\big((p \to q) \wedge (q \to r)\big) \to (p \to r)$	Direct Proof

Applications of Logical Inference

- Software Engineering
  - Express desired properties of program as set of logical constraints
  - Use inference rules to show that program implies that those constraints are satisfied
- Artificial Intelligence
  - Automated reasoning
- Algorithm design and analysis
  - e.g., Correctness, Loop invariants.
- Logic Programming, e.g. Prolog
  - Express desired outcome as set of constraints
  - Automatically apply logic inference to derive solution

Minimal Rules for Propositional Logic

Can get away with just these:

Elim ∧

$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro ∧

$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim ∨

$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro ∨

$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Excluded Middle

$$\frac{}{\therefore A \vee \neg A}$$

Note: only **this** tautology

Rules for Propositional Logic *with Tautology*

More rules makes proofs easier

Elim ∧

$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro ∧

$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim ∨

$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro ∨

$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Tautology

$$\frac{A \equiv T}{\therefore A}$$

Equivalent

$$\frac{A \equiv B\ ;\ B}{\therefore A}$$

any known

Proof by Cases

Some rules can be written in different ways

- **e.g., two different elimination rules for "∨"**

$$\text{Elim } \vee \quad \frac{A \vee B \; ; \; \neg A}{\therefore B}$$

$$\text{Cases} \quad \frac{A \vee B \; ; \; A \rightarrow C \; ; \; B \rightarrow C}{\therefore C}$$

second rule is more useful

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$ Given

Cases $\dfrac{A \vee B \; ; \; A \rightarrow C \; ; \; B \rightarrow C}{\therefore C}$

4. P ?

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \rightarrow P$	?
3. $(P \wedge Q) \rightarrow P$	?
4. P	Cases: 1, 2, 3

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$ — Given

2. $P \rightarrow P$ — Direct Proof

   3.1. $P \wedge Q$ — Assumption

   3.?. P — ?

3. $(P \wedge Q) \rightarrow P$ — Direct Proof

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof
4. P	Cases: 1, 2, 3

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2.1. P	Assumption
2.?. P	?
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2.1. P	Assumption
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof
4. P	Cases: 1, 2, 3

More Rules for Propositional Logic

More rules makes proofs easier

Principium Contradictionis

$$\frac{\neg A \; ; \; A}{\therefore F}$$

Reductio Ad Absurdum

$$\frac{B \Longrightarrow F}{\therefore \neg B}$$

Ex Falso Quodlibet

$$\frac{F}{\therefore A}$$

Ad Litteram Verum

$$\frac{}{\therefore T}$$

useful for proving things
(and necessary without the Tautology rule)

Rules for Propositional Logic *w/o Tautology*

	Elimination	Introduction
$\wedge$	Elim $\wedge$	Intro $\wedge$
$\vee$	Cases	Intro $\vee$
$\rightarrow$	Modus Ponens	Direct Proof
$\neg$	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

Recall: Important Equivalences

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $\boxed{p \vee \neg p \equiv \mathrm{T}}$
  - $p \wedge \neg p \equiv \mathrm{F}$

Does not follow from Latin rules

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$ Given

6. $(P \wedge Q) \vee (P \wedge R)$?

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1.	$P \wedge (Q \vee R)$	Given
2.	P	Elim ∧: 1
3.	$Q \vee R$	Elim ∧: 1

hint: proof by cases

6.	$(P \wedge Q) \vee (P \wedge R)$	?

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4.1. Q	Assumption
4.?. $(P \wedge Q) \vee (P \wedge R)$	?
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim ∧: 1
3. $Q \vee R$	Elim ∧: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro ∧: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro $\wedge$: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro $\vee$: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5.1. R	Assumption
5.3. $(P \wedge Q) \vee (P \wedge R)$	?
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim ∧: 1
3. $Q \vee R$	Elim ∧: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro ∧: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5.1. R	Assumption
5.2. $P \wedge R$	Intro ∧: 2, 5.1
5.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 5.2
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$ Given

4. $\neg(\boldsymbol{A} \vee \boldsymbol{B})$?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1.	$\neg A \wedge \neg B$	Given
2.	$\neg A$	Elim ∧: 1
3.	$\neg B$	Elim ∧: 1

hint: proof by contradiction

4.	$\neg(A \vee B)$	?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$ — Given
2. $\neg A$ — Elim ∧: 1
3. $\neg B$ — Elim ∧: 1

Reductio Ad Absurdum

$$\frac{A \Rightarrow F}{\therefore \neg A}$$

4. $\neg(A \vee B)$ — Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$ — Given
2. $\neg A$ — Elim ∧: 1
3. $\neg B$ — Elim ∧: 1
   - 4.1. $A \vee B$ — Assumption

can we work forward?

   - 4.4. $\mathbf{F}$ — ?
4. $\neg(A \vee B)$ — Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2. $A \rightarrow \mathrm{F}$	?
4.3. $B \rightarrow \mathrm{F}$	?
4.4. F	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$ — Given
2. $\neg A$ — Elim ∧: 1
3. $\neg B$ — Elim ∧: 1
   - 4.1. $A \vee B$ — Assumption
     - 4.2.1. A — Assumption
     - 4.2.2. $\mathbf{F}$ — ?
   - 4.2. $A \rightarrow \mathbf{F}$ — Direct Proof
   - 4.3. $B \rightarrow \mathbf{F}$ — ?
   - 4.4. $\mathbf{F}$ — Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$ — Absurdum

Principium Contradictionis

$$\frac{\neg A \ ; \ A}{\therefore \ F}$$

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \to \mathbf{F}$	Direct Proof
4.3. $B \to \mathbf{F}$	?
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3.1. B	Assumption
4.3.2. $\mathbf{F}$	?
4.3. $B \rightarrow \mathbf{F}$	Direct Proof
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3.1. B	Assumption
4.3.2. $\mathbf{F}$	Contradiction: 4.3.1, 3
4.3. $B \rightarrow \mathbf{F}$	Direct Proof
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Rules for Propositional Logic

	Elimination	Introduction
$\wedge$	Elim $\wedge$	Intro $\wedge$
$\vee$	Cases	Intro $\vee$
$\rightarrow$	Modus Ponens	Direct Proof
$\neg$	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum
	Tautology	Equivalent

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \quad \textbf{(for any } a\textbf{)}}$$

Elim ∃

Intro ∀

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$$

Elim ∀

$$\frac{\forall x\ P(x)}{\therefore\ P(a) \textbf{ for any } a}$$

5. $\forall x\ P(x) \rightarrow \exists x\ P(x)$

?

The main connective is implication so Direct Proof seems good

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\ P(x)$ Assumption

We need an ∃ we don't have
so "intro ∃" rule makes sense

1.5. $\exists x\ P(x)$?

1. $\forall x\ P(x) \rightarrow \exists x\ P(x)$ Direct Proof

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\ P(x)$ Assumption

We need an ∃ we don't have so "intro ∃" rule makes sense

1.5. $\exists x\ P(x)$ Intro ∃: ? That requires P(c) for some c.

1. $\forall x\ P(x) \rightarrow \exists x\ P(x)$ Direct Proof

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\ P(x)$ **Assumption**

1.4. $P(5)$?

1.5. $\exists x\ P(x)$ **Intro ∃: 1.4**

1. $\forall x\ P(x) \rightarrow \exists x\ P(x)$ **Direct Proof**

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\ P(x)$ Assumption

1.4. $P(5)$ Elim ∀: 1.1

1.5. $\exists x\ P(x)$ Intro ∃: 1.4

1. $\forall x\ P(x) \rightarrow \exists x\ P(x)$ Direct Proof

My First Predicate Logic Proof

Domain of Discourse
Integers

Prove $(\forall x\ P(x)) \rightarrow (\exists x\ P(x))$

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\ P(x)$ Assumption
1.2. $P(5)$ Elim ∀: 1.1
1.3. $\exists x\ P(x)$ Intro ∃: 1.2

1. $\forall x\ P(x) \rightarrow \exists x\ P(x)$ Direct Proof

This follows our usual strategy — eliminate forward, introduce backward — but it is weird...

How did we know to use 5? We didn't! We just guessed it.

Randomly guessing numbers is not good proof strategy!

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ Given

...

?. $\exists x\,P(x)$?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\,((x > 9) \rightarrow P(x))$	Given
…		
?.	$P(5)$	?
?.	$\exists x\,P(x)$	Intro ∃

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ Given

...

?. $\exists x\,P(x)$?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Our General Proof Strategy

1. $\forall x\, P(x)$ Given
2. $P(100) \rightarrow Q(100)$ Given

...

?. $\exists x\, Q(x)$?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
5.	$P(3)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Exception: Elim ∀
(**must** wait until you know which one *you need*)

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\, P(x)$ — Given

...

?. $\exists x\, P(x)$ — ?

Exception: Elim ∀
(**must** wait until you know which one *you need*)

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Domain Knowledge

- Intro ∃ and Elim ∀ are *creative* steps
  - need to know the right object to use

    make the wrong choice and the proof won't work
  - the other rules are *mechanical*

    you can apply them blindly without thinking too hard

- Requires your understanding (and intuition) of the objects in question
  - i.e., your "domain knowledge"

Predicate Logic Proofs with more content

- Want to be able to use domain knowledge so that proofs are about things we understand

- Example:

Domain of Discourse
Integers

- Given the basic properties of arithmetic on integers, define:

Predicate Definitions
$Even(x) := \exists y\ (x = 2 \cdot y)$
$Odd(x) := \exists y\ (x = 2 \cdot y + 1)$

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

1.	**6 = 2·3**	**Algebra**
2.	∃y (**6 = 2**·y)	**Intro ∃: 1**
3.	Even(**6**)	**Definition of** Even
4.	∃x Even(x)	**Intro ∃: 3**

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := $\exists y\ (x = 2 \cdot y)$
Odd(x) := $\exists y\ (x = 2 \cdot y + 1)$
Prime(x) := "…"

Prove "There is an even prime number"

Formally: prove $\exists x\ (\text{Even}(x) \wedge \text{Prime}(x))$

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)
Prime(x) := "…"

Prove "There is an even prime number"

Formally: prove ∃x (Even(x) ∧ Prime(x))

1.	**2 = 2·1**	**Algebra**
2.	∃y (**2** = **2**·y)	**Intro ∃: 1**
3.	Even(**2**)	**Def of** Even**: 3**
4.	Prime(**2**)*	**Property of integers**
5.	Even(**2**) ∧ Prime(**2**)	**Intro ∧: 3, 4**
6.	∃x (Even(x) ∧ Prime(x))	**Intro ∃: 5**

*** Later we will further break down "Prime" using quantifiers to prove statements like this**

Rules for Definitions

Each definition gives us two rules new rules, one for *eliminating* and one for introducing it:

Def of Even

$$\frac{\text{Even}(x)}{\therefore \exists y\,(x = 2y)}$$

Def of Even

$$\frac{\exists y\,(x = 2y)}{\therefore \text{Even}(x)}$$

We will write "def of" for both rules

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \quad \textbf{(for any } a\textbf{)}}$$

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore P(c) \textbf{ for some } \textbf{\textit{special}}^{**} \text{ c}}$$

Intro ∀

$$\frac{\text{“Let a be arbitrary}^{*}\text{”...}P(a)}{\therefore \quad \forall x\, P(x)}$$

** By special, we mean that c is a name for a value where P(c) is true. We can't use anything else about that value, so c has to be a NEW name!

* in the domain of P

Note: bottom two rules are *complex* but mechanical
(you can apply them blindly)

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$?

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1 $Even(a) \rightarrow Even(a^2)$?

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$ Intro ∀

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1 Even(**a**) Assumption

1.1.6 Even($\mathbf{a}^2$) ?

1.1 Even(**a**)→Even($\mathbf{a}^2$) Direct proof

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$ Intro ∀

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let **a** be an arbitrary integer

1.1.1 Even(**a**) Assumption

1.1.2 ∃y (**a** = 2y) Definition of Even: 1.1.1

1.1.6 $Even(\mathbf{a}^2)$?

1.1 $Even(\mathbf{a}) \rightarrow Even(\mathbf{a}^2)$ Direct proof

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$ Intro ∀

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1 Even(**a**) — Assumption

1.1.2 ∃y (**a** = 2y) — Definition of Even: 1.1.1

1.1.5 ∃y ($\mathbf{a}^2$ = 2y) — ?

1.1.6 Even($\mathbf{a}^2$) — Definition of Even

1.1 Even(**a**)→Even($\mathbf{a}^2$) — Direct proof

1. ∀x (Even(x)→Even(x^2)) — Intro ∀

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even: 1.1.1
1.1.3	**a** = 2**b**	Elim ∃: 1.1.2
		Need $a^2 = 2c$ for some **c**
1.1.5	∃y (a^2 = 2y)	?
1.1.6	Even(a^2)	Definition of Even
1.1	Even(**a**)→Even(a^2)	Direct proof
1.	∀x (Even(x)→Even(x^2))	Intro ∀

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even
1.1.3	**a** = 2**b**	Elim ∃
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra
1.1.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃
1.1.6	Even($\mathbf{a}^2$)	Definition of Even
1.1	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof
1.	∀x (Even(x)→Even(x^2))	Intro ∀

Used $\mathbf{a}^2 = 2\mathbf{c}$ for $\mathbf{c}=2\mathbf{b}^2$

Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even: 1.1.1
1.1.3	**a** = 2**b**	Elim ∃: 1.1.2
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra: 1.1.3
1.1.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃: 1.1.4
1.1.6	Even($\mathbf{a}^2$)	Definition of Even: 1.1.5
1.1	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof
1.	∀x (Even(x)→Even(x^2))	Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀: "Let a be arbitrary*"...P(a) / ∴ ∀x P(x)

Elim ∃: ∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: $\forall x\, \forall y\, (Odd(x) \wedge Odd(y) \rightarrow Even(x+y))$

1. $\forall x\, \forall y\, (Odd(\mathbf{x}) \wedge Odd(\mathbf{y}) \rightarrow Even(\mathbf{x+y}))$?

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: ∀x ∀y (Odd(x) ∧ Odd(y) → Even(x+y))

Let a and b be an arbitrary integer

1.1 Odd(**a**) ∧ Odd(**b**) → Even(**a+b**) ?

1. ∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**)) Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: ∀x ∀y (Odd(x) ∧ Odd(y) → Even(x+y))

Let a and b be an arbitrary integer

1.1.1 Odd(**a**) ∧ Odd(**b**) Assumption

1.1.? Even(**a** + **b**) ?

1.1 Odd(**a**) ∧ Odd(**b**) → Even(**a+b**) Direct proof

1. ∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**)) Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1

1.1.?	Even(**a** + **b**)	?
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3

1.1.?	Even(**a** + **b**)	?
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3

1.1.?	∃y (**a** + **b** = 2y)	?
1.1.?	Even(**a** + **b**)	Def of Even
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3
1.1.6	**a** = 2**c** + 1	Elim ∃: 1.1.4
1.1.7	**b** = 2**d** + 1	Elim ∃: 1.1.5
1.1.?	∃y (**a** + **b** = 2y)	?
1.1.?	Even(**a** + **b**)	Def of Even
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Odd Plus Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3
1.1.6	**a** = 2**c** + 1	Elim ∃: 1.1.4
1.1.7	**b** = 2**d** + 1	Elim ∃: 1.1.5
1.1.8	**a** + **b** = 2(**c** + **d** +1)	Algebra: 1.1.6–7
1.1.9	∃y (**a** + **b** = 2y)	Intro ∃: 1.1.8
1.1.10	Even(**a** + **b**)	Def of Even: 1.1.9
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Formal Proofs

- Formal proofs follow simple well-defined rules
  - "assembly language" (like byte code) for proofs
  - easy for a machine to check

- Important to understand
  - mental "foundations" of Computer Science
  - has useful applications, e.g., Programming Languages

Formal Proofs

- In principle, formal proofs are the standard for what it means to be “proven” in mathematics
  - almost all math (and theory CS) done in Predicate Logic

- But they can be tedious and impractical…

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Requires 35 lines in a formal proof!!

Formal Proofs

- In principle, formal proofs are the standard for what it means to be "proven" in mathematics
  - almost all math (and theory CS) done in Predicate Logic

- But they can be tedious and impractical
  - e.g., applications of commutativity and associativity
  - Russell & Whitehead's formal proof that 1+1 = 2 is *several hundred pages* long

    we allow ourselves to cite "Arithmetic", "Algebra", etc.

- *Historically*, rarely used for "real mathematics"...

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs

    they implement a community standard of correctness

- English proofs require understanding formal proofs
  - English proof follows the structure of a formal proof
  - we will learn English proofs by translating from formal

    eventually, we will write English directly

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs
  - in 311, correct iff reader sees how to formalize it

- Examples of what can be skipped (more to come):
  - Intro and Elim $\wedge$
  - explicitly stating existence claims (Elim $\exists$ immediately)
  - explicitly invoking Direct Proof (clear from context)

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: Suppose x and y are rational.

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 = (ac)/(bd). Note that ac and bd are integers. Furthermore, since b and d are both non-zero, so is bd. By definition, then, xy is rational. ■

vs more than 35 lines of formal proof

Recall: Even and Odd

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)
Domain: Integers

Prove: "The square of any even number is even."

Formal proof of: $\forall x\ (Even(x) \rightarrow Even(x^2))$

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even: 1.1.1
1.1.3	**a** = 2**b**	Elim ∃ (**b**): 1.1.2
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra: 1.1.3
1.1.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃: 1.1.4
1.1.6	Even($\mathbf{a}^2$)	Definition of Even: 1.1.5
1.1	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof
1.	$\forall x\ (Even(x) \rightarrow Even(x^2))$	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The square of every even integer is even."

Let **a** be an arbitrary integer.	Let **a** be an arbitrary integer	
Suppose **a** is even.	1.1.1 Even(**a**)	Assumption
Then, by definition, **a** = 2**b** for some integer **b**.	1.1.2 ∃y (**a** = 2y) 1.1.3 **a** = 2**b**	Definition Elim ∃
Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.	1.1.4 $a^2 = 2(2b^2)$	Algebra
So a^2 is, by definition, even.	1.1.5 ∃y (a^2 = 2y) 1.1.6 Even(a^2)	Intro ∃ Definition
Since **a** was arbitrary, we have shown that the square of every even number is even.	1.1. Even(**a**)→Even(a^2) 1. ∀x (Even(x)→Even(x^2))	Direct Proof Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The square of every even integer is even."

Proof: Let **a** be an arbitrary integer.

Suppose **a** is even. Then, by definition, **a** = 2**b** for some integer b. Squaring both sides, we get $\mathbf{a^2} = 4\mathbf{b^2} = 2(2\mathbf{b^2})$. So $\mathbf{a^2}$ is, by definition, is even.

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

Let x and y be arbitrary integers.

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

1.1. $(\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$

1. $\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(x+y))$ Intro $\forall$

Even and Odd

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

Let x and y be arbitrary integers

Suppose that both are odd.

1.1.1 Odd(**x**) ∧ Odd(**y**) Assumption

so x+y is even.

1.1.9 Even(**x+y**)

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

1.1. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) Direct..

1. ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

Suppose that both are odd.

Let x and y be arbitrary integers

1.1.1	Odd(**x**) ∧ Odd(**y**)	Assumption
1.1.2	Odd(**x**)	Elim ∧
1.1.3	Odd(**y**)	Elim ∧

so x+y is even.

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

1.1.9	Even(**x+y**)	
1.1.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	Direct..
1.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

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.

so x+y is, by definition, even.

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

Let x and y be arbitrary integers.

1.1.1	Odd(**x**) ∧ Odd(**y**)	Assumption
1.1.2	Odd(**x**)	Elim ∧
1.1.3	Odd(**y**)	Elim ∧
1.1.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 1.1.2
1.1.5	**x** = 2**a**+1	Elim ∃
1.1.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 1.1.3
1.1.7	**y** = 2**b**+1	Elim ∃
1.1.9	∃z (**x+y** = 2z)	Intro ∃
1.1.10	Even(**x+y**)	Def of Even
1.1.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	Direct..
1.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

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 = ... = 2(a+b+1)

so x+y is, by definition, even.

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

Let x and y be arbitrary integers.

1.1.1	Odd(**x**) ∧ Odd(**y**)	Assumption
1.1.2	Odd(**x**)	Elim ∧
1.1.3	Odd(**y**)	Elim ∧
1.1.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 1.1.2
1.1.5	**x** = 2**a**+1	Elim ∃
1.1.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 1.1.3
1.1.7	**y** = 2**b**+1	Elim ∃
1.1.8	**x+y** = 2(**a**+**b**+**1**)	Algebra
1.1.9	∃z (**x+y** = 2z)	Intro ∃
1.1.10	Even(**x+y**)	Def of Even

1.1.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	Direct..
1.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**))	Intro ∀

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

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. ■

Formal-to-English Translation

- Document posted on website

- Use these on homework
  - no need to match the *exact* phrasing
  - English proofs are not formal proofs

Recall: Elementary School Division

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

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

The number q is called the *quotient*.

This equation involve fractions. We want to stick to integers!

Multiplying both sides by b, this becomes

$$a = qb$$

When there exists some such q, we write "$b \mid a$".

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b (usually with $b \neq 0$):

$$b \mid a \;:=\; \exists q\,(a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
1 | 5	5 | 25	0 | 5	2 | 3

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b (usually with $b \neq 0$):

$$b \mid a \;:=\; \exists q\,(a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Example Division Proof

For every integer $\boldsymbol{a}$, if $6 \mid \boldsymbol{a}$, then $2 \mid \boldsymbol{a}$ and $3 \mid \boldsymbol{a}$.

$$\forall a\,((6 \mid a) \rightarrow ((2 \mid a) \wedge (3 \mid a)))$$

1. $\forall \boldsymbol{a}\,((6 \mid \boldsymbol{a}) \rightarrow (2 \mid \boldsymbol{a}) \wedge (3 \mid \boldsymbol{a})))$ **??**

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Let n be an arbitrary integer.

1.1	$(6 \mid n) \rightarrow ((2 \mid n) \wedge (3 \mid n))$	??
1.	$\forall a\,((6 \mid a) \rightarrow (2 \mid a) \wedge (3 \mid a)))$	Intro $\forall$

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Let n be an arbitrary integer.

1.1.1 $6 \mid n$ Assumption

1.1.? $(2 \mid n) \wedge (3 \mid n)$??

1.1 $(6 \mid n) \rightarrow ((2 \mid n) \wedge (3 \mid n))$ Direct Proof

1. $\forall a\,((6 \mid a) \rightarrow (2 \mid a) \wedge (3 \mid a)))$ Intro $\forall$

Example Division Proof

For every integer a, if 6 | a , then 2 | a and 3 | a.

Let n be an arbitrary integer.

1.1.1	6 | n	Assumption
1.1.2	∃q (n = 6q)	Def of Divides: 1.1.1

1.1.?	((2 | n) ∧ (3 | n)	??
1.1	(6 | n) →((2 | n) ∧ (3 | n))	Direct Proof
1.	∀a ((6 | a) →(2 | a) ∧ (3 | a)))	Intro ∀

Example Division Proof

For every integer a, if 6 | a , then 2 | a and 3 | a.

Let n be an arbitrary integer.

1.1.1	6 | n	Assumption
1.1.2	∃q (n = 6q)	Def of Divides: 1.1.1
1.1.3	n = 6b	Elim ∃: 1.1.2

1.1.?	((2 | n) ∧ (3 | n)	??
1.1	(6 | n) →((2 | n) ∧ (3 | n))	Direct Proof
1.	∀a ((6 | a) →(2 | a) ∧ (3 | a)))	Intro ∀

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Let n be an arbitrary integer.

1.1.1	$6 \mid n$	Assumption
1.1.2	$\exists q\ (n = 6q)$	Def of Divides: 1.1.1
1.1.3	$n = 6b$	Elim $\exists$: 1.1.2
1.1.?	$2 \mid n$	??
1.1.?	$3 \mid n$	??
1.1.?	$(2 \mid n) \wedge (3 \mid n)$	Intro $\wedge$
1.1	$(6 \mid n) \rightarrow ((2 \mid n) \wedge (3 \mid n))$	Direct Proof
1.	$\forall a\ ((6 \mid a) \rightarrow (2 \mid a) \wedge (3 \mid a)))$	Intro $\forall$

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Let **n** be an arbitrary integer.

1.1.1	$6 \mid n$	Assumption
1.1.2	$\exists q\ (n = 6q)$	Def of Divides: 1.1.1
1.1.3	$n = 6b$	Elim $\exists$: 1.1.2
1.1.?	$\exists q\ (n = 2q)$	??
1.1.?	$\exists q\ (n = 3q)$	??
1.1.?	$2 \mid n$	Def of Divides
1.1.?	$3 \mid n$	Def of Divides
1.1.?	$(2 \mid n) \wedge (3 \mid n)$	Intro $\wedge$
1.1	$(6 \mid n) \rightarrow ((2 \mid n) \wedge (3 \mid n))$	Direct Proof
1.	$\forall a\ ((6 \mid a) \rightarrow (2 \mid a) \wedge (3 \mid a)))$	Intro $\forall$

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Let **n** be an arbitrary integer.

1.1.1	$6 \mid n$	Assumption
1.1.2	$\exists q\ (n = 6q)$	Def of Divides: 1.1.1
1.1.3	$n = 6b$	Elim $\exists$: 1.1.2
1.1.4	$n = 2(3b)$	Algebra: 1.1.3
1.1.5	$n = 3(2b)$	Algebra: 1.1.3
1.1.6	$\exists q\ (n = 2q)$	Intro $\exists$: 1.1.4
1.1.7	$\exists q\ (n = 3q)$	Intro $\exists$: 1.1.5
1.1.8	$2 \mid n$	Def of Divides: 1.1.6
1.1.9	$3 \mid n$	Def of Divides: 1.1.7
1.1.10	$((2 \mid n) \wedge (3 \mid n)$	Intro $\wedge$: 1.1.8, 1.1.9
1.1	$(6 \mid n) \rightarrow ((2 \mid n) \wedge (3 \mid n))$	Direct Proof
1.	$\forall a\ ((6 \mid a) \rightarrow (2 \mid a) \wedge (3 \mid a)))$	Intro $\forall$

Example Division Proof

For every integer a, if 6 | a , then 2 | a and 3 | a.

Let n be an arbitrary integer.

Suppose that 6 divides n.

Then, n = 6b for some integer b by the definition of divides.

Hence, we can see that n = 2(3b), so 2 divides n by the defn of divides.

Likewise, we can see that n = 3(2b), so 3 divides n by the defn of divides.

Since n was arbitrary, we have proven the claim.

Let n be an arbitrary integer.

1.1.1	6 | **n**	**Assumption**
1.1.2	∃q (**n** = 6q)	**Def of Divides**
1.1.3	**n** = 6**b**	**Elim ∃**
1.1.4	**n** = 2(3**c**)	**Algebra**
1.1.5	∃q (n = 2q)	**Intro ∃**
1.1.6	2 | **n**	**Def of Divides**
1.1.4	**n** = 3(2**c**)	**Algebra**
1.1.5	∃q (n = 3q)	**Intro ∃**
1.1.6	3 | **n**	**Def of Divides**
1.1.10	(2 | **n**) ∧ (3 | **n**)	**Intro ∧**
1.1	(6 | **n**) →((2 | **n**) ∧ (3 | **n**))	**Direct Proof**
1.	∀***a*** ((6 | ***a***) →(2 | **a**) ∧ (3 | ***a***)))	**Intro ∀**

Example Division Proof

For every integer a, if $6 \mid a$, then $2 \mid a$ and $3 \mid a$.

Proof: Let n be an arbitrary integer.

Suppose that 6 divides n.

Then, n = 6b for some integer b by the definition of divides.

Hence, we can see that n = 2(3b), so 2 divides n by the definition of divides. Likewise, we can see that n = 3(2b), so 3 divides n by the definition of divides.

Since n was arbitrary, we have proven the claim. ■

Greatest Common Divisor

Domain of Discourse
Non-negative Integers

GCD Theorem

For a, b with $a > 0$
there exist a *unique* integer n s.t. $n \mid a$ and $n \mid b$
and, for all d, if $d \mid a$ and $d \mid b$, then $d \leq n$

We will denote this unique number as $n = \gcd(a, b)$

Greatest Common Divisor

gcd(a, b):

Largest integer n such that $n \mid a$ and $n \mid b$

- gcd(100, 125) =
- gcd(17, 49) =
- gcd(11, 66) =
- gcd(13, 0) =
- gcd(180, 252) =

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a, 0*) = *a.*

$\gcd(a, 0)$ is, by definition, the number n satisfying

$$(n \mid 0) \wedge (n \mid a) \wedge \forall d\, (((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq n))$$

To show that a $= \gcd(a, 0)$, we need to show that

$$(a \mid 0) \wedge (a \mid a) \wedge \forall d\, (((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$$

those facts show a $= \gcd(a, 0)$ by the defn of gcd

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a, 0*) = *a.*

$$\forall a\ ((\mathrm{a} > 0) \rightarrow (a = \gcd(a, 0))$$

1. $\forall \boldsymbol{a}\ ((\boldsymbol{a} > 0) \rightarrow (\boldsymbol{a} = \gcd(\boldsymbol{a}, 0)))$ **??**

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let $\boldsymbol{a}$ be an arbitrary non-negative integer.

1.1. $(\boldsymbol{a} > 0) \rightarrow (\boldsymbol{a} = \gcd(\boldsymbol{a}, 0))$??

1. $\forall \boldsymbol{a}\,((\boldsymbol{a} > 0) \rightarrow (\boldsymbol{a} = \gcd(\boldsymbol{a}, 0)))$ Intro ∀

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let a be an arbitrary non-negative integer.

1.1.1. $a > 0$ Assumption

1.1.?. $a = \gcd(a, 0)$??

1.1. $(a > 0) \rightarrow (a = \gcd(a, 0))$ Direct Proof

1. $\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$ Intro ∀

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let a be an arbitrary non-negative integer.

1.1.1. $a > 0$ Assumption

1.1.?. $a = \gcd(a, 0)$ Def of GCD

1.1. $(a > 0) \rightarrow (a = \gcd(a, 0))$ Direct Proof

1. $\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$ Intro ∀

First GCD Fact

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let a be an arbitrary non-negative integer.

1.1.1. $a > 0$	Assumption
1.1.1. $a \mid 0$	??
1.1.2. $a \mid a$	??
1.1.3. $\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	??
1.1.4. $(a \mid 0) \wedge (a \mid a)$	Intro $\wedge$: 1, 2
1.1.5. $(a \mid 0) \wedge (a \mid a) \wedge (\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)))$	Intro $\wedge$: 4, 3
1.1.6. $a = \gcd(a, 0)$	Def of GCD: 5
1.1. $(a > 0) \rightarrow (a = \gcd(a, 0))$	Direct Proof
1. $\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$	Intro $\forall$

First GCD Fact

$\gcd(a, 0) = a$

?. $a \mid 0$

?

First GCD Fact

$\gcd(a, 0) = a$

?. $\exists q\ (0 = q\boldsymbol{a})$

?. $\boldsymbol{a} \mid \mathbf{0}$ **Def of Divides**

First GCD Fact

$\gcd(a, 0) = a$

1.	$0 = 0a$	Algebra
2.	$\exists q\ (0 = qa)$	Intro ∃: 1
3.	$a \mid 0$	Def of Divides: 2

First GCD Fact

$\gcd(a, 0) = a$

We can see that 0 = 0a.

Thus, a | 0 by the definition of divides.

1.	$0 = 0\boldsymbol{a}$	**Algebra**
2.	$\exists q\ (0 = q\boldsymbol{a})$	**Intro ∃: 1**
3.	$\boldsymbol{a} \mid \boldsymbol{0}$	**Def of Divides: 2**

First GCD Fact

$\gcd(a, 0) = a$

?. $a \mid a$

??

First GCD Fact

$\gcd(a, 0) = a$

?. $\exists q\ (a = qa)$

?. $a \mid a$

??

Def of Divides

First GCD Fact

$\gcd(a, 0) = a$

1.	$a = 1a$	Algebra
2.	$\exists q\ (a = qa)$	Intro $\exists$: 1
3.	$a \mid a$	Def of Divides: 2

First GCD Fact

$\gcd(a, 0) = a$

We can see that a = 1a.

Thus, a | a by the definition of divides.

1.	$a = 1a$	**Algebra**
2.	$\exists q\ (a = qa)$	**Intro ∃: 1**
3.	$a \mid a$	**Def of Divides: 2**

First GCD Fact

gcd(*a*, *0*) = *a*

?. $\forall \boldsymbol{d}\ (((\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})) \rightarrow (\boldsymbol{d} \leq \boldsymbol{a}))$??

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.? $((\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})) \rightarrow (\boldsymbol{d} \leq \boldsymbol{a})$??

1. $\forall \boldsymbol{d}\,(((\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})) \rightarrow (\boldsymbol{d} \leq \boldsymbol{a}))$ Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1 $(\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})$ Assumption

1.1.? $\boldsymbol{d} \leq \boldsymbol{a}$??

1.1.? $((\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})) \rightarrow (\boldsymbol{d} \leq \boldsymbol{a})$ Direct Proof

1. $\forall \boldsymbol{d}\, (((\boldsymbol{d} \mid 0) \wedge (\boldsymbol{d} \mid \boldsymbol{a})) \rightarrow (\boldsymbol{d} \leq \boldsymbol{a}))$ Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1 $(d \mid 0) \wedge (d \mid a)$ Assumption

1.1.2 $d \mid a$ Elim ∧: 1.1.1

1.1.? $d \leq a$??

1.1.? $((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$ Direct Proof

1. $\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$ Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.?	$d \leq a$	??
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.?	$d \leq a$	??
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$d \leq a$	Prop of × : 1.1.4
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

Wait? Is this true?!?

No! Multiplication by 0 makes things smaller. **Uh oh**!

How can we handle the **case** $k = 0$?

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6	$(k = 0) \rightarrow (d \leq a)$	??
1.1.7	$(k > 0) \rightarrow (d \leq a)$	??
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6	$(k = 0) \rightarrow (d \leq a)$	??
1.1.7.1	$k > 0$	Assumption
1.1.7.2	$d \leq a$	Prop of ×: 1.1.4, 1.1.7.1
1.1.7	$(k > 0) \rightarrow (d \leq a)$	Direct Proof
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.?	$d \leq a$	??
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
...		
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.2	$a = 0$	Algebra: 1.1.4, 1.1.6.1
1.1.6.?	$d \leq a$	??
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
...		
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

Recall the Proof Outline

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let a be an arbitrary non-negative integer.

1.1.1. $a > 0$	Assumption
1.1.1. $a \mid 0$	??
1.1.2. $a \mid a$	??
1.1.3. $\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	??
1.1.4. $(a \mid 0) \wedge (a \mid a)$	Intro $\wedge$: 1, 2
1.1.5. $(a \mid 0) \wedge (a \mid a) \wedge (\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)))$	Intro $\wedge$: 4, 3
1.1.6. $a = \gcd(a, 0)$	Def of GCD: 5
1.1. $(a > 0) \rightarrow (a = \gcd(a, 0))$	Direct Proof
1. $\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$	Intro $\forall$

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.2	$a = 0$	Algebra: 1.1.4, 1.1.6.1
1.1.6.3	$\neg(a = 0)$	Prop of Positives
1.1.6.?	$d \leq a$	??
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
...		
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.2	$a = 0$	Algebra: 1.1.4, 1.1.6.1
1.1.6.3	$\neg(a = 0)$	Prop of Positives
1.1.6.4	$\mathbf{F}$	Principium Contradictionis
1.1.6.?	$d \leq a$	??
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
...		
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.2	$a = 0$	Algebra: 1.1.4, 1.1.6.1
1.1.6.3	$\neg(a = 0)$	Prop of Positives
1.1.6.4	$\mathbf{F}$	Principium Contradictionis
1.1.6.?	$d \leq a$	Ex Falso Quodlibet
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
...		
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

$\gcd(a, 0) = a$

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6.1	$k = 0$	Assumption
1.1.6.2	$a = 0$	Algebra: 1.1.4, 1.1.6.1
1.1.6.3	$\neg(a = 0)$	Prop of Positives
1.1.6.4	**F**	Principium Contradictionis
1.1.6.?	$d \leq a$	Ex Falso Quodlibet
1.1.6	$(k = 0) \rightarrow (d \leq a)$	Direct Proof
1.1.7.1	$k > 0$	Assumption
1.1.7.2	$d \leq a$	Prop of ×: 1.1.4, 1.1.7.1
1.1.7	$(k > 0) \rightarrow (d \leq a)$	Direct Proof
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

First GCD Fact

gcd(*a*, *0*) = *a*

Let d be an arbitrary non-negative integer.

Suppose that $d \mid 0$ and $d \mid a$. From the second fact, we get that $a = jd$ by the defn of divides

We continue by **cases**…

Suppose that $j = 0$. That would tell us that $a = 0d = 0$, contradicting that $a > 0$. Since false is true, anything is true. In particular, we can say that $d \leq a$ holds.

Suppose that $j > 0$. Then, $a = jd$ cannot be smaller than d, so we again have $d \leq a$.

Since the cases $j = 0$ and $j > 0$ are exhaustive, we have shown $d \leq a$ **holds in general**.

Since d was arbitrary, we have proven the claim

Let d be arbitrary…
- Assumption
- Elim ∧
- Def of Divides
- Elim ∃
- Prop of Non-negatives
  - Assumption
  - Algebra
  - Prop of Positives
  - Principium Contradictionis
  - Ex Falso Quodlibet
- Direct Proof
  - Assumption
  - Prop of ×: 1.1.4, 1.1.7.1
- Direct Proof
- Cases: 1.1.6, 1.1.7

Direct Proof

Intro ∀

Recall the Proof Outline

Domain of Discourse
Non-negative Integers

For every positive integer *a*, if *a* > 0, then gcd(*a*, *0*) = *a*.

Let a be an arbitrary non-negative integer.

1.1.1. $a > 0$	Assumption
1.1.1. $a \mid 0$	??
1.1.2. $a \mid a$	??
1.1.3. $\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	??
1.1.4. $(a \mid 0) \wedge (a \mid a)$	Intro $\wedge$: 1, 2
1.1.5. $(a \mid 0) \wedge (a \mid a) \wedge (\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)))$	Intro $\wedge$: 4, 3
1.1.6. $a = \gcd(a, 0)$	Def of GCD: 5
1.1. $(a > 0) \rightarrow (a = \gcd(a, 0))$	Direct Proof
1. $\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$	Intro $\forall$

First GCD Fact

$$\forall a\,((a > 0) \rightarrow (a = \gcd(a, 0)))$$

Let a be an arbitrary non-negative integer.

Suppose that $a > 0$. We will show that a satisfies the definition of $\gcd(a, 0)$.

First, we can see that $0 = 0a$. Thus, $a \mid 0$ by the definition of divides. And we can see that $a = 1a$. Thus, $a \mid a$ by the definition of divides. It remains to show that every number dividing 0 and a is no bigger than a.

Let d be an arbitrary non-negative integer.

Suppose that $d \mid 0$ and $d \mid a$. From the second fact, we get that $a = jd$ for some integer j by the definition of divides. We continue by cases…

Suppose that $j = 0$. That would tell us that $a = 0d = 0$, contradicting that $a > 0$. Since false is true, anything is true. In particular, we have $d \leq a$.

Now, suppose that $j > 0$. Then, $a = jd$ cannot be smaller than d, so we again have $d \leq a$.

Since these cases are exhaustive, we have shown $d \leq a$ holds in general.

Since d was arbitrary, we have proven $a = \gcd(a, 0)$ by the definition of gcd.

Since a was arbitrary, we have proven the claim.

Just One More thing?

Let **d** be an arbitrary non-negative integer.

1.1.1	$(d \mid 0) \wedge (d \mid a)$	Assumption
1.1.2	$d \mid a$	Elim ∧: 1.1.1
1.1.3	$\exists q\,(a = qd)$	Def of Divides: 1.1.2
1.1.4	$a = kd$	Elim ∃: 1.1.3
1.1.5	$(k = 0) \vee (k > 0)$	Prop of Non-negatives
1.1.6	$(k = 0) \rightarrow (d \leq a)$	??
1.1.7.1	$k > 0$	Assumption
1.1.7.2	$d \leq a$	Prop of ×: 1.1.4, 1.1.7.1
1.1.7	$(k > 0) \rightarrow (d \leq a)$	Direct Proof
1.1.8	$d \leq a$	Cases: 1.1.6, 1.1.7
1.1.?	$((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a)$	Direct Proof
1.	$\forall d\,(((d \mid 0) \wedge (d \mid a)) \rightarrow (d \leq a))$	Intro ∀

What **rule** is this? Do we need a new rule for **every** fact about numbers?

Theorems

- Facts proven previously by others (or ourselves) are "theorems" that we can use in our proofs
  - also called "lemmas" or "propositions"

- In this case, we want the following theorem:

If $x = yz$ and $y > 0$, then $z \leq x$. "Prop of ×"

$$\forall x \, \forall y \, \forall z \, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x))$$

Using Theorems

If $x = yz$ and $u > 0$, then $z \leq x$. "Prop of ×"

$$\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x))$$

- First way to use theorems in a proof:

Cite T

$\therefore \forall x\, P(x)$

where T is a well-known theorem
that says $\forall x\, P(x)$

Using Theorems

If $\boldsymbol{x = yz}$ and $\boldsymbol{u > 0}$, then $\boldsymbol{z \leq x}$. "Prop of ×"

$$\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x))$$

1. $a = kd$	**...**
2. $k > 0$	**...**
3. $\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x)$	**Cite "Prop of ×"**
4. $\forall y\, \forall z\, (((a = yz) \wedge (y > 0)) \rightarrow (z \leq a)$	**Elim ∀: 3**
5. $\forall z\, (((a = kz) \wedge (k > 0)) \rightarrow (z \leq a)$	**Elim ∀: 4**
6. $((a = kd) \wedge (k > 0)) \rightarrow (d \leq a)$	**Elim ∀: 5**
7. $(a = kd) \wedge (k > 0)$	**Intro ∧: 1, 2**
8. $d \leq a$	**MP: 7, 6**

Using Theorems

If $x = yz$ and $u > 0$, then $z \leq x$. "Prop of ×"

$$\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x))$$

most theorems look like this...
(some ∀s and then →)

- Second way to use theorems in a proof...

Apply T

$$\frac{P(c)}{\therefore Q(c)}$$

where T is a well-known theorem
that says $\forall x\, (P(x) \rightarrow Q(x))$

Using Theorems

If $x = yz$ and $u > 0$, then $z \leq x$. "Prop of ×"

$\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x))$

1. $a = kd$	...
2. $k > 0$	...
3. $\forall x\, \forall y\, \forall z\, (((x = yz) \wedge (y > 0)) \rightarrow (z \leq x)$	Cite "Prop of ×"
4. $\forall y\, \forall z\, (((a = yz) \wedge (y > 0)) \rightarrow (z \leq a)$	Elim ∀: 3
5. $\forall z\, (((a = kz) \wedge (k > 0)) \rightarrow (z \leq a)$	Elim ∀: 4
6. $((a = kd) \wedge (k > 0)) \rightarrow (d \leq a)$	Elim ∀: 5
7. $(a = kd) \wedge (k > 0)$	Intro ∧: 1, 2
8. $d \leq a$	MP: 7, 6
3. $d \leq a$	**Apply "Prop of ×": 1, 2**