Week 7 at a glance

We will be learning and practicing to:

- Clearly and unambiguously communicate computational ideas using appropriate formalism. Translate across levels of abstraction.
  - Translating between symbolic and English versions of statements using precise mathematical language
  - Using appropriate signpost words to improve readability of proofs, including 'arbitrary' and 'assume'
- Know, select and apply appropriate computing knowledge and problem-solving techniques. Reason about computation and systems. Use mathematical techniques to solve problems. Determine appropriate conceptual tools to apply to new situations. Know when tools do not apply and try different approaches. Critically analyze and evaluate candidate solutions.
  - Judging logical equivalence of compound propositions using symbolic manipulation with known equivalences, including DeMorgan's Law
  - Writing the converse, contrapositive, and inverse of a given conditional statement
  - Determining what evidence is required to establish that a quantified statement is true or false
  - Evaluating quantified statements about finite and infinite domains
- Apply proof strategies, including direct proofs and proofs by contradiction, and determine whether a proposed argument is valid or not.
  - Identifying the proof strategies used in a given proof
  - Identifying which proof strategies are applicable to prove a given compound proposition based on its logical structure
  - Carrying out a given proof strategy to prove a given statement
  - Carrying out a universal generalization argument to prove that a universal statement is true
  - Using proofs as knowledge discovery tools to decide whether a statement is true or false

$P \to Q$ Direct Proof Pf by Contrapos.

TODO:

Homework assignment 4 (due Tuesday May 14, 2024) $\forall x P(x)$ Univ Generalization Exhaustion (finite)

Review quiz based on class material each day (due Friday May 17, 2024).

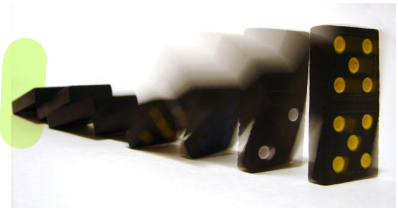
Homework assignment 5 (due Tuesday May 21, 2024)

P Proof by Contradiction

Week 7 Monday: Mathematical and Strong Induction

Visualizing induction

First domino: establishing property holds for simplest element



Proof by Mathematical Induction $\forall x \in \mathbb{Z}^{\geq b}\ P(x)$

To prove a universal quantification over the set of all integers greater than or equal to some base integer b,

Basis Step: Show the property holds for b. $P(b)$

Recursive Step: Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n+1$. $\forall n \in \mathbb{Z}^{\geq b}\ (P(n) \to P(n+1))$

Proof by Strong Induction

To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

Basis Step: Show the statement holds for b, $b+1$, …, $b+j$.

Recursive Step: Consider an arbitrary integer n greater than or equal to $b+j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b+1$, …, n, and use this and other facts to prove that the property holds for $n+1$.

different from one another

Theorem: Every positive integer is a sum of (one or more) distinct powers of 2. *Binary expansions exist!*

Recall the definition for binary expansion:

Definition For n a positive integer, the **binary expansion of** n is

n div 2 (half the number) $(a_{k-1}\cdots a_1 a_0)_2$ n mod 2

where k is a positive integer, $a_0, a_1, \ldots, a_{k-1}$ are each 0 or 1, $a_{k-1} \neq 0$, and

$$n = \sum_{i=0}^{k-1} a_i b^i$$

The idea in the "Least significant first" algorithm for computing binary expansions is that the binary expansion of *half* a number becomes *part* of the binary expansion of the number of itself. We can use this idea in a proof by strong induction that binary expansions exist for all positive integers n.

Goal: $\forall x \geq 1$ (x has a binary expansion)

Proof by strong induction, with $b = 1$ and $j = 0$.

↖ smallest integer in our domain

Basis step: WTS property is true about 1.

WTS 1 can be written as a sum of distinct powers of 2. But $2^0 = 1$. So writing 1 is a sum (with one term) of powers of 2.

Recursive step: Consider an arbitrary integer $n \geq 1$.

Assume (as the strong induction hypothesis, SIH) that the property is true about each of $1, \ldots, n$.

WTS that the property is true about $n + 1$.

Following algorithm we'd divide by 2 and $(\text{(n+1) div 2's binary expansion}\ (n+1 \bmod 2))_2$

Idea: We will apply the IH to $(n + 1)$ **div** 2.

Why is this ok?

Need to check that $(n+1)$ div 2 is an integer between 1 and n, inclusive.

- Is it an integer? Yes by def of div.
- Is $(n+1)$ div $2 \geq 1$? Yes, since $n \geq 1$ (by assumption)
- Is $(n+1)$ div $2 \leq n$? Yes, since $n+1 \leq n+n \leq 2n$ (b/c $1 \leq n$)

Why is this helpful?

By the IH, we can write $(n+1)$ **div** 2 as a sum of powers of 2. In other words, there are values $a_{k-1}, \ldots, a_0$ such that each a_i is 0 or 1, $a_{k-1} = 1$, and

$$\sum_{i=0}^{k-1} a_i 2^i = (n + 1) \textbf{ div } 2$$

Define the collection of coefficients

shift binary expansion for (n+1) div 2.

$$c_j = \begin{cases} a_{j-1} & \text{if } 1 \leq j \leq k \\ (n+1) \textbf{ mod } 2 & \text{if } j = 0 \end{cases}$$

use LSB for remainder when dividing n+1 by 2.

Calculating:

shifting means multiply by 2.

$$\sum_{j=0}^{k} c_j 2^j = c_0 + \sum_{j=1}^{k} c_j 2^j = c_0 + \sum_{i=0}^{k-1} c_{i+1} 2^{i+1} \qquad \text{re-indexing the summation}$$

$$= c_0 + 2 \cdot \sum_{i=0}^{k-1} c_{i+1} 2^i \qquad \text{factoring out a 2 from each term in the sum}$$

$$= c_0 + 2 \cdot \sum_{i=0}^{k-1} a_i 2^i \qquad \text{by definition of } c_{i+1}$$

$$= c_0 + 2\,(\,(n+1)\ \textbf{div}\ 2\,) \qquad \text{by IH}$$

$$= (\,(n+1)\ \textbf{mod}\ 2\,) + 2\,(\,(n+1)\ \textbf{div}\ 2\,) \qquad \text{by definition of } c_0$$

$$= n+1 \qquad \text{by definition of long division}$$

Thus, $n+1$ can be expressed as a sum of powers of 2, as required.

Representing positive integers with primes

A prime number is an integer >1 whose only positive factors are 1 and itself.

Theorem: Every positive integer *greater than 1* is a product of (one or more) primes.

Before we prove, let's try some examples:

$20 =$ 2 · 2 · 5

$100 =$ 2 · 2 · 5 · 5

$5 =$ 5

WTS $\forall x \in \mathbb{Z}^{\geq 2}$ x can be written as a product of primes.

Proof by strong induction, with $b = 2$ and $j = 0$.

Basis step: WTS property is true about 2.

Since 2 is itself prime, it is already written as a product of (one) prime.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume (as the strong induction hypothesis, SIH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about $n+1$: We want to show that $n+1$ can be written as a product of primes. Notice that $n+1$ is itself prime or it is composite.

Case 1: assume $n+1$ is prime and then immediately it is written as a product of (one) prime so we are done.

witness that n+1 is not prime.

Case 2: assume that $n+1$ is composite so there are integers x and y where $n+1 = xy$ and each of them is between 2 and n (inclusive). Therefore, the induction hypothesis applies to each of x and y so each of these factors of $n+1$ can be written as a product of primes. Multiplying these products together, we get a product of primes that gives $n+1$, as required.

Since both cases give the necessary conclusion, the proof by cases for the recursive step is complete.

Sending old-fashioned mail with postage stamps

Suppose we had postage stamps worth 5 cents and 3 cents. Which number of cents can we form using these stamps? In other words, which postage can we pay?

11? $2 \cdot 3 + 1 \cdot 5$

15? $0 \cdot 3 + 3 \cdot 5$

4? Impossible!

$$CanPay(0) \wedge \neg CanPay(1) \wedge \neg CanPay(2) \wedge$$
$$CanPay(3) \wedge \neg CanPay(4) \wedge CanPay(5) \wedge CanPay(6)$$
$$\neg CanPay(7) \wedge \forall n \in \mathbb{Z}^{\geq 8} CanPay(n)$$

where the predicate $CanPay$ with domain $\mathbb{N}$ is

there's a # of 5¢ stamps and there's a # of 3¢ stamps

$$CanPay(n) = \exists x \in \mathbb{N} \exists y \in \mathbb{N}(5x + 3y = n)$$

value to pay

Proof (idea): First, explicitly give witnesses or general arguments for postages between 0 and 7. To prove the universal claim, we can use mathematical induction or strong induction.

Approach 1, mathematical induction: if we have stamps that add up to n cents, need to use them (and others) to give $n + 1$ cents. How do we get 1 cent with just 3-cent and 5-cent stamps?
Either take away a 5-cent stamps and add two 3-cent stamps,
or take away three 3-cent stamps and add two 5-cent stamps.
The details of this proof by mathematical induction are making sure we have enough stamps to use one of these approaches.

Approach 2, strong induction: assuming we know how to make postage for **all** smaller values (greater than or equal to 8), when we need to make $n+1$ cents, add one 3 cent stamp to however we make $(n + 1) - 3$ cents.
The details of this proof by strong induction are making sure we stay in the domain of the universal when applying the induction hypothesis.

See Review Quiz for details

On Wednesday:

Finding a winning strategy for a game

Consider the following game: two players start with two (equal) piles of jellybeans in front of them. They take turns removing any positive integer number of jellybeans at a time from one of two piles in front of them in turns.

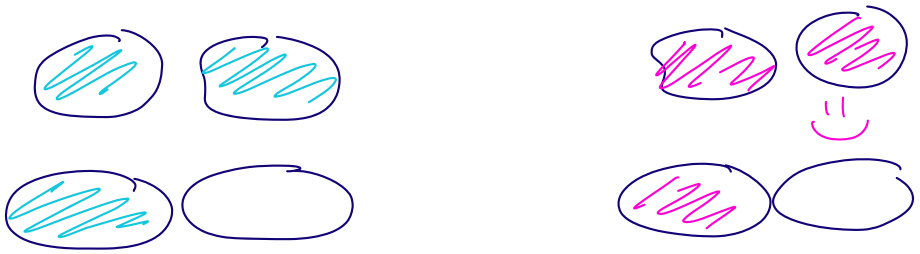
The player who removes the last jellybean wins the game.

Which player (if any) has a strategy to guarantee to win the game?

Try out some games, starting with 1 jellybean in each pile, then 2 jellybeans in each pile, then 3 jellybeans in each pile. Who wins in each game?

1 jb in each pile

2 jb in each pile



Notice that reasoning about the strategy for the 1 jellybean game is easier than about the strategy for the 2 jellybean game.

Formulate a winning strategy by working to transform the game to a simpler one we know we can win.

P2 takes the same # of jellybeans that P1 took, from the opposite pile.

Player 2's Strategy: Take the same number of jellybeans that Player 1 did, but from the opposite pile.

Why is this a good idea: If Player 2 plays this strategy, at the next turn Player 1 faces a game with the same setup as the original, just with fewer jellybeans in the two piles. Then Player 2 can keep playing this strategy to win.

Claim: Player 2's strategy guarantees they will win the game.

Proof: By strong induction, we will prove that for all positive integers n, Player 2's strategy guarantees a win in the game that starts with n jellybeans in each pile.

Basis step: WTS Player 2's strategy guarantees a win when each pile starts with 1 jellybean.

In this case, Player 1 has to take the jellybean from one of the piles (because they can't take from both piles at once). Following the strategy, Player 2 takes the jellybean from the other pile, and wins because this is the last jellybean.

Recursive step: Let n be a positive integer. As the strong induction hypothesis, assume that Player 2's strategy guarantees a win in the games where there are $1, 2, \ldots, n$ many jellybeans in each pile at the start of the game.

WTS that Player 2's strategy guarantees a win in the game where there are $n+1$ in the jellybeans in each pile at the start of the game.

In this game, the first move has Player 1 take some number, call it c (where $1 \leq c \leq n+1$), of jellybeans from one of the piles. Playing according to their strategy, Player 2 then takes the same number of jellybeans from the other pile.

whole pile

leave some jellybeans in both piles

Notice that $(c = n+1) \vee (c \leq n)$.

Case 1: Assume $c = n+1$, then in their first move, Player 2 wins because they take all of the second pile, which includes the last jellybean.

Case 2: Assume $c \leq n$. Then after Player 2's first move, the two piles have an equal number of jellybeans. The number of jellybeans in each pile is

$$(n+1) - c$$

and, since $1 \leq c \leq n$, this number is between 1 and n. Thus, at this stage of the game, the game appears identical to a new game where the two piles have an equal number of jellybeans between 1 and n. Thus, the strong induction hypothesis applies, and Player 2's strategy guarantees they win.

:)

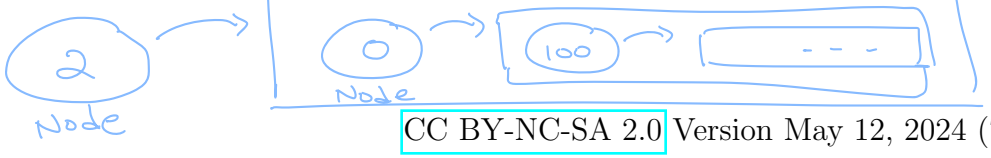
Representing collections of nonnegative integers

Data structure: * Array

| 2 | 0 | 100 | 20 | 5 | 7 | 18 |

How many?

* Linked List:

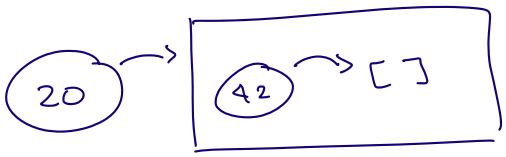


Week 7 Wednesday: Recursive Data Structures

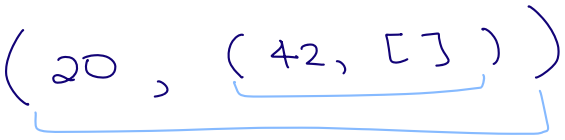
Definition The set of linked lists of natural numbers L is defined recursively by

Basis Step: $[] \in L$ (empty list)
Recursive Step: If $l \in L$ and $n \in \mathbb{N}$, then $(n, l) \in L$ (ordered pair; data stored in head node; list at "tail" i.e. rest of the list)

Visually:

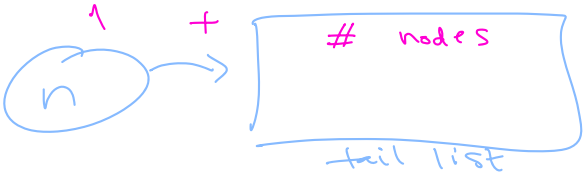


Example: the list with two nodes whose first node has 20 and whose second node has 42



Definition: The length of a linked list of natural numbers L, $length : L \to \mathbb{N}$ is defined by ("# of data nodes")

Basis Step: $length([]) = 0$ (empty list has no data nodes.)
Recursive Step: If $l \in L$ and $n \in \mathbb{N}$, then $length((n, l)) = 1 + length(l)$ ((n,l): list we care about; $length(l)$: output of function at a simpler input)



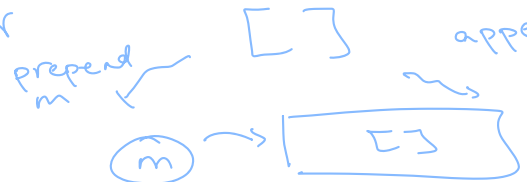
Definition: The function $prepend : L \times \mathbb{N} \to L$ that adds an element at the front of a linked list is defined by

$prepend((l, x)) = (x, l)$ (x: head; l: rest of our new list is the list we had in our input.)

Definition The function $append : L \times \mathbb{N} \to L$ that adds an element at the end of a linked list is defined by

Basis Step: If $m \in \mathbb{N}$ then (new data to add to the end.) $append((\,[\,], m)) = (m, [\,])$
Recursive Step: If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then (new data to add to the end.) $append((n, l), m) = (n, append((l, m)))$

Edge behavior



In English: The length of the result of adding a node (containing 100) to a list is greater than the length of the original list.

Claim: $\forall l \in L$ ($length($ $append($ $(l, 100)$ $)$ $) > length(l)$)

↑ domain is recursively defined.

Proof: By structural induction on L, we have two cases:

Basis Step

Goal

1. **To Show** $length($ $append($ $([], 100)$ $)$ $) > length($ $[]$ $)$	Because [] is the only element defined in the basis step of L, we only need to prove that the property holds for [].
2. **To Show** $length($ $(100, [])$ $) > length($ $[]$ $)$	By basis step in definition of *append*.
3. **To Show** $(1 + length($ $[]$ $)) > length($ $[]$ $)$	By recursive step in definition of *length*.
4. **To Show** $1 + 0 > 0$	By basis step in definition of *length*.
5. T	By properties of integers
QED	Because we got to T only by rewriting **To Show** to equivalent statements, using well-defined proof techniques, and applying definitions.

Simplify

Recursive Step

Consider an arbitrary: $l' \in L$, $n \in \mathbb{N}$, and we assume as the **induction hypothesis** that:

$$length($ $append($ $(l', 100$ $)$ $) > length(l')$$

Our goal is to show that $length($ $append($ $($ $(n, l'), 100$ $)$ $) > length($ (n, l') $)$ is also true. We start by working with one side of the candidate inequality:

$$\begin{aligned}
LHS &= length($ $append($ $($ $(n, l'), 100$ $)$ $) \\
&= length($ $(n, append($ $(l', 100)$ $)$ $) \quad \text{by the recursive definition of } append \\
&= 1 + length($ $append($ $(l', 100)$ $) \quad \text{by the recursive definition of } length \\
&> 1 + length(l') \quad \text{by the induction hypothesis} \\
&= length((n, l')) \quad \text{by the recursive definition of } length \\
&= RHS
\end{aligned}$$

Left Hand Side

right hand side

Prove or disprove: $\forall n \in \mathbb{N}\ \exists l \in L\ (\ length(l) = n\ )$

For each nonnegative integer, there is a linked list whose length is that integer.

By mathematical induction, we will prove that for each nonneg int n, $\exists l \in L\ (length(l) = n)$ is true.

Basis Step: WTS $\exists l \in L\ (length(l) = 0)$

Consider $l = []$. This is an element of L by basis step in defintion of L. Applying basis step in definition of length, $length([]) = 0$, as required.

Rec Step: Consider an arbitrary nonnegative integer n.

Assume, as the IH, that the existential statement is true about n.

WTS $\exists l \in L\ (length(l) = n+1)$

Since the existential statement is true about n, there is a witness for it, namely an element of L where the equality is true. Let's call this witness w.

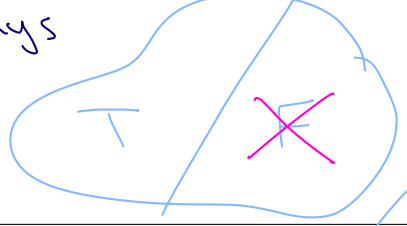
Define $l = (17, w)$

This is an element of L by the recursive step in the definition of L. Applying the recursive step in the definition of length, we get

$length(l) = 1 + length(w) \overset{IH}{=} 1+n$, as required ∎

Note: there's nothing special about 17. We can choose any nonnegative integer we like here, even one that depends on n

Contradiction: a proposition that always evaluates to F.



Week 7 Friday: Proof by Contradiction

choose r depending on context

New! Proof by Contradiction
To prove that a statement p is true, pick another statement r and once we show that $\neg p \to (r \wedge \neg r)$ then we can conclude that p is true.
Informally The statement we care about can't possibly be false, so it must be true.

if the statement were false then contradiction would be guaranteed

Least and greatest

For a set of numbers X, how do you formalize "there is a greatest X" or "there is a least X"?

$\exists a \in X \forall b \in X\ (b \leq a)$
"There is a greatest number in X"

$\exists a \in X\ (\forall b \in X\ (a \leq b))$
"There is a least number in X"

Prove ~~or disprove~~: There is a least prime number.

X = the set of prime numbers

A prime number is an integer greater than 1 whose only positive factors are 1 and itself.

Witness 2
- 2 is prime? - - - ✓
- Every prime number is greater than or equal to 2? - - - ✓

~~**Prove**~~ or **disprove**: There is a greatest integer.

X = the set of integers = $\mathbb{Z}$.
= the set given by the recursive definition:
Basis Step: $0 \in \mathbb{Z}$
Rec Step: If $n \in \mathbb{Z}$, $n+1 \in \mathbb{Z}$ and $n-1 \in \mathbb{Z}$

Approach 1, De Morgan's and universal generalization:

To disprove $\exists a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ (b \leq a)$
we need to prove $\neg \exists a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ (b \leq a)$
i.e. need to prove $\forall a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ (b > a)$
Univ generalization: consider arbitrary a. Need witness b with $b > a$. Consider $b = a+1$.
* domain ? * satisfies ?.

Approach 2, proof by contradiction:

WTS P = "There is no greatest integer"

Towards a contradiction, assume $\neg P$, namely that there is a greatest integer. WTS that this assumption leads to a contradiction.
From assumption, let C be a witness, a greatest integer.
By definition, $\forall b \in \mathbb{Z}\ (b \leq C)$. But $C+1$ is an integer so the universal guarantees that $C+1 \leq C$
By definition of $\leq$, this means $\neg (C+1 > C)$. r
But by definition of +, $C+1 > C$. r
i.e. we proved $r \wedge \neg r$ for some statement

Extra examples: Prove or disprove that $\mathbb{N}$, $\mathbb{Q}$ each have a least and a greatest element.

Definition: **Greatest common divisor** Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(\ (a,b)\ )$.

hcf highest common factor.

Why do we restrict to the situation where a and b are not both zero?

When $a=b=0$ every integer is a divisor of both a and b so there is no greatest common divisor.

Calculate $gcd(\ (10,15)\ )$

Positive factors of 10: 1, 2, 5, 10

Positive factors of 15: 1, 3, 5, 15

$gcd((10,15)) = 5$

Calculate $gcd(\ (10,20)\ )$

Positive factors of 10: 1, 2, 5, 10

Positive factors of 20: 1, 2, 4, 5, 10, 20

$gcd((10,20)) = 10$

Claim: For any integers a, b (not both zero), $gcd(\ (a,b)\ ) \geq 1$. $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ (\neg(a=0 \wedge b=0) \rightarrow gcd(a,b) \geq 1)$

Proof: *Show that* 1 *is a common factor of any two integers, so since the gcd is the greatest common factor it is greater than or equal to any common factor.*

Let a, b be arbitrary integers. Assume, towards direct proof that $\neg(a=0 \wedge b=0)$. Using DeMorgan's laws, this means $a \neq 0 \vee b \neq 0$. WTS $gcd((a,b)) \geq 1$. By assumption, $gcd((a,b))$ is well defined. Notice that $F((1,a))$, as witnessed by the integer a since $a = 1 \cdot a$. Similarly, $F((1,b))$, as witnessed by the integer b, since $b = 1 \cdot b$. Thus, 1 is a common divisor of a and b, so by definition of $gcd((a,b))$ as the greatest common divisor of a and b, $1 \leq gcd((a,b))$. ∎

Claim: For any positive integers a, b, $gcd(\ (a,b)\ ) \leq a$ and $gcd(\ (a,b)\ ) \leq b$.

Proof *Using the definition of gcd and the fact that factors of a positive integer are less than or equal to that integer.*

$\forall a \in \mathbb{Z}^+\ \forall b \in \mathbb{Z}^+\ (gcd((a,b)) \leq a \wedge gcd((a,b)) \leq b)$

Let a, b arbitrary positive integer

Subgoal ① WTS $gcd((a,b)) \leq a$. By definition $gcd((a,b))$ is a factor of a and a is positive, so by fact $gcd((a,b)) \leq a$.

Subgoal ② WTS $gcd((a,b)) \leq b$. Similarly, by definition, $gcd((a,b))$ is a factor of b and b is positive, so by fact, $gcd((a,b)) \leq b$.

Claim: For any positive integers a, b, if a divides b then $gcd(\ (a,b)\ ) = a$.

Proof *Using previous claim and definition of gcd.*

example $\gcd(\ (10,20)\ ) = 10$

Let a, b be arbitrary positive integers and assume, towards a direct proof, that $a \mid b$. Also, witnessed by the integer 1, we have that $a \mid a$. Thus, a is a common factor of a and b so (by definition of gcd), $\gcd(\ (a,b)\ ) \geq a$. However, from the previous claim we have $\gcd(\ (a,b)\ ) \leq a$. Thus, by properties of numbers, $\gcd(\ (a,b)\ ) = a$.

Claim: For any positive integers a, b, c, if there is some integer q such that $a = bq + c$,

$$gcd(\ (a,b)\ ) = gcd(\ (b,c)\ )$$

(a, b, c: remainder when divide a by b.)

Proof *Prove that any common divisor of a, b divides c and that any common divisor of b, c divides a.*

WTS $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \left(\exists q \in \mathbb{Z}(a = bq + c) \longrightarrow \gcd(\ (a,b)\ ) = \gcd(\ (b,c)\ ) \right)$

Let a, b, c be arbitrary positive integers.
Assume, towards a direct proof that $\exists q \in \mathbb{Z}(a = bq + c)$ and let q be an integer that witnesses this existential. To show $\gcd(\ (a,b)\ ) = \gcd(\ (b,c)\ )$ it's equivalent (using number properties) to show $\gcd(\ (a,b)\ ) \geq \gcd(\ (b,c)\ )$ and $\gcd(\ (a,b)\ ) \leq \gcd(\ (b,c)\ )$

Subgoal (1) WTS $\gcd(\ (a,b)\ ) \leq \gcd(\ (b,c)\ )$
By definition of gcd, it's enough to prove that $\gcd(\ (a,b)\ )$ is a common divisor of b and c.
By definition, $\gcd(\ (a,b)\ )$ is a divisor of b so it remains to prove that $\gcd(\ (a,b)\ )$ is a divisor of c.
$c = a - bq = q_1 \gcd(\ (a,b)\ ) - (q_2 \gcd(\ (a,b)\ ))q$ (where q_1 is a div $\gcd(\ (a,b)\ )$ and q_2 is b div $\gcd(\ (a,b)\ )$)
$= \gcd(\ (a,b)\ )(q_1 - q_2 q)$ ($q_1 - q_2 q$: an integer)
So $\gcd(\ (a,b)\ )$ is a divisor of c, as required

Subgoal (2) WTS $\gcd(\ (a,b)\ ) \geq \gcd(\ (b,c)\ )$
By definition of gcd, it's enough to prove that $\gcd(\ (b,c)\ )$ is a common divisor of a and b.
By definition, $\gcd(\ (b,c)\ )$ is a divisor of b, so it remains to prove that $\gcd(\ (b,c)\ )$ is a divisor of a.
$a = bq + c = (q_3 \gcd(\ (b,c)\ ))q + q_4 \gcd(\ (b,c)\ )$ (where q_3 is b div $\gcd(\ (b,c)\ )$ and q_4 is c div $\gcd(\ (b,c)\ )$)
$= \gcd(\ (b,c)\ )(q_3 q + q_4)$ ($q_3 q + q_4$: an integer)
So $\gcd(\ (b,c)\ )$ is a divisor of a, as required. ∎

Lemma: For any integers p, q (not both zero), $gcd\left(\left(\frac{p}{gcd(\ (p,q)\ )}, \frac{q}{gcd(\ (p,q)\ )} \right) \right) = 1$. In other words, can reduce to relatively prime integers by dividing by gcd.

Proof:

Write fractions in lowest terms! $\frac{10}{20} = \frac{10/10}{10/20} = \frac{1}{2}$.

Let x be arbitrary positive integer and assume that x is a factor of each of $\frac{p}{gcd(\ (p,q)\ )}$ and $\frac{q}{gcd(\ (p,q)\ )}$. This gives integers α, β such that

$$\alpha x = \frac{p}{gcd(\ (p,q)\ )} \qquad \beta x = \frac{q}{gcd(\ (p,q)\ )}$$

Multiplying both sides by the denominator in the RHS:

$$\alpha x \cdot gcd(\ (p,q)\ ) = p \qquad \beta x \cdot gcd(\ (p,q)\ ) = q$$

In other words, $x \cdot gcd(\ (p,q)\ )$ is a common divisor of p, q. By definition of gcd, this means

$$x \cdot gcd(\ (p,q)\ ) \leq gcd(\ (p,q)\ )$$

and since $gcd(\ (p,q)\ )$ is positive, this means, $x \leq 1$.

Sets of numbers

We've seen multiple representations of the set of positive integers (using base expansions and using prime factorization). Now we're going to expand our attention to other sets of numbers as well.

The **set of rational numbers**, $\mathbb{Q}$ is defined as

$$\left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\} \quad \text{or, equivalently,} \quad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^+ (p = x \cdot q)\}$$

Extra practice: Use the definition of set equality to prove that the definitions above give the same set.

We have the following subset relationships between sets of numbers:

$$\mathbb{Z}^+ \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

Which of the proper subset inclusions above can you prove?

Goal: The square root of 2 is not a rational number. In other words: $\neg\exists x \in \mathbb{Q}(x^2 - 2 = 0)$

Attempted proof: The definition of the set of rational numbers is the collection of fractions p/q where p is an integer and q is a nonzero integer. Looking for a **witness** p and q, we can write the square root of 2 as the fraction $\sqrt{2}/1$, where 1 is a nonzero integer. Since the numerator is not in the domain, this witness is not allowed, and we have shown that the square root of 2 is not a fraction of integers (with nonzero denominator). Thus, the square root of 2 is not rational.

The problem in the above attempted proof is that _____

Lemma 1: For every two integers a and b, not both zero, with $gcd(\ (a, b)\ ) = 1$, it is not the case that both a is even and b is even.

Lemma 2: For every integer x, x is even if and only if x^2 is even.

Proof: Towards a proof by contradiction, we will define a statement r such that $\sqrt{2} \in \mathbb{Q} \to (r \wedge \neg r)$.

Assume that $\sqrt{2} \in \mathbb{Q}$. Namely, there are positive integers p, q such that

$$\sqrt{2} = \frac{p}{q}$$

Let $a = \frac{p}{gcd(\ (p,q)\ )}$, $b = \frac{q}{gcd(\ (p,q)\ )}$, then

$$\sqrt{2} = \frac{a}{b} \qquad \text{and} \qquad gcd(\ (a, b)\ ) = 1$$

By Lemma 1, a and b are not both even. We define r to be the statement "a is even and b is even", and we have proved $\neg r$.

Squaring both sides and clearing denominator: $2b^2 = a^2$.

By definition of even, since b^2 is an integer, a^2 is even.

By Lemma 2, this guarantees that a is even too. So, by definition of even, there is some integer (call it c), such that $a = 2c$.

Plugging into the equation:

$$2b^2 = a^2 = (2c)^2 = 4c^2$$

and dividing both sides by 2

$$b^2 = 2c^2$$

and since c^2 is an integer, b^2 is even. By Lemma 2, b is even too. Thus, a is even and b is even and we have proved r.

In other words, assuming that $\sqrt{2} \in \mathbb{Q}$ guarantees $r \wedge \neg r$, which is impossible, so $\sqrt{2} \notin \mathbb{Q}$. QED

Review Quiz

1. Mathematical and strong induction for properties of numbers

   (a)

   In class, we proved the theorem that: Every positive integer is a sum of (one or more) distinct powers of 2.
   What's wrong with the following *attempted* proof of this fact?
   Attempted proof by mathematical induction, with $b = 1$.
   Basis step: WTS 1 can be written as a sum of (one or more) distinct powers of 2. Since $1 = 2^0$, we are done.
   Recursive step: Consider an arbitrary integer $n \geq 1$. By the IH, we can write n as a sum of distinct powers of 2. Since $1 = 2^0$, it is a power of 2 and we can add it as a term to this sum of powers of 2. When we do so, the terms sum to $n + 1$ and we are done.

   i. The basis step is not sufficient.
   ii. The induction hypothesis is not stated correctly.
   iii. It's wrong to say that 1 is a power of 2.
   iv. Adding the 2^0 to the sum of powers doesn't give the correct value.
   v. Adding the 2^0 to the sum of powers is problematic for a different reason.

   (b)

   In this question, we'll consider two possible proofs of the statement

   $$\forall n \in \mathbb{Z}^{\geq 8} \exists x \in \mathbb{N} \exists y \in \mathbb{N}(5x + 3y = n)$$

   i. First approach, using mathematical induction ($b = 8$).
   Basis step: WTS property is true about 8. Consider the witnesses $x = 1$, $y = 1$. These are nonnegative integers and $5 \cdot 1 + 3 \cdot 1 = 8$, as required.
   Recursive step: Consider an arbitrary $n \geq 8$. Assume (as the induction hypothesis, IH) that there are nonnegative integers x, y such that $n = 5x + 3y$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$. We consider two cases, depending on whether any 5 cent stamps are used for n.
   Case 1: Assume $x \geq 1$ (we assume that at least one 5 cent stamp is used for n). Define $x' = x - 1$ and $y' = y + 2$ (both in $\mathbb{N}$ by case assumption).
   Calculating:

   $$\begin{aligned} 5x' + 3y' &\overset{\text{by def}}{=} 5(x-1) + 3(y+2) = 5x - 5 + 3y + 6 \\ &\overset{\text{rearranging}}{=} (5x + 3y) - 5 + 6 \\ &\overset{\text{IH}}{=} n - 5 + 6 = n + 1 \end{aligned}$$

   Case 2: Assume $x = 0$. Therefore $n = 3y$, so since $n \geq 8$, $y \geq 3$. Define $x' = 2$ and $y' = y - 3$ (both in $\mathbb{N}$ by case assumption). Calculating:

   $$\begin{aligned} 5x' + 3y' &\overset{\text{by def}}{=} 5(2) + 3(y-3) = 10 + 3y - 9 \\ &\overset{\text{rearranging}}{=} 3y + 10 - 9 \\ &\overset{\text{IH and case}}{=} n + 10 - 9 = n + 1 \end{aligned}$$

Since the goal has been proved from each case, the proof by cases is complete and we have proved the recursive step. □

Why was the recursive step split into two cases?

A. Because there are two variables x and y that need witnesses.
B. Because the statement has alternating quantifiers $\forall$ and $\exists$
C. Because the witness values need to be nonnegative and subtraction may lead to negative values.
D. Because the domain is all integers greater than or equal to 8.
E. Because there are two steps in the recursive definition of $\mathbb{N}$

ii. Second approach, by strong induction ($b = 8$ and $j = 2$)

Basis step: WTS property is true about $8, 9, 10$

- Consider the witnesses $x = 1$, $y = 1$. These are nonnegative integers and $5 \cdot 1 + 3 \cdot 1 = 8$, as required.
- Consider the witnesses $x = 0$, $y = 3$. These are nonnegative integers and $5 \cdot 0 + 3 \cdot 3 = 9$, as required.
- Consider the witnesses $x = 2$, $y = 0$. These are nonnegative integers and $5 \cdot 2 + 3 \cdot 0 = 10$, as required.

Recursive step: Consider an arbitrary $n \geq 10$. Assume, as the strong induction hypothesis, that the property is true about each of $8, 9, 10, \ldots, n$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$.

Since Blank 1, by the strong induction hypothesis, there are nonnegative integers x, y such that $(n + 1) - 3 = 5x + 3y$. Choosing Blank 2 works because

$$5x' + 3y' = 5x + 3y + 3 = (n + 1) - 3 + 3 = n + 1.$$

Choose a true and useful statement to fill in Blank 1.

A. $n \geq 10$ and hence $(n + 1) - 3 \geq 8$
B. $n \geq 8$ and hence $(n + 1) - 3 \geq 8$
C. $n \geq 8$ and hence $(n + 1) \geq 9$

Choose the appropriate statement to fill in Blank 2.

A. $x' = x, y' = y$
B. $x' = x + 1, y' = y + 1$
C. $x' = x + 1, y' = y$
D. $x' = x, y' = y + 1$
E. $x' = x - 1, y' = y - 1$
F. $x' = x - 1, y' = y$
G. $x' = x, y' = y - 1$

2. Winning strategy.

Recall the game Nim from class.

(a) Why did we use strong induction to prove that Player 2's strategy guarantees a win?

i. Because there are two players in the game.
ii. Because each turn can involve a player taking some positive number of jellybeans from a pile, not just one jellybean.

iii. Because the strategy player 2 uses depends on what player 1 does.

iv. Because the set of natural numbers is recursively defined.

(b) If we modify the game so that in each turn, a player could take jellybeans from one or both piles, which player has a winning strategy?

i. Player 1.

ii. Player 2.

iii. Neither in general, the existence of a winning strategy for the players depends on how many jellybeans are in each pile to start.

(c) If we modify the game so that in each turn, a player must take exactly one jellybean, which player has a winning strategy?

i. Player 1.

ii. Player 2.

iii. Neither in general, the existence of a winning strategy for the players depends on how many jellybeans are in each pile to start.

3. Linked lists.

Recall the definition of linked lists from class.

Consider this (incomplete) definition:

Definition The function $increment :$ _____ that adds 1 to the data in each node of a linked list is defined by:

		$increment :$ _____	$\to$ _____
Basis Step:		$increment([])$	$= []$
Recursive Step:	If $l \in L, n \in \mathbb{N}$	$increment((n, l))$	$= (1 + n, increment(l))$

Consider this (incomplete) definition:

Definition The function $sum : L \to \mathbb{N}$ that adds together all the data in nodes of the list is defined by:

		$sum : L$	$\to \mathbb{N}$
Basis Step:		$sum([])$	$= 0$
Recursive Step:	If $l \in L, n \in \mathbb{N}$	$sum((n, l))$	$=$ _____

You will compute a sample function application and then fill in the blanks for the domain and codomain of each of these functions.

(a) Based on the definition, what is the result of $increment((4, (2, (7, []))))$? Write your answer directly with no spaces.

(b) Which of the following describes the domain and codomain of *increment*?

i. The domain is L and the codomain is $\mathbb{N}$

ii. The domain is L and the codomain is $\mathbb{N} \times L$

iii. The domain is $L \times \mathbb{N}$ and the codomain is L

iv. The domain is $L \times \mathbb{N}$ and the codomain is $\mathbb{N}$

v. The domain is L and the codomain is L

vi. None of the above

(c) Assuming we would like $sum((5, (6, [])))$ to evaluate to 11 and $sum((3, (1, (8, []))))$ to evaluate to 12, which of the following could be used to fill in the definition of the recursive case of *sum*?

i. $\begin{cases} 1 + sum(l) & \text{when } n \neq 0 \\ sum(l) & \text{when } n = 0 \end{cases}$

ii. $1 + sum(l)$

iii. $n + increment(l)$

iv. $n + sum(l)$

v. None of the above

(d) Choose only and all of the following statements that are **well-defined**; that is, they correctly reflect the domains and codomains of the functions and quantifiers, and respect the notational conventions we use in this class. Note that a well-defined statement may be true or false.

i. $\forall l \in L\,(sum(l))$

ii. $\exists l \in L\,(sum(l) \wedge length(l))$

iii. $\forall l \in L\,(sum(increment(l)) = 10)$

iv. $\exists l \in L\,(sum(increment(l)) = 10)$

v. $\forall l \in L\,\forall n \in \mathbb{N}\,((n \times l) \subseteq L)$

vi. $\forall l_1 \in L\,\exists l_2 \in L\,(increment(sum(l_1)) = l_2)$

vii. $\forall l \in L\,(length(increment(l)) = length(l))$

(e) Choose only and all of the statements in the previous part that are both well-defined and true.

4. Primes and divisors

(a)

Recall that a prime factorization is a product of primes (potentially with some of the primes occurring more than once). Select all and only the correct prime factorizations of positive integers.

i. $2 \cdot 2 \cdot 2 \cdot 2$

ii. 3

iii. $3 \cdot 4 \cdot 5$

iv. $17 \cdot 21$

v. $2 \cdot 11$

(b)

We will prove that there is no greatest prime number

Proof Assume, towards a BLANK1, that there is a greatest prime number, call it n_{BIG}. In particular, this means that there are finitely many primes. Let's label them in order $p_1, \ldots, p_n$ where $p_1 = 2$ and $p_n = n_{BIG}$. Choose $r =$ BLANK2. We proved in class that r is **true**. It remains to show that (under our assumption) r is **false**, because that would complete the contradiction argument. Define the integer

$$C = (p_1 \cdots p_n) + 1$$

This is a positive integer greater than 1. However, we will show that it does not have any prime factors and thus is not a product of primes. By our assumption, the only prime numbers are $p_1, \ldots, p_n$. Thus, to show that C does not have any prime factors means to show that p_i is not a factor of C for each value of i from 1 to n. Towards a universal generalization, let i be an arbitrary between 1 and n (inclusive). We need to prove that p_i is not a factor of C. By definition of C,

$$C = p_i(p_1 \cdots p_{i-1} p_{i+1} \cdots p_n) + 1$$

so C **div** $p_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_n$ and C **mod** $p_i = 1$ (because $p_i > 1$ since it is prime). Since C **mod** $p_i \neq 0$, p_i is not a factor of C. Thus C witnesses that the universal claim is false, and we have proved that r is false.

i. BLANK1

A. universal generalization
B. proof of existential by witness
C. direct proof
D. proof by contrapositive
E. proof by cases
F. proof by contradiction

ii. BLANK2

A. The least prime number is 2.
B. There is a greatest prime number.
C. There is a least prime number.
D. Every positive integer greater than 1 is a product of primes.
E. Every positive integer has a base expansion.
F. There is a greatest integer.
G. There is no greatest integer.

(c)

We will consider two ways for calculating the gcd. In each part of the question, you'll calculate $gcd(\ (306, 120)\ )$.

i. The first approach uses some of the claims we proved in class to get the following algorithm:

Euclidean algorithm for calculating greatest common divisor

```
1  procedure Euclidean(a: a positive integer, b: a positive integer)
2  x := a
3  y := b
4  while y ≠ 0
5     r := x mod y
6     x := y
7     y := r
8  return x {the result of gcd( (a,b) )}
```

Tracing this algorithm, lines 2 and 3 initialize the variables

$$x := 306 \qquad y := 120$$

Entering the while loop, the variable r is initialized to

$$r := 66$$

because $306 = 2 \cdot 120 + 66$ so 306 **mod** $120 = 66$. Calculate and fill in the updated value of r in each subsequent iteration of the **while** loop, and then give the value of $gcd(\ (306, 120)\ )$.

ii. The second approach uses the representation of positive integers greater than 1 as products of primes. To calculate $gcd(\ (a, b)\ )$ we find the prime factorizations of each of a and b, and then calculate the number that results from multiplying together terms p^c where p is a prime that appears in *both* prime factorizations of a and b and c is the *minimum* number of times p appears in the two factorizations.
Select the prime factorizations for 306 and 120 and express their *gcd* as a product of powers of primes.
Possible factorizations:

A. $306 = 2 \cdot 153$, $120 = 2 \cdot 60$

B. $306 = 1 \cdot 2 \cdot 3 \cdot 3 \cdot 17$, $120 = 1 \cdot 3 \cdot 5 \cdot 8$

C. $306 = 2 \cdot 3 \cdot 3 \cdot 17$, $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

Possible *gcd* choices:

A. 2

B. $2 \cdot 3$

C. $5 \cdot 17$

D. $2^3 \cdot 3^2$

E. $2^3 \cdot 3^2 \cdot 5 \cdot 8 \cdot 17$

5. Proof strategies

(a)

Select all and only the situations in which the given proof strategy would be available.

i. When might it be appropriate to use induction?

A. To prove that an existential claim over the set of integers is true.

B. To prove that a universal claim over the real numbers is true.

C. To prove that a conditional claim is true.

D. None of the above.

ii. When might it be appropriate to use proof by contradiction?

A. To prove that an existential claim over the set of integers is true.

B. To prove that a universal claim over the real numbers is true.

C. To prove that a conditional claim is true.

D. None of the above.

(b)

Goals for this question: recognize that we can prove the same statement in different ways. Trace proofs and justify why they are valid.

Below are two proofs of the same statement: fill in the blanks with the expressions below.

Claimed statement: **(a)**_____

Proof 1: Using De Morgan's law for quantifiers, we can rewrite this statement as a universal of the negation of the body of the statement. Towards a proof by universal generalization, let x be an arbitrary element of $\mathbb{Z}$. Then we need to show that

(b)_____

We proceed by contradiction to show that

(x is odd $\wedge$ x^2 is even) $\rightarrow$ **(c)**_____

We assume by direct proof that (x is odd$\wedge x^2$ is even). Then, (x^2 is even) follows directly from this assumption, so by definition of conjunction, we must show that (x^2 is not even) to complete the proof. From the assumption, we have that (x is odd). Applying the definition of odd, $x = 2k + 1$ for some $k \in \mathbb{Z}$. Then $x^2 = 4k^2 + 4k + 1$. We can rewrite the right hand side to $2(2k^2+2k)+1$. This shows that x^2 is odd by the definition of odd, since choosing $j = 2k^2 + 2k$ gives us $j \in \mathbb{Z}$ with $x^2 = 2j + 1$. Since a number is either even or odd and not both, and x^2 is odd, then it must not be even. This concludes the proof, as we have assumed the negation of the original statement and deduced a contradiction from this assumption.

Proof 2:

1.	**To Show** $\forall x \in \mathbb{Z} \neg(x \text{ is odd} \wedge x^2 \text{ is even})$	Rewriting statement using De Morgan's law for quantifiers
2.	**Choose arbitrary** $x \in \mathbb{Z}$ **To Show (d)**_____	By **(e)**_____
3.	**To Show** x is odd $\rightarrow \neg(x^2$ is even)	Rewrite previous **To Show** using logical equivalence
4.	**Assume** x is odd **To Show** $\neg(x^2$ is even)	By **(f)**_____
5.	**To Show** x^2 is odd	Rewrite previous **To Show** using definition of even, odd
6.	**Use the witness** k, an integer, where $x = 2k + 1$	By existential definition of x being odd
7.	**Choose the witness** $j = 2k^2 + 2k$, an integer **To Show** $x^2 = 2j + 1$	Show this new **To Show** is true to prove the existential definition of x^2 being odd
8.	**To Show** $(2k + 1)^2 = 2j + 1$	Rewrite previous **To Show** using definition of k
9.	**To Show** $(2k + 1)^2 = 2(2k^2 + 2k) + 1$	Rewrite previous **To Show** using definition of j
10.	**To Show** T	By algebra: multiplying out the LHS; factoring the RHS
	QED	Because we got to T only by rewriting **To Show** to equivalent statements, using valid proof techniques and definitions.

Consider the following expressions as options to fill in the two proofs above. Give your answer as one of the numbers below for each blank a-c. You may use some numbers for more than one blank, but each letter only uses one of the expressions below.

i. $\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x^2 \text{ is even})$
ii. $\neg\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x^2 \text{ is even})$
iii. $\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x \text{ is even})$
iv. $\neg\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x \text{ is even})$
v. $\exists x \in \mathbb{Z}\,(x^2 \text{ is odd} \wedge x^2 \text{ is even})$
vi. $\neg\exists x \in \mathbb{Z}\,(x^2 \text{ is odd} \wedge x^2 \text{ is even})$
vii. $(x^2 \text{ is even} \wedge x^2 \text{ is not even})$
viii. $\neg(x \text{ is odd} \wedge x^2 \text{ is even})$
ix. $(x \text{ is odd} \wedge x^2 \text{ is even})$
x. $(x \text{ is odd} \wedge x \text{ is not odd})$
xi. $\neg(x \text{ is odd} \wedge x \text{ is not odd})$
xii. x^2 is even
xiii. x^2 is odd
xiv. universal generalization
xv. proof by cases
xvi. direct proof
xvii. proof by contraposition
xviii. proof by contradiction

