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

TODO:

No class Monday of Week 7 (02/16/2026) in observance of UCSD holiday.

Review quiz based on Week 6 class material (due Monday 02/16/2026)

Midquarter feedback: please let us know what's working well for you and what isn't. `https://canvas.ucsd.edu/courses/71479/quizzes`

Review quiz based on Week 7 class material (due Monday 02/23/2026)

CC BY-NC-SA 2.0 Version February 7, 2026 (1)

Week 7 Wednesday: Recursive Data Structures

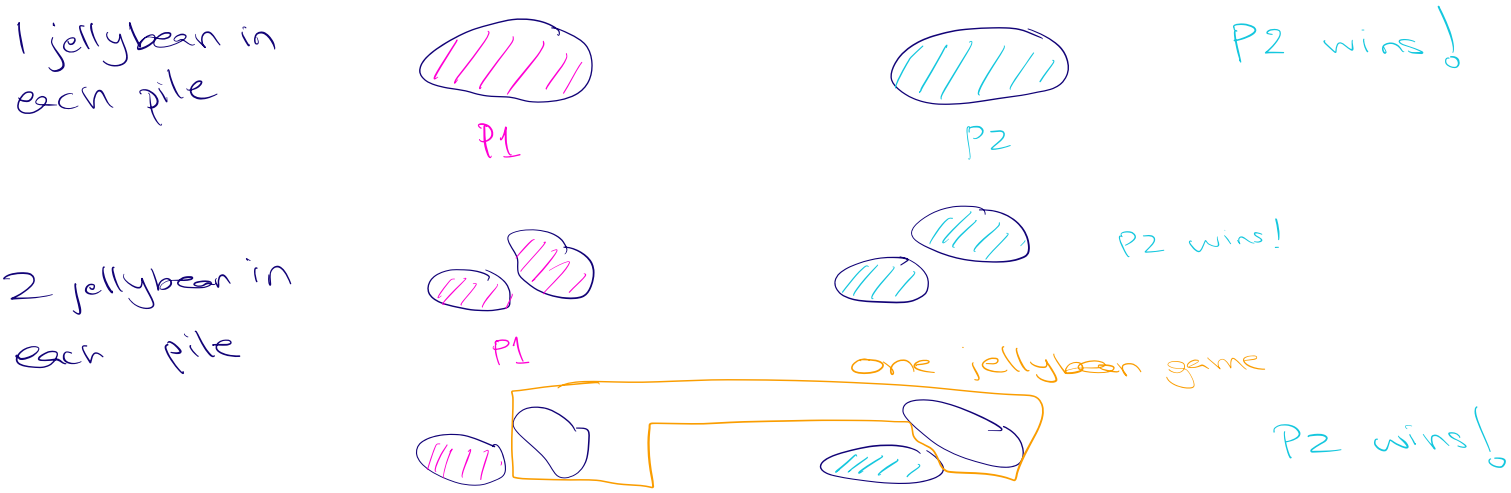
Finding a winning strategy for a game

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.

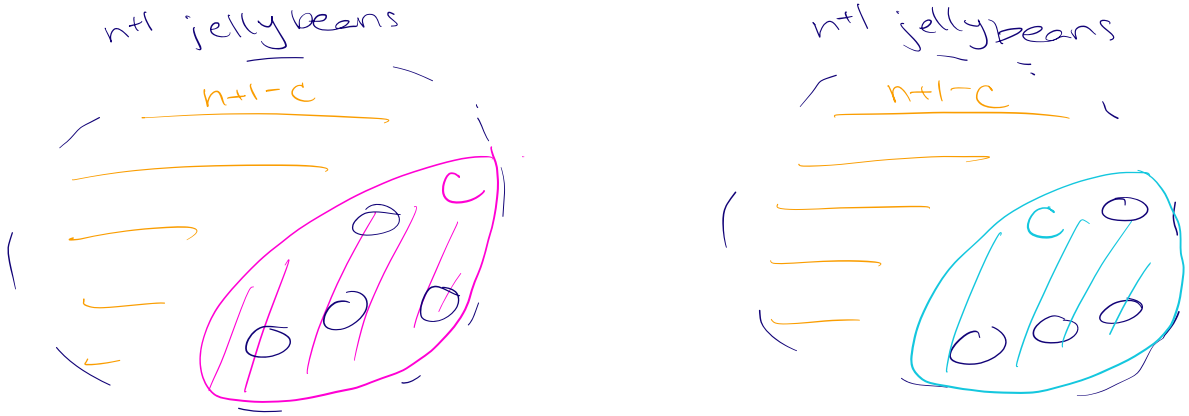
Which player (if any) has a strategy to guarantee to win the game?

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?



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.



Assumption (strong induction hypothesis): Player 2's strategy is a winning strategy for all games where pile size is $1, \ldots, n$

CC BY-NC-SA 2.0

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 $n+1$ 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.

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

$$(n+1) - c$$

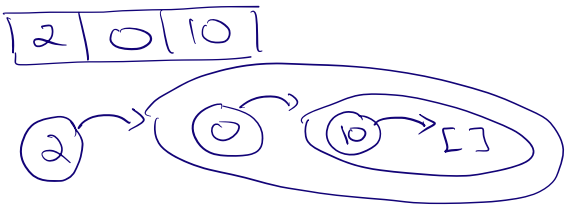
and, since $1 \leq c \leq n$, this number is between 1 and n. Thus, at this stage of the game, the game appears identical to a new game where the two piles have an equal number of jellybeans between 1 and n. Thus, the strong induction hypothesis applies, and Player 2's strategy guarantees they win. QED.

Next example: a new recursively defined set

Storing collections of nonnegative integers

Array

Linked List



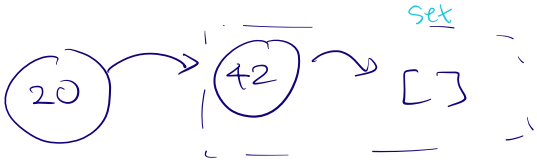
CC BY-NC-SA 2.0 Version February 7, 2026 (3)

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 $(n, l) \in L$ (simpler element of the set; data for new node; new element of the set)

Visually:



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

$(20, (42, []))$

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

Basis Step: $length([]) = 0$

Recursive Step: If $l \in L$ and $n \in \mathbb{N}$, then $length((n, l)) = 1 + length(l)$

$length((20, (42, [])))$ $n=20$, $l=(42,[])$ $= 1 + length((42, []))$ $n=42$, $l=[]$

$= 1 + 1 + length([]) = 2$

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

$prepend((l, x))$ (new data node to add at the head; existing list) $= (x, l)$ (head, tail)

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 $append([], m) = (m, [])$

Recursive Step: If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then

$append((n, l), m) = (n, append(l, m))$ (list; applying a function; list)

$l = []$ putting m at "the end" : $(m, [])$

putting m at "the end" $(n, append((l, m)))$

CC BY-NC-SA 2.0

No matter what list we start with, when we add to it a node with data 100 we get a longer list.

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

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

Basis Step

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.

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:

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

CC BY-NC-SA 2.0

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

for each there is

Proof by mathematical induction

Basis step: WTS $\exists l \in L\ (\text{length}(l) = 0)$

Need a witness, let's try $l = []$.

In domain? Yes, by basis step in recursive definition of L, $[] \in L$.

Satisfies predicate? Yes, by basis step in recursive definition of length, length $([]) = 0$, as required □

Recursive step: Let n be arbitrary nonnegative integer.

WTS $\exists l \in L(\text{length}(l) = n) \longrightarrow \exists l \in L\ (\text{length}(l) = n+1)$

Assume (as the induction hypothesis) that $\exists l \in L\ (\text{length}(l) = n)$

and let l_n be a witness for this existential claim.

Consider $(n+1, l_n)$.

In domain? Yes, by recursive step in recursive definition of L, since $l_n \in L$ and $n+1 \in \mathbb{N}$, $(n+1, l_n) \in L$.

Satisfies predicate? Yes, by recursive step in recursive definition of length $\text{length}((n+1, l_n)) = 1 + \text{length}(l_n)$

and by choice of l_n, $\text{length}(l_n) = n$

so $\text{length}((n+1, l_n)) = 1 + n = n+1$,

as required.

Thus, we have proved $\exists l \in L(\text{length}(l) = n+1)$ under the assumption $\exists l \in L\ (\text{length}(l) = n)$ ▨

CC BY-NC-SA 2.0 Version February 7, 2026 (6)

Week 7 Friday: Proof by Contradiction

"show that it's impossible for statement we care about to be false"

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.

any other contradiction would be ok too

Least and greatest

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

$\exists a \in X \; \forall b \in X \; (a \geq b)$, $\exists a \in X \; \forall b \in X \; (a \leq b)$

$a \neq b \to a > b$

$\exists a \in Primes \; \forall b \in Primes \; (a \leq b)$

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

Witness $a = 2$ works because it's prime (its only positive factors are 1 and 2) and all primes are defined to be > 1.

~~**Prove** or~~ **disprove**: There is a greatest integer. $\neg \exists a \in \mathbb{Z} \; \forall b \in \mathbb{Z} \; (a \geq b)$

Approach 1, De Morgan's and universal generalization:

WTS $\forall a \in \mathbb{Z} \; \exists b \in \mathbb{Z} \; (a < b)$

For arbitrary integer a, need witness b

Consider $b = a+1$, then it's an integer and it's strictly greater than a, so it works.

Approach 2, proof by contradiction:

WTS "There isn't a greatest integer"

Towards a contradiction, assume there is a greatest integer. WTS this assumption leads to a contradiction.

From assumption, let c be witness greatest integer. Consider $c+1$. This is an integer, and by properties of addition $c < c+1$.

By properties of inequalities, $\neg(c+1 \leq c)$.

Since $c+1$ is an integer, and c is greatest integer, $c+1 \leq c$.

So $r \wedge \neg r$, $\lightning$

CC BY-NC-SA 2.0 Version February 7, 2026 (7)

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 $gcd(\ (a,b)\ )$.

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

When $a=b=0$, all nonnegative integers are divisors of both a and b so there is no greatest common divisor.

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

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

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

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

$10 = 2 \cdot 5^1$

$20 = 2^2 \cdot 5^1$

Claim: For any integers a, b (not both zero), $gcd(\ (a,b)\ ) \geq 1$.

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 and b be be arbitrary integers
Assume, towards direct proof that $\neg(a=0 \wedge b=0)$.
WTS $\gcd((a,b)) \geq 1$. By assumption, $\gcd((a,b))$ is defined. Notice that 1 is a factor of a (as witnessed by the integer a, since $a = 1 \cdot a$) and 1 is a factor of b (as witnessed by the integer b, since $b = 1 \cdot b$), so 1 is a common divisor of a and b.
Since $\gcd((a,b))$ is 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.*

WTS $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ (\gcd((a,b)) \leq a \wedge \gcd((a,b)) \leq b)$
Let a, b be arbitrary positive integers (towards universal generalization).
Subgoal ① WTS $\gcd((a,b)) \leq a$. By definition of gcd, $\gcd((a,b))$ is a factor of a and is positive, so by facts about numbers from last week, $\gcd((a,b)) \leq a$.
Subgoal ② WTS $\gcd((a,b)) \leq b$. Identical argument, with b instead of a ☒

CC BY-NC-SA 2.0

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

Proof *Using previous claim and definition of gcd.*

Towards universal generalization, let a and b be arbitrary positive integers. Towards direct proof, assume a divides b; namely a is a factor of b. Also, a is a factor of a (as witnessed by the integer 1 since $a = 1 \cdot a$) so a is a common factor of a and b. By definition of gcd as the greatest common factor, $a \leq gcd((a,b))$. By previous claim, $gcd((a,b)) \leq a$ so the two inequalities together give $gcd((a,b)) = a$ ☑

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

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

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

WTS $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ ([\exists q \in \mathbb{Z} (a = bq + c)] \rightarrow gcd((a,b)) = gcd((b,c)))$

Let a, b, c be arbitrary positive integers. Assume $\exists q \in \mathbb{Z}$ ($a = bq + c$) and let q be an integer that witnesses this existential.

WTS $gcd((a,b)) = gcd((b,c))$. Equivalently, WTS $gcd((a,b)) \leq gcd((b,c)) \wedge gcd((a,b)) \geq gcd((b,c))$

Subgoal ① WTS $gcd((a,b)) \leq gcd((b,c))$. It's enough to show $gcd((a,b))$ is a common divisor of b and c. By definition, $gcd((a,b))$ is a divisor of b. To prove it is also a divisor of c, we notice that $a = bq + c$ means $c = a - bq$ and if $q_1 = a$ div $gcd((a,b))$ and $q_2 = b$ div $gcd((a,b))$, we have $c = q_1 gcd((a,b)) - q_2 q\ gcd((a,b)) = (q_1 - q_2 q) gcd((a,b))$ so $gcd((a,b))$ divides c ☑ ($q_1 - q_2 q$ an integer)

Subgoal ② WTS $gcd((a,b)) \geqslant gcd((b,c))$ It's enough to show $gcd((b,c))$ is a common divisor of a and b. By definition, $gcd((b,c))$ is a divisor of b. To show it's also a divisor of a, we notice $a = bq + c = r_1 gcd((b,c))\ q + r_2 gcd((b,c))$ for $r_1 = b$ div $gcd((b,c))$ and $r_2 = c$ div $gcd((b,c))$. Thus $a = (r_1 q + r_2) gcd((b,c))$ so $gcd((b,c))$ divides a ☑ ($r_1 q + r_2$ an integer)

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.

"Reducing fractions"

Proof:

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, $x \leq 1$.

CC BY-NC-SA 2.0

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

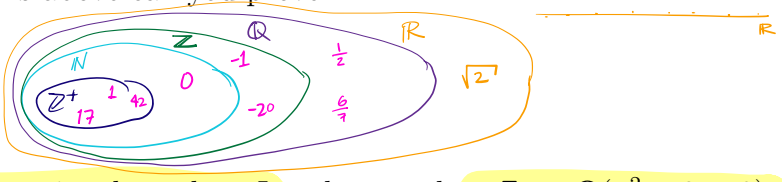
$$\left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\} \quad \text{or, equivalently,} \quad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^+ (p = x \cdot q)\}$$

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 it proves the chosen witness doesn't work, but that's not enough to rule out any other witness.

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

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

lowest terms.

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 $\neg r$.

CC BY-NC-SA 2.0

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

CC BY-NC-SA 2.0