Math 321: yet more about proofs

Kameryn J Williams

University of Hawaiʻi at Mānoa

Fall 2020

Last time

- Last time we talked about proof strategies involving negations, and before that we talked about proof strategies involving implications.
- Now let's talk about proof strategies involving quantifiers.

How to prove an existential statement

- Some statements in mathematics are existential statements, asserting that there is a mathematical object satisfying some property. These are of the form $\exists x\ P(x)$.

How to prove an existential statement

- Some statements in mathematics are existential statements, asserting that there is a mathematical object satisfying some property. These are of the form $\exists x\ P(x)$.
- One strategy to prove an existential statement is straightforward: produce an object a which satisfies $P(a)$.

A quick example

Problem

Prove there exists an even number which is the sum of two primes.

A quick example

Problem

Prove there exists an even number which is the sum of two primes.

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$

A quick example

Problem

Prove there exists an even number which is the sum of two primes.

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$
- $100 = 11 + 89$
- $\vdots$

A quick example

Problem

Prove there exists an even number which is the sum of two primes.

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$
- $100 = 11 + 89$
- $\vdots$

A much harder problem (so hard that mathematicians still don't know the answer): prove that every even number ≥ 4 is a sum of two primes.

Proving a universal statement

Let's think a bit about why it's so much harder to prove the universal statement "every even number ≥ 4 is a sum of two primes".

- Translated into logical notation, this is "$\forall x \in \mathbb{N}$ (x is even $\wedge$ $x \geq 4$) $\to$ x is the sum of two primes".

Proving a universal statement

Let's think a bit about why it's so much harder to prove the universal statement "every even number ≥ 4 is a sum of two primes".

- Translated into logical notation, this is "$\forall x \in \mathbb{N}$ (x is even $\wedge$ $x \geq 4$) $\rightarrow$ x is the sum of two primes".
- So to prove this, it's not enough to just look at one example. Instead we have to somehow prove something about infinitely many examples at once.
- This takes a different strategy.

Proving a universal statement

How do we prove $\forall x\ P(x) \to Q(x)$?

- Consider an arbitrary object a, where the only thing you know about a is that $P(a)$. (a has to be a new name for an object; you can't pick a name you've already assigned.)
- Try to prove $Q(a)$.

Proving a universal statement

How do we prove $\forall x \; P(x) \to Q(x)$?

- Consider an arbitrary object a, where the only thing you know about a is that $P(a)$. (a has to be a new name for an object; you can't pick a name you've already assigned.)
- Try to prove $Q(a)$.

You can also phrase this in terms of knowns and goals:

knowns	goals
$\vdots$	$\forall x \; P(x) \to Q(x)$

gets transformed into

knowns	goals
$P(a)$	$Q(a)$
$\vdots$	

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

This can be formulated as: $\forall x$ (x is rational $\rightarrow \exists p, q \in \mathbb{Z}$ [$x = p/q$ and $\gcd(p, q) = 1$]).

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

This can be formulated as: $\forall x$ (x is rational $\to \exists p, q \in \mathbb{Z}$ [$x = p/q$ and $\gcd(p, q) = 1$]).

So the strategy is thus: we take as a known "x is rational", where we get no other information about x, and the goal is to produce p and q with the desired property.

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

Consider an arbitrary rational number x. We are given very little information about x—only that x is rational. So let's use this piece of information: by the definition of a rational number, we know that $x = a/b$ for some integers a and b.

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

Consider an arbitrary rational number x. We are given very little information about x—only that x is rational. So let's use this piece of information: by the definition of a rational number, we know that $x = a/b$ for some integers a and b.

It could be that $\gcd(a, b) = 1$, in which case we would be done. But in general we cannot expect to be so lucky. What do in general?

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

Consider an arbitrary rational number x. We are given very little information about x—only that x is rational. So let's use this piece of information: by the definition of a rational number, we know that $x = a/b$ for some integers a and b.

It could be that $\gcd(a, b) = 1$, in which case we would be done. But in general we cannot expect to be so lucky. What do in general?

Let $c = \gcd(a, b)$. Then $p = a/c$ and $q = b/c$ are integers and $x = p/q$. The only remaining thing to see is that $\gcd(p, q) = 1$.

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

Consider an arbitrary rational number x. We are given very little information about x—only that x is rational. So let's use this piece of information: by the definition of a rational number, we know that $x = a/b$ for some integers a and b.

It could be that $\gcd(a, b) = 1$, in which case we would be done. But in general we cannot expect to be so lucky. What do in general?

Let $c = \gcd(a, b)$. Then $p = a/c$ and $q = b/c$ are integers and $x = p/q$. The only remaining thing to see is that $\gcd(p, q) = 1$.

Let's prove this by contradiction. Suppose $\gcd(p, q) = d > 1$. But then $p/d = a/(cd)$ and $q/d = b/(cd)$ are integers. So $cd > c$ divides both a and b. But this contradicts that $c = \gcd(a, b)$.

A simple example

Problem

Prove that every rational number can be written in the form p/q where p and q are integers whose greatest common divisor is 1.

Consider an arbitrary rational number x. We are given very little information about x—only that x is rational. So let's use this piece of information: by the definition of a rational number, we know that $x = a/b$ for some integers a and b.

It could be that $\gcd(a, b) = 1$, in which case we would be done. But in general we cannot expect to be so lucky. What do in general?

Let $c = \gcd(a, b)$. Then $p = a/c$ and $q = b/c$ are integers and $x = p/q$. The only remaining thing to see is that $\gcd(p, q) = 1$.

Let's prove this by contradiction. Suppose $\gcd(p, q) = d > 1$. But then $p/d = a/(cd)$ and $q/d = b/(cd)$ are integers. So $cd > c$ divides both a and b. But this contradicts that $c = \gcd(a, b)$. □

Let's write this up

Theorem

Every rational number can be written as a ratio of two integers whose greatest common divisor is 1*.*

Proof.

Let x be a rational number. Then, by definition $x = a/b$ for some integers a and b. Let $c = \gcd(a, b)$. Then $p = a/c$ and $q = b/c$ are also integers and $x = p/q$.

Suppose toward a contradiction that $\gcd(p, q) \neq 1$. Then $d = \gcd(p, q) > 1$. So we get that $p/d = a/(cd)$ and $q/d = b/(cd)$ are both integers. But this implies that $cd > c$ divides both a and b, contradicting that $c = \gcd(a, b)$. So it must be that $\gcd(p, q) = 1$. □

Using quantified statements as knowns

We've just seen an example how to use existential statements as known. Saying "x is rational" is exactly saying "there exist integers a, b so that $x = a/b$", and we don't get to know anything about a and b beyond this fact.

Using quantified statements as knowns

We've just seen an example how to use existential statements as known. Saying "x is rational" is exactly saying "there exist integers a, b so that $x = a/b$", and we don't get to know anything about a and b beyond this fact.

In general, to use $\exists x\ P(x)$ you get to introduce a new object a so that $P(a)$, but you aren't allowed to know anything else about a.

Using quantified statements as knowns

We've just seen an example how to use existential statements as known. Saying "x is rational" is exactly saying "there exist integers a, b so that $x = a/b$", and we don't get to know anything about a and b beyond this fact.

In general, to use $\exists x\ P(x)$ you get to introduce a new object a so that $P(a)$, but you aren't allowed to know anything else about a.

For using universal statements, this is usually in the form $\forall x\ (P(x) \to Q(x))$. For these, if we ever have an object a and we know $P(a)$, then we can conclude $Q(a)$.