Math 321: Introduction, II

Kameryn J Williams

University of Hawaiʻi at Mānoa

Spring 2021

Last time

Last time, we proved that $\sqrt{2}$ is irrational. An important step in the proof was the fact that any rational number p/q can be written in reduced form where the numerator and denominator have no common factors.

Last time

Last time, we proved that $\sqrt{2}$ is irrational. An important step in the proof was the fact that any rational number p/q can be written in reduced form where the numerator and denominator have no common factors.

- But we never proved this.

Last time

Last time, we proved that $\sqrt{2}$ is irrational. An important step in the proof was the fact that any rational number p/q can be written in reduced form where the numerator and denominator have no common factors.

- But we never proved this.
- Let's do so now.

A definition

Definition

Two integers p and q are relatively prime if their greatest common divisor is 1. That is, they are relatively prime if the largest integer which divides both p and q is 1.

A definition

Definition

Two integers p and q are relatively prime if their greatest common divisor is 1. That is, they are relatively prime if the largest integer which divides both p and q is 1. To be even more precise, p and q are relatively prime if the largest integer k so that $p = ka$ and $q = kb$, for some integers a, b, is $k = 1$.

Note that 1 is a divisor of any integer—$p = 1 \cdot p$—so any two integers must have a common divisor. It's when no larger integer is a common divisor that they are relatively prime.

A definition

Definition

Two integers p and q are relatively prime if their greatest common divisor is 1. That is, they are relatively prime if the largest integer which divides both p and q is 1. To be even more precise, p and q are relatively prime if the largest integer k so that $p = ka$ and $q = kb$, for some integers a, b, is $k = 1$.

Note that 1 is a divisor of any integer—$p = 1 \cdot p$—so any two integers must have a common divisor. It's when no larger integer is a common divisor that they are relatively prime.

- Are 0 and n relatively prime?

A lemma

Lemma

Any nonzero rational number can be written as p/q where p and q are relatively prime.

A lemma is a side result that's used to prove a larger theorem.

A lemma

Lemma

Any nonzero rational number can be written as p/q where p and q are relatively prime.

A lemma is a side result that's used to prove a larger theorem.

Proof.

Consider the rational number p'/q'. Let p be the smallest positive integer for which there is some integer q so that $p'/q' = p/q$.

A lemma

Lemma

Any nonzero rational number can be written as p/q where p and q are relatively prime.

A lemma is a side result that's used to prove a larger theorem.

Proof.

Consider the rational number p'/q'. Let p be the smallest positive integer for which there is some integer q so that $p'/q' = p/q$. Let's see that p and q are relatively prime. We will prove this by contradiction.

A lemma

Lemma

Any nonzero rational number can be written as p/q where p and q are relatively prime.

A lemma is a side result that's used to prove a larger theorem.

Proof.

Consider the rational number p'/q'. Let p be the smallest positive integer for which there is some integer q so that $p'/q' = p/q$. Let's see that p and q are relatively prime. We will prove this by contradiction.
Suppose that k divides both p and q, where $k > 1$. That is, $p = ka$ and $q = kb$ for some integers a and b. But then, $\frac{p}{q} = \frac{ka}{kb} = \frac{a}{b}$, and $a < p$ is positive. This contradicts that p was the smallest positive integer we could put in the numerator, so it must be impossible that p and q have a common divisor > 1. □

A further question

This proof made use of a principle, known as the least number principle:

- If there is a natural number with a certain property, there is a *smallest* natural number with that property.

A further question

This proof made use of a principle, known as the least number principle:

- If there is a natural number with a certain property, there is a *smallest* natural number with that property.
- It can also be phrased in terms of sets: if $X \subseteq \mathbb{N}$ is a nonempty set then X has a smallest element.

A further question

This proof made use of a principle, known as the least number principle:

- If there is a natural number with a certain property, there is a *smallest* natural number with that property.
- It can also be phrased in terms of sets: if $X \subseteq \mathbb{N}$ is a nonempty set then X has a smallest element.

Here's a reasonable question to have at this point:

- Why justify a fact—you can simplify fractions—I already know and love with a new principle I've never heard of and have no reason to believe?

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.
- So let's search for it!

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.
- So let's search for it!
- Start with 0. If it satisfies the property, we are done.

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.
- So let's search for it!
- Start with 0. If it satisfies the property, we are done.
- If not, look at 1. If it satisfies the property, we are done.

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.
- So let's search for it!
- Start with 0. If it satisfies the property, we are done.
- If not, look at 1. If it satisfies the property, we are done.
- If we've looked at $0, 1, \ldots, n$ and not yet found it, look at $n + 1$.

The least number principle, in brief

We'll cover this in more detail when we get to mathematical induction, but here's a brief justification for the least number principle:

- We know there are natural numbers satisfying a property, and we want to find a smallest natural number with the property.
- So let's search for it!
- Start with 0. If it satisfies the property, we are done.
- If not, look at 1. If it satisfies the property, we are done.
- If we've looked at $0, 1, \ldots, n$ and not yet found it, look at $n + 1$.
- This search will eventually stop, because we know there's some n with the property.

An alternate proof that $\sqrt{2}$ is irrational

We can prove $\sqrt{2}$ is irrational directly from the least number principle.

An alternate proof that $\sqrt{2}$ is irrational

We can prove $\sqrt{2}$ is irrational directly from the least number principle.

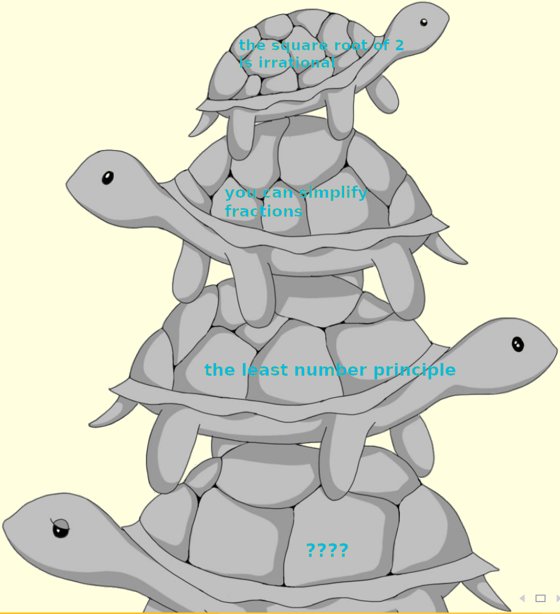
Proof.

Suppose toward a contradiction that $\sqrt{2}$ is rational. By the least number principle we may pick natural numbers p, q so that $\sqrt{2} = p/q$ and p is as small as possible for such a representation. As before, some algebra yields $p^2 = 2q^2$ so p is even, and we also get as before that q is even. That is, we can write $p = 2a$ and $q = 2b$ for natural numbers a and b. We then get

$$\sqrt{2} = \frac{p}{q} = \frac{2a}{2b} = \frac{a}{b}.$$

Then a witnesses that p was not actually least, a contradiction. □

Can we go deeper?



Can we go deeper?

- You could justify the least number principle by a proof appealing to even more fundamental ideas.
- But this has to stop somewhere, or else your proofs would be infinite in length, and no one has time to read an infinite proof.

Can we go deeper?

- You could justify the least number principle by a proof appealing to even more fundamental ideas.
- But this has to stop somewhere, or else your proofs would be infinite in length, and no one has time to read an infinite proof.
- Mathematicians call the basic starting points axioms.

Can we go deeper?

- You could justify the least number principle by a proof appealing to even more fundamental ideas.
- But this has to stop somewhere, or else your proofs would be infinite in length, and no one has time to read an infinite proof.
- Mathematicians call the basic starting points axioms.
- But we won't be breaking things down to the axioms.
  - The point of this class is to understand how proofs work, not to figure out just what minimal starting point we can take to do mathematics.
  - So for us, we will freely use mathematical facts you already know.
  - Where we do prove facts you already know—such as the fact that fractions can be simplified—the point is to practice understanding proofs, not to convince you this fact is true.
  - When writing your own proofs—homework, etc.—feel free to use things you already know. But if you're asked to prove X and you already know X, then don't use X, as that would be a circular argument.

Let's return to a question from last time

On Monday, I ended lecture with a question for you: is $\sqrt{3}$ irrational?

Let's return to a question from last time

On Monday, I ended lecture with a question for you: is $\sqrt{3}$ irrational?

- The answer is yes, and we can modify our proof that $\sqrt{2}$ is irrational to prove this.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where p and q are relatively prime.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 3q^2$. That is p^2 is a multiple of 3 and so p is also a multiple of 3.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 3q^2$. That is p^2 is a multiple of 3 and so p is also a multiple of 3. So we can write $p = 3k$ for some integer k. Substituting this into the previous equation and doing a bit of algebra gives $q^2 = 3k^2$.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 3q^2$. That is p^2 is a multiple of 3 and so p is also a multiple of 3. So we can write $p = 3k$ for some integer k. Substituting this into the previous equation and doing a bit of algebra gives $q^2 = 3k^2$. So q^2 is a multiple of 3, and hence also q is a multiple of 3.

$\sqrt{3}$ is irrational

Theorem

$\sqrt{3}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 3q^2$. That is p^2 is a multiple of 3 and so p is also a multiple of 3. So we can write $p = 3k$ for some integer k. Substituting this into the previous equation and doing a bit of algebra gives $q^2 = 3k^2$. So q^2 is a multiple of 3, and hence also q is a multiple of 3.

So p and q are relatively prime, but are both multiples of 3. This is impossible, so it must be that $\sqrt{3}$ is irrational. □

$\sqrt{4}$ is irrational????

Let's generalize this further. We replaced 2 with 3, now replace 3 with 4.

Theorem

$\sqrt{4}$ is irrational.

$\sqrt{4}$ is irrational????

Let's generalize this further. We replaced 2 with 3, now replace 3 with 4.

Theorem

$\sqrt{4}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{4}$ is rational. Then we can write $\sqrt{4} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 4p^2$. That is p^2 is a multiple of p and so p is also a multiple of 4. So we can write $p = 4k$ for some integer k. Substituting this into the previous equation and doing a bit of algebra gives $q^2 = 4k^2$. So q^2 is a multiple of 4, and hence also q is a multiple of 4. So p and q are relatively prime, but are both multiples of 4. This is impossible, so it must be that $\sqrt{4}$ is irrational. □

$\sqrt{4}$ is irrational????

Let's generalize this further. We replaced 2 with 3, now replace 3 with 4.

Theorem

$\sqrt{4}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{4}$ is rational. Then we can write $\sqrt{4} = p/q$ where p and q are relatively prime. Some algebra yields that $p^2 = 4p^2$. That is p^2 is a multiple of p and so p is also a multiple of 4. So we can write $p = 4k$ for some integer k. Substituting this into the previous equation and doing a bit of algebra gives $q^2 = 4k^2$. So q^2 is a multiple of 4, and hence also q is a multiple of 4. So p and q are relatively prime, but are both multiples of 4. This is impossible, so it must be that $\sqrt{4}$ is irrational. □

Something's wrong, since $\sqrt{4} = 2$ and 2 is rational.