Math 321: Some number theory

Kameryn J Williams

University of Hawai‘i at Mānoa

Spring 2021

Last time

Last week, we proved that $\sqrt{2}$ and $\sqrt{3}$ are irrational. We also "proved" that $\sqrt{4}$ is irrational. To understand better just why the proof didn't work for the 4 case, and to see how to properly generalize it, we need to do a bit of number theory.

Last time

Last week, we proved that $\sqrt{2}$ and $\sqrt{3}$ are irrational. We also "proved" that $\sqrt{4}$ is irrational. To understand better just why the proof didn't work for the 4 case, and to see how to properly generalize it, we need to do a bit of number theory.

Number theory is the branch of mathematics which studies the natural numbers. Central to number theory is the prime numbers.

Prime numbers

Definition

An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

Prime numbers

Definition

An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

- Why require $p > 1$? Why isn't 1 prime?

Prime numbers

Definition

An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

- Why require $p > 1$? Why isn't 1 prime?

We could define things differently and let 1 be prime. And it's straightforward to transfer from a definition disallowing 1 to a definition allowing 1—let's call this second definition prime'.

- If I prove a theorem like "all prime numbers are XYZ", you can translate it to a theorem like "all prime' numbers > 1 are XYZ".

Prime numbers

Definition

An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

- Why require $p > 1$? Why isn't 1 prime?

We could define things differently and let 1 be prime. And it's straightforward to transfer from a definition disallowing 1 to a definition allowing 1—let's call this second definition prime'.

- If I prove a theorem like "all prime numbers are XYZ", you can translate it to a theorem like "all prime' numbers > 1 are XYZ".

So the question really is which definition is more convenient.

Prime numbers

Definition

An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

- Why require $p > 1$? Why isn't 1 prime?

We could define things differently and let 1 be prime. And it's straightforward to transfer from a definition disallowing 1 to a definition allowing 1—let's call this second definition prime'.

- If I prove a theorem like "all prime numbers are XYZ", you can translate it to a theorem like "all prime' numbers > 1 are XYZ".

So the question really is which definition is more convenient.

It turns out the no 1 definition is more convenient in most contexts.

Prime factorization

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

Prime factorization

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

There's a couple corner cases we need to address.

- The prime factorization of 13 is: $13 = 13$. That is, we factor 13 as the product of just one prime. (And similar for any other prime.)

Prime factorization

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

There's a couple corner cases we need to address.

- The prime factorization of 13 is: $13 = 13$. That is, we factor 13 as the product of just one prime. (And similar for any other prime.)
- 1 is the product of zero primes, the empty product.
  - We want to define the empty product to be 1 because 1 is the multiplicative identity—for any x we have $1 \cdot x = x$.
  - Compare to how the empty sum is 0—if you add together zero many numbers their sum should be 0.

Prime factorization

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

There's a couple corner cases we need to address.

- The prime factorization of 13 is: $13 = 13$. That is, we factor 13 as the product of just one prime. (And similar for any other prime.)
- 1 is the product of zero primes, the empty product.
  - We want to define the empty product to be 1 because 1 is the multiplicative identity—for any x we have $1 \cdot x = x$.
  - Compare to how the empty sum is 0—if you add together zero many numbers their sum should be 0.
  - But at the end of the day, this is just a definition, and we could use a different one. We use this one because it's more convenient, like how we defined primes so that 1 is not prime.

The fundamental theorem of arithmetic

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

This theorem is within our grasp and we will indeed prove it.

The fundamental theorem of arithmetic

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

This theorem is within our grasp and we will indeed prove it.

- This theorem is an example of what mathematicians call a existence and uniqueness result.
- It asserts two things:
  - For each positive integer n there exists a prime factorization for n; and
  - This prime factorization is unique.

The fundamental theorem of arithmetic

Theorem (Fundamental theorem of arithmetic)

Every positive integer has a unique factorization as a product of prime numbers.

This theorem is within our grasp and we will indeed prove it.

- This theorem is an example of what mathematicians call a existence and uniqueness result.
- It asserts two things:
  - For each positive integer n there exists a prime factorization for n; and
  - This prime factorization is unique.

So we have two things to prove, and will prove them separately.

Existence

Theorem

Every positive integer has a prime factorization.

Existence

Theorem

Every positive integer has a prime factorization.

Our proof uses mathematical induction, a principle we will study in more detail shortly. To prove something is true for all positive integers we show that if it's true for all positive integers $< n$ then it must also be true for n.

Existence

Theorem

Every positive integer has a prime factorization.

Our proof uses mathematical induction, a principle we will study in more detail shortly. To prove something is true for all positive integers we show that if it's true for all positive integers $< n$ then it must also be true for n.

Proof.

The number 1 is the empty product, so it trivially works.

Existence

Theorem

Every positive integer has a prime factorization.

Our proof uses mathematical induction, a principle we will study in more detail shortly. To prove something is true for all positive integers we show that if it's true for all positive integers $< n$ then it must also be true for n.

Proof.

The number 1 is the empty product, so it trivially works. Now consider $n > 1$ and suppose that every positive integer $< n$ has a prime factorization. There are two cases to consider.

Existence

Theorem

Every positive integer has a prime factorization.

Our proof uses mathematical induction, a principle we will study in more detail shortly. To prove something is true for all positive integers we show that if it's true for all positive integers $< n$ then it must also be true for n.

Proof.

The number 1 is the empty product, so it trivially works. Now consider $n > 1$ and suppose that every positive integer $< n$ has a prime factorization. There are two cases to consider.

Case 1: Suppose n is prime. Then n has the trivial prime factorization $n = n$ and we are done.

Case 2: Suppose n is not prime. Then $n = ab$ for some positive integers $a, b < n$. Both a and b have prime factorizations. Multiplying them together gives a prime factorization for n. □

An alternate way to formulate the proof

We could instead formulate this proof using the least number principle.

An alternate way to formulate the proof

We could instead formulate this proof using the least number principle.

Proof.

Suppose toward a contradiction that there is a positive integer without a prime factorization. By the least number principle there is a smallest counterexample. That is, there is a positive integer n with no prime factorization but every positive integer $< n$ has a prime factorization.

An alternate way to formulate the proof

We could instead formulate this proof using the least number principle.

Proof.

Suppose toward a contradiction that there is a positive integer without a prime factorization. By the least number principle there is a smallest counterexample. That is, there is a positive integer n with no prime factorization but every positive integer $< n$ has a prime factorization. It cannot be that $n = 1$ or n is prime, as those trivially have prime factorizations.

An alternate way to formulate the proof

We could instead formulate this proof using the least number principle.

Proof.

Suppose toward a contradiction that there is a positive integer without a prime factorization. By the least number principle there is a smallest counterexample. That is, there is a positive integer n with no prime factorization but every positive integer $< n$ has a prime factorization. It cannot be that $n = 1$ or n is prime, as those trivially have prime factorizations.

So it must be that $n = ab$ for positive integers $a, b < n$. But by multiplying together the prime factorizations for a and b we get a prime factorization for n.

An alternate way to formulate the proof

We could instead formulate this proof using the least number principle.

Proof.

Suppose toward a contradiction that there is a positive integer without a prime factorization. By the least number principle there is a smallest counterexample. That is, there is a positive integer n with no prime factorization but every positive integer $< n$ has a prime factorization. It cannot be that $n = 1$ or n is prime, as those trivially have prime factorizations.

So it must be that $n = ab$ for positive integers $a, b < n$. But by multiplying together the prime factorizations for a and b we get a prime factorization for n. This is a contradiction, as n was supposed to have no prime factorization. So it must be that we were wrong to assume there is a positive integer without a prime factorization. □

Uniqueness

Proving the uniqueness of prime factorizations is trickier.

We will need to prove a series of lemmas to get to it.

Euclidean division

This lemma essentially says that you can do long division with integers.

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Euclidean division

This lemma essentially says that you can do long division with integers.

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

The connection to long division probably is clearer if I explain the mnemonic behind the variable names:

- n is for numerator
- d is for denominator
- q is for quotient
- r is for remainder

Euclidean division

This lemma essentially says that you can do long division with integers.

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

The connection to long division probably is clearer if I explain the mnemonic behind the variable names:

- n is for numerator
- d is for denominator
- q is for quotient
- r is for remainder

This is another existence and uniqueness result, and we have to prove both of them.

Euclidean division: uniqueness

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Uniqueness.

Euclidean division: uniqueness

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Uniqueness.

Fix n and d, and suppose both q_0, r_0 and q_1, r_1 satisfy $n = q_i d + r_i$ and $0 \leq r_i < d$.

Euclidean division: uniqueness

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Uniqueness.

Fix n and d, and suppose both q_0, r_0 and q_1, r_1 satisfy $n = q_i d + r_i$ and $0 \leq r_i < d$. Let's do a bit of algebra. We have $q_0 d + r_0 = q_1 d + r_1$, and rearrange to $r_1 - r_0 = (q_0 - q_1)d$. That is, $r_1 - r_0$ is a multiple of d.

Euclidean division: uniqueness

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Uniqueness.

Fix n and d, and suppose both q_0, r_0 and q_1, r_1 satisfy $n = q_i d + r_i$ and $0 \leq r_i < d$. Let's do a bit of algebra. We have $q_0 d + r_0 = q_1 d + r_1$, and rearrange to $r_1 - r_0 = (q_0 - q_1)d$. That is, $r_1 - r_0$ is a multiple of d. Since $-d < r_1 - r_0 < d$, we get that $r_1 - r_0 = 0$, that is $r_1 = r_0$.

Euclidean division: uniqueness

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Uniqueness.

Fix n and d, and suppose both q_0, r_0 and q_1, r_1 satisfy $n = q_i d + r_i$ and $0 \leq r_i < d$. Let's do a bit of algebra. We have $q_0 d + r_0 = q_1 d + r_1$, and rearrange to $r_1 - r_0 = (q_0 - q_1)d$. That is, $r_1 - r_0$ is a multiple of d. Since $-d < r_1 - r_0 < d$, we get that $r_1 - r_0 = 0$, that is $r_1 = r_0$. It now immediately follows that $q_1 = q_0$. □

Euclidean division: existence

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Existence.

Euclidean division: existence

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Existence.

Let $q + 1$ be the smallest natural number so that $n < (q + 1)d$. We can use the least number principle here because $(n + 1)$ works: $n < (n + 1)d$. Note that $0 < q + 1$ because $n \geq 0$.

Euclidean division: existence

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Existence.

Let $q+1$ be the smallest natural number so that $n < (q+1)d$. We can use the least number principle here because $(n+1)$ works: $n < (n+1)d$. Note that $0 < q+1$ because $n \geq 0$. Now consider $q = (q+1) - 1$. We have $q \geq 0$. And $qd \leq n < qd + d$, by choice of $q+1$.

Euclidean division: existence

Lemma

For positive integers n and d there are unique integers q and r so that $n = qd + r$ and $0 \leq r < d$.

Proof of Existence.

Let $q+1$ be the smallest natural number so that $n < (q+1)d$. We can use the least number principle here because $(n+1)$ works: $n < (n+1)d$. Note that $0 < q+1$ because $n \geq 0$. Now consider $q = (q+1) - 1$. We have $q \geq 0$. And $qd \leq n < qd + d$, by choice of $q+1$.
Because $qd \leq n$, there must be $r \geq 0$ so that $qd + r = n$, namely $r = n - qd$. And $r < d$ because $qd + r = n < qd + d$. □

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

This lemma is of the form "for all... there exists...", asserting that for all objects of a certain type there is an object satisfying a certain property. Many statements in mathematics are of this form.

The way we prove this is: we assume we are given integers a and b which are relatively prime, and then we try to find the desired x and y.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

This lemma is of the form "for all... there exists...", asserting that for all objects of a certain type there is an object satisfying a certain property. Many statements in mathematics are of this form.

The way we prove this is: we assume we are given integers a and b which are relatively prime, and then we try to find the desired x and y.

In this case, we will be indirect; rather than directly exhibiting how to compute x and y from a and b we will just show they exist.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

Proof.

By the least number principle, let d be the smallest positive integer which can be written as a integer linear combination of a and b, that is, $d = ax + by$ for some integers x and y. We can apply the least number principle because $a = a \cdot 1 + b \cdot 0$, and indeed this implies $d \leq a$. Note that if we can show that $d = 1$ then we will be done.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

d is the smallest integer > 0 so that $d = ax + by$ for some integers x and y.

Proof that $d = 1$.

To prove this, we show that d divides both a and b. This is enough, since 1 is the only positive integer with this property.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

d is the smallest integer > 0 so that $d = ax + by$ for some integers x and y.

Proof that $d = 1$.

To prove this, we show that d divides both a and b. This is enough, since 1 is the only positive integer with this property. By the Euclidean division lemma: $a = qd + r$ for q and $0 \leq r < d$.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

d is the smallest integer > 0 so that $d = ax + by$ for some integers x and y.

Proof that $d = 1$.

To prove this, we show that d divides both a and b. This is enough, since 1 is the only positive integer with this property. By the Euclidean division lemma: $a = qd + r$ for q and $0 \leq r < d$. Now some algebra:

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

We have written r as an integer linear combination of a and b. Since $r < d$ and d was the smallest *positive* such number, the only possibility is that $r = 0$.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

d is the smallest integer > 0 so that $d = ax + by$ for some integers x and y.

Proof that $d = 1$.

To prove this, we show that d divides both a and b. This is enough, since 1 is the only positive integer with this property. By the Euclidean division lemma: $a = qd + r$ for q and $0 \leq r < d$. Now some algebra:

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

We have written r as an integer linear combination of a and b. Since $r < d$ and d was the smallest *positive* such number, the only possibility is that $r = 0$. So $a = qd$, meaning that d divides a.

Bézout's identity

Lemma

For any integers a and b which are relatively prime, there are integers x and y so that $1 = ax + by$.

d is the smallest integer > 0 so that $d = ax + by$ for some integers x and y.

Proof that $d = 1$.

To prove this, we show that d divides both a and b. This is enough, since 1 is the only positive integer with this property. By the Euclidean division lemma: $a = qd + r$ for q and $0 \leq r < d$. Now some algebra:

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

We have written r as an integer linear combination of a and b. Since $r < d$ and d was the smallest *positive* such number, the only possibility is that $r = 0$. So $a = qd$, meaning that d divides a. A similar argument, where we divide b by d, shows that d is a divisor of b. □

A criticism of this proof

This proof is non-constructive: we argued that x and y must exist, but we didn't give any way to calculate them.

A criticism of this proof

This proof is non-constructive: we argued that x and y must exist, but we didn't give any way to calculate them.

- This is good enough for proving Bézout's identity, and it will be good enough for applying the lemma.
- But if you want to actually know what x and y are for a specific a and b, this doesn't help at all.

A criticism of this proof

This proof is non-constructive: we argued that x and y must exist, but we didn't give any way to calculate them.

- This is good enough for proving Bézout's identity, and it will be good enough for applying the lemma.
- But if you want to actually know what x and y are for a specific a and b, this doesn't help at all.
- There are other proofs which do give you a way to explicitly compute x and y.
- These are good, because they give you extra information.
- But they are also longer. I went with the shorter proof that gives less info because it's enough for what we need.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

A few comments before the proof:

- This theorem is an "if... then..." statement. This is a common form to see in mathematical statements.
- We prove it by assuming the if and proving the then.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

A few comments before the proof:

- This theorem is an "if... then..." statement. This is a common form to see in mathematical statements.
- We prove it by assuming the if and proving the then.
- The then here is an or statement—p divides a or p divides b.
- In mathematics, we use "or" to mean the inclusive or, allowing both options to be true. This is in contrast to ordinary English usage, but in math it's generally more convenient.
  - We don't want to rule out cases like $p = a = b = 2$.
  - If you do want to rule out having both options being true, you can say something like "... then precisely one of the following is true:..."

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

A few comments before the proof:

- This theorem is an "if... then..." statement. This is a common form to see in mathematical statements.
- We prove it by assuming the if and proving the then.
- The then here is an or statement—p divides a or p divides b.
- In mathematics, we use "or" to mean the inclusive or, allowing both options to be true. This is in contrast to ordinary English usage, but in math it's generally more convenient.
  - We don't want to rule out cases like $p = a = b = 2$.
  - If you do want to rule out having both options being true, you can say something like "... then precisely one of the following is true:..."
- To prove this "A or B" statement we will prove that if A is false then B must be true. So either A is true, in which case we are done, or A is false in which case B is true and we are done.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

Proof.

Suppose that p is prime and p divides ab.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

Proof.

Suppose that p is prime and p divides ab. Suppose that p does not divide a, and we want to now see that p divides b.

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

Proof.

Suppose that p is prime and p divides ab. Suppose that p does not divide a, and we want to now see that p divides b.
Since p is prime and p does not divide a, it must be that p and a are relatively prime. So we can apply Bézout's identity: $1 = px + ay$ for some integers x and y. Multiplying both sides by b:

$$b = pxb + aby.$$

Euclid's lemma

Lemma

If p is prime and p divides ab then p divides a or p divides b.

Proof.

Suppose that p is prime and p divides ab. Suppose that p does not divide a, and we want to now see that p divides b.
Since p is prime and p does not divide a, it must be that p and a are relatively prime. So we can apply Bézout's identity: $1 = px + ay$ for some integers x and y. Multiplying both sides by b:

$$b = px + aby.$$

Since ab is a multiple of p, this shows that b is a multiple of p, as desired. □

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a^2 then p divides a.

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a^2 then p divides a.

Proof.

This is just the special case of Euclid's lemma where $a = b$. □

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a^2 then p divides a.

Proof.

This is just the special case of Euclid's lemma where $a = b$. □

Keep this version of Euclid's lemma in mind. We'll use it to prove that $\sqrt{p}$ is irrational for every prime p.

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a product of k many integers $a_1 a_2 \cdots a_k$ then p divides one of the multiplicands a_i in the product.

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a product of k many integers $a_1 a_2 \cdots a_k$ then p divides one of the multiplicands a_i in the product.

We will prove this by mathematical induction on k. We assume that this is true if you multiply together $< k$ many numbers, and show it must be true if you multiply together k many.

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a product of k many integers $a_1 a_2 \cdots a_k$ then p divides one of the multiplicands a_i in the product.

We will prove this by mathematical induction on k. We assume that this is true if you multiply together $< k$ many numbers, and show it must be true if you multiply together k many.

Proof.

The $k = 1$ case is trivial, so let's consider the $k > 1$ case. Think of the product as the product of two things: $a_1 a_2 \cdots a_k = a_1 \cdot (a_2 \cdots a_k)$.

Corollaries of Euclid's lemma

Corollary

If p is prime and p divides a product of k many integers $a_1 a_2 \cdots a_k$ then p divides one of the multiplicands a_i in the product.

We will prove this by mathematical induction on k. We assume that this is true if you multiply together $< k$ many numbers, and show it must be true if you multiply together k many.

Proof.

The $k = 1$ case is trivial, so let's consider the $k > 1$ case. Think of the product as the product of two things: $a_1 a_2 \cdots a_k = a_1 \cdot (a_2 \cdots a_k)$.
By Euclid's lemma, either p divides a_1 or p divides $a_2 \cdots a_k$. If p divides a_1 then we are done. In the other case, we have that p divides a product of $k - 1$ many multiplicands, so p must divide one of them. □

No more lemmas

With these three lemmas out of the way, we are now in a position to prove that prime factorizations are unique. We already proved prime factorizations exist, so once we prove uniqueness we have finished proving the fundamental theorem of arithmetic.

Uniqueness of prime factorizations

Let n be a positive integer, and suppose we have two prime factorizations of n:

$$n = p_1 \cdots p_k \qquad \text{and} \qquad n = q_1 \cdots q_\ell.$$

Proof these two factorizations are rearrangements of each other.

We prove this by mathematical induction. We assume that all positive integers $< n$ have a unique prime factorization, and use that to show n has a unique factorization.

Uniqueness of prime factorizations

Let n be a positive integer, and suppose we have two prime factorizations of n:

$$n = p_1 \cdots p_k \qquad \text{and} \qquad n = q_1 \cdots q_\ell.$$

Proof these two factorizations are rearrangements of each other.

We prove this by mathematical induction. We assume that all positive integers $< n$ have a unique prime factorization, and use that to show n has a unique factorization.

Because p_1 divides $n = q_1 \cdots q_\ell$, by the strong form of Euclid's lemma we get that p_1 divides q_j for some $1 \leq j \leq \ell$. Rearranging the multiplicands if necessary, we may assume that this is q_1. But since p_1 and q_1 are both prime this means that $p_1 = q_1$.

Uniqueness of prime factorizations

Let n be a positive integer, and suppose we have two prime factorizations of n:

$$n = p_1 \cdots p_k \qquad \text{and} \qquad n = q_1 \cdots q_\ell.$$

Proof these two factorizations are rearrangements of each other.

We prove this by mathematical induction. We assume that all positive integers $< n$ have a unique prime factorization, and use that to show n has a unique factorization.

Because p_1 divides $n = q_1 \cdots q_\ell$, by the strong form of Euclid's lemma we get that p_1 divides q_j for some $1 \leq j \leq \ell$. Rearranging the multiplicands if necessary, we may assume that this is q_1. But since p_1 and q_1 are both prime this means that $p_1 = q_1$. So then we have two prime factorizations for n/p_1, namely $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_\ell$.

Uniqueness of prime factorizations

Let n be a positive integer, and suppose we have two prime factorizations of n:

$$n = p_1 \cdots p_k \qquad \text{and} \qquad n = q_1 \cdots q_\ell.$$

Proof these two factorizations are rearrangements of each other.

We prove this by mathematical induction. We assume that all positive integers $< n$ have a unique prime factorization, and use that to show n has a unique factorization.

Because p_1 divides $n = q_1 \cdots q_\ell$, by the strong form of Euclid's lemma we get that p_1 divides q_j for some $1 \leq j \leq \ell$. Rearranging the multiplicands if necessary, we may assume that this is q_1. But since p_1 and q_1 are both prime this means that $p_1 = q_1$. So then we have two prime factorizations for n/p_1, namely $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_\ell$.

Since $n/p_1 < n$, these two factorizations must be rearrangements of each other. So the original factorizations are rearrangements of each other. □

Take a break

It took a while, but we proved a significant result!

How many primes are there?

Theorem

There are infinitely many primes.

How many primes are there?

Theorem

There are infinitely many primes.

Proof.

Suppose you have a finite list of primes $p_1, \ldots, p_k$. Multiply them together and add 1:

$$N = p_1 \cdots p_k + 1.$$

How many primes are there?

Theorem

There are infinitely many primes.

Proof.

Suppose you have a finite list of primes $p_1, \ldots, p_k$. Multiply them together and add 1:

$$N = p_1 \cdots p_k + 1.$$

Observe that if you divide N by any prime in your list, then the remainder is 1. So none of the primes in the prime factorization of N can show up in your list.

How many primes are there?

Theorem

There are infinitely many primes.

Proof.

Suppose you have a finite list of primes $p_1, \ldots, p_k$. Multiply them together and add 1:

$$N = p_1 \cdots p_k + 1.$$

Observe that if you divide N by any prime in your list, then the remainder is 1. So none of the primes in the prime factorization of N can show up in your list. Since this reasoning works for any finite list, there can be no finite list of all primes. That is to say, there are infinitely many primes. □

Rephrasing this proof

One sometimes sees this proof formulated as a proof by contradiction.

Rephrasing this proof

One sometimes sees this proof formulated as a proof by contradiction.

Proof.

Suppose toward a contradiction there are finitely many primes. Then we can list them out: $p_1, \ldots, p_k$. Set $N = p_1 \cdots p_k + 1$. Then no prime can divide N, so N has no prime factorization. But we know that every positive integer has a prime factorization, so this is impossible. So it must be that there are infinitely many primes. $\square$

Direct proofs versus proofs by contradiction

- Sometimes you can prove something directly, or you can prove it by contradiction.

Direct proofs versus proofs by contradiction

- Sometimes you can prove something directly, or you can prove it by contradiction.
- Usually, direct proofs are better, because they give more information.

Direct proofs versus proofs by contradiction

- Sometimes you can prove something directly, or you can prove it by contradiction.
- Usually, direct proofs are better, because they give more information.
  - To prove "if A then B", you assume A and try to show B.
  - Along the way, you prove a bunch of smaller facts about what's true if you assume A.
  - If you try to prove B by contradiction, you assume B is false and then try to derive a contradiction. But then any smaller facts you prove along the way are only 'true' in an impossible setting—because, as is the whole point, if A is true then it's impossible for B to be false.
  - So you don't get that extra info!

Direct proofs versus proofs by contradiction

- Sometimes you can prove something directly, or you can prove it by contradiction.
- Usually, direct proofs are better, because they give more information.
  - To prove "if A then B", you assume A and try to show B.
  - Along the way, you prove a bunch of smaller facts about what's true if you assume A.
  - If you try to prove B by contradiction, you assume B is false and then try to derive a contradiction. But then any smaller facts you prove along the way are only 'true' in an impossible setting—because, as is the whole point, if A is true then it's impossible for B to be false.
  - So you don't get that extra info!
- One thing it's easy to do is prove "if A then B" by something like: Assume A. Suppose toward a contradiction that B is false. [Argue that B is true, without using the assumption that B is false.] So we get a contradiction, so B is true.
- You can immediately turn any proof like this into a direct proof!

Square roots

Way back at the beginning of these slides, I promised we would get some more light on when $\sqrt{n}$ is irrational. It was a long detour—through some results which are of interest in their own right—but let's finally return to that question.

Square roots of primes

Equipped with Euclid's lemma, we can generalize the proof that $\sqrt{2}$ is irrational.

Theorem

If p is prime then $\sqrt{p}$ is irrational.

Square roots of primes

Equipped with Euclid's lemma, we can generalize the proof that $\sqrt{2}$ is irrational.

Theorem

If p is prime then $\sqrt{p}$ is irrational.

Proof.

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

Can we push this further?

- An integer n is a perfect square if $n = a^2$ for some integer a.

Can we push this further?

- An integer n is a perfect square if $n = a^2$ for some integer a.
- The square root of a perfect square is an integer, hence rational: if $n = a^2$ then $\sqrt{n} = |a|$.

This puts a limit on what square roots of natural numbers can be irrational.

Can we push this further?

- An integer n is a perfect square if $n = a^2$ for some integer a.
- The square root of a perfect square is an integer, hence rational: if $n = a^2$ then $\sqrt{n} = |a|$.

This puts a limit on what square roots of natural numbers can be irrational.

But it's the only limit!

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

- This theorem is an "A if and only if B" statement, saying that two things are equivalent.
- "A if and only if B" is the same as saying: "if A then B, and if B then A".
- So to prove an if-and-only-if statement, we need to prove two things: the forward if-then and the backward if-then.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

- This theorem is an "A if and only if B" statement, saying that two things are equivalent.
- "A if and only if B" is the same as saying: "if A then B, and if B then A".
- So to prove an if-and-only-if statement, we need to prove two things: the forward if-then and the backward if-then.
- Sometimes when proving "if A then B", it's easier to prove the contrapositive "if B is false then A is false".
- As we'll talk more when we discuss some logic, any if-then statement is logically equivalent to its contrapositive.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Leftarrow$ direction.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Leftarrow$ direction.

This is the observation from a couple slides ago: if $n = a^2$ then $\sqrt{n} = |a|$. □

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

We prove this by contrapositive. That is, we assume n is not a perfect square and we want to show $\sqrt{n}$ is irrational.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

We prove this by contrapositive. That is, we assume n is not a perfect square and we want to show $\sqrt{n}$ is irrational. Since n is not a perfect square, in particular $n > 1$. So n has a nontrivial prime factorization. Here, it's convenient to group together copies of the same prime:

$$n = p_1^{m_1} \cdots p_k^{m_k}.$$

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

We prove this by contrapositive. That is, we assume n is not a perfect square and we want to show $\sqrt{n}$ is irrational. Since n is not a perfect square, in particular $n > 1$. So n has a nontrivial prime factorization. Here, it's convenient to group together copies of the same prime:

$$n = p_1^{m_1} \cdots p_k^{m_k}.$$

Each of the exponents m_i is either even or odd. Let's look at the two cases to see what's going on.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

Even exponent: $\sqrt{p^{2k}} = p^k$ is an integer, and hence rational.

Odd exponent: $\sqrt{p^{2k+1}} = p^k\sqrt{p}$ is irrational.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

Even exponent: $\sqrt{p^{2k}} = p^k$ is an integer, and hence rational.

Odd exponent: $\sqrt{p^{2k+1}} = p^k\sqrt{p}$ is irrational.

So $\sqrt{n}$ is an integer multiplied by some square roots of different primes. There has to be at least one, because if all exponents were even then n would be a perfect square.

Square roots of natural numbers

Theorem

Consider a natural number n. Then $\sqrt{n}$ is rational if and only if n is a perfect square.

Proof of $\Rightarrow$ direction.

Even exponent: $\sqrt{p^{2k}} = p^k$ is an integer, and hence rational.

Odd exponent: $\sqrt{p^{2k+1}} = p^k\sqrt{p}$ is irrational.

So $\sqrt{n}$ is an integer multiplied by some square roots of different primes. There has to be at least one, because if all exponents were even then n would be a perfect square. Multiplying a number by a nonzero integer won't change whether it's irrational—proof: homework :)—so we've reduced the problem down to checking that the product of a bunch of square roots of different primes must be irrational. Once we have done that, we are done. □

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

For the sake of readability, I will present the case where the list has 2 primes.

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

For the sake of readability, I will present the case where the list has 2 primes.

Proof.

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

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

For the sake of readability, I will present the case where the list has 2 primes.

Proof.

Suppose toward a contradiction that $\sqrt{pq}$ is rational, where $p \neq q$ are prime. Then, we can write $\sqrt{pq} = a/b$ where a and b are relatively prime. We can rearrange this to get $a^2 = pqb^2$. That is, a^2 is a multiple of p, and so by Euclid's lemma a is a multiple of p. Similarly, a must be a multiple of q. Therefore, a must be a multiple of pq. That is, $a = pqk$ for some integer k.

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

For the sake of readability, I will present the case where the list has 2 primes.

Proof.

Suppose toward a contradiction that $\sqrt{pq}$ is rational, where $p \neq q$ are prime. Then, we can write $\sqrt{pq} = a/b$ where a and b are relatively prime. We can rearrange this to get $a^2 = pqb^2$. That is, a^2 is a multiple of p, and so by Euclid's lemma a is a multiple of p. Similarly, a must be a multiple of q. Therefore, a must be a multiple of pq. That is, $a = pqk$ for some integer k. Substituting this in and rearranging, we get $b^2 = pqk^2$. By the same reasoning as before, b is a multiple of pq.

The missing step

Lemma

The product of the square roots of a nonempty list of distinct primes is irrational.

For the sake of readability, I will present the case where the list has 2 primes.

Proof.

Suppose toward a contradiction that $\sqrt{pq}$ is rational, where $p \neq q$ are prime. Then, we can write $\sqrt{pq} = a/b$ where a and b are relatively prime. We can rearrange this to get $a^2 = pqb^2$. That is, a^2 is a multiple of p, and so by Euclid's lemma a is a multiple of p. Similarly, a must be a multiple of q. Therefore, a must be a multiple of pq. That is, $a = pqk$ for some integer k. Substituting this in and rearranging, we get $b^2 = pqk^2$. By the same reasoning as before, b is a multiple of pq. So we've seen that a and b have pq as a common factor, contradicting that they are relatively prime. So it must be that $\sqrt{pq}$ is irratinonal, as desired. □

The real last missing step

One step in this needs to be justified.

Lemma

Suppose p and q are distinct primes which both divide n. Then pq divides n. More generally, if you have a list of distinct primes which all divide n, then the product of the primes also divides n.

The real last missing step

One step in this needs to be justified.

Lemma

Suppose p and q are distinct primes which both divide n. Then pq divides n. More generally, if you have a list of distinct primes which all divide n, then the product of the primes also divides n.

Proof.

The real last missing step

One step in this needs to be justified.

Lemma

Suppose p and q are distinct primes which both divide n. Then pq divides n. More generally, if you have a list of distinct primes which all divide n, then the product of the primes also divides n.

Proof.

Homework :)