Prime numbers

Nashville Math Club

September 3, 2019

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p.

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p. An integer $n > 1$ which is not prime is said to be **composite**.

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p. An integer $n > 1$ which is not prime is said to be **composite**.

What numbers are prime?

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p.
An integer $n > 1$ which is not prime is said to be **composite**.

What numbers are prime?
2, 3, 5, 7, 11, 13, ...

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p. An integer $n > 1$ which is not prime is said to be **composite**.

What numbers are prime?
2, 3, 5, 7, 11, 13, . . .

Why do we care about prime numbers?

What are prime numbers?

A **prime number** is an integer $p > 1$ whose only divisors are 1 and p.
An integer $n > 1$ which is not prime is said to be **composite**.

What numbers are prime?
2, 3, 5, 7, 11, 13, ...

Why do we care about prime numbers?
All positive integers factor *uniquely* (up to reordering) into primes.

How many primes are there?

How many primes are there?

Infinitely many!

How many primes are there?

Infinitely many! Perhaps this seems obvious, but how do we prove it?

How many primes are there?

Infinitely many! Perhaps this seems obvious, but how do we prove it?

Proof.

Suppose there were only finitely many primes $p_1, p_2, \ldots, p_k$, and let $n = p_1 \ldots p_k + 1$.

How many primes are there?

Infinitely many! Perhaps this seems obvious, but how do we prove it?

Proof.

Suppose there were only finitely many primes $p_1, p_2, \ldots, p_k$, and let $n = p_1 \ldots p_k + 1$. Notice that every prime p_i does not divide n since it has remainder 1 when dividing n by p_i.

How many primes are there?

Infinitely many! Perhaps this seems obvious, but how do we prove it?

Proof.

Suppose there were only finitely many primes $p_1, p_2, \ldots, p_k$, and let $n = p_1 \ldots p_k + 1$. Notice that every prime p_i does not divide n since it has remainder 1 when dividing n by p_i. This contradicts the fact that every integer bigger than 1 has a prime that divides it. $\square$

Primes of certain forms

We now know that there are infinitely many primes. Sometimes, we want to know that there are infinitely many of some "form".

Primes of certain forms

We now know that there are infinitely many primes. Sometimes, we want to know that there are infinitely many of some "form". What does this mean?

Primes of certain forms

We now know that there are infinitely many primes. Sometimes, we want to know that there are infinitely many of some “form”. What does this mean?

Definition

An **even number** is a number of the form $2n$, where n is an integer. An **odd number** is a number of the form $2n + 1$, where n is an integer.

Problem: Use this definition to show that the sum of two even numbers is even, the sum of two odd numbers is even, and the sum of an even and odd number is odd.

Primes of certain forms

We now know that there are infinitely many primes. Sometimes, we want to know that there are infinitely many of some “form”. What does this mean?

Definition

An **even number** is a number of the form $2n$, where n is an integer. An **odd number** is a number of the form $2n+1$, where n is an integer.

Problem: Use this definition to show that the sum of two even numbers is even, the sum of two odd numbers is even, and the sum of an even and odd number is odd.

Problem: Use this definition to show that the product of two odd numbers is odd.

Primes of the form $4n + 3$

Question: What even numbers are prime?

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

We now want to show that there are infinitely many primes of the form $4n + 3$ using the same techniques as in the proof before.

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

We now want to show that there are infinitely many primes of the form $4n + 3$ using the same techniques as in the proof before.

Question: Why does every prime other than 2 have to be of the form $4n + 1$ or $4n + 3$?

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

We now want to show that there are infinitely many primes of the form $4n + 3$ using the same techniques as in the proof before.

Question: Why does every prime other than 2 have to be of the form $4n + 1$ or $4n + 3$?
Problem: Show that the product of two numbers of the form $4n + 1$ is again of this form.

Primes of the form $4n+3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n+1$.

We now want to show that there are infinitely many primes of the form $4n+3$ using the same techniques as in the proof before.

Question: Why does every prime other than 2 have to be of the form $4n+1$ or $4n+3$?
Problem: Show that the product of two numbers of the form $4n+1$ is again of this form.

Problem: Show that there are infinitely many primes of the form $4n+3$ using the idea of the proof for the infinitude of primes and the above problem.

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

We now want to show that there are infinitely many primes of the form $4n + 3$ using the same techniques as in the proof before.

Question: Why does every prime other than 2 have to be of the form $4n + 1$ or $4n + 3$?
Problem: Show that the product of two numbers of the form $4n + 1$ is again of this form.

Problem: Show that there are infinitely many primes of the form $4n + 3$ using the idea of the proof for the infinitude of primes and the above problem.
Question: Why doesn't this work for primes of the form $4n + 1$?

Primes of the form $4n + 3$

Question: What even numbers are prime?
This tells us that there are only finitely many primes of the form $2n$, but there are infinitely many of the form $2n + 1$.

We now want to show that there are infinitely many primes of the form $4n + 3$ using the same techniques as in the proof before.

Question: Why does every prime other than 2 have to be of the form $4n + 1$ or $4n + 3$?
Problem: Show that the product of two numbers of the form $4n + 1$ is again of this form.

Problem: Show that there are infinitely many primes of the form $4n + 3$ using the idea of the proof for the infinitude of primes and the above problem.
Question: Why doesn't this work for primes of the form $4n + 1$? Does this mean that there are only finitely many of them?

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$. *Then there are infinitely many primes of the form* $an + b$.

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$*. Then there are infinitely many primes of the form* $an + b$*.*

Question: Why do we ask that $\gcd(a, b) = 1$?

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$. *Then there are infinitely many primes of the form* $an + b$.

Question: Why do we ask that $\gcd(a, b) = 1$?

Another way to think about this: Let $f(x) = ax + b$ for a, b integers.

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$. *Then there are infinitely many primes of the form* $an + b$.

Question: Why do we ask that $\gcd(a, b) = 1$?

Another way to think about this: Let $f(x) = ax + b$ for a, b integers. If $\gcd(a, b) = 1$, then Dirichlet's Theorem says it takes on prime values infinitely often.

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$. *Then there are infinitely many primes of the form* $an + b$.

Question: Why do we ask that $\gcd(a, b) = 1$?

Another way to think about this: Let $f(x) = ax + b$ for a, b integers. If $\gcd(a, b) = 1$, then Dirichlet's Theorem says it takes on prime values infinitely often. If $\gcd(a, b) > 1$, we just noticed that it only takes on prime values finitely often.

Dirichlet's Theorem

Theorem

Suppose $\gcd(a, b) = 1$. *Then there are infinitely many primes of the form* $an + b$.

Question: Why do we ask that $\gcd(a, b) = 1$?

Another way to think about this: Let $f(x) = ax + b$ for a, b integers. If $\gcd(a, b) = 1$, then Dirichlet's Theorem says it takes on prime values infinitely often. If $\gcd(a, b) > 1$, we just noticed that it only takes on prime values finitely often.

We understand linear functions taking on prime values. What about other functions?

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$.

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Answer: $f(41) = 41^2 - 41 + 41$ is divisible by 41 and is not prime.

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Answer: $f(41) = 41^2 - 41 + 41$ is divisible by 41 and is not prime.
Question: Even if it doesn't taken on prime values for *all* n, does it take on prime values for infinitely many?

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Answer: $f(41) = 41^2 - 41 + 41$ is divisible by 41 and is not prime.
Question: Even if it doesn't taken on prime values for *all* n, does it take on prime values for infinitely many?
Answer: We don't know!

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Answer: $f(41) = 41^2 - 41 + 41$ is divisible by 41 and is not prime.
Question: Even if it doesn't taken on prime values for *all* n, does it take on prime values for infinitely many?
Answer: We don't know!

Question: What about an easier quadratic like $f(n) = n^2 + 1$?

Problem: Let $f(n) = n^2 - n + 41$. Write down the value of f for $n = 0, 1, 2, 3, 4, 5, 6, 7$. What do you notice about these values?
Question: Is $f(n)$ prime for all values of n?

Answer: $f(41) = 41^2 - 41 + 41$ is divisible by 41 and is not prime.
Question: Even if it doesn't taken on prime values for *all* n, does it take on prime values for infinitely many?
Answer: We don't know!

Question: What about an easier quadratic like $f(n) = n^2 + 1$?
Answer: We still don't know!

Ulam's spiral

Problem: Write down the numbers starting from 1 in a spiral and circle the prime numbers.

Ulam's spiral

Problem: Write down the numbers starting from 1 in a spiral and circle the prime numbers. Do you notice any patterns?

Ulam's spiral

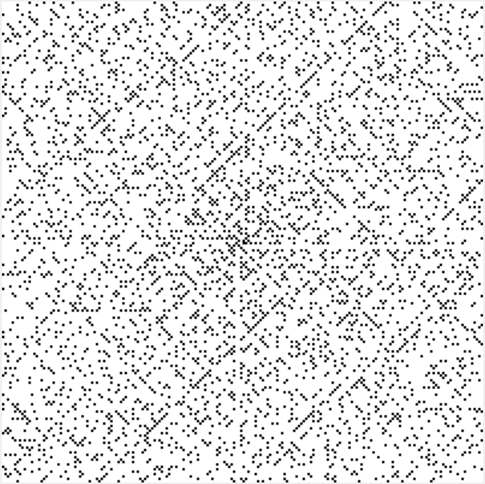

Figure: By Grontesca at the English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1924394

Random squares

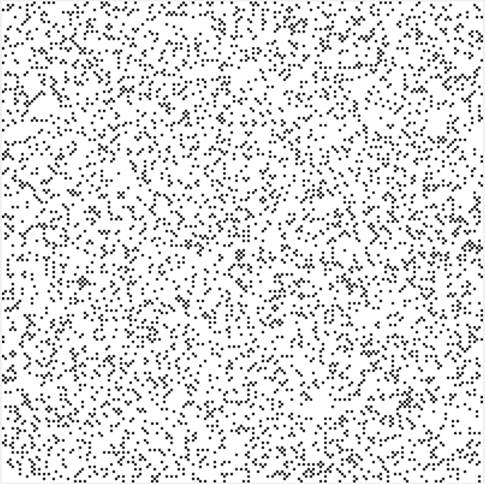

Figure: By Thanassis Tsiodras - https://github.com/ttsiodras/PrimeSpirals, GPL, https://commons.wikimedia.org/w/index.php?curid=65680576

Altered Ulam's spiral

Insert Ulam's spiral starting at 41

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

The Sieve of Eratosthenes gives all prime numbers up to a certain number.

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

The Sieve of Eratosthenes gives all prime numbers up to a certain number. Shouldn't this be sufficient for finding prime numbers?

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

The Sieve of Eratosthenes gives all prime numbers up to a certain number. Shouldn't this be sufficient for finding prime numbers?

- Can take too long

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

The Sieve of Eratosthenes gives all prime numbers up to a certain number. Shouldn't this be sufficient for finding prime numbers?

- Can take too long
- Doesn't tell us about the "nature" of primes

Sieve of Eratosthenes

We know certain kinds of numbers are infinitely often prime. How can we find *all* primes though?

The Sieve of Eratosthenes gives all prime numbers up to a certain number. Shouldn't this be sufficient for finding prime numbers?

- Can take too long
- Doesn't tell us about the "nature" of primes
- Is inherently a finite method

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.
Problem: What are the first 15 prime gaps?

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.

Problem: What are the first 15 prime gaps?

Answer: The first 16 primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$$

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.
Problem: What are the first 15 prime gaps?
Answer: The first 16 primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$$

The first 15 prime gaps:

$$1, 2, 2, 4, 2, 6, 2, 4, 6, 2, 6, 4, 2, 4, 6$$

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.
Problem: What are the first 15 prime gaps?
Answer: The first 16 primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$$

The first 15 prime gaps:

$$1, 2, 2, 4, 2, 6, 2, 4, 6, 2, 6, 4, 2, 4, 6$$

Problem: Come up with a reason for why all the prime gaps after the first one appear to be even.

Prime gaps

List out the primes as $p_1, p_2, \ldots, p_n, \ldots$ in ascending order. The n^{th} **prime gap** is $p_{n+1} - p_n$.
Problem: What are the first 15 prime gaps?
Answer: The first 16 primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$$

The first 15 prime gaps:

$$1, 2, 2, 4, 2, 6, 2, 4, 6, 2, 6, 4, 2, 4, 6$$

Problem: Come up with a reason for why all the prime gaps after the first one appear to be even.
Question: What kind of prime gaps can occur in general?

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded.

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Proof.

Consider the set of numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Proof.

Consider the set of numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

We claim that all of these numbers are composite.

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Proof.

Consider the set of numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

We claim that all of these numbers are composite.For $2 \leq k \leq n+1$, k divides both $(n+1)!$ and itself, so it divides $(n+1)!+k$.

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Proof.

Consider the set of numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

We claim that all of these numbers are composite.For $2 \leq k \leq n+1$, k divides both $(n+1)!$ and itself, so it divides $(n+1)!+k$. Since this number is bigger than k, it must be composite.

Arbitrarily long prime gaps

We want to show that the collection of prime gaps is not bounded. In other words, given a number n, we want to show that there is a prime gap of size at least n.

Proof.

Consider the set of numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

We claim that all of these numbers are composite.For $2 \leq k \leq n+1$, k divides both $(n+1)!$ and itself, so it divides $(n+1)!+k$. Since this number is bigger than k, it must be composite.
Why does this finish the proof? □

Twin Primes Conjecture

We now have talked about long gaps between numbers.

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin primes are a pair of primes of the form p and $p+2$.

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin primes are a pair of primes of the form p and $p+2$.

Problem: Use the prime gaps we wrote down before to find 6 pairs of twin primes.

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin primes are a pair of primes of the form p and $p+2$.

Problem: Use the prime gaps we wrote down before to find 6 pairs of twin primes.
Question: How many pairs are there?

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin primes are a pair of primes of the form p and $p+2$.

Problem: Use the prime gaps we wrote down before to find 6 pairs of twin primes.
Question: How many pairs are there?

Conjecture

There are infinitely many pairs of twin primes.

Twin Primes Conjecture

We now have talked about long gaps between numbers. What about short ones?

Twin primes are a pair of primes of the form p and $p + 2$.

Problem: Use the prime gaps we wrote down before to find 6 pairs of twin primes.
Question: How many pairs are there?

Conjecture

There are infinitely many pairs of twin primes.

Question: Can you find examples of primes p such that $p + 2$ and $p + 4$ are both also prime? How many?

Advanced ideas about primes

It turns out that you can ask about the "average" prime gap.

Advanced ideas about primes

It turns out that you can ask about the "average" prime gap. In other words, we have the n^{th} prime p_n, we can ask how far away the next prime p_{n+1} should "typically" be.

Advanced ideas about primes

It turns out that you can ask about the "average" prime gap. In other words, we have the n^{th} prime p_n, we can ask how far away the next prime p_{n+1} should "typically" be.

Theorem

The "average" prime gap for p_n is $\log p_n$.