Hilbert's 8^{th} Problem

Brandon Alberts

University of Connecticut Math Club

October 16, 2019

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

- primes: 2, 3, 5, 7, 11, 13, 17,...

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

- primes: 2, 3, 5, 7, 11, 13, 17,...
- composites: 4, 6, 8, 9,...

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

- primes: 2, 3, 5, 7, 11, 13, 17,...
- composites: 4, 6, 8, 9,...

Theorem (Fundamental Theorem of Arithmetic (Euclid 300BC))

Every integer > 1 can be written as a product of prime numbers in exactly one way (up to reordering).

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

- primes: 2, 3, 5, 7, 11, 13, 17,...
- composites: 4, 6, 8, 9,...

Theorem (Fundamental Theorem of Arithmetic (Euclid 300BC))

Every integer > 1 can be written as a product of prime numbers in exactly one way (up to reordering).

- $4 = 2 \cdot 2$, $6 = 2 \cdot 3$,...

Prime Numbers

Definition

An integer > 1 is called a **prime number** if its only divisors are 1 and itself.

- primes: 2, 3, 5, 7, 11, 13, 17,...
- composites: 4, 6, 8, 9,...

Theorem (Fundamental Theorem of Arithmetic (Euclid 300BC))

Every integer > 1 can be written as a product of prime numbers in exactly one way (up to reordering).

- $4 = 2 \cdot 2$, $6 = 2 \cdot 3$,... $236 = 2 \cdot 2 \cdot 59$,...

What about 1?

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time.

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

In modern days, it generally accepted that 1 is not a prime.

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

In modern days, it generally accepted that 1 is not a prime.

- $12 = 2 \cdot 2 \cdot 3$

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

In modern days, it generally accepted that 1 is not a prime.

- $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 1$

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

In modern days, it generally accepted that 1 is not a prime.

- $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 1 = 2 \cdot 2 \cdot 3 \cdot 1 \cdot 1 = \cdots$

What about 1?

There is some real history about whether mathematicians have considered 1 to be a prime number, and the answer has changed over time. (In fact, there have been times where 1 was not even considered a number, let alone a prime.)

In modern days, it generally accepted that 1 is not a prime.

- $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 1 = 2 \cdot 2 \cdot 3 \cdot 1 \cdot 1 = \cdots$

1 has some very different properties compared to other positive integers, and is sometimes called a **unit**.

How many prime numbers are there?

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

Suppose $p_1, p_2, \ldots, p_n$ are the first n prime numbers.

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

Suppose $p_1, p_2, ..., p_n$ are the first n prime numbers.

Let $N = p_1 p_2 \cdots p_n + 1$. $N > 1$, so it can be written as a nonempty product of prime numbers.

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

Suppose $p_1, p_2, ..., p_n$ are the first n prime numbers.

Let $N = p_1 p_2 \cdots p_n + 1$. $N > 1$, so it can be written as a nonempty product of prime numbers. In particular, there exists at least one prime number ℓ dividing N.

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

Suppose $p_1, p_2, ..., p_n$ are the first n prime numbers.

Let $N = p_1 p_2 \cdots p_n + 1$. $N > 1$, so it can be written as a nonempty product of prime numbers. In particular, there exists at least one prime number ℓ dividing N.

None of $p_1, p_2, ..., p_n$ divide N.

How many prime numbers are there?

Theorem (Euclid, 300BC)

There are infinitely many prime numbers.

Suppose $p_1, p_2, \ldots, p_n$ are the first n prime numbers.

Let $N = p_1 p_2 \cdots p_n + 1$. $N > 1$, so it can be written as a nonempty product of prime numbers. In particular, there exists at least one prime number ℓ dividing N.

None of $p_1, p_2, \ldots, p_n$ divide N. Thus $\ell \neq p_1, p_2, \ldots, p_n$, so ℓ must be a new prime number not on our original list. $\square$

How do we find prime numbers?

Sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

How do we find prime numbers?

Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

How do we find prime numbers?

Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

How do we find prime numbers?

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Primes in Arithmetic Progressions

Theorem (Dirichlet, 1837)

Given integers a and d with share no common divisors larger than 1, the arithmetic progression

$$a, a+d, a+2d, a+3d, a+4d, a+5d, \ldots$$

has infinitely many prime numbers.

Primes in Arithmetic Progressions

Theorem (Dirichlet, 1837)

Given integers a and d with share no common divisors larger than 1, the arithmetic progression

$$a, a+d, a+2d, a+3d, a+4d, a+5d, \ldots$$

has infinitely many prime numbers.

- The numbers 3 and 10 share no common divisors larger than 1: 3, 13, 23, 33, 43, 53, 63, 73, 83, 93, 103,...

Primes in Arithmetic Progressions

Theorem (Dirichlet, 1837)

Given integers a and d with share no common divisors larger than 1, the arithmetic progression

$$a, a+d, a+2d, a+3d, a+4d, a+5d, \ldots$$

has infinitely many prime numbers.

- The numbers 3 and 10 share no common divisors larger than 1: 3, 13, 23, 33, 43, 53, 63, 73, 83, 93, 103,...
- The numbers 1 and 4 share no common divisors larger than 1: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41,...

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

- $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$, $(41, 43)$, $(71, 73)$,...

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

- $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(71,73)$,...

We can ask a similar question about other **constellations**, such as triples $(p, p+2, p+6)$ such that p, $p+2$, and $p+6$ are all prime.

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

- $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(71,73)$,...

We can ask a similar question about other **constellations**, such as triples $(p, p+2, p+6)$ such that p, $p+2$, and $p+6$ are all prime.

Trivial cases: $(p+a_0, p+a_1, ..., p+a_k)$ such that there exists an integer n for which the remainders of $a_0, a_1, ..., a_k$ divided by n cover all the integers $0, 1, 2, ..., n-1$ (i.e., $\{a_0, a_1, ..., a_k \mod n\} = \mathbb{Z}/n\mathbb{Z}$).

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

- $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(71,73)$,...

We can ask a similar question about other **constellations**, such as triples $(p, p+2, p+6)$ such that p, $p+2$, and $p+6$ are all prime.

Trivial cases: $(p+a_0, p+a_1, ..., p+a_k)$ such that there exists an integer n for which the remainders of $a_0, a_1, ..., a_k$ divided by n cover all the integers $0, 1, 2, ..., n-1$ (i.e., $\{a_0, a_1, ..., a_k \mod n\} = \mathbb{Z}/n\mathbb{Z}$).

- $(p, p+2, p+4)$, at least one of p, $p+2$, or $p+4$ is divisible by 3, and so is not prime if $p > 3$.

Twin Prime Conjecture

Conjecture (Twin Prime Conjecture)

The are infinitely many pairs of positive integers $(p, p+2)$ for which p and $p+2$ are both prime.

- $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(71,73)$,...

We can ask a similar question about other **constellations**, such as triples $(p, p+2, p+6)$ such that p, $p+2$, and $p+6$ are all prime.

Trivial cases: $(p+a_0, p+a_1, ..., p+a_k)$ such that there exists an integer n for which the remainders of $a_0, a_1, ..., a_k$ divided by n cover all the integers $0, 1, 2, ..., n-1$ (i.e., $\{a_0, a_1, ..., a_k \mod n\} = \mathbb{Z}/n\mathbb{Z}$).

- $(p, p+2, p+4)$, at least one of p, $p+2$, or $p+4$ is divisible by 3, and so is not prime if $p > 3$.

Nontrivial cases: there is not single case which is proven!

Infinite series

Infinite series

Theorem (Euler, 1737)

$$\sum_{p \text{ prime}} \frac{1}{p} = \infty$$

Infinite series

Theorem (Euler, 1737)

$$\sum_{p \text{ prime}} \frac{1}{p} = \infty$$

Proving this result is an alternative way to show that there are infinitely many primes.

Infinite series

Theorem (Euler, 1737)

$$\sum_{p \text{ } prime} \frac{1}{p} = \infty$$

Proving this result is an alternative way to show that there are infinitely many primes.

Can we show that

$$\sum_{\substack{(p,p+2) \\ p,p+2 \text{ prime}}} \frac{1}{p} + \frac{1}{p+2} = \infty$$

as a way to prove the twin prime conjecture?

Infinite series

Theorem (Euler, 1737)

$$\sum_{p \text{ prime}} \frac{1}{p} = \infty$$

Proving this result is an alternative way to show that there are infinitely many primes.

Theorem (Brun, 1919)

$$\sum_{\substack{(p,p+2) \\ p,p+2 \text{ prime}}} \frac{1}{p} + \frac{1}{p+2} < \infty$$

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At worst:

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At worst:

- The gap between p_n and p_{n+1} can be arbitrarily large.

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?

At worst:

- The gap between p_n and p_{n+1} can be arbitrarily large.
- Bertrand's Postulate (Chebyshev, 1894): there is always a prime between N and $2N$. This implies $p_n < p_{n+1} < 2p_n$.

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At worst:

- The gap between p_n and p_{n+1} can be arbitrarily large.
- Bertrand's Postulate (Chebyshev, 1894): there is always a prime between N and $2N$. This implies $p_n < p_{n+1} < 2p_n$.

  This bound can be improved so that $p_{n+1} < p_n^\theta$ for some $\theta < 1$. The best known bound is given by $\theta = 0.525$ (Baker, Harmon, Pintz 2001).

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At worst:

- The gap between p_n and p_{n+1} can be arbitrarily large.
- Bertrand's Postulate (Chebyshev, 1894): there is always a prime between N and $2N$. This implies $p_n < p_{n+1} < 2p_n$.

  This bound can be improved so that $p_{n+1} < p_n^\theta$ for some $\theta < 1$. The best known bound is given by $\theta = 0.525$ (Baker, Harmon, Pintz 2001).
- The gap between p_n and p_{n+1} can be arbitrarily larger than $\log(p_n)$ (Westzynthius, 1931).

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At worst:

- The gap between p_n and p_{n+1} can be arbitrarily large.
- Bertrand's Postulate (Chebyshev, 1894): there is always a prime between N and $2N$. This implies $p_n < p_{n+1} < 2p_n$.

  This bound can be improved so that $p_{n+1} < p_n^\theta$ for some $\theta < 1$. The best known bound is given by $\theta = 0.525$ (Baker, Harmon, Pintz 2001).
- The gap between p_n and p_{n+1} can be arbitrarily larger than $\log(p_n)$ (Westzynthius, 1931).

  In particular, $\dfrac{p_{n+1} - p_n}{\log(p_n)}$ is an unbounded sequence.

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At best:

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?

At best:

- The Twin Prime Conjecture predicts that the gap $p_{n+1} - p_n$ is equal to 2 infinitely many times.

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At best:

- The Twin Prime Conjecture predicts that the gap $p_{n+1} - p_n$ is equal to 2 infinitely many times.
- (Zhang, 2013) The gap $p_{n+1} - p_n$ is smaller than 70 million infinitely many times

What do we know?

How far do we have to go from one prime p_n to the next prime p_{n+1}?
At best:

- The Twin Prime Conjecture predicts that the gap $p_{n+1} - p_n$ is equal to 2 infinitely many times.
- (Zhang, 2013) The gap $p_{n+1} - p_n$ is smaller than 70 million infinitely many times
- A polymath project has improved this number to 246, refining Zhang's approach.

How common are prime numbers on average?

How common are prime numbers on average?

Answer: Not very

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%.

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%. Less than 17% of numbers less than 1000 are prime.

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%. Less than 17% of numbers less than 1000 are prime. In fact, we know that:

$$\lim_{x\to\infty} \frac{\text{number of primes below } x}{x} = 0\,.$$

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%. Less than 17% of numbers less than 1000 are prime. In fact, we know that:

$$\lim_{x\to\infty} \frac{\text{number of primes below } x}{x} = 0\,.$$

The **Prime Number Theorem** is a way to quantify how quickly this proportion tends to zero.

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%. Less than 17% of numbers less than 1000 are prime. In fact, we know that:

$$\lim_{x\to\infty} \frac{\text{number of primes below } x}{x} = 0\,.$$

The **Prime Number Theorem** is a way to quantify how quickly this proportion tends to zero.

$$\pi(x) = \text{number of primes below } x$$

How common are prime numbers on average?

Answer: Not very

We found 25 primes below 100 using the sieve of Eratosthenes, which is about 25%. Less than 17% of numbers less than 1000 are prime. In fact, we know that:

$$\lim_{x\to\infty} \frac{\text{number of primes below } x}{x} = 0\,.$$

The **Prime Number Theorem** is a way to quantify how quickly this proportion tends to zero.

$$\pi(x) = \text{number of primes below } x$$

(Go to wolframcloud.com)

Prime Number Theorem

Theorem (Prime Number Theorem (Poussin, Hadamard 1896))

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Prime Number Theorem

Theorem (Prime Number Theorem (Poussin, Hadamard 1896))

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Also written:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

Prime Number Theorem

Theorem (Prime Number Theorem (Poussin, Hadamard 1896))

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Also written:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

This says that the percentage of primes below x is about $1/\ln(x)$.

Prime Number Theorem

Theorem (Prime Number Theorem (Poussin, Hadamard 1896))

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Also written:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

This says that the percentage of primes below x is about $1/\ln(x)$.

We can interpret this “heuristically” to say that the probability that n is prime is $1/\ln(n)$.

Heuristic argument for the twin prime conjecture

Heuristic argument for the twin prime conjecture

- The probability that n is prime is heuristically $1/\ln(n)$.

Heuristic argument for the twin prime conjecture

- The probability that n is prime is heuristically $1/\ln(n)$.
- The probability of both n and $n+2$ being prime is heuristically

$$\frac{1}{\ln(n)\ln(n+2)}.$$

Heuristic argument for the twin prime conjecture

- The probability that n is prime is heuristically $1/\ln(n)$.
- The probability of both n and $n+2$ being prime is heuristically

$$\frac{1}{\ln(n)\ln(n+2)}.$$

- The expected number of pairs $(n, n+2)$ for which both n and $n+2$ are prime is

$$\sum_{n=2}^{\infty}\frac{1}{\ln(n)\ln(n+2)}.$$

Heuristic argument for the twin prime conjecture

- The probability that n is prime is heuristically $1/\ln(n)$.
- The probability of both n and $n+2$ being prime is heuristically

$$\frac{1}{\ln(n)\ln(n+2)}.$$

- The expected number of pairs $(n, n+2)$ for which both n and $n+2$ are prime is

$$\sum_{n=2}^{\infty} \frac{1}{\ln(n)\ln(n+2)}.$$

- This is a divergent sum by comparison with $1/n$.

A "better" Prime Number Theorem

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

Theorem (Prime Number Theorem)

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

Theorem (Prime Number Theorem)

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

Also written:

$$\pi(x) \sim \mathrm{Li}(x)\,.$$

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

Theorem (Prime Number Theorem)

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

Also written:

$$\pi(x) \sim \mathrm{Li}(x)\,.$$

What makes this better?

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

Theorem (Prime Number Theorem)

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

Also written:

$$\pi(x) \sim \mathrm{Li}(x)\,.$$

What makes this better?

$$|\pi(x) - \mathrm{Li}(x)| \text{ is ``small''}$$

A "better" Prime Number Theorem

Define the logarithmic integral function by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\, dt\,.$$

Theorem (Prime Number Theorem)

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

Also written:

$$\pi(x) \sim \mathrm{Li}(x)\,.$$

What makes this better?

$$|\pi(x) - \mathrm{Li}(x)| \text{ is “small”}$$

(Go back to wolframcloud.com)

The Riemann Hypothesis?

The Riemann Hypothesis?

Conjecture (Riemann Hypothesis)

All the nontrivial zeroes of the Riemann zeta function have real part $1/2$.

The Riemann Hypothesis?

Conjecture (Riemann Hypothesis)

All the nontrivial zeroes of the Riemann zeta function have real part $1/2$.

For $s = \sigma + it$ a complex number with $\sigma > 1$ the Riemann zeta function is defined by the convergent series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The Riemann Hypothesis?

Conjecture (Riemann Hypothesis)

All the nontrivial zeroes of the Riemann zeta function have real part $1/2$.

For $s = \sigma + it$ a complex number with $\sigma > 1$ the Riemann zeta function is defined by the convergent series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

- What is $\zeta(s)$ at other complex numbers?

The Riemann Hypothesis?

Conjecture (Riemann Hypothesis)

All the nontrivial zeroes of the Riemann zeta function have real part $1/2$.

For $s = \sigma + it$ a complex number with $\sigma > 1$ the Riemann zeta function is defined by the convergent series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} .$$

- What is $\zeta(s)$ at other complex numbers?
- What does this have to do with the prime numbers?

Relation to the primes

Relation to the primes

- $\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$

Relation to the primes

- $\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$
- Apply Taylor series to the logarithm and rearrange to get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \zeta(s) - \sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$$

Relation to the primes

- $\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$
- Apply Taylor series to the logarithm and rearrange to get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \zeta(s) - \sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$$

- The series $\sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$ is convergent for $\mathrm{Re}(s) > 1/2$.

Relation to the primes

- $\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$
- Apply Taylor series to the logarithm and rearrange to get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \zeta(s) - \sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$$

- The series $\sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$ is convergent for $\mathrm{Re}(s) > 1/2$.
- The function $\log \zeta(s)$ has singularities at
  - $s = 1$, because $\zeta(s)$ has a singularity at $s = 1$,

Relation to the primes

- $\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$
- Apply Taylor series to the logarithm and rearrange to get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \zeta(s) - \sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$$

- The series $\sum_{k=2}^{\infty} \sum_{p \text{ prime}} \frac{1}{kp^{ks}}$ is convergent for $\mathrm{Re}(s) > 1/2$.
- The function $\log \zeta(s)$ has singularities at
  - $s = 1$, because $\zeta(s)$ has a singularity at $s = 1$,
  - $s = \rho$ a zero of $\zeta(s)$, because $\log(z)$ has a singularity at $z = 0$.

Generating functions

arithmetic	complex analysis

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	the first singularity of $P(s)$ at $s = 1$

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	the first singularity of $P(s)$ at $s = 1$
closest to power x^ρ	the other singularities for $s = \rho$ a zero of the $\zeta(s)$

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	the first singularity of $P(s)$ at $s = 1$
closest to power x^ρ	the other singularities for $s = \rho$ a zero of the $\zeta(s)$

Theorem

Let a be the largest real part of a zero of $\zeta(s)$. Then for every $\epsilon > 0$ there exists a constant C such that

$$|\pi(x) - \mathrm{Li}(x)| \leqslant C \cdot x^{a+\epsilon}$$

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	the first singularity of $P(s)$ at $s = 1$
closest to power x^ρ	the other singularities for $s = \rho$ a zero of the $\zeta(s)$

Theorem

Let a be the largest real part of a zero of $\zeta(s)$. Then for every $\epsilon > 0$ there exists a constant C such that

$$|\pi(x) - \mathrm{Li}(x)| \leqslant C \cdot x^{a+\epsilon}$$

The Riemann Hypothesis says that $a = 1/2$.

Generating functions

arithmetic	complex analysis
prime numbers	$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}$
bounds on the growth of $\pi(x)$	places where $P(s)$ converges
$\mathrm{Li}(x)$ (closest to power x^1)	the first singularity of $P(s)$ at $s = 1$
closest to power x^ρ	the other singularities for $s = \rho$ a zero of the $\zeta(s)$

Theorem

Let a be the largest real part of a zero of $\zeta(s)$. Then for every $\epsilon > 0$ there exists a constant C such that

$$|\pi(x) - \mathrm{Li}(x)| \leqslant C \cdot x^{a+\epsilon}$$

The Riemann Hypothesis says that $a = 1/2$.
(Go back to wolframcloud.com?)

Goldbach's Conjecture

Goldbach's Conjecture

Conjecture (Goldbach)

- *Every integer* > 5 *can be written as the sum of three primes.*

Goldbach's Conjecture

Conjecture (Goldbach)

- *Every integer > 5 can be written as the sum of three primes.*
- *Every even integer > 2 can be written as the sum of two primes.*

Goldbach's Conjecture

Conjecture (Goldbach)

- *Every integer* > 5 *can be written as the sum of three primes.*
- *Every even integer* > 2 *can be written as the sum of two primes.*

It turns out the two bullet points above are equivalent.

Goldbach's Conjecture

Conjecture (Goldbach)

- *Every integer* > 5 *can be written as the sum of three primes.*
- *Every even integer* > 2 *can be written as the sum of two primes.*

It turns out the two bullet points above are equivalent.

Conjecture (weak Goldbach)

Every odd integer > 5 *can be written as the sum of three primes.*

What do we know?

What do we know?

- "Almost all" even integers satisfy the Goldbach conjecture. (Estermann 1938)

What do we know?

- "Almost all" even integers satisfy the Goldbach conjecture. (Estermann 1938)

$$\lim_{x\to\infty} \frac{\text{number of even } n \leqslant x \text{ satisfying Goldbach}}{\text{number of even } n \leqslant x} = 1\,.$$

What do we know?

- "Almost all" even integers satisfy the Goldbach conjecture. (Estermann 1938)

$$\lim_{x\to\infty} \frac{\text{number of even } n \leqslant x \text{ satisfying Goldbach}}{\text{number of even } n \leqslant x} = 1\,.$$

- The weak Goldbach conjecture is true (Helfgott, 2013)

Thanks for coming!!