Calculus and Prime Numbers

Shahriar Shahriari

Department of Mathematics
Pomona College
Claremont, CA 91711

December 8, 2010

The sequence of primes

The sequence of primes

$$2, 3, 5,$$

The sequence of primes

$$2, 3, 5, 7, 11, 13, 17, 19,$$

The sequence of primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23,$$

The sequence of primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,$$

The sequence of primes

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

The sequence of primes

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

The sequence of primes

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

is mysterious, haphazard, and important.

The sequence of primes

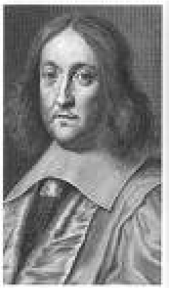
$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

is mysterious, haphazard, and important.

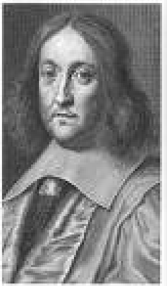
What can we say about them, and do techniques from calculus help at all?

Question

Are there any nice formulas for finding primes?



Fermat (1601–1661)



Fermat (1601–1661)

Definition (Fermat Numbers)

$$F_n = 2^{(2^n)} + 1 \quad \text{for} \quad n = 0, 1, \ldots$$

Example

The first few Fermat numbers $(2^{(2^n)} + 1)$ are:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

$$F_5 = 4294967297, \quad F_6 = 18446744073709551617.$$

Example

The first few Fermat numbers $(2^{(2^n)} + 1)$ are:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

$$F_5 = 4294967297, \quad F_6 = 18446744073709551617.$$

Conjecture (Fermat)

Fermat: F_0, F_1, F_2, F_3, and F_4 are all prime numbers and so F_n should always be prime.

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Example (Euler)

In 1732, Leonhard Euler (1707–1783) showed that

$$641 \quad \text{divides} \quad F_5 = 4{,}294{,}967{,}297.$$

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Example (Euler)

In 1732, Leonhard Euler (1707–1783) showed that

$$641 \quad \text{divides} \quad F_5 = 4{,}294{,}967{,}297.$$

Question

- *Are there any other Fermat numbers that are prime?*

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Example (Euler)

In 1732, Leonhard Euler (1707–1783) showed that

$$641 \quad \text{divides} \quad F_5 = 4{,}294{,}967{,}297.$$

Question

- *Are there any other Fermat numbers that are prime?*
- *Is the number of Fermat primes finite?*

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Example (Euler)

In 1732, Leonhard Euler (1707–1783) showed that

$$641 \quad \text{divides} \quad F_5 = 4{,}294{,}967{,}297.$$

Question

- *Are there any other Fermat numbers that are prime?*
- *Is the number of Fermat primes finite?*
- *Is F_{33} prime or composite?*

Unfortunately, for Fermat, *no* other Fermat numbers have been found to be primes.

Example (Euler)

In 1732, Leonhard Euler (1707–1783) showed that

$$641 \quad \text{divides} \quad F_5 = 4{,}294{,}967{,}297.$$

Question

- *Are there any other Fermat numbers that are prime?*
- *Is the number of Fermat primes finite?*
- *Is F_{33} prime or composite?*

All are open problems.

Latest results

On March 27, 2010, Michael Vang of USA discovered the sixth known factor of the F_{12}:

Latest results

On March 27, 2010, Michael Vang of USA discovered the sixth known factor of the F_{12}:

$$17353230210429594579133099699123162989482444520899 \times 2^{15} + 1.$$

The previously known factors of F_{12} had been discovered in 1877, 1903, 1903, 1974 and 1986, respectively.

Latest results

On March 27, 2010, Michael Vang of USA discovered the sixth known factor of the F_{12}:

$$17353230210429594579133099699123162989482444520899 \times 2^{15} + 1.$$

The previously known factors of F_{12} had been discovered in 1877, 1903, 1903, 1974 and 1986, respectively.

On November 20, 2010 Alexey V. Komkov found the following new factor of the Fermat number F_{299}:

$$272392805475 \times 2^{304} + 1.$$

Definition (Mersenne Numbers)

Father Marin Mersenne (1588–1648) suggested that the numbers

$$M_p = 2^p - 1 \quad \text{where} \quad p \quad \text{is a prime,}$$

called *Mersenne numbers*, may generate many primes.

Definition (Mersenne Numbers)

Father Marin Mersenne (1588–1648) suggested that the numbers

$$M_p = 2^p - 1 \quad \text{where} \quad p \quad \text{is a prime,}$$

called *Mersenne numbers*, may generate many primes.

Through December 2010, 47 Mersenne primes have been found

Definition (Mersenne Numbers)

Father Marin Mersenne (1588–1648) suggested that the numbers

$$M_p = 2^p - 1 \quad \text{where} \quad p \quad \text{is a prime,}$$

called *Mersenne numbers*, may generate many primes.

Through December 2010, 47 Mersenne primes have been found. M_p is a prime for the following values of p:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609.

As of December 2010, the largest prime known

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits,

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits, found on August 23, 2008 by the computers of the UCLA's Math Dept as part of the Great Internet Mersenne Prime Search (GIMPS).

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits, found on August 23, 2008 by the computers of the UCLA's Math Dept as part of the Great Internet Mersenne Prime Search (GIMPS). Awarded a $100,000 prize for being the first prime with more than 10 million digits.

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits, found on August 23, 2008 by the computers of the UCLA's Math Dept as part of the Great Internet Mersenne Prime Search (GIMPS). Awarded a $100,000 prize for being the first prime with more than 10 million digits.

On April 12th, 2009

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits, found on August 23, 2008 by the computers of the UCLA's Math Dept as part of the Great Internet Mersenne Prime Search (GIMPS). Awarded a $100,000 prize for being the first prime with more than 10 million digits.
On April 12th, 2009, the 47th known Mersenne prime, $M_{42,643,801} = 2^{42,643,801} - 1$, a 12,837,064 digit number was found by Odd Magnar Strindmo from Melhus, Norway! Second largest known prime, 141,125 digits smaller than the largest prime.

As of December 2010, the largest prime known was the Mersenne prime

$$M_{43,112,609} = 2^{43112609} - 1.$$

This gigantic prime has 12,978,189 digits, found on August 23, 2008 by the computers of the UCLA's Math Dept as part of the Great Internet Mersenne Prime Search (GIMPS). Awarded a $100,000 prize for being the first prime with more than 10 million digits.

On April 12th, 2009, the 47th known Mersenne prime, $M_{42,643,801} = 2^{42,643,801} - 1$, a 12,837,064 digit number was found by Odd Magnar Strindmo from Melhus, Norway! Second largest known prime, 141,125 digits smaller than the largest prime.

See http://www.mersenne.org/ to join the hunt and to see the latest records.

Why do Mersenne primes hold the record for the largest primes?

Why do Mersenne primes hold the record for the largest primes? The reason is the following Theorem that gives a criterion for Mersenne primes:

Why do Mersenne primes hold the record for the largest primes? The reason is the following Theorem that gives a criterion for Mersenne primes:

Theorem (Lucas-Lehmer Test)

p a prime greater than two. Construct the sequence:

$$4, 14, 194, 37634, 1416317954, 2005956546822746114, \ldots$$

where the first term is $r_1 = 4$ *and* $r_n = r_{n-1}^2 - 2$.

Why do Mersenne primes hold the record for the largest primes? The reason is the following Theorem that gives a criterion for Mersenne primes:

Theorem (Lucas-Lehmer Test)

p a prime greater than two. Construct the sequence:

$$4, 14, 194, 37634, 1416317954, 2005956546822746114, \ldots$$

where the first term is $r_1 = 4$ *and* $r_n = r_{n-1}^2 - 2$.
Now $M_p = 2^p - 1$ *is a prime if and only if* M_p *is a divisor of* r_{p-1}, *the* $(p-1)$*st term of the above sequence.*

$$
\begin{aligned}
&F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = \\
&\quad [k+2][1-(wz+h+j-q)^2-(2n+p+q+z-e)^2 \\
&\quad -(y^2(a^2-1)+1-x^2)^2-((e^4+2e^3)(a+1)^2+1-o^2)^2 \\
&\quad -(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2 \\
&\quad -\left(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2\right)^2 \\
&\quad -(ai+k+1-l-i)^2-(16r^2y^4(a^2-1)+1-u^2)^2 \\
&\quad -((g(k+2)+k+1)(h+j)+h-z)^2 \\
&\quad -(p-m+l(a-n-1)+b(2a(n+1)-n(n+2)-2))^2 \\
&\quad -(z-pm+pl(a-p)+t(2ap-p^2-1))^2 \\
&\quad -(q-x+y(a-p-1)+s(2a(p+1)-p(p+2)-2))^2 \\
&\quad -(l^2(a^2-1)+1-m^2)^2-(n+l+v-y)^2].
\end{aligned}
$$

$$
\begin{aligned}
F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = \\
& [k+2][1-(wz+h+j-q)^2-(2n+p+q+z-e)^2 \\
& -(y^2(a^2-1)+1-x^2)^2-((e^4+2e^3)(a+1)^2+1-o^2)^2 \\
& -(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2 \\
& -\left(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2\right)^2 \\
& -(ai+k+1-l-i)^2-(16r^2y^4(a^2-1)+1-u^2)^2 \\
& -((g(k+2)+k+1)(h+j)+h-z)^2 \\
& -(p-m+l(a-n-1)+b(2a(n+1)-n(n+2)-2))^2 \\
& -(z-pm+pl(a-p)+t(2ap-p^2-1))^2 \\
& -(q-x+y(a-p-1)+s(2a(p+1)-p(p+2)-2))^2 \\
& -(l^2(a^2-1)+1-m^2)^2-(n+l+v-y)^2].
\end{aligned}
$$

Theorem

p is a prime if and only if p is a positive value of the polynomial F.

Question

How are primes distributed?

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2,$$

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2, 47! + 3,$$

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2, 47! + 3, 47! + 4,$$

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2, 47! + 3, 47! + 4, \ldots, 47! + 47$$

is a sequence of 46 consecutive composite numbers.

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2, 47! + 3, 47! + 4, \ldots, 47! + 47$$

is a sequence of 46 consecutive composite numbers.
So, there are prime deserts of arbitrary length.

Question

How are primes distributed?

Prime Deserts

Can you find 1,000,000 consecutive composite numbers?

$$47! + 2, 47! + 3, 47! + 4, \dots, 47! + 47$$

is a sequence of 46 consecutive composite numbers.
So, there are prime deserts of arbitrary length.
Does it seem as if the primes are further and further apart as we go forward on the number line?

Twin Primes

$$\{3, 5\},$$

Twin Primes

$$\{3, 5\}, \{11, 13\},$$

Twin Primes

$$\{3,5\},\{11,13\},\{41,43\}$$

are examples of “twin primes” as are

$$\{101,103\},$$

Twin Primes

$$\{3, 5\}, \{11, 13\}, \{41, 43\}$$

are examples of "twin primes" as are

$$\{101, 103\}, \{10006427,\ 10006429\},$$

Twin Primes

$$\{3,5\},\{11,13\},\{41,43\}$$

are examples of "twin primes" as are

$$\{101,103\},\{10006427,\ 10006429\},$$

and

$$\{65516468355\times 2^{333333}-1\ \&\ 65516468355\times 2^{333333}+1\}.$$

Twin Primes

$$\{3,5\},\{11,13\},\{41,43\}$$

are examples of "twin primes" as are

$$\{101,103\},\{10006427,\ 10006429\},$$

and

$$\{65516468355\times 2^{333333}-1\ \&\ 65516468355\times 2^{333333}+1\}.$$

Could there be an infinite pair of twin primes?

Twin Primes

$$\{3,5\},\{11,13\},\{41,43\}$$

are examples of "twin primes" as are

$$\{101,103\},\{10006427,\ 10006429\},$$

and

$$\{65516468355\times 2^{333333}-1\ \&\ 65516468355\times 2^{333333}+1\}.$$

Could there be an infinite pair of twin primes?
The twin prime conjecture says that the answer is yes.

Twin Primes

$$\{3,5\},\{11,13\},\{41,43\}$$

are examples of "twin primes" as are

$$\{101,103\},\{10006427,\ 10006429\},$$

and

$$\{65516468355\times 2^{333333}-1\ \&\ 65516468355\times 2^{333333}+1\}.$$

Could there be an infinite pair of twin primes?
The twin prime conjecture says that the answer is yes.

Conjecture (Schinzel's Conjecture)

There exists an infinite number of positive integers n such that each of the numbers $n+1$, $n+3$, $n+7$, $n+9$, and $n+13$ is a prime.

Definition

$\pi(x) =$ the number of primes between up to and including x.

Definition

$\pi(x) =$ the number of primes between up to and including x.

Example

$$\pi(4) = 2, \qquad \pi(10) = 4$$
$$\pi(47) = 15, \qquad \pi(100) = 25$$

Question

$\pi(x)$ *is a discontinuous function. Can we find a smooth function that approximates* $\pi(x)$*?*

x	$\pi(x)$	$\pi(x)/x$	$x/\pi(x)$
10	4	.4	2.5
100	25	.25	4
1000	168	.168	5.95238
10000	1229	.1229	8.1367
100000	9592	.09592	10.4254
10^6	78498	.078498	12.7392
10^7	664579	.0664579	15.0471
10^8	5761455	.0576146	17.3567
10^9	50847534	.0508475	19.6666

Table: The number of primes up to 10^9

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

When in doubt, differentiate

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

When in doubt, differentiate

$$10f'(10x) \quad = \quad f'(x)$$

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

When in doubt, differentiate

$$\begin{aligned} 10f'(10x) &= f'(x) \\ \text{Assume} \qquad f'(1) &= 1 \end{aligned}$$

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

When in doubt, differentiate

$$\begin{aligned} 10f'(10x) &= f'(x) \\ \text{Assume} \qquad f'(1) &= 1 \\ \text{get} \qquad f'(10) &= 1/10 \end{aligned}$$

Let $f(x)$ be a smooth function that approximates $\frac{x}{\pi(x)}$.
If we can find $f(x)$ then we can approximate $\pi(x)$.
We notice:

$$f(10x) = f(x) + 2.3$$

When in doubt, differentiate

$$\begin{aligned} 10f'(10x) &= f'(x) \\ \text{Assume} \quad f'(1) &= 1 \\ \text{get} \quad f'(10) &= 1/10 \\ \text{and} \quad f'(100) &= 1/100. \end{aligned}$$

Theorem

f a differentiable function, $f(10x) = f(x) + 2.3$, and $f'(1) = 1$, then

Theorem

f a differentiable function, $f(10x) = f(x) + 2.3$, and $f'(1) = 1$, then

$$f'(10^n) = \frac{1}{10^n},$$

for all positive integers n.

Bigger tables can convince you that, for any $a \in \mathbb{R}$, you want

$$f(ax) = f(x) + g(a),$$

where $g(a)$ is a constant (depending on a).

Bigger tables can convince you that, for any $a \in \mathbb{R}$, you want

$$f(ax) = f(x) + g(a),$$

where $g(a)$ is a constant (depending on a).

Theorem

f a differentiable function. For every $a \in \mathbb{R}$, we have $f(ax) = f(x) + g(a)$. Assume $f'(1) = 1$, then

Bigger tables can convince you that, for any $a \in \mathbb{R}$, you want

$$f(ax) = f(x) + g(a),$$

where $g(a)$ is a constant (depending on a).

Theorem

f a differentiable function. For every $a \in \mathbb{R}$, we have $f(ax) = f(x) + g(a)$. Assume $f'(1) = 1$, then

$$f'(x) = 1/x.$$

Bigger tables can convince you that, for any $a \in \mathbb{R}$, you want

$$f(ax) = f(x) + g(a),$$

where $g(a)$ is a constant (depending on a).

Theorem

f a differentiable function. For every $a \in \mathbb{R}$, we have $f(ax) = f(x) + g(a)$. Assume $f'(1) = 1$, then

$$f'(x) = 1/x.$$

Definition

For all $x > 0$, we define $\ln(x)$ by

$$\ln(x) = \int_1^x \frac{1}{t} dt.$$

$$\frac{x}{\pi(x)} \approx f(x) = \ln x$$

$$\frac{x}{\pi(x)} \approx f(x) = \ln x \qquad \Rightarrow \qquad \pi(x) \approx \frac{x}{\ln x}.$$

Theorem (The Prime Number Theorem—PNT)

Let $\pi(x)$ denote the number of primes up to x then

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

$$\frac{x}{\pi(x)} \approx f(x) = \ln x \qquad \Rightarrow \qquad \pi(x) \approx \frac{x}{\ln x}.$$

Theorem (The Prime Number Theorem—PNT)

Let $\pi(x)$ denote the number of primes up to x then

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

PNT conjectured by Gauss in 1792 when he was fifteen. It was proved by Hadamard and Poussin in 1896.

$$\frac{x}{\pi(x)} \approx f(x) = \ln x \qquad \Rightarrow \qquad \pi(x) \approx \frac{x}{\ln x}.$$

Theorem (The Prime Number Theorem—PNT)

Let $\pi(x)$ *denote the number of primes up to* x *then*

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

PNT conjectured by Gauss in 1792 when he was fifteen. It was proved by Hadamard and Poussin in 1896.

Whenever he had a few spare minutes, Gauss would find the next so many primes. He had a list of primes up to 3 million. His list has only about 72 mistakes!

Carl Friedrich Gauss (1777–1855)

Corollary

$$\lim_{x \to \infty} \frac{\pi(2x)}{\pi(x)}$$

Corollary

$$\lim_{x\to\infty}\frac{\pi(2x)}{\pi(x)} = \lim_{x\to\infty}\frac{\pi(2x)}{2x/\ln(2x)}\frac{x/\ln(x)}{\pi(x)}\frac{2x/\ln(2x)}{x/\ln(x)}$$

Corollary

$$\lim_{x\to\infty} \frac{\pi(2x)}{\pi(x)} = \lim_{x\to\infty} \frac{\pi(2x)}{2x/\ln(2x)} \frac{x/\ln(x)}{\pi(x)} \frac{2x/\ln(2x)}{x/\ln(x)} = 2.$$

Corollary

$$\lim_{x\to\infty} \frac{\pi(2x)}{\pi(x)} = \lim_{x\to\infty} \frac{\pi(2x)}{2x/\ln(2x)} \frac{x/\ln(x)}{\pi(x)} \frac{2x/\ln(2x)}{x/\ln(x)} = 2.$$

A theorem in number theory (Bertrand's postulate): there is always a prime between n and $2n$.

Corollary

$$\lim_{x\to\infty} \frac{\pi(2x)}{\pi(x)} = \lim_{x\to\infty} \frac{\pi(2x)}{2x/\ln(2x)} \frac{x/\ln(x)}{\pi(x)} \frac{2x/\ln(2x)}{x/\ln(x)} = 2.$$

A theorem in number theory (Bertrand's postulate): there is always a prime between n and $2n$.

We have now argued that, for large enough x, there is roughly the same number of primes between x and $2x$ as there are between 1 and x.

Corollary

$$\lim_{x\to\infty} \frac{\pi(2x)}{\pi(x)} = \lim_{x\to\infty} \frac{\pi(2x)}{2x/\ln(2x)} \frac{x/\ln(x)}{\pi(x)} \frac{2x/\ln(2x)}{x/\ln(x)} = 2.$$

A theorem in number theory (Bertrand's postulate): there is always a prime between n and $2n$.

We have now argued that, for large enough x, there is roughly the same number of primes between x and $2x$ as there are between 1 and x.

Gauss improves PNT

Pick a random integer between 1 and n. What is the probability that it will be prime?

Gauss improves PNT

Pick a random integer between 1 and n. What is the probability that it will be prime?

There are n integers and $\pi(n)$ of them are primes.

Gauss improves PNT

Pick a random integer between 1 and n. What is the probability that it will be prime?

There are n integers and $\pi(n)$ of them are primes.

So the probability of getting a prime is

$$\frac{\pi(n)}{n}$$

Gauss improves PNT

Pick a random integer between 1 and n. What is the probability that it will be prime?

There are n integers and $\pi(n)$ of them are primes.

So the probability of getting a prime is

$$\frac{\pi(n)}{n} \approx \frac{n/\ln(n)}{n} = \frac{1}{\ln(n)}$$

Gauss improves PNT

Pick a random integer between 1 and n. What is the probability that it will be prime?

There are n integers and $\pi(n)$ of them are primes.

So the probability of getting a prime is

$$\frac{\pi(n)}{n} \approx \frac{n/\ln(n)}{n} = \frac{1}{\ln(n)}$$

Heuristic: The "probability" that a large number x is prime is

$$\approx \frac{1}{\ln(x)}$$

Li(x)

n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1

Li(x)

n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1
Prob n prime						

Li(x)

n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1
Prob n prime	$1/\ln(2)$	$1/\ln(3)$	$1/\ln(4)$			

Li(x)

n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1
Prob n prime	$1/\ln(2)$	$1/\ln(3)$	$1/\ln(4)$	...	$1/\ln(46)$	$1/\ln(47)$

$\mathrm{Li}(x)$

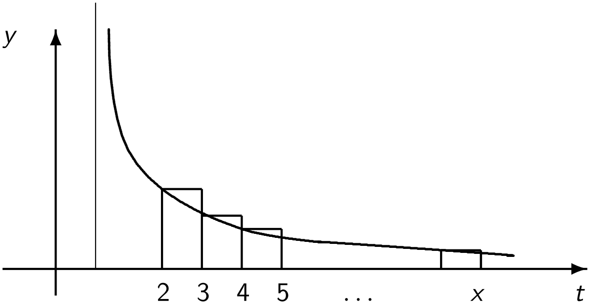
n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1
Prob n prime	$1/\ln(2)$	$1/\ln(3)$	$1/\ln(4)$	...	$1/\ln(46)$	$1/\ln(47)$

$$\pi(x) \approx \frac{1}{\ln(2)} + \frac{1}{\ln(3)} + \cdots + \frac{1}{\ln(x)}$$

Li(x)

n	2	3	4	...	46	47
Prob n prime	1	1	0	...	0	1
Prob n prime	$1/\ln(2)$	$1/\ln(3)$	$1/\ln(4)$	...	$1/\ln(46)$	$1/\ln(47)$

$$\pi(x) \approx \frac{1}{\ln(2)} + \frac{1}{\ln(3)} + \cdots + \frac{1}{\ln(x)}$$



So

$$\pi(x) \approx \frac{1}{\ln(2)} + \frac{1}{\ln(3)} + \cdots + \frac{1}{\ln(x)} \approx \int_2^x \frac{1}{\ln(t)} dt$$

So

$$\pi(x) \approx \frac{1}{\ln(2)} + \frac{1}{\ln(3)} + \cdots + \frac{1}{\ln(x)} \approx \int_2^x \frac{1}{\ln(t)} dt$$

Definition

$$\mathrm{Li}(x) = \text{Logarithmic integral} = \int_2^x \frac{1}{\ln(t)} dt$$

How good is Li(x)?

Gauss had found **6762** primes between $\mathbf{2,600,000}$ and $\mathbf{2,700,000}$.

How good is Li(x)?

Gauss had found $\mathbf{6762}$ primes
between $\mathbf{2,600,000}$ and $\mathbf{2,700,000}$.

To test the new approximation for $\pi(x)$ he calculates

How good is Li(x)?

Gauss had found **6762** primes
between $\mathbf{2,600,000}$ and $\mathbf{2,700,000}$.

To test the new approximation for $\pi(x)$ he calculates

$$\int_{2600000}^{2700000} \frac{dx}{\ln(x)} =$$

How good is Li(x)?

Gauss had found **6762** primes
between **2,600,000** and **2,700,000**.

To test the new approximation for $\pi(x)$ he calculates

$$\int_{2600000}^{2700000} \frac{dx}{\ln(x)} = \mathbf{6761.332}$$

How good is Li(x)?

Gauss had found **6762** primes
between $\mathbf{2,600,000}$ and $\mathbf{2,700,000}$.

To test the new approximation for $\pi(x)$ he calculates

$$\int_{2600000}^{2700000} \frac{dx}{\ln(x)} = \mathbf{6761.332}$$

Maple gives the number of primes as 6765 and approximates the integral as 6761.3243

x	$\pi(x)$	$x/\ln x - \pi(x)$
10^2	25	-3
10^3	168	-23
10^4	1,229	-143
10^5	9,592	-906
10^6	78,498	$-6,116$
10^7	664,579	$-44,158$
10^8	5,761,455	$-332,774$
10^9	50,847,534	$-2,592,592$
10^{10}	455,052,511	$-20,758,029$

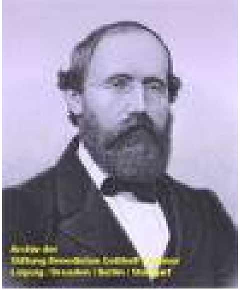
x	$\pi(x)$	$x/\ln x - \pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^2	25	-3	
10^3	168	-23	
10^4	1,229	-143	
10^5	9,592	-906	
10^6	78,498	$-6,116$	
10^7	664,579	$-44,158$	
10^8	5,761,455	$-332,774$	
10^9	50,847,534	$-2,592,592$	
10^{10}	455,052,511	$-20,758,029$	

x	$\pi(x)$	$x/\ln x - \pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^2	25	−3	5
10^3	168	−23	10
10^4	1,229	−143	
10^5	9,592	−906	
10^6	78,498	−6,116	
10^7	664,579	−44,158	
10^8	5,761,455	−332,774	
10^9	50,847,534	−2,592,592	
10^{10}	455,052,511	−20,758,029	

x	$\pi(x)$	$x/\ln x - \pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^2	25	-3	5
10^3	168	-23	10
10^4	1,229	-143	17
10^5	9,592	-906	38
10^6	78,498	$-6,116$	
10^7	664,579	$-44,158$	
10^8	5,761,455	$-332,774$	
10^9	50,847,534	$-2,592,592$	
10^{10}	455,052,511	$-20,758,029$	

x	$\pi(x)$	$x/\ln x - \pi(x)$	$\text{Li}(x) - \pi(x)$
10^2	25	-3	5
10^3	168	-23	10
10^4	1,229	-143	17
10^5	9,592	-906	38
10^6	78,498	$-6,116$	130
10^7	664,579	$-44,158$	339
10^8	5,761,455	$-332,774$	754
10^9	50,847,534	$-2,592,592$	
10^{10}	455,052,511	$-20,758,029$	

x	$\pi(x)$	$x/\ln x - \pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^2	25	-3	5
10^3	168	-23	10
10^4	1,229	-143	17
10^5	9,592	-906	38
10^6	78,498	$-6,116$	130
10^7	664,579	$-44,158$	339
10^8	5,761,455	$-332,774$	754
10^9	50,847,534	$-2,592,592$	1,701
10^{10}	455,052,511	$-20,758,029$	3,104



Georg Bernhard Riemann (1826–1866)

Riemann in 1860

Gauss counted primes as 1 and composites as 0 and got

$$\mathrm{Li}(x) \approx \pi(x)$$

Riemann in 1860

Gauss counted primes as 1 and composites as 0 and got

$$\mathrm{Li}(x) \approx \pi(x)$$

Riemann: squares of primes as $1/2$, cubes of primes as $1/3$, ...

n	2	3	4	...	46	47
Prob n prime	1	1	$1/2$	...	0	1

Riemann in 1860

Gauss counted primes as 1 and composites as 0 and got

$$\mathrm{Li}(x) \approx \pi(x)$$

Riemann: squares of primes as 1/2, cubes of primes as 1/3, ...

n	2	3	4	...	46	47
Prob n prime	1	1	1/2	...	0	1
Prob n prime	$1/\ln(2)$	$1/\ln(3)$	$1/\ln(4)$	...	$1/\ln(46)$	$1/\ln(47)$

$$\Rightarrow \mathrm{Li}(x) \approx \pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots$$

$$\Rightarrow \mathrm{Li}(x) \approx \pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots$$

Or equivalently

$$\pi(x) \approx \underbrace{\mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(\sqrt{x}) - \frac{1}{3}\mathrm{Li}(\sqrt[3]{x}) - \dots}_{R(x)}$$

Riemann found that

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\ln x)^n}{n!}$$

where

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

is the Riemann zeta function.

How good is $R(x)$?

x	$\pi(x)$
$100,000,000$	$5,761,455$
$200,000,000$	$11,078,937$
$300,000,000$	$16,252,323$
$400,000,000$	$21,336,326$
$500,000,000$	$26,355,867$
$600,000,000$	$31,324,703$
$700,000,000$	$36,252,931$
$800,000,000$	$41,146,179$
$900,000,000$	$46,009,215$
$1,000,000,000$	$50,847,534$

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
100,000,000	5,761,455	
200,000,000	11,078,937	
300,000,000	16,252,323	
400,000,000	21,336,326	
500,000,000	26,355,867	
600,000,000	31,324,703	
700,000,000	36,252,931	
800,000,000	41,146,179	
900,000,000	46,009,215	
1,000,000,000	50,847,534	

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
$100,000,000$	$5,761,455$	$5,761,552$
$200,000,000$	$11,078,937$	$11,079,090$
$300,000,000$	$16,252,323$	
$400,000,000$	$21,336,326$	
$500,000,000$	$26,355,867$	
$600,000,000$	$31,324,703$	
$700,000,000$	$36,252,931$	
$800,000,000$	$41,146,179$	
$900,000,000$	$46,009,215$	
$1,000,000,000$	$50,847,534$	

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
100, 000, 000	5, 761, 455	5, 761, 552
200, 000, 000	11, 078, 937	11, 079, 090
300, 000, 000	16, 252, 323	16, 252, 355
400, 000, 000	21, 336, 326	21, 336, 185
500, 000, 000	26, 355, 867	
600, 000, 000	31, 324, 703	
700, 000, 000	36, 252, 931	
800, 000, 000	41, 146, 179	
900, 000, 000	46, 009, 215	
1, 000, 000, 000	50, 847, 534	

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
100, 000, 000	5, 761, 455	5, 761, 552
200, 000, 000	11, 078, 937	11, 079, 090
300, 000, 000	16, 252, 323	16, 252, 355
400, 000, 000	21, 336, 326	21, 336, 185
500, 000, 000	26, 355, 867	26, 355, 517
600, 000, 000	31, 324, 703	31, 324, 622
700, 000, 000	36, 252, 931	36, 252, 719
800, 000, 000	41, 146, 179	
900, 000, 000	46, 009, 215	
1, 000, 000, 000	50, 847, 534	

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
100,000,000	5,761,455	5,761,552
200,000,000	11,078,937	11,079,090
300,000,000	16,252,323	16,252,355
400,000,000	21,336,326	21,336,185
500,000,000	26,355,867	26,355,517
600,000,000	31,324,703	31,324,622
700,000,000	36,252,931	36,252,719
800,000,000	41,146,179	41,146,248
900,000,000	46,009,215	46,009,949
1,000,000,000	50,847,534	

How good is $R(x)$?

x	$\pi(x)$	$R(x)$
100, 000, 000	5, 761, 455	5, 761, 552
200, 000, 000	11, 078, 937	11, 079, 090
300, 000, 000	16, 252, 323	16, 252, 355
400, 000, 000	21, 336, 326	21, 336, 185
500, 000, 000	26, 355, 867	26, 355, 517
600, 000, 000	31, 324, 703	31, 324, 622
700, 000, 000	36, 252, 931	36, 252, 719
800, 000, 000	41, 146, 179	41, 146, 248
900, 000, 000	46, 009, 215	46, 009, 949
1, 000, 000, 000	50, 847, 534	50, 847, 455

Riemann does even more!

$$\zeta(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \cdots$$

is only defined for $z > 1$.

Riemann does even more!

$$\zeta(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \cdots$$

is only defined for $z > 1$.

Riemann finds a way to define $\zeta(z)$ for all complex numbers $z = r + it$ except $z = 1$.

Riemann does even more!

$$\zeta(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \cdots$$

is only defined for $z > 1$.

Riemann finds a way to define $\zeta(z)$ for all complex numbers $z = r + it$ except $z = 1$.
He then proves the following *exact* formula:

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

where $\rho \in \{\text{zeroes of the } \zeta \text{ function}\}$

Conjecture (The Riemann Hypothesis)

The complex roots of the Riemann zeta function are of the form $\frac{1}{2} + it$.

Conjecture (The Riemann Hypothesis)

The complex roots of the Riemann zeta function are of the form $\frac{1}{2} + it$.

This conjecture—which has been the object of intense recent effort—is one of the most important outstanding mathematics problems.