Questions of Prime Importance

Brian Heinold

Primes

A *prime number* is an integer greater than 1 whose only divisors are 1 and itself.

The first few primes:

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, 101, ...

Number of primes

How many primes are there?

Number of primes

How many primes are there?

Infinitely many!

Number of primes

How many primes are there?

Infinitely many!

How common are primes? What percent of numbers are primes?

Number of primes

How many primes are there?

Infinitely many!

How common are primes? What percent of numbers are primes?

Proportion of integers between 1 and n that are prime $\approx \dfrac{1}{\ln n}$.

Number of primes

How many primes are there?

Infinitely many!

How common are primes? What percent of numbers are primes?

Proportion of integers between 1 and n that are prime $\approx \dfrac{1}{\ln n}$.

Roughly $\dfrac{1}{\ln(1000)} = 14.5\%$ between 2 and 1000

Roughly $\dfrac{1}{\ln(1000000)} = 7.2\%$ between 2 and 1,000,000

Number of primes, continued

This result is called the *Prime Number Theorem*.

Number of primes, continued

This result is called the *Prime Number Theorem*.

It predicts 72,382 primes less than 1,000,000, but the actual number is 78,498.

Number of primes, continued

This result is called the *Prime Number Theorem*.

It predicts 72,382 primes less than 1,000,000, but the actual number is 78,498.

Better estimate: Number of primes less than n is approximately

$$\int_2^n \frac{1}{\ln x}\, dx$$

It predicts 78628 (versus exact value 78498).

Mersenne primes

A *Mersenne prime* is a prime of the form $2^n - 1$.

$2^2 - 1 = 3$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^7 - 1 = 127$

Mersenne primes

A *Mersenne prime* is a prime of the form $2^n - 1$.

$2^2 - 1 = 3$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^7 - 1 = 127$
$2^{13} - 1 = 8191$
$2^{17} - 1 = 131071$
$2^{19} - 1 = 524287$
$2^{31} - 1 = 2147483647$
$2^{61} - 1 = 2305843009213693951$

Mersenne primes

A *Mersenne prime* is a prime of the form $2^n - 1$.

$2^2 - 1 = 3$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^7 - 1 = 127$
$2^{13} - 1 = 8191$
$2^{17} - 1 = 131071$
$2^{19} - 1 = 524287$
$2^{31} - 1 = 2147483647$
$2^{61} - 1 = 2305843009213693951$

They are getting large very fast. Are there infinitely many?

Mersenne primes, continued

No one knows, but people think there are.

Mersenne primes, continued

No one knows, but people think there are.

There are only 48 known Mersenne primes.

Mersenne primes, continued

No one knows, but people think there are.

There are only 48 known Mersenne primes.

Largest known: $2^{57885161} - 1$ (17 million digits)

Mersenne primes, continued

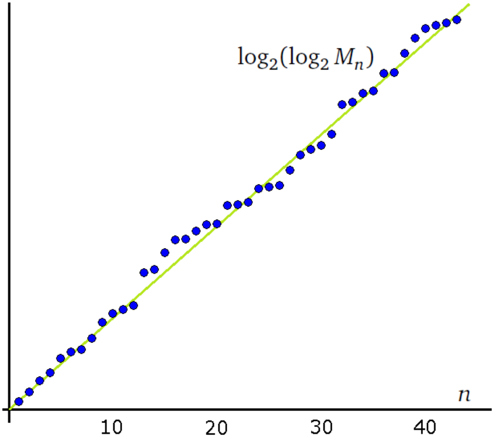
No one knows, but people think there are.

There are only 48 known Mersenne primes.

Largest known: $2^{57885161} - 1$ (17 million digits)

The exponents n in $2^n - 1$ corresponding to Mersenne primes are 2, 3, 5, 7, 13, 17, 19, 31, 61, ... Plotting the logarithm of these numbers gives:

Log of the exponent of Mersenne primes



Sophie Germain primes

Sophie Germain primes are primes p where $2p + 1$ is also prime.

2 (because $2 \cdot 2 + 1 = 5$ is also prime
3 (because $2 \cdot 3 + 1 = 7$ is also prime
5 (because $2 \cdot 5 + 1 = 11$ is also prime)
11 (because $2 \cdot 11 + 1 = 23$ is also prime)

Sophie Germain primes

Sophie Germain primes are primes p where $2p + 1$ is also prime.

2 (because $2 \cdot 2 + 1 = 5$ is also prime
3 (because $2 \cdot 3 + 1 = 7$ is also prime
5 (because $2 \cdot 5 + 1 = 11$ is also prime)
11 (because $2 \cdot 11 + 1 = 23$ is also prime)

They are important in cryptography. Are there infinitely many?

Sophie Germain primes

Sophie Germain primes are primes p where $2p+1$ is also prime.

2 (because $2 \cdot 2 + 1 = 5$ is also prime
3 (because $2 \cdot 3 + 1 = 7$ is also prime
5 (because $2 \cdot 5 + 1 = 11$ is also prime)
11 (because $2 \cdot 11 + 1 = 23$ is also prime)

They are important in cryptography. Are there infinitely many?

No one knows, but people think there are.

Fermat numbers

A *Fermat number* is a number of the form $2^{2^n}+1$.

$n = 1, 2, 3, 4, 5$ all give primes: 3, 5, 17, 257, 65537.

Fermat numbers

A *Fermat number* is a number of the form $2^{2^n} + 1$.

$n = 1, 2, 3, 4, 5$ all give primes: 3, 5, 17, 257, 65537.

Fermat conjectured that all Fermat numbers are prime.

Fermat numbers

A *Fermat number* is a number of the form $2^{2^n} + 1$.

$n = 1, 2, 3, 4, 5$ all give primes: 3, 5, 17, 257, 65537.

Fermat conjectured that all Fermat numbers are prime.

Many mathematicians now think that there are *no others*.

Fermat numbers

A *Fermat number* is a number of the form $2^{2^n} + 1$.

$n = 1, 2, 3, 4, 5$ all give primes: 3, 5, 17, 257, 65537.

Fermat conjectured that all Fermat numbers are prime.

Many mathematicians now think that there are *no others*.

But no one knows for sure. These numbers get very big, very fast ($2^{2^{32}} + 1$ has about a billion digits)

Patterns

Red curve: $n^2 + n + 41$ (generates primes at a high rate)

Progressions

Are there infinitely many primes that end in 01?

101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 01?
101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 123?
1123, 2123, 3123, 4123, 5123, 6123, 7123, **8123**, 9123, 10123, ...

Progressions

Are there infinitely many primes that end in 01?
101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 123?
1123, 2123, 3123, 4123, 5123, 6123, 7123, **8123**, 9123, 10123, ...

Yes, to both questions.

Progressions

Are there infinitely many primes that end in 01?
101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 123?
1123, 2123, 3123, 4123, 5123, 6123, 7123, **8123**, 9123, 10123, ...

Yes, to both questions.

Dirichlet's Theorem: If a and b have no factors in common, then there are infinitely many primes of the form $ak + b$.

Progressions

Are there infinitely many primes that end in 01?
101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 123?
1123, 2123, 3123, 4123, 5123, 6123, 7123, **8123**, 9123, 10123, ...

Yes, to both questions.

Dirichlet's Theorem: If a and b have no factors in common, then there are infinitely many primes of the form $ak + b$.

Numbers ending in 01: $a = 100$, $b = 1$
Numbers ending in 123: $a = 1000, b = 123$

Progressions

Are there infinitely many primes that end in 01?
101, 201, 301, **401**, 501, **601**, **701**, 801, 901, 1001, 1101, **1201**, ...

Are there infinitely many primes that end in 123?
1123, 2123, 3123, 4123, 5123, 6123, 7123, **8123**, 9123, 10123, ...

Yes, to both questions.

Dirichlet's Theorem: If a and b have no factors in common, then there are infinitely many primes of the form $ak + b$.

Numbers ending in 01: $a = 100$, $b = 1$
Numbers ending in 123: $a = 1000, b = 123$

Applies to many other cases as well.

Progressions, continued

How about sequences of equally-spaced primes?

3, 5, 7 (each 2 apart)
5, 11, 17, 23, 29 (each 6 apart)

Is it possible to find arbitrarily long progressions?

Progressions, continued

How about sequences of equally-spaced primes?

3, 5, 7 (each 2 apart)
5, 11, 17, 23, 29 (each 6 apart)

Is it possible to find arbitrarily long progressions?

Yes [Green & Tao, 2004]

Progressions, continued

How about sequences of equally-spaced primes?

3, 5, 7 (each 2 apart)
5, 11, 17, 23, 29 (each 6 apart)

Is it possible to find arbitrarily long progressions?

Yes [Green & Tao, 2004]

Longest known is 25 terms long, starting at 43,142,846,595,714,191

A simple question

Is there always a prime between consecutive squares?

between 1 and 4: 2, 3
between 4 and 9: 5, 7
between 9 and 16: 11, 13
between 16 and 25: 17, 19, 23

A simple question

Is there always a prime between consecutive squares?

between 1 and 4: 2, 3
between 4 and 9: 5, 7
between 9 and 16: 11, 13
between 16 and 25: 17, 19, 23
between 10,000 and 10,201: 23 primes
between 1,000,000 and 1,002,001: 152 primes

A simple question

Is there always a prime between consecutive squares?

between 1 and 4: 2, 3
between 4 and 9: 5, 7
between 9 and 16: 11, 13
between 16 and 25: 17, 19, 23
between 10,000 and 10,201: 23 primes
between 1,000,000 and 1,002,001: 152 primes

No one can prove the fact, though it is very likely true.

A simple question, continued

Gap between n^2 and $(n+1)^2$ is $2n+1$

Gap between consecutive primes near n^2 is about $\ln(n^2)$ (by Prime Number Theorem)

A simple question, continued

Gap between n^2 and $(n+1)^2$ is $2n+1$

Gap between consecutive primes near n^2 is about $\ln(n^2)$ (by Prime Number Theorem)

$\ln n$ is much smaller than $2n+1$
$\ln(n^2) = 14$ vs. $2n+1 = 2001$

A simple question, continued

Gap between n^2 and $(n+1)^2$ is $2n+1$

Gap between consecutive primes near n^2 is about $\ln(n^2)$ (by Prime Number Theorem)

$\ln n$ is much smaller than $2n+1$
$\ln(n^2) = 14$ vs. $2n+1 = 2001$

Roughly one in every 14 numbers in that range is prime, and the range is 2001 numbers long. So we would expect lots of primes in there.

A simple question, continued

Gap between n^2 and $(n+1)^2$ is $2n+1$

Gap between consecutive primes near n^2 is about $\ln(n^2)$ (by Prime Number Theorem)

$\ln n$ is much smaller than $2n+1$
$\ln(n^2) = 14$ vs. $2n+1 = 2001$

Roughly one in every 14 numbers in that range is prime, and the range is 2001 numbers long. So we would expect lots of primes in there.But maybe the primes have some unexpectedly huge gap at some point?

A simple question, continued

Gap between n^2 and $(n+1)^2$ is $2n+1$

Gap between consecutive primes near n^2 is about $\ln(n^2)$ (by Prime Number Theorem)

$\ln n$ is much smaller than $2n+1$
$\ln(n^2) = 14$ vs. $2n+1 = 2001$

Roughly one in every 14 numbers in that range is prime, and the range is 2001 numbers long. So we would expect lots of primes in there.But maybe the primes have some unexpectedly huge gap at some point?

Gaps between first 100 primes:

1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14, 4, 6, 2, 10, 2, 6, 6, 4, 6, 6, 2, 10, 2, 4, 2, 12, 12, 4, 2, 4, 6, 2, 10, 6, 6, 6, 2, 6, 4, 2, 10, 14, 4, 2, 4, 14, 6, 10, 2, 4, 6, 8, 6, 6, 4, 6, 8, 4, 8, 10, 2, 10, 2, 6, 4, 6, 8, 4, 2, 4, 12, 8, 4, 8, 4, 6, 12, 2, 18

Twin Primes

Twin primes are primes that are 2 apart.

..., 23, 29, 31, 37, **41**, **43**, 47, 53, **59**, **61**, 67, **71**, **73**, 79, 83, ...

Twin Primes

Twin primes are primes that are 2 apart.

$\ldots, 23, 29, 31, 37, \mathbf{41}, \mathbf{43}, 47, 53, \mathbf{59}, \mathbf{61}, 67, \mathbf{71}, \mathbf{73}, 79, 83, \ldots$

Are there infinitely many pairs?

Twin Primes

Twin primes are primes that are 2 apart.

$\ldots, 23, 29, 31, 37, \mathbf{41}, \mathbf{43}, 47, 53, \mathbf{59}, \mathbf{61}, 67, \mathbf{71}, \mathbf{73}, 79, 83, \ldots$

Are there infinitely many pairs?

Probably (*Twin Primes Conjecture*).

Twin Primes

Twin primes are primes that are 2 apart.
$\ldots, 23, 29, 31, 37, \mathbf{41}, \mathbf{43}, 47, 53, \mathbf{59}, \mathbf{61}, 67, \mathbf{71}, \mathbf{73}, 79, 83, \ldots$

Are there infinitely many pairs?

Probably (*Twin Primes Conjecture*).

There are some partial results:

- Chen Jingrun 1973: There are infinitely many pairs $(p, p+2)$ where p is prime and $p+2$ is either prime or the product of two primes.

Twin Primes

Twin primes are primes that are 2 apart.

$\ldots, 23, 29, 31, 37, \mathbf{41}, \mathbf{43}, 47, 53, \mathbf{59}, \mathbf{61}, 67, \mathbf{71}, \mathbf{73}, 79, 83, \ldots$

Are there infinitely many pairs?

Probably (*Twin Primes Conjecture*).

There are some partial results:

- Chen Jingrun 1973: There are infinitely many pairs $(p, p+2)$ where p is prime and $p+2$ is either prime or the product of two primes.
- Recent work (Zhang et al. 2013-2014): There are infinitely many primes p such that one of $p+2, p+4, \ldots, p+246$ is also prime.

Twin Primes

Twin primes are primes that are 2 apart.

$\ldots, 23, 29, 31, 37, \mathbf{41}, \mathbf{43}, 47, 53, \mathbf{59}, \mathbf{61}, 67, \mathbf{71}, \mathbf{73}, 79, 83, \ldots$

Are there infinitely many pairs?

Probably (*Twin Primes Conjecture*).

There are some partial results:

- Chen Jingrun 1973: There are infinitely many pairs $(p, p+2)$ where p is prime and $p+2$ is either prime or the product of two primes.
- Recent work (Zhang et al. 2013-2014): There are infinitely many primes p such that one of $p+2, p+4, \ldots, p+246$ is also prime.
- Largest known twin prime pair: $3756801695685 \cdot 2^{666669} \pm 1$ (about 200,000 digits)

Goldbach's Conjecture

Goldbach's Conjecture: Every even number greater than 2 is the sum of two primes

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 5 + 3$
$10 = 5 + 5$ or $3 + 7$

Goldbach's Conjecture

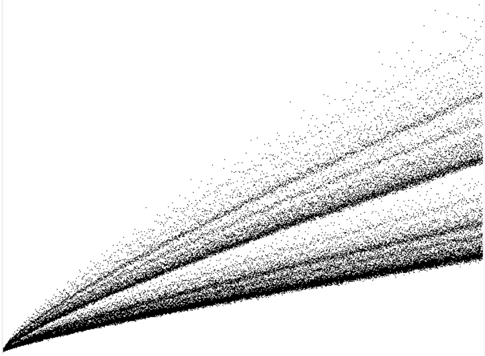
Goldbach's Conjecture: Every even number greater than 2 is the sum of two primes

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 5 + 3$
$10 = 5 + 5$ or $3 + 7$

$100 = 3 + 97,\ 11 + 89,\ 17 + 83,\ 29 + 71,\ 41 + 59,\ 47 + 53$
28 ways to write 1000
127 ways to write 10,000
810 ways to write 100,000

Goldbach's Conjecture, continued

Here is a graph showing how the number of possible ways to write a number as a sum of two primes increases with n. (The horizontal axis runs from $n = 4$ to $n =$100,000 and the vertical axis runs to about 2000.)



Goldbach's Conjecture, continued

The number of ways to write a number as a sum of two primes seems to be getting quite large.

Goldbach's Conjecture, continued

The number of ways to write a number as a sum of two primes seems to be getting quite large.

Yet no one can prove that there is even *one* way to write every number as a sum of two primes.

Goldbach's Conjecture, continued

The number of ways to write a number as a sum of two primes seems to be getting quite large.

Yet no one can prove that there is even *one* way to write every number as a sum of two primes.

Partial results:

- Chen Jingrun early 1970s: Every sufficiently large even number can be written as a sum $p + q$, where p is prime and q is either prime or a product of two primes.
- *Weak Goldbach conjecture* Every odd number greater than 7 is the sum of three primes. Seems to have been proved true in 2013.
- The (strong) Goldbach conjecture has been verified by computer for all integers less than 10^{18}.

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.
- There is a $1,000,000 prize for solving it.

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.
- There is a $1,000,000 prize for solving it.
- Its solution would answer many questions about primes.

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.
- There is a $1,000,000 prize for solving it.
- Its solution would answer many questions about primes.
- There are many “theorems” in math that start out: “If the Riemann Hypothesis is true, then…”

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.
- There is a $1,000,000 prize for solving it.
- Its solution would answer many questions about primes.
- There are many "theorems" in math that start out: "If the Riemann Hypothesis is true, then..."
- If RH is true, it would mean that we have a pretty good understanding of distribution of primes, that they are distributed pretty regularly.

The Riemann Hypothesis

- The most famous unsolved problem in math is the *Riemann Hypothesis*.
- There is a $1,000,000 prize for solving it.
- Its solution would answer many questions about primes.
- There are many "theorems" in math that start out: "If the Riemann Hypothesis is true, then…"
- If RH is true, it would mean that we have a pretty good understanding of distribution of primes, that they are distributed pretty regularly.
- If false, then we don't understand primes as well as we thought.

The *zeta function* (very important in number theory):

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

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \quad \text{(diverges)}$$

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3} = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots \approx 1.202$$

$$\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \cdots = \frac{\pi^4}{90}.$$

Zeta function and the Riemann Hypothesis

The Zeta Function has a connection with primes:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}$$

For example:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots = \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times \frac{10}{11} \times \cdots .$$

A process called *analytic continuation* is used to create a function defined for most real and complex numbers that agrees with the Zeta function wherever it is defined.

Statement of the Riemann Hypothesis

A process called *analytic continuation* is used to create a function defined for most real and complex numbers that agrees with the Zeta function wherever it is defined.

This new function, called the *Riemann Zeta function* has zeroes at -2, -4, -6, $\ldots$.

Statement of the Riemann Hypothesis

A process called *analytic continuation* is used to create a function defined for most real and complex numbers that agrees with the Zeta function wherever it is defined.

This new function, called the *Riemann Zeta function* has zeroes at -2, -4, -6, $\ldots$.

It has many other zeroes whose real parts are all equal to 1/2.

Statement of the Riemann Hypothesis

A process called *analytic continuation* is used to create a function defined for most real and complex numbers that agrees with the Zeta function wherever it is defined.

This new function, called the *Riemann Zeta function* has zeroes at -2, -4, -6, ...

It has many other zeroes whose real parts are all equal to 1/2.

The *Riemann Hypothesis* states that there are no other zeroes.

Statement of the Riemann Hypothesis

A process called *analytic continuation* is used to create a function defined for most real and complex numbers that agrees with the Zeta function wherever it is defined.

This new function, called the *Riemann Zeta function* has zeroes at -2, -4, -6, $\ldots$.

It has many other zeroes whose real parts are all equal to $1/2$.

The *Riemann Hypothesis* states that there are no other zeroes.

The locations of those zeroes have important consequences for what we know about primes.

Thanks!

Thank you for your attention.