The beauty, mystery, and utility of prime numbers

Tom Marley

University of Nebraska-Lincoln

February 7, 2015

The natural numbers

In this talk, by *number* we will mean one of the whole numbers

$$1, 2, 3, 4, 5, ...$$

Mathematicians call these the *natural numbers*.

The natural numbers

In this talk, by *number* we will mean one of the whole numbers

$$1, 2, 3, 4, 5, ...$$

Mathematicians call these the *natural numbers*.

"God made the natural numbers, all else is the work of man."
(Leopold Kronecker, 1823-1891)

The natural numbers

In this talk, by *number* we will mean one of the whole numbers

$$1, 2, 3, 4, 5, ...$$

Mathematicians call these the *natural numbers*.

"God made the natural numbers, all else is the work of man."
(Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which evenly divides the number; i.e., divides with no remainder.

The natural numbers

In this talk, by *number* we will mean one of the whole numbers

$$1, 2, 3, 4, 5, ...$$

Mathematicians call these the *natural numbers*.

"God made the natural numbers, all else is the work of man."
(Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which evenly divides the number; i.e., divides with no remainder.

- 4 is a factor of 20 because 20 divided by 4 is 5 with no remainder.

The natural numbers

In this talk, by *number* we will mean one of the whole numbers

$$1, 2, 3, 4, 5, ...$$

Mathematicians call these the *natural numbers*.

"God made the natural numbers, all else is the work of man." (Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which evenly divides the number; i.e., divides with no remainder.

- 4 is a factor of 20 because 20 divided by 4 is 5 with no remainder.
- 3 is **not** a factor of 20 because 20 divided by 3 is 6 with remainder 2.

What is a prime number?

For small numbers, we can easily list all its factors:

What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.

What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

For reasons we'll discuss later, we exclude the number 1 from being prime.

What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

For reasons we'll discuss later, we exclude the number 1 from being prime.

The first few prime numbers are:

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

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$48 = 8 \times 6$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned} 48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \end{aligned}$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$
\begin{aligned}
48 &= 8 \times 6 \\
&= 2 \times 4 \times 2 \times 3 \\
&= 2 \times 2 \times 2 \times 2 \times 3
\end{aligned}
$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned} 48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3 \end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned} 48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3 \end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$48 = 12 \times 4$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned} 48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3 \end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned} 48 &= 12 \times 4 \\ &= 3 \times 4 \times 2 \times 2 \end{aligned}$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned} 48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3 \end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned} 48 &= 12 \times 4 \\ &= 3 \times 4 \times 2 \times 2 \\ &= 3 \times 2 \times 2 \times 2 \times 2 \end{aligned}$$

Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6\\ &= 2 \times 4 \times 2 \times 3\\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned}48 &= 12 \times 4\\ &= 3 \times 4 \times 2 \times 2\\ &= 3 \times 2 \times 2 \times 2 \times 2\end{aligned}$$

This fact is known as *The Fundamental Theorem of Arithmetic*

How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

He did this using *Proof by Contradiction*.

How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

He did this using *Proof by Contradiction*.

This is a method of logic whereby one assumes a statement is false and shows this leads to an ‘absurdity’.

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number N.

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number N.

Question: What is the remainder when you divide N by one of the primes?

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number N.

Question: What is the remainder when you divide N by one of the primes?
Answer: One!

Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abusdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number N.

Question: What is the remainder when you divide N by one of the primes?
Answer: One!

This means that N is not divisible by any prime! This is our 'abusurdity'.

A simple primality test

A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.

A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.
So, to see if a number between 2 and 100 is prime, we just have to check if it is divisible by 2, 3, 5, or 7.

A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.
So, to see if a number between 2 and 100 is prime, we just have to check if it is divisible by 2, 3, 5, or 7.

We can make an algorithm out of this, which is called the

Sieve of Eratosthenes.

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

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~~

Prime: 2

All multiples of 2 crossed out.

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~~

Primes: 2, 3

All multiples of 2 and 3 crossed out.

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

Primes: 2, 3, 5

All multiples of 2, 3, and 5 crossed out.

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~~

Primes: 2, 3, 5, 7 and all other uncrossed numbers

All multiples of 2, 3, 5, and 7 crossed out.

The prime number theorem

Question: Suppose we want to check if large number is prime. Is the Sieve a good method?

The prime number theorem

Question: Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

The prime number theorem

Question: Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

The Prime Number Theorem, which was proved around 1900, states that for an n-digit number N, the number of primes less than or equal to $\sqrt{N}$ is (approximately) at least

$$\frac{(3.16)^n}{(1.15)n}.$$

The prime number theorem

Question: Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

The Prime Number Theorem, which was proved around 1900, states that for an n-digit number N, the number of primes less than or equal to $\sqrt{N}$ is (approximately) at least

$$\frac{(3.16)^n}{(1.15)n}.$$

This function grows very fast with n. Consequently, it would take thousands of years for even the world's fastest supercomputers to check if a 400-digit number is prime using the Sieve.

Pascal's Triangle

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

Fact: If n is prime then n divides all the middle terms in it's row.

Fermat's Theorem

For example,

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Fermat's Theorem

For example,

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a+b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

Fermat's Theorem

For example,

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a+b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

In general, if p is prime then $(a+b)^p - a^p - b^p$ is divisible by p for all numbers a and b.

Fermat's Theorem

For example,

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a+b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

In general, if p is prime then $(a+b)^p - a^p - b^p$ is divisible by p for all numbers a and b.
It's a very short argument from there to...

Fermat's Theorem: If p is a prime number then p divides $a^p - a$ for all numbers a.

Carmichael numbers

Question: Does Fermat's Theorem only work for prime numbers?

That is, suppose n is a number and $a^n - a$ is divisible by n for all numbers a. Must n be prime?

Carmichael numbers

Question: Does Fermat's Theorem only work for prime numbers?

That is, suppose n is a number and $a^n - a$ is divisible by n for all numbers a. Must n be prime?

Unfortunately, the answer is no! There are numbers, called Carmichael numbers, which have the Fermat property but are not prime. The smallest Carmichael number is $561 = (3)(11)(17)$.

Carmichael numbers

Question: Does Fermat's Theorem only work for prime numbers?

That is, suppose n is a number and $a^n - a$ is divisible by n for all numbers a. Must n be prime?

Unfortunately, the answer is no! There are numbers, called Carmichael numbers, which have the Fermat property but are not prime. The smallest Carmichael number is $561 = (3)(11)(17)$.

The good news is: Carmichael numbers are quite rare relative to prime numbers!

A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number N is prime.

A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number N is prime.

Step 1: Choose a random number a and compute the remainder of $a^N - a$ upon dividing by N.

A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number N is prime.

Step 1: Choose a random number a and compute the remainder of $a^N - a$ upon dividing by N.

Step 2: If the remainder is not zero, then STOP: N is not prime.

A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number N is prime.

Step 1: Choose a random number a and compute the remainder of $a^N - a$ upon dividing by N.

Step 2: If the remainder is not zero, then STOP: N is not prime.

Step 3: If the remainder is zero, repeat Step 1 with a new random number a.

A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number N is prime.

Step 1: Choose a random number a and compute the remainder of $a^N - a$ upon dividing by N.

Step 2: If the remainder is not zero, then STOP: N is not prime.

Step 3: If the remainder is zero, repeat Step 1 with a new random number a.

Continue the loop until, with increasing probability, you conclude that N is either prime or (if you are really unlucky) a Carmichael number.

A polynomial time algorithm

Question: Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

A polynomial time algorithm

Question: Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a polynomial function of the number of digits (n) of the number being tested.

A polynomial time algorithm

Question: Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a polynomial function of the number of digits (n) of the number being tested.

For example, $5n^3 + 3n^2 - 20n + 7$ is a polynomial function in n.

A polynomial time algorithm

Question: Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a polynomial function of the number of digits (n) of the number being tested.

For example, $5n^3 + 3n^2 - 20n + 7$ is a polynomial function in n.

However, the function

$$\frac{(3.16)^n}{(1.15)n}$$

is **not** bounded by a polynomial function of n.

A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.

A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.

In fact, Kayal and Saxena were undergraduates!!

A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.

In fact, Kayal and Saxena were undergraduates!!

Their algorithm, now known as the AKS primality test, determines with certainty whether an n-digit number. The number of divisions needed in their algorithm is bounded by a polynomial function in n of degree 12.

This has now been improved to a polynomial of degree 6.

Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose n is a 400-digit number which is the product of two prime numbers, p and q. Using the best known algorithms, it would take a supercomputer thousands of years to find p and q!

Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose n is a 400-digit number which is the product of two prime numbers, p and q. Using the best known algorithms, it would take a supercomputer thousands of years to find p and q!

The good news: This phenomenon has practical applications!

Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose n is a 400-digit number which is the product of two prime numbers, p and q. Using the best known algorithms, it would take a supercomputer thousands of years to find p and q!

The good news: This phenomenon has practical applications!

It forms the basis for *public key cryptography*, which was discovered by three mathematicians at M.I.T.: Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. It is now known as the RSA cryptosystem.

RSA cryptosystem

Here is roughly the idea behind RSA:

RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers p and q and multiply them together to get $N = pq$.

RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers p and q and multiply them together to get $N = pq$.

Now I choose any number e which has no common divisor with $p - 1$ or $q - 1$.

RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers p and q and multiply them together to get $N = pq$.

Now I choose any number e which has no common divisor with $p - 1$ or $q - 1$.

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number m.

RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers p and q and multiply them together to get $N = pq$.

Now I choose any number e which has no common divisor with $p - 1$ or $q - 1$.

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number m.

Then Bob should compute the remainder of m^e divided by N. Call this remainder r.

RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers p and q and multiply them together to get $N = pq$.

Now I choose any number e which has no common divisor with $p - 1$ or $q - 1$.

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number m.

Then Bob should compute the remainder of m^e divided by N. Call this remainder r.

Bob then sends r to me using any public channel he wishes (e.g., the internet).

RSA - decryption

So I receive from Bob the number r. How do I recover the original message m?

RSA - decryption

So I receive from Bob the number r. How do I recover the original message m?

Since I know p and q, I can compute a number d such that the remainder of ed divided by $(p-1)(q-1)$ is 1.

RSA - decryption

So I receive from Bob the number r. How do I recover the original message m?

Since I know p and q, I can compute a number d such that the remainder of ed divided by $(p-1)(q-1)$ is 1.

By the magic of Fermat's Theorem, one can show that the remainder of r^d divided by N is m!

RSA - decryption

So I receive from Bob the number r. How do I recover the original message m?

Since I know p and q, I can compute a number d such that the remainder of ed divided by $(p-1)(q-1)$ is 1.

By the magic of Fermat's Theorem, one can show that the remainder of r^d divided by N is m!

Why is this secure? Because there is no known way to find d without first knowing p and q. So the security depends on the factorization problem being "hard".

Fermat Primes

A prime number of the form $2^n + 1$ is called a Fermat prime.

Fermat Primes

A prime number of the form $2^n + 1$ is called a Fermat prime.

Some Fermat primes:

$$3 = 2^1 + 1$$
$$5 = 2^2 + 1$$
$$17 = 2^4 + 1$$
$$257 = 2^8 + 1$$
$$65,537 = 2^{16} + 1$$

Fermat Primes

A prime number of the form $2^n + 1$ is called a Fermat prime.

Some Fermat primes:

$$
\begin{aligned}
3 &= 2^1 + 1 \\
5 &= 2^2 + 1 \\
17 &= 2^4 + 1 \\
257 &= 2^8 + 1 \\
65,537 &= 2^{16} + 1
\end{aligned}
$$

Fact: If $2^n + 1$ is prime then n must be a power of 2.

Fermat Primes

A prime number of the form $2^n + 1$ is called a Fermat prime.

Some Fermat primes:

$$\begin{aligned} 3 &= 2^1 + 1 \\ 5 &= 2^2 + 1 \\ 17 &= 2^4 + 1 \\ 257 &= 2^8 + 1 \\ 65,537 &= 2^{16} + 1 \end{aligned}$$

Fact: If $2^n + 1$ is prime then n must be a power of 2.

It is unknown if any other Fermat primes exist.

Mersenne primes

A prime number of the form $2^n - 1$ is called a Mersenne prime.
(Mersenne was a French monk who lived in the 17th century.)
Some Mersenne primes:

$$
\begin{aligned}
3 &= 2^2 - 1 \\
7 &= 2^3 - 1 \\
31 &= 2^5 - 1 \\
127 &= 2^7 - 1
\end{aligned}
$$

Mersenne primes

A prime number of the form $2^n - 1$ is called a Mersenne prime. (Mersenne was a French monk who lived in the 17th century.)
Some Mersenne primes:

$$\begin{aligned} 3 &= 2^2 - 1 \\ 7 &= 2^3 - 1 \\ 31 &= 2^5 - 1 \\ 127 &= 2^7 - 1 \end{aligned}$$

Fact: If $2^n - 1$ is prime then n must be prime.

Mersenne primes

A prime number of the form $2^n - 1$ is called a Mersenne prime. (Mersenne was a French monk who lived in the 17th century.) Some Mersenne primes:

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

Fact: If $2^n - 1$ is prime then n must be prime.

There are 48 known Mersenne primes. (In fact, these are the largest known prime numbers.)

Mersenne primes

A prime number of the form $2^n - 1$ is called a Mersenne prime. (Mersenne was a French monk who lived in the 17th century.) Some Mersenne primes:

$$\begin{aligned} 3 &= 2^2 - 1 \\ 7 &= 2^3 - 1 \\ 31 &= 2^5 - 1 \\ 127 &= 2^7 - 1 \end{aligned}$$

Fact: If $2^n - 1$ is prime then n must be prime.

There are 48 known Mersenne primes. (In fact, these are the largest known prime numbers.)

It is unknown if there are infinitely many Mersenne primes.

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since $1 + 2 + 3 = 6$, 6 is a perfect number.

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since $1 + 2 + 3 = 6$, 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since $1 + 2 + 4 + 7 + 14 = 28$, 28 is a perfect number.

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since $1 + 2 + 3 = 6$, 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since $1 + 2 + 4 + 7 + 14 = 28$, 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since $1 + 2 + 3 = 6$, 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since $1 + 2 + 4 + 7 + 14 = 28$, 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

It can be shown (with a little arithmetic) that if N is a Mersenne prime, then $\frac{N(N+1)}{2}$ is a perfect number.

Perfect numbers

A number is called perfect if it is equal to the sum of all it's divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since $1 + 2 + 3 = 6$, 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since $1 + 2 + 4 + 7 + 14 = 28$, 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

It can be shown (with a little arithmetic) that if N is a Mersenne prime, then $\frac{N(N+1)}{2}$ is a perfect number.

Moreover, every even perfect number has this form. So there are exactly as many even perfect numbers as there are Mersenne primes!

Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

Goldbach's Conjecture, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

Goldbach's Conjecture, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

For example:

- $10=7+3$
- $32=19+13$
- $68=61+7$
- $100=47+53$

Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

Goldbach's Conjecture, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

For example:

- 10=7+3
- 32=19+13
- 68=61+7
- 100=47+53

This problem has been unsolved for over 350 years!

The Twin Prime Conjecture

Two prime numbers which differ by two are called twin primes.

The Twin Prime Conjecture

Two prime numbers which differ by two are called twin primes.

Here are some examples of twin primes:

- $11, 13$
- $29, 31$
- $41, 43$
- $71, 73$

The Twin Prime Conjecture asserts that there are infinitely many twin prime pairs.

The Twin Prime Conjecture

Two prime numbers which differ by two are called twin primes.

Here are some examples of twin primes:

- $11, 13$
- $29, 31$
- $41, 43$
- $71, 73$

The Twin Prime Conjecture asserts that there are infinitely many twin prime pairs.

This problem has remained unsolved for centuries (perhaps even millenia).

A recent breakthrough

One could ask an even weaker question:

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

Even the answer to this question was unknown

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

Yitang Zhang, a mathematician at the University of New Hampshire, proved that there exists an $N \leq 70,000,000$ such that there are infinitely many prime pairs exactly N units apart.

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

Yitang Zhang, a mathematician at the University of New Hampshire, proved that there exists an $N \leq 70,000,000$ such that there are infinitely many prime pairs exactly N units apart.

This bound has since been improved to $N \leq 246$.

A recent breakthrough

One could ask an even weaker question:

Question: Does there exist any number N such that there are infinitely many prime pairs which are exactly N units apart?

(The case $N = 2$ is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

Yitang Zhang, a mathematician at the University of New Hampshire, proved that there exists an $N \leq 70,000,000$ such that there are infinitely many prime pairs exactly N units apart.

This bound has since been improved to $N \leq 246$.

The case $N = 2$ remains elusive....waiting for YOU to solve it.

Thank you!