A puzzle

Alice and **Bob** are trying to send each other a message without **Eve the Eavesdropper** being able to read it.

There are some positive integers in each column. **Only Alice** can access the numbers in her column. **Only Bob** can access the numbers in his column. **Anyone** can access the numbers in the public column.

Alice	Public	Bob
a	$g \qquad n$	b
a is between 1 and n.	g is a small prime number. n is a **very** big number.	b is between 1 and n.

If Eve can read anything Alice and Bob send to each other, how can Alice and Bob both know a number without Eve knowing that number as well?

Cryptography

Vincent Macri

Table of Contents

Quick review
Modular Arithmetic

We define the mod operator as being the remainder when dividing two numbers. That is:

$$a \bmod b = \text{the remainder of } a \div b$$

In some programming languages, modulo is written as $\%$ or rem. Use whichever notation you are most comfortable with.

Examples

$$4 \bmod 2 = 0 \qquad 7 \bmod 3 = 1$$

$$5 \bmod 2 = 1 \qquad 9 \bmod 5 = 4$$

The definition of modulo (mod for short) is a bit trickier with negative numbers. It also doesn't matter for today, as we're only looking at mod with positive numbers.

We will also introduce a new notation, which is more of a shortcut.
If b divides a with no remainder, then we will write $b \mid a$.
More formally:

$$b \mid a \equiv a \bmod b = 0$$

Or:

$$b \mid a \iff a = bc$$

Where a, b, and c and positive integers.

Table of Contents

What is a prime number?
Primes

A **prime number** is a positive integer that is only divisible by 1 and itself.

Examples

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

If an integer greater than 1 is not prime, it is called a **composite number**.

1 is special, and is called the **unit number**

What is a prime number?
Primes

A **prime number** is a positive integer that is only divisible by 1 and itself.

Examples

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

If an integer greater than 1 is not prime, it is called a **composite number**.

1 is special, and is called the **unit number**

Proof 1 is not prime.

In the past, some mathematicians said that 1 is prime. All of them are dead now.

$$\therefore 1 \notin \mathbb{P}$$

$\square$

The largest known prime number[1] is:

$$M_{77\,232\,917} = 2^{77\,232\,917} - 1$$

If you were to print this number out, it would be 6055 pages long!

This prime was discovered by Jonathan Pace on December 26, 2017 after 6 days of continuous computer computations. The discovery was published on January 3, 2018.

[1] As of January 5th, 2018

The largest prime number
Primes

The largest known prime number[1] is:

$$M_{77\,232\,917} = 2^{77\,232\,917} - 1$$

If you were to print this number out, it would be 6055 pages long!

This prime was discovered by Jonathan Pace on December 26, 2017 after 6 days of continuous computer computations. The discovery was published on January 3, 2018.

This number is a **Mersenne prime**. These are prime numbers of the form $2^n - 1$, and we label these primes as M_n for short.

[1] As of January 5th, 2018

The largest known prime number[1] is:

$$M_{77\,232\,917} = 2^{77\,232\,917} - 1$$

If you were to print this number out, it would be 6055 pages long!

This prime was discovered by Jonathan Pace on December 26, 2017 after 6 days of continuous computer computations. The discovery was published on January 3, 2018.

This number is a **Mersenne prime**. These are prime numbers of the form $2^n - 1$, and we label these primes as M_n for short.

What's special and useful about Mersenne primes?

[1] As of January 5th, 2018

The largest known prime number[1] is:

$$M_{77\,232\,917} = 2^{77\,232\,917} - 1$$

If you were to print this number out, it would be 6055 pages long!

This prime was discovered by Jonathan Pace on December 26, 2017 after 6 days of continuous computer computations. The discovery was published on January 3, 2018.

This number is a **Mersenne prime**. These are prime numbers of the form $2^n - 1$, and we label these primes as M_n for short.

What's special and useful about Mersenne primes? Not much.

[1] As of January 5th, 2018

Is the number of primes finite?

How many primes are there?

Primes

Is the number of primes finite?

No! There are infinite prime numbers!
This was proved thousands of years ago by Euclid.

Proof of infinite primes

Assume the list of primes is finite, and there are only n prime numbers. We will call our list of prime numbers P.

$$P = \{p_1, p_2, \ldots, p_{n-1}, p_n\}$$

Where p_k is the kth prime number.

Proof of infinite primes

Primes

Assume the list of primes is finite, and there are only n prime numbers. We will call our list of prime numbers P.

$$P = \{p_1, p_2, \ldots, p_{n-1}, p_n\}$$

Where p_k is the kth prime number.

Now, let m be the product of all numbers in P plus 1.

$$m = (p_1 \times p_2 \times \cdots \times p_{n-1} \times p_n) + 1 = \left(\sum_{i=1}^{n} p_i \right) + 1$$

m is either prime or not prime. Let's look at both cases.

Proof of infinite primes: m is prime

First, let's consider the case that m is prime.

Proof of infinite primes: m is prime

Primes

First, let's consider the case that m is prime.

Note that m is not in our original list, P.

Proof of infinite primes: m is prime

First, let's consider the case that m is prime.

Note that m is not in our original list, P.

If m is prime, our original list is incomplete, and there are more prime numbers than we listed.

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

For example:

$$P = \{2, 3, 5, 7, 11, 13\}$$

$$m = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$$

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

For example:

$$P = \{2, 3, 5, 7, 11, 13\}$$

$$m = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$$

$$30\,031 \bmod 2 = 1 \qquad 30\,031 \bmod 7 = 1$$

$$30\,031 \bmod 3 = 1 \qquad 30\,031 \bmod 11 = 1$$

$$30\,031 \bmod 5 = 1 \qquad 30\,031 \bmod 13 = 1$$

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

For example:

$$P = \{2, 3, 5, 7, 11, 13\}$$

$$m = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$$

$$30\,031 \bmod 2 = 1 \qquad 30\,031 \bmod 7 = 1$$

$$30\,031 \bmod 3 = 1 \qquad 30\,031 \bmod 11 = 1$$

$$30\,031 \bmod 5 = 1 \qquad 30\,031 \bmod 13 = 1$$

Here, we can see that since $30\,031$ is a multiple plus 1 of every number in P, no numbers in P will divide it.

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

For example:

$$P = \{2, 3, 5, 7, 11, 13\}$$

$$m = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$$

$$30\,031 \bmod 2 = 1 \qquad 30\,031 \bmod 7 = 1$$

$$30\,031 \bmod 3 = 1 \qquad 30\,031 \bmod 11 = 1$$

$$30\,031 \bmod 5 = 1 \qquad 30\,031 \bmod 13 = 1$$

Here, we can see that since $30\,031$ is a multiple plus 1 of every number in P, no numbers in P will divide it. But if $30\,031$ is not prime, then it divisible by a prime number, so there must be some prime numbers missing from our original list.

Proof of infinite primes: m is not prime

If m is not prime, then it must be divisible by a prime number. Notice that m cannot be divisible by any numbers in P, as they would not divide a number that is a multiple of themselves plus 1.

For example:

$$P = \{2, 3, 5, 7, 11, 13\}$$

$$m = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$$

$$30\,031 \bmod 2 = 1 \qquad 30\,031 \bmod 7 = 1$$

$$30\,031 \bmod 3 = 1 \qquad 30\,031 \bmod 11 = 1$$

$$30\,031 \bmod 5 = 1 \qquad 30\,031 \bmod 13 = 1$$

Here, we can see that since $30\,031$ is a multiple plus 1 of every number in P, no numbers in P will divide it. But if $30\,031$ is not prime, then it divisible by a prime number, so there must be some prime numbers missing from our original list. $30\,031$ is divisible by 59 and 509, so these numbers are missing from our list.

How do we check if a number is prime?

How do we check if a number is prime?

How do we check if a number is prime **quickly**?

How do we check if a number is prime?

How do we check if a number is prime **quickly**?

With a **very** fast computer. Algorithms exist (some of which run in polynomial time) but they are **very** slow.
Here, "quickly" means the computer will finish before we die.

Theorem (The Unique Factorization Theorem)

Every positive integer has a unique representation as a product of prime numbers.
That is, for all numbers $n \in \mathbb{Z}^+$*:*

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$$

Where p_i *is prime, and* a_i *is a positive integer.*

Theorem (The Unique Factorization Theorem)

Every positive integer has a unique representation as a product of prime numbers.
That is, for all numbers $n \in \mathbb{Z}^+$*:*

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$$

Where p_i *is prime, and* a_i *is a positive integer.*

Example (180)

$$180 = 2^2 \times 3^2 \times 5$$

$$180 = 2 \times 2 \times 3 \times 3 \times 5$$

How do we factor a number?

Factoring
Primes

How do we factor a number?

How do we factor a **large** number?

Factoring

Primes

How do we factor a number?

How do we factor a **large** number?

Try this one:

RSA-2048

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588 07
844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618
963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151
726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242
811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784
240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273
81951378636564391212010397122822120720357

How do we factor a number?

How do we factor a **large** number?

Try this one:

RSA-2048

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588 07
8440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026 18
963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151
726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242
811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784
240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273
819513786365643912120103971228221207203 57

This number has two factors. Nobody knows what they are. There was a $\$200\,000$ prize to factor this number. People had over 15 years to factor it, but nobody was able to before the contest period ended.

Table of Contents

What are factors used for?
Introduction to Cryptography

Factorization of numbers is very useful in cryptography.
The reason for this is that factoring large numbers takes a **very** long time, but the maths for checking factorization are quick.
We can use this to develop a way to encode messages so they can only be read by certain people. This is called cryptography.

Simply put, cryptography is the study of ways to encrypt messages.

Encryption is when you transform a message so that it cannot easily be read by someone without a key. Encryption is like a lock, but instead of locking your house, it locks information.

The use of encryption goes back thousands of years.

One example of encryption was used by Julius Caesar to keep military messages protected from spies.
Caesar's encryption worked like this:

The Caesar cipher
Introduction to Cryptography

One example of encryption was used by Julius Caesar to keep military messages protected from spies.
Caesar's encryption worked like this:

Pick a number, n, between 1 and 25.
Shift every letter in the message that many letters to the right, wrapping around when you reach z.

One example of encryption was used by Julius Caesar to keep military messages protected from spies.
Caesar's encryption worked like this:

Pick a number, n, between 1 and 25.
Shift every letter in the message that many letters to the right, wrapping around when you reach z.

For example, with $n = 3$:
`Plaintext message: 'Crypto is fun!'`
`Encrypted message: 'Fubswr lv ixq!'`
Caesar's generals knew what value for n Caesar used, and would reverse the process to decode his messages.

One example of encryption was used by Julius Caesar to keep military messages protected from spies.
Caesar's encryption worked like this:

Pick a number, n, between 1 and 25.
Shift every letter in the message that many letters to the right, wrapping around when you reach z.

For example, with $n = 3$:
`Plaintext message: 'Crypto is fun!'`
`Encrypted message: 'Fubswr lv ixq!'`
Caesar's generals knew what value for n Caesar used, and would reverse the process to decode his messages.

Obviously, this isn't very secure. Why?