Cryptography

Vincent Macri

Table of Contents

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 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?

Is the number of primes finite?

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

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

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

Primes

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.