# Prime Numbers

DR. RACHEL NEVILLE

HIGH SCHOOL MATH DAY

NOVEMBER 2, 2022

# What is a prime number?

A **prime number** is a number that can only be divided exactly by 1 and itself.

Examples:

7
is prime
12
is not prime: 12=3*2*2

4219
is prime

15,233
is prime

523,147
is not prime: 523,147=967*541

# Why do we care about prime numbers?

- Prime numbers are the building blocks of whole numbers:
  - Every single number can be written uniquely as a product of prime numbers.
- There are beautiful mathematical patterns and properties that only hold for prime numbers.
- They remain mysterious.
  - Example: Distribution of Primes:

    2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, …

# Why do we care about prime numbers?

- Prime numbers keep your private information safe online (RSA Encryption)
  - Private information on the computer is all recorded as a secret code associated with a VERY large number, one that would take even the fastest computers a long time to find it's prime factors.
  - Another computer or user can only unlock that code if it knows exactly what prime numbers to multiply together to equal the very large number.

# How many prime numbers are there?

# Proof: There are infinitely many primes

Assume there are finitely many primes

$$p_1, p_2, p_3, p_4, \dots, p_n$$

Let $Q = p_1 p_2 p_3 p_4 \dots p_n + 1$

Case 1: $Q$ is prime.

$Q$ isn't on my list

Case 2: $Q$ is not prime

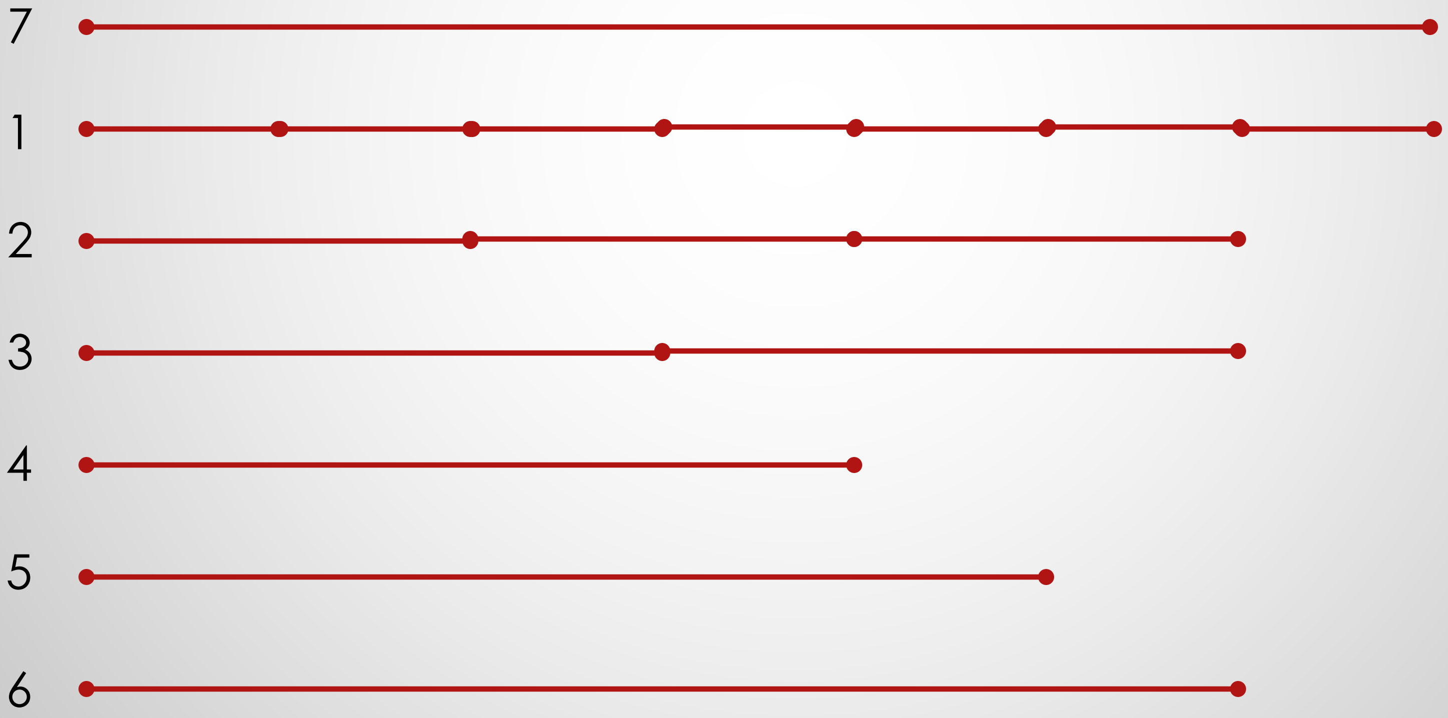
None of the primes on my list divide $Q$

# Euclid (300 BC)

- Gave the first proof that there are infinitely many primes in *Elements*
- In his (translated) words: prime numbers are more than any assigned multitude of prime numbers
- He assumed that there is a list of primes and shows that you can always add to the list.
- Written before algebra (so all his proofs used straight lines and circles)

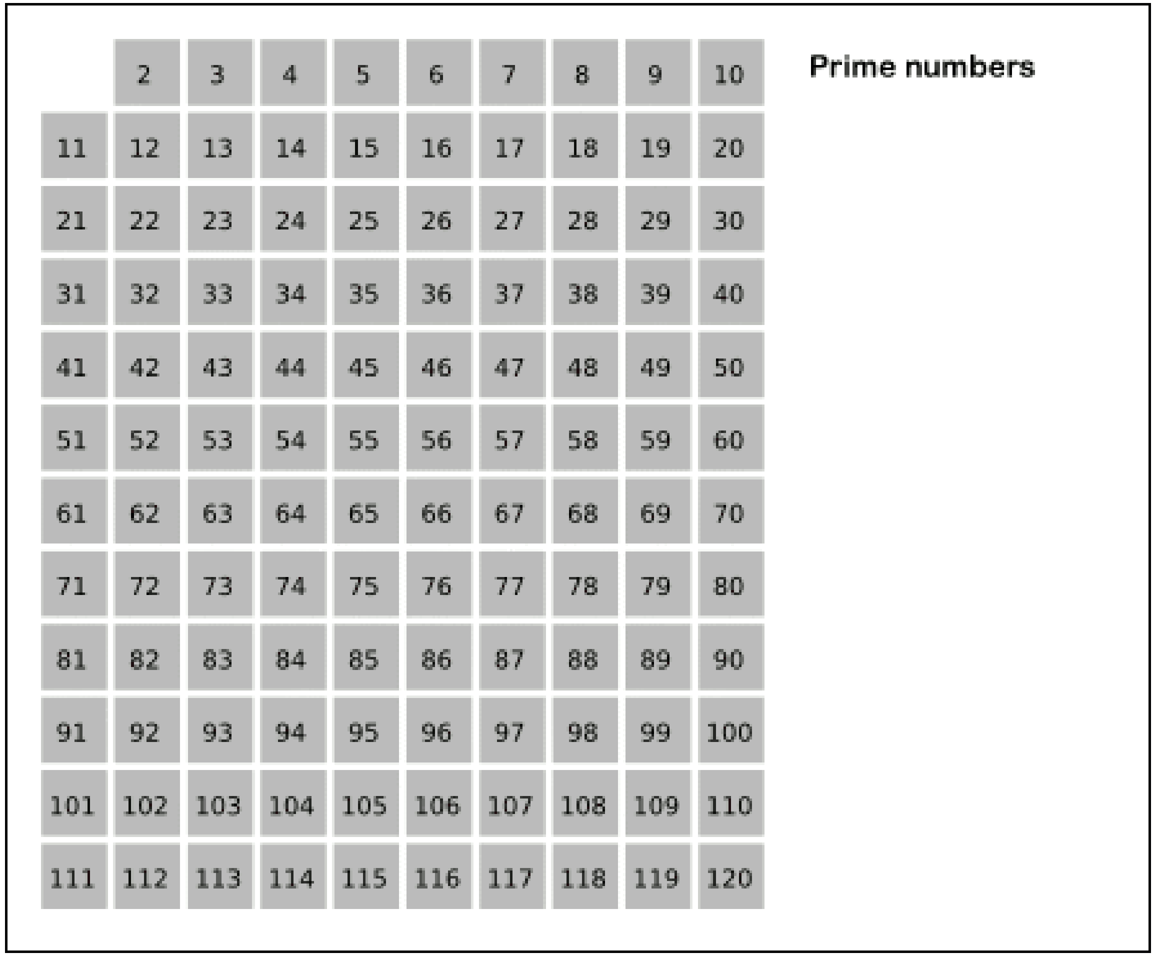
# Euclid’s Definition of Primes

A **prime number** is that which is measured by a unit alone.



# Sieve of Eratosthenese

- Ancient algorithm for finding prime numbers up to a certain limit (n)
- List all the numbers
  - Cross off all multiples of 2
  - Cross off all multiples of 3
  - …
  - Cross off all multiples of the nearest whole number less than $\sqrt{n}$
  - Remaining numbers are prime



# How do we search for prime numbers?

- **Look for patterns:**
  - 2 is the only even prime
  - If a number's digits add to a multiple of 3, it is divisible by 3.
  - Ex: 561:
    - 5+6+1=12
    - 561=3*187

# The hunt for prime numbers

- 17th century French monk Marin Mersenne: numbers of the form $2^p - 1$ are possibly (but not certainly) prime
- By 1588 Pietro Cataldi had correctly verified that $2^{17}$-1 = 131071 and $2^{19}$-1 = 524287 are both prime
- In 1876 Édouard Lucas showed that $2^{127} - 1$ is a prime
  - 39 digits – remains the highest prime discovered by manual calculations
- In 1951, computers began to be used
  - that year a new record was set with a 79-digit number
- In 1999, the largest Mersenne prime $2^{6972593} - 1$ had 2,098,960 digits

# What's the largest prime number?

- The current record is held by the 51st known Mersenne prime.
- Discovered on December 7, 2018 by Florida programmer Patrick Laroche.

$$2^{82,589,933} - 1$$

- 24,862,048 digits
  - 1.5 million digits bigger than the next largest known prime
- if you were to try to print it on paper, it would take almost 10,000 pages
- 12 days of nonstop computing to verify this is a prime number

# Verifying a Prime – Lucas Test

**Lucas Numbers:**

1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, …

- Add the previous two terms to get the next one

**Test:** For any number, n,

- 1. find the nth term in the Lucas sequence, $L_n$
- 2. Subtract 1: $L_n - 1$
- 3. Check if $L_n - 1$ is a multiple of n
- If YES, then n is *probably* a prime number. If NO, then n is *definitely not* prime.

Example: n=11

$L_n - 1$ =199-1=198

198=11*18 so 11 is probably prime

Example: n=8

$L_n - 1$ =47-1=46

46 is not a multiple of 8, so 8 is definitely not prime

# Verifying a Prime: Lucas-Lehmer Test

- 4, 14, 194, 37634, 1416317954, 2005956546822746114,….
- To find the next term, square the previous term and subtract 2

- **Test:** For any number of the form $2^p - 1$
  - 1. Take p and find the p-1 term in the sequence
  - 2. If $L_{p-1}$ Is a multiple of $2^p - 1$ , then $2^p - 1$ is definitely a prime

    If $L_{p-1}$ is a not multiple of $2^p - 1$ , then $2^p - 1$ is definitely not a prime

Lucas used this method to show $2^{67} - 1$ is not prime without ever finding factors.

# Can you find the next prime?

- $3,000 GIMPS Research Discovery Award for any new prime
- $150,000 prize for finding a 100 million digit prime number

- The easiest way to get started is to download the Great Internet Mersenne Prime Search software and start searching.
  - https://www.mersenne.org/

# Thank you!