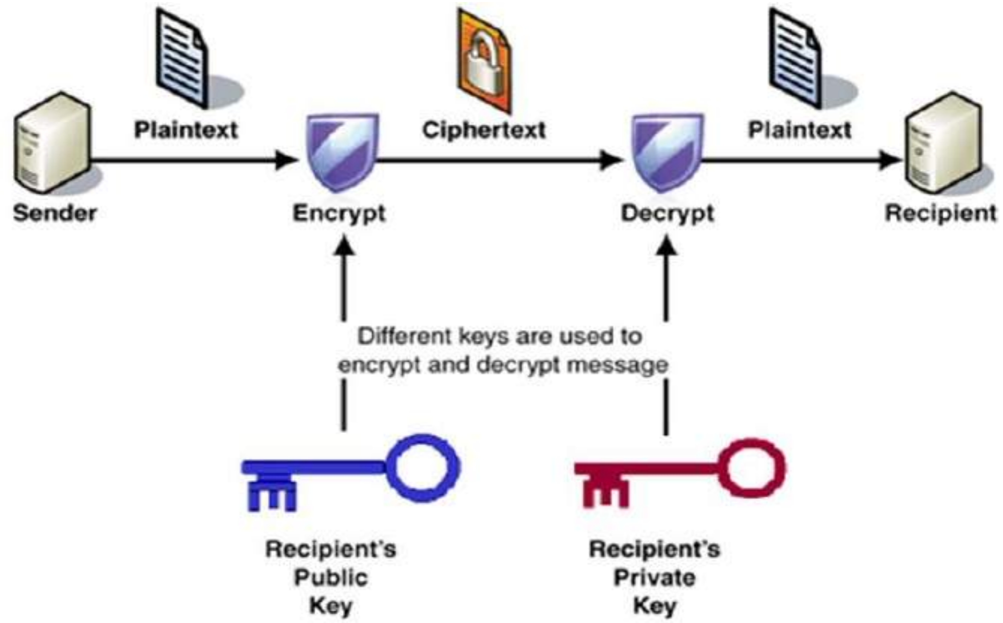
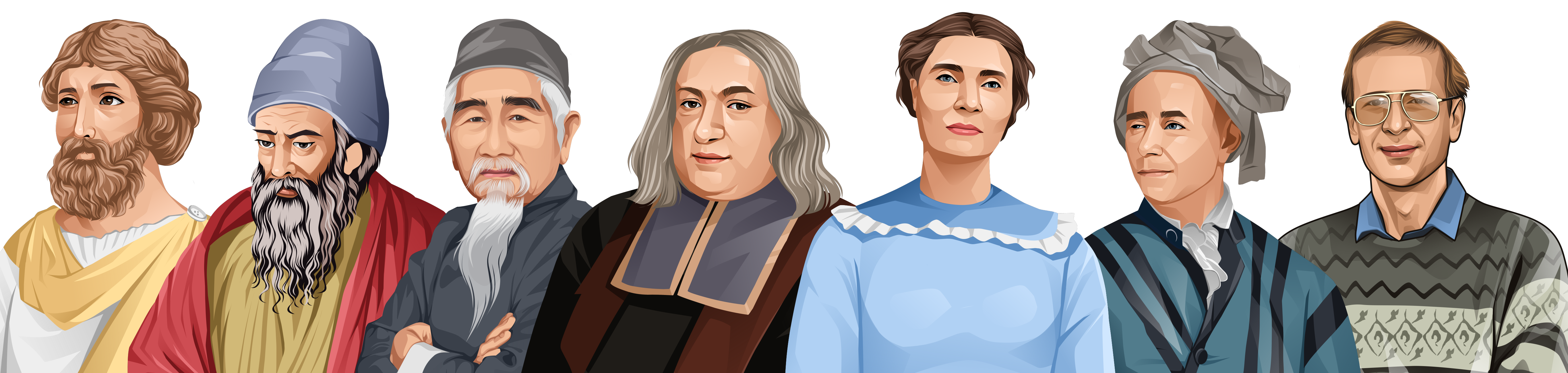


2^P-1 Great Internet Mersenne Prime Search

Finding World Record Primes Since 1996

Chapter 5: Number Theory



Back to the Pythagoreans

Back to the Pythagoreans

- Reminder: Every story about the Pythagoreans must be taken with many grains of salt. But…

Back to the Pythagoreans

- Reminder: Every story about the Pythagoreans must be taken with many grains of salt. But…
- It is said that Pythagoreans believed that numbers have mystical powers—especially integers.

Back to the Pythagoreans

- Reminder: Every story about the Pythagoreans must be taken with many grains of salt. But…

- It is said that Pythagoreans believed that numbers have mystical powers—especially integers.

- Their beliefs held that all lengths are *rational numbers.* That is, a ratio of integers.

Hippasus

Hippasus

- The most famous story about the Pythagoreans is about Hippasus.

Hippasus

- The most famous story about the Pythagoreans is about Hippasus.
- It is said that he proved that *irrational numbers* exist. In particular, he proved that $\sqrt{2}$ is irrational.

Hippasus

- The most famous story about the Pythagoreans is about Hippasus.
- It is said that he proved that *irrational numbers* exist. In particular, he proved that $\sqrt{2}$ is irrational.
- The Pythagoreans were so horrified by this that they took him out to sea and through him overboard, killing him, in order to hide the secret.

Hippasus

- The most famous story about the Pythagoreans is about Hippasus.
- It is said that he proved that *irrational numbers* exist. In particular, he proved that $\sqrt{2}$ is irrational.
- The Pythagoreans were so horrified by this that they took him out to sea and through him overboard, killing him, in order to hide the secret.
- They failed. We know the secret. And I can prove it.

Theorem: $\sqrt{2}$ is irrational

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., gcd$(b, c) = 1$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., gcd$(b, c) = 1$

- Then,

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., $\text{gcd}(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

$\implies b = 2k$ for some integer k

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

$\implies b = 2k$ for some integer k

- Thus,

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\text{gcd}(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

$$\implies b = 2k \text{ for some integer } k$$

- Thus,

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

$\implies b = 2k$ for some integer k

- Thus,

$$2c^2 = (2k)^2$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$

$$\implies 2c^2 = b^2$$

$$\implies 2 \mid b^2$$

$$\implies 2 \mid b$$

$\implies b = 2k$ for some integer k

- Thus,

$$2c^2 = (2k)^2$$

$$\implies 2c^2 = 4k^2$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies 2 \mid b$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies 2 \mid b$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$

$\implies b = 2k$ for some integer k

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

  I.e., gcd$(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies 2 \mid b$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies 2 \mid c$$

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\text{gcd}(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies 2 \mid b$$

$\implies b = 2k$ for some integer k

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies 2 \mid c$$

- We have a contradiction!

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies \boxed{2 \mid b}$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies 2 \mid c$$

- We have a contradiction!

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.

I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies \boxed{2 \mid b}$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies \boxed{2 \mid c}$$

- We have a contradiction!

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.
  I.e., $\gcd(b,c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies \boxed{2 \mid b}$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies \boxed{2 \mid c}$$

- We have a contradiction!

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms.
  I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies \boxed{2 \mid b}$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies \boxed{2 \mid c}$$

- We have a contradiction!
- We assumed $\sqrt{2} = \dfrac{b}{c}$ was written in lowest terms, and then proved it can't be.

Theorem: $\sqrt{2}$ is irrational

- **Proof.** Assume for a contradiction that $\sqrt{2}$ is rational. That is, suppose that $\sqrt{2} = b/c$ for some non-zero integers b and c, written in lowest terms. I.e., $\gcd(b, c) = 1$

- Then,

$$\sqrt{2}c = b$$
$$\implies 2c^2 = b^2$$
$$\implies 2 \mid b^2$$
$$\implies \boxed{2 \mid b}$$
$$\implies b = 2k \text{ for some integer } k$$

- Thus,

$$2c^2 = (2k)^2$$
$$\implies 2c^2 = 4k^2$$
$$\implies c^2 = 2k^2$$
$$\implies 2 \mid c^2$$
$$\implies \boxed{2 \mid c}$$

- We have a contradiction!
- We assumed $\sqrt{2} = \dfrac{b}{c}$ was written in lowest terms, and then proved it can't be.

QED

Poem on Hippasus

Hippasus

Hippasus

- The Greeks' language around this was different. They talked about numbers being *commensurable*.

Hippasus

- The Greeks' language around this was different. They talked about numbers being *commensurable*.

- Example: $\frac{1}{3}$ and $\frac{1}{4}$ are commensurable because they can bother be "measured" by $\frac{1}{12}$.

Hippasus

- The Greeks' language around this was different. They talked about numbers being *commensurable*.
- Example: $\frac{1}{3}$ and $\frac{1}{4}$ are commensurable because they can bother be "measured" by $\frac{1}{12}$.
- They hoped and believed that all pairs of numbers were commensurable.

Hippasus

- The Greeks' language around this was different. They talked about numbers being *commensurable*.
- Example: $\dfrac{1}{3}$ and $\dfrac{1}{4}$ are commensurable because they can bother be "measured" by $\dfrac{1}{12}$.
- They hoped and believed that all pairs of numbers were commensurable.
- Hippasus showed 1 and $\sqrt{2}$ are incommensurable.

Perfect Numbers

Perfect Numbers

- **Definition.** The *proper divisors* of a number N are the positive numbers less than N that divide N.

Perfect Numbers

- **Definition.** The *proper divisors* of a number N are the positive numbers less than N that divide N.
- Example: The proper divisors of 10 are 1, 2, and 5.

Perfect Numbers

- **Definition.** The *proper divisors* of a number N are the positive numbers less than N that divide N.
- Example: The proper divisors of 10 are 1, 2, and 5.
- Example: The proper divisors of 12 are 1, 2, 3, 4 and 6.

Perfect Numbers

- **Definition.** The *proper divisors* of a number N are the positive numbers less than N that divide N.

- Example: The proper divisors of 10 are 1, 2, and 5.

- Example: The proper divisors of 12 are 1, 2, 3, 4 and 6.

- **Definition.** A number N to be *perfect* if N's proper divisors sum to N.

Challenge: Try to find a perfect number

Perfect Numbers

Perfect Numbers

- **Example.** 6 is a perfect number. Its proper divisors are 1, 2 and 3, and 1+2+3=6.

Perfect Numbers

- **Example.** 6 is a perfect number. Its proper divisors are 1, 2 and 3, and 1+2+3=6.

- **Non-Example.** 20 is not a perfect number. Its proper divisors are 1, 2, 4, 5 and 10, and 1+2+4+5+10=22.

Perfect Numbers

- **Example.** 6 is a perfect number. Its proper divisors are 1, 2 and 3, and 1+2+3=6.

- **Non-Example.** 20 is not a perfect number. Its proper divisors are 1, 2, 4, 5 and 10, and 1+2+4+5+10=22.

- **Example.** 28 is a perfect number. Its proper divisors are 1, 2, 4, 7 and 14, and 1+2+4+7+14=28.

Perfect Numbers

- **Example.** 6 is a perfect number. Its proper divisors are 1, 2 and 3, and 1+2+3=6.

- **Non-Example.** 20 is not a perfect number. Its proper divisors are 1, 2, 4, 5 and 10, and 1+2+4+5+10=22.

- **Example.** 28 is a perfect number. Its proper divisors are 1, 2, 4, 7 and 14, and 1+2+4+7+14=28.

- Perfect numbers may have originated with the Pythagoreans.

Perfect Numbers

Perfect Numbers

- Euclid included them in *Elements*, and in Proposition IX.36 he proved this:

  If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

Perfect Numbers

- Euclid included them in *Elements*, and in Proposition IX.36 he proved this:

  If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

- **Example.** If $n = 2$, then $2^n - 1 = 3$ is prime, and so $2^{n-1}(2^n - 1) = 2(4 - 1) = 6$ is perfect.

Perfect Numbers

- Euclid included them in *Elements*, and in Proposition IX.36 he proved this:

  If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

- **Example.** If $n = 2$, then $2^n - 1 = 3$ is prime, and so $2^{n-1}(2^n - 1) = 2(4 - 1) = 6$ is perfect.

- **Example.** If $n = 3$, then $2^n - 1 = 7$ is prime, and so $2^{n-1}(2^n - 1) = 4(8 - 1) = 28$ is perfect.

Perfect Numbers

Perfect Numbers

- **Proposition IX.36.** If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

Perfect Numbers

- **Proposition IX.36.** If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

- **Proof.** Since $2^n - 1$ is prime, the only primes that divide $2^{n-1}(2^n - 1)$ are 2 and $2^n - 1$.

Perfect Numbers

- **Proposition IX.36.** If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is a perfect number.

- **Proof.** Since $2^n - 1$ is prime, the only primes that divide $2^{n-1}(2^n - 1)$ are 2 and $2^n - 1$.

- And the only proper divisors of $2^{n-1}(2^n - 1)$ are
$1 \ , \ 2 \ , \ 2^2 \ , \ 2^3 \ , \ \ldots \ , \ 2^{n-1}$
and
$2^n - 1 \ , \ 2(2^n - 1) \ , \ 2^2(2^n - 1) \ , \ \ldots \ , \ 2^{n-2}(2^n - 1) \ .$

Perfect Numbers

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$

and

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$

and

$$(2^n - 1) + 2(2^n - 1) + 2^2(2^n - 1) + \ldots + 2^{n-2}(2^n - 1)$$

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$

and

$$(2^n - 1) + 2(2^n - 1) + 2^2(2^n - 1) + \ldots + 2^{n-2}(2^n - 1)$$

$$= (2^n - 1)(1 + 2 + 2^2 + \ldots + 2^{n-2})$$

Perfect Numbers

- To check if $2^{n-1}(2^n - 1)$ is perfect, we must sum its proper divisors to see if the sum equals $2^{n-1}(2^n - 1)$. Using the geometric sum formula:

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$

and

$$(2^n - 1) + 2(2^n - 1) + 2^2(2^n - 1) + \ldots + 2^{n-2}(2^n - 1)$$

$$= (2^n - 1)(1 + 2 + 2^2 + \ldots + 2^{n-2})$$

$$= (2^n - 1)(2^{n-1} - 1)\,.$$

Perfect Numbers

Perfect Numbers

- Thus, the total sum is

$$(2^n - 1) + (2^n - 1)(2^{n-1} - 1)$$

Perfect Numbers

- Thus, the total sum is

$$(2^n - 1) + (2^n - 1)(2^{n-1} - 1)$$
$$= (2^n - 1) + (2^n - 1)2^{n-1} - (2^n - 1)$$

Perfect Numbers

- Thus, the total sum is

$$\begin{aligned}(2^n - 1) &+ (2^n - 1)(2^{n-1} - 1)\\ &= (2^n - 1) + (2^n - 1)2^{n-1} - (2^n - 1)\\ &= 2^{n-1}(2^n - 1)\,.\end{aligned}$$

Perfect Numbers

- Thus, the total sum is

$$\begin{aligned}(2^n - 1) &+ (2^n - 1)(2^{n-1} - 1) \\ &= (2^n - 1) + (2^n - 1)2^{n-1} - (2^n - 1) \\ &= 2^{n-1}(2^n - 1)\,.\end{aligned}$$

- Since the proper divisors of $2^{n-1}(2^n - 1)$ sum to $2^{n-1}(2^n - 1)$, this means that $2^{n-1}(2^n - 1)$ is a perfect number.

Perfect Numbers

- Thus, the total sum is

$$
\begin{aligned}
&(2^n - 1) + (2^n - 1)(2^{n-1} - 1) \\
&\qquad = (2^n - 1) + (2^n - 1)2^{n-1} - (2^n - 1) \\
&\qquad = 2^{n-1}(2^n - 1)\,.
\end{aligned}
$$

- Since the proper divisors of $2^{n-1}(2^n - 1)$ sum to $2^{n-1}(2^n - 1)$, this means that $2^{n-1}(2^n - 1)$ is a perfect number.

Q.E.D.

Perfect Numbers

Perfect Numbers

- Centuries later, Leonhard Euler proved the converse:

  If $2^{n-1}(2^n - 1)$ is a perfect number, then $2^n - 1$ is a prime number.

Perfect Numbers

- Centuries later, Leonhard Euler proved the converse:

  If $2^{n-1}(2^n - 1)$ is a perfect number, then $2^n - 1$ is a prime number.

- Primes of the form $2^n - 1$ are called *Mersenne primes* and most of the biggest primes we know are Mersenne primes.

2^P-1 Great Internet Mersenne Prime Search

Finding World Record Primes Since 1996

Perfect Numbers

- Centuries later, Leonhard Euler proved the converse:

  If $2^{n-1}(2^n - 1)$ is a perfect number, then $2^n - 1$ is a prime number.

- Primes of the form $2^n - 1$ are called *Mersenne primes* and most of the biggest primes we know are Mersenne primes.

- Largest known prime (Feb 2023) is $2^{82,589,933} - 1$.

2^P-1 Great Internet Mersenne Prime Search

Finding World Record Primes Since 1996

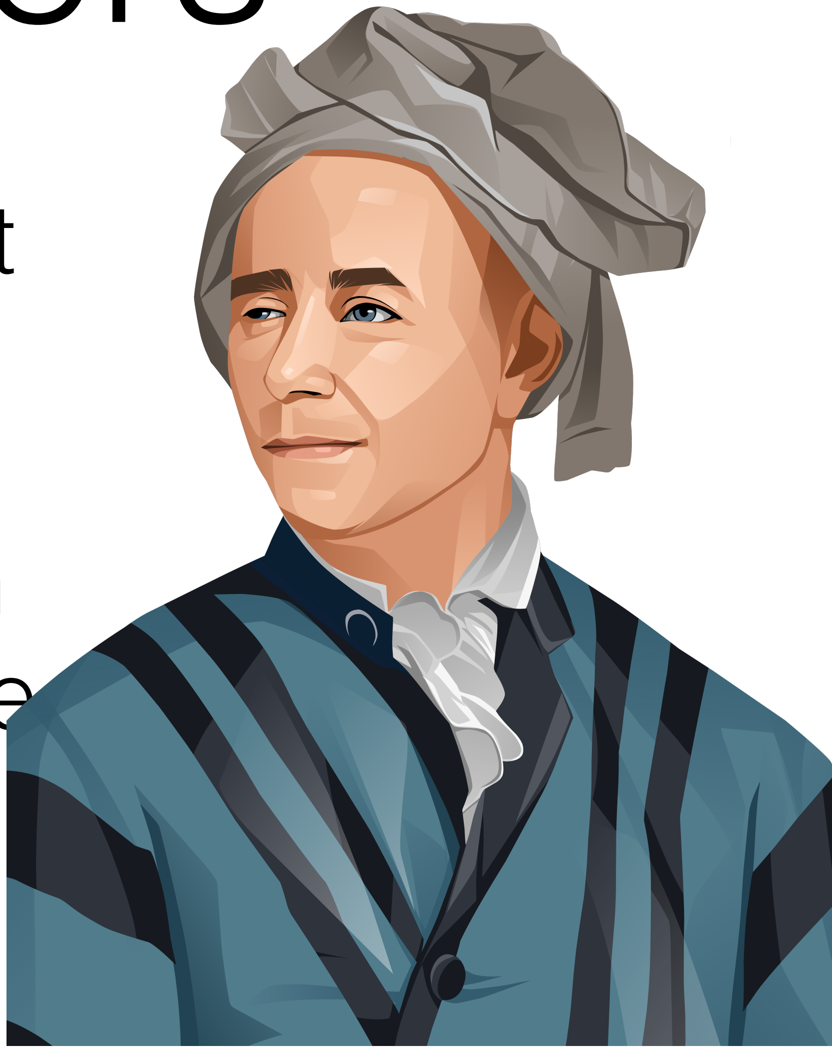
Perfect Numbers

Perfect Numbers

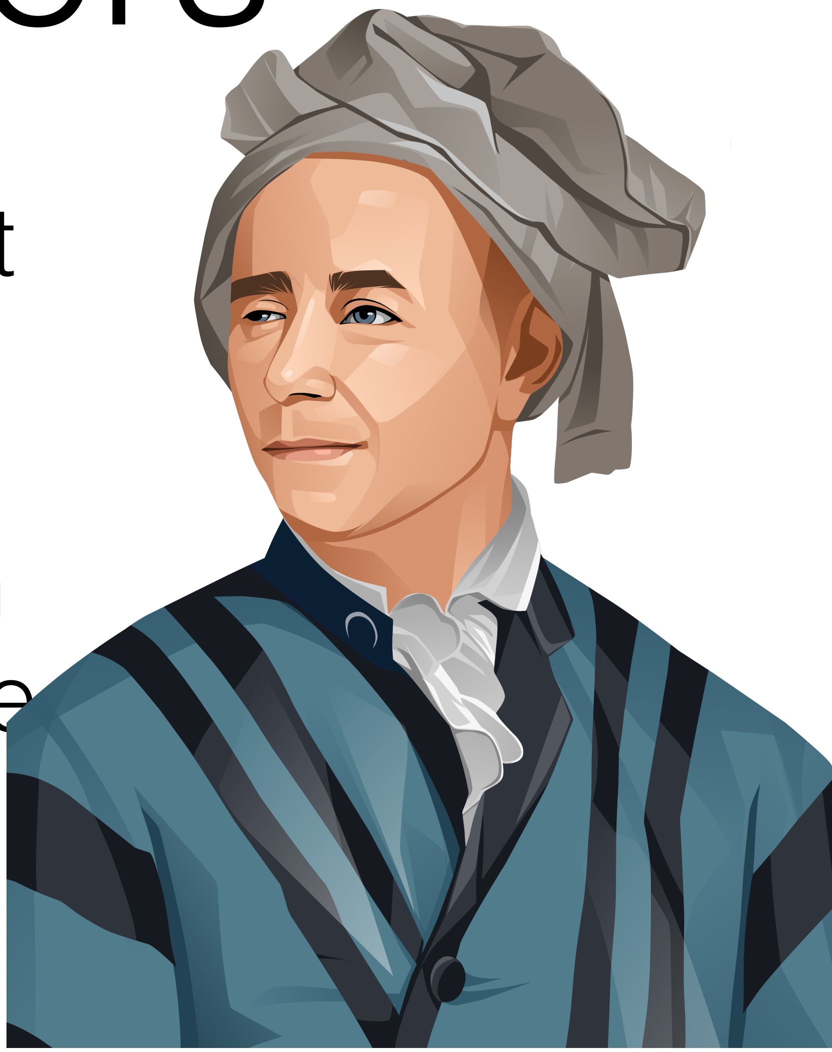
- The Greeks knew the first four perfect numbers (6, 28, 496 and 8128).

Perfect Numbers

- The Greeks knew the first four perfect numbers (6, 28, 496 and 8128).
- 13th-century Egyptian mathematician Ismail ibn Ibrahim ibn Fallus found the next three (33550336, 8589869056 and 137438691328).



Perfect Numbers

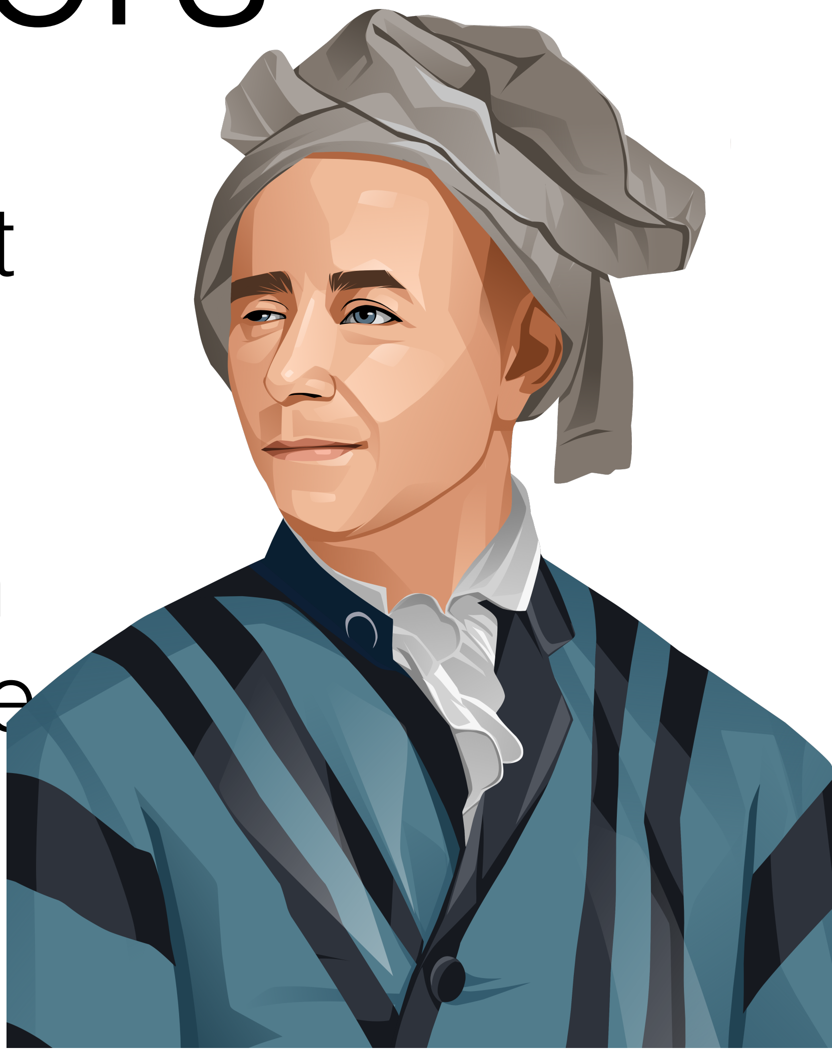


- The Greeks knew the first four perfect numbers (6, 28, 496 and 8128).

- 13th-century Egyptian mathematician Ismail ibn Ibrahim ibn Fallus found the next three (33550336, 8589869056 and 137438691328).

- In 1772, Leonhard Euler found the next one (2305843008139952128).

Perfect Numbers



- The Greeks knew the first four perfect numbers (6, 28, 496 and 8128).
- 13th-century Egyptian mathematician Ismail ibn Ibrahim ibn Fallus found the next three (33550336, 8589869056 and 137438691328).
- In 1772, Leonhard Euler found the next one (2305843008139952128).
- Today, 51 are known.

Perfect Numbers

<u>**Open questions:**</u>

Perfect Numbers

Open questions:

- Are there infinitely many perfect numbers?

Perfect Numbers

Open questions:

- Are there infinitely many perfect numbers?
- Is there an odd perfect number?

Perfect Numbers

Open questions:

- Are there infinitely many perfect numbers?
- Is there an odd perfect number?
- Are there infinitely many Mersenne primes?

The Aftermath: Fermat’s Little Theorem

The Aftermath: Fermat's Little Theorem

- While studying perfect numbers, Fermat proved what today is called *Fermat's little theorem*. It says:

  If p is a prime and a is an integer not divisible by p, then p divides $a^{p-1} - 1$.

The Aftermath: Fermat's Little Theorem

- While studying perfect numbers, Fermat proved what today is called *Fermat's little theorem*. It says:

  If p is a prime and a is an integer not divisible by p, then p divides $a^{p-1} - 1$.

- This is very important in number theory, including in public key cryptography.

Pierre de Fermat

Pierre de Fermat

- Fermat was the great “amateur” mathematician. Professionally, he was a lawyer and government official.

Pierre de Fermat

- Fermat was the great “amateur” mathematician. Professionally, he was a lawyer and government official.
- Born in 1601, lived his whole life in France.

Pierre de Fermat

- Fermat was the great “amateur” mathematician. Professionally, he was a lawyer and government official.
- Born in 1601, lived his whole life in France.
- He is one of the great number theorists in history.

Pierre de Fermat

- Fermat was the great “amateur” mathematician. Professionally, he was a lawyer and government official.
- Born in 1601, lived his whole life in France.
- He is one of the great number theorists in history.
- He rarely published but was well-known in math circles. He communicated via letter with top mathematicians. He often withheld his proofs.

RSA Cryptosystem

RSA Cryptosystem

Amicable Numbers

Amicable Numbers

- x and y are amicable if x's divisors sum to y and y's divisors sum to x.

Amicable Numbers

- x and y are amicable if x's divisors sum to y and y's divisors sum to x.
- Pythagoreans discovered the first pair: 220 and 284.

Amicable Numbers

- x and y are amicable if x's divisors sum to y and y's divisors sum to x.
- Pythagoreans discovered the first pair: 220 and 284.
- In the 1300s, Ibn al-Banna discovered the next pair: 17,296 and 18,416.

Amicable Numbers

- x and y are amicable if x's divisors sum to y and y's divisors sum to x.
- Pythagoreans discovered the first pair: 220 and 284.
- In the 1300s, Ibn al-Banna discovered the next pair: 17,296 and 18,416.
- The third pair is 9,363,584 and 9,437,056. There is wide dispute over who deserves credit.

Amicable Numbers

- x and y are amicable if x's divisors sum to y and y's divisors sum to x.
- Pythagoreans discovered the first pair: 220 and 284.
- In the 1300s, Ibn al-Banna discovered the next pair: 17,296 and 18,416.
- The third pair is 9,363,584 and 9,437,056. There is wide dispute over who deserves credit.
- In the 1700s, Euler discovered the next 58 pairs (!!)

Primes

Primes

- **Proposition VII.31** from Euclid's *Elements*:

Primes

- **Proposition VII.31** from Euclid's *Elements*:

$$\boxed{\text{Any composite number is divisible by some prime number}}$$

Primes

- **Proposition VII.31** from Euclid's *Elements*:

  Any composite number is divisible by some prime number

- **Proof.** Let N be a composite number. That is, it is a positive integer with some divisor, call it d_1. If d_1 is prime, then we are done!

Primes

- **Proposition VII.31** from Euclid's *Elements*:

  $\boxed{\text{Any composite number is divisible by some prime number}}$

- **Proof.** Let N be a composite number. That is, it is a positive integer with some divisor, call it d_1. If d_1 is prime, then we are done!

- If not, then d_1 is composite, meaning it has some divisor, call it d_2. If d_2 is prime, done! Otherwise… (repeat)

Primes

- **Proposition VII.31** from Euclid's *Elements*:

  $$\boxed{\text{Any composite number is divisible by some prime number}}$$

- **Proof.** Let N be a composite number. That is, it is a positive integer with some divisor, call it d_1. If d_1 is prime, then we are done!

- If not, then d_1 is composite, meaning it has some divisor, call it d_2. If d_2 is prime, done! Otherwise… (repeat)

- This process will eventually find a prime, because otherwise we get the infinite sequence $N > d_1 > d_2 > d_3 > \ldots > 1$, which is impossible.

Primes

- **Proposition VII.31** from Euclid's *Elements*:

  Any composite number is divisible by some prime number

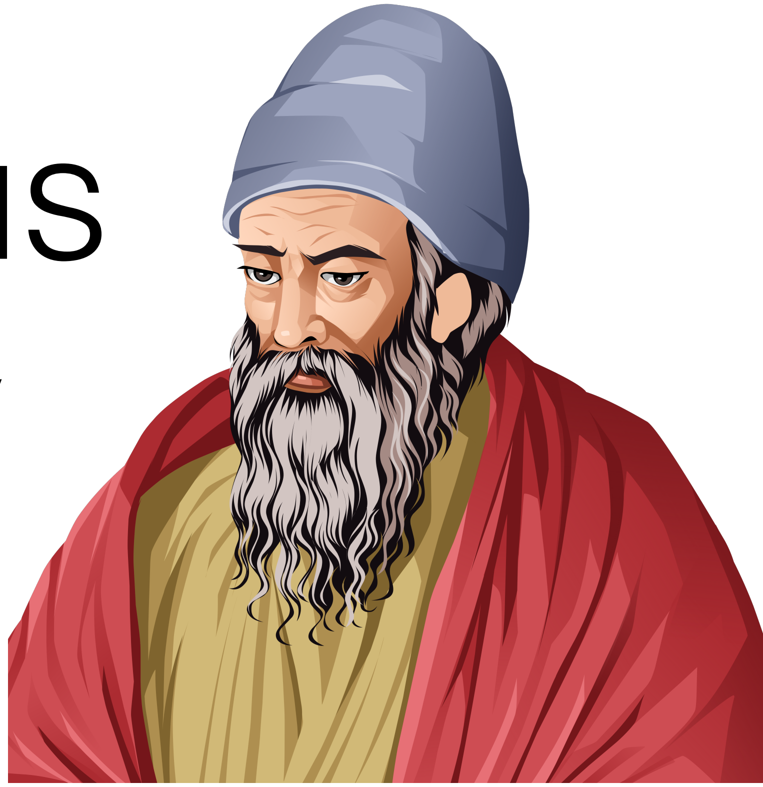
- **Proof.** Let N be a composite number. That is, it is a positive integer with some divisor, call it d_1. If d_1 is prime, then we are done!

- If not, then d_1 is composite, meaning it has some divisor, call it d_2. If d_2 is prime, done! Otherwise… (repeat)

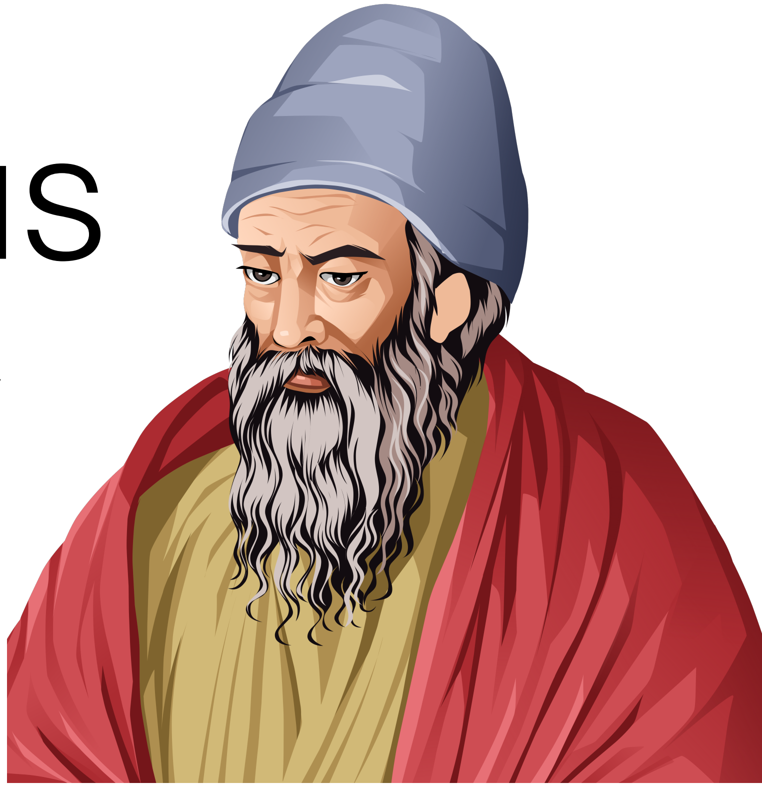
- This process will eventually find a prime, because otherwise we get the infinite sequence $N > d_1 > d_2 > d_3 > \ldots > 1$, which is impossible.

Q.E.D.

The Most Famous Proof in History

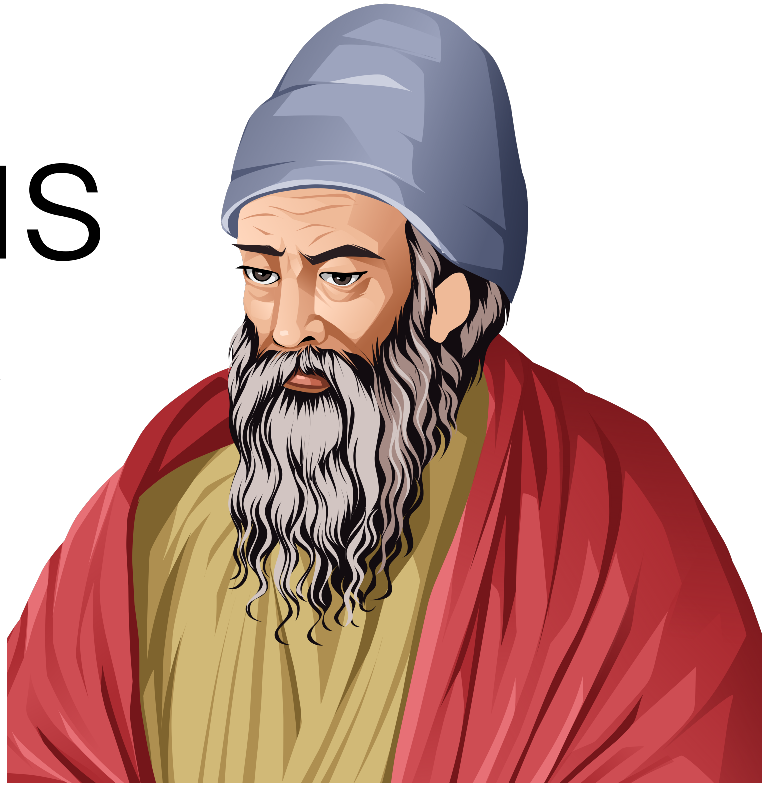


The Most Famous Proof in History



- **Proposition IX.20** from *Elements*:

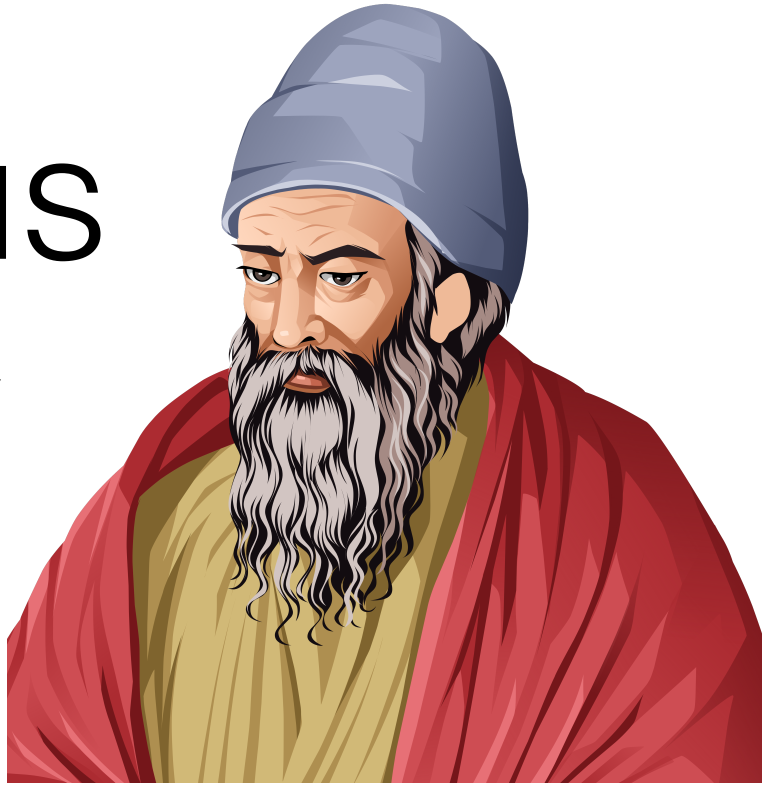
The Most Famous Proof in History



- **Proposition IX.20** from *Elements*:

There are infinitely many primes.

The Most Famous Proof in History

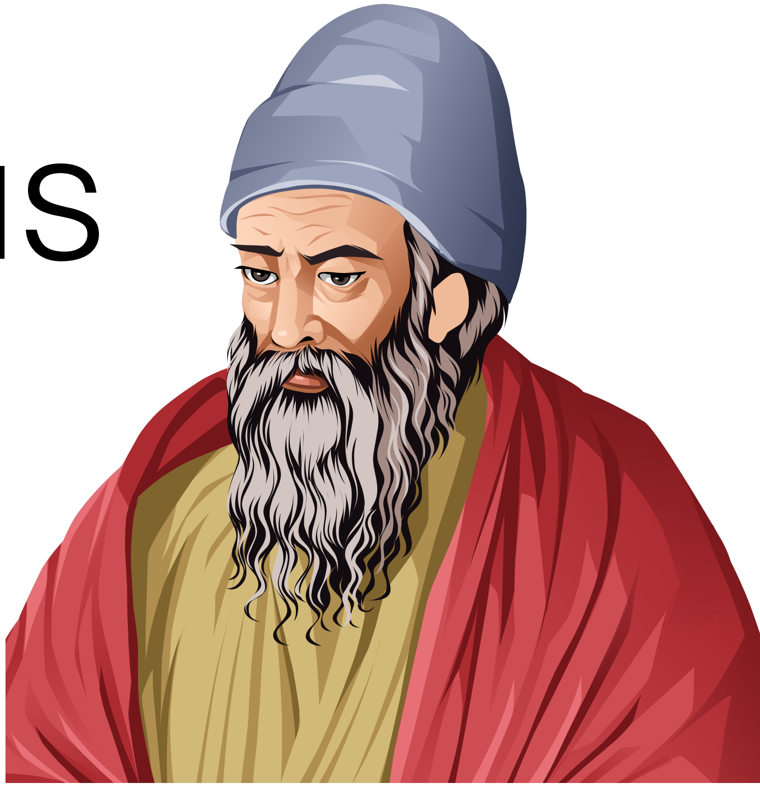


- **Proposition IX.20** from *Elements*:

  There are infinitely many primes.

- **Proof.** Given any final collection of primes, consider $N = p_1 p_2 p_3 \cdots p_k$. Now consider $N + 1$.

The Most Famous Proof in History



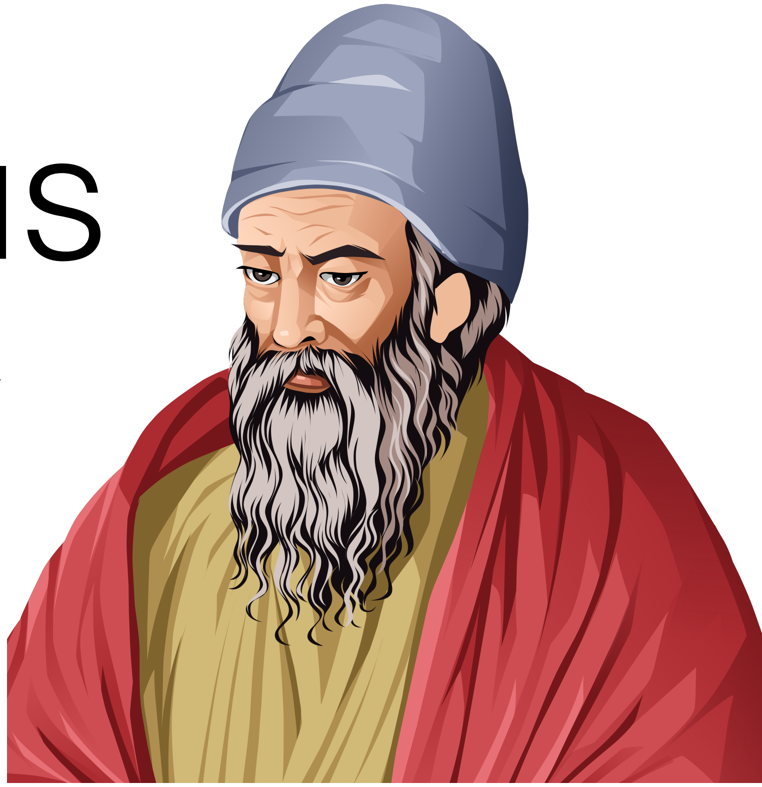
- **Proposition IX.20** from *Elements*:

  $\boxed{\text{There are infinitely many primes.}}$

- **Proof.** Given any final collection of primes, consider $N = p_1 p_2 p_3 \cdots p_k$. Now consider $N + 1$.

- <u>Case 1: $N + 1$ is prime.</u> Then it must be a new prime because it is larger than all the p_i.

The Most Famous Proof in History



- **Proposition IX.20** from *Elements*:

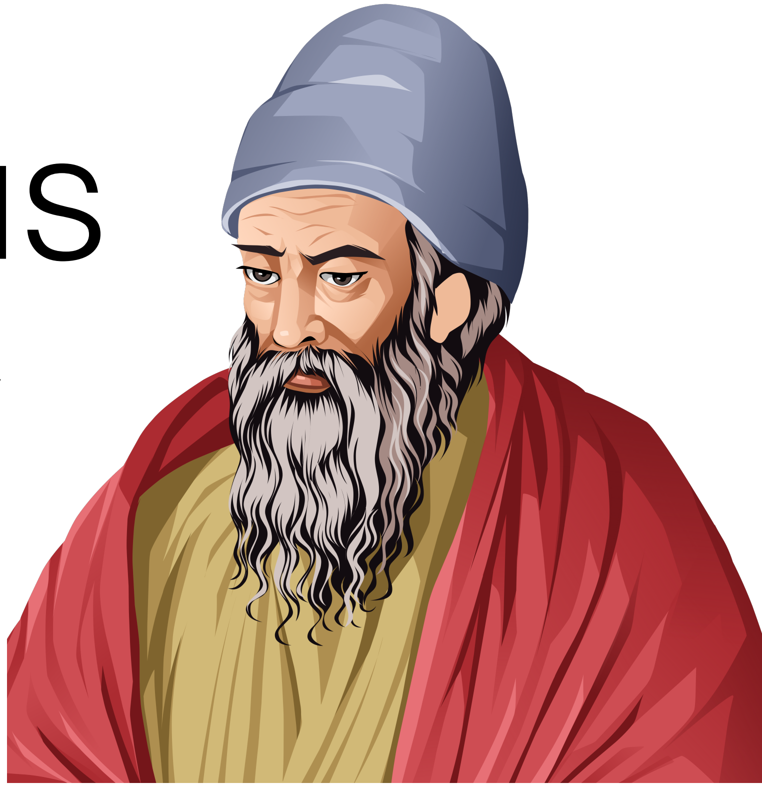
  There are infinitely many primes.

- **Proof.** Given any final collection of primes, consider $N = p_1 p_2 p_3 \cdots p_k$. Now consider $N + 1$.

- <u>Case 1: $N+1$ is prime.</u> Then it must be a new prime because it is larger than all the p_i.

- <u>Case 2: $N+1$ is composite.</u> Then by Proposition IX.20, it is divisible by a prime p. This must be a new prime since if it divides $N+1$ and N, then it would also divide $(N+1) - N = 1$, but no primes divide 1.

The Most Famous Proof in History



- **Proposition IX.20** from *Elements*:

  There are infinitely many primes.

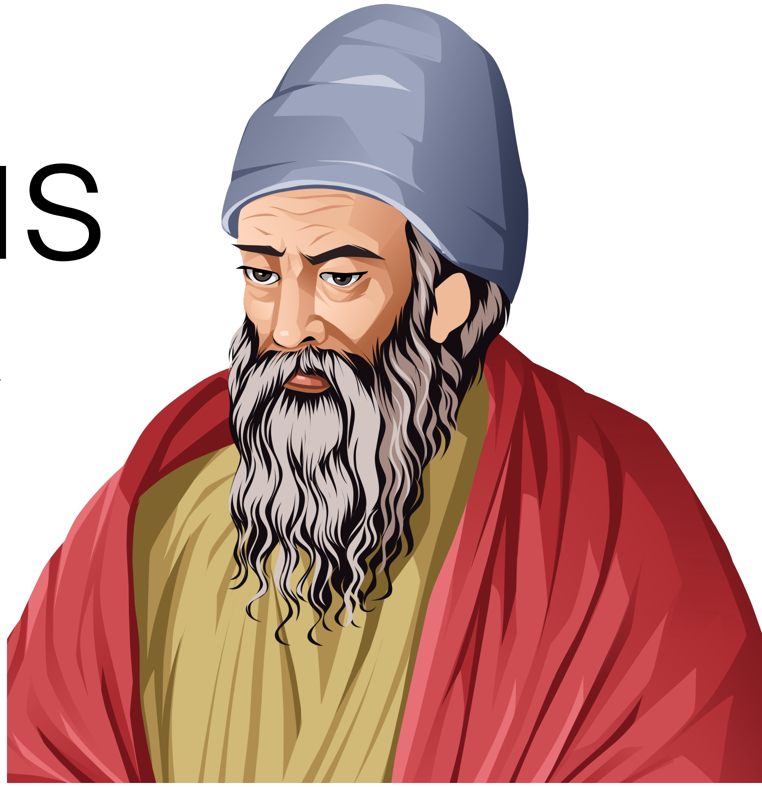
- **Proof.** Given any final collection of primes, consider $N = p_1 p_2 p_3 \cdots p_k$. Now consider $N+1$.

- <u>Case 1: $N+1$ is prime.</u> Then it must be a new prime because it is larger than all the p_i.

- <u>Case 2: $N+1$ is composite.</u> Then by Proposition IX.20, it is divisible by a prime p. This must be a new prime since if it divides $N+1$ and N, then it would also divide $(N+1) - N = 1$, but no primes divide 1.

- Thus, no collection of primes is complete, implying there are infinitely many primes.

The Most Famous Proof in History



- **Proposition IX.20** from *Elements*:

  There are infinitely many primes.

- **Proof.** Given any final collection of primes, consider $N = p_1 p_2 p_3 \cdots p_k$. Now consider $N + 1$.

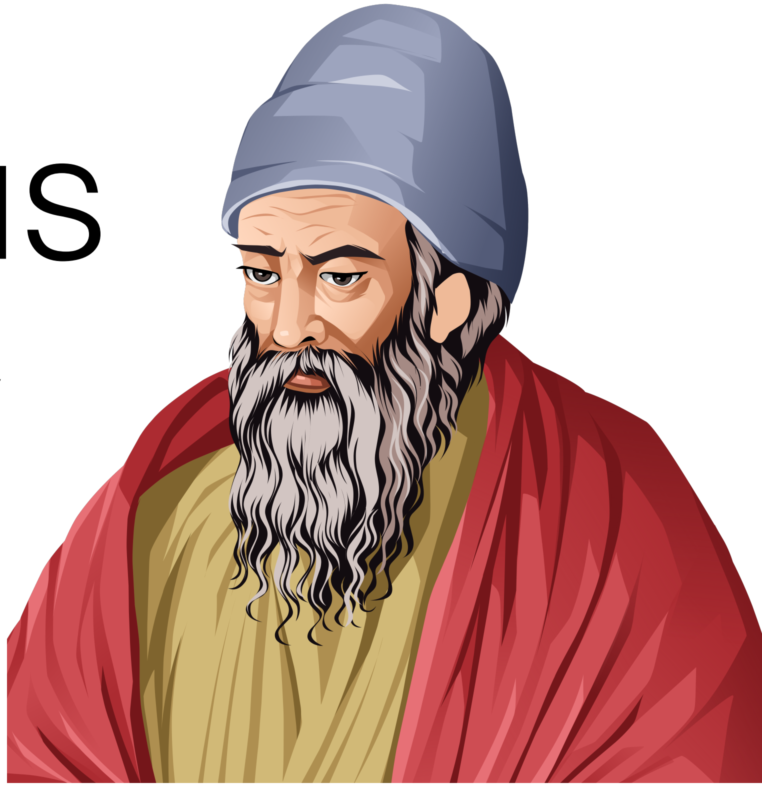
- Case 1: $N+1$ is prime. Then it must be a new prime because it is larger than all the p_i.

- Case 2: $N+1$ is composite. Then by Proposition IX.20, it is divisible by a prime p. This must be a new prime since if it divides $N+1$ and N, then it would also divide $(N+1) - N = 1$, but no primes divide 1.

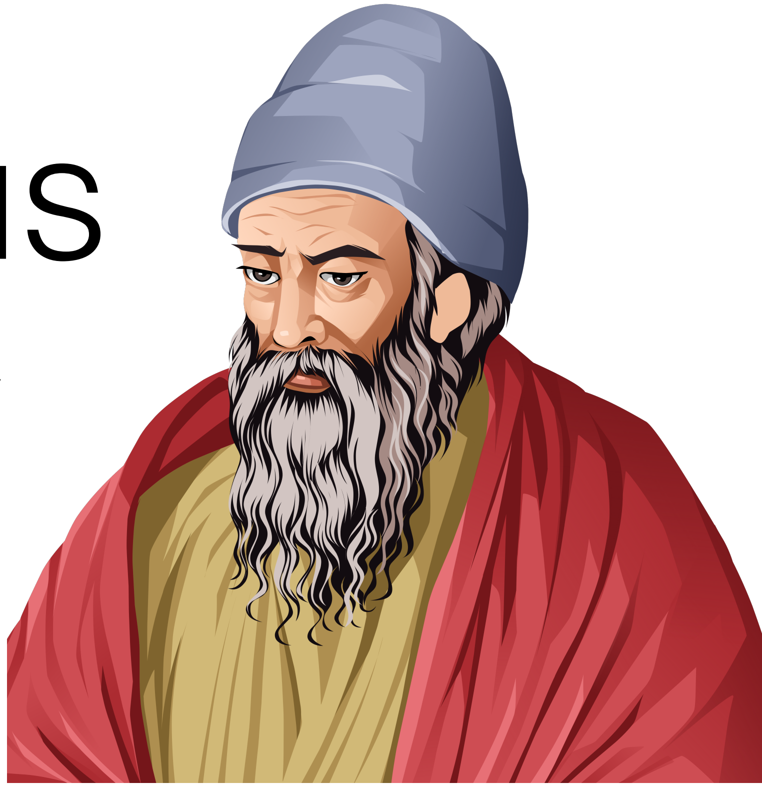
- Thus, no collection of primes is complete, implying there are infinitely many primes.

Q.E.D.

The Most Famous Proof in History

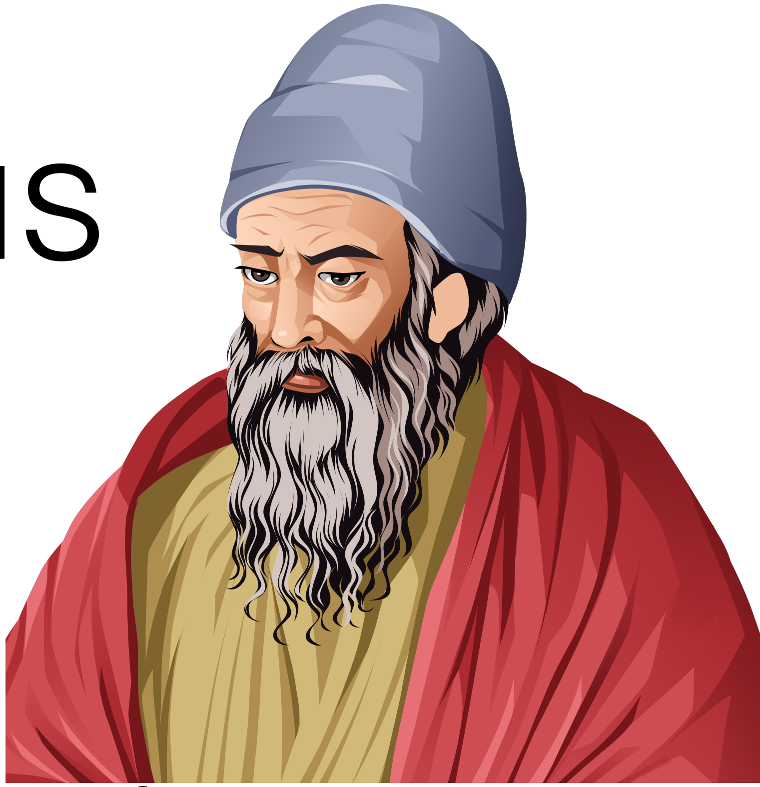


The Most Famous Proof in History



- Today's interpretation:

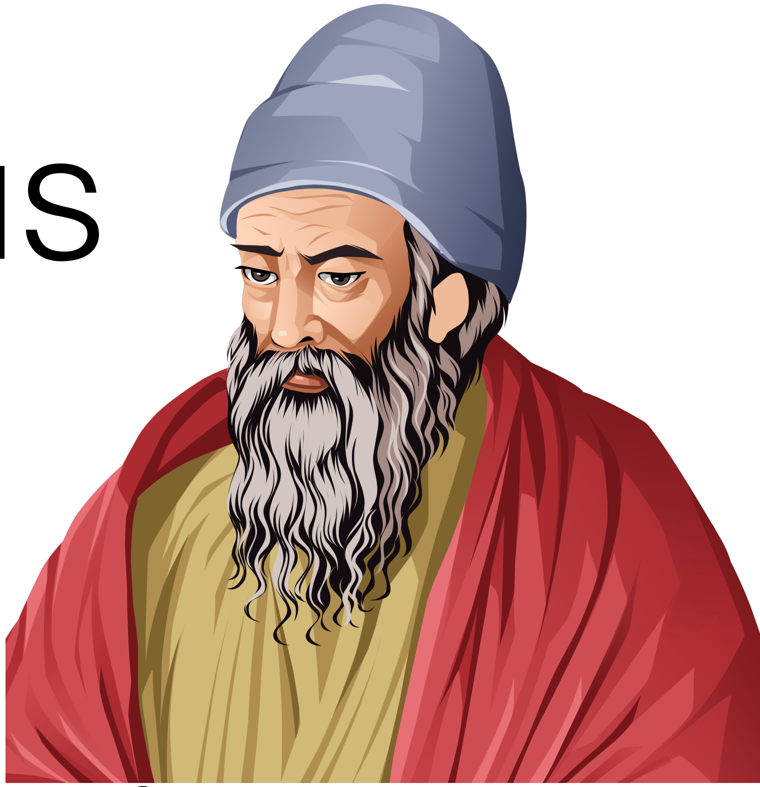
The Most Famous Proof in History



- Today's interpretation:

- Assume for a contradiction there are only finitely many primes. Call them $p_1, p_2, p_3, \ldots, p_k$.

The Most Famous Proof in History

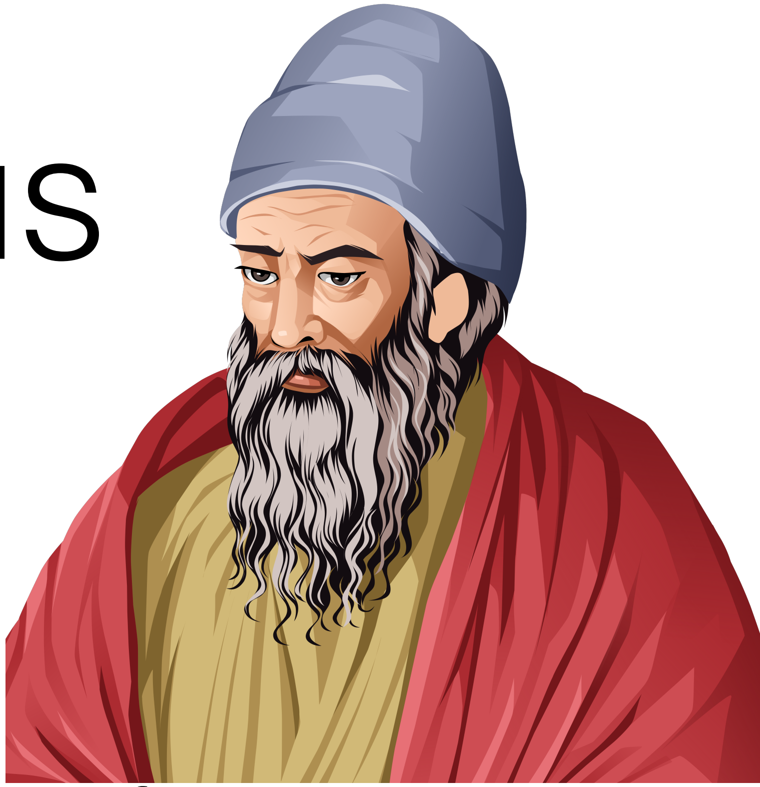


- Today's interpretation:

- Assume for a contradiction there are only finitely many primes. Call them $p_1, p_2, p_3, \ldots, p_k$.

- Consider $N = p_1 p_2 p_3 \ldots p_k$.

The Most Famous Proof in History



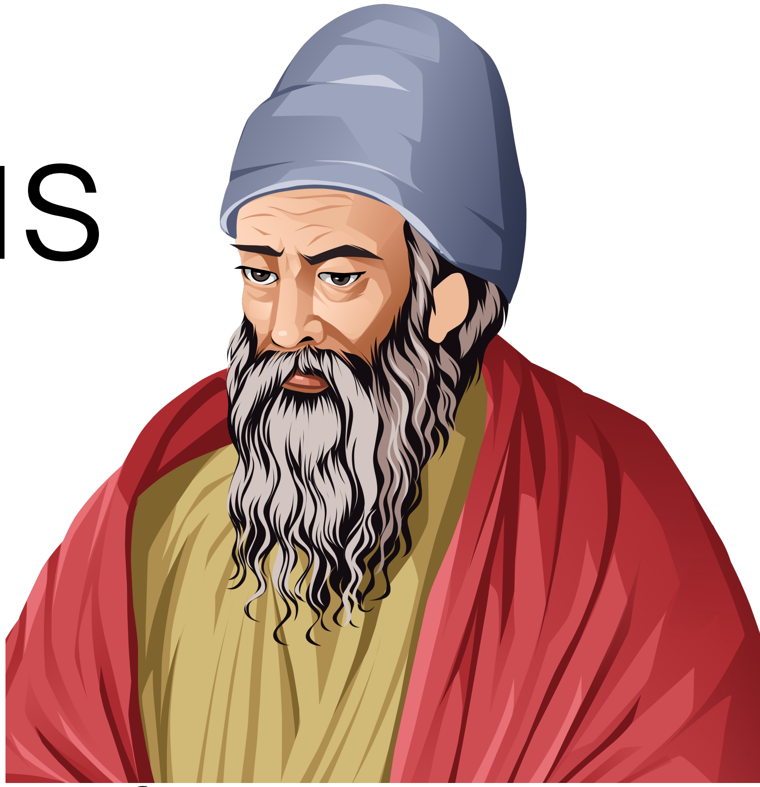
- Today's interpretation:

- Assume for a contradiction there are only finitely many primes. Call them $p_1, p_2, p_3, \ldots, p_k$.

- Consider $N = p_1 p_2 p_3 \ldots p_k$.

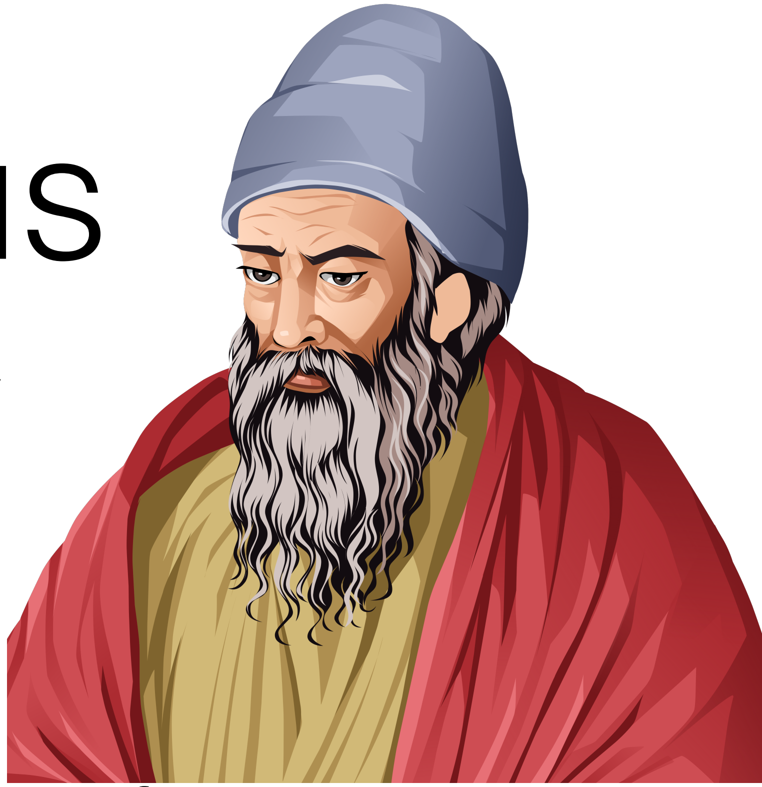
- Every prime divides N, so no prime divides $N + 1$.

The Most Famous Proof in History



- Today's interpretation:
- Assume for a contradiction there are only finitely many primes. Call them $p_1, p_2, p_3, \ldots, p_k$.
- Consider $N = p_1 p_2 p_3 \ldots p_k$.
- Every prime divides N, so no prime divides $N + 1$.
- But every integer is a product of primes. This gives the contradiction.

The Most Famous Proof in History



- Today's interpretation:

- Assume for a contradiction there are only finitely many primes. Call them $p_1, p_2, p_3, \ldots, p_k$.

- Consider $N = p_1 p_2 p_3 \ldots p_k$.

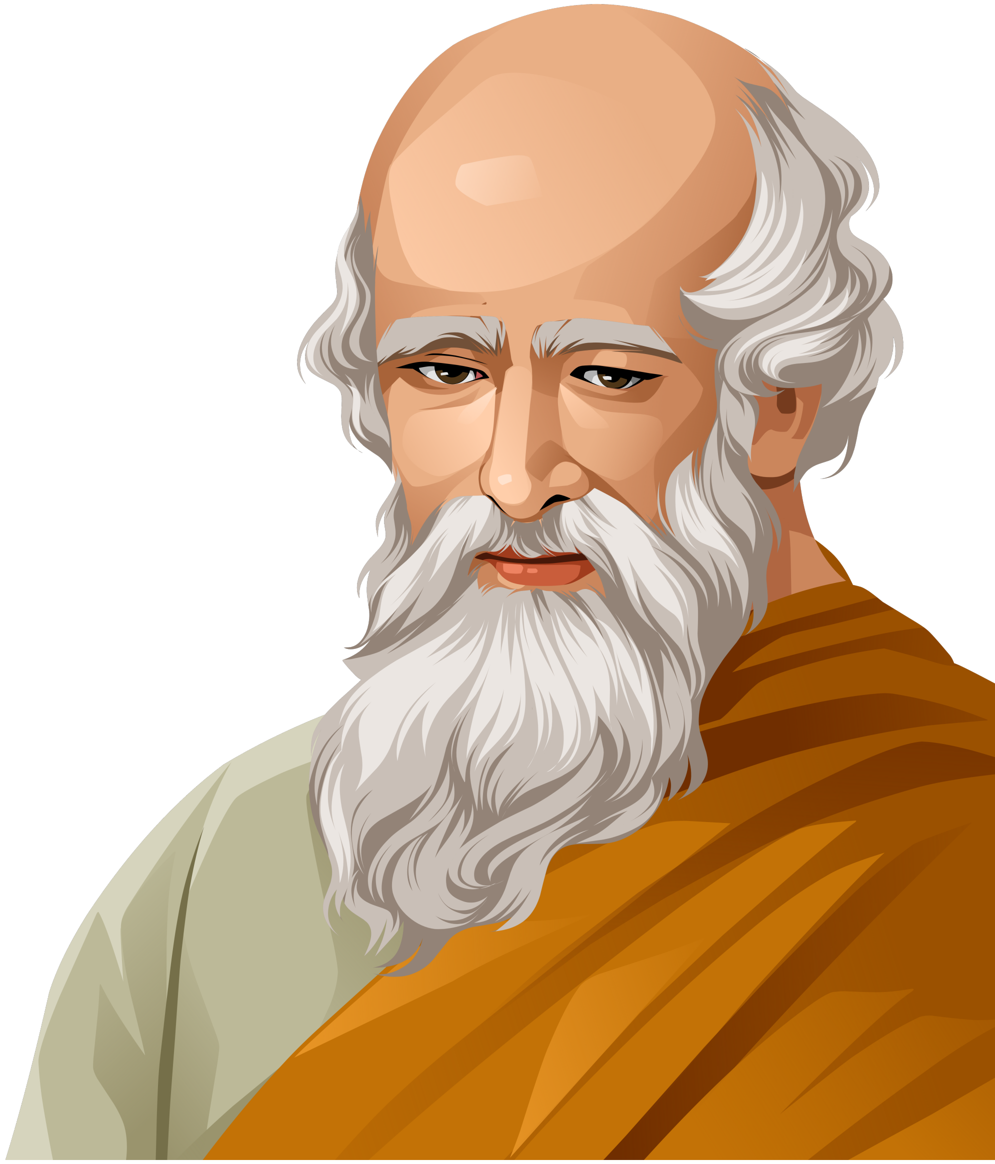
- Every prime divides N, so no prime divides $N + 1$.

- But every integer is a product of primes. This gives the contradiction.

Q.E.D.

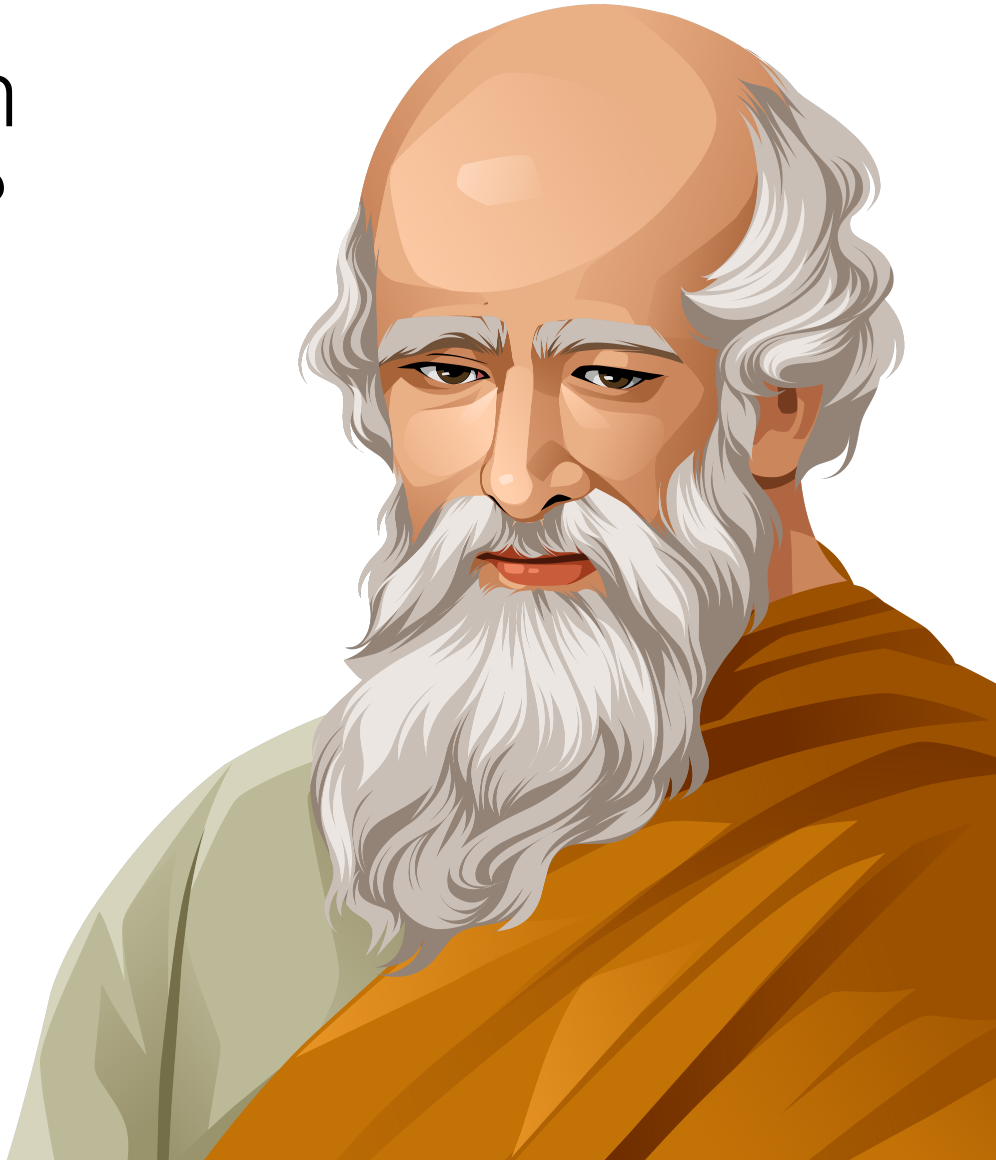
Euclid Poem

Where’s Archimedes?



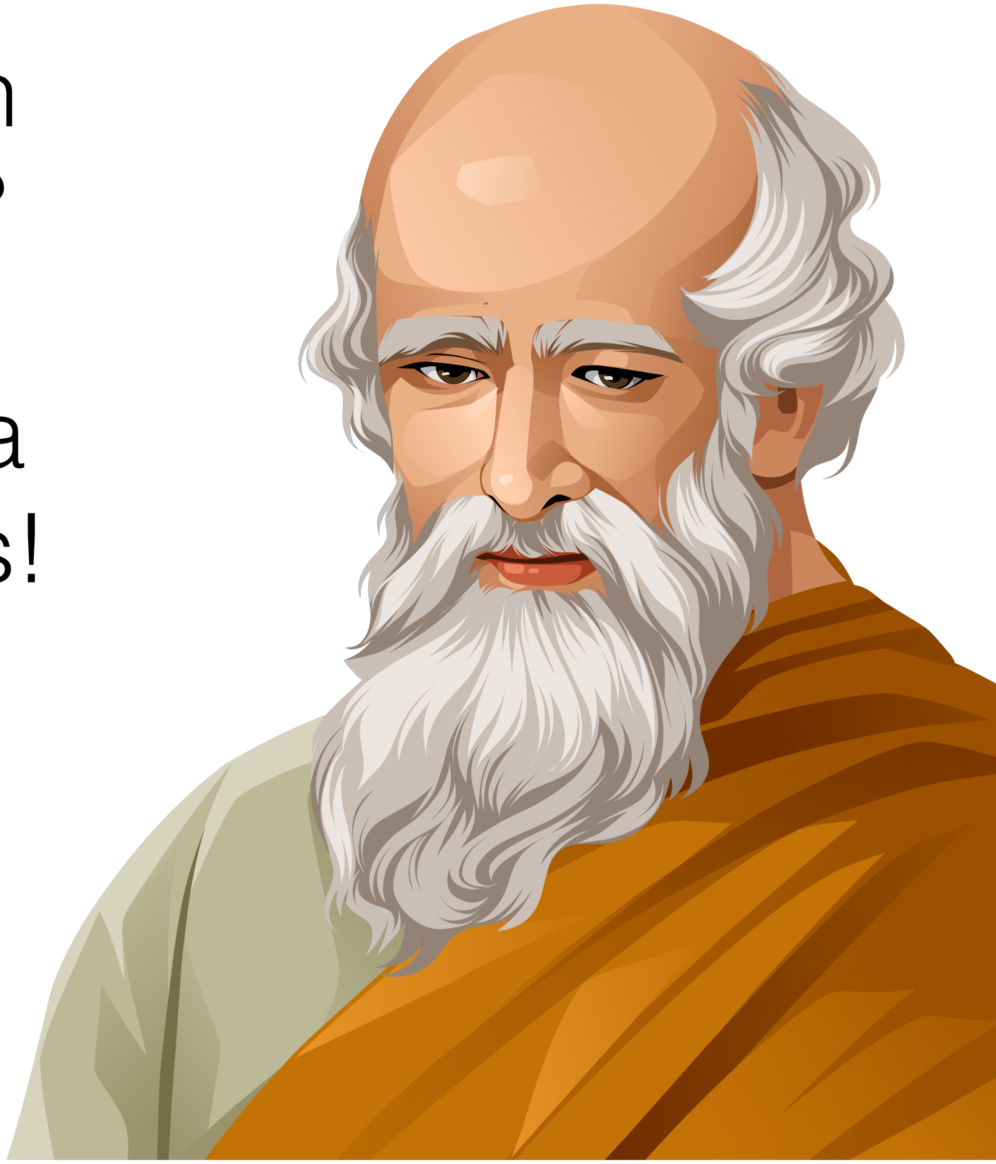
Where’s Archimedes?

- Most people end Greek math with Euclid. But where is Archimedes?



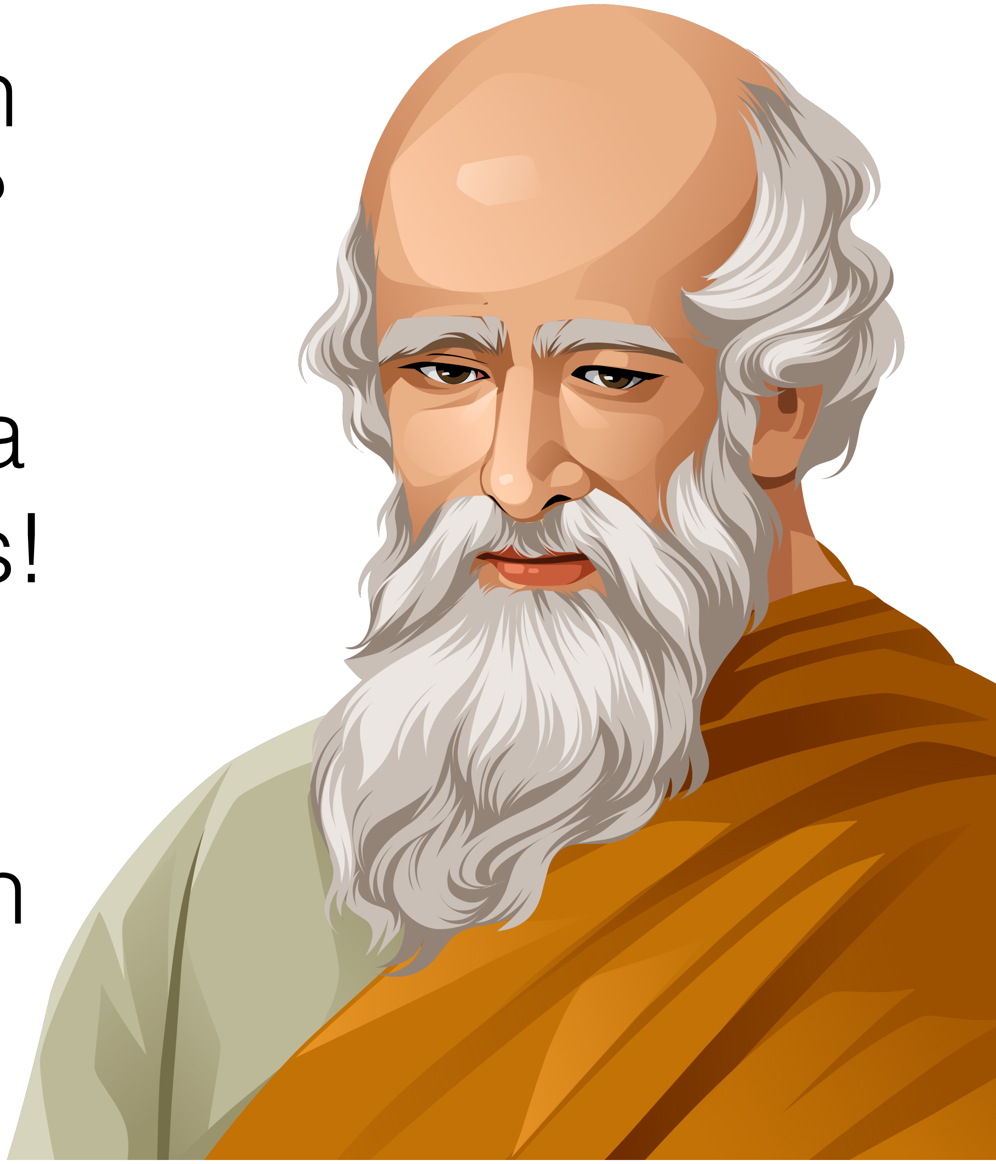
Where's Archimedes?

- Most people end Greek math with Euclid. But where is Archimedes?
- Archimedes was the GMOAT for a long, long time. And maybe still is!



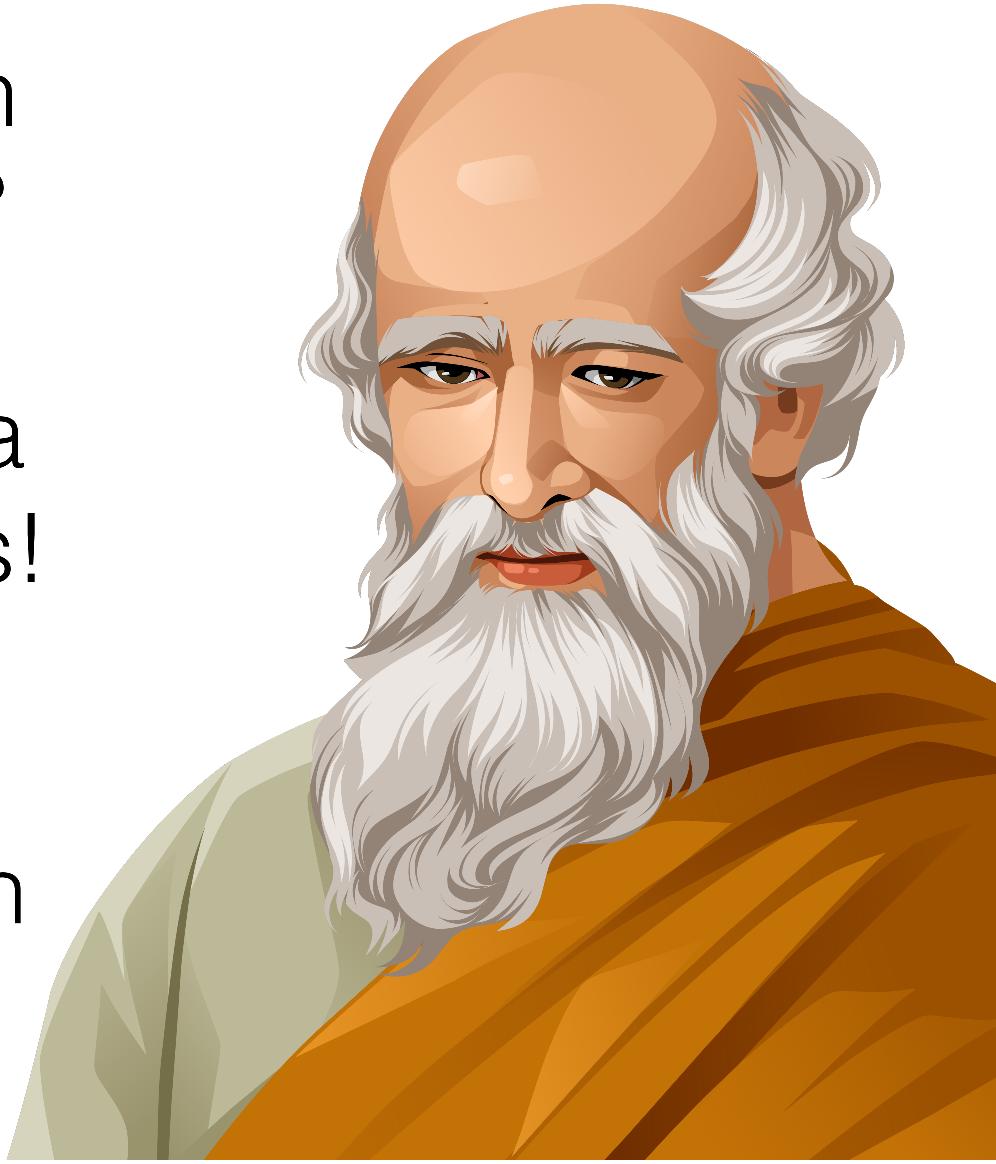
Where's Archimedes?

- Most people end Greek math with Euclid. But where is Archimedes?
- Archimedes was the GMOAT for a long, long time. And maybe still is!
- So much so that it makes more sense to discuss him with modern mathematicians.



Where’s Archimedes?

- Most people end Greek math with Euclid. But where is Archimedes?
- Archimedes was the GMOAT for a long, long time. And maybe still is!
- So much so that it makes more sense to discuss him with modern mathematicians.
- We will discuss him in Chapter 7.



Three Notable Problems About Primes

Problem 1

Problem 1

- What do you notice:

$$
\begin{aligned}
4 &= 2 + 2 \\
6 &= 3 + 3 \\
8 &= 5 + 3 \\
10 &= 7 + 3 \\
12 &= 7 + 5 \\
14 &= 7 + 7 \\
16 &= 13 + 3 \\
18 &= 13 + 5 \\
20 &= 17 + 3 \\
&\vdots
\end{aligned}
$$

Goldbach’s Conjecture

Goldbach’s Conjecture

- In 1742, in a letter to Leonhard Euler, German mathematician Christian Goldbach wrote:

Goldbach's Conjecture

- In 1742, in a letter to Leonhard Euler, German mathematician Christian Goldbach wrote:

- Notes: This was a conjecture, and Goldbach considered 1 to be prime.

Goldbach's Conjecture

- In 1742, in a letter to Leonhard Euler, German mathematician Christian Goldbach wrote:

- Notes: This was a conjecture, and Goldbach considered 1 to be prime.

- Euler's reply pointed out this this conjecture follows from what is today called *Goldbach's conjecture*:

Goldbach's Conjecture

- In 1742, in a letter to Leonhard Euler, German mathematician Christian Goldbach wrote:

> *Every integer greater than 2 can be written as the sum of three primes.*

- Notes: This was a conjecture, and Goldbach considered 1 to be prime.

- Euler's reply pointed out this this conjecture follows from what is today called *Goldbach's conjecture*:

Goldbach's Conjecture

- In 1742, in a letter to Leonhard Euler, German mathematician Christian Goldbach wrote:

  Every integer greater than 2 can be written as the sum of three primes.

- Notes: This was a conjecture, and Goldbach considered 1 to be prime.

- Euler's reply pointed out this this conjecture follows from what is today called *Goldbach's conjecture*:

  Every positive even integer can be written as the sum of two primes.

Problem 2

Problem 2

- What do you notice:

3 and 5
5 and 7
11 and 13
17 and 19
29 and 31
41 and 43
59 and 61
71 and 73
$\vdots$

Twin Prime Conjecture

Twin Prime Conjecture

- Definition: Twin primes are primes that differ by 2.

Twin Prime Conjecture

- Definition: Twin primes are primes that differ by 2.
- Twin prime conjecture: There are infinitely many twin primes.

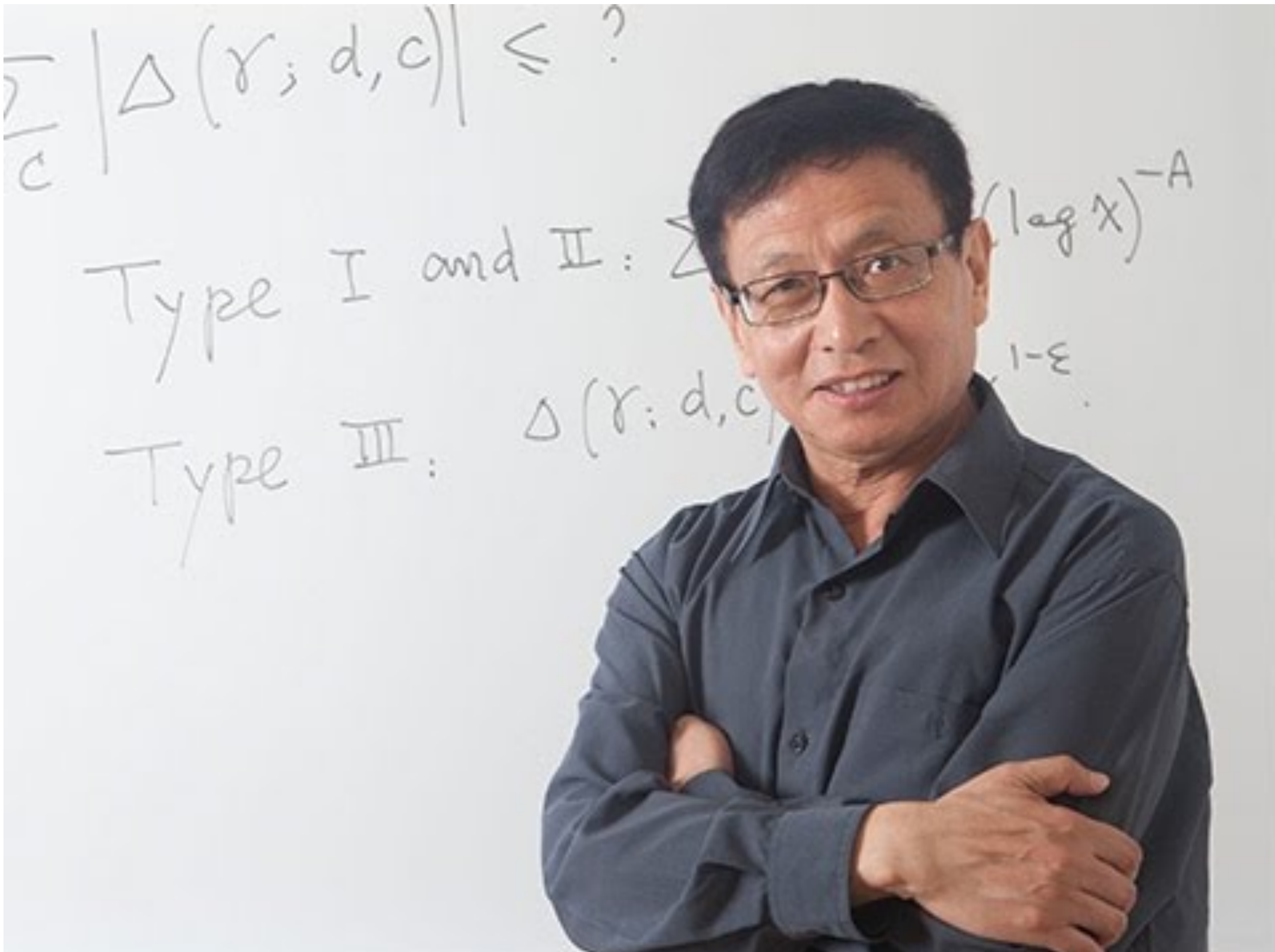
Twin Prime Conjecture

- Definition: Twin primes are primes that differ by 2.
- Twin prime conjecture: There are infinitely many twin primes.
- Yitang Zhang in April 2013: There are infinitely many primes that differ by less than 70 million.

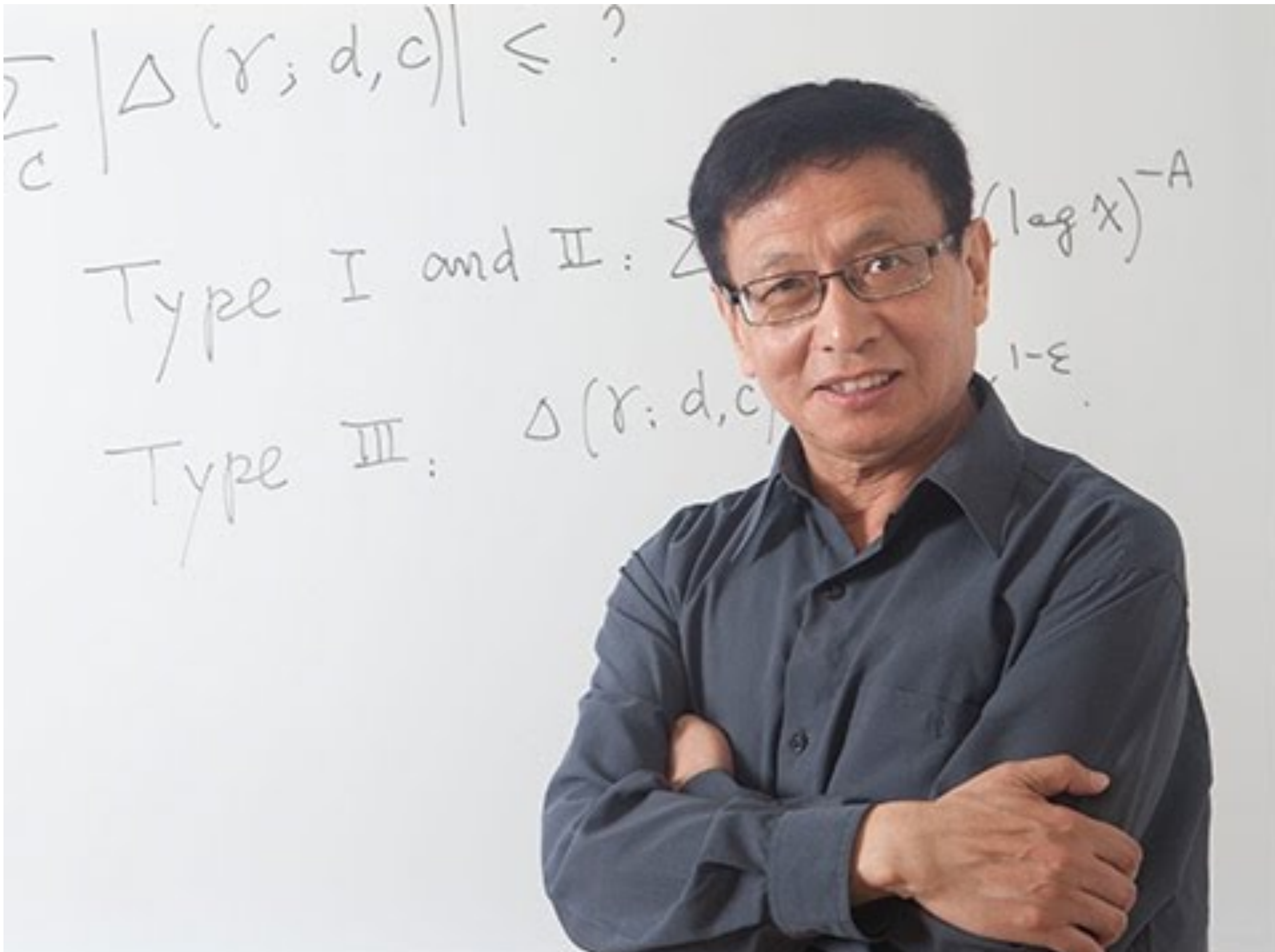
Twin Prime Conjecture

- Definition: Twin primes are primes that differ by 2.
- Twin prime conjecture: There are infinitely many twin primes.
- Yitang Zhang in April 2013: There are infinitely many primes that differ by less than 70 million.
- Over the next year, a riveting polymath project brought the gap down to 246.

Twin Prime Conjecture



Twin Prime Conjecture



Problem 3

Problem 3

- Euclid proved there are infinitely many primes.

Problem 3

- Euclid proved there are infinitely many primes.
- Can we say more? Over time the primes thin out. How quickly do they do so?

Prime Number Theorem

- Euclid proved there are infinitely many primes.
- Can we say more? Over time the primes thin out. How quickly do they do so?

Prime Number Theorem

- Euclid proved there are infinitely many primes.
- Can we say more? Over time the primes thin out. How quickly do they do so?
- Let $\pi(N)$ be the number of primes between 1 and N.

Prime Number Theorem

- Euclid proved there are infinitely many primes.
- Can we say more? Over time the primes thin out. How quickly do they do so?
- Let $\pi(N)$ be the number of primes between 1 and N.
- The prime number theorem says

$$\lim_{N \to \infty} \frac{\pi(N)}{N/\log(N)} = 1.$$

Chinese Remainder Theorem

Chinese Remainder Theorem

Chinese Remainder Theorem

- According to legend, ancient Chinese generals needed to record how many troops they had but wanted to do so in a cryptic way that could not be easily leaked to their enemies.

Chinese Remainder Theorem

- According to legend, ancient Chinese generals needed to record how many troops they had but wanted to do so in a cryptic way that could not be easily leaked to their enemies.

- Their strategy was to record some information related to the number.

Chinese Remainder Theorem

- According to legend, ancient Chinese generals needed to record how many troops they had but wanted to do so in a cryptic way that could not be easily leaked to their enemies.

- Their strategy was to record some information related to the number.

- Example: “If my troops march in rows of 5, there are 4 soldiers left over. If they march in rows of 8 there are 2 left over. In rows of 9, there are 7 left over.”

Chinese Remainder Theorem

Chinese Remainder Theorem

- Given this information, and a ballpark idea of how many troops there are, one can determine it exactly.

Chinese Remainder Theorem

- Given this information, and a ballpark idea of how many troops there are, one can determine it exactly.

- The method to do so is called the Chinese remainder theorem.

Chinese Remainder Theorem

- Given this information, and a ballpark idea of how many troops there are, one can determine it exactly.
- The method to do so is called the Chinese remainder theorem.
- It first appeared in Sun Zi's book *Mathematical Manual*, written in the 3rd century AD.

Chinese Remainder Theorem

Chinese Remainder Theorem

- If you feel comfortable with modular arithmetic, check it out in the notes.

Theorem.

Theorem 1.4 (Sun Zi)**.** Suppose $n_1, n_2, \ldots, n_k$ are integers larger than 1. If the n_i are pairwise relatively prime, then for any integers $a_1, a_2, \ldots, a_k$, the system of modular congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution. Moreover, if x_1 and x_2 are both solutions to this system, then $x_1 \equiv x_2 \pmod{n_1 n_2 \cdots n_k}$.

Pythagorean Triples

Pythagorean Triples

- Recall that there are infinitely many *Pythagorean triples*. That is, infinitely many positive integers x, y and z for which
$$a^2 + b^2 = c^2.$$

Pythagorean Triples

- Recall that there are infinitely many *Pythagorean triples*. That is, infinitely many positive integers x, y and z for which
$$a^2 + b^2 = c^2.$$

- Example: 3, 4, 5 is a Pythagorean triple.

Pythagorean Triples

- Recall that there are infinitely many *Pythagorean triples*. That is, infinitely many positive integers x, y and z for which
$$a^2 + b^2 = c^2.$$

- Example: 3, 4, 5 is a Pythagorean triple.

- Question: Can you think of a triple of positive integers that satisfy
$$x^3 + y^3 = z^3 \,?$$

Fermat's Last Theorem

"Theorem." Suppose n is an integer larger than 2. There are no positive integers x, y and z such that

$$x^n + y^n = z^n \,.$$

Fermat’s Last Theorem

Fermat's Last Theorem

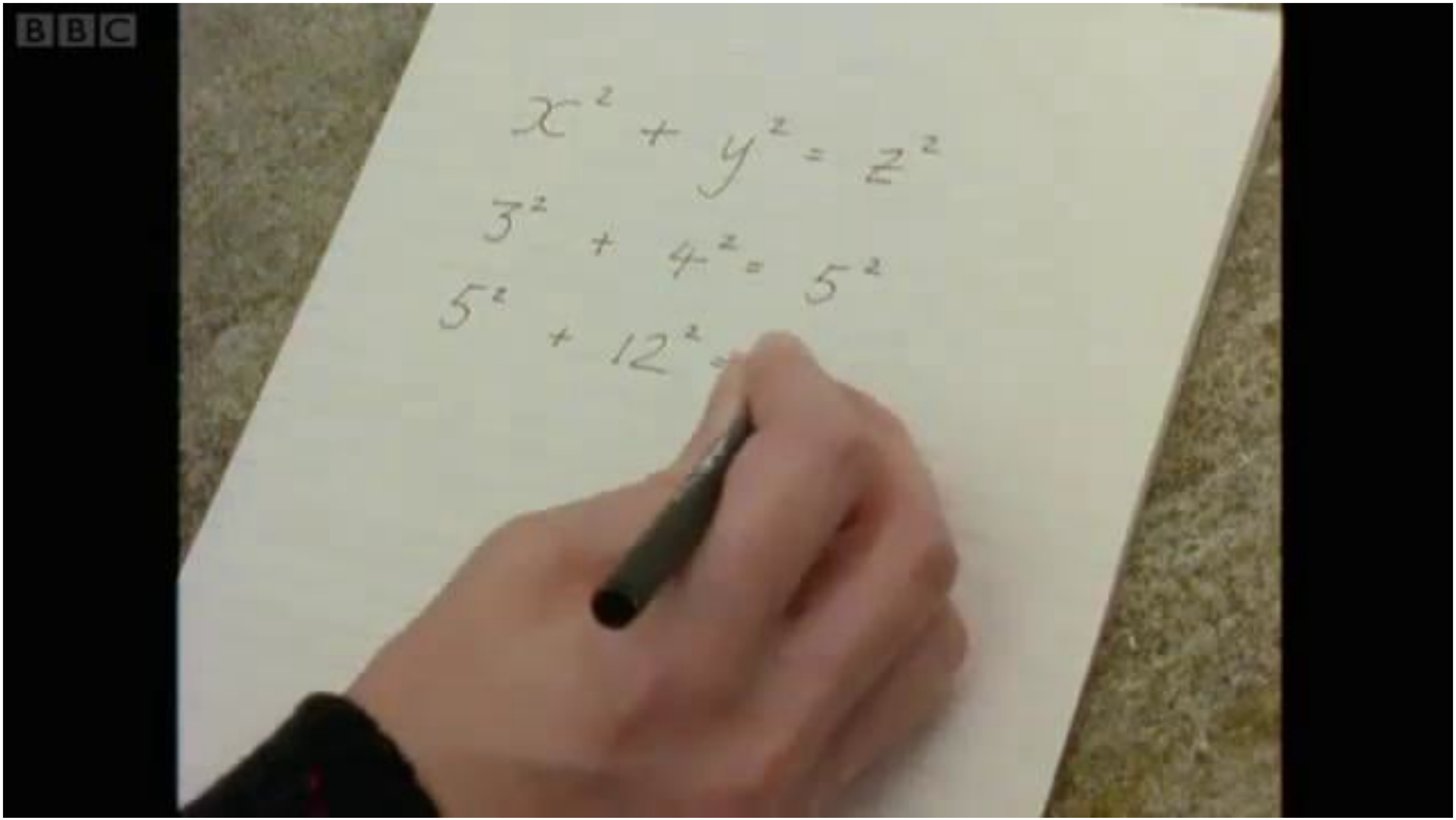
- The first person to make progress on a general approach to solve it was Sophie Germain.

Fermat's Last Theorem

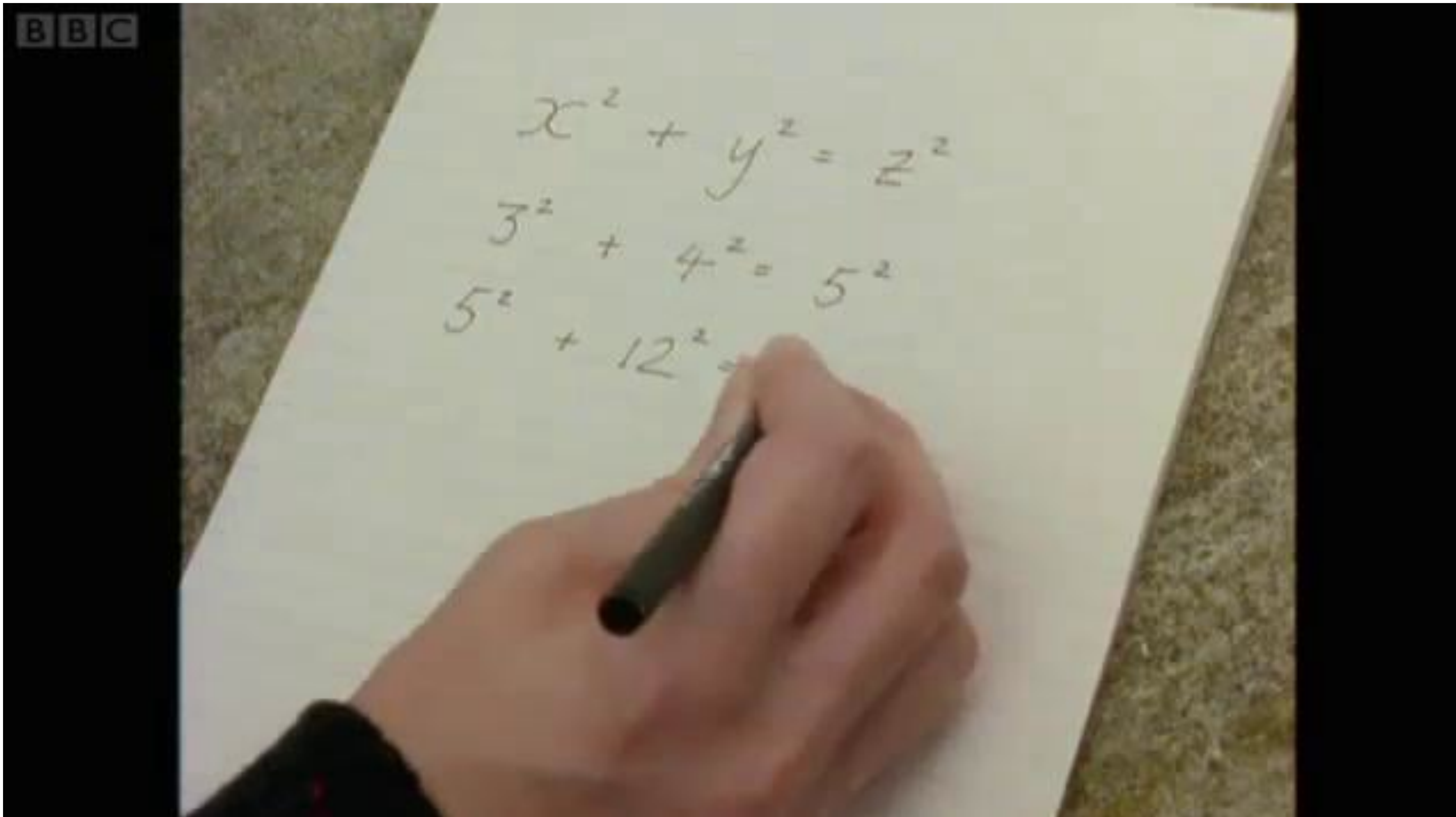
- The first person to make progress on a general approach to solve it was Sophie Germain.

- If you are comfortable with modular arithmetic, you should check out her proof in the notes.

Fermat’s Last Theorem



Fermat’s Last Theorem



The Aftermath

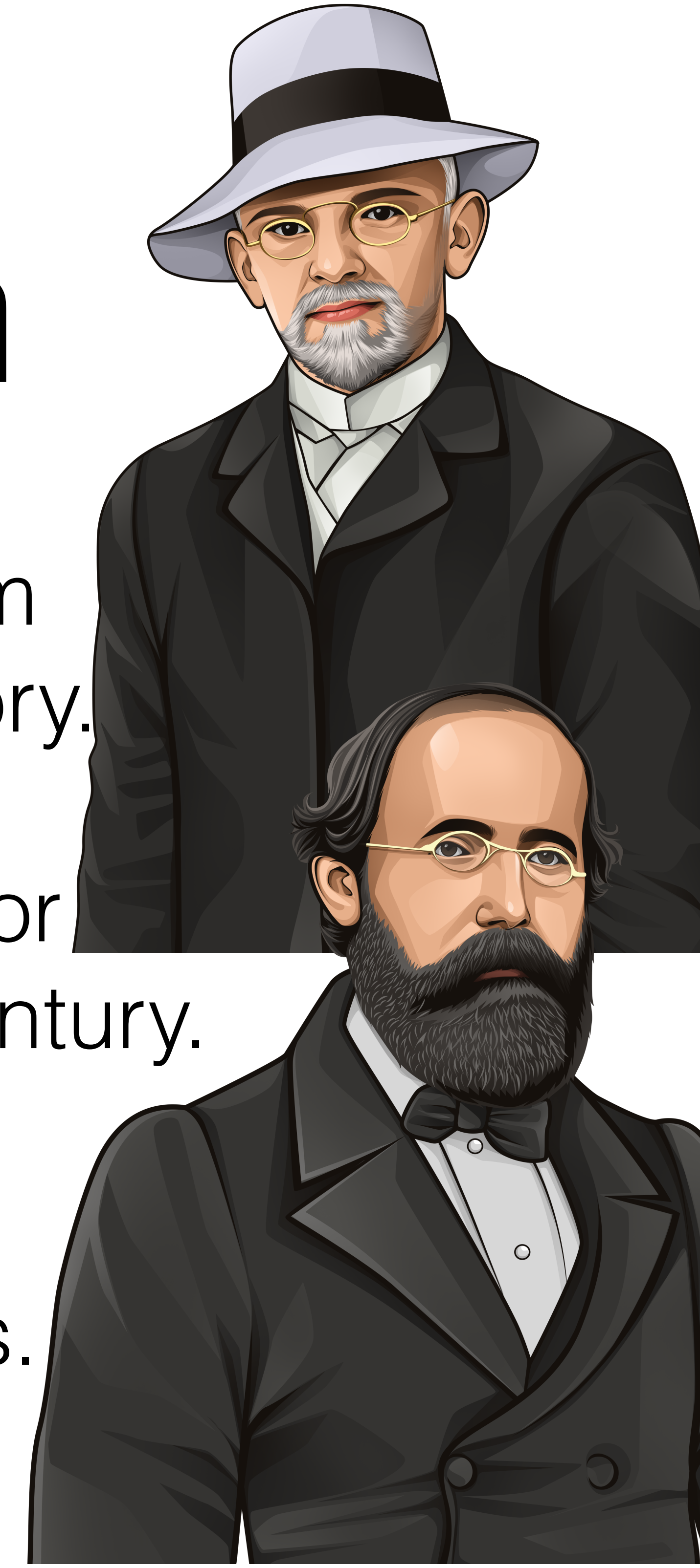
The Aftermath

- The most important unsolved math problem relates to prime numbers and number theory.

The Aftermath

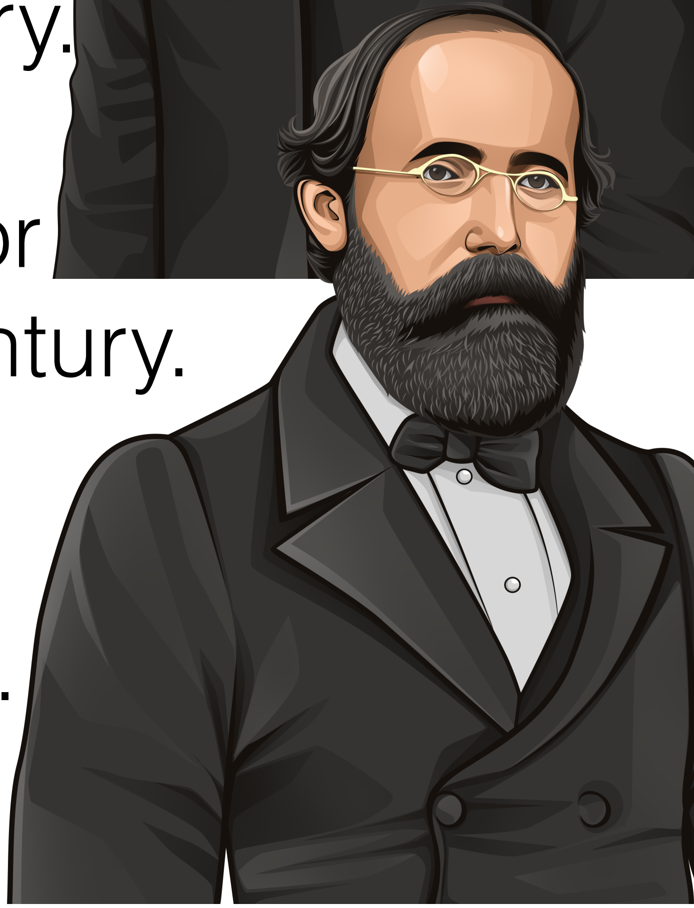
- The most important unsolved math problem relates to prime numbers and number theory.
- In 1900, David Hilbert listed 23 problems for mathematicians to focus on for the next century.

The Aftermath



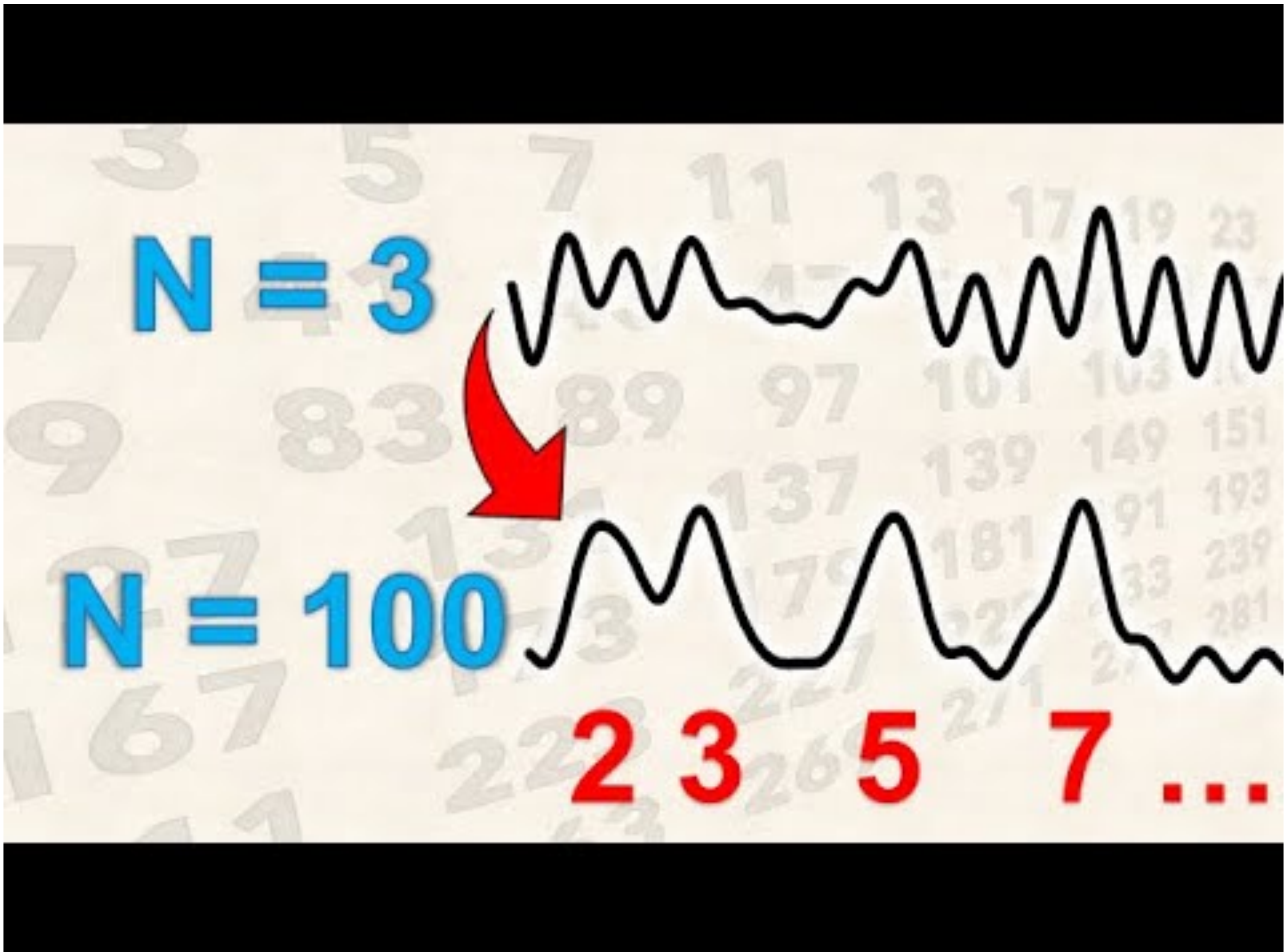
- The most important unsolved math problem relates to prime numbers and number theory.
- In 1900, David Hilbert listed 23 problems for mathematicians to focus on for the next century.
- 3 remain completely unsolved. The most notable of these is the Riemann hypothesis. Solving it would tell us a lot of about the distribution of primes.

The Aftermath

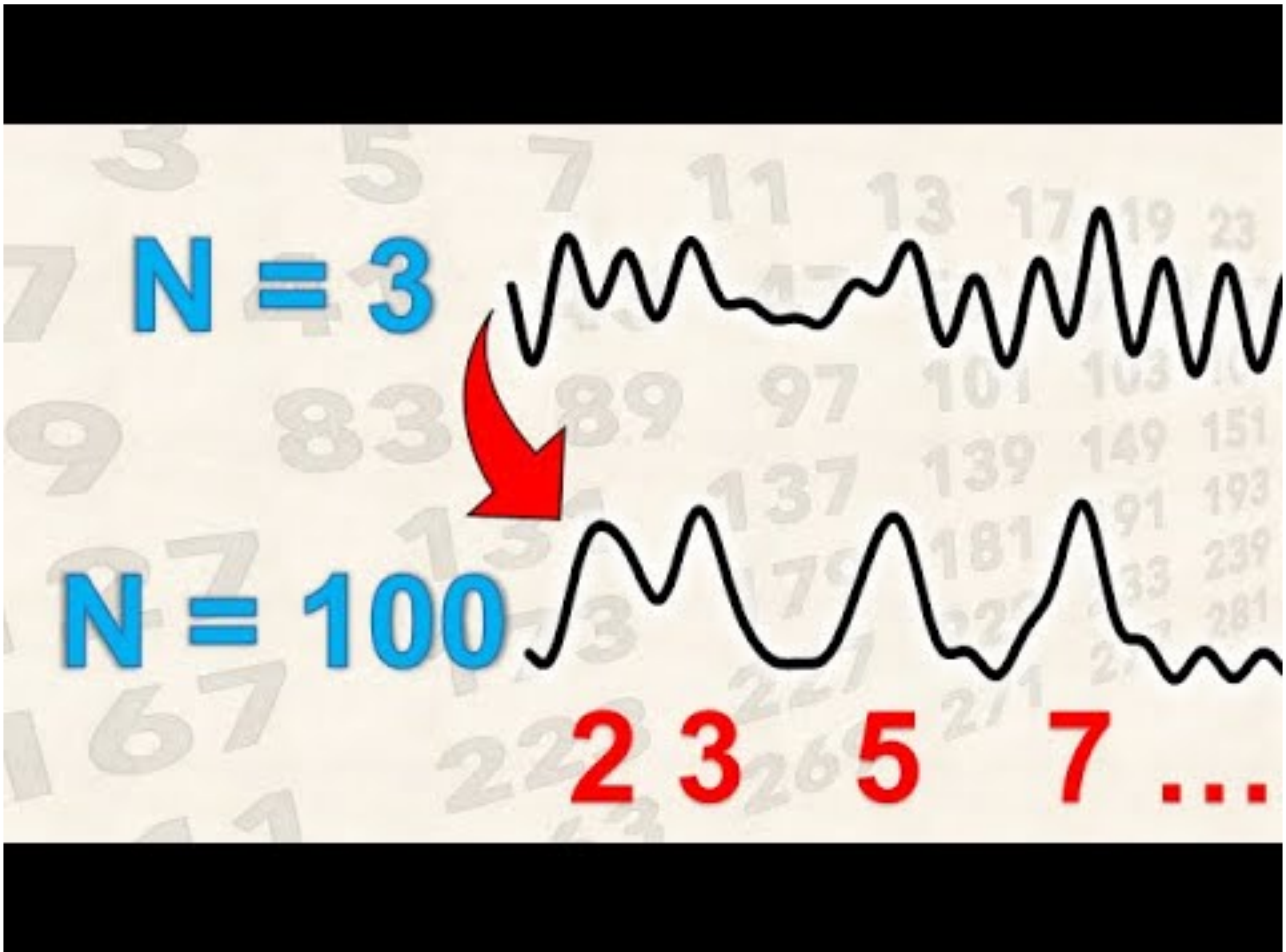


- The most important unsolved math problem relates to prime numbers and number theory.
- In 1900, David Hilbert listed 23 problems for mathematicians to focus on for the next century.
- 3 remain completely unsolved. The most notable of these is the Riemann hypothesis. Solving it would tell us a lot of about the distribution of primes.
- In 2000, the Clay Institute published 7 problems for the next century and offered $1 million for any solution.

The Riemann Hypothesis

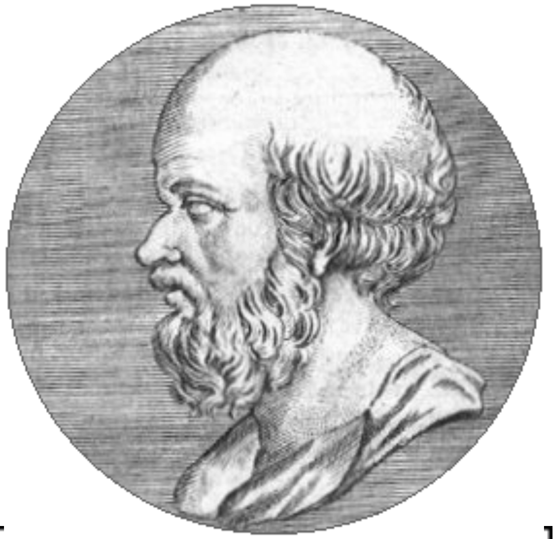


The Riemann Hypothesis



Shout-outs

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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Eratosthenes

- Eratosthenes lived 296 - 194 BC, modern-day Libya.

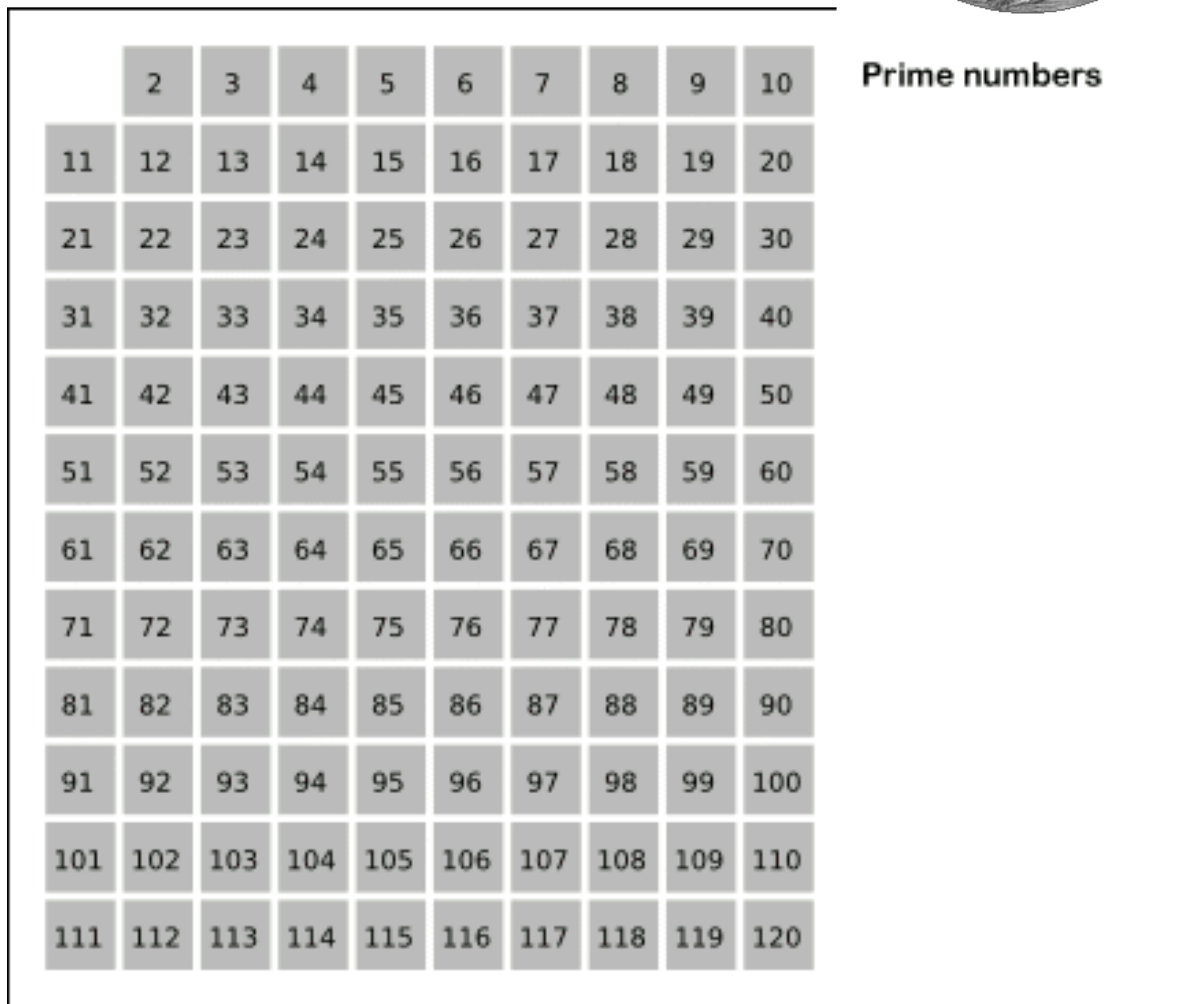
	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Eratosthenes

- Eratosthenes lived 296 - 194 BC, modern-day Libya.

- Sieve of Eratosthenes: Method for finding primes.



Eratosthenes

- Eratosthenes lived 296 - 194 BC, modern-day Libya.
- Sieve of Eratosthenes: Method for finding primes.

Prime numbers

	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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Eratosthenes

- Eratosthenes lived 296 - 194 BC, modern-day Libya.
- Sieve of Eratosthenes: Method for finding primes.
- First to calculate the circumference of the Earth.

	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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Sofie Germain

Sofie Germain

- Grew up in Paris during the French Revolution.

Sofie Germain

- Grew up in Paris during the French Revolution.
- Studied math against the wishes of her parents, using the books in her dad's library.

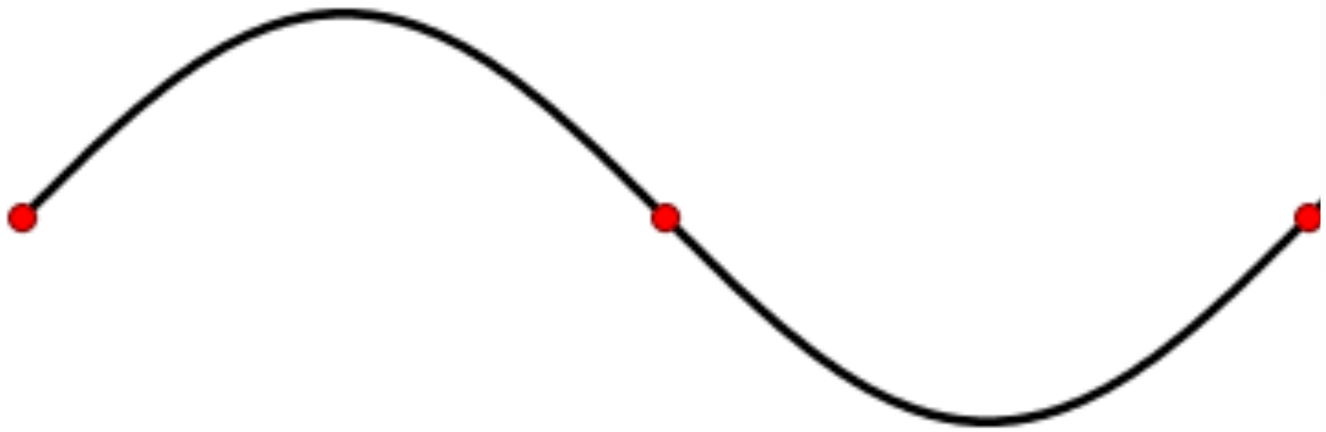
Sofie Germain

- Grew up in Paris during the French Revolution.

- Studied math against the wishes of her parents, using the books in her dad's library.

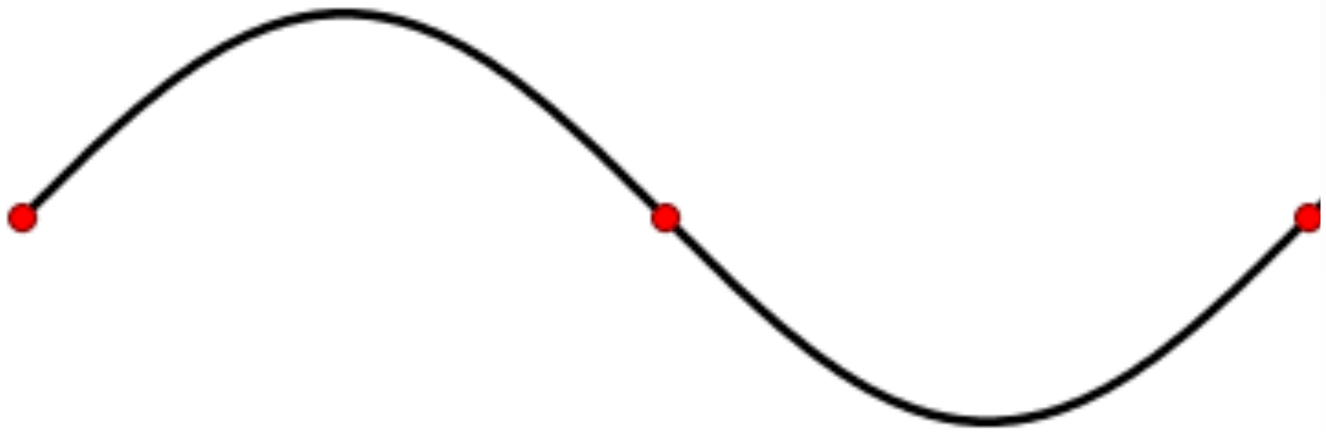
- Solved the problem of vibrating plates, winning a prestigious prize for her work.

Sofie Germain



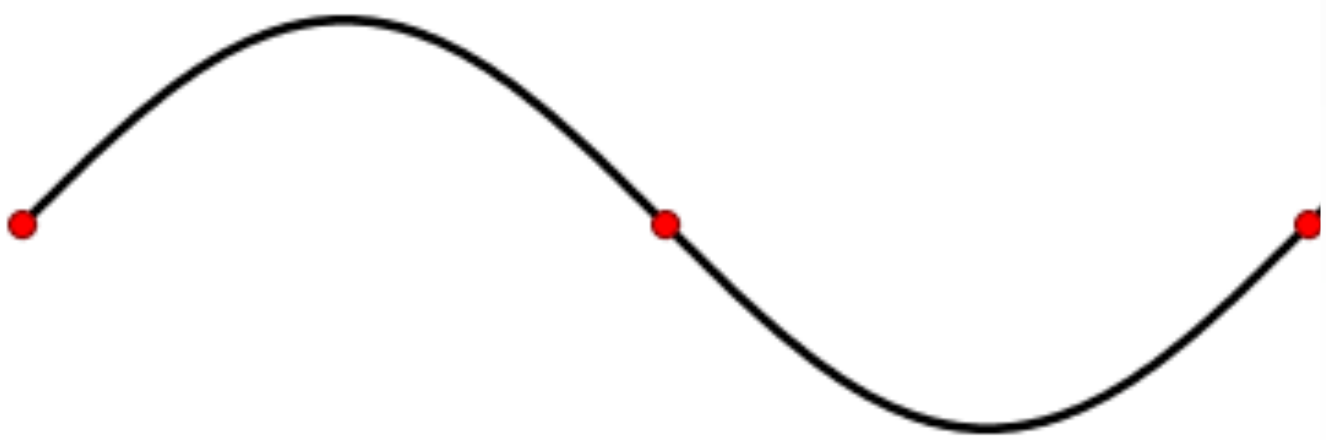
Sofie Germain

- Standing wave:



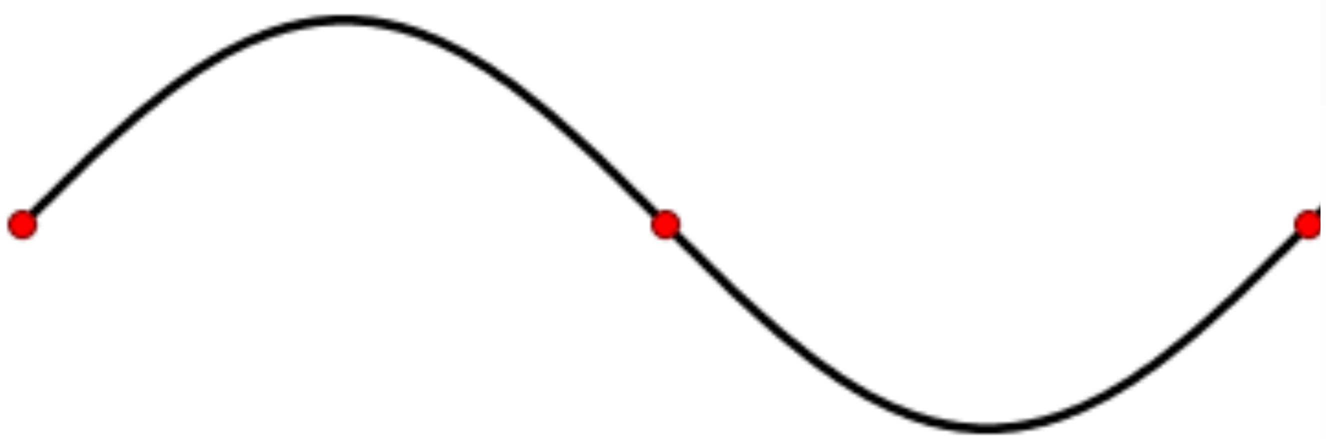
Sofie Germain

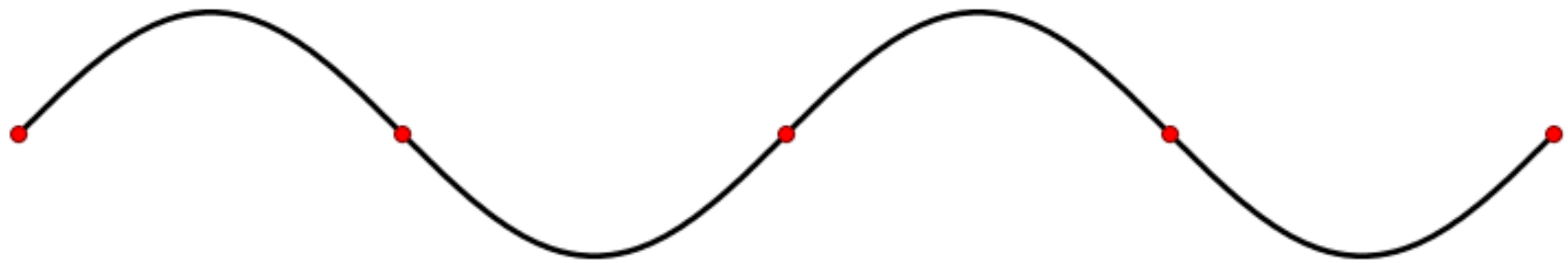
- Standing wave:



Sofie Germain

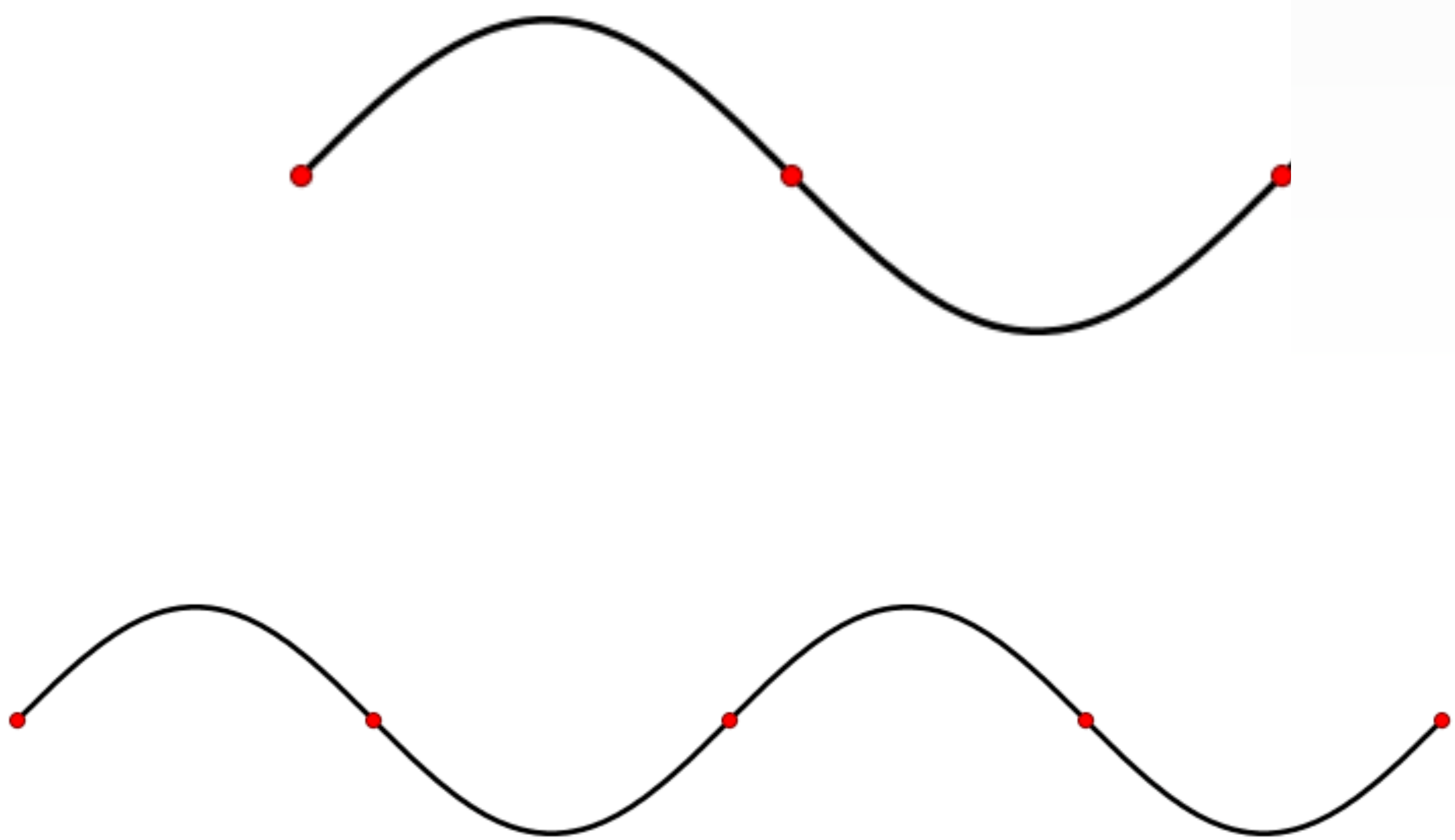
- Standing wave:





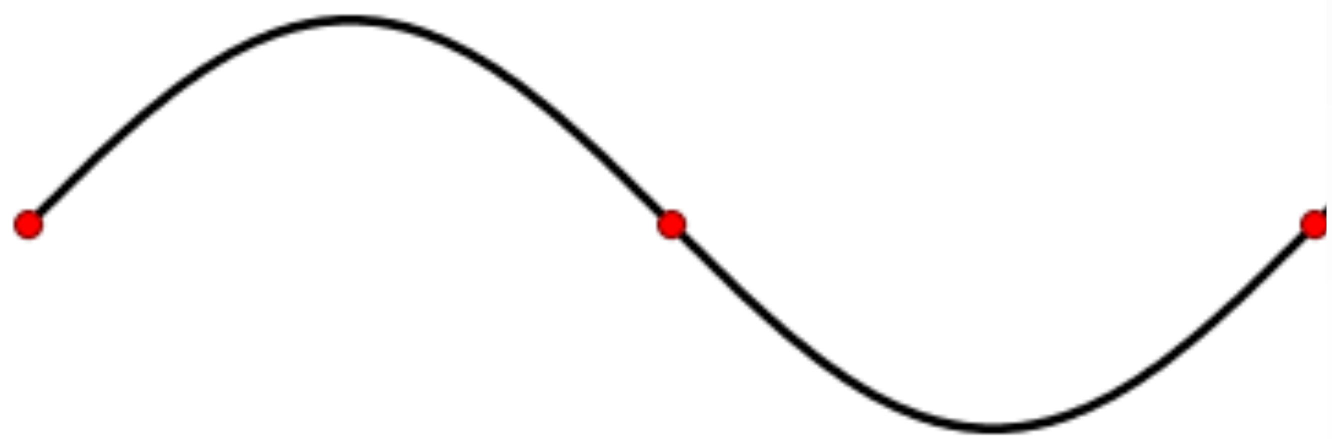
Sofie Germain

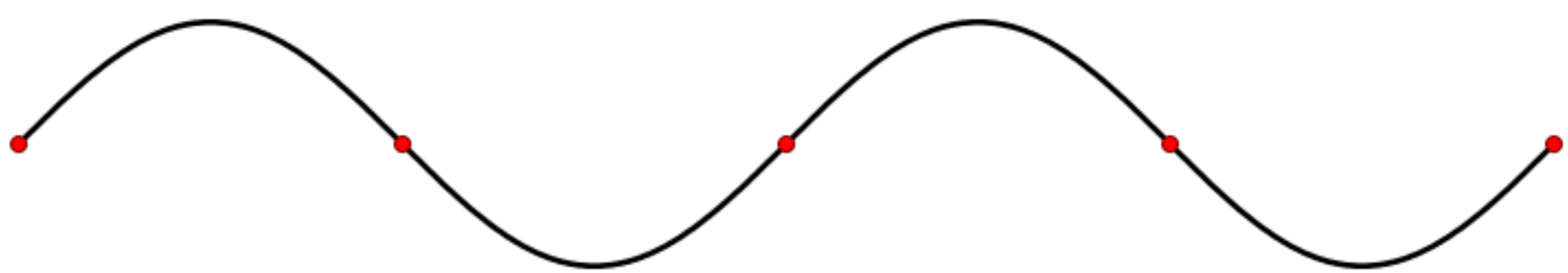
- Standing wave:



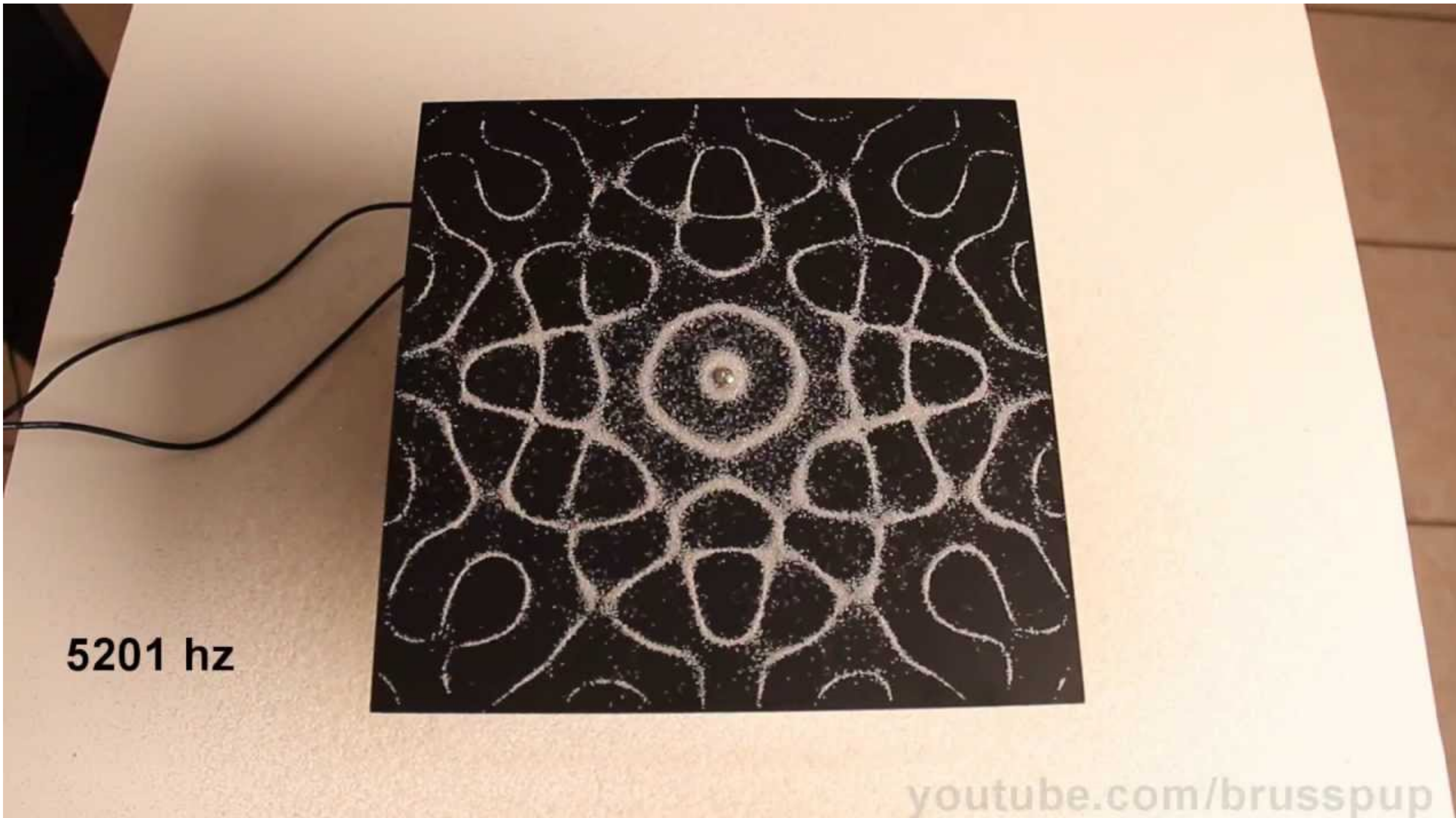
Sofie Germain

- Standing wave:

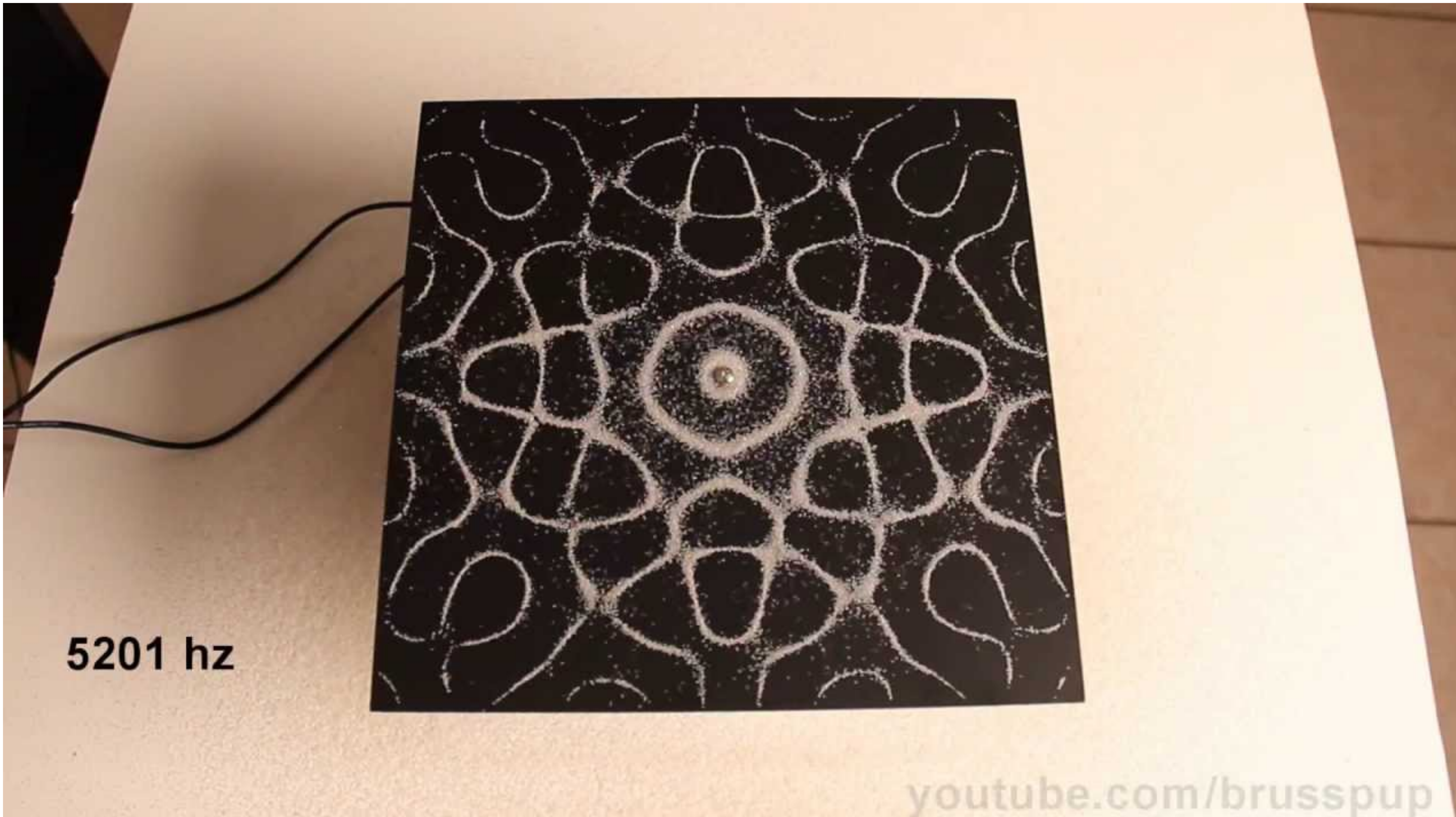




Sofie Germain



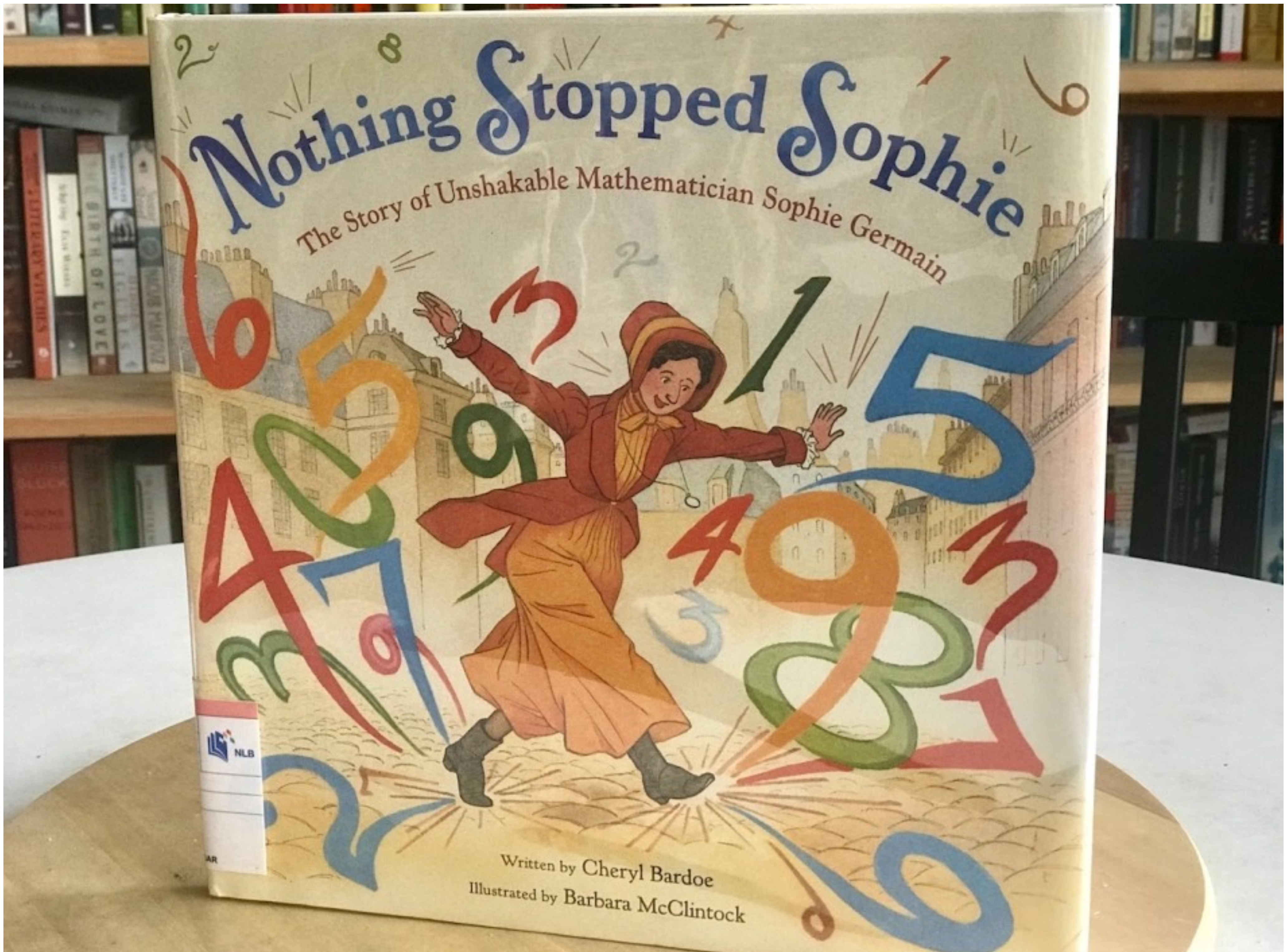
Sofie Germain



Sofie Germain

Sofie Germain

Sofie Germain



Carl Friedrich Gauss

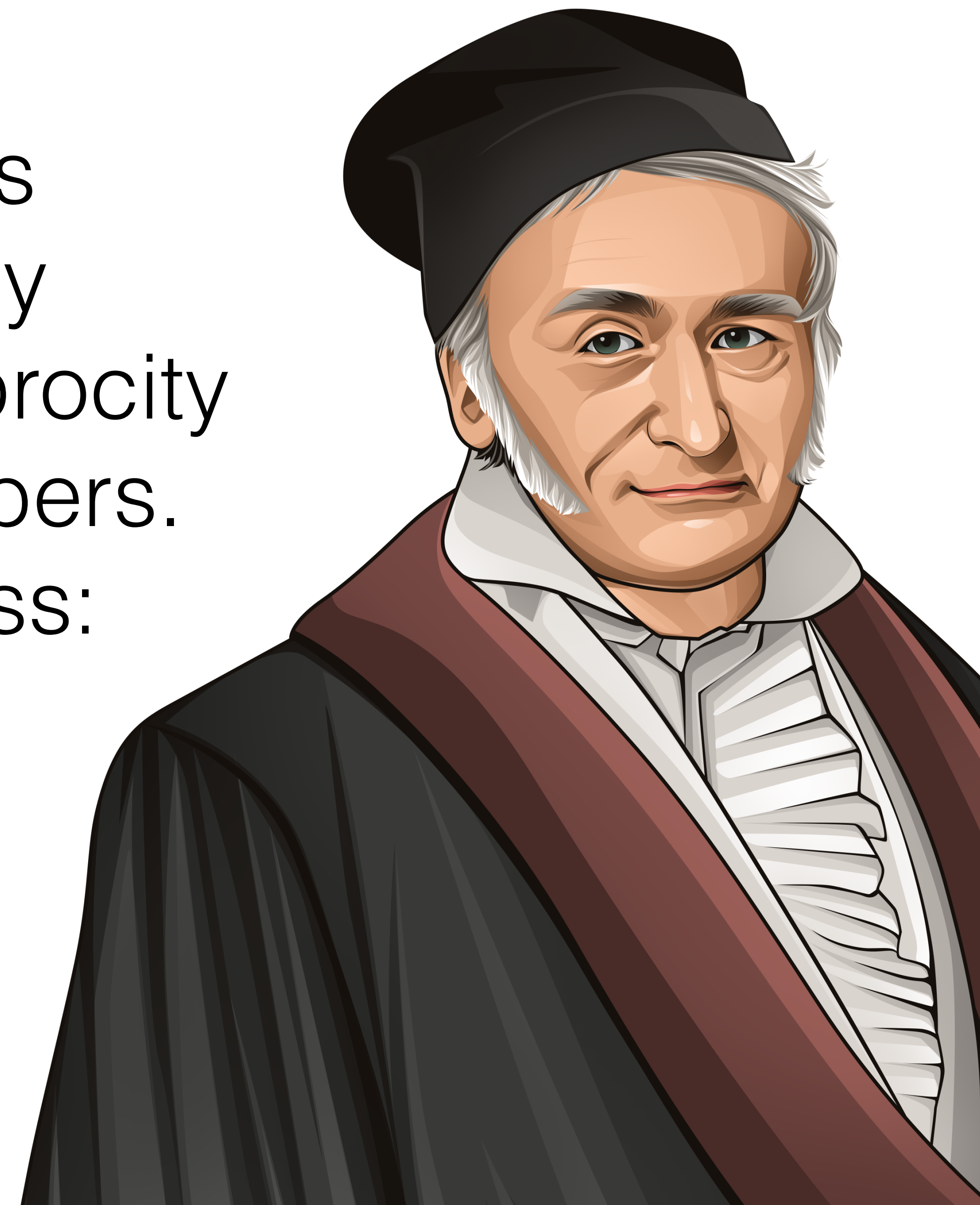
Carl Friedrich Gauss

- Gauss: “Mathematics is the queen of sciences and number theory is the queen of mathematics.”

Carl Friedrich Gauss

- Gauss: "Mathematics is the queen of sciences and number theory is the queen of mathematics."

- One of the greatest mathematicians in history. Did a lot in number theory including his law of quadratic reciprocity and development of complex numbers. Sample of things named after Gauss:

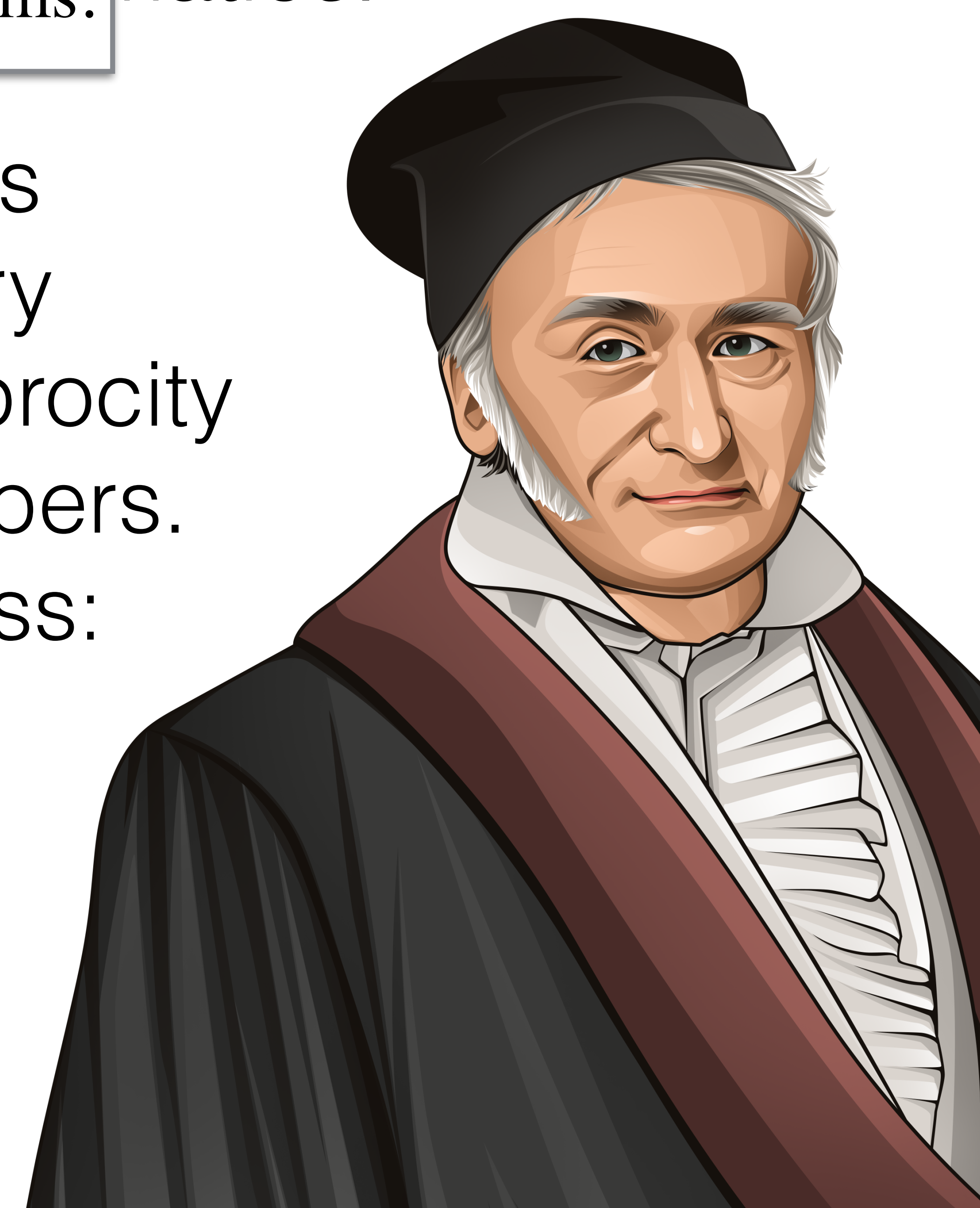


Gauss

sciences and
matics."

Gauss' braid, Gauss's constant, Gaussian curvature, Gaussian distribution, Gaussian filter, Gaussian fixed point, Gauss's formula, Gaussian function, Gauss's inequality, Gaussian integer, Gauss line, Gauss map, Gaussian measure, Gaussian quadrature, Gauss sum, Gaussian surface, Gauss transformation, several Gauss's lemmas, and at least a dozen Gauss's theorems.

- One of the greatest mathematicians in history. Did a lot in number theory including his law of quadratic reciprocity and development of complex numbers. Sample of things named after Gauss:



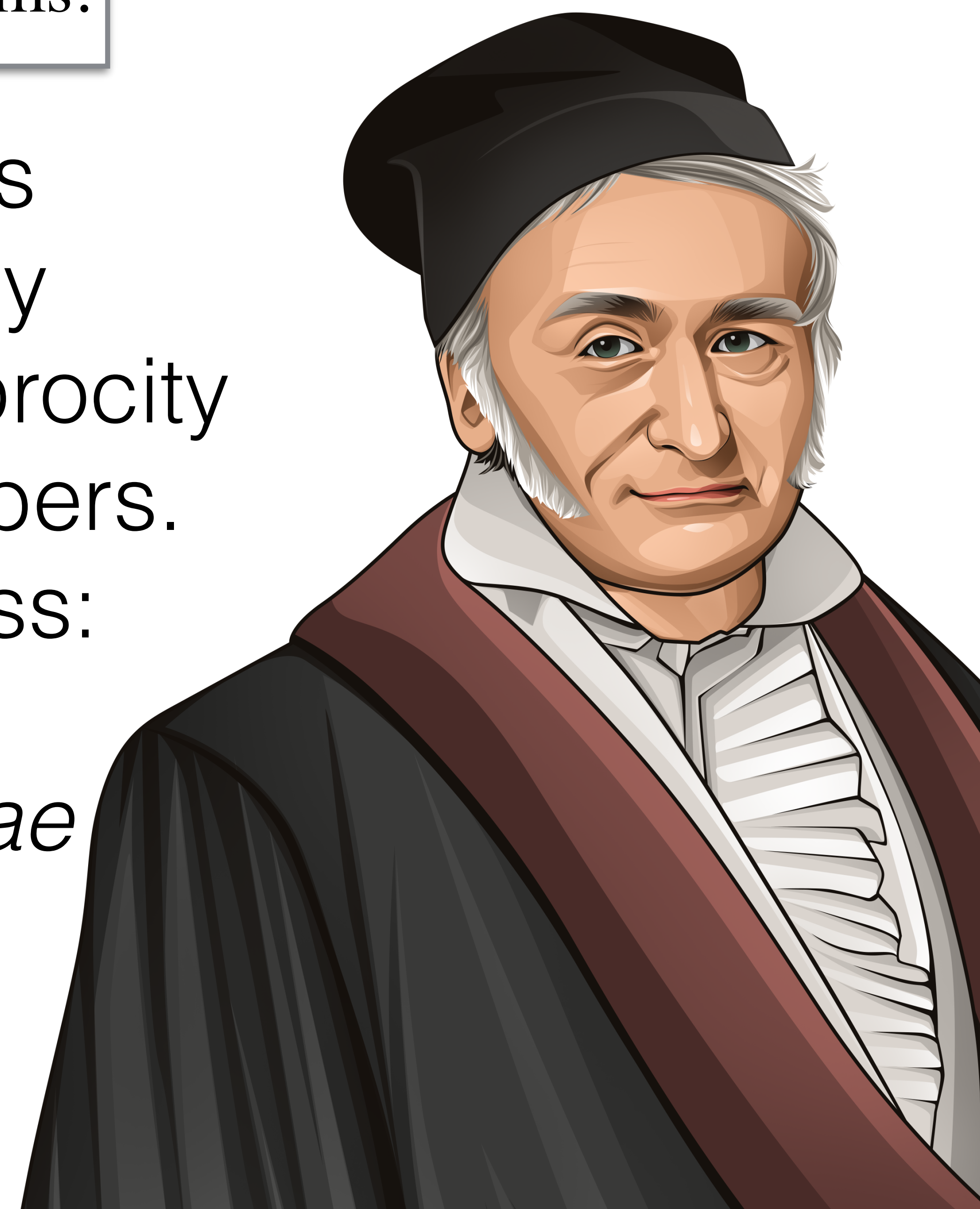
Gauss

sciences and
matics.”

Gauss' braid, Gauss's constant, Gaussian curvature, Gaussian distribution, Gaussian filter, Gaussian fixed point, Gauss's formula, Gaussian function, Gauss's inequality, Gaussian integer, Gauss line, Gauss map, Gaussian measure, Gaussian quadrature, Gauss sum, Gaussian surface, Gauss transformation, several Gauss's lemmas, and at least a dozen Gauss's theorems.

- One of the greatest mathematicians in history. Did a lot in number theory including his law of quadratic reciprocity and development of complex numbers. Sample of things named after Gauss:

- His book *Disquisitiones Arithmeticae* is probably the most important number theory book in history.



People’s History

People’s History of Equality

People’s History of Equality

- Sophie Germain’s story of triumph over adversity is extremely common among historical women in math.

People’s History of Equality

- Sophie Germain’s story of triumph over adversity is extremely common among historical women in math.
- These difficulties kept countless women from doing math or for being remembered for the math they did.

People’s History of Equality

- Sophie Germain’s story of triumph over adversity is extremely common among historical women in math.
- These difficulties kept countless women from doing math or for being remembered for the math they did.
- As gender inequality has decreased, the number of women in math has increased.

People's History of Equality

People’s History of Equality

- Many math histories ignore most of the work of non-Europeans.

People’s History of Equality

- Many math histories ignore most of the work of non-Europeans.
- And many discoveries outside of Europe are named after the first European to discover them.

People's History of Equality

- Many math histories ignore most of the work of non-Europeans.
- And many discoveries outside of Europe are named after the first European to discover them.
- Things are way better than they were.

People's History of Equality

- Many math histories ignore most of the work of non-Europeans.
- And many discoveries outside of Europe are named after the first European to discover them.
- Things are way better than they were.
- But the demographics of math PhD-holders indicate that there is a lot more work to go.