MAS114: Lecture 8

James Cranch

http://cranch.staff.shef.ac.uk/mas114/

2021–2022

Elementary number theory

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.
This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.
This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Remark

In the sense that mathematicians use the word, "elementary" doesn't mean "easy": it means "using no deep theory" (we're only four weeks into your first semester, so haven't had time to develop any deep theory).

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.
This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Remark

In the sense that mathematicians use the word, "elementary" doesn't mean "easy": it means "using no deep theory" (we're only four weeks into your first semester, so haven't had time to develop any deep theory). It can still be difficult, and in fact it can still be deep.

Divisibility

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$:

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*, or that *a goes into b*.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*, or that *a goes into b*.
In symbols, we write $a \mid b$ to say that a divides b,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*, or that *a goes into b*.
In symbols, we write $a \mid b$ to say that a divides b, and write $a \nmid b$ to say that a does not divide b.

Examples

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$,

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$,

or (equivalently)

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$,

or (equivalently)

for all $n \in \mathbb{Z}$, we have $an \neq b$.

The trivial cases

The trivial cases

It's worth sorting out the trivial cases:

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

- When do we have $a \mid 1$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

- When do we have $a \mid 1$?

  When $a = \pm 1$.

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?
  When $a = \pm 1$.
- When do we have $1 \mid b$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?
  When $a = \pm 1$.
- When do we have $1 \mid b$?
  Always (since $1b = b$ for all b).

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?
  When $a = \pm 1$.
- When do we have $1 \mid b$?
  Always (since $1b = b$ for all b).

For the next few lectures, we'll be studying the integers from the point of view of divisibility.

Prime numbers

Prime numbers

The following definition is a natural one:

Prime numbers

The following definition is a natural one:

Definition

An integer $p > 1$ is said to be *prime* if it has no positive factors except for 1 and p itself.

Prime numbers

The following definition is a natural one:

Definition

An integer $p > 1$ is said to be *prime* if it has no positive factors except for 1 and p itself.

Primes are clearly a good thing to study: they're the numbers with no complicated factors.

Prime numbers

The following definition is a natural one:

Definition

An integer $p > 1$ is said to be *prime* if it has no positive factors except for 1 and p itself.

Primes are clearly a good thing to study: they're the numbers with no complicated factors.
It's good to have a word meaning roughly the same thing as "not prime":

Prime numbers

The following definition is a natural one:

Definition

An integer $p > 1$ is said to be *prime* if it has no positive factors except for 1 and p itself.

Primes are clearly a good thing to study: they're the numbers with no complicated factors.
It's good to have a word meaning roughly the same thing as "not prime":

Definition

An integer $n > 1$ is said to be *composite* if it is not prime: that is, if it does have positive factors other than 1 and n.

The number 1

The number 1

Remark

Notice that we have chosen our definitions so that 1 will be neither prime nor composite.

The number 1

Remark

Notice that we have chosen our definitions so that 1 will be neither prime nor composite. This was a choice, and it seems a bit mysterious at first.

The number 1

Remark

Notice that we have chosen our definitions so that 1 will be neither prime nor composite. This was a choice, and it seems a bit mysterious at first.

Indeed, until the late 19th century, mathematicians treated 1 as prime.

The number 1

Remark

Notice that we have chosen our definitions so that 1 will be neither prime nor composite. This was a choice, and it seems a bit mysterious at first.

Indeed, until the late 19th century, mathematicians treated 1 as prime. But it was found to be so much simpler to do it this way that nobody considers 1 to be prime any more.

Primes are building blocks

Primes are building blocks

The main thing about primes is that all other positive integers are built from them by multiplication.

Primes are building blocks

The main thing about primes is that all other positive integers are built from them by multiplication.
Before we get to that, it's worth explaining something about multiplication.

The empty product

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

I could split the work up in other ways:

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

I could split the work up in other ways:

$$(2 \times 4) \times (3 \times 5) = 8 \times 15 = 120$$

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

I could split the work up in other ways:

$$(2 \times 4) \times (3 \times 5) = 8 \times 15 = 120$$
$$(2 \times 3 \times 4) \times (5) = 24 \times 5 = 120$$

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

I could split the work up in other ways:

$$(2 \times 4) \times (3 \times 5) = 8 \times 15 = 120$$
$$(2 \times 3 \times 4) \times (5) = 24 \times 5 = 120$$

What if I give all the numbers to the first person?

$$(2 \times 3 \times 4 \times 5) \times (?) = 120 \times ? = 120$$

The empty product

You're all used to the fact that the sum of an empty list of numbers is zero. I want to persuade you that the product of an empty list of numbers is one.

Suppose I'm trying to find $2 \times 3 \times 4 \times 5$.

One way of doing this would be to ask one person to find 2×3 and another to find 4×5, and then multiply the results:

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120.$$

I could split the work up in other ways:

$$(2 \times 4) \times (3 \times 5) = 8 \times 15 = 120$$
$$(2 \times 3 \times 4) \times (5) = 24 \times 5 = 120$$

What if I give all the numbers to the first person?

$$(2 \times 3 \times 4 \times 5) \times (?) = 120 \times ? = 120$$

For the right answer, the product of no numbers must be 1.

Back to primes as building blocks

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

We'll prove this by strong induction on n.

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

We'll prove this by strong induction on n.

For our base case, we observe that when $n = 1$, we can write n as the product of no primes.

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

We'll prove this by strong induction on n.
For our base case, we observe that when $n = 1$, we can write n as the product of no primes.
So now we have to do our induction step: let k be a positive integer. We assume that every positive integer i with $1 \leqslant i < k$ can be written as a product of primes, and we try to prove that k can.

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

Now, either k is prime, or it is composite. If it is prime, then k is the product of just one prime (namely, k itself).

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

Now, either k is prime, or it is composite. If it is prime, then k is the product of just one prime (namely, k itself).
If, however, k is composite, then it has a positive integer factor a which is not 1 nor k itself: in other words, we have $k = ab$, where both a and b are between 1 and k.

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

Now, either k is prime, or it is composite. If it is prime, then k is the product of just one prime (namely, k itself).
If, however, k is composite, then it has a positive integer factor a which is not 1 nor k itself: in other words, we have $k = ab$, where both a and b are between 1 and k. By the induction hypothesis, a and b can both be written as products of primes, say:

$$a = p_1 p_2 \cdots p_m, \quad \text{and} \quad b = q_1 q_2 \cdots q_n.$$

Back to primes as building blocks

Theorem

Every positive integer n can be written as a product of primes (in at least one way).

Proof.

Now, either k is prime, or it is composite. If it is prime, then k is the product of just one prime (namely, k itself).
If, however, k is composite, then it has a positive integer factor a which is not 1 nor k itself: in other words, we have $k = ab$, where both a and b are between 1 and k. By the induction hypothesis, a and b can both be written as products of primes, say:

$$a = p_1 p_2 \cdots p_m, \quad \text{and} \quad b = q_1 q_2 \cdots q_n.$$

But then $k = ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$, which proves it for k.
That completes the induction step (and the proof). □

More to come

More to come

Remark

Later on, we'll prove a stronger result, that every number can be written as a product of primes in *exactly* one way (rearranging the factors doesn't count).

More to come

Remark

Later on, we'll prove a stronger result, that every number can be written as a product of primes in *exactly* one way (rearranging the factors doesn't count). That's much, much harder.

Questions about primes

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

What are sensible questions to ask? Here are some obvious examples:

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

What are sensible questions to ask? Here are some obvious examples:

(a) How many primes are there?

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

What are sensible questions to ask? Here are some obvious examples:

(a) How many primes are there?

(b) There's quite a lot of primes between 1 and 50. Do they tend to get rarer as we go on?

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

What are sensible questions to ask? Here are some obvious examples:

(a) How many primes are there?

(b) There's quite a lot of primes between 1 and 50. Do they tend to get rarer as we go on?

(c) Other than 2 and 5, all primes must end in 1, 3, 7 or 9. Is there a bias: do more end in 3 than in 9, for example?

Questions about primes

Because of this we can be sure that primes are reasonably important. The first few are:

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

What are sensible questions to ask? Here are some obvious examples:

(a) How many primes are there?

(b) There's quite a lot of primes between 1 and 50. Do they tend to get rarer as we go on?

(c) Other than 2 and 5, all primes must end in 1, 3, 7 or 9. Is there a bias: do more end in 3 than in 9, for example?

(d) There seem to be several pairs of small primes which differ by 2 (eg 3 and 5, and 5 and 7, and 11 and 13). How many such pairs are there?

More questions about primes

More questions about primes

(e) Are there quick ways of testing if a number is prime?

More questions about primes

(e) Are there quick ways of testing if a number is prime?

(f) Are there quick ways of finding large primes?

More questions about primes

(e) Are there quick ways of testing if a number is prime?

(f) Are there quick ways of finding large primes?

Some of these have had well-known answers for more than a century, some are still unsolved, and some are currently the focus of tremendous interest.

More questions about primes

(e) Are there quick ways of testing if a number is prime?

(f) Are there quick ways of finding large primes?

Some of these have had well-known answers for more than a century, some are still unsolved, and some are currently the focus of tremendous interest.

We'll start off by giving the answer to that first question, which was known to the ancient Greeks:

How many primes?

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

We'll construct a sequence $p_1, p_2, p_3 \ldots$ of different primes by induction (so, the statement we're doing induction on is, "there are at least n different primes").

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

We'll construct a sequence $p_1, p_2, p_3 \ldots$ of different primes by induction (so, the statement we're doing induction on is, "there are at least n different primes").

For our base case we take $n = 1$, and then take $p_1 = 2$, which is a prime.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

We'll construct a sequence $p_1, p_2, p_3 \ldots$ of different primes by induction (so, the statement we're doing induction on is, "there are at least n different primes").

For our base case we take $n = 1$, and then take $p_1 = 2$, which is a prime.

For our induction step we suppose we have primes $p_1, \ldots, p_n$, and our job is to show that there's another prime.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

Consider the natural number

$$p_1 p_2 \cdots p_n + 1$$

obtained by multiplying all our primes so far and adding 1.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

Consider the natural number

$$p_1 p_2 \cdots p_n + 1$$

obtained by multiplying all our primes so far and adding 1. This number is not a multiple of p_1, because $p_1 \cdots p_n$ is: so $p_1 \cdots p_n + 1$ leaves a remainder of 1 when you divide by p_1.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

Consider the natural number

$$p_1 p_2 \cdots p_n + 1$$

obtained by multiplying all our primes so far and adding 1. This number is not a multiple of p_1, because $p_1 \cdots p_n$ is: so $p_1 \cdots p_n + 1$ leaves a remainder of 1 when you divide by p_1. Similarly, it's not a multiple of p_i for any $i = 1, \ldots, n$, because $p_1 \cdots p_n$ is, and so $p_1 \cdots p_n + 1$ leaves a remainder of 1 upon division by p_i.

How many primes?

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

Here's the proof, the way I prefer to think of it:

Proof.

Consider the natural number

$$p_1 p_2 \cdots p_n + 1$$

obtained by multiplying all our primes so far and adding 1.
This number is not a multiple of p_1, because $p_1 \cdots p_n$ is: so $p_1 \cdots p_n + 1$ leaves a remainder of 1 when you divide by p_1.
Similarly, it's not a multiple of p_i for any $i = 1, \ldots, n$, because $p_1 \cdots p_n$ is, and so $p_1 \cdots p_n + 1$ leaves a remainder of 1 upon division by p_i.
But as we proved this number has at least one prime factor: we can take our next prime p_{n+1} to be one such prime factor, and that completes the induction step.

Another proof

Another proof

Here's pretty much exactly the same proof, phrased in a slightly different way.

Another proof

Here's pretty much exactly the same proof, phrased in a slightly different way.

Proof (of the same theorem again).

We prove this by *contradiction*: we show that it's true by showing that the negation is absurd.
Indeed, suppose there were only finitely many primes, $p_1, \ldots, p_n$.
Then consider (as before) the natural number

$$p_1 \cdots p_n + 1.$$

This isn't divisible by any of the primes $p_1, \ldots, p_n$ (since it leaves a remainder of 1 upon division by any of them). But that's absurd, since we were assuming those were all the primes,
and we've proved that that every number can be written as a product of primes. □

On contradiction

On contradiction

Remark

Some people find proof by contradiction slightly startling when they see it first.

On contradiction

Remark

Some people find proof by contradiction slightly startling when they see it first.

In fact, it's perfectly familiar in daily life.

On contradiction

Remark

Some people find proof by contradiction slightly startling when they see it first.

In fact, it's perfectly familiar in daily life. When you find someone who disagrees with you, you show that you are right by pointing out that if you were wrong, then that would contradict something well-known to be correct.

On contradiction 2

On contradiction 2

From a logical perspective, it's all to do with the contrapositive.

On contradiction 2

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

On contradiction 2

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

Now, we proved that if there are only finitely many primes, then some number doesn't have a prime factor.

On contradiction 2

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

Now, we proved that if there are only finitely many primes, then some number doesn't have a prime factor. That's exactly $\neg P \Rightarrow \neg T$.

On contradiction 2

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

Now, we proved that if there are only finitely many primes, then some number doesn't have a prime factor. That's exactly $\neg P \Rightarrow \neg T$. But that means that its contrapositive $T \Rightarrow P$ is true.

On contradiction 2

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

Now, we proved that if there are only finitely many primes, then some number doesn't have a prime factor. That's exactly $\neg P \Rightarrow \neg T$. But that means that its contrapositive $T \Rightarrow P$ is true. And once we know that, then, since we know T is true, we also know P is true.

Comparing the proofs

Comparing the proofs

Remark

The second form above, the proof by contradiction, is a more standard form. It appears in the majority of textbooks (and maybe the majority of mathematicians' minds).

Comparing the proofs

Remark

The second form above, the proof by contradiction, is a more standard form. It appears in the majority of textbooks (and maybe the majority of mathematicians' minds).
This makes me sad, because it's not as good. The proof by contradiction spends all its time making fun of the idea that there might not be infinitely many primes; the first one just goes and builds them.

Comparing the proofs

Remark

The second form above, the proof by contradiction, is a more standard form. It appears in the majority of textbooks (and maybe the majority of mathematicians' minds).
This makes me sad, because it's not as good. The proof by contradiction spends all its time making fun of the idea that there might not be infinitely many primes; the first one just goes and builds them.

Remark

There are (quite a lot of) other proofs of Euclid's theorem, but Euclid himself probably only knew the way we've discussed.

Constructions

Constructions

That means that you can actually use the first proof to construct primes:

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$. It turns out that's not prime: in fact, $1807 = 13 \times 139$.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$. It turns out that's not prime: in fact, $1807 = 13 \times 139$. So we could take p_5 to be either 13 or 139...

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$. It turns out that's not prime: in fact, $1807 = 13 \times 139$. So we could take p_5 to be either 13 or 139...

This is genuinely a way of producing primes.

Constructions

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$. It turns out that's not prime: in fact, $1807 = 13 \times 139$. So we could take p_5 to be either 13 or 139...

This is genuinely a way of producing primes. Admittedly, it's not a very intelligent one.

A better method

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

1

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form.

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

1. Find the first untouched number and mark it as a prime.

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

1. Find the first untouched number and mark it as a prime.
2. Mark all its multiples as being composite.

[1] An *algorithm* is a method for calculating something.

The Sieve of Eratosthenes

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	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

As you can see, when we find a number uncrossed, it's because it has no factors that would have caused it to be crossed out, so it's prime.

More comments

More comments

Remark

The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them.

More comments

Remark

The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them. Unless we'd found a proof of Euclid's theorem, we could have nightmares that one day we'll find ourself crossing off all the remaining natural numbers and not finding any more primes.