MAS114: Lecture 9

James Cranch

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

2017–2018

Divisibility

Divisibility

In order to study division, we defined $a \mid b$ (for integers a and b) to mean "there exists an integer n such that $an = b$".

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 $a \mid 0$?

$\boxed{?}$

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

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

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

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

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

The trivial cases

It's worth sorting out the trivial cases:

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

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

  $\boxed{?}$

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:

Theorem

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

Primes are building blocks

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

Theorem

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

$\boxed{?}$

Primes are building blocks

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

Theorem

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

$\boxed{?}$

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).

Primes are building blocks

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

Theorem

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

$\boxed{?}$

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:

$$\boxed{?}$$

Questions about primes

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

$$\boxed{?}$$

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:

$$\boxed{?}$$

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:

$$\boxed{?}$$

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:

$\boxed{?}$

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:

$\boxed{?}$

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,

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,

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.

How many primes?

How many primes?

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

How many primes?

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

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

How many primes?

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

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?

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

Theorem (Euclid's theorem)

There are infinitely many prime numbers.

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

Proof.

$\boxed{?}$

$\square$

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).

$$\boxed{?}$$

$\square$

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.

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 can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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 can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can 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.