MAS114: Lecture 11

James Cranch

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

2021–2022

A general recipe

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there.

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there. We then have

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{k-1}, 0) = a_{k-1}.$$

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there. We then have

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{k-1}, 0) = a_{k-1}.$$

Let's write $d = \gcd(a, b)$ for this.

A general recipe

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.

We have $a_{k-4} = q_{k-4}a_{k-3} + a_{k-2}$, so $a_{k-2} = a_{k-4} - q_{k-4}a_{k-3}$, so substituting in we can write d as a linear combination of a_{k-4} and a_{k-3}.

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.

We have $a_{k-4} = q_{k-4}a_{k-3} + a_{k-2}$, so $a_{k-2} = a_{k-4} - q_{k-4}a_{k-3}$, so substituting in we can write d as a linear combination of a_{k-4} and a_{k-3}.

Proceeding in this way, we end up with d as a linear combination of a_0 and a_1: in other words, of a and b.

Bezout's Lemma

Bezout's Lemma

We've proved the following:

Bezout's Lemma

We've proved the following:

Proposition (Bezout's Lemma)

Let a and b be two integers with $\gcd(a, b) = d$.

Bezout's Lemma

We've proved the following:

Proposition (Bezout's Lemma)

Let a and b be two integers with $\gcd(a, b) = d$. Then there are integers m and n such that $ma + nb = d$. □

A better version

A better version

In fact, slightly more is true:

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

The "if" part: We must prove that, if $d \mid e$, then we can write e as a linear combination of a and b.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$*. Then, for an integer e, we can write e in the form* $e = ma + nb$ *if and only if* $d \mid e$*.*

Proof.

The "if" part: We must prove that, if $d \mid e$, then we can write e as a linear combination of a and b.
However, since $d \mid e$, we can write $e = dk$ for some k. Also, by the above Proposition we can write $d = ma + nb$ for some m and n. But then

$$e = dk = (mk)a + (nk)b,$$

as required.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

The "only if" part: We must prove that if $e = ma + nb$, then $d \mid e$. But, since $d = \gcd(a, b)$ we have $d \mid a$ and $d \mid b$, and hence also $d \mid ma$ and $d \mid nb$, and therefore $d \mid ma + nb$ as required. □

Factorisation into primes

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.
Of course we've proved that every positive integer can be written as a product of primes.

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Of course we've proved that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Of course we've proved that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Of course, we should be careful to say what we mean by "only one way". We certainly do have:

$$\begin{aligned} 420 &= 2 \times 2 \times 3 \times 5 \times 7 \\ &= 5 \times 2 \times 3 \times 7 \times 2 \\ &= 7 \times 5 \times 3 \times 2 \times 2, \quad \text{and so on\ldots} \end{aligned}$$

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Of course we've proved that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Of course, we should be careful to say what we mean by “only one way”. We certainly do have:

$$\begin{aligned} 420 &= 2 \times 2 \times 3 \times 5 \times 7 \\ &= 5 \times 2 \times 3 \times 7 \times 2 \\ &= 7 \times 5 \times 3 \times 2 \times 2, \quad \text{and so on...} \end{aligned}$$

Clearly, what we mean is that every positive integer can be written as a product of primes in only one way, where reordering doesn't count as different.

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Of course we've proved that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Of course, we should be careful to say what we mean by "only one way". We certainly do have:

$$\begin{aligned} 420 &= 2 \times 2 \times 3 \times 5 \times 7 \\ &= 5 \times 2 \times 3 \times 7 \times 2 \\ &= 7 \times 5 \times 3 \times 2 \times 2, \quad \text{and so on\ldots} \end{aligned}$$

Clearly, what we mean is that every positive integer can be written as a product of primes in only one way, where reordering doesn't count as different. Or, more precisely, that any two ways of writing a positive integer as a product of primes differ only by reordering.

Factorisation into primes

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes.

Of course we've proved that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Of course, we should be careful to say what we mean by "only one way". We certainly do have:

$$\begin{aligned} 420 &= 2 \times 2 \times 3 \times 5 \times 7 \\ &= 5 \times 2 \times 3 \times 7 \times 2 \\ &= 7 \times 5 \times 3 \times 2 \times 2, \quad \text{and so on...} \end{aligned}$$

Clearly, what we mean is that every positive integer can be written as a product of primes in only one way, where reordering doesn't count as different. Or, more precisely, that any two ways of writing a positive integer as a product of primes differ only by reordering. Mathematicians say, "in only one way, up to reordering".

Unique factorisation

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).
One wants to say something like "as the right-hand side is clearly divisible by 7, the left-hand side must be divisible by 7 too, but there isn't a 7 listed among the primes on the left".

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).
One wants to say something like "as the right-hand side is clearly divisible by 7, the left-hand side must be divisible by 7 too, but there isn't a 7 listed among the primes on the left".
But if we have $7 \mid (487 \times 205339)$, why must we have either $7 \mid 487$ or $7 \mid 205339$?

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).
One wants to say something like "as the right-hand side is clearly divisible by 7, the left-hand side must be divisible by 7 too, but there isn't a 7 listed among the primes on the left".
But if we have $7 \mid (487 \times 205339)$, why must we have either $7 \mid 487$ or $7 \mid 205339$? It wouldn't be true if 7 weren't a prime.

Unique factorisation

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).

One wants to say something like "as the right-hand side is clearly divisible by 7, the left-hand side must be divisible by 7 too, but there isn't a 7 listed among the primes on the left".

But if we have $7 \mid (487 \times 205339)$, why must we have either $7 \mid 487$ or $7 \mid 205339$? It wouldn't be true if 7 weren't a prime. But this is true for primes!

The key lemma

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Remark

This result is not only not obvious, we should expect it to be difficult.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Remark

This result is not only not obvious, we should expect it to be difficult. The definition of "p being prime" talks about what things divide p.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Remark

This result is not only not obvious, we should expect it to be difficult. The definition of "p being prime" talks about what things divide p. But this result says something about what things p divides, which is completely unrelated.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Suppose that $p \mid ab$, and consider $\gcd(p, a)$. Since $\gcd(p, a) \mid p$, we either have $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Suppose that $p \mid ab$, and consider $\gcd(p, a)$. Since $\gcd(p, a) \mid p$, we either have $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

If $\gcd(p, a) = p$, then as $\gcd(p, a) \mid a$, we have $p \mid a$.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Suppose that $p \mid ab$, and consider $\gcd(p, a)$. Since $\gcd(p, a) \mid p$, we either have $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

If $\gcd(p, a) = p$, then as $\gcd(p, a) \mid a$, we have $p \mid a$.

If $\gcd(p, a) = 1$, however, then by Bezout's Lemma, we know that there are integers m and n such that $mp + na = 1$. Now suppose we multiply both sides by b; we get $mpb + nab = b$.

The key lemma

Proposition

Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Suppose that $p \mid ab$, and consider $\gcd(p, a)$. Since $\gcd(p, a) \mid p$, we either have $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.
If $\gcd(p, a) = p$, then as $\gcd(p, a) \mid a$, we have $p \mid a$.
If $\gcd(p, a) = 1$, however, then by Bezout's Lemma, we know that there are integers m and n such that $mp + na = 1$. Now suppose we multiply both sides by b; we get $mpb + nab = b$.
Clearly $p \mid mpb$, and also we have $p \mid nab$ since we are supposing that $p \mid ab$. Hence $p \mid mpb + nab$, so $p \mid b$, as needed. □

Comments

Comments

Remark

The second part of this proof can in fact be used to show that, for any integers n, a and b, that if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

Comments

Remark

The second part of this proof can in fact be used to show that, for any integers n, a and b, that if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

We can also boost it to a result about a product of *lots* of terms:

Comments

Remark

The second part of this proof can in fact be used to show that, for any integers n, a and b, that if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

We can also boost it to a result about a product of *lots* of terms:

Proposition

Let p be a prime and let $a_1, \ldots, a_n$ be integers. Then if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

Comments

Remark

The second part of this proof can in fact be used to show that, for any integers n, a and b, that if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

We can also boost it to a result about a product of *lots* of terms:

Proposition

Let p be a prime and let $a_1, \ldots, a_n$ be integers. Then if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

This is an easy induction argument using the result above.

The “fundamental theorem”

The “fundamental theorem”

Now, equipped with that tricky result, we’re ready to prove the main result of this section:

The “fundamental theorem”

Now, equipped with that tricky result, we’re ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

The "fundamental theorem"

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

Proof.

We have shown that any positive integer can be written as a product of primes. We need to show that this expression is unique. We'll prove it by contradiction.

The "fundamental theorem"

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

Proof.

We have shown that any positive integer can be written as a product of primes. We need to show that this expression is unique.
We'll prove it by contradiction.
Suppose not: there is a number n with two genuinely different prime factorisations $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$. We can suppose that the p's and the q's have nothing in common (if $p_i = q_j$, then we can cancel them out and use $p_1 \cdots p_{i-1} p_{i+1} \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$, which is a smaller example).

The "fundamental theorem"

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

Proof.

The "fundamental theorem"

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

Proof.

Now, that means that p_1 is different to all of $q_1, q_2, \ldots, q_s$.

The "fundamental theorem"

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem (Fundamental Theorem of Arithmetic)

Any positive integer n can be written as a product of primes in exactly one way, up to reordering.

Proof.

Now, that means that p_1 is different to all of $q_1, q_2, \ldots, q_s$. We have $p_1 \mid n$, since $n = p_1 \cdots p_r$. But then we also have $p_1 \mid q_1 \cdots q_s$. But by our previous result, this means that $p_1 \mid q_j$ for some j. But, by the definition of q_j being a prime number, that means that $p_1 = q_j$, which we said didn't happen: that gives us our contradiction. □

Diophantine equations

Diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$.

Diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$. They're named after the ancient Greek mathematician Diophantus of Alexandria.

Diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$. They're named after the ancient Greek mathematician Diophantus of Alexandria.
An example of a diophantine equation is the Fermat equation for exponent 7:

$$x^7 + y^7 = z^7.$$

Diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$. They're named after the ancient Greek mathematician Diophantus of Alexandria.
An example of a diophantine equation is the Fermat equation for exponent 7:

$$x^7 + y^7 = z^7.$$

If we were interested in solutions to this equation over $\mathbb{R}$, the story would be really, really simple: we could take any x and any y we wanted and then just take

$$z = \sqrt[7]{x^7 + y^7}.$$

Diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$. They're named after the ancient Greek mathematician Diophantus of Alexandria.
An example of a diophantine equation is the Fermat equation for exponent 7:

$$x^7 + y^7 = z^7.$$

If we were interested in solutions to this equation over $\mathbb{R}$, the story would be really, really simple: we could take any x and any y we wanted and then just take

$$z = \sqrt[7]{x^7 + y^7}.$$

The Fermat equation becomes more interesting because of our inability to reliably take nth roots in $\mathbb{Z}$ or $\mathbb{N}$: which x and y can we take for which this recipe works?

Linear diophantine equations

Linear diophantine equations

While they're much easier, a similar thing is true of *linear diophantine equations*: equations of the form

$$ax + by = c,$$

where a, b and c are integer constants.

Linear diophantine equations

While they're much easier, a similar thing is true of *linear diophantine equations*: equations of the form

$$ax + by = c,$$

where a, b and c are integer constants.
Consider, for example, the equation $39x + 54y = 120$.

Linear diophantine equations

While they're much easier, a similar thing is true of *linear diophantine equations*: equations of the form

$$ax + by = c,$$

where a, b and c are integer constants.
Consider, for example, the equation $39x + 54y = 120$.
This equation would be simple if we cared about real solutions: we could take any x we like and then just take $y = (120 - 39x)/54$.

Linear diophantine equations

While they're much easier, a similar thing is true of *linear diophantine equations*: equations of the form

$$ax + by = c,$$

where a, b and c are integer constants.
Consider, for example, the equation $39x + 54y = 120$.
This equation would be simple if we cared about real solutions: we could take any x we like and then just take $y = (120 - 39x)/54$.
However, because we can't do division reliably in $\mathbb{Z}$, this recipe is not very helpful: how do we know which x will give us an integer y?
Next lecture, we'll see how to get a general solution.