MAS114: Lecture 11

James Cranch

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

2017–2018

Better yet

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n.

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b).

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!
Let's see how this works with an example.

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!

Let's see how this works with an example. We saw earlier that $\gcd(126, 70) = 14$, so we expect to be able to find integers m and n such that $126m + 70n = 14$.

The calculation

The calculation

Along the way we found that:

The calculation

Along the way we found that:

$$126 \quad = 1 \times 70 + 56, \tag{1}$$

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \tag{1}$$

$$70 = 1 \times 56 + 14. \tag{2}$$

Working through that backwards, we get that

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \tag{1}$$
$$70 = 1 \times 56 + 14. \tag{2}$$

Working through that backwards, we get that

$$14 = 1 \times 70 - 1 \times 56 \quad \text{(using (2))}$$

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \tag{1}$$
$$70 = 1 \times 56 + 14. \tag{2}$$

Working through that backwards, we get that

$$\begin{aligned} 14 &= 1 \times 70 - 1 \times 56 && \text{(using (2))} \\ &= 1 \times 70 - 1 \times (1 \times 126 - 1 \times 70) && \text{(using (1))} \end{aligned}$$

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \tag{1}$$
$$70 = 1 \times 56 + 14. \tag{2}$$

Working through that backwards, we get that

$$\begin{aligned} 14 &= 1 \times 70 - 1 \times 56 && \text{(using (2))} \\ &= 1 \times 70 - 1 \times (1 \times 126 - 1 \times 70) && \text{(using (1))} \\ &= 2 \times 70 - 1 \times 126. \end{aligned}$$

Another calculation

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$556 = 1 \times 296 + 260, \tag{3}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$556 = 1 \times 296 + 260, \tag{3}$$

$$296 = 1 \times 260 + 36, \tag{4}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$556 = 1 \times 296 + 260, \tag{3}$$

$$296 = 1 \times 260 + 36, \tag{4}$$

$$260 = 7 \times 36 + 8, \tag{5}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$4 = 36 - 4 \times 8 \qquad \text{(using (6))}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260 \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260 \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260\\ &= 29 \times 296 - 33 \times (556 - 296) && \text{(using (3))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260\\ &= 29 \times 296 - 33 \times (556 - 296) && \text{(using (3))}\\ &= 62 \times 296 - 33 \times 556. \end{aligned}$$

Bezout's Lemma

Bezout's Lemma

One can prove without too much difficulty that this technique always works (though we won't):

Bezout's Lemma

One can prove without too much difficulty that this technique always works (though we won't):

Proposition (Bezout's Lemma)

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

Bezout's Lemma

One can prove without too much difficulty that this technique always works (though we won't):

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.

?

□

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 shown 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 shown 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 shown 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:

?

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 shown 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:

?

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 shown 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:

?

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 shown 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:

?

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 $p \mid b$.

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.

Proof.

?

□

Comments

Comments

Remark

Exactly the same proof can 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

Exactly the same proof can 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

Exactly the same proof can 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

Exactly the same proof can 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.

?

□