MAS114: Lecture 13

James Cranch

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

2020–2021

Hello again!

Hello again!

Welcome back.

Hello again!

Welcome back.
Online tests start again tomorrow.

Now where were we?

Now where were we?

I had started to talk about the question of finding a general solution to $39x + 54y = 120$.

Using Euclid's algorithm

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$\gcd(54, 39)$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\gcd(54, 39) = \gcd(1 \times 39 + 15, 39)$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\gcd(54, 39) = \gcd(1 \times 39 + 15, 39) = \gcd(15, 39)$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\gcd(54, 39) = \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15)$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\ &= \gcd(2 \times 15 + 9, 15)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\ &= \gcd(2\times 15+9,15) = \gcd(9,15)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39)=\gcd(15,39)=\gcd(39,15)\\ &= \gcd(2\times 15+9,15)=\gcd(9,15)=\gcd(15,9)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\ &= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9)\\ &= \gcd(1\times 9+6,9)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\ &= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9)\\ &= \gcd(1\times 9+6,9) = \gcd(6,9)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39)=\gcd(15,39)=\gcd(39,15)\\ &= \gcd(2\times 15+9,15)=\gcd(9,15)=\gcd(15,9)\\ &= \gcd(1\times 9+6,9)=\gcd(6,9)=\gcd(9,6)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6)
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15) \\
&= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9) \\
&= \gcd(1\times 9+6,9) = \gcd(6,9) = \gcd(9,6) \\
&= \gcd(1\times 6+3,6) = \gcd(3,6)
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3)
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\
&= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9)\\
&= \gcd(1\times 9+6,9) = \gcd(6,9) = \gcd(9,6)\\
&= \gcd(1\times 6+3,6) = \gcd(3,6) = \gcd(6,3)\\
&= \gcd(2\times 3+0,3)
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\ &= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9)\\ &= \gcd(1\times 9+6,9) = \gcd(6,9) = \gcd(9,6)\\ &= \gcd(1\times 6+3,6) = \gcd(3,6) = \gcd(6,3)\\ &= \gcd(2\times 3+0,3) = \gcd(0,3)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3) \\
&= \gcd(2 \times 3 + 0, 3) = \gcd(0, 3) = 3.
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39)=\gcd(15,39)=\gcd(39,15)\\ &= \gcd(2\times 15+9,15)=\gcd(9,15)=\gcd(15,9)\\ &= \gcd(1\times 9+6,9)=\gcd(6,9)=\gcd(9,6)\\ &= \gcd(1\times 6+3,6)=\gcd(3,6)=\gcd(6,3)\\ &= \gcd(2\times 3+0,3)=\gcd(0,3)=3.\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$3$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$
\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3) \\
&= \gcd(2 \times 3 + 0, 3) = \gcd(0, 3) = 3.
\end{aligned}
$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$
3 = 9 - 6
$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39)=\gcd(15,39)=\gcd(39,15)\\ &= \gcd(2\times 15+9,15)=\gcd(9,15)=\gcd(15,9)\\ &= \gcd(1\times 9+6,9)=\gcd(6,9)=\gcd(9,6)\\ &= \gcd(1\times 6+3,6)=\gcd(3,6)=\gcd(6,3)\\ &= \gcd(2\times 3+0,3)=\gcd(0,3)=3.\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned}3 &= 9-6\\ &= 9-(15-9)\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54,39) &= \gcd(1\times 39+15, 39) = \gcd(15,39) = \gcd(39,15)\\
&= \gcd(2\times 15+9, 15) = \gcd(9,15) = \gcd(15,9)\\
&= \gcd(1\times 9+6, 9) = \gcd(6,9) = \gcd(9,6)\\
&= \gcd(1\times 6+3, 6) = \gcd(3,6) = \gcd(6,3)\\
&= \gcd(2\times 3+0, 3) = \gcd(0,3) = 3.
\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned}
3 &= 9-6\\
&= 9-(15-9) = 2\times 9 - 15
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54,39) &= \gcd(1\times 39+15,39) = \gcd(15,39) = \gcd(39,15)\\
&= \gcd(2\times 15+9,15) = \gcd(9,15) = \gcd(15,9)\\
&= \gcd(1\times 9+6,9) = \gcd(6,9) = \gcd(9,6)\\
&= \gcd(1\times 6+3,6) = \gcd(3,6) = \gcd(6,3)\\
&= \gcd(2\times 3+0,3) = \gcd(0,3) = 3.
\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned}
3 &= 9 - 6\\
&= 9 - (15 - 9) = 2\times 9 - 15\\
&= 2\times(39 - 2\times 15) - 15
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3) \\
&= \gcd(2 \times 3 + 0, 3) = \gcd(0, 3) = 3.
\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned}
3 &= 9 - 6 \\
&= 9 - (15 - 9) = 2 \times 9 - 15 \\
&= 2 \times (39 - 2 \times 15) - 15 = 2 \times 39 - 5 \times 15
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3) \\
&= \gcd(2 \times 3 + 0, 3) = \gcd(0, 3) = 3.
\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned}
3 &= 9 - 6 \\
&= 9 - (15 - 9) = 2 \times 9 - 15 \\
&= 2 \times (39 - 2 \times 15) - 15 = 2 \times 39 - 5 \times 15 \\
&= 2 \times 39 - 5 \times (54 - 39)
\end{aligned}$$

Using Euclid's algorithm

We've developed techniques to find *one* solution. Euclid's algorithm gives us that

$$\begin{aligned}\gcd(54,39) &= \gcd(1\times 39+15,39)=\gcd(15,39)=\gcd(39,15)\\ &= \gcd(2\times 15+9,15)=\gcd(9,15)=\gcd(15,9)\\ &= \gcd(1\times 9+6,9)=\gcd(6,9)=\gcd(9,6)\\ &= \gcd(1\times 6+3,6)=\gcd(3,6)=\gcd(6,3)\\ &= \gcd(2\times 3+0,3)=\gcd(0,3)=3.\end{aligned}$$

Then, we can work backwards to find a solution to $39x+54y=3$:

$$\begin{aligned}3 &= 9-6\\ &= 9-(15-9)=2\times 9-15\\ &= 2\times(39-2\times 15)-15=2\times 39-5\times 15\\ &= 2\times 39-5\times(54-39)=7\times 39-5\times 54.\end{aligned}$$

Putting that together

Putting that together

So

$$39 \times 7 + 54 \times (-5) = 3,$$

Putting that together

So

$$39 \times 7 + 54 \times (-5) = 3,$$

and we multiply both sides by 40 to get

$$39 \times 280 + 54 \times (-200) = 120,$$

Putting that together

So

$$39 \times 7 + 54 \times (-5) = 3,$$

and we multiply both sides by 40 to get

$$39 \times 280 + 54 \times (-200) = 120,$$

or in other words, that $x = 280$, $y = -200$ gives a solution.

Putting that together

So

$$39 \times 7 + 54 \times (-5) = 3,$$

and we multiply both sides by 40 to get

$$39 \times 280 + 54 \times (-200) = 120,$$

or in other words, that $x = 280$, $y = -200$ gives a solution. Now, you might wonder whether this is the *only* solution.

Other solutions?

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

This means that, as 18 divides the right-hand side, then we also have $18 \mid 13(x - x')$.

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

This means that, as 18 divides the right-hand side, then we also have $18 \mid 13(x - x')$. But since 13 and 18 are coprime, we have $18 \mid (x - x')$ by our remark earlier.

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

This means that, as 18 divides the right-hand side, then we also have $18 \mid 13(x - x')$. But since 13 and 18 are coprime, we have $18 \mid (x - x')$ by our remark earlier. So we can write $x - x' = 18k$.

Other solutions?

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

This means that, as 18 divides the right-hand side, then we also have $18 \mid 13(x - x')$. But since 13 and 18 are coprime, we have $18 \mid (x - x')$ by our remark earlier. So we can write $x - x' = 18k$. But then we can solve to get $y - y' = -13k$, and it's easy to check that any such k works.

Other solutions?

Other solutions?

Hence the general solution is

$$x = 280 - 18k, \qquad y = 13k - 200.$$

Other solutions?

Hence the general solution is

$$x = 280 - 18k, \qquad y = 13k - 200.$$

While I haven't stated (and certainly haven't proved) any theorems about it, this approach works perfectly well in general, as you can imagine.

Common divisors

Common divisors

Here's a useful result about common divisors.

Common divisors

Here's a useful result about common divisors.

Proposition

Let a and b be positive integers. Any common divisor of a and b is a divisor of the greatest common divisor.

Proof.

If $d \mid a$ and $d \mid b$, then $d \mid (a - qb)$ for any q. Hence d is a divisor of the numbers obtained after every step of Euclid's algorithm, and so it is a divisor of the gcd. □

Common divisors

Here's a useful result about common divisors.

Proposition

Let a and b be positive integers. Any common divisor of a and b is a divisor of the greatest common divisor.

Proof.

If $d \mid a$ and $d \mid b$, then $d \mid (a - qb)$ for any q. Hence d is a divisor of the numbers obtained after every step of Euclid's algorithm, and so it is a divisor of the gcd. □

We defined the gcd to be the greatest of all common divisors. This property is arguably a more natural one: this says that the gcd is somehow the "best" common divisor.

Common divisors

Here's a useful result about common divisors.

Proposition

Let a and b be positive integers. Any common divisor of a and b is a divisor of the greatest common divisor.

Proof.

If $d \mid a$ and $d \mid b$, then $d \mid (a - qb)$ for any q. Hence d is a divisor of the numbers obtained after every step of Euclid's algorithm, and so it is a divisor of the gcd. □

We defined the gcd to be the greatest of all common divisors. This property is arguably a more natural one: this says that the gcd is somehow the "best" common divisor.

As an unexpected advantage, if we think of the gcd as being defined in this way, then we can get that $\gcd(0, 0) = 0$. This was undefined previously.

More notation needed

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;
- even numbers;

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;
- even numbers;
- remainders upon division;

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;
- even numbers;
- remainders upon division;
- numbers of the form $4n + 1$ or $18k - 440$, and so on.

More notation needed

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;
- even numbers;
- remainders upon division;
- numbers of the form $4n + 1$ or $18k - 440$, and so on.

All these things look pretty similar, and it's time we got ourselves a language for discussing these things better.

Congruence

Congruence

Definition

We say that *a is congruent to b modulo m* if $m \mid (a - b)$.

Congruence

Definition

We say that a *is congruent to* b *modulo* m if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod* m.

Congruence

Definition

We say that a *is congruent to* b *modulo* m if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod* m.
We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a and b are congruent modulo m.

Congruence

Definition

We say that a *is congruent to* b *modulo* m if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod* m.
We use the notation
$$a \equiv b \pmod{m}$$
to indicate that a and b are congruent modulo m.

For example,
$$3167 \equiv 267 \pmod{100};$$

Congruence

Definition

We say that *a is congruent to b modulo m* if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod m*.

We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a and b are congruent modulo m.

For example,

$$3167 \equiv 267 \pmod{100};$$

indeed, the fact that these two positive integers have the same last two digits means that their difference is a multiple of 100.

Congruence

Definition

We say that *a is congruent to b modulo m* if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod m*.
We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a and b are congruent modulo m.

For example,

$$3167 \equiv 267 \pmod{100};$$

indeed, the fact that these two positive integers have the same last two digits means that their difference is a multiple of 100.
We can now say that an even number is a number congruent to 0 (modulo 2), and an odd number is a number congruent to 1 (modulo 2).

More uses of the words

More uses of the words

Rather than saying that "n is of the form $18k - 440$", we can say that "n is congruent to -440, modulo 18".

More uses of the words

Rather than saying that "n is of the form $18k - 440$", we can say that "n is congruent to -440, modulo 18".
Arguments about time frequently involve understandings of congruences. For example, I was born on a Sunday, and the closing ceremony of the 2012 Summer Olympics took place on a Sunday too. So the number of days since the former is congruent to the number of days since the latter, modulo 7.

More uses of the words

Rather than saying that "n is of the form $18k - 440$", we can say that "n is congruent to -440, modulo 18".

Arguments about time frequently involve understandings of congruences. For example, I was born on a Sunday, and the closing ceremony of the 2012 Summer Olympics took place on a Sunday too. So the number of days since the former is congruent to the number of days since the latter, modulo 7.

Notice that saying that a is congruent to 0, modulo m, is exactly the same as saying that a is a multiple of m (since it's saying that $m \mid (a - 0)$).

Congruence says numbers are somehow similar

Congruence says numbers are somehow similar

As we've defined it, a congruence modulo m doesn't say that two things are equal, just that their difference is a multiple of m.

Congruence says numbers are somehow similar

As we've defined it, a congruence modulo m doesn't say that two things are equal, just that their difference is a multiple of m.
But it does behave suspiciously like an equality, as we're about to see.