MAS114: Lecture 13

James Cranch

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

2021–2022

Hello again!

Hello again!

Welcome back.

Hello again!

Welcome back.
Online tests start again tomorrow.

Where were we?

Where were we?

We were just starting the subject of *modular arithmetic*, to give new language for discussing some things we keep seeing.

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.

Congruence facts

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$*;*

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$*;*

(b) *If* $a \equiv b \pmod{m}$*, then* $b \equiv a \pmod{m}$*;*

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$;

(b) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;

(c) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$;

(b) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;

(c) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;

(d) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$;

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$;

(b) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;

(c) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;

(d) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$;

(e) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a - c \equiv b - d \pmod{m}$;

Congruence facts

Proposition

Here are some properties of congruences, true for all integers:

(a) *We always have* $a \equiv a \pmod{m}$;

(b) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;

(c) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;

(d) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$;

(e) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a - c \equiv b - d \pmod{m}$;

(f) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$.

Proof.

Proof.

For (a): *(which says* $a \equiv a \pmod{m}$*)*

Proof.

For (a): *(which says* $a \equiv a \pmod{m}$*)*

Since $a - a = 0$, we have $m \mid (a - a)$.

Proof.

Proof.

For (b): *(which says that, if* $a \equiv b \pmod{m}$*, then* $b \equiv a \pmod{m}$*)*

Proof.

For (b): *(which says that, if* $a \equiv b \pmod{m}$*, then* $b \equiv a \pmod{m}$*)*
If $a \equiv b \pmod{m}$, we have $m \mid (a - b)$. But then $m \mid -(a - b)$, which says $m \mid (b - a)$, or in other words $b \equiv a \pmod{m}$.

Proof.

Proof.

For (c): *(which says that, if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$*)*

Proof.

For (c): *(which says that, if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$*, then* $a \equiv c \pmod{m}$*)*

As $a \equiv b \pmod{m}$, we have $m \mid (a - b)$; similarly as $b \equiv c \pmod{m}$, we have $m \mid (b - c)$.

Proof.

For (c): *(which says that, if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$*, then* $a \equiv c \pmod{m}$*)*
As $a \equiv b \pmod{m}$, we have $m \mid (a - b)$; similarly as $b \equiv c \pmod{m}$, we have $m \mid (b - c)$. But then

$$m \mid ((a - b) + (b - c)) = (a - c),$$

which says that $a \equiv c \pmod{m}$.

Proof.

Proof.

For (d): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$*)*

Proof.

For (d): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$*)*

As $a \equiv b \pmod{m}$, we can write $a - b = km$ for some integer k;

Proof.

For (d): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$*)*

As $a \equiv b \pmod{m}$, we can write $a - b = km$ for some integer k; similarly, as $c \equiv d \pmod{m}$, we can write $c - d = lm$ for some integer l.

Proof.

For (d): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$*)*

As $a \equiv b \pmod{m}$, we can write $a - b = km$ for some integer k; similarly, as $c \equiv d \pmod{m}$, we can write $c - d = lm$ for some integer l.

As a result,

$$(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m,$$

so $m \mid ((a + c) - (b + d))$, so $a + c \equiv b + d \pmod{m}$.

Proof.

Proof.

For (e): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a - c \equiv b - d \pmod{m}$*)*

Proof.

For (e): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a - c \equiv b - d \pmod{m}$*)*

As above, we can write $a - b = km$, and $c - d = lm$.

Proof.

For (e): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a - c \equiv b - d \pmod{m}$*)*
As above, we can write $a - b = km$, and $c - d = lm$. Then

$$(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m,$$

so $m \mid ((a - c) - (b - d))$, so $a - c \equiv b - d \pmod{m}$.

Proof.

Proof.

For (f): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$*)*

Proof.

For (f): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $ac \equiv bd \pmod{m}$*)*

As $a \equiv b \pmod{m}$, then we can write $a = b + km$ for some integer k (since $a - b$ is a multiple of m). Similarly, as $c \equiv d \pmod{m}$ we can write $c = d + lm$.

Proof.

For (f): *(which says that, if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $ac \equiv bd \pmod{m}$*)*

As $a \equiv b \pmod{m}$, then we can write $a = b + km$ for some integer k (since $a - b$ is a multiple of m). Similarly, as $c \equiv d \pmod{m}$ we can write $c = d + lm$.

But then $ac = (b + km)(d + lm) = bd + (bl + dk + klm)m$, which says that $ac \equiv bd \pmod{m}$. □

The moral of that

The moral of that

I interpret all that as saying that, provided you're careful and justify any unusual steps, the language of congruences behaves somewhat like equality.

The moral of that

I interpret all that as saying that, provided you're careful and justify any unusual steps, the language of congruences behaves somewhat like equality. (In particular, our choice of notation, looking a bit like an overenthusiastic equals sign, wasn't a bad choice).

The moral of that

I interpret all that as saying that, provided you're careful and justify any unusual steps, the language of congruences behaves somewhat like equality. (In particular, our choice of notation, looking a bit like an overenthusiastic equals sign, wasn't a bad choice). This philosophy will get heavy use from now on!

Manipulating congruences

Manipulating congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”.

Manipulating congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. We can now give an systematic explanation of facts like these, using modular arithmetic.

Manipulating congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. We can now give an systematic explanation of facts like these, using modular arithmetic.

If a is odd and b is even then

$$a \equiv 1 \pmod 2$$
$$b \equiv 0 \pmod 2$$

Manipulating congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. We can now give an systematic explanation of facts like these, using modular arithmetic.

If a is odd and b is even then

$$a \equiv 1 \pmod 2$$
$$b \equiv 0 \pmod 2$$

and then (because we can multiply congruences)

$$ab \equiv 1 \times 0 = 0 \pmod 2,$$

which says that ab is even.

Manipulating congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. We can now give an systematic explanation of facts like these, using modular arithmetic.

If a is odd and b is even then

$$a \equiv 1 \pmod 2$$
$$b \equiv 0 \pmod 2$$

and then (because we can multiply congruences)

$$ab \equiv 1 \times 0 = 0 \pmod 2,$$

which says that ab is even.

Since we can add congruences, we can give similar explanations of addition facts (like “an odd number plus an even number is an odd number”).

Manipulating congruences

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.
For example, if $a \equiv 3 \pmod 7$, and $b \equiv 4 \pmod 7$, then $ab \equiv 12$

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.
For example, if $a \equiv 3 \pmod 7$, and $b \equiv 4 \pmod 7$, then $ab \equiv 12 \equiv 5 \pmod 7$.

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.
For example, if $a \equiv 3 \pmod 7$, and $b \equiv 4 \pmod 7$, then $ab \equiv 12 \equiv 5 \pmod 7$.
We can use these ideas to make multiplication tables of congruences. For example, here's a multiplication table modulo 5:

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.
For example, if $a \equiv 3 \pmod 7$, and $b \equiv 4 \pmod 7$, then $ab \equiv 12 \equiv 5 \pmod 7$.
We can use these ideas to make multiplication tables of congruences. For example, here's a multiplication table modulo 5:

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Manipulating congruences

The language of congruences gives us ways of writing down similar facts about other moduli.
For example, if $a \equiv 3 \pmod 7$, and $b \equiv 4 \pmod 7$, then $ab \equiv 12 \equiv 5 \pmod 7$.
We can use these ideas to make multiplication tables of congruences. For example, here's a multiplication table modulo 5:

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So, for example, this tells us that $2 \times 4 \equiv 3 \pmod 5$.

Some comments on that

Some comments on that

Notice that this shares some features with a usual multiplication table.

Some comments on that

Notice that this shares some features with a usual multiplication table. For example, there is a column and a row of zeroes, because if you multiply something by something congruent to zero mod 5, you get something congruent to zero mod 5.

Some comments on that

Notice that this shares some features with a usual multiplication table. For example, there is a column and a row of zeroes, because if you multiply something by something congruent to zero mod 5, you get something congruent to zero mod 5. Also, multiplying by 1 doesn't change anything.

Some comments on that

Notice that this shares some features with a usual multiplication table. For example, there is a column and a row of zeroes, because if you multiply something by something congruent to zero mod 5, you get something congruent to zero mod 5. Also, multiplying by 1 doesn't change anything.
Why do we only need to consider rows and columns numbered from 0 to 4? This is a consequence of division with remainder.

Special forms

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

We'll show that such a number exists, first, and then we'll show that it's unique.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

We'll show that such a number exists, first, and then we'll show that it's unique.

By division with remainder, we can write $a = qb + r$ for some integer q and some integer r with $0 \leqslant r < b$.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

We'll show that such a number exists, first, and then we'll show that it's unique.

By division with remainder, we can write $a = qb + r$ for some integer q and some integer r with $0 \leqslant r < b$. But then that says that $a - r = qb$, and hence $a \equiv r \pmod{b}$. That shows that a is congruent to some number in that set.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

Now, we'll prove uniqueness. In fact we never proved that division with a *unique* remainder was possible, so let's mend that now.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

Now, we'll prove uniqueness. In fact we never proved that division with a *unique* remainder was possible, so let's mend that now. Suppose that $a \equiv r_1 \pmod{b}$ and also $a \equiv r_2 \pmod{b}$. Then $0 = a - a \equiv r_2 - r_1 \pmod{b}$ by subtracting, so $b \mid (r_2 - r_1)$.

Special forms

Proposition

Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set

$$\{0, 1, \ldots, b-1\}.$$

Proof.

Now, we'll prove uniqueness. In fact we never proved that division with a *unique* remainder was possible, so let's mend that now. Suppose that $a \equiv r_1 \pmod{b}$ and also $a \equiv r_2 \pmod{b}$. Then $0 = a - a \equiv r_2 - r_1 \pmod{b}$ by subtracting, so $b \mid (r_2 - r_1)$. But since $0 \leqslant r_1 < b$ and $0 \leqslant r_2 < b$, we have

$$-b = 0 - b < r_2 - r_1 < b - 0 = b.$$

So $r_2 - r_1$ is a multiple of b strictly between $-b$ and b: it must be zero, so $r_1 = r_2$, which proves uniqueness. $\square$

Residue classes

Residue classes

This proposition has a lot of consequences.

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to.

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);
- $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, all congruent to 1 (mod 5);

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);
- $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, all congruent to 1 (mod 5);
- $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$, all congruent to 2 (mod 5);

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);
- $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, all congruent to 1 (mod 5);
- $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$, all congruent to 2 (mod 5);
- $\{\ldots, -7, -2, 3, 8, 13, \ldots\}$, all congruent to 3 (mod 5);

Residue classes

This proposition has a lot of consequences.
It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);
- $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, all congruent to 1 (mod 5);
- $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$, all congruent to 2 (mod 5);
- $\{\ldots, -7, -2, 3, 8, 13, \ldots\}$, all congruent to 3 (mod 5);
- $\{\ldots, -6, -1, 4, 9, 14, \ldots\}$, all congruent to 4 (mod 5).