MAS114: Lecture 14

James Cranch

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

2020–2021

Online tests

Online tests

A new online test will be released later; we're back to normal with them.

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).

About congruence classes

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b - 1$).

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0, 1, 2, 3, 4, 5, 6\}$, there's nothing much special about that set.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0, 1, 2, 3, 4, 5, 6\}$, there's nothing much special about that set. It's also true that every number is congruent (modulo 7) to a unique number in the set $\{1, 2, 3, 4, 5, 6, 7\}$.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0, 1, 2, 3, 4, 5, 6\}$, there's nothing much special about that set. It's also true that every number is congruent (modulo 7) to a unique number in the set $\{1, 2, 3, 4, 5, 6, 7\}$. And it's also true that every number is congruent (modulo 7) to a unique number in the set $\{-3, -2, -1, 0, 1, 2, 3\}$.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0, 1, 2, 3, 4, 5, 6\}$, there's nothing much special about that set. It's also true that every number is congruent (modulo 7) to a unique number in the set $\{1, 2, 3, 4, 5, 6, 7\}$. And it's also true that every number is congruent (modulo 7) to a unique number in the set $\{-3, -2, -1, 0, 1, 2, 3\}$. And, in fact, I can think of situations where all those facts are useful.

About congruence classes

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, which in some languages is written "%", which gives the remainder upon division (so that $a\%b$ is an integer between 0 and $b-1$). So they say, for example, that $137\%100 = 37$.

This works fairly well for the computer programmers, but for us it's a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0,1,2,3,4,5,6\}$, there's nothing much special about that set. It's also true that every number is congruent (modulo 7) to a unique number in the set $\{1,2,3,4,5,6,7\}$. And it's also true that every number is congruent (modulo 7) to a unique number in the set $\{-3,-2,-1,0,1,2,3\}$. And, in fact, I can think of situations where all those facts are useful.

So it's important we just think of the unique number in $\{0,\ldots,b-1\}$ as just one out of many equally good ways of describing our number, up to congruence modulo b.

The arithmetic of congruence classes

The arithmetic of congruence classes

Next semester, you'll come to regard the integers, considered up to congruence modulo m, as a system of numbers in its own right (and why not?

The arithmetic of congruence classes

Next semester, you'll come to regard the integers, considered up to congruence modulo m, as a system of numbers in its own right (and why not? We can add them and subtract them and multiply them, all considered only up to congruence modulo m).

The arithmetic of congruence classes

Next semester, you'll come to regard the integers, considered up to congruence modulo m, as a system of numbers in its own right (and why not? We can add them and subtract them and multiply them, all considered only up to congruence modulo m). This system of numbers is commonly called $\mathbb{Z}/m\mathbb{Z}$ (for reasons which will remain obscure at least for a year or two more).

The arithmetic of congruence classes

Next semester, you'll come to regard the integers, considered up to congruence modulo m, as a system of numbers in its own right (and why not? We can add them and subtract them and multiply them, all considered only up to congruence modulo m). This system of numbers is commonly called $\mathbb{Z}/m\mathbb{Z}$ (for reasons which will remain obscure at least for a year or two more).
So, for example, the system $\mathbb{Z}/2\mathbb{Z}$ consists of two "numbers" which could be called "even" and "odd" (or 0 and 1), subject to the arithmetic laws you'd expect (like even $+$ odd $=$ odd).

The arithmetic of congruence classes

The arithmetic of congruence classes

This is novel in one important sense.

The arithmetic of congruence classes

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

The arithmetic of congruence classes

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

But $\mathbb{Z}/m\mathbb{Z}$ doesn't seem to work like this in this framework. It's related to $\mathbb{Z}$, but doesn't really live inside it.

The arithmetic of congruence classes

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

But $\mathbb{Z}/m\mathbb{Z}$ doesn't seem to work like this in this framework. It's related to $\mathbb{Z}$, but doesn't really live inside it. Similarly, the set of "times of day" isn't a subset of the set of times: for example, there's no one special point of time in history called "2pm", just many examples of 2pm on many different days.

The arithmetic of congruence classes

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

But $\mathbb{Z}/m\mathbb{Z}$ doesn't seem to work like this in this framework. It's related to $\mathbb{Z}$, but doesn't really live inside it. Similarly, the set of "times of day" isn't a subset of the set of times: for example, there's no one special point of time in history called "2pm", just many examples of 2pm on many different days.

In the case where $m = 2$, you're probably comfortable with the fact that "odd" and "even" form something like a system of numbers (because you can add them and subtract them and multiply them), but while they've obviously got something to do with $\mathbb{Z}$, there's no one integer called "odd" and no one integer called "even".

The arithmetic of congruence classes

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

But $\mathbb{Z}/m\mathbb{Z}$ doesn't seem to work like this in this framework. It's related to $\mathbb{Z}$, but doesn't really live inside it. Similarly, the set of "times of day" isn't a subset of the set of times: for example, there's no one special point of time in history called "2pm", just many examples of 2pm on many different days.

In the case where $m = 2$, you're probably comfortable with the fact that "odd" and "even" form something like a system of numbers (because you can add them and subtract them and multiply them), but while they've obviously got something to do with $\mathbb{Z}$, there's no one integer called "odd" and no one integer called "even".

Modular arithmetic, to other moduli, is similar (we just don't have clever names like "even" and "odd").

Describing numbers by congruences

Describing numbers by congruences

We've now laid the foundations of *modular arithmetic*, the study of congruences.

Describing numbers by congruences

We've now laid the foundations of *modular arithmetic*, the study of congruences. After all that philosophy, we should do some sums.

Describing numbers by congruences

We've now laid the foundations of *modular arithmetic*, the study of congruences. After all that philosophy, we should do some sums. The set of all solutions to $x \equiv 3 \pmod{7}$ seems like a perfectly explicit description of a class of numbers: it's a congruence class modulo 7, the class of numbers of the form $7n + 3$.

Describing numbers by congruences

We've now laid the foundations of *modular arithmetic*, the study of congruences. After all that philosophy, we should do some sums. The set of all solutions to $x \equiv 3 \pmod{7}$ seems like a perfectly explicit description of a class of numbers: it's a congruence class modulo 7, the class of numbers of the form $7n + 3$. So we can start listing them easily:

$$\ldots, -11, -4, 3, 10, 17, \ldots.$$

Solving congruences

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod{7}$?

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod{7}$?
That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod{7}$?
That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.
However, we can get a more satisfactory list just using techniques we already know.

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod 7$?
That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.
However, we can get a more satisfactory list just using techniques we already know. The condition $5x \equiv 3 \pmod 7$ says that $7 \mid 5x - 3$, which in turn says that $7k = 5x - 3$ for some k.
Rearranging, that says that $5x - 7k = 3$.

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod 7$?
That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.
However, we can get a more satisfactory list just using techniques we already know. The condition $5x \equiv 3 \pmod 7$ says that $7 \mid 5x - 3$, which in turn says that $7k = 5x - 3$ for some k.
Rearranging, that says that $5x - 7k = 3$. But we *know* how to get a general solution for those!

Solving congruences

But what is the set of solutions to $5x \equiv 3 \pmod 7$?
That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.
However, we can get a more satisfactory list just using techniques we already know. The condition $5x \equiv 3 \pmod 7$ says that $7 \mid 5x - 3$, which in turn says that $7k = 5x - 3$ for some k.
Rearranging, that says that $5x - 7k = 3$. But we *know* how to get a general solution for those!
Indeed, we find that $\gcd(5, 7) = 1$, and as $1 \mid 3$ there are solutions.
First we try to find a single one.

Harder equations

Harder equations

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$.

Harder equations

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$. This means (by tripling both sides) that a solution to $5x - 7k = 3$ is given by $x = 9, k = 6$.

Harder equations

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$. This means (by tripling both sides) that a solution to $5x - 7k = 3$ is given by $x = 9, k = 6$.
To find other solutions, we subtract $5 \times 9 - 7 \times 6 = 3$ from $5x - 7k = 3$ to get $5(x - 9) - 7(k - 6) = 0$.

Harder equations

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$. This means (by tripling both sides) that a solution to $5x - 7k = 3$ is given by $x = 9, k = 6$.

To find other solutions, we subtract $5 \times 9 - 7 \times 6 = 3$ from $5x - 7k = 3$ to get $5(x - 9) - 7(k - 6) = 0$.

Hence $5(x - 9) = 7(k - 6)$, so $7 \mid 5(x - 9)$. As 7 and 5 are coprime, this means that $7 \mid (x - 9)$.

Harder equations

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$. This means (by tripling both sides) that a solution to $5x - 7k = 3$ is given by $x = 9, k = 6$.

To find other solutions, we subtract $5 \times 9 - 7 \times 6 = 3$ from $5x - 7k = 3$ to get $5(x - 9) - 7(k - 6) = 0$.

Hence $5(x - 9) = 7(k - 6)$, so $7 \mid 5(x - 9)$. As 7 and 5 are coprime, this means that $7 \mid (x - 9)$. So it's equivalent to $x \equiv 2 \pmod 7$, which *is* a nice description!

Division

Division

We can regard linear equations in modular arithmetic as asking about *division*.

Division

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking “can we divide 3 by 5”?

Division

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking "can we divide 3 by 5"? So the fact that $2 \times 5 \equiv 3 \pmod{7}$ might be regarded as saying that we *can* divide 3 by 5 (modulo 7), and we get 2 when we do so.

Division

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking "can we divide 3 by 5"? So the fact that $2 \times 5 \equiv 3 \pmod 7$ might be regarded as saying that we *can* divide 3 by 5 (modulo 7), and we get 2 when we do so.
But division in modular arithmetic is more complicated than in the integers.

Division

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking "can we divide 3 by 5"? So the fact that $2 \times 5 \equiv 3 \pmod 7$ might be regarded as saying that we *can* divide 3 by 5 (modulo 7), and we get 2 when we do so.
But division in modular arithmetic is more complicated than in the integers. Of course, integer division is unique where it exists.

Division

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking "can we divide 3 by 5"? So the fact that $2 \times 5 \equiv 3 \pmod 7$ might be regarded as saying that we *can* divide 3 by 5 (modulo 7), and we get 2 when we do so.
But division in modular arithmetic is more complicated than in the integers. Of course, integer division is unique where it exists. In other words, if I choose integers a and b (with b nonzero) and ask about integer solutions to

$$ax = b,$$

then two things can happen: either there is a unique solution (as with $3x = 6$), or there's no solution at all (as with $4x = 7$).

Division in modular arithmetic

Division in modular arithmetic

That's not true in modular arithmetic, as the following examples show:

Division in modular arithmetic

That's not true in modular arithmetic, as the following examples show:

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 6$?

  None: the lhs is even and the rhs odd.

Division in modular arithmetic

That's not true in modular arithmetic, as the following examples show:

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 6$?

  None: the lhs is even and the rhs odd.

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 7$?

  One: $x \equiv 6 \pmod 7$.

Division in modular arithmetic

That's not true in modular arithmetic, as the following examples show:

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 6$?

  None: the lhs is even and the rhs odd.

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 7$?

  One: $x \equiv 6 \pmod 7$.

- How many residue classes of solutions are there to $2x \equiv 6 \pmod 8$?

  Two: $x \equiv 3 \pmod 8$ *and* $x \equiv 7 \pmod 8$.

Division in modular arithmetic

That's not true in modular arithmetic, as the following examples show:

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 6$?

  None: the lhs is even and the rhs odd.

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 7$?

  One: $x \equiv 6 \pmod 7$.

- How many residue classes of solutions are there to $2x \equiv 6 \pmod 8$?

  Two: $x \equiv 3 \pmod 8$ *and* $x \equiv 7 \pmod 8$.

- How many residue classes of solutions are there to $4x \equiv 4 \pmod 8$?

  Four: $x \equiv 1, 3, 5, 7 \pmod 8$.