MAS114: Lecture 14

James Cranch

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

2021–2022

Online tests

Online tests

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

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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 $137\%100 = 37$, and $7\%2 = 1$.

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; or 1 and 2), 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 (and the same goes for "days of the week", and "months of the year").

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 (and the same goes for "days of the week", and "months of the year").

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 (and the same goes for "days of the week", and "months of the year").

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

Cancellation in modular arithmetic

Cancellation in modular arithmetic

Even if you don't want to do division in modular arithmetic, you still have to be careful about *cancellation*.

Cancellation in modular arithmetic

Even if you don't want to do division in modular arithmetic, you still have to be careful about *cancellation*.
In ordinary arithmetic over the integers, we know that $ax = ay$ implies $x = y$ (provided that a isn't zero, of course).

Cancellation in modular arithmetic

Even if you don't want to do division in modular arithmetic, you still have to be careful about *cancellation*.
In ordinary arithmetic over the integers, we know that $ax = ay$ implies $x = y$ (provided that a isn't zero, of course). This is true even though we don't know how to divide integers in general.

Cancellation in modular arithmetic

Even if you don't want to do division in modular arithmetic, you still have to be careful about *cancellation*.
In ordinary arithmetic over the integers, we know that $ax = ay$ implies $x = y$ (provided that a isn't zero, of course). This is true even though we don't know how to divide integers in general.
But we can't always cancel in modular arithmetic: the third example above tells (for example) that $2 \cdot 3 \equiv 2 \cdot 7 \pmod 8$, but that $3 \not\equiv 7 \pmod 8$.

Multiplying to get 1

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

We deal with existence first.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

We deal with existence first.
Using Bezout's lemma, we know we can find integers b and c such that

$$ab + mc = 1$$

if and only if $\gcd(a, m) \mid 1$.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

We deal with existence first.
Using Bezout's lemma, we know we can find integers b and c such that

$$ab + mc = 1$$

if and only if $\gcd(a, m) \mid 1$.
But $\gcd(a, m) \mid 1$ if and only if $\gcd(a, m) = 1$, and the equation $ab + mc = 1$ says exactly that $ab \equiv 1 \pmod{m}$.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

Now we deal with uniqueness.

Multiplying to get 1

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things in modular arithmetic.

Proposition

Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.
When such a number b does exist, it's unique (modulo m).

Proof.

Now we deal with uniqueness.
Suppose that we have two numbers b and b' such that $ab \equiv 1 \pmod{m}$ and $ab' \equiv 1 \pmod{m}$. Then

$$b \equiv b1 \equiv b(ab') \equiv (ba)b' \equiv 1b' \equiv b' \pmod{m},$$

which shows uniqueness modulo m. □