

# MAS114: Lecture 13

James Cranch

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

2017–2018

By way of a reminder

## By way of a reminder

We'd been working with *divisibility*: for integers  $m$ ,  $n$ , we defined  $m \mid n$  to mean that there exists an integer  $k$  such that  $mk = n$ .

## By way of a reminder

We'd been working with *divisibility*: for integers  $m, n$ , we defined  $m \mid n$  to mean that there exists an integer  $k$  such that  $mk = n$ .  
More recently, we defined *congruence*: for integers  $a, b$  and  $n$ , we defined  $a \equiv b \pmod{n}$  to mean  $n \mid (a - b)$ .

## By way of a reminder

We'd been working with *divisibility*: for integers  $m, n$ , we defined  $m \mid n$  to mean that there exists an integer  $k$  such that  $mk = n$ .  
More recently, we defined *congruence*: for integers  $a, b$  and  $n$ , we defined  $a \equiv b \pmod{n}$  to mean  $n \mid (a - b)$ .  
We'd just proved some sensible things about it.

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).

# Multiplying congruences

# Multiplying congruences

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

# Multiplying congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. Being odd or even is about being congruent to 1 or 0 modulo 2.

## Multiplying congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. Being odd or even is about being congruent to 1 or 0 modulo 2. The language of congruences gives us ways of writing down similar facts about other moduli: for example, “a number congruent to 3 (mod 7) times a number congruent to 4 (mod 7) is a number congruent to 12 (mod 7) and hence to 5 (mod 7)”.

## Multiplying congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. Being odd or even is about being congruent to 1 or 0 modulo 2. The language of congruences gives us ways of writing down similar facts about other moduli: for example, “a number congruent to 3 (mod 7) times a number congruent to 4 (mod 7) is a number congruent to 12 (mod 7) and hence to 5 (mod 7)”.

In fact, we can use this ideas to make multiplication tables of congruences. For example, here’s a multiplication table modulo 5:

## Multiplying congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. Being odd or even is about being congruent to 1 or 0 modulo 2. The language of congruences gives us ways of writing down similar facts about other moduli: for example, “a number congruent to 3 (mod 7) times a number congruent to 4 (mod 7) is a number congruent to 12 (mod 7) and hence to 5 (mod 7)”.

In fact, we can use this ideas to make multiplication tables of congruences. For example, here’s a multiplication table modulo 5:



## Multiplying congruences

Back at school, you probably learned facts like “an odd number times an even number is an even number”. Being odd or even is about being congruent to 1 or 0 modulo 2. The language of congruences gives us ways of writing down similar facts about other moduli: for example, “a number congruent to 3 (mod 7) times a number congruent to 4 (mod 7) is a number congruent to 12 (mod 7) and hence to 5 (mod 7)”.

In fact, we can use this ideas to make multiplication tables of congruences. For example, here’s a multiplication table modulo 5:



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.

In the above multiplication table, we managed to write every number congruent to 0, 1, 2, 3 or 4 modulo 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.

In the above multiplication table, we managed to write every number congruent to 0, 1, 2, 3 or 4 modulo 5. Is this a general feature?

## 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.

In the above multiplication table, we managed to write every number congruent to 0, 1, 2, 3 or 4 modulo 5. Is this a general feature? Yes, it is, and it turns out to be a consequence of our earlier observation on 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*

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

# 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*

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

Proof.



# 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  $\{0, \dots, b - 1\}$  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  $\{0, \dots, b - 1\}$  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  $\{0, \dots, b - 1\}$  they're congruent to. So, for  $b = 5$ , we divide the integers into:

- ▶  $\{\dots, -10, -5, 0, 5, 10, \dots\}$ , 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  $\{0, \dots, b - 1\}$  they're congruent to. So, for  $b = 5$ , we divide the integers into:

- ▶  $\{\dots, -10, -5, 0, 5, 10, \dots\}$ , all congruent to 0 (mod 5);
- ▶  $\{\dots, -9, -4, 1, 6, 11, \dots\}$ , 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  $\{0, \dots, b - 1\}$  they're congruent to. So, for  $b = 5$ , we divide the integers into:

- ▶  $\{\dots, -10, -5, 0, 5, 10, \dots\}$ , all congruent to 0 (mod 5);
- ▶  $\{\dots, -9, -4, 1, 6, 11, \dots\}$ , all congruent to 1 (mod 5);
- ▶  $\{\dots, -8, -3, 2, 7, 12, \dots\}$ , 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  $\{0, \dots, b - 1\}$  they're congruent to. So, for  $b = 5$ , we divide the integers into:

- ▶  $\{\dots, -10, -5, 0, 5, 10, \dots\}$ , all congruent to 0 (mod 5);
- ▶  $\{\dots, -9, -4, 1, 6, 11, \dots\}$ , all congruent to 1 (mod 5);
- ▶  $\{\dots, -8, -3, 2, 7, 12, \dots\}$ , all congruent to 2 (mod 5);
- ▶  $\{\dots, -7, -2, 3, 8, 13, \dots\}$ , 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  $\{0, \dots, b - 1\}$  they're congruent to. So, for  $b = 5$ , we divide the integers into:

- ▶  $\{\dots, -10, -5, 0, 5, 10, \dots\}$ , all congruent to 0 (mod 5);
- ▶  $\{\dots, -9, -4, 1, 6, 11, \dots\}$ , all congruent to 1 (mod 5);
- ▶  $\{\dots, -8, -3, 2, 7, 12, \dots\}$ , all congruent to 2 (mod 5);
- ▶  $\{\dots, -7, -2, 3, 8, 13, \dots\}$ , all congruent to 3 (mod 5);
- ▶  $\{\dots, -6, -1, 4, 9, 14, \dots\}$ , 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ).

## 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

## 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ . This works fairly well for the computer programmers, but I find it 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

This works fairly well for the computer programmers, but I find it 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

This works fairly well for the computer programmers, but I find it 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

This works fairly well for the computer programmers, but I find it 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

This works fairly well for the computer programmers, but I find it 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, also called “mod”, which gives the remainder upon division (so that  $a \bmod b$  is an integer between 0 and  $b$ ). So they say, for example, that  $137 \bmod 100 = 37$ .

This works fairly well for the computer programmers, but I find it 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  $\{0, \dots, b - 1\}$  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).

This is novel in one important sense.

# 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).

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

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).

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

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).

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, "times of day" aren't a subset 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 “odd” and “even”

# The arithmetic of “odd” and “even”

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 “odd” and “even”

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.

# Easy equations

# Easy equations

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

## Easy equations

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

## Easy equations

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  $7n + 3$ .

## Easy equations

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:

$$\dots, -11, -4, 3, 10, 17, \dots$$

# Harder equations

## Harder equations

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

## Harder equations

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.

## Harder equations

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.

## Harder equations

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  $5x - 7k = 3$ .

## Harder equations

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!

## Harder equations

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  $x \equiv 9 \pmod{7}$ , which *is* a nice description!