MAS114: Lecture 14

James Cranch

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

2017–2018

Online tests

Online tests

Online tests start again this week.

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 $2x \equiv 5 \pmod 6$?

?

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 $2x \equiv 5 \pmod 6$?

$\boxed{?}$

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

$\boxed{?}$

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 $2x \equiv 5 \pmod 6$?

$$\boxed{?}$$

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

$$\boxed{?}$$

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

$$\boxed{?}$$

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 $2x \equiv 5 \pmod 6$?

$\boxed{?}$

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

$\boxed{?}$

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

$\boxed{?}$

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

$\boxed{?}$

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.

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.

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.

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.

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.

?

□

Modular inverses

Modular inverses

When there is a number b such that $ab \equiv 1 \pmod{m}$, we call it the *inverse* of a, modulo m (and we say that a is *invertible*).

Modular inverses

When there is a number b such that $ab \equiv 1 \pmod{m}$, we call it the *inverse* of a, modulo m (and we say that a is *invertible*). We write a^{-1} for the inverse of a.

Modular inverses

When there is a number b such that $ab \equiv 1 \pmod{m}$, we call it the *inverse* of a, modulo m (and we say that a is *invertible*). We write a^{-1} for the inverse of a.

Notice that, as a consequence modular arithmetic modulo a prime p is *fantastically* well-behaved: any nonzero residue $a \not\equiv 0 \pmod{p}$ has an inverse (since we have $\gcd(a, p) = 1$ unless a is a multiple of p).

Some inverses mod m

Some inverses mod m

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.

Some inverses mod m

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.
There are a few exceptions:

Some inverses mod m

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.
There are a few exceptions:

- The inverse of 1 modulo m is always

$$\boxed{?}$$

Some inverses mod m

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.
There are a few exceptions:

- The inverse of 1 modulo m is always

$$\boxed{?}$$

- The inverse of -1 modulo m is always

$$\boxed{?}$$

Some inverses mod m

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.
There are a few exceptions:

- The inverse of 1 modulo m is always

  $\boxed{?}$

- The inverse of -1 modulo m is always

  $\boxed{?}$

- If m is odd, then 2 is invertible modulo m, because $\gcd(m, 2) = 1$. The inverse is:

  $\boxed{?}$