MAS114: Lecture 15

James Cranch

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

2017–2018

The inverse: reminder

The inverse: reminder

In the last lecture, I defined the *inverse* a^{-1} of a number a, considered modulo m, to be a number such that $a^{-1}a \equiv 1 \pmod{m}$.

The inverse: reminder

In the last lecture, I defined the *inverse* a^{-1} of a number a, considered modulo m, to be a number such that $a^{-1}a \equiv 1 \pmod{m}$.
I proved that this was unique modulo m when it existed.

More handy inverse facts

More handy inverse facts

Two other fairly easy, but useful, facts are as follows:

More handy inverse facts

Two other fairly easy, but useful, facts are as follows:

Proposition

If a is invertible modulo m, then so is a^{-1}, with inverse given by $(a^{-1})^{-1} \equiv a \pmod{m}$.

More handy inverse facts

Two other fairly easy, but useful, facts are as follows:

Proposition

If a is invertible modulo m, then so is a^{-1}, with inverse given by $(a^{-1})^{-1} \equiv a \pmod{m}$.

Proof.

?

□

More handy inverse facts

Two other fairly easy, but useful, facts are as follows:

Proposition

If a is invertible modulo m, then so is a^{-1}, with inverse given by $(a^{-1})^{-1} \equiv a \pmod{m}$.

Proof.

?

□

Proposition

If a and b are both invertible, then ab is too, with inverse given by

$$(ab)^{-1} \equiv b^{-1}a^{-1} \pmod{m}.$$

More handy inverse facts

Two other fairly easy, but useful, facts are as follows:

Proposition

If a is invertible modulo m, then so is a^{-1}, with inverse given by $(a^{-1})^{-1} \equiv a \pmod{m}$.

Proof.

?

□

Proposition

If a and b are both invertible, then ab is too, with inverse given by

$$(ab)^{-1} \equiv b^{-1}a^{-1} \pmod{m}.$$

Proof.

?

A big example

A big example

Just by way of example (and partly as a reminder of the whole Euclid's algorithm thing), let's find an inverse for 37, modulo 100.

A big example

Just by way of example (and partly as a reminder of the whole Euclid's algorithm thing), let's find an inverse for 37, modulo 100. So we want x with $37x \equiv 1 \pmod{100}$.

A big example

Just by way of example (and partly as a reminder of the whole Euclid's algorithm thing), let's find an inverse for 37, modulo 100. So we want x with $37x \equiv 1 \pmod{100}$. In other words, we seek a solution to $37x + 100k = 1$ in the integers.

A big example

Just by way of example (and partly as a reminder of the whole Euclid's algorithm thing), let's find an inverse for 37, modulo 100. So we want x with $37x \equiv 1 \pmod{100}$. In other words, we seek a solution to $37x + 100k = 1$ in the integers. We'll get one from working through Euclid's algorithm:

?

What we've done

What we've done

We've come to understand congruence equations: given something like

$$123x \equiv 456 \pmod{789},$$

we can, with some effort, turn it into something nice like

$$x \equiv 132 \pmod{263}.$$

Simultaneous congruences

Simultaneous congruences

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number?

Simultaneous congruences

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number? For example,

$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 7?$$

Simultaneous congruences

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number? For example,

$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 7?$$

These things happen all the time: two things happening periodically with different periods.

Simultaneous congruences

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number? For example,

$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 7?$$

These things happen all the time: two things happening periodically with different periods.
And it turns out we can solve them using exactly the same machinery as we've been using all along.

Simultaneous congruences

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number? For example,

$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 7?$$

These things happen all the time: two things happening periodically with different periods.
And it turns out we can solve them using exactly the same machinery as we've been using all along. Indeed, these equations say that

$$x - 1 = 4a$$
$$x - 3 = 7b,$$

for some numbers a and b.

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$.

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.
A solution to $4a - 7b = 1$ is given by $a = 2$, $b = 1$, and so a solution to $4a - 7b = 2$ is given by doubling that to get $a = 4$, $b = 2$.

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.
A solution to $4a - 7b = 1$ is given by $a = 2$, $b = 1$, and so a solution to $4a - 7b = 2$ is given by doubling that to get $a = 4$, $b = 2$.
What's the general solution? Well, if we have $4a - 7b = 2$, then subtracting $4 \times 4 - 7 \times 2 = 2$ gives

$$4(a - 4) - 7(b - 2) = 0.$$

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.
A solution to $4a - 7b = 1$ is given by $a = 2$, $b = 1$, and so a solution to $4a - 7b = 2$ is given by doubling that to get $a = 4$, $b = 2$.
What's the general solution? Well, if we have $4a - 7b = 2$, then subtracting $4 \times 4 - 7 \times 2 = 2$ gives

$$4(a - 4) - 7(b - 2) = 0.$$

This means that $7 \mid 4(a - 4)$, so $7 \mid (a - 4)$. Hence a is of the form $7k + 4$. and in fact any such a works.

How to solve them

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.
A solution to $4a - 7b = 1$ is given by $a = 2$, $b = 1$, and so a solution to $4a - 7b = 2$ is given by doubling that to get $a = 4$, $b = 2$.
What's the general solution? Well, if we have $4a - 7b = 2$, then subtracting $4 \times 4 - 7 \times 2 = 2$ gives

$$4(a - 4) - 7(b - 2) = 0.$$

This means that $7 \mid 4(a - 4)$, so $7 \mid (a - 4)$. Hence a is of the form $7k + 4$. and in fact any such a works.
So $4a$ is of the form $28k + 16$, so x is of the form $28k + 17$, in other words:

$$x \equiv 17 \pmod{28}.$$

No solutions?

No solutions?

There need not always be solutions to simultaneous congruences.

No solutions?

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod{6}$$
$$x \equiv 3 \pmod{8}$$

don't have solutions.

No solutions?

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod{6}$$
$$x \equiv 3 \pmod{8}$$

don't have solutions. Why is this obvious?

?

No solutions?

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod 6$$
$$x \equiv 3 \pmod 8$$

don't have solutions. Why is this obvious?

?

Of course, if we go through the same solution process as above it will fail.

No solutions?

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod 6$$
$$x \equiv 3 \pmod 8$$

don't have solutions. Why is this obvious?

?

Of course, if we go through the same solution process as above it will fail. We set

$$x = 4 + 6a$$
$$x = 3 + 8b$$

and find that $4 + 6a = 3 + 8b$, and hence $8b - 6a = 1$.

No solutions?

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod 6$$
$$x \equiv 3 \pmod 8$$

don't have solutions. Why is this obvious?

$$\boxed{?}$$

Of course, if we go through the same solution process as above it will fail. We set

$$x = 4 + 6a$$
$$x = 3 + 8b$$

and find that $4 + 6a = 3 + 8b$, and hence $8b - 6a = 1$. This has no solutions because $\gcd(8, 6) = 2$, and $2 \nmid 1$.

The Chinese Remainder Theorem

The Chinese Remainder Theorem

It would be good to know something that reassures us that there *will* be a solution in some family of cases, and here's a result, named after its discovery by the ancient Chinese:

The Chinese Remainder Theorem

It would be good to know something that reassures us that there *will* be a solution in some family of cases, and here's a result, named after its discovery by the ancient Chinese:

Theorem (Chinese Remainder Theorem)

Let m_1 and m_2 be coprime, and let a_1 and a_2 be any integers. The simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

have a solution modulo $m_1 m_2$.

The Chinese Remainder Theorem

It would be good to know something that reassures us that there *will* be a solution in some family of cases, and here's a result, named after its discovery by the ancient Chinese:

Theorem (Chinese Remainder Theorem)

Let m_1 and m_2 be coprime, and let a_1 and a_2 be any integers. The simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

have a solution modulo $m_1 m_2$.

Proof.

?

□

A worked example

A worked example

This gives us a new way of finding solutions, which I'll show off:

A worked example

This gives us a new way of finding solutions, which I'll show off:
What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14:

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

This has a solution $5 \times 17 - 6 \times 14 = 1$.

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

This has a solution $5 \times 17 - 6 \times 14 = 1$.
As a result $5 \times 17 = 85$ is congruent to 1 mod 14 and 0 modulo 17,

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

This has a solution $5 \times 17 - 6 \times 14 = 1$.
As a result $5 \times 17 = 85$ is congruent to 1 mod 14 and 0 modulo 17, and $-6 \times 14 = -84$ is congruent to 0 mod 14 and 1 modulo 17.

A worked example

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$x \equiv 11 \pmod{14}$$
$$x \equiv 10 \pmod{17}?$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

This has a solution $5 \times 17 - 6 \times 14 = 1$.
As a result $5 \times 17 = 85$ is congruent to 1 mod 14 and 0 modulo 17, and $-6 \times 14 = -84$ is congruent to 0 mod 14 and 1 modulo 17.
Hence our solution is

$$11 \times 85 + 10 \times (-84) \equiv 95 \pmod{238}.$$