MAS114: Lecture 15

James Cranch

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

2021–2022

Where were we?

Where were we?

We were thinking about cancellation in modular arithmetic.

Where were we?

We were thinking about cancellation in modular arithmetic.
We'd just proved a useful result:

Where were we?

We were thinking about cancellation in modular arithmetic.
We'd just proved a useful result:
Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Where were we?

We were thinking about cancellation in modular arithmetic.
We'd just proved a useful result:
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).

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

  $1.$

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
  $1.$
- The inverse of -1 modulo m is always
  $-1.$

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

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.

We have $aa^{-1} \equiv 1 \pmod{m}$, which says that a is an inverse for a^{-1}. □

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.

We have $aa^{-1} \equiv 1 \pmod{m}$, which says that a is an inverse for a^{-1}. □

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.

We have $aa^{-1} \equiv 1 \pmod{m}$, which says that a is an inverse for a^{-1}. □

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.

We have $(ab)b^{-1}a^{-1} \equiv aa^{-1}bb^{-1} \equiv 1 \cdot 1 \equiv 1 \pmod{m}$. □

A big example

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. We want x with $37x \equiv 1 \pmod{100}$.

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$

$$26 = 2 \times 11 + 4$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$

$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

So we have that

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$
\begin{aligned}
100 &= 2 \times 37 + 26 & \qquad 37 &= 1 \times 26 + 11 \\
26 &= 2 \times 11 + 4 & \qquad 11 &= 2 \times 4 + 3 \\
4 &= 1 \times 3 + 1 & \qquad 3 &= 3 \times 1.
\end{aligned}
$$

So we have that

$$1 = 1 \times 4 - 1 \times 3$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$\begin{aligned} 100 &= 2 \times 37 + 26 & 37 &= 1 \times 26 + 11 \\ 26 &= 2 \times 11 + 4 & 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 & 3 &= 3 \times 1. \end{aligned}$$

So we have that

$$1 = 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4)$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$\begin{aligned} 100 &= 2 \times 37 + 26 & 37 &= 1 \times 26 + 11 \\ 26 &= 2 \times 11 + 4 & 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 & 3 &= 3 \times 1. \end{aligned}$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 \end{aligned}$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$\begin{aligned} 100 &= 2 \times 37 + 26 & 37 &= 1 \times 26 + 11 \\ 26 &= 2 \times 11 + 4 & 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 & 3 &= 3 \times 1. \end{aligned}$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11 \end{aligned}$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

So we have that

$$1 = 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4)$$
$$= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11$$
$$= 3 \times 26 - 7 \times 11$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

So we have that

$$1 = 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4)$$
$$= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11$$
$$= 3 \times 26 - 7 \times 11 = 3 \times 26 - 7 \times (37 - 26)$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$\begin{aligned} 100 &= 2 \times 37 + 26 & 37 &= 1 \times 26 + 11 \\ 26 &= 2 \times 11 + 4 & 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 & 3 &= 3 \times 1. \end{aligned}$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11 \\ &= 3 \times 26 - 7 \times 11 = 3 \times 26 - 7 \times (37 - 26) \\ &= 10 \times 26 - 7 \times 37 \end{aligned}$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$\begin{aligned} 100 &= 2 \times 37 + 26 & 37 &= 1 \times 26 + 11 \\ 26 &= 2 \times 11 + 4 & 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 & 3 &= 3 \times 1. \end{aligned}$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11 \\ &= 3 \times 26 - 7 \times 11 = 3 \times 26 - 7 \times (37 - 26) \\ &= 10 \times 26 - 7 \times 37 = 10 \times (100 - 2 \times 37) - 7 \times 37 \end{aligned}$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11 \\ &= 3 \times 26 - 7 \times 11 = 3 \times 26 - 7 \times (37 - 26) \\ &= 10 \times 26 - 7 \times 37 = 10 \times (100 - 2 \times 37) - 7 \times 37 \\ &= 10 \times 100 - 27 \times 37. \end{aligned}$$

A big example

As a big example of all of this, let's find an inverse for 37, modulo 100. 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:

$$100 = 2 \times 37 + 26 \qquad 37 = 1 \times 26 + 11$$
$$26 = 2 \times 11 + 4 \qquad 11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1.$$

So we have that

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 = 1 \times 4 - 1 \times (11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 = 3 \times (26 - 2 \times 11) - 1 \times 11 \\ &= 3 \times 26 - 7 \times 11 = 3 \times 26 - 7 \times (37 - 26) \\ &= 10 \times 26 - 7 \times 37 = 10 \times (100 - 2 \times 37) - 7 \times 37 \\ &= 10 \times 100 - 27 \times 37. \end{aligned}$$

That means that $(-27) \times 37 \equiv 1 \pmod{100}$, so the inverse of 37 is -27, which is congruent to 73 (mod 100).

Checking our working

Checking our working

And, of course, we can check this easily: $37 \times 73 = 2701 \equiv 1 \pmod{100}$ as claimed.

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,

$$\begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{7}? \end{aligned}$$

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,

$$\begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{7}? \end{aligned}$$

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.

Now, we had $x = 4a + 1$, which in turn is $28k + 17$. 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?

The first equation implies x even, the second x odd.

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?

The first equation implies x even, the second x odd.

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?

The first equation implies x even, the second x odd.

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?

The first equation implies x even, the second x odd.

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 $2 \nmid 1$.