MAS114: Lecture 16

James Cranch

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

2017–2018

No surgery hour this Thursday

No surgery hour this Thursday

I'll be unavailable Thursday afternoon: I'll be running a maths competition for school students in Doncaster.

No surgery hour this Thursday

I'll be unavailable Thursday afternoon: I'll be running a maths competition for school students in Doncaster.
If you need to chat about maths, email me and I'll arrange something.

What we've been up to

What we've been up to

We've got good at solving equations. Starting from being able to solve equations like $ax + by = c$ in the integers, we've developed:

What we've been up to

We've got good at solving equations. Starting from being able to solve equations like $ax + by = c$ in the integers, we've developed:

- A way of solving linear congruence equations of the form

$$ax \equiv b \pmod{m}$$

What we've been up to

We've got good at solving equations. Starting from being able to solve equations like $ax + by = c$ in the integers, we've developed:

- A way of solving linear congruence equations of the form

$$ax \equiv b \pmod{m}$$

- Two ways of solving simultaneous congruences

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

Arithmetic mod p

Arithmetic mod p

Earlier, we pointed out that modular arithmetic modulo primes is very well-behaved: every nonzero residue is invertible.

Arithmetic mod p

Earlier, we pointed out that modular arithmetic modulo primes is very well-behaved: every nonzero residue is invertible.
We'll going to go on and use that.

Arithmetic mod p

Earlier, we pointed out that modular arithmetic modulo primes is very well-behaved: every nonzero residue is invertible.
We'll going to go on and use that.
The first thing we'll talk about is *exponentiation* in modular arithmetic.

Exponentiation mod p

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

$$3^2 = 3 \times 3 \equiv 9 \pmod{10},$$

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

$$\begin{aligned} 3^2 &= 3 \times 3 \equiv 9 \pmod{10}, \\ 3^3 &= 3 \times 3^2 \equiv 3 \times 9 \equiv 7 \pmod{10}, \end{aligned}$$

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

$$\begin{aligned} 3^2 &= 3 \times 3 \equiv 9 \pmod{10}, \\ 3^3 &= 3 \times 3^2 \equiv 3 \times 9 \equiv 7 \pmod{10}, \\ 3^4 &= 3 \times 3^3 \equiv 3 \times 7 \equiv 1 \pmod{10} \ldots \end{aligned}$$

Exponentiation mod p

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

$$\begin{aligned} 3^2 &= 3 \times 3 \equiv 9 \pmod{10}, \\ 3^3 &= 3 \times 3^2 \equiv 3 \times 9 \equiv 7 \pmod{10}, \\ 3^4 &= 3 \times 3^3 \equiv 3 \times 7 \equiv 1 \pmod{10} \ldots \end{aligned}$$

That's still going to be a lot of multiplication, if we keep multiplying by 3 (modulo 10) more than a thousand times!

Better yet?

Better yet?

There are considerably more intelligent ways.

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = \left(3^2\right)^4 = \left(3^2\right)^{2\times 2} = \left(\left(3^2\right)^2\right)^2.$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = \left(3^2\right)^4 = \left(3^2\right)^{2\times 2} = \left(\left(3^2\right)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234}$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617}$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617}$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617} \equiv 9^{617}$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617} \equiv 9^{617} \equiv 9^{2\times 308+1}$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617} \equiv 9^{617} \equiv 9^{2\times 308+1} \equiv (9^2)^{308}9$$

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617} \equiv 9^{617} \equiv 9^{2\times 308+1} \equiv (9^2)^{308}9$$

and end up getting the answer.

Better yet?

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.
That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = (3^2)^4 = (3^2)^{2\times 2} = \left((3^2)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv (3^2)^{617} \equiv 9^{617} \equiv 9^{2\times 308+1} \equiv (9^2)^{308}9$$

and end up getting the answer.
Tricks like that are much, much faster than multiplying by three lots of times mod 10.

Even better yet

Even better yet

But, in fact, there's a method that's even faster still for this situation.

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k}$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

3^{1234}

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$3^{1234} = 3^{4\times 308+2}$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2 \equiv 1^{308}3^2$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2 \equiv 1^{308}3^2 \equiv 3^2$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2 \equiv 1^{308}3^2 \equiv 3^2 \equiv 9 \pmod{10}.$$

Even better yet

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2 \equiv 1^{308}3^2 \equiv 3^2 \equiv 9 \pmod{10}.$$

That makes the whole thing easy.

Making 1 as a power

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$.

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?
2. When it does exist, can we compute it?

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?
2. When it does exist, can we compute it?

Our answer to the first is not too difficult:

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?
2. When it does exist, can we compute it?

Our answer to the first is not too difficult:

Theorem

Let a and m be coprime integers. Then there is some positive n such that

$$a^n \equiv 1 \pmod{m}.$$

Making 1 as a power

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?
2. When it does exist, can we compute it?

Our answer to the first is not too difficult:

Theorem

Let a and m be coprime integers. Then there is some positive n such that

$$a^n \equiv 1 \pmod{m}.$$

Proof.

?

A comment

A comment

That proof is somewhat *nonconstructive*: it tells us it exists, but doesn't give much help looking for it.

Fermat's Little Theorem

Fermat's Little Theorem

It turns out that that we can calculate it. First we'll do an easier case, valid when the modulus is prime.

Fermat's Little Theorem

It turns out that that we can calculate it. First we'll do an easier case, valid when the modulus is prime.

Theorem (Fermat's Little Theorem)

Let p be prime, and let a be an integer coprime to p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem

It turns out that that we can calculate it. First we'll do an easier case, valid when the modulus is prime.

Theorem (Fermat's Little Theorem)

Let p be prime, and let a be an integer coprime to p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof.

?

□