MAS114: Lecture 17

James Cranch

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

2021–2022

Where were we?

Where were we?

We were talking about powers in modular arithmetic, and observed it was useful to have powers congruent to one.

Powers congruent to 1

Powers congruent to 1

Theorem

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

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

Powers congruent to 1

Theorem

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

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

Proof.

There are only m different residues modulo m, so some two of the sequence

$$1, a, a^2, a^3, a^4, \ldots, a^m$$

must be congruent modulo m (they can't all be different).

Powers congruent to 1

Theorem

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

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

Proof.

There are only m different residues modulo m, so some two of the sequence

$$1, a, a^2, a^3, a^4, \ldots, a^m$$

must be congruent modulo m (they can't all be different).
Let's say that $a^i \equiv a^j \pmod{m}$, with $i < j$.

Powers congruent to 1

Theorem

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

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

Proof.

There are only m different residues modulo m, so some two of the sequence

$$1, a, a^2, a^3, a^4, \ldots, a^m$$

must be congruent modulo m (they can't all be different).
Let's say that $a^i \equiv a^j \pmod{m}$, with $i < j$.
But a is invertible modulo m, and so

$$(a^{-1})^i a^i \equiv (a^{-1})^i a^j \pmod{m},$$

which gives that

$$a^{j-i} \equiv 1 \pmod{m}.$$

A comment

A comment

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

Fermat's Little Theorem

Fermat's Little Theorem

It turns out that that we can get an explicit result. First we'll do a relatively easy case, valid when the modulus is prime.

Fermat's Little Theorem

It turns out that that we can get an explicit result. First we'll do a relatively easy 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 get an explicit result. First we'll do a relatively easy 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

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

Before we prove it, we'll talk a while longer about invertible elements and multiplication modulo a prime.

Arithmetic progressions modulo a prime

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$0 \equiv 0$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$0 \equiv 0$$

$$3 \equiv 3$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$0 \equiv 0$$

$$6 \equiv 6$$

$$3 \equiv 3$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$0 \equiv 0$$

$$9 \equiv 2 \qquad 6 \equiv 6$$

$$3 \equiv 3$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$0 \equiv 0 \qquad 12 \equiv 5$$
$$9 \equiv 2 \qquad 6 \equiv 6$$
$$3 \equiv 3$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$\begin{aligned} 0 &\equiv 0 \\ 15 &\equiv 1 & 12 &\equiv 5 \\ 9 &\equiv 2 & 6 &\equiv 6 \\ 3 &\equiv 3 \end{aligned}$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$\begin{aligned} 0 &\equiv 0 & 18 &\equiv 4 \\ 15 &\equiv 1 & 12 &\equiv 5 \\ 9 &\equiv 2 & 6 &\equiv 6 \\ 3 &\equiv 3 \end{aligned}$$

Arithmetic progressions modulo a prime

Let's start with an example, and consider the seven integers

$$0, 3, 6, 9, 12, 15, 18.$$

Regarded modulo 7, each is congruent to something different:

$$\begin{aligned} 0 &\equiv 0 & 18 &\equiv 4 \\ 15 &\equiv 1 & 12 &\equiv 5 \\ 9 &\equiv 2 & 6 &\equiv 6 \\ 3 &\equiv 3 \end{aligned}$$

Can we explain this systematically?

Arithmetic progressions in modular arithmetic

Arithmetic progressions in modular arithmetic

It comes down to the fact that 3 is invertible modulo 7 (with inverse 5, as $3 \times 5 \equiv 1 \pmod{7}$).

Arithmetic progressions in modular arithmetic

It comes down to the fact that 3 is invertible modulo 7 (with inverse 5, as $3 \times 5 \equiv 1 \pmod 7$).
By multiplying congruences, $3 \times 5 \times a \equiv a \pmod 7$

Arithmetic progressions in modular arithmetic

It comes down to the fact that 3 is invertible modulo 7 (with inverse 5, as $3 \times 5 \equiv 1 \pmod{7}$).
By multiplying congruences, $3 \times 5 \times a \equiv a \pmod{7}$ so if we want to solve $3x \equiv a \pmod{7}$, we simply take $x \equiv 5a \pmod{7}$.

Arithmetic progressions in modular arithmetic

It comes down to the fact that 3 is invertible modulo 7 (with inverse 5, as $3 \times 5 \equiv 1 \pmod 7$).
By multiplying congruences, $3 \times 5 \times a \equiv a \pmod 7$ so if we want to solve $3x \equiv a \pmod 7$, we simply take $x \equiv 5a \pmod 7$.
So as there are seven numbers in the list, and one is congruent to each possible residue $0, 1, \ldots, 6$ (modulo 7), they're all different.

Arithmetic progressions in modular arithmetic

It comes down to the fact that 3 is invertible modulo 7 (with inverse 5, as $3 \times 5 \equiv 1 \pmod{7}$).
By multiplying congruences, $3 \times 5 \times a \equiv a \pmod{7}$ so if we want to solve $3x \equiv a \pmod{7}$, we simply take $x \equiv 5a \pmod{7}$.
So as there are seven numbers in the list, and one is congruent to each possible residue $0, 1, \ldots, 6$ (modulo 7), they're all different.
This is true in general, for the same reason: if a is coprime to m, then the integers

$$0, a, 2a, \ldots, (m-1)a$$

contain each of the m residues (and so exactly once each, because there's m of them).

Proving Fermat's Little Theorem

Proving Fermat's Little Theorem

Proof.

Proving Fermat's Little Theorem

Proof.

Consider the product

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a),$$

regarded up to congruence modulo p.

Proving Fermat's Little Theorem

Proof.

Consider the product

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a),$$

regarded up to congruence modulo p.

One way of thinking about it is that it's $(p-1)!$ but with every term multiplied by an a, so is congruent to $a^{p-1}(p-1)!$.

Proving Fermat's Little Theorem

Proof.

Consider the product

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a),$$

regarded up to congruence modulo p.
One way of thinking about it is that it's $(p-1)!$ but with every term multiplied by an a, so is congruent to $a^{p-1}(p-1)!$.
Another is that, since the product contains a copy of every nonzero residue modulo p, it is congruent to $(p-1)!$.

Proving Fermat's Little Theorem

Proof.

Proving Fermat's Little Theorem

Proof.

But, putting these observations together, we discover that

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

Proving Fermat's Little Theorem

Proof.

But, putting these observations together, we discover that

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

But all the residues from 1 to $p-1$ are invertible, and the product of invertible residues is invertible, so $(p-1)!$ is invertible.

Proving Fermat's Little Theorem

Proof.

But, putting these observations together, we discover that

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

But all the residues from 1 to $p-1$ are invertible, and the product of invertible residues is invertible, so $(p-1)!$ is invertible. Multiplying both sides by $(p-1)!^{-1}$ leaves us with

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

exactly as promised. □

A remark

A remark

Remark

Fermat's Little Theorem should not be confused with *Fermat's Last Theorem*.

A remark

Remark

Fermat's Little Theorem should not be confused with *Fermat's Last Theorem*. The latter says there are no solutions in positive integers to $a^n + b^n = c^n$ with $n \geqslant 3$

A remark

Remark

Fermat's Little Theorem should not be confused with *Fermat's Last Theorem*. The latter says there are no solutions in positive integers to $a^n + b^n = c^n$ with $n \geqslant 3$, and was *much, much* harder to prove.

More generality

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together.

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated.

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition

Euler's function (sometimes known as the *totient function*) $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers from 1 to n which are coprime to n.

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition

Euler's function (sometimes known as the *totient function*) $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers from 1 to n which are coprime to n.

For example, $\varphi(p) = p - 1$ if p is prime

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition

Euler's function (sometimes known as the *totient function*) $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers from 1 to n which are coprime to n.

For example, $\varphi(p) = p - 1$ if p is prime, since every number from 1 to $p - 1$ is coprime to p (and p isn't coprime to p).

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition

Euler's function (sometimes known as the *totient function*) $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers from 1 to n which are coprime to n.

For example, $\varphi(p) = p - 1$ if p is prime, since every number from 1 to $p - 1$ is coprime to p (and p isn't coprime to p).
For another example, $\varphi(6) = 2$

More generality

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition

Euler's function (sometimes known as the *totient function*) $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers from 1 to n which are coprime to n.

For example, $\varphi(p) = p - 1$ if p is prime, since every number from 1 to $p - 1$ is coprime to p (and p isn't coprime to p).
For another example, $\varphi(6) = 2$, since 1 and 5 are the only numbers between 1 and 6 which are coprime to 6.

Fermat-Euler

Fermat-Euler

Using this concept, we can generalise Fermat's Little Theorem considerably:

Fermat-Euler

Using this concept, we can generalise Fermat's Little Theorem considerably:

Theorem (Fermat-Euler Theorem)

Let a and n be integers with $\gcd(a, n) = 1$*. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proving Fermat-Euler

Proving Fermat-Euler

Proof.

The proof is exactly the same as Fermat's Little Theorem, but instead of working with all the integers $1, 2, \ldots, n-1$, we just consider those that are invertible modulo n: let's write these as $x_1, x_2, \ldots, x_{\varphi(n)}$.

Proving Fermat-Euler

Proof.

The proof is exactly the same as Fermat's Little Theorem, but instead of working with all the integers $1, 2, \ldots, n - 1$, we just consider those that are invertible modulo n: let's write these as $x_1, x_2, \ldots, x_{\varphi(n)}$.

If a is invertible, then $ax_1, \ldots, ax_{\varphi(n)}$ are all invertible too, and any invertible residue is of this form: b can be written as $a(a^{-1}b)$.

Proving Fermat-Euler

Proof.

The proof is exactly the same as Fermat's Little Theorem, but instead of working with all the integers $1, 2, \ldots, n-1$, we just consider those that are invertible modulo n: let's write these as $x_1, x_2, \ldots, x_{\varphi(n)}$.

If a is invertible, then $ax_1, \ldots, ax_{\varphi(n)}$ are all invertible too, and any invertible residue is of this form: b can be written as $a(a^{-1}b)$.

Hence $ax_1, ax_2, \ldots, ax_{\varphi(n)}$ are congruent to $x_1, x_2, \ldots, x_{\varphi(n)}$ in some order.

Proving Fermat-Euler

Proof.

The proof is exactly the same as Fermat's Little Theorem, but instead of working with all the integers $1, 2, \ldots, n-1$, we just consider those that are invertible modulo n: let's write these as $x_1, x_2, \ldots, x_{\varphi(n)}$.
If a is invertible, then $ax_1, \ldots, ax_{\varphi(n)}$ are all invertible too, and any invertible residue is of this form: b can be written as $a(a^{-1}b)$.
Hence $ax_1, ax_2, \ldots, ax_{\varphi(n)}$ are congruent to $x_1, x_2, \ldots, x_{\varphi(n)}$ in some order.
Hence if we consider the products of these we have

$$\begin{aligned} & x_1 x_2 \cdots x_{\varphi(n)} \\ \equiv & (ax_1)(ax_2) \cdots (ax_{\varphi(n)}) \\ \equiv & a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod{n} \end{aligned}$$

Proving Fermat-Euler

Proof.

The proof is exactly the same as Fermat's Little Theorem, but instead of working with all the integers $1, 2, \ldots, n-1$, we just consider those that are invertible modulo n: let's write these as $x_1, x_2, \ldots, x_{\varphi(n)}$.

If a is invertible, then $ax_1, \ldots, ax_{\varphi(n)}$ are all invertible too, and any invertible residue is of this form: b can be written as $a(a^{-1}b)$.

Hence $ax_1, ax_2, \ldots, ax_{\varphi(n)}$ are congruent to $x_1, x_2, \ldots, x_{\varphi(n)}$ in some order.

Hence if we consider the products of these we have

$$\begin{aligned} & x_1 x_2 \cdots x_{\varphi(n)} \\ \equiv & (ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \\ \equiv & a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod{n} \end{aligned}$$

Since all the elements $x_1, x_2, \ldots, x_{\varphi(n)}$ are invertible, we can cancel them out to get $a^{\varphi(n)} \equiv 1 \pmod{n}$. □