MAS114: Lecture 17

James Cranch

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

2017–2018

An early Christmas present

An early Christmas present

I've put online my number theory tool, to help you revise.

An early Christmas present

I've put online my number theory tool, to help you revise.
`http://cranch.staff.shef.ac.uk/ntaas/`

An early Christmas present

I've put online my number theory tool, to help you revise.
`http://cranch.staff.shef.ac.uk/ntaas/`
It's linked from the main course webpage.

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 between 1 and n (inclusive) 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 between 1 and n (inclusive) 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 between 1 and n (inclusive) 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 between 1 and n (inclusive) 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 between 1 and n (inclusive) 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*

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

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*

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

Proof.

?

□

Squaring mod p

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it.

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$.

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.
But then, either $p \mid a - 1$

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.
But then, either $p \mid a-1$ (in which case $a \equiv 1 \pmod{p}$)

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.
But then, either $p \mid a-1$ (in which case $a \equiv 1 \pmod{p}$), or $p \mid a+1$

Squaring mod p

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.
However, we'll need a fact first:

Proposition

Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof.

If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.
But then, either $p \mid a-1$ (in which case $a \equiv 1 \pmod{p}$), or $p \mid a+1$ (in which case $a \equiv -1 \pmod{p}$). $\square$

A comment

A comment

Remark

This theorem is not true for some composite moduli!

A comment

Remark

This theorem is not true for some composite moduli! For example, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

A comment

Remark

This theorem is not true for some composite moduli! For example, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

I regard this as more evidence that prime moduli behave very nicely indeed!

Wilson's Theorem

Wilson's Theorem

Now, this allows us to do this:

Wilson's Theorem

Now, this allows us to do this:

Theorem (Wilson's Theorem)

We have $(n-1)! \equiv -1 \pmod{n}$ *if and only if* n *is prime.*

Wilson's Theorem

Now, this allows us to do this:

Theorem (Wilson's Theorem)

We have $(n-1)! \equiv -1 \pmod{n}$ *if and only if* n *is prime.*

Proof.

?

□

Examples and remarks

Examples and remarks

Here's an example or two:

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.
- 7 is prime, and $(7-1)! = 6! = 720 \equiv -1 \pmod 7$.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.
- 7 is prime, and $(7-1)! = 6! = 720 \equiv -1 \pmod 7$.

Remark

You could use this as a way of testing if a number is prime.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.
- 7 is prime, and $(7-1)! = 6! = 720 \equiv -1 \pmod 7$.

Remark

You could use this as a way of testing if a number is prime.
As a matter of fact, it's not a good way of doing it: if we want to check a large number N, it's quicker to do trial division to see if N has any factors, than it is to multiply lots of numbers together.

Examples and remarks

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod 4$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod 5$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.
- 7 is prime, and $(7-1)! = 6! = 720 \equiv -1 \pmod 7$.

Remark

You could use this as a way of testing if a number is prime.
As a matter of fact, it's not a good way of doing it: if we want to check a large number N, it's quicker to do trial division to see if N has any factors, than it is to multiply lots of numbers together.
But this result was psychologically important in the development of modern fast primality tests: it was the first evidence that there are ways of investigating whether a number N is prime or not by looking at how arithmetic modulo N behaves.