Fermat's little theorem

Mathematics Explained and Clarified

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Technical lemmas without proofs

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

Technical lemmas without proofs

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

Lemma 2

For any natural numbers a and b and a prime number p, if both a and b are not divisible by p, then their product ab is not divisible by p either.

Technical lemmas without proofs

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

Lemma 2

For any natural numbers a and b and a prime number p, if both a and b are not divisible by p, then their product ab is not divisible by p either.

Lemma 1 and Lemma 2 are trivially equivalent to each other. Sometimes, it is more convenient to use the statement in the form of Lemma 1 and sometimes in the form of Lemma 2.

Technical lemmas without proofs

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

Lemma 1 should be intuitively more or less obvious. It is a straightforward corollary of the fundamental theorem of arithmetic, which states that any natural number can be expressed as a product of prime numbers, and that this expression is unique up to the order of the prime divisors. Although it is sometimes proved without using the fundamental theorem of arithmetic as it is a simpler statement than the fundamental theorem of arithmetic.

Technical lemmas without proofs

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

And, if proving Lemma 1 as a corollary of the fundamental theorem of arithmetic, we need to make sure that the fundamental theorem of arithmetic is proved without using Lemma 1 to avoid circular reasoning.

Technical lemmas without proofs

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

Technical lemmas without proofs

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

Lemma 3 is a straightforward corollary of Lemma 1.

Technical lemmas without proofs

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

Lemma 3 is a straightforward corollary of Lemma 1.
The full proofs are given at the end of the video. Viewers are encouraged to skip that part of the video.

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Consider n, $2n$, $\ldots$, $(p-1)n$.

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Consider n, $2n$, $\ldots$, $(p-1)n$.
(by Lemma 2) $\implies$ they are not divisible by p

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Consider n, $2n$, $\ldots$, $(p-1)n$.
(by Lemma 2) $\implies$ they are not divisible by p:

- for $1 \leq i \leq p-1$, i is not divisible by p because $i < p$.
-

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Consider n, $2n$, $\ldots$, $(p-1)n$.
(by Lemma 2) $\implies$ they are not divisible by p:

- for $1 \leq i \leq p-1$, i is not divisible by p because $i < p$.
- n is not divisible by p by the condition in the statement of the theorem.

The main result

Theorem 1 (Fermat's little theorem)

Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.

Consider n, $2n$, $\ldots$, $(p-1)n$.
(by Lemma 2) $\implies$ they are not divisible by p:

- for $1 \leq i \leq p-1$, i is not divisible by p because $i < p$.
- n is not divisible by p by the condition in the statement of the theorem.

(by Lemma 2) $\implies$ in is not divisible by p.

The main result

Let us prove that these $p - 1$ numbers (n, $2n$, $\ldots$, $(p-1)n$) all have different remainders when divided by p.

The main result

Let us prove that these $p-1$ numbers $(n, 2n, \ldots, (p-1)n)$ all have different remainders when divided by p.
If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p

The main result

Let us prove that these $p-1$ numbers $(n, 2n, \ldots, (p-1)n)$ all have different remainders when divided by p.

If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.

The main result

Let us prove that these $p-1$ numbers $(n, 2n, \ldots, (p-1)n)$ all have different remainders when divided by p.
If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.
So, these $p-1$ numbers all have different remainders when divided by p

The main result

Let us prove that these $p-1$ numbers $(n, 2n, \ldots, (p-1)n)$ all have different remainders when divided by p.
If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.
So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0.

The main result

Let us prove that these $p-1$ numbers $(n, 2n, \ldots, (p-1)n)$ all have different remainders when divided by p.

If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.

So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: $1, 2, \ldots, p-1$.

The main result

Let us prove that these $p - 1$ numbers (n, $2n$, ..., $(p-1)n$) all have different remainders when divided by p.

If in and jn have the same remainder, where $1 \leq i < j \leq p - 1$, then $jn - in = (j - i)n$ is divisible by p, a contradiction with the previously proved fact.

So, these $p - 1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p - 1$ such possible remainders: 1, 2, ..., $p - 1$. So, these $p - 1$ numbers must have exactly these remainders, possibly in different order.

The main result

Let us prove that these $p - 1$ numbers $(n, 2n, \dots, (p-1)n)$ all have different remainders when divided by p.
If in and jn have the same remainder, where $1 \le i < j \le p - 1$, then $jn - in = (j - i)n$ is divisible by p, a contradiction with the previously proved fact.
So, these $p - 1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p - 1$ such possible remainders: $1, 2, \dots, p - 1$. So, these $p - 1$ numbers must have exactly these remainders, possibly in different order.
Then the product of these $p - 1$ numbers must be congruent to the product of these $p - 1$ remainders modulo p

The main result

Let us prove that these $p-1$ numbers (n, $2n$, $\ldots$, $(p-1)n$) all have different remainders when divided by p.
If in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.
So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: 1, 2, $\ldots$, $p-1$. So, these $p-1$ numbers must have exactly these remainders, possibly in different order.
Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p:

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

The main result

So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: 1, 2, ..., $p-1$. So, these $p-1$ numbers must have exactly these remainders, possibly in different order. Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p:

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

$$n^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

The main result

So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: 1, 2, ..., $p-1$. So, these $p-1$ numbers must have exactly these remainders, possibly in different order. Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p:

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

$$n^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

None of the numbers 1, 2, ..., $p-1$ is divisible by p (because they are all strictly smaller than p).

The main result

So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: 1, 2, ..., $p-1$. So, these $p-1$ numbers must have exactly these remainders, possibly in different order. Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p:

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

$$n^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

None of the numbers 1, 2, ..., $p-1$ is divisible by p (because they are all strictly smaller than p).
(applying Lemma 2 repeatedly $p-1$ times) $\Longrightarrow$ their product $1 \cdot 2 \cdot \ldots \cdot (p-1)$ is not divisible by p either.

The main result

So, these $p-1$ numbers must have exactly these remainders, possibly in different order.
Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p:

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

$$n^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

None of the numbers 1, 2, ..., $p-1$ is divisible by p (because they are all strictly smaller than p).
(applying Lemma 2 repeatedly $p-1$ times) $\implies$ their product $1 \cdot 2 \cdot \ldots \cdot (p-1)$ is not divisible by p either.
(by Lemma 3) $\implies$ $n^{p-1} \equiv 1 \pmod{p}$.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies$ $a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).

$ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies$ $a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).

$ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$.

By the fundamental theorem of arithmentic, this expression is unique up to the order of the prime divisors.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).
$ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$.
By the fundamental theorem of arithmentic, this expression is unique up to the order of the prime divisors.
Suppose that ab is divisible by p.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).
$ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$.
By the fundamental theorem of arithmentic, this expression is unique up to the order of the prime divisors.
Suppose that ab is divisible by p. Let us prove that p must be among q_i or q'_i.

Proofs of the technical lemmas

Lemma 1 (Euclid's lemma)

For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.

(by the fundamental theorem of arithmetic) $\implies a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).
$ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$.
By the fundamental theorem of arithmentic, this expression is unique up to the order of the prime divisors.
Suppose that ab is divisible by p. Let us prove that p must be among q_i or q'_i.
ab is divisible by $p \implies ab = px$ for some $x \in \mathbb{N}$.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.
$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.

$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.

(by the fundamental theorem of arithmetic) $\implies$ the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.
$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.
(by the fundamental theorem of arithmetic) $\implies$ the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements.
$(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ must contain p.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.
$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.
(by the fundamental theorem of arithmetic) $\implies$ the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements.
$(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ must contain p.
$\implies p$ must be among q_i or q'_i.

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.

$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.

(by the fundamental theorem of arithmetic) $\implies$ the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements.

$(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ must contain p.

$\implies p$ must be among q_i or q'_i.

- if p is among q_i, then a is divisible by p.
-

Proofs of the technical lemmas

(by the fundamental theorem of arithmetic) $\implies x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime.

$ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$.

(by the fundamental theorem of arithmetic) $\implies$ the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements.

$(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ must contain p.

$\implies p$ must be among q_i or q'_i.

- if p is among q_i, then a is divisible by p.
- if p is among q'_i, then b is divisible by p.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.
$ab - ac = a(b - c)$.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.
$ab - ac = a(b - c)$.
(by Lemma 1) $\implies$ either a is divisible by p or $b - c$ is divisible by p.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.
$ab - ac = a(b - c)$.
(by Lemma 1) $\implies$ either a is divisible by p or $b - c$ is divisible by p.
But a is not divisible by p by the condition in the statement of the lemma.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.
$ab - ac = a(b - c)$.
(by Lemma 1) $\implies$ either a is divisible by p or $b - c$ is divisible by p.
But a is not divisible by p by the condition in the statement of the lemma.
$\implies$ $b - c$ is divisible by p.

Proofs of the technical lemmas

Lemma 3

If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.

By definition, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p.
$ab - ac = a(b - c)$.
(by Lemma 1) $\implies$ either a is divisible by p or $b - c$ is divisible by p.
But a is not divisible by p by the condition in the statement of the lemma.
$\implies$ $b - c$ is divisible by p.
(by definition) $\implies$ $b \equiv c \pmod{p}$.