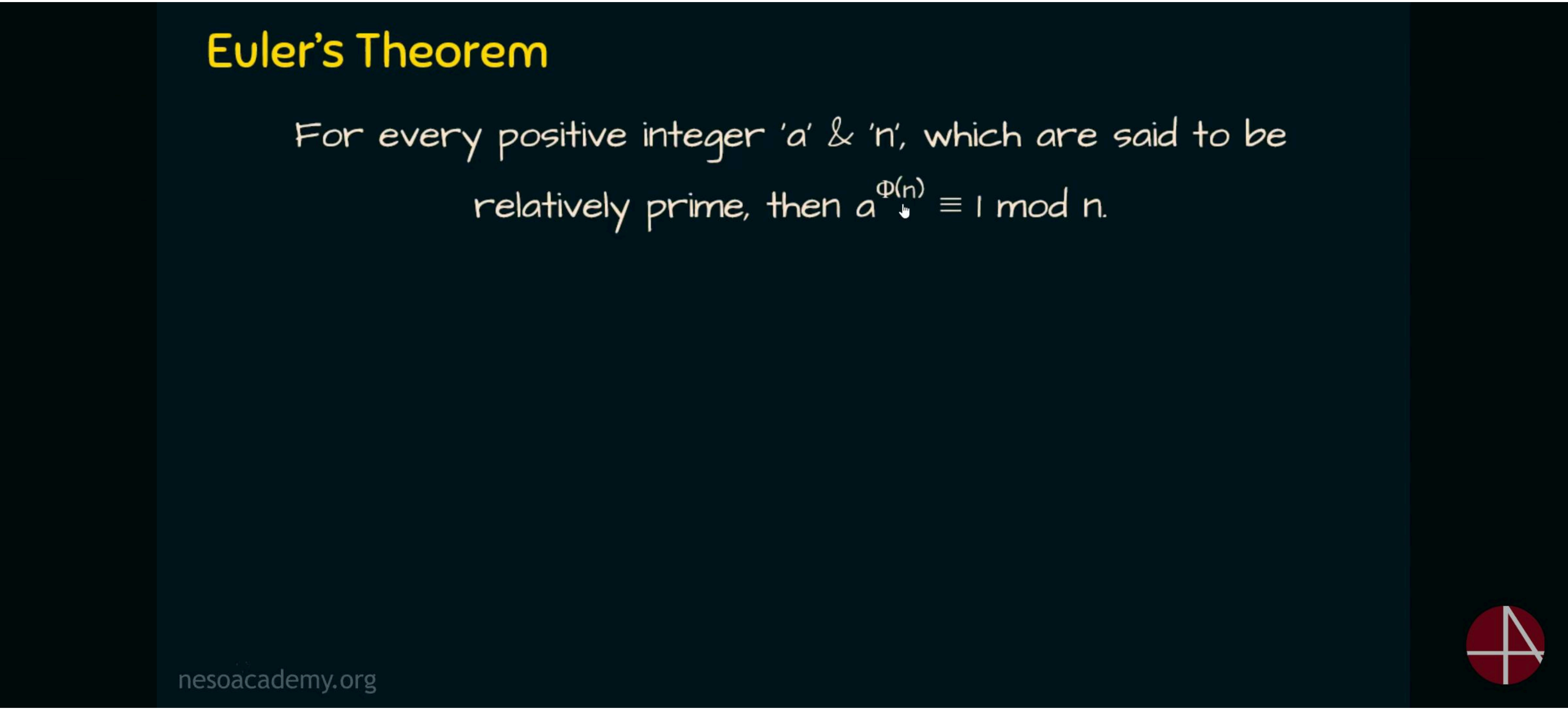
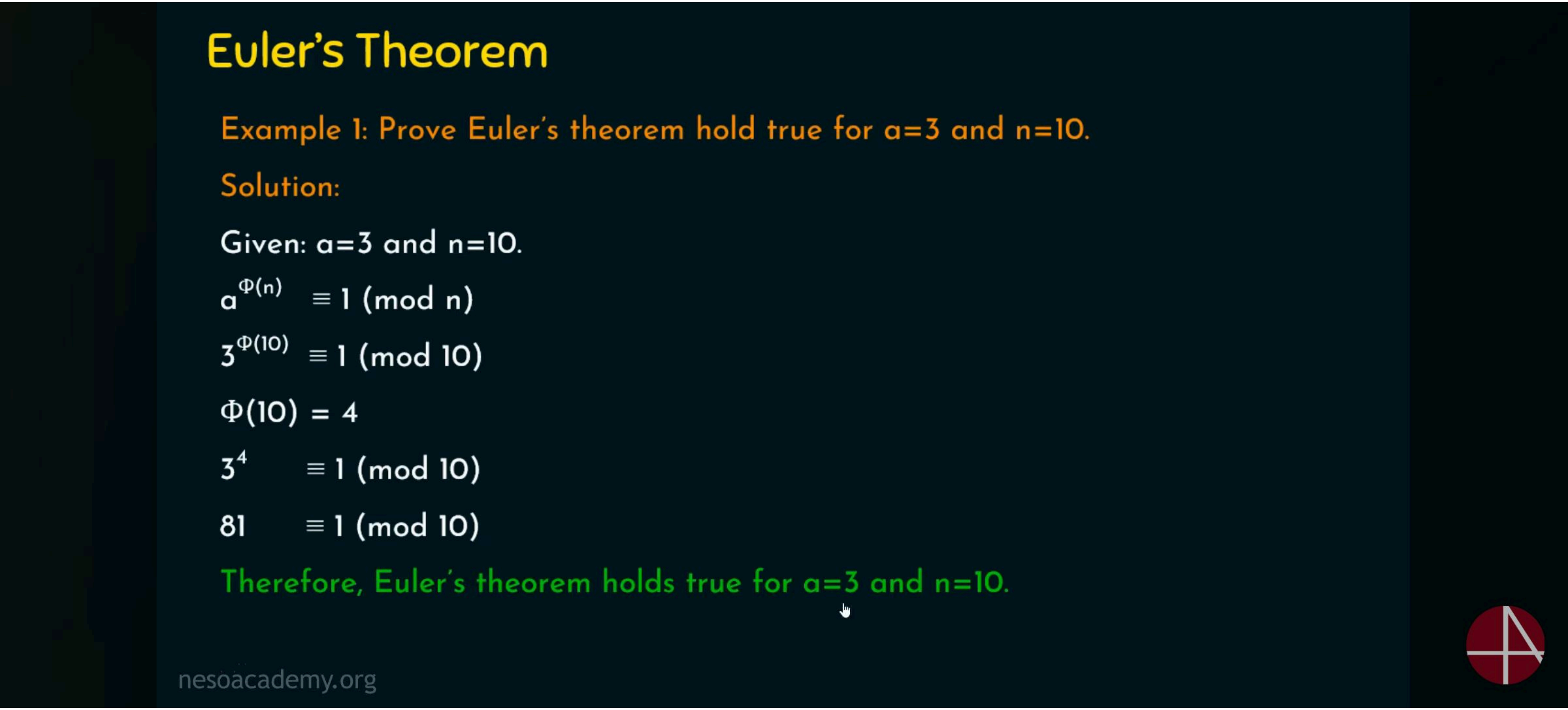
Euler's Theorem



Euler's Theorem

For every positive integer 'a' & 'n', which are said to be relatively prime, then $a^{\Phi(n)} \equiv 1 \bmod n$.

nesoacademy.org



Euler’s Theorem

Example 1: Prove Euler’s theorem hold true for a=3 and n=10.

Solution:

Given: a=3 and n=10.

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

$3^{\Phi(10)} \equiv 1 \pmod{10}$

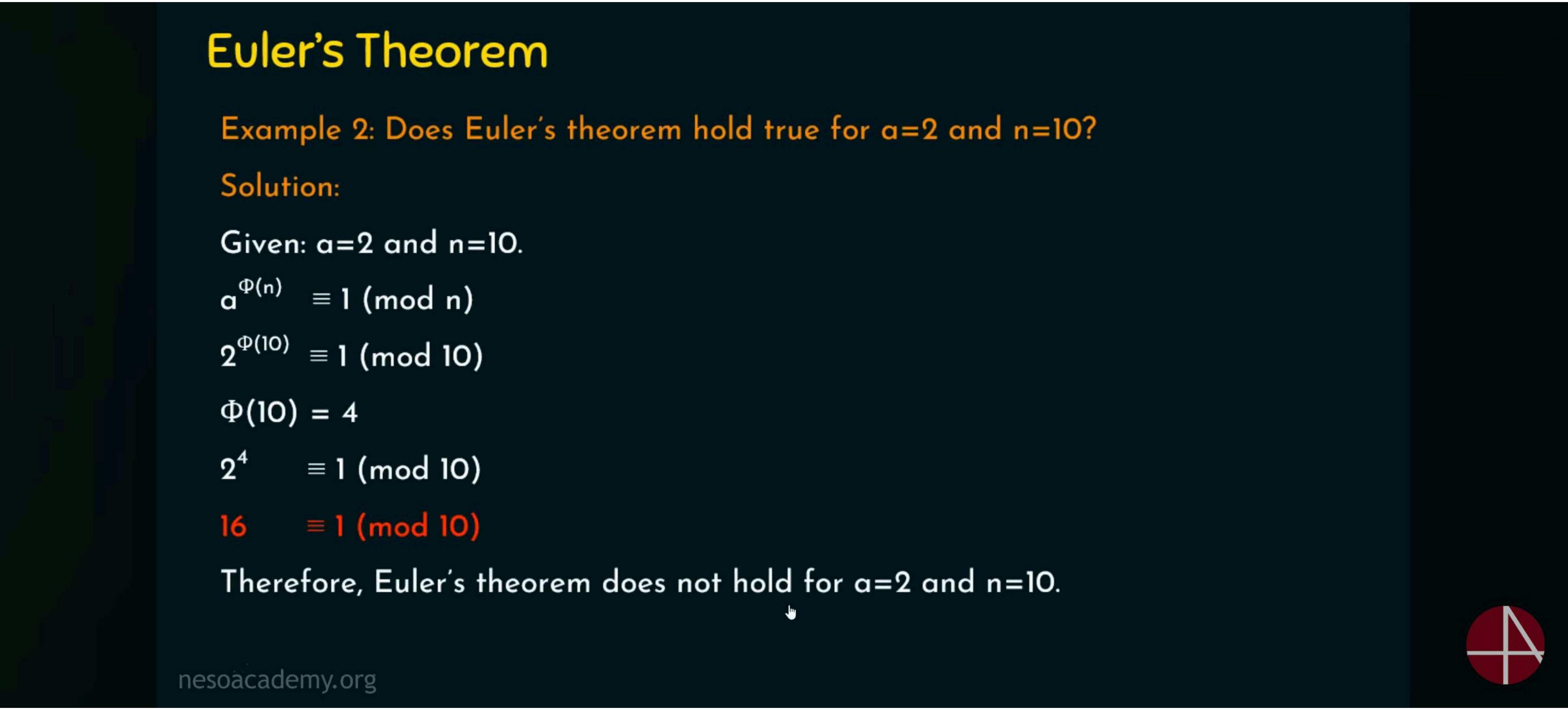
$\Phi(10) = 4$

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

$81 \equiv 1 \pmod{10}$

Therefore, Euler’s theorem holds true for a=3 and n=10.

nesoacademy.org



Euler's Theorem

Example 2: Does Euler's theorem hold true for a=2 and n=10?

Solution:

Given: a=2 and n=10.

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

$2^{\Phi(10)} \equiv 1 \pmod{10}$

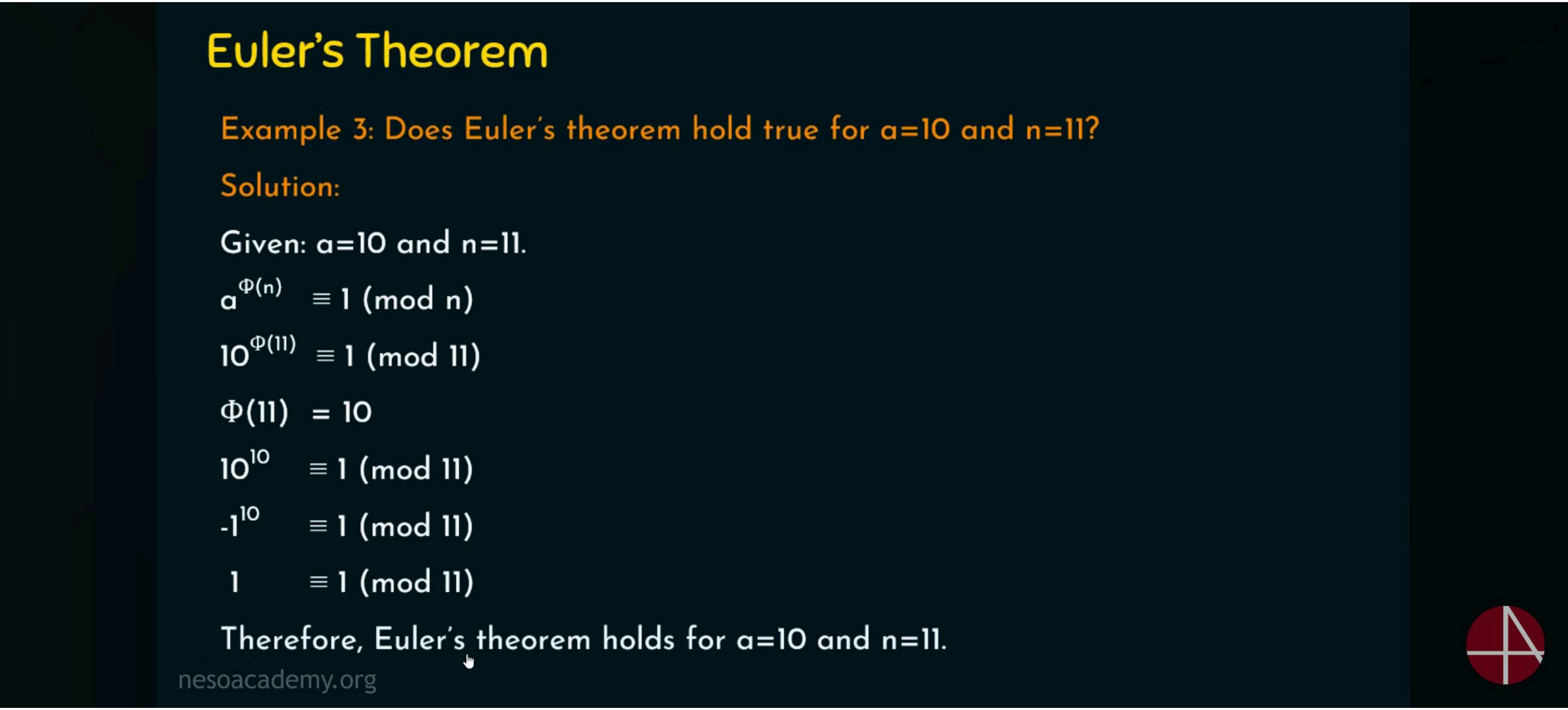
$\Phi(10) = 4$

$2^{4} \equiv 1 \pmod{10}$

$16 \equiv 1 \pmod{10}$

Therefore, Euler's theorem does not hold for a=2 and n=10.

nesoacademy.org



Euler's Theorem

Example 3: Does Euler's theorem hold true for a=10 and n=11?

Solution:

Given: a=10 and n=11.

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

$$10^{\Phi(11)} \equiv 1 \pmod{11}$$

$$\Phi(11) = 10$$

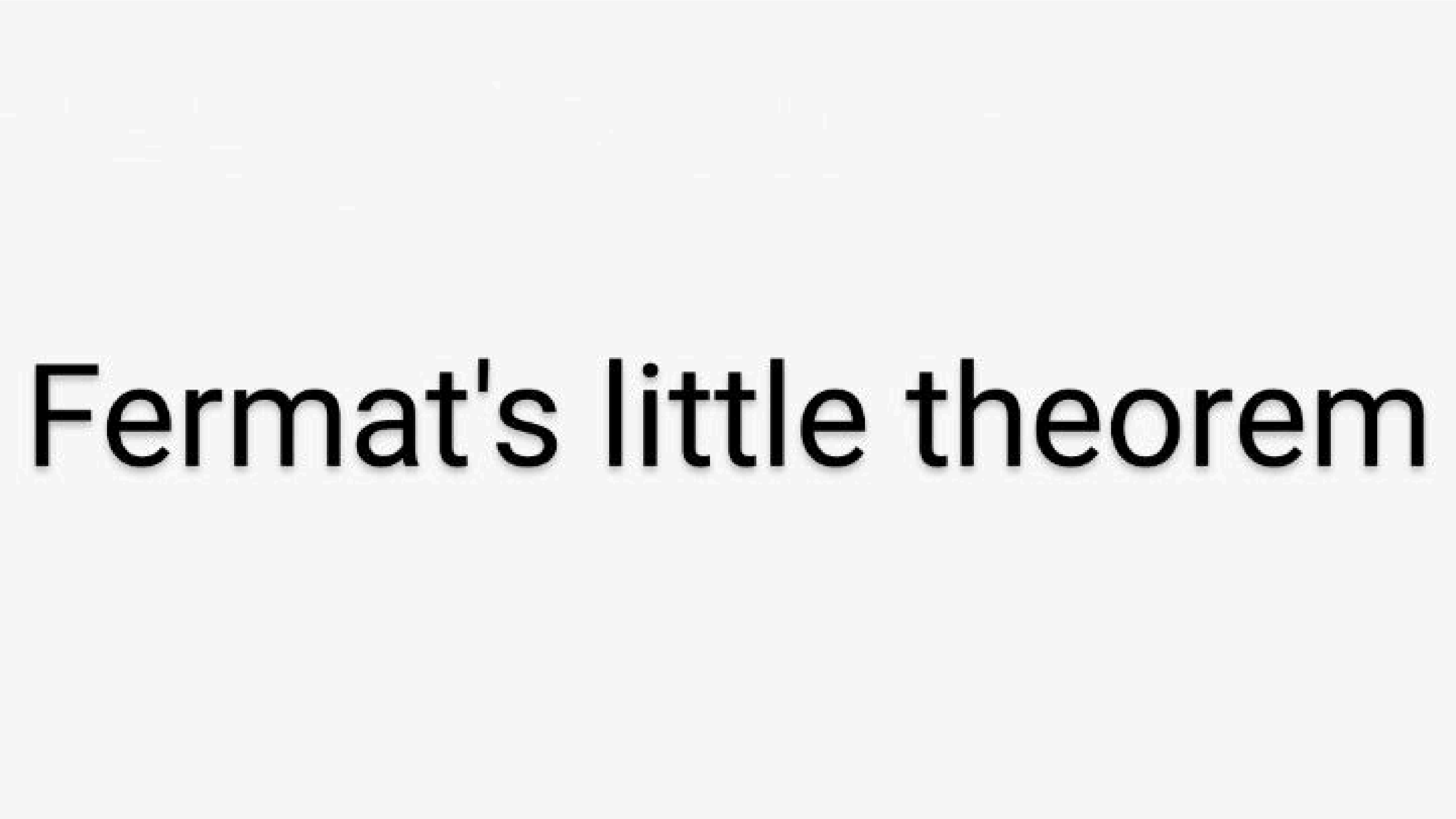
$$10^{10} \equiv 1 \pmod{11}$$

$$-1^{10} \equiv 1 \pmod{11}$$

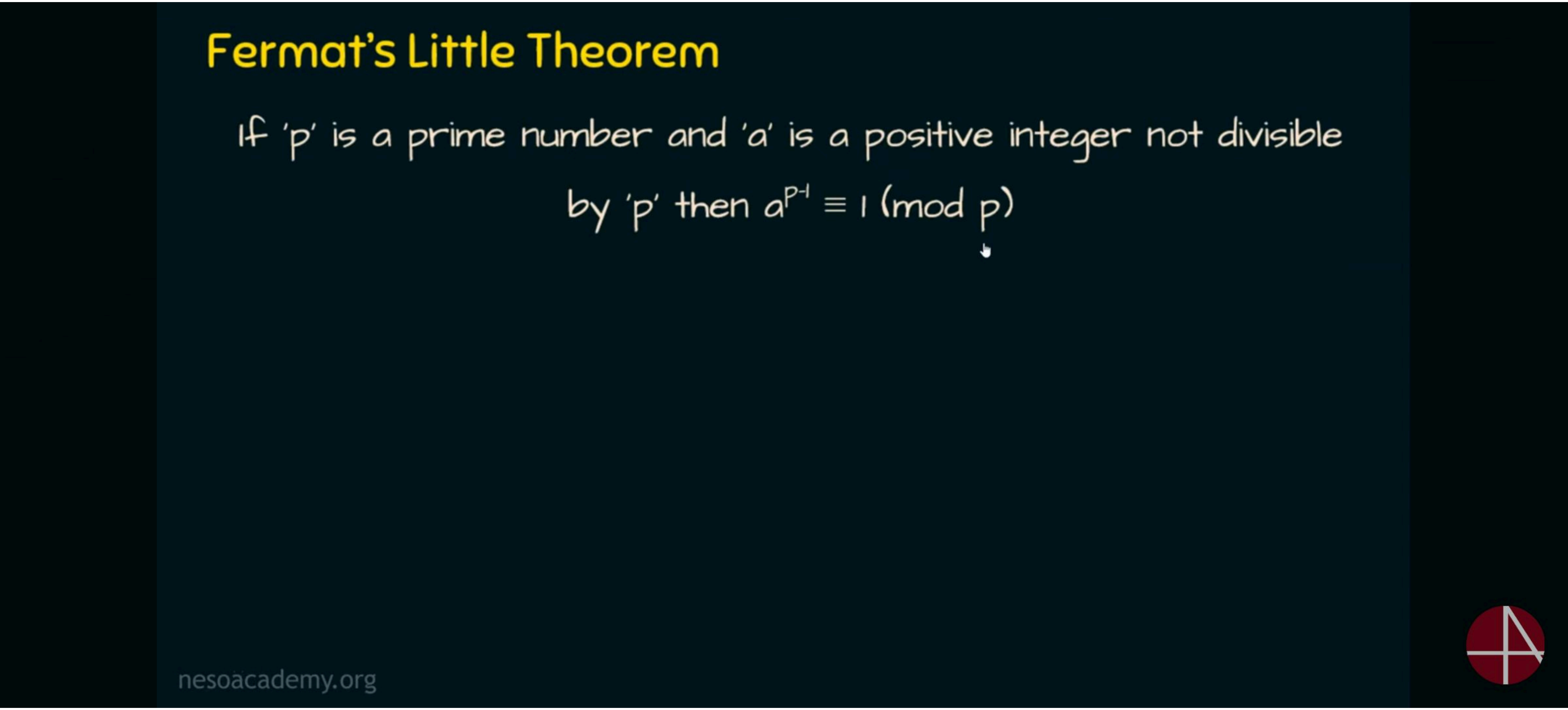
$$1 \equiv 1 \pmod{11}$$

Therefore, Euler's theorem holds for a=10 and n=11.

nesoacademy.org



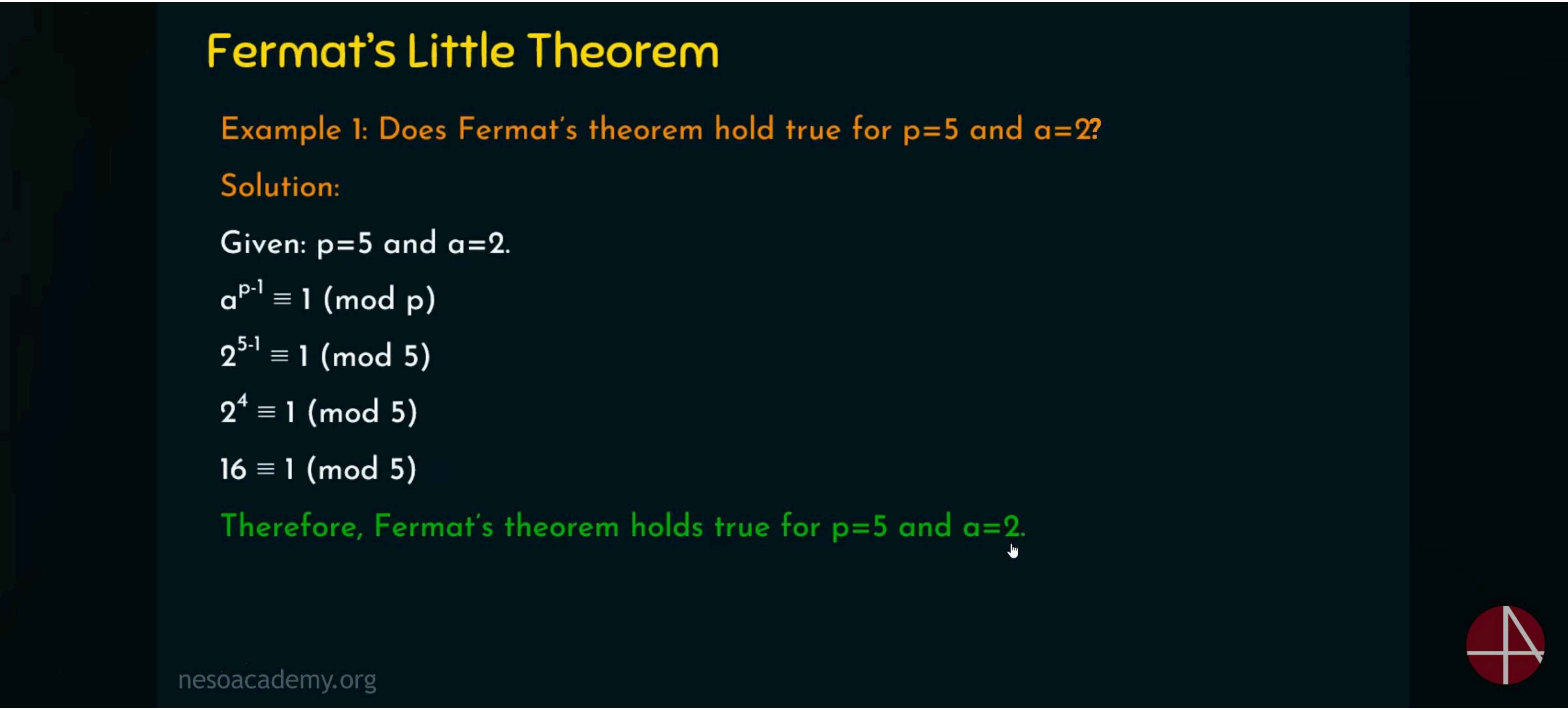
Fermat's little theorem



Fermat's Little Theorem

If 'p' is a prime number and 'a' is a positive integer not divisible by 'p' then $a^{p-1} \equiv 1 \pmod{p}$

nesoacademy.org



Fermat's Little Theorem

Example 1: Does Fermat's theorem hold true for p=5 and a=2?

Solution:

Given: p=5 and a=2.

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

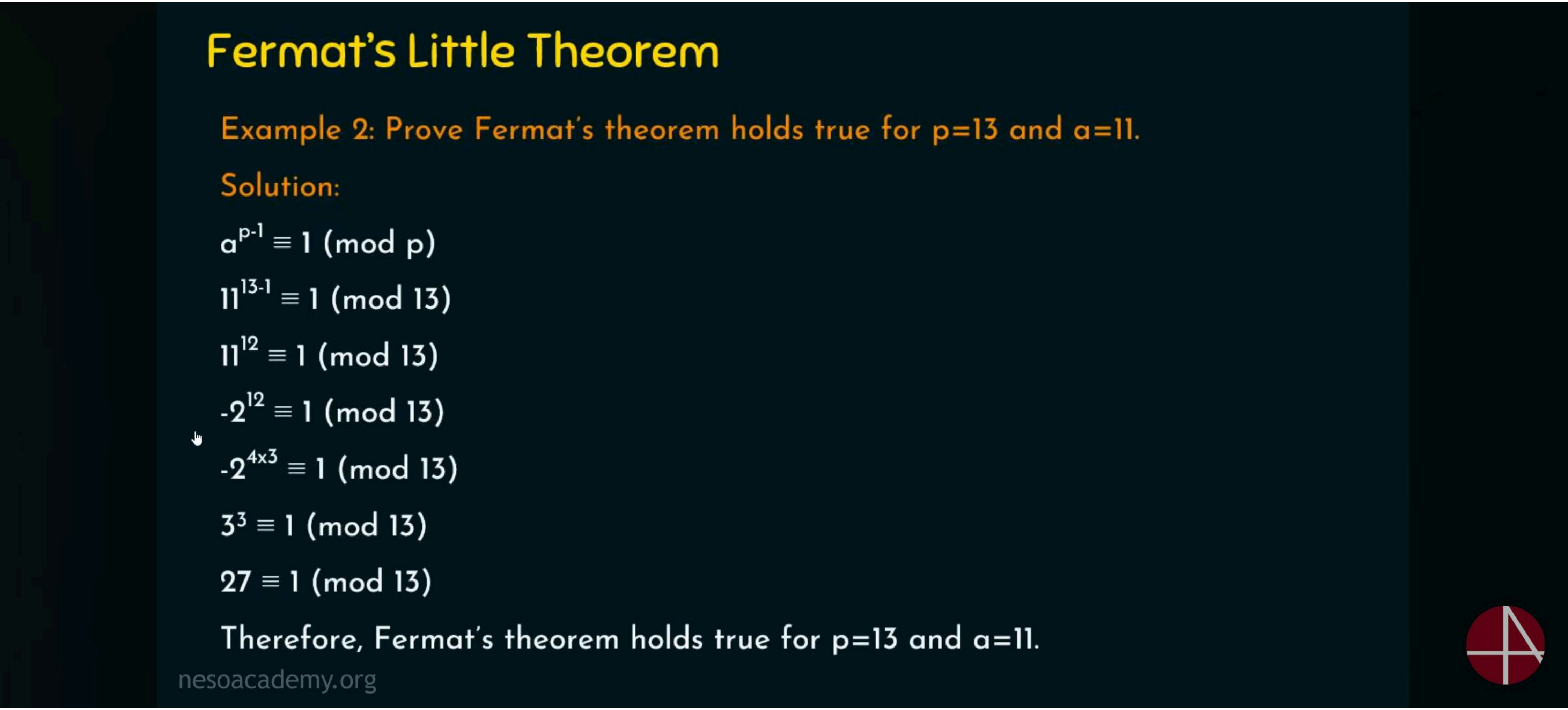
$2^{5-1} \equiv 1 \pmod{5}$

$2^{4} \equiv 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$

Therefore, Fermat's theorem holds true for p=5 and a=2.

nesoacademy.org



Fermat's Little Theorem

Example 2: Prove Fermat's theorem holds true for p=13 and a=11.

Solution:

$a^{p-1} \equiv 1 \text{ (mod p)}$

$11^{13-1} \equiv 1 \text{ (mod 13)}$

$11^{12} \equiv 1 \text{ (mod 13)}$

$-2^{12} \equiv 1 \text{ (mod 13)}$

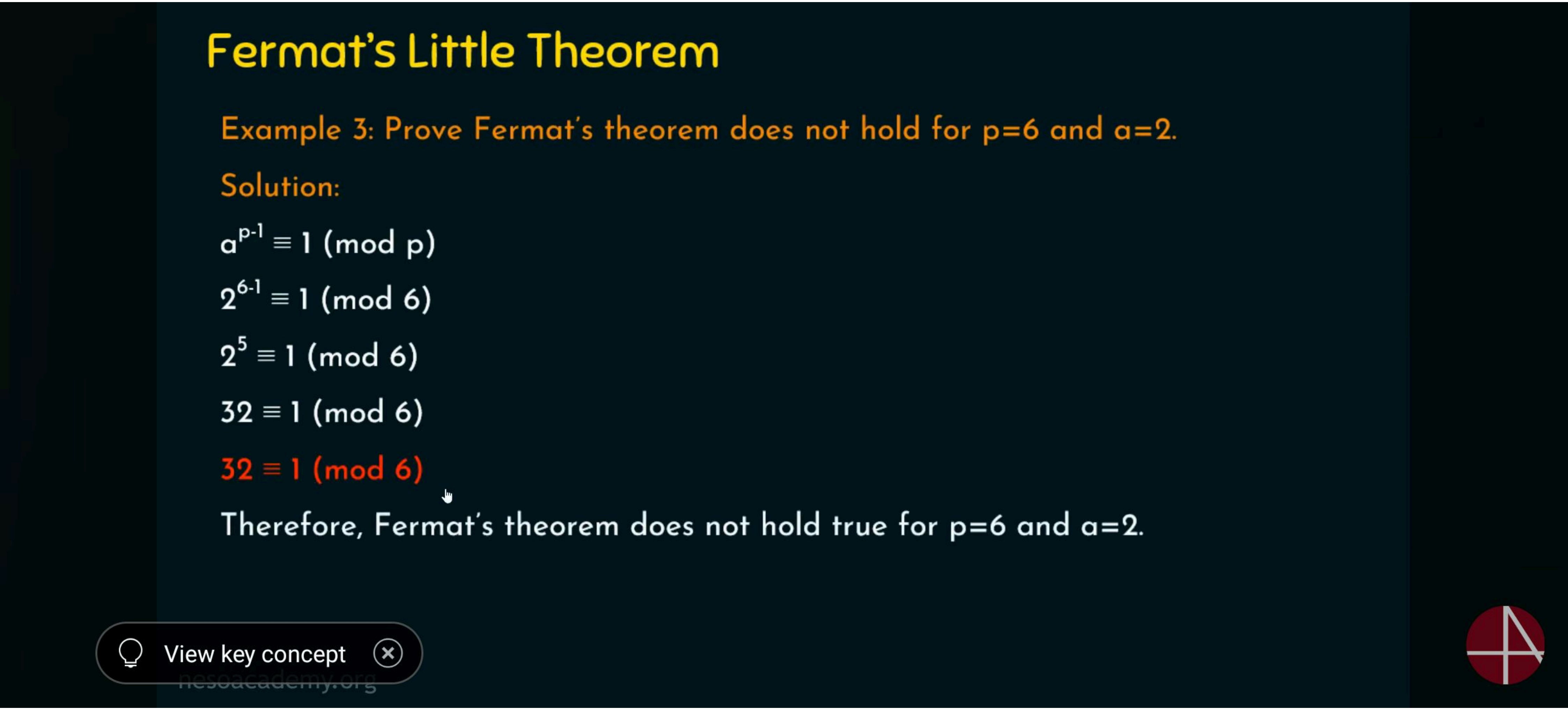
$-2^{4x3} \equiv 1 \text{ (mod 13)}$

$3^3 \equiv 1 \text{ (mod 13)}$

$27 \equiv 1 \text{ (mod 13)}$

Therefore, Fermat's theorem holds true for p=13 and a=11.

nesoacademy.org



Fermat's Little Theorem

Example 3: Prove Fermat's theorem does not hold for p=6 and a=2.

Solution:

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

$2^{6-1} \equiv 1 \pmod{6}$

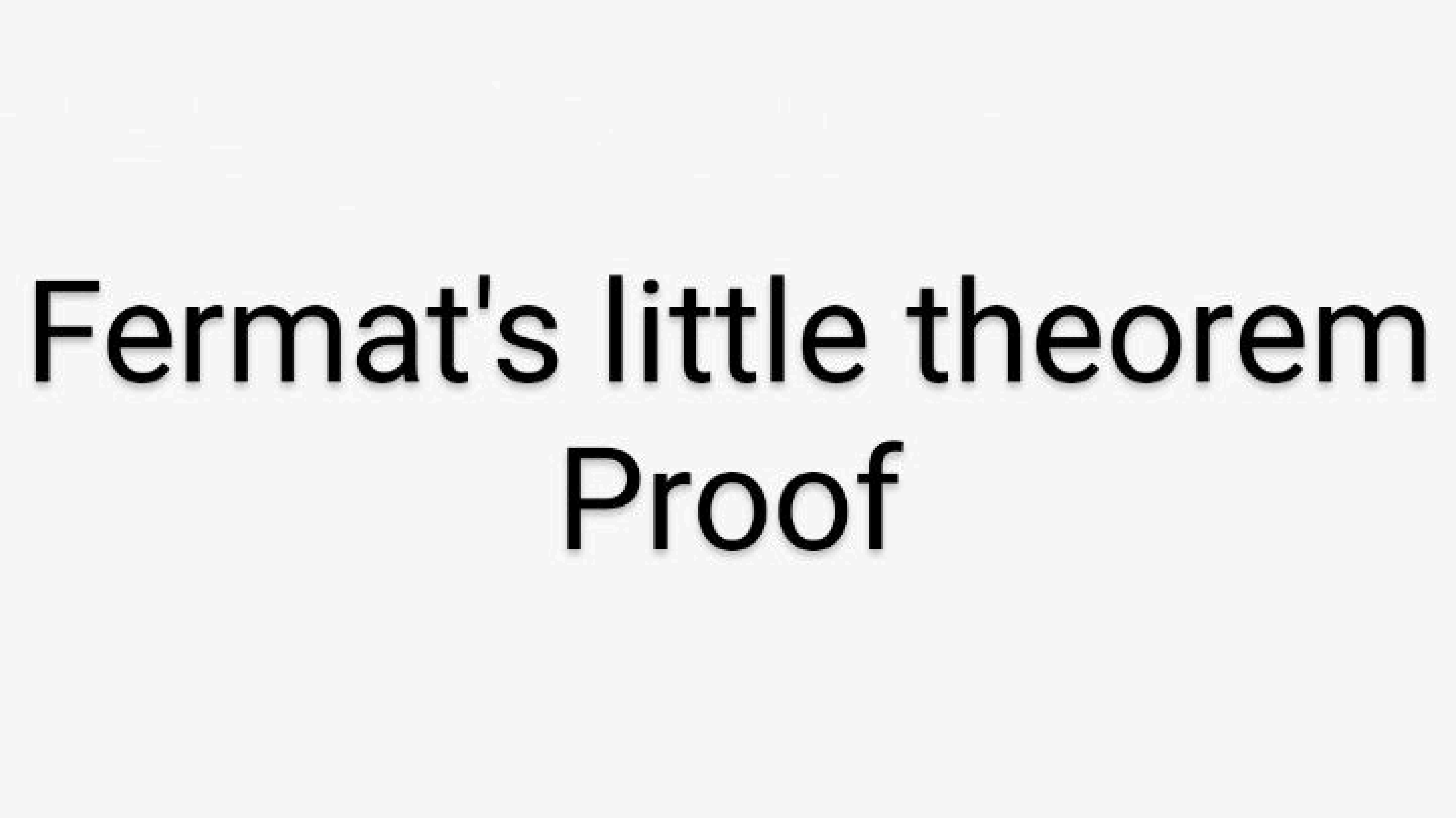
$2^{5} \equiv 1 \pmod{6}$

$32 \equiv 1 \pmod{6}$

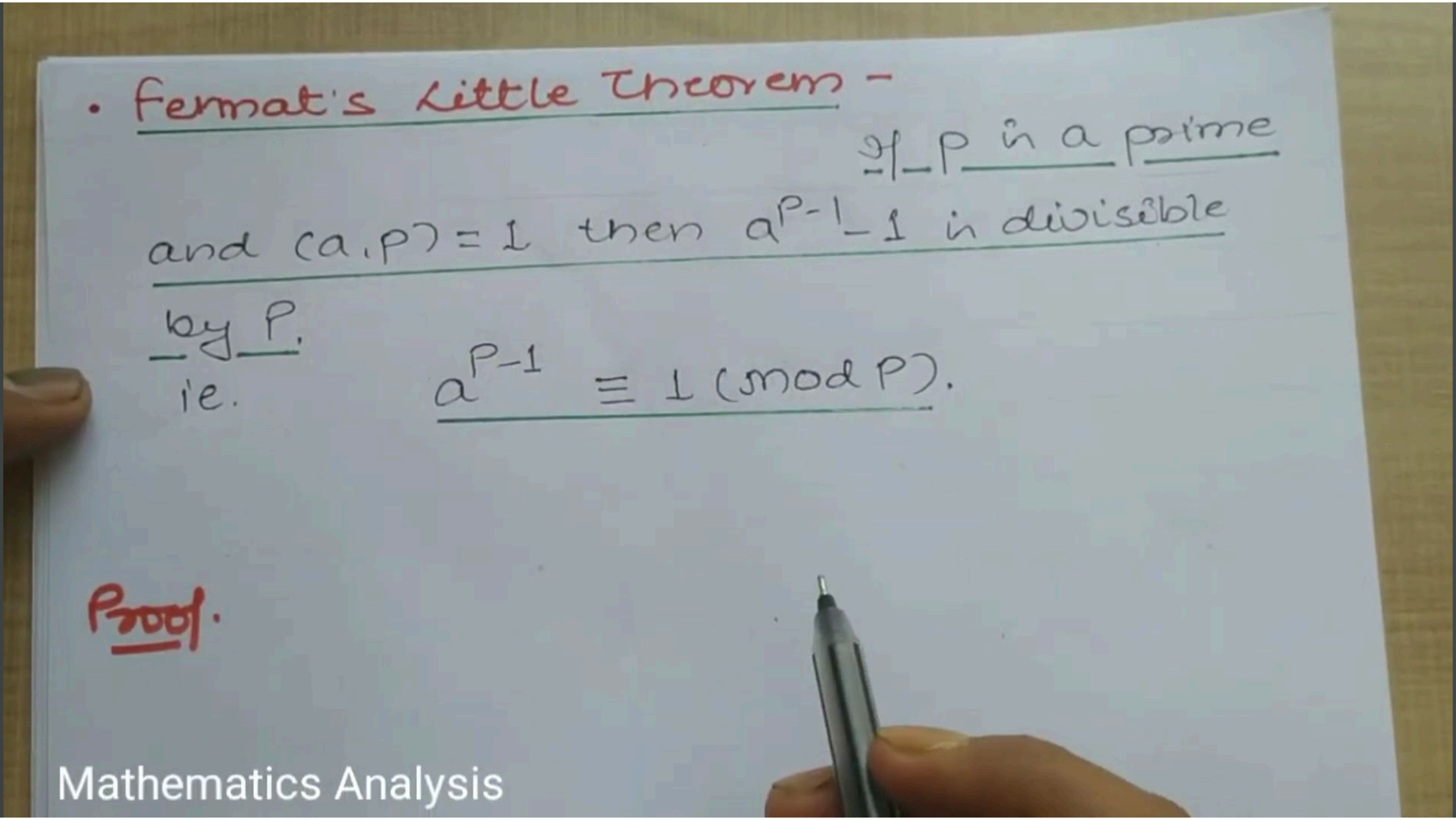
$32 \equiv 1 \pmod{6}$

Therefore, Fermat's theorem does not hold true for p=6 and a=2.

nesoacademy.org



Fermat's little theorem Proof



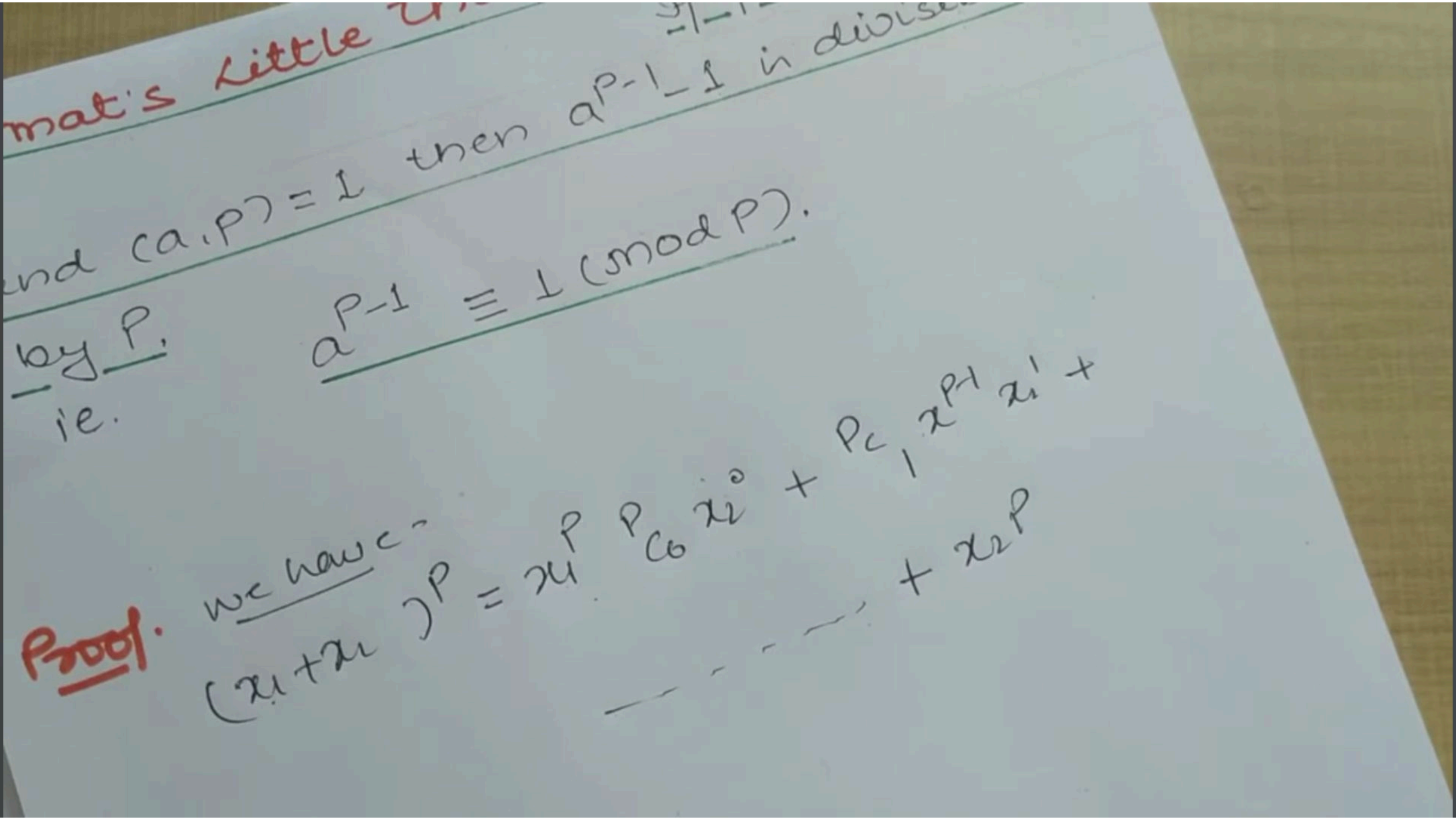
• Fermat's Little Theorem -

If P is a prime and $(a,p) = 1$ then $a^{P-1} - 1$ is divisible by P.

i.e. $$a^{P-1} \equiv 1 \pmod{P}.$$

Proof.

Mathematics Analysis



mat's Little Th

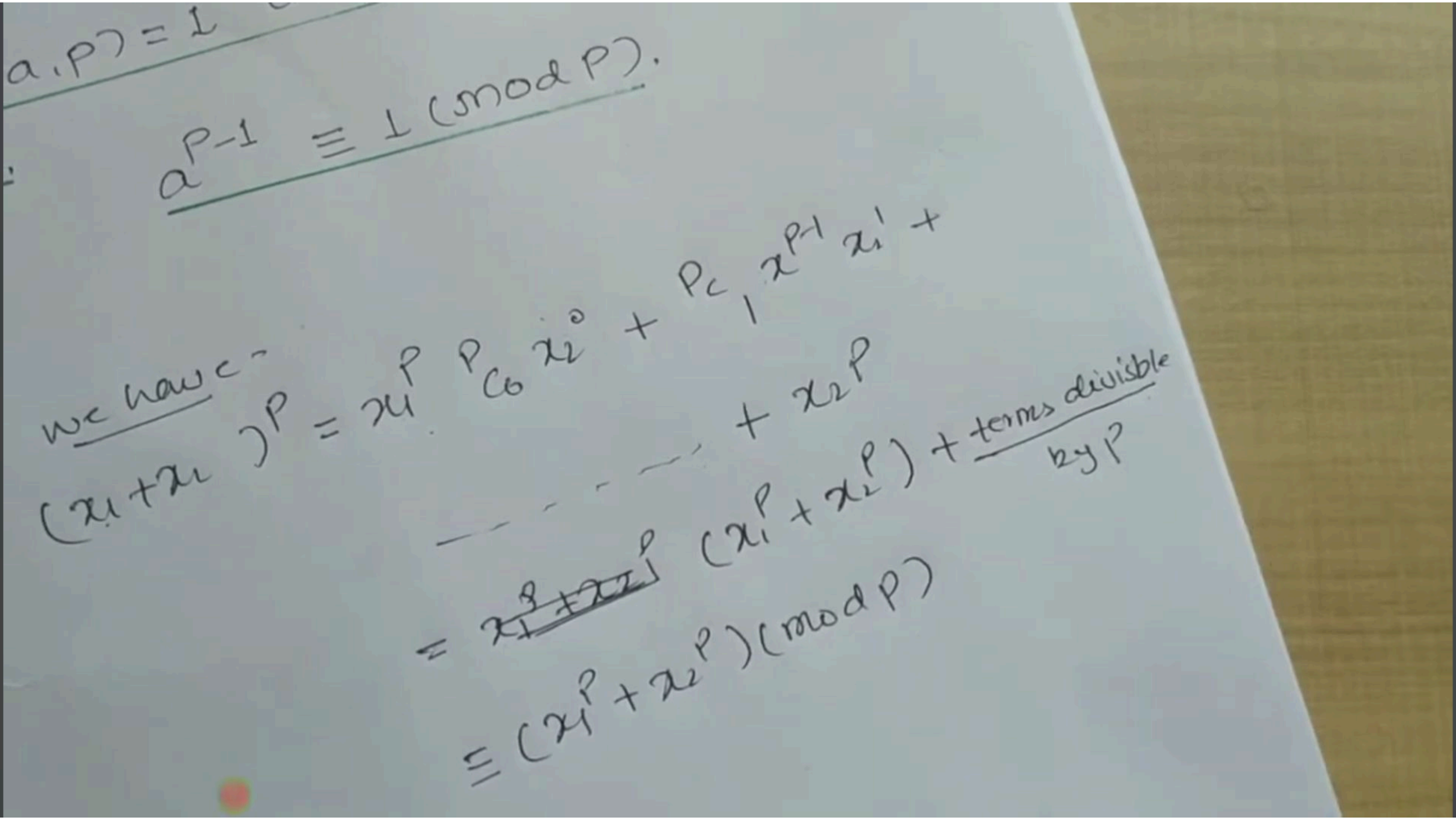
nd $(a,p) = 1$ then $a^{p-1} - 1$ is divis

by p.

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

Proof. we have:-

$(x_1 + x_2)^p = x_1^p \, {}^pC_0 \, x_2^0 + {}^pC_1 \, x^{p-1} x_1^1 + \dots + x_2^p$



$(a, p) = 1$

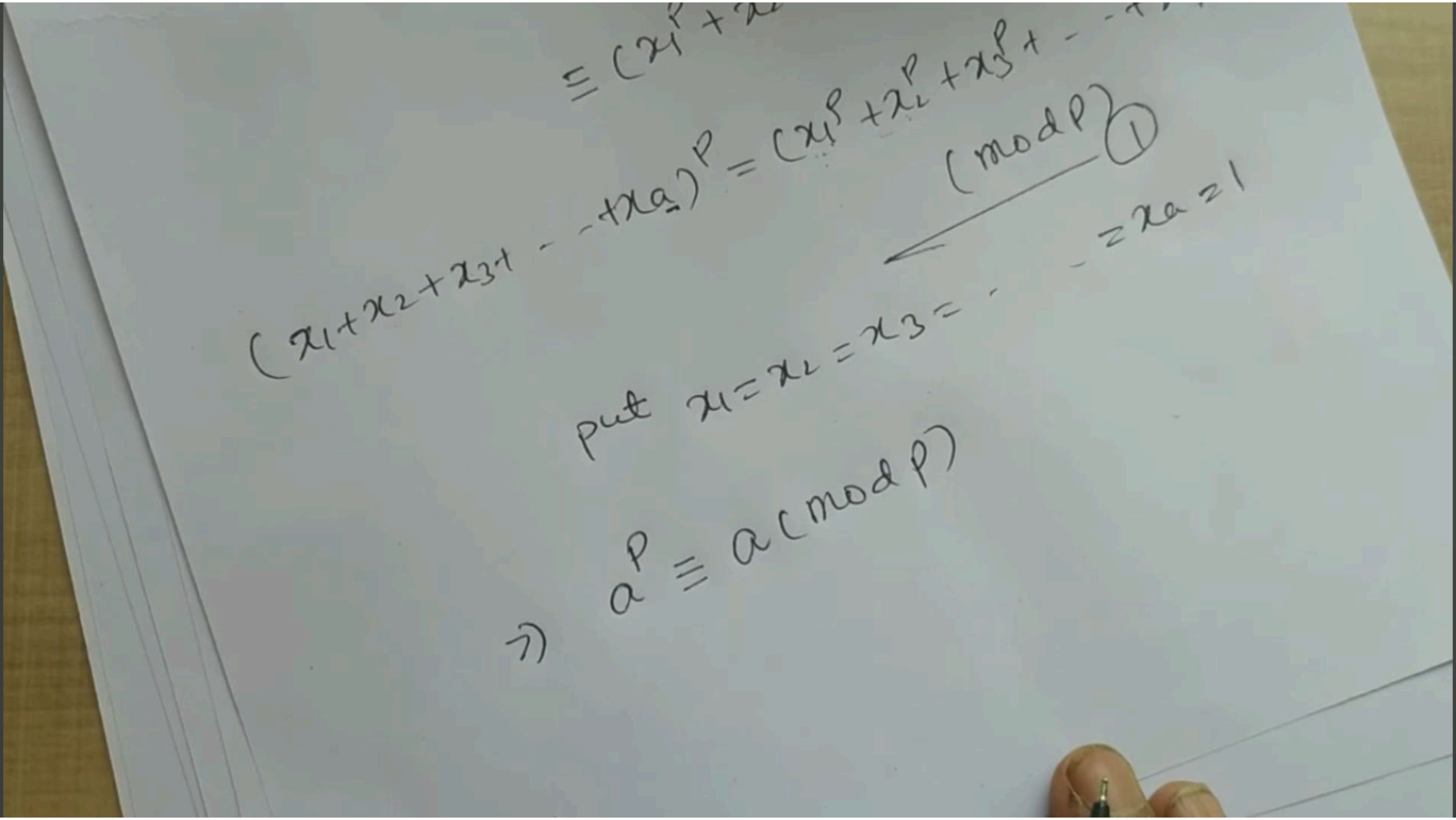
$\underline{a^{p-1} \equiv 1 \pmod{p}}.$

we have:-

$(x_1 + x_2)^p = x_1^p \; {}^pC_0 \, x_2^0 + {}^pC_1 \, x^{p-1} x_1^1 + \dots + x_2^p$

$=$ ~~$x_1^p + x_2$~~ $(x_1^p + x_2^p) + \underline{\text{terms divisible by } p}$

$\equiv (x_1^p + x_2^p) \pmod{p}$

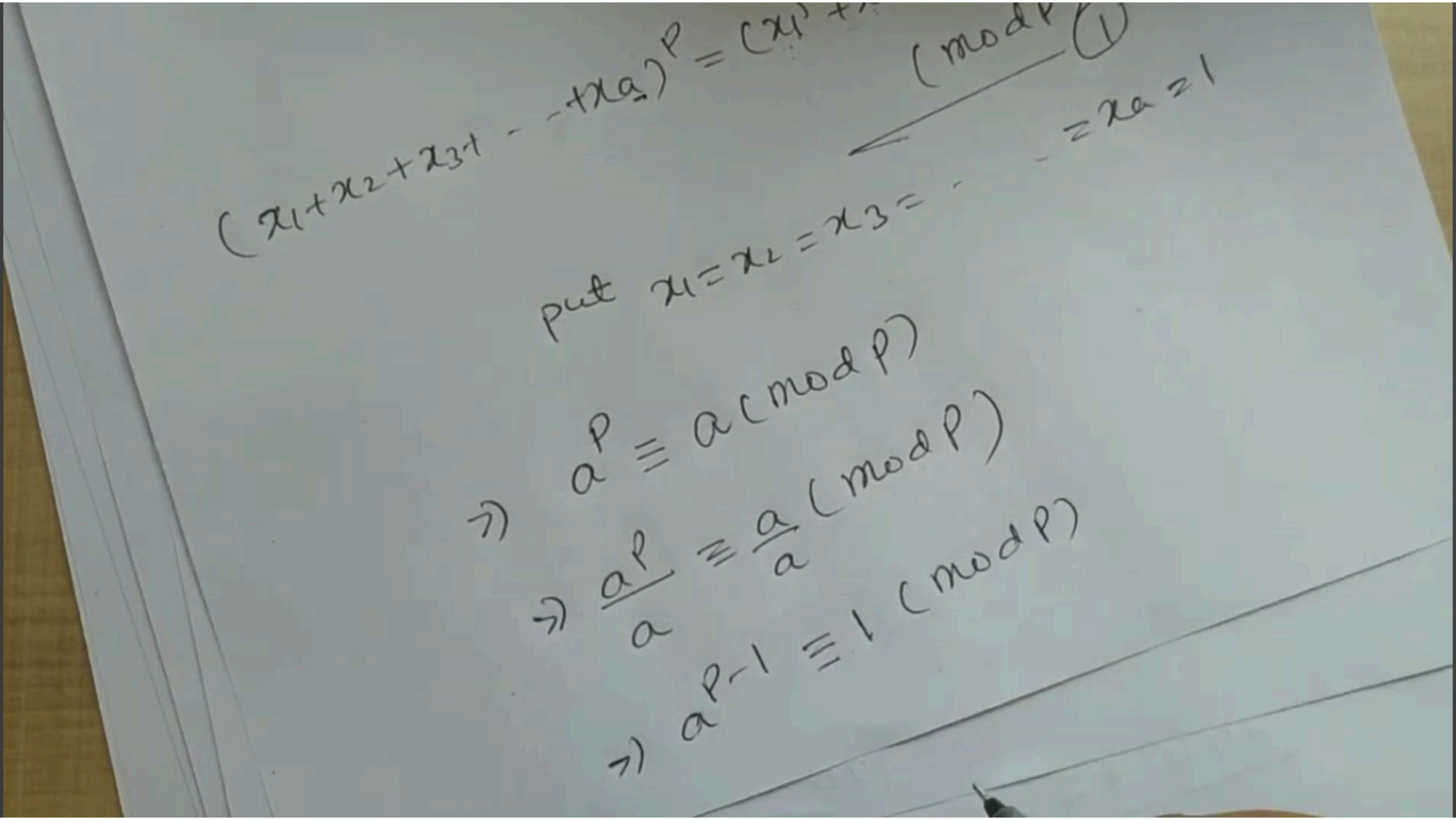


$\equiv (x_1^p + x_2$

$(x_1+x_2+x_3+ \cdots +x_a)^p = (x_1^p + x_2^p + x_3^p + \cdots$ $(\bmod p)$ ①

put $x_1 = x_2 = x_3 = \cdots = x_a = 1$

$\Rightarrow a^p \equiv a \pmod p$



$(x_1+x_2+x_3+ \cdots +x_a)^p = (x_1^p +$

$(\bmod p)$ ①

put $x_1 = x_2 = x_3 = \cdots = x_a = 1$

$\Rightarrow a^p \equiv a \pmod p$

$\Rightarrow \frac{a^p}{a} \equiv \frac{a}{a} \pmod p$

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