Euler's Theorem

- **Euler's Theorem** is a key concept in number theory, named after the Swiss mathematician **Leonhard Euler**.
- It states that if **a** is any integer that is **coprime** with a positive integer **n**, then:

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

- This means that raising **a** to the power of **ϕ(n)** (Euler’s Totient Function) will always leave a remainder of 1 when divided by **n**.
- This is generalized version of **Fermat’s Little Theorem**.
- Interestingly, **Fermat’s Little Theorem** is just a special case of Euler’s Theorem. When **n** is a **prime number p**, $\phi(p) = p - 1$, so Euler’s Theorem becomes Fermat’s Theorem.

Example:

Let's say a = 2 and n = 5.

1. **Calculate φ (5):**

   Euler's totient function, **φ(n)**, counts the number of positive integers less than or equal to n that are relatively prime to **n**. Since 5 is a prime number, all integers from 1 to 4 are relatively prime to it. Therefore, $\varphi(5) = 4$.

2. **Apply Euler's Theorem:**

   According to Euler's theorem, $2^{\varphi(5)} \equiv 1 \pmod 5$. Substituting $\varphi(5) = 4$, we get $2^4 \equiv 1 \pmod 5$.

3. **Verify the result:**

   $2^4 = 16$. When 16 is divided by 5, the remainder is 1. So, $16 \equiv 1 \pmod 5$ is true, which confirms Euler's theorem.

Fermat's Theorem

- It is the specific version of Euler's Theorem, i.e., if one number among the 2 coprime numbers is prime, then this Theorem is applied.
- Fermat's theorem is also called a Fermat's little theorem defines that is P is prime and 'a' is a positive integer not divisible by P then −
  - **$a^{P-1} \equiv 1 \bmod P$**
- Another form is $a^P \equiv a \bmod P$.
  Example a=3, p=5

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.

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.

Primality Testing

- Primality testing is the problem of determining whether a given positive integer is a prime number (divisible only by 1 and itself) or a composite number (having more than two divisors). This field is crucial in modern cryptography, particularly for generating keys in systems like RSA, which rely on large prime numbers.
- Basic Methods of Primality Testing
    1. Trial Division (Basic and Deterministic)
    2. Fermat Primality Test
    3. Miller-Rabin Primality Test
    4. AKS Primality Test (Agrawal–Kayal–Saxena)

Fermat Primality Test

- The Fermat Primality Test is a probabilistic method for determining whether a given number is prime.
- It's based on Fermat's Little Theorem, a fundamental result in number theory.
- **As we know Fermat's Little Theorem**

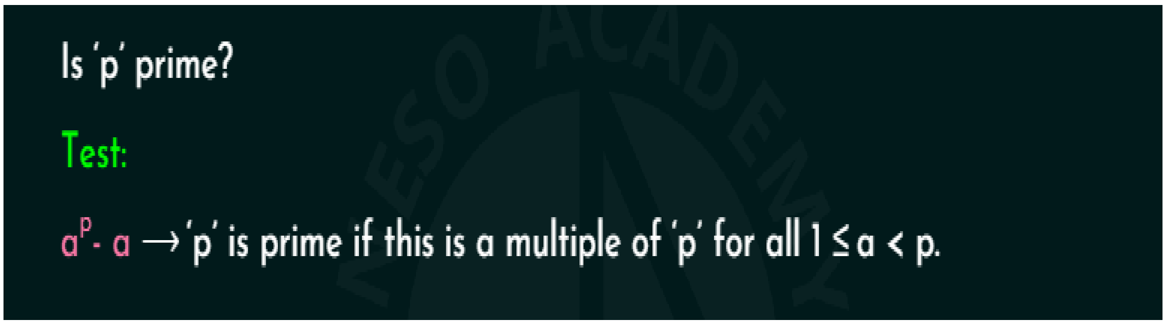
    ✓ Fermat's Little Theorem states that if p is a prime number, then for any integer a not divisible by p (i.e., gcd (a, p) =1), the following congruence holds:

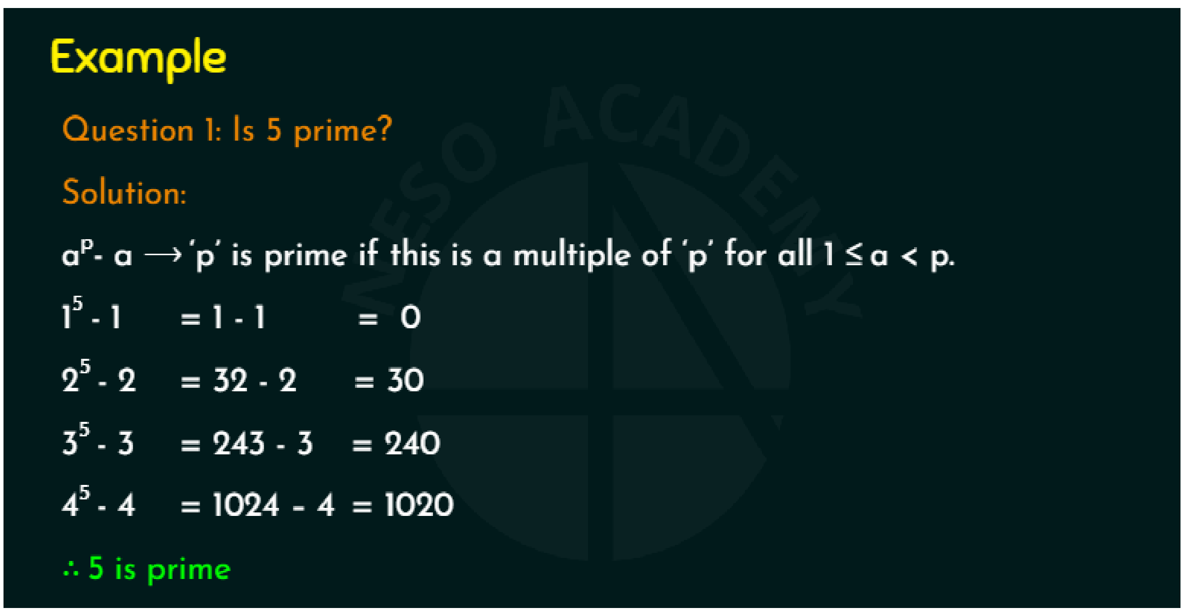
    - $\mathbf{a^{P-1} \equiv 1 \bmod P}$

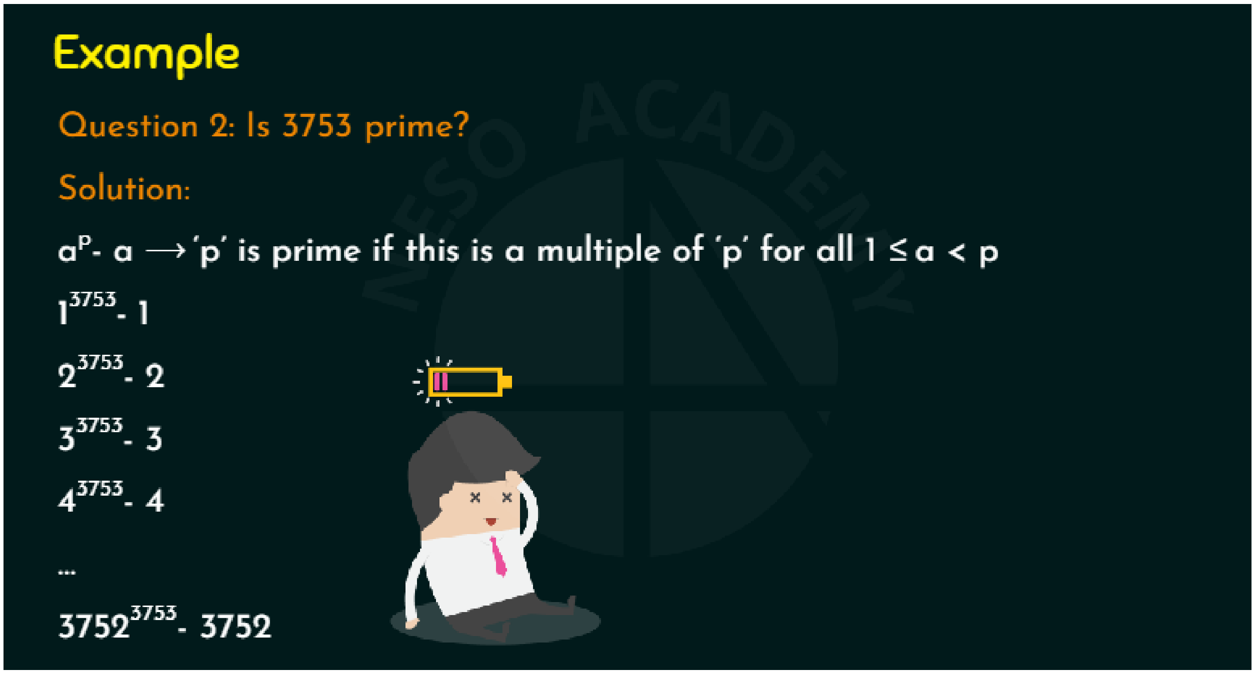
    ✓ This means that if you raise a to the power of p−1 and then divide by p, the remainder will be 1.

How the Fermat Primality Test Works

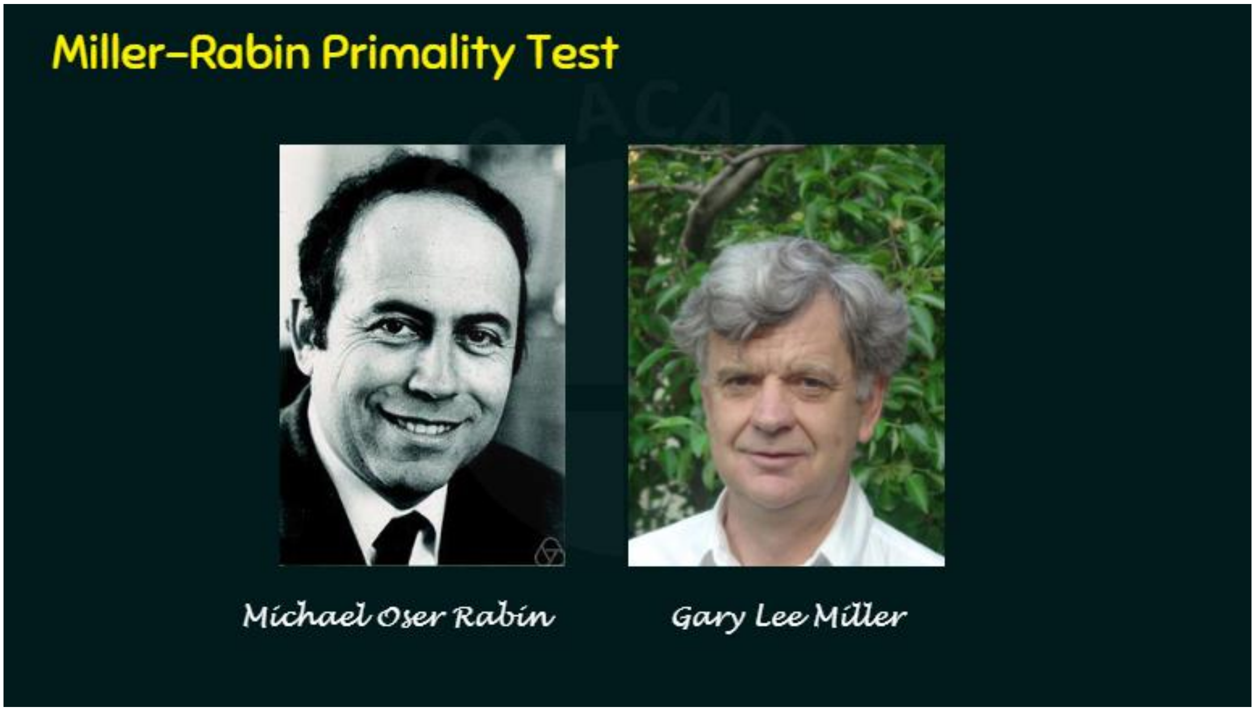
- **Choose a number to test:** Let n be the odd integer you want to test for primality.
- **Choose a random base**: Select a random integer a such that 1< a < n−1.







Miller-Rabin Primality Test



- Miller-Rabin primality test or Rabin-Miller primality test.
- Probabilistic primality test.
- Similar to Fermat primality test and the Solovay-Strassen primality test.
- Checks whether a specific property, which is known to hold for prime values, holds for the number under testing.

Algorithm

Step 1: Find $n-1 = 2^k \times m$

Step 2: Choose 'a' such that $1<a<n-1$

Step 3: Compute $b_0 = a^m \pmod n), \dots, b_i = b^2_{i-1} \pmod n$

$+1 \longrightarrow$ Composite

$-1 \longrightarrow$ Probably Prime

Example

Question: Is 561 prime?

Solution:

Given $n = 561$.

Step 1:

$n-1 = 2^k \times m$

$560 = 2^4 \times 35$

So $k = 4$, and $m = 35$

$\frac{560}{2^1} = 280$ | $\frac{560}{2^2} = 140$ | $\frac{560}{2^3} = 70$ | $\frac{560}{2^4} = 35$ | $\frac{560}{2^5} = 17.5$

Example

Question: Is 561 prime?

Solution:

Given $n = 561$.

Step 2:

Choosing $a = 2$; $1<2<560$

Example

Question: Is 561 prime?

Solution:

Given $n = 561$.

Step 3:

Compute $b_0 = a^m \pmod{n}$

$b_0 = a^m \pmod{n}$

$b_0 = 2^{35} \pmod{561} = 263$

Is $b_0 = \pm 1 \pmod{561}$? NO

So calculate b_1

$b_1 = b_0^2 \pmod{n}$

$b_1 = 263^2 \pmod{561}$

$b_1 = 166$

Is $b_1 = \pm 1 \pmod{561}$? NO

$b_2 = b_1^2 \pmod{n}$

$b_2 = 166^2 \pmod{561}$

$b_2 = 67$

Is $b_2 = \pm 1 \pmod{561}$? NO

$b_3 = b_2^2 \pmod{n}$

$b_3 = 67^2 \pmod{561}$

$b_3 = 1 \longrightarrow$ Composite

$\therefore$ 561 is composite.

❖ Assignment Modular Exponentiation