Theorem: Euler's Theorem

Euler's Theorem

For any integer a coprime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is Euler's totient function.

Statement

Let $n \geq 1$ be an integer and let a be an integer with $\gcd(a, n) = 1$. Then:

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

where $\phi(n)$ counts the number of integers k with $1 \leq k \leq n$ and $\gcd(k, n) = 1$.

Euler's Totient Function

For a positive integer n: - If $n = p$ is Prime Number, then $\phi(p) = p - 1$ - If $n = p^k$, then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ - If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$ (multiplicative)

Proof Using Group Theory

The integers coprime to n form a Group under multiplication modulo n, denoted $(\mathbb{Z}/n\mathbb{Z})^*$. This group has order $\phi(n)$, so by Lagrange's theorem, any element raised to the group order equals the identity.

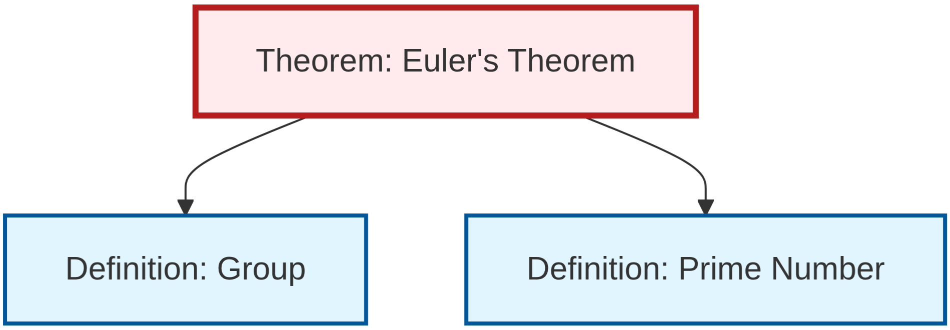
Special Cases

- **Fermat's Little Theorem**: When $n = p$ is prime, $\phi(p) = p - 1$, giving $a^{p-1} \equiv 1 \pmod{p}$
- **Carmichael's Theorem**: A refinement using the Carmichael function $\lambda(n)$

Applications

- RSA cryptography
- Primality testing
- Computing modular inverses: $a^{\phi(n)-1} \equiv a^{-1} \pmod{n}$

Dependency Graph



Local dependency graph