ISSN 2231-3478 (Print)
JUSPS-B Vol. 32(1), 1-3 (2020). Periodicity-Monthly
**Section B**
ISSN 2319-8052 (Online)

**JOURNAL OF ULTRA SCIENTIST OF PHYSICAL SCIENCES**
**An International Open Free Access Peer Reviewed Research Journal of Physical Sciences**
website:- www.ultrascientist.org
Estd. 1989

# A modern proof of fermat's little theorem

LOKANATH SAHOO

Reader in Mathematics Gopabandhu Science College, Athgarh , Cuttack (India)
Corresponding Author Email: lokanath.math@gmail.com
http://dx.doi.org/10.22147/jusps-B/320101

**Acceptance Date 10th June, 2020, Online Publication Date 13th June, 2020**

**Abstract**

Fermat's Little Theorem states that if p is a prime number and a is an integer then $a^p$ is congruent to a modulo p . This result is of huge importance in elementary and algebraic number theory. This theorem has many interesting and sometimes unexpected proofs. One modern proof is based upon Euler's phi function and Euler's theorem.

*Key words :* Prime numbers, relatively prime, Euler's $\phi$ function, group, congruence modulo relation.
**2000 AMS Subject classification Primary 11A99.**

## Introduction

Fermat's Little Theorem states that if p is a prime number and a is an integer then $a^p$ is congruent to a modulo p.This result is of huge importance in elementary and algebraic number theory. This theorem has many interesting and sometimes unexpected proofs. One modern proof is based upon Euler's phi function and Euler's theorem.

*Prime number:* A positive integer p>1 is said to be a prime number if its only divisors are $\pm 1$ or $\pm p$.

*Relatively Prime*: Two positive integers a and b are said to be relatively prime if their greatest common divisor is 1.

*Euler's $\phi$ function:*

Let n be a positive integer. If n=1, then $\phi(n)=1$.

If $n \neq 1$, then $\phi(n)$ is the number of positive integers less than n and relatively prime to n.

*Group:* A non-empty set of elements G is said to be a group if in G there is defined a binary operation o such that the following properties are satisfied:

i. $a, b \in G \Rightarrow a \circ b \in G$ (Closure Property)

ii. a, b, c $\in$ G => a o (b o c) = (a o b) o c (Associative Property)
iii. There exists an element e in G such that a o e =e o a =a for all a $\in$ G.
(Existence of identity element in G)
iv. For every a in G there exists an element b in G such that a o b = b o a = e.
(Existence of identity element in G)

*Congruence modulo relation:* Let a and b be any two integers. Let n be a fixed positive integer. a is said to be congruent to b modulo n if n divides (a-b). It is denoted by a $\equiv$ b mod n.

It can be proved that if G is the set of positive integers less than n and relatively prime to n, then G is a group under the binary operation multiplication modulo n and o(G)= $\phi$(n).

*Theorem-1 ( Euler's Theorem )* If n is a positive integer and a is relatively prime to n , then $a^{\phi(n)} \equiv 1$ mod n.

*Proof:* **case-I** : when a < n.

Then a is a positive integer less than n and relatively prime to n. Then a $\in$ G .

Hence $a^{o(G)}$ =1.

$\Rightarrow$ $a^{\phi(n)}$=1.

$\Rightarrow$ $a^{\phi(n)}$-1=0.

$\Rightarrow$ n / $a^{\phi(n)}$ -1.

$\Rightarrow$ $a^{\phi(n)} \equiv 1$ mod n. ( as n/0 )

**case-II** : when a > n .

By Division Algorithm, there exists integers q and r such that a = q n + r where 0 < r < n .

$\Rightarrow$ a – r = q n .

$\Rightarrow$ n / (a – r ) .

$\Rightarrow$ n / ($a^{\phi(n)}$ - $r^{\phi(n)}$) .

$\Rightarrow$ $a^{\phi(n)} \equiv r^{\phi(n)}$ mod n .

Now, r is a positive integer less than n and relatively prime to n .

Then r $\in$ G .

$\Rightarrow$ $r^{o(G)} = 1$ .

$\Rightarrow$ $r^{\phi(n)} = 1$ .

$\Rightarrow$ $r^{\phi(n)} - 1 = 0$ .

$\Rightarrow$ n / ( $r^{\phi(n)} - 1$ ) .

$\Rightarrow$ $r^{\phi(n)} \equiv 1$ mod n.

Then by transitive , $a^{\phi(n)} \equiv 1$ mod n.

By the use of Euler's Theorem, the famous Fermat's Theorem can be proved as follows:

*Theorem-2 ( Fermat's Theorem )* If p is a prime number and a is any integer, then $a^p \equiv$ a mod p .

Proof : Since p is a prime number, so $\phi$(p) = p - 1 .

**Case -1 :** when a is relatively prime to p .

Now , p is a positive integer and a is relatively prime to p .

⇨ $a^{\phi(p)} \equiv 1 \bmod p$ . ( By Euler's Theorem )

⇨ $a^{p-1} \equiv 1 \bmod p$.

⇨ p / ($a^{p-1}$ - 1 ) .

⇨ p / a ($a^{p-1}$ - 1 ) .

⇨ p / ($a^{p}$ - a ) .

⇨ $a^{p} \equiv a \bmod p$ .

**Case-2** : when a is not relatively prime to p .

Since p is prime, so p / a .

⇨ p / a ($a^{p-1}$ - 1 ) .

⇨ p / ($a^{p}$ - a ) .

⇨ $a^{p} \equiv a \bmod p$ .

**References**

1. Wikipedia, the Free Encyclopedia , Several Classical and less know proofs of Fermat's Little Theorem available at http://en.wikipedia.org/wiki/proofs_of_Fermat's_little_theorem (2008).
2. S. Padhi and Lokanath Sahoo "Topics In Algebra" Kalyn Publishers, New Delhi (2006).
3. Conway J. H. and Guy R. K., The book of numbers , Springer, New York (1996).
4. Hardy G. H. and Wright E. M. An introduction to theory of numbers, Oxford University Press, New York (2008).