Generalization of the Fermat's and Euler's Theorems

Kurmet Sultan (kurmetsultan@mail.ru)
Non

Research Article

Keywords: Fermat's little theorem, Euler's theorem, remainder, generalization.

Posted Date: February 15th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1360013/v1

Generalization of the Fermat's and Euler's Theorems

Kurmet Sultan

Abstract: The article contains extended versions of Fermat's little theorem and Euler's theorem, as well as a theorem intended for any remainder, which generalizes Fermat's and Euler's theorems.
Key words: Fermat's little theorem, Euler's theorem, remainder, generalization.

1. Introduction

Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then $a^{p-1}-1$ is divisible by p, i.e. $a^{p-1} \equiv 1\ (mod\ p)$. An alternative formulation of this theorem is as follows: if a is any integer, then $a^p \equiv a\ (mod\ p)$.

Euler's Theorem, which generalizes Fermat's Little Theorem, states: if the numbers *a* and *m* are coprime, then $a^{\varphi(m)} \equiv 1\ (mod\ m)$, where $\varphi(m)$ is the Euler function[1, 2, 3].

A study of papers [1 ,2, 3, 4, 5] in which the theorems of Fermat and Euler are described, as well as the laws of power residues, shows that these and other similar theorems are intended mainly for the remainder equal to 1, (-1), the base a of degree divisible number a^n, as well as some individual remainders, i.e. in the known sources, there is no clear structuring of power residues. It follows that the generalization of Fermat's Little Theorem and Euler's theorem, as a result of which the cyclicity of all remainders is established, is important, so it can be used to solve some open problems of mathematics.

2. Extended versions of the Fermat's Little Theorem and Euler's Theorem

Based on the results of our research, we propose the following extended versions of Fermat's Little Theorem and Euler's Theorem:

2.1. Extended version of Fermat's Little Theorem

If p is a prime number and a is an integer not divisible by p, then $a^{(p-1)t} \equiv 1\ (mod\ p)$*, and if a is any integer, then* $a^{p+(p-1)t} \equiv a\ (mod\ p)$.

2.2. Extended version of Euler's Theorem

If the numbers a and m are coprime, then $a^{\varphi(m)t} \equiv 1\ (mod\ m)$*, where φ (m) is the Euler function; t = 1,2, ...*

The importance of the extended versions of Fermat's Little Theorem and Euler's Theorem is that they show the cyclicity of the remainders in terms of the exponents of divisible numbers.

3. Generalization of the Fermat's and Euler's Theorems

Below is a theorem that generalizes Fermat and Euler's theorems:

Theorem 3.1 (Generalization of Fermat's and Euler's Theorems)

1) If a^n *is a natural power of a natural number,* p^x *is a natural power of a prime number, and* $a^n \equiv r\ (mod\ p^x)$*, then* $a^{n+(p^x-p^{(x-1)})t} \equiv r\ (mod\ p^x)$*, where r = 0,1,2, ...,* p^x-1*; n, t = 1,2,....*

2) If a^n *is a natural power of a natural number, m is a natural number, and* $a^n \equiv r\ (mod\ m)$*, then* $a^{n+\varphi(m)t} \equiv r\ (mod\ m)$*, where r = 0,1,2, ... ,* $m-1$*; n, t = 1, 2, ...*

Example 1: if $p^x = 3^2$, $a^n = 7^1$, $7^1 \equiv 7\ (mod\ 3^2)$, $t = 1$, then $7^{1+(3^2-3)\cdot 1} \equiv 7\ (mod\ 3^2)$.

Example 2: if $p^x = 5^2$, $a^n = 3^3$, $3^3 \equiv 2\ (mod\ 5^2)$, $t = 4$, then $3^{3+(5^2-5)\cdot 4} \equiv 2\ (mod\ 5^2)$.

Example 3: if $m = 14$, $a^n = 5^2$, $5^2 \equiv 11\ (mod\ 14)$, $\varphi(14) = 6$, $t = 8$, then $5^{2+6\cdot 8} \equiv 11\ (mod\ 14)$.

Theorem 3.1, which is based on the Fermat and Euler theorems, is explained as follows.

It is known that $a^0 \equiv 1\ (mod\ p)$ and $a^1 \equiv a\ (mod\ p)$, and Fermat's Little Theorem implies that $a^{p-1} \equiv 1\ (mod\ p)$ and $a^p \equiv a\ (mod\ p)$, it follows that the cycle length of the exponent is $p - 1$. In the case when the divisor is a composite number, then, in accordance with Euler's theorem, the cycle length of the exponent will be equal to $\varphi(m)$.

Theorem 3.1 defines the search area for solutions of equations of the form $p^x + b^y = c^z$, where p is a prime number, by the remainder matrix of size $(p^x - 1)$ x $(p^x - p^{(x-1)})$, which is shown in Table 1. Table 1 shows the remainders r_{ij} obtained by dividing natural numbers of the form a^n by a natural power of a prime p^x.

Table 1. Matrix of remainders for the divisor p^x

a	a^1	a^2	a^3	…	$a^{p^x - p^{x-1}}$
0	$r_{01} = 0$	$r_{02} = 0$	$r_{03} = 0$	…	$r_{0(p^x - p^{x-1})} = 0$
1	$r_{11} = 1$	$r_{12} = 1$	$r_{13} = 1$	…	$r_{1(p^x - p^{x-1})} = 1$
2	$r_{21} = 2$	r_{22}	r_{23}	…	$r_{2(p^x - p^{x-1})} = 1$
3	$r_{31} = 3$	r_{32}	r_{33}	…	$r_{3(p^x - p^{x-1})} = 1$
…	…	…	…	…	…
p^x**-1**	$r_{(p^x-1)1} = p^x$-1	$r_{(p^x-1)2}$	$r_{(p^x-1)3}$	…	$r_{(p^x-1)(p^x - p^{x-1})} = 1$

When the divisor is a composite number m, the remainder matrix has size $(m - 1)$x $a^{\varphi(m)}$, which looks like Table 2, this matrix shows the search area for solutions of equations of the form $a^x + b^y = c^z$.

Table 2. Matrix of remainders for composite divisor m

a	a^1	a^2	a^3	…	$a^{\varphi(m)}$
0	$r_{01} = 0$	$r_{02} = 0$	$r_{03} = 0$	…	$r_{0a^{\varphi(m)}} = 0$
1	$r_{11} = 1$	$r_{12} = 1$	$r_{13} = 1$	…	$r_{1a^{\varphi(m)}} = 1$
2	$r_{21} = 2$	r_{22}	r_{23}	…	$r_{2a^{\varphi(m)}} = 1$
3	$r_{31} = 3$	r_{32}	r_{33}	…	$r_{3a^{\varphi(m)}} = 1$
…	…	…	…	…	…
m**-1**	$r_{(m-1)1} = m$-1	$r_{(m-1)2}$	$r_{(m-1)3}$	…	$r_{(m-1)a^{\varphi(m)}} = 1$

If we expand the above matrices (Tables 1 and 2), then the remainders will be repeated both in rows and columns of the matrix. Therefore, if all the elements of the above matrices for a given divisor are known, then using the formulas of Theorem 3.1, you can calculate any remainder resulting from dividing any power of any natural number by a given natural number.

Conclusion

Theorem 3.1 differs from Fermat's and Euler's theorems, which use the remainder 1 and the base a of the divisible number a^n, in that it is intended for any remainder *r*, i.e. it generalizes the

theorems of Fermat and Euler. Theorem 3.1 precisely defines the search area for solutions of equations of the form $a^x + b^y = c^z$ or $A + B = C$.

Statements and Declarations

This work was not funded by anyone, and no one except the author took part in the research and writing of the manuscript.

References

[1] GODFREY H. HARDY, EDWARD M. WRIGHT, JOSEPH SILVERMAN, ANDREW WILES, An Introduction to the Theory of Numbers: OUP Oxford, 2008.

[2] SENGADIR T, Discrete Mathematics and Combinatorics. Chennai, India: Pearson Education India, 2009.

[3] CARGAL J. M., Discrete Mathematics for Neophytes: Number Theory, Probability, Algorithms, and Other Stuff, 1988.

[4] IRELAND, KENNETH; ROSEN, MICHAEL, A Classical Introduction to Modern Number Theory (Second edition), New York: Springer, 1990.

[5] LEMMERMEYER, FRANZ, Reciprocity Laws: from Euler to Eisenstein,
Berlin: Springer, 2000.