Generalization of the Fermat's and Euler's Theorems

Курмет Султан

Abstract: the article contains extended versions of Fermat's little theorem and Euler's theorem, as well as a theorem that 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. $a^{p-1} \equiv 1 \ (mod\ p)$, and if a is any integer, then $a^p \equiv a \ (mod\ p)$ [1].

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

Based on the results of his research, the author proposes 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 differs from the theorems of Fermat, Euler, and Carmichael, which use only the remainder 1 or the base of the divisible number, in that it is intended for any remainder. The proof of Theorem 3.1 is omitted, since it is based on the theorems of Fermat and Euler.

References

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