ABSTRACT

CHARACTERISTIC OF CARMICHAEL NUMBER

By

DEVI PURNAMA SARI

Recall that Fermat's "little theorem" says that if p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1$ (mod p). This theorem gives a possible way to detect primes, or more exactly, non-primes: if for a certain a coprime to n, a^{n-1} is not congruent to 1 mod n, then, by the theorem, n is not prime. A lot of composite numbers can indeed be detected by this test, but there are some that evade it.

For a fixed $a > 1$, we write $F(a)$ for the set of positive integers n satisfying $a^{n-1} \equiv 1$ mod n. By Fermat's theorem, $F(a)$ includes all primes that are not divisors of a. If n ∈ F(a), then $\gcd(a,n) = 1$, since, clearly, $\gcd(a^{n-1}, n) = 1$. Also, $a^{n} \equiv a$ mod n;the reverse implication is true provided that a and n are coprime. A composite number n belonging to $F(a)$ is called an a-pseudoprime, or a pseudoprime to the base a. A number n that is a-pseudoprime for all a coprime to n is called a Carmichael number.

Numbers of the form (6m + 1)(12m + 1)(18m + 1) where all three factors are simultaneously prime are the best known examples of Carmichael numbers.

Keywords : Carmichael number, positive integer , prime number, composite number, coprime, pseudoprima.