Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-898-4_13

Chapter 13: A study of Fermat Numbers and Generalized Fermat numbers

Santana Hazarika[1]

[1]*Department of Mathematics, Jengraimukh College, Assam, India.*

Abstract: We have studied Fermat numbers of the form $F_n = 2^{2^n} + 1$, where n is a non-negative integer. We have also studied various properties of Fermat numbers and factorization of Fermat numbers and their applications. We have also studied generalized Fermat numbers and generalized Fermat primes.

Keywords: Fermat numbers, Fermat primes, Composite Fermat numbers, Generalized Fermat numbers, generalized Fermat primes.

Introduction

The French mathematician Pierre de Fermat (1601-1665) became well known for Fermat's last theorem and Fermat little theorem (proved by Euler), but also the number of the form $F_n = 2^{2^n} + 1$ for $n = 0,1,2, \ldots$ the number F_n are known as Fermat numbers after him. If F_n is prime, then it is called the Fermat prime. The first five numbers $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are Fermat primes.

The necessary condition for $2^m + 1$ to be prime for a positive integer m is that the exponent m be of the form 2^n for $n = 0,1,2, \ldots$ this is because if k is a positive integer and $t \geq 3$ is an odd integer, then $2^{kt} + 1 = (2^k + 1)(2^{k(t-1)} - 2^{k(t-2)} + \cdots - 2^k + 1)$.

From this is follows that the number $2^m + 1$ is composite whenever the exponent m is divisible by an odd number $t \geq 3$.

In 1732 Euler found that $F_5 = 641.6700417$ is composite and thus disproved the Fermat conjecture [1].

In these studies we have seen that how can be applied Fermat numbers to prove that there exist infinitely many primes, strong pseudoprimes. However, the Fermat numbers also have several practical applications. They are used in the construction of generations of pseudorandom numbers.

Fermat Numbers

For numbers having a special form, there are some methods to they are primes or composites. The number of the form $2^m + 1$ were considered long ago. If $2^m + 1$ is prime, then m must be of the form $m = 2^n$.

We have following some theorem.

Theorem 1. If $2^n + 1$ is an odd prime, then n is power of 2.

Proof. If n is a positive integer but not a power of 2, then $a^m - b^m = (a - b)\sum_{k=0}^{m-1} a^k b^{m-1-k}$, for