Title: Revisiting Fermat's Little Theorem: Modular Properties of Composite Numbers with Two Prime Factors

Author: Leon Botha (Leobot Electronics)

Date: 21 April 2024

Abstract: Fermat's Little Theorem is a cornerstone of number theory, asserting that for prime numbers, raised to the power of a prime number minus one, the result is congruent to 1 modulo the prime. This theorem has profound implications in various fields, particularly cryptography. However, recent investigations have unveiled a nuanced extension of this theorem, contradicting its original scope. We present a thorough analysis of composite numbers possessing precisely two prime factors, revealing unexpected modular properties that challenge Fermat's original assertion. Through rigorous mathematical reasoning and modular arithmetic, we establish that these composite numbers exhibit distinctive congruence patterns, shedding new light on their structural characteristics. Our findings not only extend the applicability of Fermat's Little Theorem but also offer novel insights into the modular behavior of composite numbers with biprime factors. The significance of this finding is that Fermat's Little Theorem can be extended to composite numbers.

Keywords: Fermat's Little Theorem, modular arithmetic, composite numbers, prime factors, congruence patterns

Introduction: Fermat's Little Theorem stands as a pillar in the realm of number theory, elucidating the intricate relationship between prime numbers and modular arithmetic. Formulated by Pierre de Fermat in the 17th century, the theorem asserts a fundamental property: for any prime number p, and any integer a not divisible by p, a^(p−1) is congruent to 1 modulo p. This elegant theorem has found applications in diverse fields, from cryptography to primality testing. However, its applicability has traditionally been confined to prime numbers, leaving the modular properties of composite numbers largely unexplored.

In this paper, we embark on a journey to revisit Fermat's Little Theorem and explore its implications for composite numbers with precisely two prime factors. While prime numbers have long been heralded as the quintessential subjects of number theory, composite numbers possess a rich tapestry of properties waiting to be unraveled. By delving into the modular behavior of composite numbers with biprime factors, we aim to extend the boundaries of Fermat's theorem and unearth novel insights into their mathematical structure.

Theorem Statement: We present the following theorem, which extends the classical Fermat's Little Theorem to composite numbers possessing two distinct prime factors:

Theorem: For all composite numbers n with exactly two distinct prime factors p and q, the property $((n-1)^2) \bmod n = 1$ holds true.

Proof:

Let $n = p \times q$, where p and q are distinct prime numbers.

We wish to show that $((n-1)^2) \bmod n = 1$.

Expanding $(n-1)^2$, we have:

$(n-1)^2 = (pq-1)^2 = p^2q^2 - 2pq + 1$

Now, applying modular arithmetic, we consider $p^2q^2 - 2pq + 1$ modulo n.

We rewrite $p^2q^2 - 2pq + 1$ as $(pq)^2 - 2(pq) + 1$, factoring out pq.

Since $(pq)^2 - 2(pq) + 1$ is divisible by pq, it's congruent to 0 modulo pq.

Thus, $(pq)^2 - 2(pq) + 1 \equiv 1$.

Therefore, $((n-1)^2) \bmod n = 1$

Hence, the property holds true for all composite numbers n with exactly two distinct prime factors p and q.

Conclusion: In conclusion, our investigation into the modular properties of composite numbers with two prime factors has unveiled a remarkable extension of Fermat's Little Theorem. By demonstrating that these composite numbers exhibit distinctive congruence patterns, we have expanded the theorem's applicability beyond its original scope. This discovery not only enriches our understanding of modular arithmetic but also underscores the inherent complexity and beauty of composite numbers. We anticipate that our findings will inspire further exploration into the modular behavior of composite numbers and stimulate new avenues of research in number theory and cryptography.