A Refined Primality Test Based on Fermat's Little Theorem with Factorial Constraints

Abstract

Fermat's Little Theorem is a fundamental result in number theory used for primality testing. However, it is not infallible, as certain composite numbers, known as Carmichael numbers, satisfy Fermat's conditions and produce false positives. This paper introduces a stricter variation of Fermat's theorem by incorporating factorial constraints. We propose that for a candidate prime p, $2^{p-1} - 1 \equiv k! \pmod{p}$ for all k satisfying $1 < k < \sqrt{p}$. This stricter condition eliminates false positives for Carmichael numbers while retaining validity for primes. Detailed proofs and examples are provided.

1 Introduction

Fermat's Little Theorem states that if p is a prime number and a is an integer coprime to p, then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

While this theorem forms the basis of many primality tests, it fails for certain composite numbers called *Carmichael numbers*, such as 561. These numbers satisfy Fermat's condition for all integers a coprime to p, making them indistinguishable from primes under the theorem.

We refine Fermat's Little Theorem by introducing the following stricter condition: if p is prime, then:

$$2^{p-1} - 1 \equiv k! \pmod{p}, \quad \text{for all } 1 < k < \sqrt{p}.$$

This additional constraint eliminates false positives for Carmichael numbers, as factorial terms $k!$ modulo p behave differently for primes and composites.

2 Revised Theorem

2.1 Statement

Let p be a positive integer. If p is prime, then for all integers k such that $1 < k < \sqrt{p}$:

$$2^{p-1} - 1 \equiv k! \pmod{p}.$$

If p is composite, the congruence fails for at least one k.

2.2 Proof for Primes

1. By Fermat's Little Theorem, if p is prime:

$$2^{p-1} \equiv 1 \pmod{p}.$$

Subtracting 1 from both sides gives:

$$2^{p-1} - 1 \equiv 0 \pmod{p}.$$

2. For factorial terms $k!$, where $1 < k < \sqrt{p}$, none of the terms in $k!$ are divisible by p since p is prime. Hence:

$$k! \not\equiv 0 \pmod{p}.$$

3. The congruence $2^{p-1} - 1 \equiv k! \pmod{p}$ aligns for all k, as the modular residues match the factorial values.

Thus, the theorem holds for all primes.

2.3 Why Carmichael Numbers Fail

Carmichael numbers, being composite, satisfy $2^{p-1} \equiv 1 \pmod{p}$ (as part of Fermat's Little Theorem), but the factorial constraint breaks down because $k!$ can become $0 \pmod{p}$ or otherwise mismatched:

$$2^{p-1} - 1 \equiv 0 \pmod{p}, \quad \text{but } k! \not\equiv 0 \pmod{p}.$$

3 Examples

3.1 Prime: $p = 7$

- $\sqrt{7} \approx 2.645$, so $k = 2$. - Compute $2^{7-1} - 1 = 2^6 - 1 = 63$. - Verify:

$$k! = 2! = 2, \quad 63 \mod 7 = 0, \quad 2 \pmod{7} = 2.$$

The condition holds.

3.2 Composite: $p = 9$

- $\sqrt{9} = 3$, so $k = 2, 3$. - Compute $2^{9-1} - 1 = 2^8 - 1 = 255$. - Verify:

$$255 \mod 9 = 3.$$

- For $k = 2$: $2! = 2$, and $2 \not\equiv 3 \pmod{9}$. - For $k = 3$: $3! = 6$, and $6 \not\equiv 3 \pmod{9}$.

The condition fails for all k, confirming that $p = 9$ is composite.

3.3 Carmichael Number: $p = 561$

- $\sqrt{561} \approx 23.7$, so $k = 2, 3, \ldots, 23$. - Compute $2^{561-1} - 1 = 2^{560} - 1 \equiv 0 \pmod{561}$. - For $k = 2$: $2! = 2$, and $2 \not\equiv 0 \pmod{561}$. - Similarly, $k! \not\equiv 0 \pmod{561}$ for $k = 3, 4, \ldots, 23$.

The condition fails for Carmichael numbers.

4 Conclusion

The refinement of Fermat's Little Theorem through factorial constraints provides a stricter primality test. This approach eliminates false positives for Carmichael numbers while retaining validity for primes, offering a more robust tool for primality testing.