A Deterministic Primality Test: Proof

Joseph M. Shunia

July 28, 2023

Abstract

This paper presents a mathematical proof for a deterministic primality test. The test posits that an integer n satisfying the conditions of the theorem is prime. Using number theory and combinatorics, the proof operates on the basis of certain modular congruences and the Binomial Theorem, particularly exploiting the properties of Fermat's Little Theorem and Korselt's Criterion. While this theorem offers a deterministic primality test that can be implemented using polynomial time algorithms and significantly improves upon previous methods, the details on how to compute the test efficiently are beyond the scope of this proof.

Theorem. *Suppose we let n be an odd integer that satisfies $2^{n-1} \equiv 1 \pmod{n}$. Denote D as the smallest integer strictly greater than 2 which does not divide $n-1$. If it holds that $2^{\lfloor \frac{n-1}{D} \rfloor} + 1 \equiv (2^{\lfloor \frac{n-1}{D} \rfloor} + 1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$, then n is prime.*

Proof. **Step 1: Proof that $2^{\lfloor \frac{n-1}{D} \rfloor} \not\equiv 1 \pmod{n}$:**

Assume there exists a prime p such that $p^{n-1} \equiv 1 \pmod{n}$. Then, according to the properties of the order of an integer modulo n, the smallest k for which $p^k \equiv 1 \pmod{n}$ must be a divisor of $n-1$ or equal to $n-1$.

Given that $\lfloor \frac{n-1}{D} \rfloor$ is strictly smaller than $n-1$ and D doesn't divide $n-1$, it follows that $p^{\lfloor \frac{n-1}{D} \rfloor}$ cannot be equivalent to $1 \pmod{n}$. Since n was selected to satisfy $2^{n-1} \equiv 1 \pmod{n}$ and D was defined as the smallest integer which does not divide $n-1$, it is demonstrated that $2^{\lfloor \frac{n-1}{D} \rfloor} \not\equiv 1 \pmod{n}$.

Step 2: Proof that our test holds when n is prime:

Firstly, we define the function $a(k) = 2^{\lfloor \frac{k-1}{D} \rfloor}$.

Consider the congruence:

$$2^{\lfloor \frac{n-1}{D} \rfloor} + 1 \equiv (2^{\lfloor \frac{n-1}{D} \rfloor} + 1)^n \pmod{n}$$

By substitution, we get:

$$a(n) + 1 \equiv (a(n) + 1)^n \pmod{n}$$

Which is obviously true for a prime n by Fermat's Little Theorem. Additionally, we observe that:

$$a(n) + 1 \equiv (a(n) + 1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} 2^{\left\lfloor \frac{k}{D} \right\rfloor} \pmod{n}$$

Substituting with $a(k)$ yields:

$$a(n) + 1 \equiv (a(n) + 1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} a(k+1) \pmod{n}$$

Utilizing the Binomial Theorem to expand $(a(n) + 1)^n$, we find $(a(n) + 1)^n = \sum_{k=0}^{n} \binom{n}{k} a(n)^k$. Therefore, we have:

$$a(n) + 1 \equiv \sum_{k=0}^{n} \binom{n}{k} a(n)^k \equiv \sum_{k=0}^{n} \binom{n}{k} a(k+1) \pmod{n}$$

Analyzing the congruence:

$$\sum_{k=0}^{n} \binom{n}{k} a(n)^k \equiv \sum_{k=0}^{n} \binom{n}{k} a(k+1) \pmod{n}$$

It is apparent that when n is prime, $\binom{n}{k} \equiv 0 \pmod{n}$ for every $0 < k < n$ by the Binomial Theorem, and so the congruence must be true. Since all conditions of our test are satisfied when n is prime, it is proven that our complete test is valid when n is prime.

Step 3: Proof that our test does not hold when n is composite:

Consider again the following congruence:

$$a(n) + 1 \equiv (a(n) + 1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} a(k+1) \pmod{n}$$

(a) Firstly, examine the left portion of this congruence:

$$a(n) + 1 \equiv (a(n) + 1)^n \pmod{n}$$

In the case where n is composite, the congruence can only hold if n is a Fermat pseudoprime to the base $a(n) + 1$. Such a scenario is not sufficient but necessary for n to be coprime to $a(n) + 1$ and possess a prime factor p that satisfies the condition: $p - 1$ divides $n - 1$. This observation follows a generalization of Korselt's Criterion applicable to Carmichael numbers.

(b) Secondly, consider the right portion of the congruence:

$$\sum_{k=0}^{n} \binom{n}{k} a(n)^k \equiv \sum_{k=0}^{n} \binom{n}{k} a(k+1) \pmod{n}$$

When n is composite, it is plausible that $\binom{n}{k} \not\equiv 0 \pmod{n}$. Consequently, cases should exist where $\binom{n}{k} a(n)^k \not\equiv \binom{n}{k} a(k+1) \pmod{n}$. To justify this, consider the term $a(n)^k = 2^{\left\lfloor \frac{n-1}{D} \right\rfloor k}$. For $0 < k < n$, $a(n)^k$ cycles among the residues of 2 modulo n.

Conversely, for the term $a(k+1) = 2^{\left\lfloor \frac{k}{D} \right\rfloor}$, D is chosen as the least integer that does not divide $n-1$. Given $D > 2$, and D cannot exceed the logarithm of n to the base 2, the exponent $\left\lfloor \frac{k}{D} \right\rfloor$ is restricted to have at most $\left\lfloor \frac{n-1}{D} \right\rfloor < n-1$ distinct values as k ranges from 0 to $n-1$. Additionally, $D > 2$ indicates fewer distinct values for the exponents $\left\lfloor \frac{k}{D} \right\rfloor$ than the exponents of $a(n)^k$ for k in $[0, n-1]$.

Applying the Pigeonhole Principle, at least one k value in $[0, n-1]$ must exist such that $a(n)^k \not\equiv a(k+1)$, leading to the inequality $\binom{n}{k} a(n)^k \not\equiv \binom{n}{k} a(k+1) \pmod{n}$. Thus, it is highly likely for a contradiction in the equivalence of the two sums modulo n. Despite the failure of the individual congruences, the sums can still be congruent modulo n if the k values for which $\binom{n}{k} \not\equiv 0 \pmod{n}$ align with the k values for which $a(n)^k \equiv a(k+1) \pmod{n}$.

Nevertheless, as $a(n) \not\equiv 1 \pmod{n}$ and $a(n) + 1 \equiv (a(n)+1)^n \pmod{n}$, such a scenario is impossible. For the sums to be equivalent, despite their individual terms being different, the sum of all differences must be divisible by n. Yet, $a(n) \not\equiv 1 \pmod{n}$ suggests that the term $\binom{n}{k} a(n)^k - \binom{n}{k} a(k+1)$ cannot be divided by n for some k where $\binom{n}{k} \not\equiv 0 \pmod{n}$. Consequently, the sum of all differences is not divisible by n, causing a contradiction in the equality of the two sums modulo n. This proves that our test does not hold for composite n.

Conclusion:
The test holds if and only if n is prime. Therefore, an odd integer n that satisfies the conditions of the theorem must be prime. □