Primality Test Proof

Joseph M. Shunia

July 5, 2023

Theorem 1. *Let n be an odd integer > 3 such that $2^{n-1} \equiv 1 \pmod{n}$. Let D be the least integer > 2 which does not divide $n-1$. If $2^{\lfloor (n-1)/D \rfloor} + 1 \equiv (2^{\lfloor (n-1)/D \rfloor} + 1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor k/D \rfloor} \pmod{n}$, then n is prime.*

Proof. **Step 1: Proof that $2^{\lfloor \frac{n-1}{D} \rfloor} \not\equiv 1 \pmod{n}$:** Given $2^{n-1} \equiv 1 \pmod{n}$, by the properties of the order of an integer modulo n, the smallest k such that $2^k \equiv 1 \pmod{n}$ must be $k = n-1$ or a divisor of $n-1$. Since $\lfloor \frac{n-1}{D} \rfloor$ is strictly less than $n-1$ and D does not divide $n-1$, it follows that $2^{\lfloor \frac{n-1}{D} \rfloor}$ can't be equivalent to $1 \pmod{n}$.

Step 2: Proof that the congruence holds for n being prime:

Suppose n is prime. The Binomial Theorem gives us

$$(2^{\lfloor \frac{n-1}{D} \rfloor} + 1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor k/D \rfloor}$$

When we consider the terms of this sum modulo n, we can use the fact that for prime p and $1 \le k < p$, $\binom{p}{k} \equiv 0 \pmod{p}$ (from Lucas's Theorem) to conclude that all the terms where $1 \le k < n$ disappear.

We are then left with:

$$(2^{\lfloor \frac{n-1}{D} \rfloor} + 1)^n \equiv \binom{n}{0} + \binom{n}{n} 2^{\lfloor n/D \rfloor} \pmod{n}$$

But we know $\binom{n}{0} = \binom{n}{n} = 1$, which reduces the above congruence to

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

This congruence matches with the condition given in the theorem, thus the condition holds if n is prime.

Step 3: Proof that the congruence does not hold for n being composite:

Suppose n is not prime, and let p be a prime divisor of n.

Let $m = \left\lfloor \frac{n-1}{D} \right\rfloor$. Since n is not a prime, $1 < m < n-1$. From Step 1, we have $2^m \not\equiv 1 \pmod{n}$.

Consider the congruence:

$$\sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor k/D \rfloor} \equiv (2^m + 1)^n \pmod{n}$$

If we examine the terms of the sum for $k = p$, we get $\binom{n}{p} 2^{\lfloor p/D \rfloor}$. Since p is a divisor of n, this term is not equivalent to zero modulo n. Therefore, the sum on the left side of the congruence is not equivalent to $(2^m + 1)^n \pmod{n}$, contradicting the assumption that n satisfies the given congruence condition.

Hence, if n is not prime, it does not satisfy the given congruence. This completes the proof. $\square$