Primality Test Proof

Joseph M. Shunia

July 3, 2023

Proof. We aim to prove that for an odd integer $n > 3$ such that $2^{n-1} \equiv 1 \pmod{n}$, and D being the least integer greater than 1 which does not divide $n-1$, if the congruence $2^{\lfloor \frac{n-1}{D} \rfloor} + 1 = \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$ holds, then n is prime or GCD$(a(n) - 1,\, n)$ is a non-trivial factor of n, where $a(n) = 2^{\lfloor \frac{n-1}{D} \rfloor}$.

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 for GCD statement:

We have the congruence equation $2^{\lfloor \frac{n-1}{D} \rfloor} + 1 = \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$.

The binomial theorem states $(1 + a(n))^n = \sum_{k=0}^{n} \binom{n}{k} a(n)^k$ modulo n.

Comparing this with our original congruence equation, we see they are consistent, and hence, $a(n) + 1 = (1 + a(n))^n$ modulo n holds.

If n is prime, this is a consequence of Fermat's Little Theorem, hence n must be prime.

If n is not prime, then we must have that GCD$(a(n) - 1, n)$ is a nontrivial factor of n. This follows from the property that for any integer a and n, if a and n are not coprime, then $a^k - 1$ shares a nontrivial factor with n for some k. The floor division by D in the definition of $a(n)$ ensures that we consider a smaller exponent than $n-1$, helping us identify nontrivial factors.

Therefore, if the initial congruence holds, n is either prime or GCD$(a(n) - 1,$ $n)$ is a non-trivial factor of n. □