Primality Test Proof

Joseph M. Shunia

July 3, 2023

Theorem Let $n > 3$ be an odd integer such that $2^{n-1} \equiv 1 \pmod{n}$, and let D be 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 $a(n) = 2^{\lfloor \frac{n-1}{D} \rfloor}$.

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 for GCD statement:

By the binomial theorem and substituting with $a(n)$ in:

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

We see that:

$$a(n) + 1 \equiv (1 + a(n))^n \mod n$$

Now, by Fermat's little theorem, we know that if n is prime and $\gcd(a(n), n) = 1$, then $(a(n))^n \equiv a(n) \pmod{n}$.

Therefore, we can rewrite the above congruence as:

$$(a(n))^n + 1 \equiv (a(n))^2 + a(n) + 1 \pmod{n}$$

This implies that $(a(n))^n - (a(n))^2 - a(n)$ is divisible by n.

If we factor this expression, we get:

$$(a(n) - 1)(a(n)^{n-1} + a(n)^{n-2} + ... + a(n) + 1)$$

So, either $(a(n) - 1)$ or $(a(n)^{n-1} + a(n)^{n-2} + ... + a(n) + 1)$ is divisible by n.

If $(a(n) - 1)$ is divisible by n, then $\gcd(a(n) - 1, n)$ is a non-trivial factor of n.

If $(a(n)^{n-1} + a(n)^{n-2} + ... + a(n) + 1)$ is divisible by n, then we can use the fact that $(a(n))^2 + a(n) + 1$ is also divisible by n to show that $\gcd(a(n)^2 - a(n), n)$ is also a non-trivial factor of n.

To see this, note that:

$$(a(n)^{n-3} - a(n))(a(n)^2 + a(n) + 1) = (a(n)^{n-3})(a(n)^2 - a(n)) - (a(n))^3$$

Since both terms on the right-hand side are divisible by n, so is their difference. This means that $(a(n)^{n-3} - a(n))$ is divisible by n.

Repeating this process, we can show that $(a(n)^k - a(k))$ is divisible by n for any positive integer $k < n$. In particular, for $k = 2$, we get that $(a(2) - a(2)) = (a(2))^2 - a(2)$ is divisible by n.

Hence, $\gcd(a(n)^2 - a(n), n)$ is a non-trivial factor of n.

Therefore, in either case, we have shown that if the congruence holds, then n is prime or $\gcd(a(n) - 1, n)$ is a non-trivial factor of n. $\square$