Primality Test Proof

Joseph M. Shunia

July 20, 2023

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

Proof. Define the function $a(k) = 2^{\lfloor (k-1)/D \rfloor}$, then $2^{\lfloor (n-1)/D \rfloor}+1 \equiv (2^{\lfloor (n-1)/D \rfloor}+1)^n \pmod{n}$ can be rewritten as $a(n)+1 \equiv (a(n)+1)^n \pmod{n}$. This means that either n is prime or n is a Fermat psuedoprime to base $a(n)+1$. However, we also have that $(a(n)+1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor k/D \rfloor} \pmod{n}$ which is equivalent to $(a(n)+1)^n \equiv \sum_{k=0}^{n} \binom{n}{k} a(k) \pmod{n}$.

By expanding $(a(n)+1)^n$ using the binomial theorem, we get $\sum_{k=0}^{n} \binom{n}{k} a(n)^k$, and it is easy to see that this is equal to the right hand side $\sum_{k=0}^{n} \binom{n}{k} a(k)$ if and only if $a(n)^k \equiv a(k) \pmod{n}$ for all $0 \leq k \leq n$.

Note that $a(n)^k = 2^{k\left\lfloor \frac{n-1}{D} \right\rfloor}$. On the other hand, $a(k) = 2^{\left\lfloor \frac{k-1}{D} \right\rfloor}$, so $a(n)^k \equiv a(k) \pmod{n}$ if and only if $2^{k\left\lfloor \frac{n-1}{D} \right\rfloor} \equiv 2^{\left\lfloor \frac{k-1}{D} \right\rfloor} \pmod{n}$ for all $0 \leq k \leq n$. This is only possible if D is a divisor of $n-1$ or n is prime. Since we assumed that D does not divide $n-1$, the only possibility is that n is prime. Therefore, the theorem is proved. □