An Efficient Deterministic Primality Test: Proof

Joseph M. Shunia

May 2024

Theorem 1. *Let $n \in \mathbb{Z}^+$ be a Carmichael number. Hence, $n = p_1 p_2 \cdots p_m$ is odd, composite, and squarefree, where the p_i are distinct odd prime factors.*

Let $r \in \mathbb{Z}^+$ be the least odd prime such that $r \nmid n(n-1)$.

Consider the polynomial $f(x) := (x+1)^n - x^n - 1 \in \mathbb{Z}[x]$.

Let $(x^r - 2, n)$ be the ideal generated by $x^r - 2$ and n in the polynomial ring $\mathbb{Z}[x]$.

Suppose $x^n \not\equiv x \pmod{(x^r - 2, n)}$. Then

$$f(x) \not\equiv 0 \pmod{(x^r - 2, n)}.$$

Proof. Assume, for the sake of contradiction, that $f(x) \equiv 0 \pmod{(x^r - 2, n)}$.

Since the congruence holds mod $(x^r - 2, n)$, it must also hold mod $(x^r - 2, p)$ for each prime factor p of n. Thus, for all primes $p \mid n$, we have

$$\begin{aligned}
&f(x) \equiv (x+1)^n - x^n - 1 \equiv (x+1)^p - x^p - 1 \equiv 0 \pmod{(x^r - 2, p)} \\
\iff &(x+1)^n - x^n \equiv (x+1)^p - x^p \equiv 1 \pmod{(x^r - 2, p)}
\end{aligned}$$

From this, we deduce

$$\left((x+1)^{n/p} - x^{n/p}\right)^p \equiv 1 \pmod{(x^r - 2, p)}$$

Leading to

$$\left((x+1)^{n/p} - x^{n/p}\right)^p \equiv (x+1)^n - x^n \equiv (x+1)^p - x^p \equiv 1 \pmod{(x^r - 2, p)}$$

This implies

$$\zeta_p \equiv (x+1)^{n/p} - x^{n/p} \pmod{(x^r - 2, p)},$$

where ζ_p is a pth root of unity.

By the Chinese Remainder Theorem (CRT), since the congruences hold mod $(x^r - 2, p)$ for each prime factor p of n, they also hold mod $(x^r - 2, n)$. Thus, we have

$$\begin{aligned}
\zeta_n &\equiv (x+1)^{n/n} - x^{n/n} \pmod{(x^r - 2, n)} \\
&\equiv (x+1)^1 - x^1 \pmod{(x^r - 2, n)} \\
&\equiv (x+1) - x \pmod{(x^r - 2, n)} \\
&\equiv 1 \pmod{(x^r - 2, n)}.
\end{aligned}$$

This is consistent with the possibility

$$\zeta_p \equiv (x+1)^{n/p} - x^{n/p} \equiv (x+1)^n - x^n \equiv (x+1)^p - x^p \equiv 1 \pmod{(x^r - 2, p)}.$$

Then, for each p, we must consider the following cases:

(i) $x^n \equiv x^{n/p} \pmod{(x^r-2, p)} \iff (x+1)^n \equiv (x+1)^{n/p} \pmod{(x^r-2, p)}$,

(ii) $x^p \equiv x^{n/p} \pmod{(x^r-2, p)} \iff (x+1)^p \equiv (x+1)^{n/p} \pmod{(x^r-2, p)}$,

(iii) $x^n \equiv x^p \pmod{(x^r-2, p)} \iff (x+1)^n \equiv (x+1)^p \pmod{(x^r-2, p)}$.

Each case, taken individually, allows for $f(x) \equiv 0 \pmod{(x^r-2, p)}$. A prime p may satisfy one or all cases, since any two cases being true implies the third.

For n, the three cases (i), (ii), (iii) collapse to a single case, since p is replaced by n in the exponents when lifting via the CRT:

$$x^n \equiv x \pmod{(x^r-2, n)} \iff (x+1)^n \equiv x+1 \pmod{(x^r-2, n)}$$

However, this is a contradiction, since $x^n \not\equiv x \pmod{(x^r-2, n)}$ by assumption in the theorem. Therefore $f(x) \not\equiv 0 \pmod{(x^r-2, n)}$. This completes the proof. $\square$