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. The assumption $r \nmid n(n-1)$ implies that $r \nmid n$ and $r \nmid (n-1)$. First, we will show why this is necessary.

Suppose $r \mid n$, therefore $r = p$ where $p \mid n$. Then

$$x^n \equiv 2 \pmod{(x^r - 2, p)} \implies (x+1)^n \equiv 3 \pmod{(x^r - 2, p)}.$$

Hence, we have trivially

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

Next, suppose $r \mid (n-1)$. Then $r \mid (p-1)$ for some $p \mid n$, and since p is prime, $(p-1) = \phi(p)$. Leading to

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

Again, we have trivially

$$f(x) \equiv (x+1)^n - x^n - 1 \equiv 0 \pmod{(x^r - 2, p)}.$$

We will finish the proof by showing $f(x) \equiv 0 \pmod{(x^r - 2, n)}$ leads to a contradiction under the given conditions.

Assume, for the sake of contradiction, that

$$f(x) \equiv (x+1)^n - x^n - 1 \equiv 0 \pmod{(x^r - 2, n)}.$$

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. Otherwise, n could not divide $f(x)$. 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

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

Leading to

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

This also implies

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

where ζ_p is a p-th root of unity modulo $(x^r - 2, p)$.

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 that ζ_p is a trivial p-th root of unity modulo $(x^r - 2, n)$. That is

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

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

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

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

Each case, taken individually, allows for $f(x) \equiv 0 \pmod{(x^r-2, p)}$. These cases are mutually exclusive, since satisfying both (i) and (ii) leads to

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

implying that $p = r$ and $r \mid n$, contradicting the theorem.

Now, suppose cases (i), (ii) are both false. If $x^n \equiv \zeta_p x \pmod{(x^r-2, p)}$, where ζ_p is a non-trivial p-th root of unity modulo (x^r-2, p), then $(x+1)^n \equiv \zeta_p(x+1) \pmod{(x^r-2, p)}$. This is possible because the polynomial ring $\mathbb{Z}[x]/(x^r-2, p)$ is isomorphic to the direct product of fields $\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_r)$, where the α_i are the roots of $x^r - 2$ in an algebraic closure of $\mathbb{F}_p$. In some of these fields, there may exist non-trivial p-th roots of unity, allowing for this. However, we showed above that $\zeta_n \equiv 1 \pmod{(x^r-2, n)}$, so this would imply $x^n \equiv \zeta_n x \equiv x \pmod{(x^r-2, n)}$, contradicting the assumption in the theorem that $x^n \not\equiv x \pmod{(x^r-2, n)}$.

Finally, suppose either case is true for all primes $p \mid n$. For n, the two cases (i) and (ii) 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 again, $x^n \not\equiv x \pmod{(x^r-2, n)}$ by assumption in the theorem. Therefore $f(x) \not\equiv 0 \pmod{(x^r-2, n)}$. This completes the proof. $\square$