An Efficient Deterministic Primality Test: Proof

Joseph M. Shunia

May 2024

1 Supporting Lemmas

We begin by presenting the supporting lemmas for our main theorem (§ 2).

Lemma 1. *Let $n \in \mathbb{Z}_{>1}$ 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. Furthermore, $(p_i - 1) \mid (n-1)$ for all $p_i \mid n$. Let $r \in \mathbb{P}_{\geq 3}$ be the least odd prime such that $r \nmid n(n-1)$. Let $(x^r - 2, n)$ be the ideal generated by $x^r - 2$ and n in the polynomial ring $\mathbb{Z}[x]$. Consider the polynomial $f(x) := (x+1)^n - x^n - 1 \in \mathbb{Z}[x]$.*

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 $r \nmid (n-1)$. We will begin by briefly 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 $p \mid n$. 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, it is easy to see that $f(x) \equiv 0 \pmod{(x^r - 2, p)}$ in such case.

We will now show that $f(x) \equiv 0 \pmod{(x^r - 2, n)}$ 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

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

Leading to

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

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

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

Hence, we have

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

Then, for each p, we must consider the following 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) and (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 (i) or (ii) 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. □

Lemma 2. *Let $n, r \in \mathbb{Z}_{>1}$ such that n is odd, $r \geq 3$, and $r \nmid n$. 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

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

Then it is necessary, but not sufficient, that n is a Carmichael number.

Proof. Let $p \mid n$ be prime. Consider

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

Expanding the term $(x+1)^n$ via the Binomial Theorem and simplifying, we see

$$f(x) = \sum_{k=1}^{n-1} \binom{n}{k} x^k.$$

From Lucas Theorem, since $p \neq n$, we know that p cannot divide all $\binom{n}{k}$. Furthermore, since $r \geq 3$, the reduction of $f(x)$ mod $(x^r - 2)$ will leave a polynomial remainder of degree $d \geq 1$. In other words, $f(x)$ is not a constant modulo $(x^r - 2)$. Then, for $f(x)$ to be zero, it must vanish for all $a \in \mathbb{Z}$ when evaluated modulo p. That is,

$$\forall a \in \mathbb{Z}, \quad f(a) \equiv (a+1)^n - a^n - 1 \equiv 0 \pmod{p}.$$

Re-arranging this, we have

$$\forall a \in \mathbb{Z}, \quad f(a) \equiv (a+1)^n \equiv a^n + 1 \pmod{p}.$$

Thus,

$$\forall a \in \mathbb{Z}, \quad a^n \equiv a \pmod{p}.$$

By Fermat's Little Theorem (FLT), this implies $(p-1) \mid (n-1)$. Since this must be true for all primes $p \mid n$, we conclude that n must be a Carmichael number. However, this condition is not sufficient, as we did not prove the conditions under which $f(x) \equiv 0 \pmod{(x^r - 2, n)}$ holds for Carmichael numbers. □

Lemma 3. *Let $n \in \mathbb{Z}_{>1}$ be a Carmichael number. Hence, n is odd, composite, and squarefree. Let $r \in \mathbb{P}_{\geq 3}$ be the least odd prime such that $r \nmid n(n-1)$. Let $(x^r - 2, n)$ be the ideal generated by $x^r - 2$ and n in the polynomial ring $\mathbb{Z}[x]$. Then, $x^n \not\equiv x \pmod{(x^r - 2, n)}$.*

Proof. The reduction of $x^n \pmod{(x^r - 2)}$ leaves a polynomial remainder of degree $d = (n \bmod r)$. Formally, we have

$$x^n \equiv 2^{\lfloor n/r \rfloor} x^d \equiv 2^{\lfloor n/r \rfloor} x^{n \bmod r} \pmod{(x^r - 2)}$$

Since $n = p_1 p_2 \cdots p_m$ is a Carmichael number, we know that $(p_i - 1) \mid (n-1)$ for all prime factors $p_i \mid n$. In such case

$$r \nmid (n-1) \implies n \not\equiv 1 \pmod{r}.$$

Thus, $d \neq 1$. Leading to

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

□

2 Main Theorem

Theorem 4. *Let $n \in \mathbb{Z}_{>1}$ such that n is odd. Let $r \in \mathbb{P}_{\geq 3}$ be the least odd prime such that $r \nmid n(n-1)$. Let $(x^r - 2, n)$ be the ideal generated by $x^r - 2$ and n in the polynomial ring $\mathbb{Z}[x]$. Consider the polynomial $f(x) := (x+1)^n - x^n - 1 \in \mathbb{Z}[x]$. Suppose $f(x) \equiv 0 \pmod{(x^r - 2, n)}$. Then, n is prime.*

Proof. Expanding $f(x)$ by the Binomial Theorem and simplifying, we see

$$f(x) = (x+1)^n - x^n - 1 = \sum_{k=1}^{n-1} \binom{n}{k} x^k.$$

If n is prime, then $\binom{n}{k} \equiv 0 \pmod{n}$ for all k in the sum. Clearly then, $f(x) \equiv 0 \pmod{n}$ when n is prime.

On the other hand, suppose n is composite. In this case, Lucas Theorem tells us that n cannot possibly divide all $\binom{n}{k}$ in the sum. Applying Lemma 2, we see that n must be a Carmichael number for $f(x)$ to be zero. Furthermore, by Lemma 3, since $r \geq 3$ and $r \nmid (n-1)$, we have $x^n \not\equiv x \pmod{(x^r - 2, n)}$. Under these constraints, we have

$$f(x) \equiv (x+1)^n - x^n - 1 \not\equiv 0 \pmod{(x^r - 2, n)} \quad \text{(By Lemma 1)}.$$

Therefore, under the given conditions, if $f(x) \equiv 0 \pmod{(x^r - 2, n)}$, then n is prime. $\square$