An Efficient Deterministic Primality Test

Joseph M. Shunia

December 2023
Revised: January 2024

Abstract

A deterministic primality test with a polynomial time complexity of $\tilde{O}(\log^3(n))$ is presented. The test posits that an integer n satisfying the conditions of the main theorem is prime. Combining elements of number theory and combinatorics, the proof operates on the basis of simultaneous modular congruences relating to binomial transforms of powers of two.

1 Introduction

Primality testing has seen remarkable advancements over the past few decades. A significant breakthrough in this field was the AKS primality test, introduced by Agrawal, Kayal, and Saxena (2002) [1]. The AKS test was the first to offer determinism and polynomial-time complexity, a monumental achievement that resolved a longstanding open question in computational number theory [2]. However, despite its theoretical importance, the AKS test has practical limitations due to its relatively high polynomial time complexity, rendering it inefficient for most applications. Agrawal, Kayal, and Saxena gave a time complexity of $\tilde{O}(\log^{12}(n))$ for the AKS test [1]. This bound was lowered significantly by Lenstra and Pomerance (2011) to $\tilde{O}(\log^6(n))$ [3]. Despite this reduction, AKS remains impractical and is mostly unused.

In the field of cryptography, the unique properties of prime numbers are widely exploited to create cryptographic primitives. It is often the case that many large primes must be generated in rapid succession [4]. To make these cryptographic operations practical, fast probabilistic primality tests such as the Baille-PSW primality test (BPSW) [5] or Miller-Rabin (MR) [6] [7] are used instead of AKS when searching for large primes. Probabilistic primality tests are by definition non-deterministic and may erroneously report a composite integer as being prime. Composite integers which pass a probabilistic primality test are relatively rare and are known as pseudoprimes (PSPs) for the respective test [8]. When generating primes for cryptographic purposes, probabilistic primality tests are often combined or repeated with different parameters in order to achieve an acceptable error-bound that makes it almost certain that no composite integer will pass. However, reducing the error-bound requires additional compute and increases running-time, creating a trade-off.

We present a new deterministic primality test that operates in polynomial time with a time complexity of $\tilde{O}(\log^3(n))$. This efficiency gain opens new avenues for practical applications, particularly in cryptography, where fast and reliable primality testing is desirable [9].

Our test is based on a famous conjecture issued by Manindra Argawal while he was an undergraduate student [1]. Let n and r be two coprime positive integers. If the following polynomial congruence holds, then n is prime or $n^2 = 1 \pmod{r}$:

$$(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1} \tag{1}$$

We alter the conditions slightly to use roots of 2 instead of roots of unity. Through the proof of our

main theorem, we demonstrate that our modified test is equivalent to checking the polynomial congruence $(1+x)^n \equiv 1 + x^n \pmod{n} \in \mathbb{Z}[x]$, which is known to hold for only prime integers n [10].

1.1 Structure of the Paper

This paper is structured as follows: We begin by presenting the main theorem which defines our primality test. We follow up with supporting lemmas and theorems. Then, we present the proof of our main theorem, which demonstrates the test's validity for odd prime numbers and its failure for odd composite numbers. Through this, we establish the deterministic nature of our test. We then describe the algorithm used to compute our test and analyze its computational complexity. We conclude with a link to an open source implementation of our test.

2 Statement of Main Theorem

Theorem 1 (Main theorem)**.** Let $n > 3$ be an odd integer such that $2^{n-1} \equiv 1 \pmod{n}$. Let $d > 2$ be the least prime integer such that $n \not\equiv 1 \pmod{d}$. If the following polynomial congruence holds, then either n is prime or n has a prime divisor $p \leq d$:

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

3 Supporting Lemmas and Theorems

3.1 Supporting Lemmas

Lemma 1. Given $a, b \in \mathbb{Z}^+$ with $b \nmid a$ and $1 < b < \left\lfloor \frac{a}{b} \right\rfloor$, then $\left\lfloor \frac{a}{b} \right\rfloor$ cannot divide a.

Proof. Let $q = \left\lfloor \frac{a}{b} \right\rfloor$. By definition, q is the greatest integer that is less than $\frac{a}{b}$. Thus, $q \cdot b < a < b \cdot (q+1)$.

Suppose, for contradiction, that q divides a. Then there exists an integer k such that $a = k \cdot q$. Substituting $a = k \cdot q$ into the inequality $q \cdot b < a < b \cdot (q+1)$, we get $q \cdot b < k \cdot q < b \cdot (q+1)$. Dividing this inequality by q, we obtain $b < k < b + \frac{b}{q}$.

Since k is an integer, and $b \nmid a$ implies $k \neq b$, the next possible integer value for k is $b+1$. Therefore, $k = b+1$, which gives $a = k \cdot q = q \cdot (b+1)$. However, this leads to a contradiction: $a = q \cdot (b+1)$ implies $a \geq b \cdot (q+1)$, contradicting the established fact that $a < b \cdot (q+1)$. Hence, our assumption that q divides a is false. Therefore, $\left\lfloor \frac{a}{b} \right\rfloor \nmid a$. □

Lemma 2 (Upper bound on floor function and indivisibility)**.** Given $a, b \in \mathbb{Z}^+$ with $1 < b < \left\lfloor \frac{a}{b} \right\rfloor$, then $b \leq \lfloor \sqrt{a} \rfloor$.

Proof. Assume $a, b \in \mathbb{Z}^+$ and $1 < b < \left\lfloor \frac{a}{b} \right\rfloor$. By definition, $\left\lfloor \frac{a}{b} \right\rfloor$ is the greatest integer less than or equal to $\frac{a}{b}$. Hence, $\left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$. Since $b < \left\lfloor \frac{a}{b} \right\rfloor$, we have $b^2 < b \cdot \left\lfloor \frac{a}{b} \right\rfloor \leq a$. Taking square roots on both sides of the inequality $b^2 < a$ and considering that b and $\sqrt{a}$ are both positive, we get $b < \sqrt{a}$. Since b and $\sqrt{a}$ are positive integers, and $b < \sqrt{a}$, it follows that $b \leq \lfloor \sqrt{a} \rfloor$. □

Lemma 3 (Multiplicative order inequality)**.** Let n be an odd composite integer greater than 3 such that $2^{n-1} \equiv 1 \pmod{n}$. Denote by d the least prime integer > 2 which does not divide $n-1$. Then, $\left\lfloor \frac{n-1}{d} \right\rfloor \neq \operatorname{ord}_n(2)$.

Proof. Consider an odd composite integer $n > 3$ for which $2^{n-1} \equiv 1 \pmod{n}$. According to the properties of the multiplicative order modulo n, the smallest positive integer k such that $2^k \equiv 1 \pmod{n}$ defines $\mathrm{ord}_n(2)$, that is, $k = \mathrm{ord}_n(2)$. Since n is composite and $2^{n-1} \equiv 1 \pmod{n}$, this order, $\mathrm{ord}_n(2)$, must divide $n-1$.

Given d is the least integer greater than 2 and less than n that does not divide $n-1$, and $\mathrm{ord}_n(2)$ divides $n-1$, it follows that d cannot equal $\mathrm{ord}_n(2)$. Furthermore, by Lemma 1, we know that if an integer b does not divide an integer a, and $1 < b < \left\lfloor \frac{a}{b} \right\rfloor$, then $\left\lfloor \frac{a}{b} \right\rfloor$ does not divide a. Applying this to our current context with $a = n-1$ and $b = d$: The least odd composite integer such that $2^{n-1} \equiv 1 \pmod{n}$ is 341 [11]. It follows from Lemma 4 that d must be less than or equal to $\lfloor \log_2(n-1) \rfloor + 2$. For $n \geq 341$, clearly $d < \lfloor \sqrt{n} \rfloor$ which satisfies Lemma 2. Thus we have $1 < d < \left\lfloor \frac{n-1}{d} \right\rfloor$ and hence, $\left\lfloor \frac{n-1}{d} \right\rfloor$ cannot divide $n-1$.

Since $\mathrm{ord}_n(2)$ is a divisor of $n-1$ and $\left\lfloor \frac{n-1}{d} \right\rfloor$ is not, it must be that $\left\lfloor \frac{n-1}{d} \right\rfloor$ is not equal to $\mathrm{ord}_n(2)$, as this would imply a contradiction with the nature of $\mathrm{ord}_n(2)$ as a divisor of $n-1$. Therefore, $\left\lfloor \frac{n-1}{d} \right\rfloor \neq \mathrm{ord}_n(2)$. □

Lemma 4 (Upper bound on d)**.** Let n be an odd composite integer > 3. Then there exists an odd prime integer $d \leq (1 + o(1)) \log(n)$ such that $n \not\equiv 0 \pmod{d}$.

Proof. Define $f(n)$ as the least odd prime not dividing n. For primorials $q_m = \prod_{k=1}^{m} p_k$, with $m \geq 2$, $f(q_m)$ is the $(m+1)$-th prime, as q_m is divisible by the first m primes (including 2).

By the Prime Number Theorem, $p_m \approx m \log m$, so for a primorial q_m, $f(q_m) = p_{m+1} \approx (m+1)\log(m+1)$.

Since the function f is maximized at primorials, for a general n, especially when n is large and not necessarily a primorial, we can estimate that $f(n) \leq (1 + o(1)) \log n$. This upper bound is asymptotic and becomes more accurate for larger n.

Therefore, for any odd composite integer n, the least odd prime non-divisor of n is bounded above by $(1 + o(1)) \log n$. □

Remark. The proof for Lemma 4 was adapted from a proof given by a MathOverflow user [12].

Lemma 5 (Incongruence modulo n)**.** Let $n > 3$ be an odd composite integer such that $2^{n-1} \equiv 1 \pmod{n}$. Denote by d the least prime integer > 2 which does not divide $n-1$. Then, $2^{\left\lfloor \frac{n-1}{d} \right\rfloor} \not\equiv 1 \pmod{n}$.

Proof. Consider an odd composite integer $n > 3$ for which $2^{n-1} \equiv 1 \pmod{n}$. According to the properties of the multiplicative order modulo n, the smallest positive integer k such that $2^k \equiv 1 \pmod{n}$ defines $\mathrm{ord}_n(2)$, that is, $k = \mathrm{ord}_n(2)$. Since n is composite and $2^{n-1} \equiv 1 \pmod{n}$, this order, $\mathrm{ord}_n(2)$, must divide $n-1$.

Given d is the least prime integer greater than 2 and less than n that does not divide $n-1$, and $\mathrm{ord}_n(2)$ divides $n-1$, it follows that d cannot equal $\mathrm{ord}_n(2)$. Furthermore, by Lemma 1, we know that if an integer b does not divide an integer a, and $1 < b < \left\lfloor \frac{a}{b} \right\rfloor$, then $\left\lfloor \frac{a}{b} \right\rfloor$ does not divide a.

Applying this to our current context with $a = n-1$ and $b = d$: The least odd composite integer such that $2^{n-1} \equiv 1 \pmod{n}$ is 341 [11]. By Lemma 4, we have $d \leq (1 + o(1)) \log(n)$, which is significantly less than $\lfloor \sqrt{n} \rfloor$ as n grows large. For $n \geq 341$, clearly $d < \lfloor \sqrt{n} \rfloor$ which satisfies Lemma 2. Thus we have $1 < d < \left\lfloor \frac{n-1}{d} \right\rfloor$ and hence, $\left\lfloor \frac{n-1}{d} \right\rfloor$ cannot divide $n-1$.

By the properties of the order of an integer modulo composite n, the smallest $k \in \mathbb{Z}$ such that $2^k \equiv 1 \pmod{n}$, that is $k = \mathrm{ord}_n(2)$, must be a divisor of $n-1$. Hence, $\mathrm{ord}_n(2) \mid n-1$. Since $\left\lfloor \frac{n-1}{d} \right\rfloor$ is strictly less than $n-1$ and d does not divide $n-1$, it follows that $2^{\left\lfloor \frac{n-1}{D} \right\rfloor} \not\equiv 1 \pmod{n}$. □

Lemma 6. Let $n > 3$ be an odd composite integer such that $2^{n-1} \equiv 1 \pmod{n}$. Let $d > 2$ be the least prime integer such that $n \not\equiv 1 \pmod{d}$. If $2^{\left\lfloor \frac{n-1}{d} \right\rfloor} \not\equiv 1 \pmod{n}$, then n has at least one prime divisor p such that 2 is not a dth power residue modulo p. That is, there are no solutions $b \in \mathbb{Z}_{\text{ı}}$ such that $b^d \equiv 2 \pmod{p}$.

Proof. Let $p \in \mathbb{Z}$ be prime and $\beta = \gcd(p-1, d)$. Euler's criterion [13] states that $a \not\equiv 0 \pmod{p}$ is a dth power residue modulo p if and only if:

$$a^{\frac{p-1}{\beta}} \equiv 1 \pmod{p} \tag{3}$$

Applying to Euler's criterion to our situation, since p and d are both odd primes and $p \neq d$, we have that $a = 2$ is a dth power residue modulo p if and only if $d \mid p-1$ and $2^{\frac{p-1}{d}} \equiv 1 \pmod{p}$.

For the sake of contradiction, let's assume that for all prime divisors p_j of n, $d \mid p_j - 1$ and $2^{\frac{p_j-1}{d}} \equiv 1 \pmod{p}_j$. Then by the Chinese Remainder Theorem (CRT) [14], we must have $d \mid n-1$. However, this is a contradiction, as we have defined d such that $n \not\equiv 1 \pmod{d}$.

Furthermore, by the properties of the multiplicative order modulo composite n, we must also have $2^{\frac{n-1}{d}} \equiv 1 \pmod{p}$. However, this also conflicts with of n which requires $2^{\frac{n-1}{d}} \not\equiv 1 \pmod{p}$.

Therefore, we deduce that there must exist at least one prime divisor p of n such that $2^{\lfloor \frac{p-1}{d} \rfloor} \not\equiv 1 \pmod{p}$. For this p, Euler's criterion fails to hold, and thus it follows that 2 is not a dth power residue modulo p. □

3.2 Supporting Theorems

3.3 Primes Case

Theorem 2 (Primes pass)**.** Let n be an odd prime integer such that $n > 3$. Denote d as the least integer greater than 2 such that $n \not\equiv 1 \pmod{d}$. Then $(1+x)^n \equiv 1 + x^n \pmod{n, x^d - 2}$.

Proof. We aim to show that the following polynomial congruence holds for all odd prime integers $n > 3$:

$$(1+x)^n \equiv 1 + x^n \pmod{n, x^d - 2}, \tag{4}$$

where d is the least integer greater than 2 such that $n \not\equiv 1 \pmod{d}$.

We begin by taking the binomial expansion of the left-hand side:

$$\sum_{k=0}^{n} \binom{n}{k} x^k \equiv 1 + x^n \pmod{n, x^d - 2} \tag{5}$$

When n is prime, $\binom{n}{k} \equiv 0 \pmod{n}$ for all integers k in the range $1 \leq k \leq n-1$. Thus, we have $\sum_{k=1}^{n-1} \binom{n}{k} x^k \equiv 0 \pmod{n, x^d - 2}$. With this in mind, we isolate the inner terms in our original congruence and simplify:

$$\binom{n}{0} x^0 + \binom{n}{n} x^n + \sum_{k=1}^{n-1} \binom{n}{k} x^k \equiv 1 + x^n \pmod{n, x^d - 2} \tag{6}$$

$$\binom{n}{0} x^0 + \binom{n}{n} x^n \equiv 1 + x^n \pmod{n, x^d - 2} \tag{7}$$

By the binomial theorem, we have $\binom{n}{0} = \binom{n}{n} = 1$ for all $n \in \mathbb{Z}$. Substituting values and simplifying further reveals:

$$1 \cdot x^0 + 1 \cdot x^n \equiv 1 + x^n \pmod{n, x^d - 2} \tag{8}$$

$$1 + x^n \equiv 1 + x^n \pmod{n, x^d - 2} \tag{9}$$

Hence, we have shown that the left-hand side of the congruence is equal to the right-hand side when n is prime. Therefore, we conclude that the polynomial congruence holds under the given conditions. □

3.4 Composites Case

A fundamental theorem in polynomial ring theory states that an integer n is prime if and only if $(1+x)^n \equiv 1 + x^n \pmod{n} \in \mathbb{Z}[x]$ [10]. This congruence was used as the basis for the AKS test [1]. A short proof of the theorem, given by Granville (2004) [10], is that since $(x+1)^n - (x^n+1) = \sum_{k=1}^{n-1} \binom{n}{k} x^k$, we may have $(1+x)^n \equiv 1 + x^n \pmod{n}$ if and only if n divides $\binom{n}{k}$ for all k in the range $1 \leq k \leq n-1$. It is important to note that for the polynomial congruence to be valid, x^n and $(1+x)^n$ must be irreducible in $\mathbb{Z}_n[x]$.

Kopparty and Wang (2014) [15] proved several interesting theorems related to limits on the counts of consecutive zero coefficients in polynomials over finite fields. We take significant inspiration from their approach to show that composite integers will always fail our test.

Theorem 3 (Composites case)**.** Let $n = pq$ be an odd composite integer greater than 3 such that $2^{n-1} \equiv 1 \pmod{n}$, with p a prime divisor. Let $d > 2$ be the least prime integer such that $n \not\equiv 1 \pmod{d}$. Suppose n does not have a prime divisor $\leq d-1$ and $x^n \not\equiv 1 \pmod{n, x^d - 2}$. Then $(1+x)^n \not\equiv 1 + x^n \pmod{n, x^d - 2}$.

Proof. First, consider the polynomial $f(x) = (1+x)^n - (1+x^n) \in \mathbb{Z}_n[x]$. Notice that taking $f(x)$ modulo $x^d - 2$ and asserting that the result is nonzero is equivalent to showing $(1+x)^n \not\equiv 1 + x^n \pmod{n, x^d - 2}$.

We are given composite n with $x^n \not\equiv 1 \pmod{n, x^d - 2}$. In the quotient ring $\mathbb{Z}_n[x]/(x^d - 2)$, we have $x^d = 2$ and thus:

$$\left(x^n = (x^{\frac{1}{d}})^n = (2^{\frac{1}{d}})^n = 2^{\lfloor \frac{n}{d} \rfloor}\right) \not\equiv 1 \pmod{n, x^d - 2} \tag{10}$$

Since n is odd and $d > 2$, by the properties of the floor function, $\lfloor \frac{n}{d} \rfloor = \lfloor \frac{n-1}{d} \rfloor$. It follows that:

$$\left(2^{\lfloor \frac{n}{d} \rfloor} = 2^{\lfloor \frac{n-1}{d} \rfloor}\right) \not\equiv 1 \pmod{n, x^d - 2} \tag{11}$$

If $f(x) \pmod{x^d - 2}$ is to be zero in $\mathbb{Z}[x]_n$, it is necessary that $f(x)$ be zero modulo all of the individual prime factors of n up to at least the power that appears in the prime factorization of n. This is because if any of the polynomial's coefficients are indivisible by some prime power p^k dividing n (and therefore all $\{p^j \text{ — } 1 < j \leq k\}$), then they cannot be divisible by n (since n is the unique product of its prime factorization).

Hence, to prove the theorem, it suffices to show that under the given conditions, there must exist a prime divisor p of n such that $f(x) = (1+x)^n - (1+x^n) \in \mathbb{Z}_p[x]$ is nonzero when reduced modulo $x^d - 2$. Or equivalently, that $(1+x)^n \not\equiv 1 + x^n \pmod{p, x^d - 2}$.

Under the given conditions, by Lemma 6, there must exist at least one prime divisor p of n such that 2 is not a dth power residue modulo p.

Now, consider the polynomial ring $\mathbb{Z}_p[x]$. We examine the reduction of $f(x) \pmod{x^d - 2} \in \mathbb{Z}[x]_p$, which is the same as $f(x) \in \mathbb{Z}_p[x]/(x^d - 2)$. After reduction modulo $x^d - 2$, the polynomial $f(x)$ has $\deg(f(x)) = d-1$, and can be written as $f(x) = \sum_{i=0}^{d-1} c_i x^i$.

Assume for contradiction that $f(x)$ is the zero polynomial in $\mathbb{Z}_p[x]/(x^d - 2)$. This would imply that all coefficients c_i are zero.

Since p is prime, $\mathbb{Z}_p$ is a finite field and $\mathbb{Z}_p[x]$ is a polynomial ring over this field. We aim to establish that $\mathbb{Z}_p[x]/(x^d - 2)$ forms a field. To do so, we must show that $x^d - 2$ is irreducible over $\mathbb{Z}_p[x]$.

We recall a classical theorem from field theory (Irreducibility Theorem) [16]:

Suppose $c \in F$ where F is a field, and $0 < d \in \mathbb{Z}$. The polynomial $x^k - c$ is irreducible over F if and only if c is not a qth power in F for any prime q dividing k, and c is not in $-4F^4$ when 4 divides k.

In our case, $F = \mathbb{Z}_p$, $c = 2$, and $k = d$, where d is prime.

Regarding the first criterion, given d is prime, d does not have any divisors q, and hence it suffices to check only d itself. We have chosen p such that 2 is not a dth power residue modulo p, which informs that there is no element $b \in \mathbb{Z}_p$ such that $b^d \equiv 2 \pmod{p}$. The first criterion is satisfied. Since d is prime, it is not divisible by 4, and thus second criterion is also satisfied.

By the Irreducibility Theorem, $x^d - 2$ is irreducible over $\mathbb{Z}_p[x]$ and hence, the quotient ring $\mathbb{Z}_p[x]/(x^d - 2)$ forms a finite field.

In a finite field, a polynomial of degree r can have at most r roots [17]. This is because a polynomial of degree r in a finite field can be factored into at most r linear factors (each corresponding to a root), within an algebraic closure of that field. However, within the field itself, the number of roots can be fewer than r, but never more.

In our case, if $\mathbb{Z}_p[x]/(x^d - 2)$ is a finite field and $\deg(f(x)) = d - 1$, then $f(x)$ can have at most $d - 1$ roots in this field. The assumption that $f(x)$ is the zero polynomial is a direct contradiction unless $p \leq d - 1$, as it would necessarily imply that $f(x)$ has infinitely many roots (or more precisely, that every element of $\mathbb{Z}_p$ is a root) [15]. However, this is clearly not the case, as we are given n which does not have a prime divisor $\leq d$.

Therefore, we conclude that under the given conditions, $f(x)$ must be nonzero in $\mathbb{Z}_p[x]/(x^d - 2)$ for at least one prime p which divides n and therefore, $(1 + x)^n \not\equiv 1 + x^n \pmod{n, x^d - 2}$. This completes the proof. □

4 Proof of the Main Theorem

Proof of Theorem 1. Let n be an odd integer > 3 such that $2^{n-1} \equiv 1 \pmod{n}$. Let $d > 2 \in \mathbb{Z}$ be the least prime such that $n \not\equiv 1 \pmod{d}$. Suppose n does not have a prime divisor $\leq d - 1$.

Case 1: n is prime

If n is prime, then by *Theorem* 2, the polynomial congruence holds and n passes the test as expected.

Case 2: n is composite If n composite and is divisible by d, then clearly n fails the test as expected.

If n not divisible by d, then by Lemma 5 we infer $2^{\lfloor n-1 \rfloor d} \not\equiv 1 \pmod{n}$. By Lemma 6, it follows that n must have a prime divisor p such that 2 is not a dth power residue modulo p. Therefore, all the necessary preconditions for Theorem 3 are satisfied and it applies. by Theorem 3, the polynomial congruence cannot hold, and thus, n fails the test as expected.

Conclusion:

Under the given conditions, when n is prime, the polynomial congruence holds and n passes the test as expected. When n is composite, the polynomial congruence does not hold and n fails the test as expected. The theorem is proven. □

5 Algorithm

INPUT: An integer $n > 1$.

1. If $n \equiv 0 \mod 2$:
   (a) If n equals 2, output PRIME.
   (b) Otherwise, output COMPOSITE.
2. If n equals 3, output PRIME.
3. If $2^{n-1} \bmod n$ does not equal 1, output COMPOSITE.

4. Find the least prime integer d that is greater than 2 such that $n \not\equiv 1 \pmod{d}$.
5. If n has a prime divisor less than d, output COMPOSITE.
6. Compute the polynomial expansion of $x^n \bmod n$ in the ring $\mathbb{Z}_n[x]/(x^d - 2)$ with degree d, and store the result.
7. Compute the polynomial expansion of $(1 + x)^n \bmod n$ in the ring $\mathbb{Z}_n[x]/(x^d - 2)$ with degree d, and store the result.
8. If $(1 + x)^n \neq 1 + x^n$, output COMPOSITE.
9. Output PRIME;

5.1 Time Complexity Analysis

The given algorithm is a primality test that involves several computational steps, including modular arithmetic and polynomial exponentiation in the ring $\mathbb{Z}_n[x]/(x^d - 2)$. In this subsection, we use $M(n)$ to denote the worst-case time complexity of integer multiplication in terms of n.

5.1.1 Analysis of Individual Operations

1. **Check for Even** n:

   This step involves calculating $n \bmod 2$ and has a time complexity of $T_1(n) = O(1)$.

2. **Finding** d:

   Finding the least prime integer $d > 2$ such that $n \not\equiv 1 \pmod{d}$ takes at most $O((1 + o(1)) \log(n))$ steps (See Lemma 4), with each step requiring $O(1)$ time for the mod operation. Hence, the overall complexity is $T_2(n) = O((1 + o(1)) \log(n))$.

3. **Computing** $x^n \bmod n, x^d - 2$:

   Computing the polynomial expansion of $x^n \pmod{n}$ in the ring $\mathbb{Z}_n[x]/(x^d - 2)$ with degree d is equivalent to calculating $2^{\lfloor \frac{n}{d} \rfloor} \pmod{n}$. This step requires modular exponentiation with a $\log(n)$-digit base and a $\log(n)$-digit exponent. The time complexity of modular exponentiation is $T_3(n) = O(\log(n)M(n))$.

4. **Computing** $(1 + x)^n \bmod n, x^d - 2$:

   Computing the polynomial expansion of $(1 + x)^n \pmod{n}$ in the ring $\mathbb{Z}_n[x]/(x^d - 2)$ with degree d involves exponentiating a polynomial in $\mathbb{Z}_n[x]/(x^d - 2)$ with $D = O((1 + o(1)) \log(n))$ terms. Exponentiation using repeated squaring takes $O(\log(n))$ steps, and each step requires $O((1 + o(1)) \log(n)M(n))$ time due to the multiplication of polynomials of size $O((1 + o(1)) \log(n))$. Therefore, the overall complexity of this step is $T_4(n) = O((1 + o(1)) \log^2(n)M(n))$.

5. **Checking the equality** $(1+x)^n = 1+x^n \pmod{n} \in \mathbb{Z}_n[x]/(x^d-2)$: The final steps involve comparing the equality of coefficients in the polynomials $(1+x)^n$ and $1+x^n$. This requires $O(\log(n))$ comparisons, which are themselves $O(1)$ operations. The overall time complexity of this step is $T_5(n) = O(\log(n))$.

5.1.2 Overall Time Complexity

The dominant time complexity in the algorithm comes from computing $(1+x)^n \pmod{n} \in \mathbb{Z}_n[x]/(x^d-2)$. Therefore, the overall time complexity of the algorithm is $T(n) = O((1+o(1))\log^2(n)M(n))$.

Harvey and van Der Heoven (2021) [18] have given an algorithm for integer multiplication which has a time complexity $M(n) = O(\log(n)\log\log(n))$. This would give our algorithm an overall time complexity of:

$$T(n) = O((1+o(1))\log^2(n)M(n)) \tag{12}$$

$$= O((1+o(1))\log^2(n)\log(n)\log\log(n)) \tag{13}$$

$$= O((1+o(1))\log^3(n)\log\log(n)) \tag{14}$$

In soft-O notation [19], typically denoted as $\tilde{O}$, simplicity is achieved by omitting slower-growing logarithmic and lower-order factors that do not significantly contribute to the overall growth rate of the function.

In the context of our time complexity $T(n) = O((1+o(1))\log^3(n)\log\log(n))$, where the dominant term is $O(\log^3(n))$, the linear factors $1+o(1)$ and $\log\log(n)$ are omitted, and the time complexity simplifies to:

$$\tilde{T}(n) = \tilde{O}(\log^3(n)) \tag{15}$$

5.1.3 Conclusion

The overall complexity is polynomial in the size of n when expressed in terms of bit operations, making the algorithm efficient for large values of n.

6 Implementation Details

Sample open source .NET and Python implementations, along with test data, are available on the author's Github page [20].

7 Acknowledgements

I am indebted to Professor Seth Pettie for his invaluable insights and advice on both the content and presentation of this paper. His expertise in academic writing and research methodologies has been incredibly helpful, and I am particularly thankful for his mentorship and constructive criticism that significantly shaped this work. To Professor Pettie: I am forever grateful for your open mindedness and willingness to engage with me. I also extend my gratitude to the graduate students in his department, for the engaging session we shared and their input and earnest interest in my research.

I owe a great deal of inspiration to the proofs by Kopparty and Wang in their paper on polynomial roots and coefficients over finite fields [15]. Their ingenious approach was instrumental in the development of the key proof in my paper. I also extend my heartfelt gratitude to Professor Kopparty, for his encouraging and constructive feedback, which came at a challenging time when I was ready to give up.

I extend my sincere gratitude to Professor Oded Goldreich for his guidance and support throughout the publication process at the ECCC. His patience and motivational guidance, particularly during moments of uncertainty, were invaluable. His expertise in navigating the complex landscape of academic publishing has been indispensable.

A special thanks to the community at `mersenneforum.org`, particularly to users Charybdis, R. D. Silverman, and Dr. Sardonicus, for their insightful feedback and scrutiny of my earliest proof attempts. Their contributions were fundamental in refining my approach.

Disclaimer: The views and any errors in this paper are solely my own and do not necessarily reflect those of the individuals acknowledged herein.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of Mathematics*, pages 781–793, 2002.

[2] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.

[3] Hendrik W Lenstra and Carl Pomerance. Primality testing with gaussian periods. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 369(1951): 3376–3390, 2011.

[4] Hendrik W Lenstra. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[5] Robert Baillie and Samuel S Jr Wagstaff. Lucas pseudoprimes. *Mathematics of Computation*, 35(152): 1391–1417, 1980.

[6] Michael O Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1): 128–138, 1980.

[7] Gary L Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3):300–317, 1976.

[8] Samuel S Jr Wagstaff. Pseudoprimes and a generalization of artin's conjecture. *Acta Arithmetica*, 41 (2):141–150, 1983.

[9] Carl Pomerance. The use of elliptic curves in cryptography. *Advances in Cryptology*, pages 203–208, 1984.

[10] Andrew Granville. It is easy to determine whether a given integer is prime. *Bulletin of the American Mathematical Society*, 42:3–38, 2004. URL `https://www.ams.org/journals/bull/2005-42-01/S0273-0979-04-01037-7`.

[11] N. J. A. Sloane. Entry a001567 in the on-line encyclopedia of integer sequences. `https://oeis.org/A001567`, 2023. Fermat pseudoprimes to base 2.

[12] 2734364041 (https://mathoverflow.net/users/111215/2734364041). Least number coprime to a given integer. MathOverflow, 2021. URL `https://mathoverflow.net/q/409792`. URL:https://mathoverflow.net/q/409792 (version: 2021-12-01).

[13] Kowalewski G. Euler L. *Adnotationum ad calculum integralem Euleri*, volume 12 of *Opera Omnia Ser. 1; opera mat.* Teubner, 1914.

[14] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. MIT Press, 3 edition, 2009. ISBN 978-0-262-03384-8.

[15] Swastik Kopparty and Qiang Wang. Roots and coefficients of polynomials over finite fields. *Finite Fields and Their Applications*, 29:198–201, 2014. ISSN 1071-5797. doi: https://doi.org/10.1016/j.ffa.2014.04.002. URL `https://www.sciencedirect.com/science/article/pii/S1071579714000574`.

[16] Gregory Karpilovsky. *Topics in Field Theory*. North-Holland Mathematics Studies. North-Holland, 1989. ISBN 9780444705207.

[17] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3 edition, 2004. ISBN 978-0-471-43334-7.

[18] Joris van Der Hoeven David Harvey. Integer multiplication in time o(n log n). *Annals of Mathematics*, 2021. doi: 10.4007/annals.2021.193.2.4.hal-02070778v2.

[19] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3 edition, 2013. ISBN 978-1107039032.

[20] Joseph M. Shunia. A sample .net implementation of the primality test. `https://github.com/jshunia/Shunia.Primes`, 2023. Accessed: December 2023.