An Efficient Deterministic Primality Test

Joseph M. Shunia

December 2023

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 psuedoprimes (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 main theorem posits a condition for an odd integer n to be prime, based on specific modular congruences related to the binomial transforms of powers of 2. The basis for our test is the following main theorem: Let n be an odd integer satisfying $2^{n-1} \equiv 1 \pmod{n}$. Denote D as the least integer strictly greater than 2 and less than n which does not divide $n-1$. Then, n is prime if and only if a set of simultaneous modular congruences involving D, n, and binomial coefficients hold.

This paper is structured as follows: We begin by presenting the main theorem and its proof, substantiated by supporting lemmas. The proof of our main theorem 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. A notable challenge in this regard is the computation of a specific congruence that remains infeasible with existing methods. To address this, we introduce an innovative approach utilizing a specialized polynomial ring which provides efficient calculations. We conclude with pseudocode for our test, and a link to an open source implementation, to demonstrate how our test can be implemented.

2 Main Theorem

Theorem 1. Let n be an odd integer > 3 satisfying $2^{n-1} \equiv 1 \pmod{n}$. Denote D as the least integer greater than 2 and less than n which does not divide $n-1$. If D does not divide n and the following congruence holds, then n is prime:

$$1 + 2^{\left\lfloor \frac{n-1}{D} \right\rfloor} \equiv \left(1 + 2^{\left\lfloor \frac{n-1}{D} \right\rfloor}\right)^n \equiv \sum_{k=0}^{n} \binom{n}{k} 2^{\left\lfloor \frac{k}{D} \right\rfloor} \pmod{n} \tag{1}$$

2.1 Supporting Lemmas

Lemma 1 (Floor function and indivisibility)**.** 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 (Bounds on least non-divisor)**.** Let n be an integer such that $n > 3$, then there exists an integer $1 < D \leq \lfloor \log_2(n-1) \rfloor + 2$ which does not divide $n-1$.

Proof. If n is a composite integer > 3, clearly $n-1$ can have at most $\lfloor \log_2(n-1) \rfloor$ prime factors (when $n-1$ is a power of 2). Since 2 is the least prime that may divide $n-1$, there must exist a $D \leq \lfloor \log_2(n-1) \rfloor + 2$ which does not divide $n-1$. □

Lemma 4 (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 smallest integer $2 < D < n$ 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 $\text{ord}_n(2)$, that is, $k = \text{ord}_n(2)$. Since n is composite and $2^{n-1} \equiv 1 \pmod{n}$, this order, $\text{ord}_n(2)$, must divide $n-1$.

Given D is the least integer greater than 2 and less than n that does not divide $n-1$, and $\text{ord}_n(2)$ divides $n-1$, it follows that D cannot equal $\text{ord}_n(2)$. 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 [10]. It follows from Lemma 3 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 $\text{ord}_n(2)$ 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 $\text{ord}_n(2)$, as this would imply a contradiction with the nature of $\text{ord}_n(2)$ as a divisor of $n-1$. Therefore, $\left\lfloor \frac{n-1}{D} \right\rfloor \neq \text{ord}_n(2)$. □

Lemma 5 (Binomial term inequality for composites)**.** Let n be an odd composite integer greater than 3 such that $2^{n-1} \equiv 1 \pmod{n}$. Denote by D the smallest integer $2 < D < n$ which does not divide $n-1$. If D does not divide n, then there exists at least one integer k in $1 < k < n$ for which $\binom{n}{k} \not\equiv 0 \pmod{n}$ and $2^{\left\lfloor \frac{n-1}{D} \right\rfloor k} \not\equiv 2^{\left\lfloor \frac{k}{D} \right\rfloor} \pmod{n}$.

Proof. Let p be a prime factor of n. We will examine the cases $k = p$ and $k = n - p$.

As shown in [11], for any prime p dividing n, we have $\binom{n}{p} \not\equiv 0 \pmod{n}$. Due to the inherit symmetry of binomial coefficients, $\binom{n}{k} = \binom{n}{n-k}$, it follows that $\binom{n}{n-p} = \binom{n}{p} \not\equiv 0 \pmod{n}$.

Let $k = p$ and assume that p satisfies $2^{\left\lfloor \frac{n-1}{D} \right\rfloor p} - 2^{\left\lfloor \frac{p}{D} \right\rfloor} \equiv 0 \pmod{n}$. Regarding $\text{ord}_n(2)$, this implies:

$$\left\lfloor \frac{n-1}{D} \right\rfloor p \equiv \left\lfloor \frac{p}{D} \right\rfloor \pmod{\text{ord}_n(2)} \tag{2}$$

This implies that there is an integer x such that:

$$\left\lfloor \frac{n-1}{D} \right\rfloor p - \left\lfloor \frac{p}{D} \right\rfloor = x \cdot \text{ord}_n(2) \tag{3}$$

We examine a well-known identity for the floor function [12]:

$$\left\lfloor \frac{a}{b} \right\rfloor = \frac{a - (a \bmod b)}{b} \tag{4}$$

Applying it to our equation gives:

$$\frac{(n - 1 - ((n-1) \bmod D)) \cdot p}{D} - \frac{p - (p \bmod D)}{D} = x \cdot \text{ord}_n(2) \tag{5}$$

Multiplying both sides by D:

$$(n - 1 - ((n-1) \bmod D)) \cdot p - (p - (p \bmod D)) = (D \cdot x) \cdot \text{ord}_n(2) \tag{6}$$

The above equation informs us that any solutions to the congruence at both $k = p$ and $k = n - p$ must be of the form $y = D \cdot x$, where x is an integer. Translating this to modular arithmetic, we now look at the corresponding congruence for $k = p$:

$$n - 1 - ((n-1) \bmod D)) \equiv p - (p \bmod D) \pmod{\text{ord}_n(2)} \tag{7}$$

Re-arranging terms and simplifying:

$$n-1 \equiv p-(p \bmod D)+((n-1) \bmod D)) \pmod{\operatorname{ord}_n(2)} \tag{8}$$
$$n-p-1 \equiv ((n-1) \bmod D))-(p \bmod D) \pmod{\operatorname{ord}_n(2)} \tag{9}$$
$$-p-1 \equiv ((n-1) \bmod D))-(p \bmod D)-n \pmod{\operatorname{ord}_n(2)} \tag{10}$$
$$p+1 \equiv -((n-1) \bmod D))+(p \bmod D)+n \pmod{\operatorname{ord}_n(2)} \tag{11}$$
$$p+1 \equiv (p \bmod D)-((n-1) \bmod D))+n \pmod{\operatorname{ord}_n(2)} \tag{12}$$
$$p \equiv (p \bmod D)-((n-1) \bmod D))+n-1 \pmod{\operatorname{ord}_n(2)} \tag{13}$$

Comparing to the simplification at $k = n - p$:

$$n-1-((n-1) \bmod D)) \equiv n-p-((n-p) \bmod D) \pmod{\operatorname{ord}_n(2)} \tag{14}$$
$$n-1 \equiv n-p-((n-p) \bmod D)+((n-1) \bmod D)) \pmod{\operatorname{ord}_n(2)} \tag{15}$$
$$n-n-p-1 \equiv ((n-1) \bmod D))-((n-p) \bmod D) \pmod{\operatorname{ord}_n(2)} \tag{16}$$
$$-p-1 \equiv ((n-1) \bmod D))-((n-p) \bmod D) \pmod{\operatorname{ord}_n(2)} \tag{17}$$
$$p+1 \equiv ((n-p) \bmod D)-((n-1) \bmod D)) \pmod{\operatorname{ord}_n(2)} \tag{18}$$
$$p \equiv ((n-p) \bmod D)-((n-1) \bmod D))-1 \pmod{\operatorname{ord}_n(2)} \tag{19}$$

Notice that the final congruences for $k = p$ and $k = n - p$, eq. (14) and eq. (20) respectively, both contain an equivalence to p on the left-hand side. Hence, the right-hand sides must be equivalent. Setting it up:

$$((n-p) \bmod D)-((n-1) \bmod D))-1 \equiv (p \bmod D)-((n-1) \bmod D))+n-1 \pmod{\operatorname{ord}_n(2)} \tag{20}$$

We may simplify further using the fact that $((n-1) \bmod D) = D-1$, which follows from the definition of D as the least non-divisor of $n-1$:

$$((n-p) \bmod D)-(D-1)-1 \equiv (p \bmod D)-(D-1)+n-1 \pmod{\operatorname{ord}_n(2)} \tag{21}$$
$$((n-p) \bmod D)-D+1-1 \equiv (p \bmod D)-D+1+n-1 \pmod{\operatorname{ord}_n(2)} \tag{22}$$
$$((n-p) \bmod D)-D \equiv (p \bmod D)+n-D \pmod{\operatorname{ord}_n(2)} \tag{23}$$
$$((n-p) \bmod D) \equiv (p \bmod D)+n \pmod{\operatorname{ord}_n(2)} \tag{24}$$
$$((n-p) \bmod D)-(p \bmod D) \equiv n \pmod{\operatorname{ord}_n(2)} \tag{25}$$

Recall that any solutions to this congruence must be of the form $y = D \cdot x$, where x is an integer. However, this would imply that $n = D \cdot x$ and hence, D is a factor of n. However, this contradicts our requirement that n not have a prime factor $\leq D$. Therefore, the values at $k = p$ and $k = n - p$ cannot be equivalent. We may conclude:

$$2^{\left\lfloor \frac{n-1}{D} \right\rfloor (n-p)} - 2^{\left\lfloor \frac{n-p}{D} \right\rfloor} \not\equiv 0 \pmod{n} \tag{26}$$

Furthermore, we have already established $\binom{n}{n-p} = \binom{n}{p} \not\equiv 0 \pmod{n}$. This completes the proof. □

2.2 Proof of the Main Theorem

Proof of Theorem 1. Let n be an odd integer > 3 satisfying $2^{n-1} \equiv 1 \pmod{n}$.

Define $f(x) = 2^{\left\lfloor \frac{x-1}{D} \right\rfloor}$ and D as the least integer greater than 2 that does not divide $n-1$. We begin with the congruence:

$$(1+f(n))^n \equiv \sum_{k=0}^{n} \binom{n}{k} f(k+1) \pmod{n} \tag{27}$$

Using the binomial theorem, we expand the left-hand side:

$$\sum_{k=0}^{n} \binom{n}{k} f(n)^k \equiv \sum_{k=0}^{n} \binom{n}{k} f(k+1) \pmod{n} \tag{28}$$

Rewriting this, we must have:

$$\sum_{k=0}^{n} \binom{n}{k} \left(f(n)^k - f(k+1)\right) \equiv 0 \pmod{n}. \tag{29}$$

As a necessary condition of our test, we also require:

$$\sum_{k=0}^{n} \binom{n}{k} f(n)^k \equiv \sum_{k=0}^{n} \binom{n}{k} f(k+1) \equiv 1 + f(n) \pmod{n} \tag{30}$$

By the binomial theorem, we isolate the inner terms:

$$1 + f(n)^n + \sum_{k=1}^{n-1} \binom{n}{k} f(n)^k \equiv 1 + f(n) + \sum_{k=1}^{n-1} \binom{n}{k} f(k+1) \equiv 1 + f(n) \pmod{n} \tag{31}$$

Setting common terms to zero:

$$\sum_{k=1}^{n-1} \binom{n}{k} f(n)^k \equiv \sum_{k=1}^{n-1} \binom{n}{k} f(k+1) \equiv 0 \pmod{n} \tag{32}$$

We have defined n such that $2^{n-1} \equiv 1 \pmod{n}$, which implies $2^n - 2 \equiv \sum_{k=1}^{n-1} \binom{n}{k} \equiv 0 \pmod{n}$. Plugging it in:

$$\sum_{k=1}^{n-1} \binom{n}{k} \equiv \sum_{k=1}^{n-1} \binom{n}{k} f(n)^k \equiv \sum_{k=1}^{n-1} \binom{n}{k} f(k+1) \equiv 0 \pmod{n} \tag{33}$$

Subtracting $\sum_{k=1}^{n-1} \binom{n}{k}$ gives:

$$\left(\sum_{k=1}^{n-1} \binom{n}{k} f(n)^k\right) - \sum_{k=1}^{n-1} \binom{n}{k} \equiv \left(\sum_{k=1}^{n-1} \binom{n}{k} f(k+1)\right) - \sum_{k=1}^{n-1} \binom{n}{k} \equiv 0 \pmod{n} \tag{34}$$

Combining the summations:

$$\sum_{k=1}^{n-1} \left(\binom{n}{k} f(n)^k - \binom{n}{k}\right) \equiv \sum_{k=1}^{n-1} \left(\binom{n}{k} f(k+1) - \binom{n}{k}\right) \equiv 0 \pmod{n} \tag{35}$$

$$\sum_{k=1}^{n-1} \left(\binom{n}{k} f(n)^k - \binom{n}{k} f(k+1) - \binom{n}{k}\right) \equiv 0 \pmod{n} \tag{36}$$

Factoring out the common $\binom{n}{k}$ from the inner terms reveals:

$$\sum_{k=1}^{n-1} \binom{n}{k} \left(f(n)^k - f(k+1) - 1\right) \equiv 0 \pmod{n} \tag{37}$$

For the above congruence, there are three potential cases we must examine.

Case 1: n is prime

In this case, the congruence always holds. By the binomial theorem, $\binom{n}{k} \equiv 0 \pmod{n}$ for $0 < k < n$ and the congruence simplifies trivially to zero.

Case 2: n is composite and $f(n) \equiv 1 \pmod{n}$

In this case, the congruence may or may not hold. With $f(n) \equiv 1 \pmod{n}$, the congruence simplifies significantly, making it possible:

$$\sum_{k=1}^{n-1} \binom{n}{k} \left(f(n)^k - f(k+1) - 1\right) \equiv 0 \pmod{n} \tag{38}$$

$$\sum_{k=1}^{n-1} \binom{n}{k} \left(1^k - f(k+1) - 1\right) \equiv 0 \pmod{n} \tag{39}$$

$$\sum_{k=1}^{n-1} \binom{n}{k} \cdot (-f(k+1)) \equiv 0 \pmod{n} \tag{40}$$

Case 3: n is composite and $f(n) \not\equiv 1 \pmod{n}$

In this case, the congruence cannot hold.

Since $\sum_{k=1}^{n-1} \binom{n}{k} \equiv 0 \pmod{n}$, we may add or subtract $\sum_{k=1}^{n-1} \binom{n}{k}$ from our congruence an arbitrary number of times and n must still divide the sum. The same applies to $\sum_{k=1}^{n-1} \binom{n}{k} f(n)^k$ and $\sum_{k=1}^{n-1} \binom{n}{k} f(k+1)$. Therefore, we surmise that the following must hold for all $W, X, Y \in \mathbb{Z}$:

$$W\left(\sum_{k=1}^{n-1} \binom{n}{k} f(n)^k\right) - X\left(\sum_{k=1}^{n-1} \binom{n}{k} f(k+1)\right) - Y\left(\sum_{k=1}^{n-1} \binom{n}{k}\right) \equiv 0 \pmod{n} \tag{41}$$

$$\left(\sum_{k=1}^{n-1} \binom{n}{k} f(n)^k W\right) - \left(\sum_{k=1}^{n-1} \binom{n}{k} f(k+1) X\right) - \left(\sum_{k=1}^{n-1} \binom{n}{k} Y\right) \equiv 0 \pmod{n} \tag{42}$$

$$\sum_{k=1}^{n-1} \binom{n}{k} \left(W \cdot f(n)^k - X \cdot f(k+1) - Y\right) \equiv 0 \pmod{n} \tag{43}$$

If $\binom{n}{k} \not\equiv 0 \pmod{n}$ for any k, as we know it must be for some k, and $f(n)^k \not\equiv f(k+1) \pmod{n}$, then the summation within our congruence may sum to any value by adjusting the values of W, X, and Y. For the congruence to hold, we would require all integers to be equivalent to 0 (mod n). However, this is a contradiction, as $n \neq 1$ and it is impossible.

Consequently, to prove that the congruence cannot hold, it suffices to show that $f(n)^k \not\equiv f(k+1) \pmod{n}$ for some k with $\binom{n}{k} \not\equiv 0 \pmod{n}$. By Lemma 5, we know that at least one such k exists. For this k, the non-zero term in the sum, when multiplied by the non-zero binomial coefficient, ensures that the sum cannot be congruent to zero modulo n for all possible permutations of W, X, Y and hence, the congruence fails.

Conclusion:

When n is an odd prime integer > 3, the congruence holds. When n is an odd composite integer > 3 satisfying the initial conditions, by Lemma 4 we have $f(n) \not\equiv 1 \pmod{n}$ and therefore, the congruence cannot hold. The theorem is proven. □

3 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. Find the least integer D that is greater than 2 and less than n which does not divide $n-1$.
4. If $n \equiv 0 \mod D$, output COMPOSITE.
5. If $2^{n-1} \not\equiv 1 \pmod{n}$, output COMPOSITE.
6. Set $A = 2^{\lfloor \frac{n-1}{D} \rfloor} \bmod n$.
7. Set $B = (1+A)^n \bmod n$.
8. If $B \not\equiv 1 + A \pmod{n}$, output COMPOSITE.
9. Set $C = \sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \bmod n$.
10. If $C \not\equiv 1 + A \pmod{n}$, output COMPOSITE.
11. Output PRIME;

3.1 Time Complexity Analysis

3.1.1 Algorithm Overview

The given algorithm is a primality test that involves several computational steps, including modular arithmetic and polynomial exponentiation in the ring $\mathbb{Z}/n\mathbb{Z}$.

3.1.2 Analysis of Individual Operations

1. **Check for Even** n:
   This step involves calculating $n \bmod 2$ and has a time complexity of $O(1)$.
2. **Finding** D:
   Finding the least integer $D > 2$ that does not divide $n-1$ takes at most $O(\log(n))$ steps, with each step requiring $O(1)$ time for the mod operation. Hence, the overall complexity is $O(\log(n))$.
3. **Checking if** D **Divides** n:
   Checking if n is divisible by D requires $O(1)$ time for the mod operation.
4. **Modular Exponentiation** $2^{n-1} \bmod n$:
   This step requires modular exponentiation with a $\log(n)$-digit base and a $\log(n)$-digit exponent. The time complexity of modular exponentiation is $O(\log(n)M(n))$.

5. **Computing A and B**:

   Each of these steps involves modular exponentiation similar to Step 2, and thus each has a time complexity of $O(\log(n)M(n))$.

6. **Computing C**:

   Computing C involves exponentiating a polynomial in the ring $\mathbb{Z}/n\mathbb{Z}$ with $O(\log(n))$ terms and summing the coefficients. The mathematics underlying the computation of C is described and proven in §4.

   (a) Summing the polynomial coefficients can be done in $O(\log^2(n))$ time.

   (b) Exponentiation using repeated squaring takes $O(\log(n))$ steps, and each step requires $O(M(n)\log(n))$ time due to the multiplication of polynomials of size $O(\log(n))$.

   Therefore, the overall complexity for computing C is $O(\log^2(n)M(n))$.

7. **Comparisons**:

   The final steps involve comparisons which are $O(1)$ operations.

3.1.3 Overall Time Complexity

The dominant time complexity in the algorithm comes from computing C. Therefore, the overall time complexity of the algorithm is $T(n) = O(\log^2(n)M(n))$.

Harvey and van Der Heoven (2021) have given an algorithm for integer multiplication which has a time complexity $M(n) = O(\log(n)\log\log(n))$ [13]. This would give our algorithm an overall time complexity of:

$$T(n) = O(\log^2(n)M(n)) = O(\log^2(n)\log(n)\log\log(n)) = O(\log^3(n)\log\log(n)) = \tilde{O}(\log^3(n)) \tag{44}$$

3.1.4 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.

4 Efficient Calculations via Polynomial Rings

In this section, we define a special polynomial ring R with a modular variation M, and show how M can be used to efficiently calculate the value of $\sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod n$. The standard approach to calculating this value requires evaluating $\binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod n$ for each k and summing the results, which takes time exponential in n. Conversely, our approach offers an efficient polynomial time complexity of $\tilde{O}(D\log^2(n))$ (See: §3.1).

4.1 Ring Definition

Definition 1 (Polynomial ring R)**.** We construct a polynomial ring $R = \mathbb{Z}[x]$ in which addition is carried out as usual, and multiplication is followed by polynomial degree reduction via a special substitution function, denoted Φ [14]. The multiplication operation $*$ is defined as follows:

$$P(x) * Q(x) = \Phi(P(x) \cdot Q(x)) \text{ for all } P(x), Q(x) \in R, \tag{45}$$

Φ is an operation that enforces any defined substitution rules for the polynomial's terms upon multiplication. In our case, for the generator x, we have:

$$x * x^{d-1} = x^d = \Phi(x^d) = N, \text{ where } N \in R \tag{46}$$

For any polynomial in our ring R, the function Φ is distributed to the individual terms and implicitly applied to reduce terms. Whenever the term x^d appears, it is replaced with its defined mapping. The mappings in Φ are extended to terms of higher degrees, meaning $\Phi(x^{d+k}) = \Phi(x^d * x^k) = Nx^k$, for $k > 1$. Φ is applied recursively to the polynomial until and its terms until the degree of the polynomial is less than d. For terms which do not match a defined substitution rule, Φ returns them as they are.

Example 1. We take the ring R as defined in Definition 1 with $N = 2$, $d = 3$. Hence, $\Phi(x^3) = 2$. $P(x) := 1 + x + 3x^3 + x^4 + x^6, P(x) \in R$.

$$\begin{aligned}
\Phi(P(x)) &= \Phi(1 + x + 3x^3 + x^4 + x^6) && (47)\\
&= \Phi(1) + \Phi(x) + \Phi(3x^3) + \Phi(x^4) + \Phi(x^6) && (48)\\
&= 1 + x + \Phi(2 \cdot 3) + \Phi(2 \cdot x) + \Phi(2 \cdot x^3) && (49)\\
&= 1 + x + 6 + 2x + \Phi(2 \cdot 2) && (50)\\
&= 7 + 3x + 4 && (51)\\
&= 11 + 3x && (52)
\end{aligned}$$

4.2 Ring Axioms

We assert that the ring R with the modified operation $*$ still satisfies the standard ring axioms. Specifically, we show that $(R, +, *)$ is associative, commutative (with respect to addition), and has an additive identity and an additive inverse for every element. Additionally, the distributive property of multiplication over addition is preserved under the operation $*$.

4.2.1 Multiplicative Properties

Proposition 1 (Distributivity of $*$)**.** The operation $*$ is distributive over addition in the ring R.

Proof. The modified multiplication $*$ is distributive over addition because for any $P(x), Q(x), S(x) \in R$,

$$\begin{aligned}
P(x) * (Q(x) + S(x)) &= \Phi(P(x) \cdot (Q(x) + S(x))) && (53)\\
&= \Phi(P(x) \cdot Q(x) + P(x) \cdot S(x)) && (54)\\
&= \Phi(P(x) \cdot Q(x)) + \Phi(P(x) \cdot S(x)) && (55)\\
&= P(x) * Q(x) + P(x) * S(x) && (56)
\end{aligned}$$

Where the second equality uses the distributive property of the standard multiplication in $\mathbb{Z}[x]$ and the linearity of Φ with respect to polynomial addition. □

Proposition 2 (Associativity of $*$)**.** The multiplication operation $*$ in the ring R is associative.

Proof. To prove associativity, we need to show that for any $P(x), Q(x), S(x) \in R$:

$$(P(x) * Q(x)) * S(x) = P(x) * (Q(x) * S(x)) \tag{57}$$

Expanding the left-hand side:

$$(P(x) * Q(x)) * S(x) = \Phi(P(x) \cdot Q(x)) * S(x) \tag{58}$$
$$= \Phi(\Phi(P(x) \cdot Q(x)) \cdot S(x)) \tag{59}$$

Similarly, for the right-hand side:

$$P(x) * (Q(x) * S(x)) = P(x) * \Phi(Q(x) \cdot S(x)) \tag{60}$$
$$= \Phi(P(x) \cdot \Phi(Q(x) \cdot S(x))) \tag{61}$$

Since the standard multiplication in $\mathbb{Z}[x]$ is associative and Φ is a well-defined operation that respects this associativity, we have:

$$\Phi(\Phi(P(x) \cdot Q(x)) \cdot S(x)) = \Phi(P(x) \cdot \Phi(Q(x) \cdot S(x))) \tag{62}$$

Which shows that:

$$(P(x) * Q(x)) * S(x) = P(x) * (Q(x) * S(x)) \tag{63}$$

□

4.2.2 Additive Properties

Proposition 3 (Preservation of additive properties)**.** The commutative and associative properties of addition, and the existence of an additive identity and inverses, are maintained in the ring R.

Proof. The additive structure of R remains unchanged. Thus, the commutative and associative properties of addition, and the existence of an additive identity and inverses, are inherited directly from $\mathbb{Z}[x]$. □

4.3 Modular Ring Definition

Definition 2 (Modular polynomial ring M)**.** Let $R = \mathbb{Z}[x]$ be our polynomial ring as defined in Definition 1, where the multiplication is modified by a substitution function Φ as described previously. Let n be a positive integer. We define the modular variation of R, denoted as M, to be the ring of polynomials with coefficients in $\mathbb{Z}/n\mathbb{Z}$ and with multiplication modified by a corresponding substitution function Φ_M. Formally, $M = (\mathbb{Z}/n\mathbb{Z})[x]$, where the coefficients of the polynomials in M are taken modulo n, and the multiplication in M is given by

$$P(x) * Q(x) = \Phi_M(P(x) \cdot Q(x)) \text{ for all } P(x), Q(x) \in M, \tag{64}$$

Φ_M is defined analogously to Φ but operates within the context of the coefficients being in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 4. The ring $M = (\mathbb{Z}/n\mathbb{Z})[x]$ with the modified multiplication operation $*$, as defined by the substitution function Φ_M, inherits the standard ring axioms from $R = \mathbb{Z}[x]$.

Proof. Since the ring M is structurally analogous to R with the only difference being the coefficient domain ($\mathbb{Z}/n\mathbb{Z}$ instead of $\mathbb{Z}$), and the modified multiplication operation $*$ in M is defined similarly to R using Φ_M, analogous to Φ, M inherits the ring properties of R. This includes the associativity and commutativity of addition, the existence of an additive identity and inverses, the distributivity of multiplication over addition, and the associativity of multiplication. These properties are preserved under the transition from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ coefficients and the analogous definition of $*$ in M. □

4.4 Ring Calculations

We now demonstrate how our modular polynomial ring M can be used to efficiently calculate the value of $\sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$.

In an earlier paper relating the central binomial coefficients and Gould's sequence to polynomial rings [14], we showed how a multivariate polynomial ring, analogous to the univariate polynomial ring we have defined herein, can be used generally to compute the binomial transforms of recursive integer sequences. We apply the same technique here.

Theorem 2. Let n, k be non-negative integers. Let D be an integer > 2. Define the ring M as in Definition 2 with $d = D - 1$, $N = 2$, hence $\Phi(x^{D-1}) = 2$. $P(x) := x, P(x) \in M$. Taking the sum of the coefficients modulo n in the polynomial expansion of $P(x)^k$, gives $2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$.

Proof. Examining $D = 2$, we can see:

$$
\begin{aligned}
P(x)^0 &= 1 = 2^{\lfloor 0/2 \rfloor} \\
P(x)^1 &= x = 1 = 2^{\lfloor 1/2 \rfloor} \\
P(x)^2 &= x^2 = 2 = 2^{\lfloor 2/2 \rfloor} \\
P(x)^3 &= x^3 = 2x = 2 = 2^{\lfloor 3/2 \rfloor} \\
P(x)^4 &= x^4 = 2x^2 = 4 = 2^{\lfloor 4/2 \rfloor} \\
P(x)^5 &= x^5 = 4x = 4 = 2^{\lfloor 5/2 \rfloor} \\
P(x)^6 &= x^6 = 4x^2 = 8 = 2^{\lfloor 6/2 \rfloor} \\
&\vdots
\end{aligned}
$$

We proceed by induction.

Base Case: For $k = 0$, we have $P(x)^0 = 1$, and the sum of coefficients is $2^{\lfloor \frac{0-1}{D} \rfloor} = 2^0 = 1$.

Inductive Step: Assume the theorem holds for some $k \geq 0$, i.e., the sum of coefficients modulo n in $P(x)^k$ is $2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$. We need to show it also holds for $k + 1$.

Consider $P(x)^{k+1} = P(x)^k * P(x)$. By the definition of $*$ and Φ, the degree of $P(x)^{k+1}$ gets reduced by Φ every time it reaches D. The number of times this reduction happens is $\lfloor \frac{k}{D} \rfloor$. Therefore, the sum of coefficients in $P(x)^{k+1}$ should be $2^{\lfloor \frac{k+1}{D} \rfloor}$, as each reduction by Φ doubles the sum of coefficients. Hence, the theorem holds for $k + 1$.

Conclusion: By the principle of mathematical induction, the theorem is proven. □

Theorem 3. Let n an integer > 0. Let D be an integer > 2. Define the ring M as in Definition 2 with $d = D - 1$, $N = 2$, hence $\Phi(x^{D-1}) = 2$. $P(x) := x, P(x) \in M$. Then taking the sum of the coefficients modulo n in the polynomial expansion of $(1 + P(x))^n$ is equivalent to $\sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \pmod{n}$.

Proof. By the binomial theorem, we have:

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} P(x)^k \tag{65}$$

Hence, when we evaluate this polynomial at $x = 1$, we sum the coefficients of the polynomial to get:

$$\sum_{k=0}^{n} \binom{n}{k} 2^{\lfloor \frac{k}{D} \rfloor} \quad \text{(by Theorem 2)} \tag{66}$$

This completes the proof. □

5 Implementation Details

5.1 Reference Implementation

Sample open source .NET and Python implementations, along with test data, are available on the author's Github page [15].

5.2 Pseudocode Implementation

To demonstrate how our test may be implemented, we offer a pseudocode implementation of the key functions involved.

5.2.1 IsPrime Function

Require: An integer $n > 1$
  function IsPrime(n)
    if $n \bmod 2 = 0$ **then**
      if $n = 2$ **then**
        return true ▷ n is prime
      else
        return false ▷ n is composite
      end if
    end if
    if $n = 3$ **then**
      return true ▷ n is prime
    end if
    $fermat \leftarrow \text{Pow}(2, n-1, n)$ ▷ Fermat pseudoprime test to base 2
    if $fermat \neq 1$ **then**
      return false ▷ n is composite
    end if
    $D \leftarrow 2$
    $log \leftarrow \text{Log2}(n)$
    for $i \leftarrow 3$ **to** $\text{Max}(log, 3)$ **do** ▷ Find D, the least non-divisor of $n-1$
      $D \leftarrow i$
      $m \leftarrow (n-1) \bmod D$
      if $m \neq 0$ **then**
        break
      end if
    end for
    for $i \leftarrow 3$ **to** $D+1$ **do** ▷ Check for divisibility of n up to D
      $m \leftarrow n \bmod i$
      if $m = 0$ **then return false** ▷ n is composite
      end if
    end for
    $A \leftarrow \text{Pow}(2, \lfloor (n-1)/D \rfloor, n)$
    $expectedValue \leftarrow (A+1) \bmod n$
    $B \leftarrow \text{Pow}(A+1, n, n)$

```
    if B ≠ expectedValue then
        return false                                              ▷ n is composite
    end if
    polyDegree ← D − 1                    ▷ Subtract 1 to account for zero indexing in arrays
    poly ← PolyPow([1, 1], n, n, polyDegree, [2])
    C ← PolyEval(poly, 1) mod n                          ▷ Evaluate at x=1 to sum coefficients
    if C ≠ expectedValue then
        return false                                              ▷ n is composite
    end if
    return true                                                   ▷ n is prime
end function
```

5.2.2 PolyPow Function

```
function PolyPow(poly_A, k, n, d, polyMapping)
    polyB ← [1]                  ▷ Initialize polyB as a polynomial with constant term 1
    while k > 0 do
        if k mod 2 = 1 then
            polyB ← PolyMul(polyA, polyB, n)                  ▷ Multiply polynomials modulo n
            polyB ← PolyReduce(polyB, d, polyMapping, n)      ▷ Reduce degree of polyB
            if k = 1 then
                break
            end if
        end if
        polyA ← PolyMul(polyA, polyA, n)                      ▷ Square polyA modulo n
        polyA ← PolyReduce(polyA, d, polyMapping, n)          ▷ Reduce degree of polyA
        k ← k/2
    end while
    return polyB
end function
```

5.2.3 PolyReduce Function

```
function PolyReduce(polyA, d, mappingPoly, n)
    if Length(polyA) ≤ d then
        return polyA
    end if
    polyB ← Clone(polyA)                          ▷ Copy the polynomial to a new array
    polyDegree ← Degree(mappingPoly)              ▷ Find degree of the mapping polynomial
    degreeDelta ← d − polyDegree
    for i ← Length(polyB) − 1 downto d + 1 do
        if polyB[i] = 0 then
            continue
        end if
        for j ← i − 1 − degreeDelta, k ← polyDegree downto 0 do
            polyB[j] ← polyB[j] + polyB[i] × mappingPoly[k]   ▷ Degree reduction step
        end for
        polyB[i] ← 0
    end for
    polyC ← new array of size d + 1
    for i ← 0 to min(Length(polyC), Length(polyB)) − 1 do     ▷ Take coefficients modulo n
```

```
        polyC[i] ← polyB[i]
        if n ≠ 0 then
            polyC[i] ← polyC[i] mod n
        end if
    end for
    return polyC
end function
```

6 Acknowledgements

The author would like to thank the kind users at `mersenneforum.org` for their helpful feedback.

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

[11] C. S. Ogilvy. *Through the Mathescope*. Oxford University Press, New York, 13 edition, 1956.

[12] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 2008.

[13] 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.

[14] Joseph M. Shunia. A polynomial ring connecting central binomial coefficients and gould's sequence, 2023. URL https://arxiv.org/abs/2312.00302.

[15] Joseph M. Shunia. A sample .net implementation of the primality test. https://github.com/jshunia/Shunia.Primes, 2023. Accessed: December 4 2023.