Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 200 (2023)

Deterministic Polynomial-Time Primality Testing with a Single Binomial Congruence

Joseph M. Shunia

October 29, 2026

Abstract

We give a deterministic polynomial-time primality test whose main verification is the congruence $(1+X)^n = 1+X^n$ in $C_n[X]/(X^r - b(Y))$, where $C_n = (\mathbb{Z}/n\mathbb{Z})[Y]/(\Phi_r(Y))$. Two identities in the coefficient ring normalize b and ensure compatibility with the main congruence. A finite-field root count and a lattice bound show that an accepted input is a prime power; elementary preprocessing excludes nontrivial perfect powers. We construct b deterministically using Jacobi sums and the uniform Dedekind-zeta zero-free theorem of Cureton and Thorner, which extends OpenAI's Hecke zero-free theorem. The total bit complexity is $L^{32+o(1)}$, where $L = \lceil \log_2 n \rceil$, and verification after constructing b costs $L^{6+o(1)}$. We also state a fixed-base modification of Agrawal's conjecture, using the modulus $X^r - 2$ with r the least positive integer not dividing $n(n-1)$.

1 Introduction

For a prime n, the identity

$$(1+X)^n = 1+X^n \tag{1}$$

holds in every commutative algebra of characteristic n. A primality test based on this identity must choose an algebra small enough to compute in and sufficiently restrictive to exclude composite inputs. We construct such an algebra deterministically, using one shift, one binomial relation, and exponent n.

The coefficient ring and the final algebra are

$$C_n = (\mathbb{Z}/n\mathbb{Z})[Y]/(\Phi_r(Y)), \qquad \mathcal{A}_n = C_n[X]/(X^r - b(Y)), \tag{2}$$

where r is odd and squarefree and Φ_r is the rth cyclotomic polynomial. Thus the test can equally be written in the multivariate quotient

$$(\mathbb{Z}/n\mathbb{Z})[X,Y]/\big(\Phi_r(Y), X^r - b(Y)\big).$$

Arithmetic is performed in the full quotient, which may have zero divisors. Field quotients enter only in the proof.

For a suitable auxiliary integer D, the acceptance equalities are

$$b(Y)^{(n^D-1)/r} = Y \qquad \text{in } C_n, \tag{3}$$

$$b(Y)^n = b(Y^n) \qquad \text{in } C_n, \tag{4}$$

$$(1+X)^n = 1+X^n \qquad \text{in } \mathcal{A}_n. \tag{5}$$

ISSN 1433-8092

The single binomial congruence is (5), evaluated in $\mathcal{A}_n$. The two checks in C_n and elementary integer preprocessing complete the test.

The deterministic parameter construction uses a uniform zero-free theorem. OpenAI proved a common width 10^{-6} for finite-order Hecke L-functions over cyclotomic fields containing μ_{12} [11, Theorem 1.2]. Cureton and Thorner extended this approach to all number fields and obtained the following stronger result.

Theorem 1.1 (Cureton–Thorner [9, Theorem 1.1])**.** *For every number field K, its Dedekind zeta function satisfies*

$$\zeta_K(s) \neq 0 \qquad \left(\Re s > \frac{31}{32},\ s \neq 1\right).$$

The theorem has a published Lean formalization generated with AxiomProver [3]. Its uniformity over number fields is what permits a polynomial bound for our auxiliary-prime search. Throughout, $\delta = 1/32$; we retain δ in the estimates to make their dependence on the zero-free width explicit. The algebraic acceptance criterion is independent of this analytic bound.

Theorem 1.2 (Main result)**.** *There is a deterministic primality algorithm using (3)–(5) with total bit complexity*

$$L^{32+o(1)}, \qquad L = \lceil \log_2 n \rceil.$$

Its parameters satisfy

$$D = L^{o(1)}, \qquad r = L^{2+o(1)}, \qquad \varphi(r) \leq r.$$

Verification after constructing b costs $L^{6+o(1)}$ bit operations.

The proof has three components. A normalized coefficient first produces a cyclic orbit of r linear factors in a field extension. Bernstein's root-counting and lattice method [4] then excludes inputs with two distinct prime factors. Next, an Odlyzko–Pomerance construction gives $r = L^{2+o(1)}$, with every prime factor of r of size $L^{o(1)}$. Finally, we construct the coefficient by combining Jacobi sums for those small prime factors. Treating the prime degrees separately keeps the number-field degrees in the auxiliary-prime estimate small.

The AKS theorem established deterministic polynomial-time primality testing [2]. Berrizbeitia and Cheng developed tests using binomial extensions and a small number of congruences [6, 7]. Bernstein gave an essentially quartic random-time primality-proving algorithm [4]; its group-size argument is the algebraic foundation used here. Lenstra and Pomerance subsequently obtained an unconditional $L^{6+o(1)}$ deterministic algorithm using Gaussian periods [10]. The present construction concerns the deterministic realization of the particular congruence (5), with a normalized coefficient in the full cyclotomic quotient. Its auxiliary-prime search dominates the stated total bound.

Throughout, log is the natural logarithm unless a base is displayed. The notation $\widetilde{O}$ suppresses factors polynomial in logarithms. All complexity statements count bit operations; $o(1)$ is as $L \to \infty$, with δ fixed.

2 An algebraic acceptance criterion

We first prove that the three acceptance identities force n to be a prime power. This part of the argument depends only on the identities and the sizes of the degrees, not on how the coefficient is constructed.

Let $n > 3$ be odd, and choose an odd squarefree integer $r > 2$ and a positive integer D such that

$$\gcd(n, r) = \gcd(D, r) = 1, \qquad q - 1 \mid D \quad \text{for every prime } q \mid r. \tag{6}$$

In particular, $\lambda(r) \mid D$, so $n^D \equiv 1 \pmod r$ and the exponent in (3) is integral. For odd r, define

$$h = \frac{r-1}{2}, \qquad B_r = \sum_{j=0}^{h} \binom{r}{j}\binom{h}{j}\binom{r-j+h}{h}. \tag{7}$$

Our exact size condition is

$$3\lfloor \log_2 B_r \rfloor^2 \geq D^2 L^2 r, \qquad L = \lceil \log_2 n \rceil. \tag{8}$$

This condition uses integer arithmetic only: the logarithm floor is the bit length of B_r minus one.

Lemma 2.1 (Cyclotomic coefficient ring)**.** *Under (6), substitution $Y \mapsto Y^n$ defines an automorphism σ of C_n with $\sigma^D = 1$. Each field quotient of C_n is $\mathbb{F}_{p^e}$ for some prime $p \mid n$, where $e = \mathrm{ord}_r(p) \mid D$. In every such quotient the image of Y has order exactly r.*

Proof. Since $\gcd(n, r) = 1$, raising a primitive rth root to its nth power permutes the primitive roots. The integral cyclotomic relation therefore makes the substitution well-defined. An inverse is substitution by Y^v for $nv \equiv 1 \pmod r$. Also $Y^r = 1$ and $n^D \equiv 1 \pmod r$, which prove $\sigma^D = 1$.

A maximal ideal of C_n lies over a prime divisor p of n. Because $p \nmid r$, the polynomial $X^r - 1$ is squarefree in $\mathbb{F}_p[X]$. The roots of Φ_r are precisely the primitive rth roots, whose Frobenius orbits have length $\mathrm{ord}_r(p)$. The quotient fields consequently have the stated degrees. Finally, $p^D \equiv 1 \pmod r$ implies $e \mid D$. □

Lemma 2.2 (Iteration of the main congruence)**.** *If (4) and (5) hold, then*

$$(1+X)^{n^j} = 1 + X^{n^j} \quad \text{in } \mathcal{A}_n \qquad (j \geq 0).$$

Proof. Equation (4) gives $\sigma^i(b) = b^{n^i}$ by induction. Put $F(X) = (1+X)^n - 1 - X^n$. Equation (5) says $X^r - b \mid F(X)$ in $C_n[X]$. Applying σ^i to its coefficients gives $X^r - b^{n^i} \mid F(X)$. Substituting X^{n^i} and using

$$X^r - b \mid X^{rn^i} - b^{n^i}$$

gives $(1 + X^{n^i})^n = 1 + X^{n^{i+1}}$ in $\mathcal{A}_n$. Starting at $j = 0$, this proves the assertion by induction. No additivity of nth powering for composite n is used. □

Theorem 2.3 (Acceptance criterion)**.** *Suppose (6) and (8) hold. If (3)–(5) hold, then n is a prime power. If n is not a nontrivial perfect power, it is prime.*

Proof. Put $N = n^D$. The element Y is a unit, so (3) makes b a unit. Suppose for a contradiction that n has at least two distinct prime divisors. Choose a field quotient $k = \mathbb{F}_{p^e}$ of C_n as in Lemma 2.1, and put $P = p^e$. We use the same names for the images of Y and b. One has $P \mid N$, and Y has order r in $k^\times$.

Choose a root α of $X^r - b$ in an algebraic closure of k. Normalization and Lemma 2.2 imply

$$\alpha^N = Y\alpha, \qquad u_i := 1 + Y^i\alpha, \qquad u_i^N = u_{i+1} \quad (i \bmod r).$$

For the last identity, substitute $Y^i\alpha$ in $(1+X)^N = 1 + X^N$ and use $N \equiv 1 \pmod r$. Each u_i is nonzero: otherwise $\alpha = -Y^{-i}$, so $b = (-1)^r$ and $Y = b^{(N-1)/r}$ would have order at most two. Let G be the finite multiplicative group generated by the u_i in $k(\alpha)^\times$.

We first prove $|G| \geq B_r$, using the signed-product count recorded by Bernstein [4, Section 3]. Consider all integer vectors $a = (a_0, \ldots, a_{r-1})$ for which the positive entries sum to at most h and the absolute values of the negative entries also sum to at most h. If exactly j entries are negative,

their positions can be chosen in $\binom{r}{j}$ ways, their absolute values in $\binom{h}{j}$ ways, and the remaining nonnegative entries in $\binom{r-j+h}{h}$ ways. This gives exactly B_r vectors.

Their products $\prod_i u_i^{a_i}$ are distinct. Indeed, suppose two such products are equal. Taking successive Nth powers rotates all indices, so the equality holds with α replaced by each of the r distinct elements $Y^j\alpha$. Clearing denominators produces an equality of two polynomials at all those elements; each polynomial has degree at most $2h = r - 1$. Their difference is therefore zero by the field root bound. Unique factorization into the pairwise distinct factors $1 + Y^iZ$, whose constant terms are all 1, makes the original exponent vectors equal. Hence

$$|G| \geq B_r. \tag{9}$$

For the upper bound, $r \mid P - 1$, and $b \in k$ gives $\alpha^P = Y^t\alpha$ for some integer t. Set $H = N/P > 1$. Frobenius in characteristic p, followed by injectivity of Pth powering, gives

$$u_i^P = u_{i+t}, \qquad u_i^H = u_{i+1-t}. \tag{10}$$

Consider the lattice

$$\Lambda = \{(a, c) \in \mathbb{Z}^2 : (1 - t)a + tc \equiv 0 \pmod{r}\}.$$

It has determinant r, because $1 - t$ and t generate the unit ideal in $\mathbb{Z}/r\mathbb{Z}$. The symmetric convex hexagon

$$\max\{|a \log H|, |c \log P|, |a \log H + c \log P|\} \leq \sqrt{r/3} \log N$$

has area

$$\frac{r(\log N)^2}{\log H \log P} \geq 4r,$$

since $\log H + \log P = \log N$. Minkowski's convex body theorem gives a nonzero lattice point in this closed hexagon. The equality case follows by slightly enlarging the hexagon and using discreteness. Change its sign if necessary to make $a \geq 0$. If $c \geq 0$, put $U = H^aP^c$ and $V = 1$; if $c < 0$, put $U = H^a$ and $V = P^{-c}$. Equation (10) and the lattice relation give $g^U = g^V$ for every $g \in G$, and

$$\max(U, V) \leq N^{\sqrt{r/3}}.$$

Moreover, $U \neq V$. For $c \geq 0$ this follows from $(a, c) \neq (0, 0)$. For $c < 0$, equality would contradict the fact that H has a prime factor other than p when $a > 0$; when $a = 0$, it would give $1 = P^{-c} > 1$.

Every element of G is consequently a root of $Z^{|U-V|} - 1$ in a field. Thus

$$|G| \leq |U - V| < N^{\sqrt{r/3}} \leq B_r.$$

The last inequality follows from (8), because $\log_2 N \leq DL$. This contradicts (9). Therefore n has only one distinct prime divisor. □

Remark 2.4. The argument does not require $X^r - b$ to be irreducible modulo every prime divisor of n. It takes a root in a field extension and obtains the needed distinct products from the cyclic rotation and the field root bound. Likewise, C_n itself may have zero divisors. Its rank $\varphi(r)$ measures arithmetic cost, whereas the smaller number $e \mid D$ controls the lattice bound.

3 Choosing the degrees

We first record the size of the signed-product count. The improvement from signed products is due to Voloch and Vaaler, as explained in Bernstein's analysis [4, Section 3].

Proposition 3.1. *For odd $r \to \infty$,*

$$\log_2 B_r = \kappa r + O(\log r), \qquad \kappa = \log_2(3 + 2\sqrt{2}).$$

Consequently, for every fixed $\epsilon > 0$,

$$r > (c_0 + \epsilon)D^2L^2, \qquad c_0 = \frac{1}{3\kappa^2} = 0.051540616989\ldots,$$

implies (8) for sufficiently large r. A simpler sufficient condition valid for odd $r \geq 7$ is $r \geq D^2L^2$.

Proof. In (7), retain the term with $j = \lfloor (1 - 1/\sqrt{2})r \rfloor$. Stirling's formula for its three binomial coefficients gives $\log_2 B_r \geq \kappa r - O(\log r)$. For the upper bound, set $t = \sqrt{2} - 1$. The generating function for one signed exponent, recording positive and negative weights separately, is $1 + z/(1 - z) + w/(1 - w)$. Every vector counted by B_r has combined weight at most $2h$, so

$$B_r t^{2h} \leq \left(1 + \frac{2t}{1-t}\right)^r = t^{-r}.$$

Since $2h = r - 1$, this has the asserted exponential rate. The asymptotic threshold follows on substituting this estimate in (8). For the simpler bound, the count includes all nonnegative 0–1 vectors of weight at most h and their negatives, with zero counted once. Their number is $2^r - 1$. Hence $\lfloor \log_2 B_r \rfloor \geq r - 1$, and $3(r-1)^2 \geq r^2 \geq D^2L^2r$ for the stated range. □

To meet the size condition with small D, we build r from primes q for which $q - 1 \mid D$. The following parameter theorem is due to Odlyzko and Pomerance; we use the form in Adleman–Pomerance–Rumely [1, Theorem 3], also used by Bernstein [4]. There is an absolute constant C such that, for every sufficiently large H, some positive integer D satisfies

$$D \leq \exp(C \log\log H \log\log\log H), \qquad \prod_{\substack{q-1 \mid D \\ q \text{ prime}}} q \geq H. \tag{11}$$

Proposition 3.2. *There is a deterministic search for D and odd squarefree $r > 2$ satisfying $\gcd(D, r) = 1$, $q - 1 \mid D$ for every prime $q \mid r$, and (8), with*

$$D = L^{o(1)}, \qquad r = L^{2+o(1)}, \qquad q \leq D + 1 = L^{o(1)} \quad (q \mid r). \tag{12}$$

Its cost is at most $L^{4+o(1)}$ bit operations.

Proof. Enumerate even positive integers D. For each, enumerate the primes $q \leq D+1$ with $q-1 \mid D$ and $q \nmid D$. Multiply these primes in increasing order, checking (8) after each prefix whose product exceeds 2. If all primes are exhausted without success, continue to the next D.

To bound the search, apply (11) with $H = L^3$. The supplied D is $L^{o(1)}$. Deleting the primes dividing D removes a product at most D, so the remaining product is at least $H/D \geq D^2L^2$ for sufficiently large L. Such a successful D is even: if D were odd, the product in (11) would contain only the prime 2. For even D, excluding $q \mid D$ also excludes 2. Proposition 3.1 now guarantees success. For each fixed smaller L, applying (11) with H sufficiently large gives the same termination argument.

At the first successful prefix the product obeys

$$r \le (D+1)\max\{6, D^2L^2\} = L^{2+o(1)}.$$

Conversely, Proposition 3.1's upper estimate and (8) give $r \gg D^2L^2$, establishing the stated asymptotic scale. Each trial has $L^{o(1)}$ small primes and divisibility checks. The exact count B_r can be evaluated from binomial recurrences in $\widetilde{O}(r^2)$ bit operations: there are $O(r)$ terms, each with $O(r)$ bits. The $L^{o(1)}$ trials fit the claimed bound. □

The factorization of r is known from its construction. To enforce $\gcd(n, r) = 1$, test its known prime factors against n. A common prime factor proves compositeness unless it equals n, in which case n is prime.

4 A uniform auxiliary-prime bound

For each prime $q \mid r$, we seek a prime ℓ modulo which n is a qth power nonresidue. Such a prime will define the character used in Section 5. We prove its existence for prime inputs by applying Theorem 1.1 to Kummer extensions of degree q. The following smoothed estimate makes the dependence on the number field explicit.

Lemma 4.1 (Smoothed prime-ideal estimate)**.** *Fix a nonzero nonnegative smooth function w supported in $(1, 2)$. Let F be a number field of degree d_F and absolute discriminant Δ_F, and suppose its Dedekind zeta function has no zeros in $\Re s > 1 - \delta$. Put*

$$\Psi_F(x) = \sum_{\mathfrak{p}} \sum_{a \ge 1} \log N\mathfrak{p}\; w((N\mathfrak{p})^a/x).$$

Then, uniformly in F and $x \ge 2$,

$$\Psi_F(x) = x\widehat{w}(1) + O_w(x^{1-\delta}(\log \Delta_F + d_F)), \qquad \widehat{w}(s) = \int_0^\infty w(u)u^{s-1}\,du. \tag{13}$$

The implied constant is effective.

Proof. This is the smoothed explicit-formula calculation in [11, Section 9.2, especially (9.9)]; we recall the dependence on the field. Mellin inversion applied to $-\zeta_F'/\zeta_F$ and a contour shift from $\Re s = 2$ to $\Re s = -1/2$ give

$$\Psi_F(x) = x\widehat{w}(1) - \sum_{\rho} x^\rho \widehat{w}(\rho) - (r_1 + r_2 - 1)\widehat{w}(0) + O_w(x^{-1/2}(\log \Delta_F + d_F)),$$

where ρ runs over nontrivial zeros with multiplicity and (r_1, r_2) is the signature. The functional equation bounds the integral on the left line with the displayed dependence. The uniform zero count in a unit interval at height T is $O(\log \Delta_F + d_F \log(2 + |T|))$. The Mellin transform decays faster than every inverse power of $|T|$ in bounded vertical strips. Since $\Re\rho \le 1 - \delta$, the zero sum is absolutely convergent and is bounded by $O_w(x^{1-\delta}(\log \Delta_F + d_F))$. The residue at zero and the left-line integral are absorbed in the same bound. These estimates have effective absolute constants for fixed w. □

Lemma 4.2 (Auxiliary prime for one prime degree)**.** *There is an effective constant C_δ such that, for every prime $n > 3$ and every odd prime $q \ne n$, there is a prime ℓ satisfying*

$$\ell \le C_\delta\big(q(L + \log q + 2)\big)^{1/\delta}, \tag{14}$$

$$\ell \equiv 1 \pmod{12q}, \qquad \ell \nmid n, \qquad n^{(\ell-1)/q} \not\equiv 1 \pmod{\ell}. \tag{15}$$

Proof. Set $K = \mathbb{Q}(\mu_{12q})$ and $M = K(n^{1/q})$. The prime n is unramified in K, so $X^q - n$ is Eisenstein at a prime of K above n. Thus $[M : K] = q$, and M/K is cyclic because $\mu_q \subset K$. Theorem 1.1 gives the same zero-free half-plane $\Re s > 1 - \delta$ for both ζ_K and ζ_M, with $\delta = 1/32$.

The cyclotomic discriminant bound and the discriminant of $X^q - n$ give

$$\begin{aligned} [K : \mathbb{Q}] &= O(q), & \log \Delta_K &= O(q \log q), \\ [M : \mathbb{Q}] &= O(q^2), & \log \Delta_M &= O(q^2(L + \log q)). \end{aligned}$$

More explicitly, the relative discriminant divides $(q^q n^{q-1})\mathcal{O}_K$, and the discriminant tower formula gives the second bound. Lemma 4.1 therefore yields

$$\Psi_K(x) - \frac{1}{q}\Psi_M(x) = \left(1 - \frac{1}{q}\right) x\widehat{w}(1) + O_w(q(L + \log q + 2)x^{1-\delta}). \tag{16}$$

Consider an unramified degree-one prime of K. If it splits in M, its first-power contribution cancels against the contributions of the q primes above it, after the factor $1/q$. Otherwise it is inert, since the extension has prime degree, and its positive first-power contribution remains. A surviving prime lies above a rational prime $\ell \equiv 1 \pmod{12q}$ for which n is not a qth power in $\mathbb{F}_\ell^\times$. This is exactly the last condition in (15).

All terms of prime-ideal residue degree at least two, and all higher prime powers, contribute in absolute value at most $O_w(q\sqrt{x}\log^2(2x))$ to (16). To see the field dependence, a field of degree d contributes at most $O_w(d\sqrt{x}\log^2(2x))$; the weighted total degree here is $[K : \mathbb{Q}] + [M : \mathbb{Q}]/q = O(q)$. Ramified degree-one first powers contribute at most $O_w(q \log(6qn))$, since the ramified rational primes divide $6qn$.

Take $x = T_\delta(q(L + \log q + 2))^{1/\delta}$. For an effectively large constant T_δ, the error in (16) is less than half its main term. The discarded terms are smaller as well, uniformly in q and n, because $\delta < 1/2$. Some surviving prime lies in $(x, 2x)$. Absorbing $2T_\delta$ in C_δ proves the lemma. □

All primes $q \mid r$ are at most $D + 1$. Hence a common search bound, increased by rounding if needed, is

$$B = \left\lceil C_\delta((D+1)(L + \lceil \log_2(D+1) \rceil + 3))^{1/\delta} \right\rceil = L^{1/\delta + o(1)} = L^{32 + o(1)}. \tag{17}$$

For the search itself it suffices to test primes $\ell \equiv 1 \pmod{q}$; Lemma 4.2 supplies a prime even in the smaller progression. Only prime-input existence is needed. If a search fails within the bound, the algorithm rejects.

5 Constructing the normalized coefficient

5.1 Characters defined by the input

For each prime $q \mid r$, choose a prime $\ell_q \le B$ with $q \mid \ell_q - 1$, $\ell_q \nmid n$, and $n^{(\ell_q - 1)/q} \not\equiv 1 \pmod{\ell_q}$. Put

$$t_q = n^{(\ell_q - 1)/q} \bmod \ell_q.$$

Its order in $\mathbb{F}_{\ell_q}^\times$ is exactly q. For $u \neq 0$ define $j_q(u) \in \{0, \dots, q-1\}$ by

$$u^{(\ell_q - 1)/q} = t_q^{j_q(u)} \pmod{\ell_q}.$$

This is a multiplicative-group homomorphism to $\mathbb{Z}/q\mathbb{Z}$, written additively, and $j_q(n \bmod \ell_q) = 1$. Its values are computed by a table of the q powers of t_q.

Choose $s_q \in \{1, \dots, q-1\}$ satisfying

$$s_q \equiv -\big(D(r/q)\big)^{-1} \pmod{q}. \tag{18}$$

The inverse exists by (6) and squarefreeness. In $R_q = (\mathbb{Z}/n\mathbb{Z})[Z]/(\Phi_q(Z))$, define the order-$q$ character

$$\chi_q(u) = Z^{s_q j_q(u)} \quad (u \neq 0), \qquad \chi_q(0) = 0. \tag{19}$$

In particular, $\chi_q(n) = Z^{s_q}$ and $\chi_q(-1) = 1$, since q is odd. This construction needs neither a primitive root modulo ℓ_q nor a factorization of $\ell_q - 1$.

5.2 Jacobi sums and a binary recurrence

For positive integers a, c, set

$$J(\chi^a, \chi^c) = \sum_{u \in \mathbb{F}_\ell} \chi(u)^a \chi(1-u)^c.$$

Here $\chi = \chi_q$ and $\ell = \ell_q$. The terms for $u = 0, 1$ vanish. The other terms are powers of Z, so the sum is computed by counting q possible exponents before reduction modulo $(n, \Phi_q(Z))$. Define

$$\beta_q(Z) = \ell_q \prod_{j=1}^{q-2} J(\chi_q, \chi_q^j) \quad \text{in } R_q. \tag{20}$$

Lemma 5.1. *The element β_q is the qth power of its Gauss sum in a cyclotomic extension of R_q. It can be computed in R_q using only $O(\log q)$ Jacobi sums, without constructing that extension.*

Proof. For this proof only, work in $R_q[T]/(\Phi_\ell(T))$ and put $\tau_a = \sum_{u \neq 0} \chi(u)^a T^u$. The integral Gauss–Jacobi identities give

$$\tau_a \tau_c = J(\chi^a, \chi^c)\tau_{a+c} \qquad (a, c, a+c \not\equiv 0 \pmod{q}), \tag{21}$$

$$\tau_1 \tau_{q-1} = \ell. \tag{22}$$

These follow by grouping the two summation indices according to their sum; the zero-sum terms vanish in (21) because the product character is nontrivial. They are identities in integral cyclotomic rings and remain valid after reduction modulo n; see also [8, Theorem 2.4]. Iteration gives $\tau_1^q = \beta_q$.

For a shorter computation, maintain $a < q$ and $A \in R_q$ with $\tau_1^a = A\tau_a$, starting at $a = 1, A = 1$. Follow the binary expansion of $q - 1$ after its leading bit. On a doubling, set

$$A \longleftarrow A^2 J(\chi^a, \chi^a), \qquad a \longleftarrow 2a.$$

If the next bit is 1, then set

$$A \longleftarrow A J(\chi^a, \chi), \qquad a \longleftarrow a + 1.$$

Every resulting index is at most $q - 1$, so no step uses a trivial product character. At the end, $\tau_1^{q-1} = A\tau_{q-1}$; multiplying by τ_1 gives $\beta_q = \ell A$. The coefficient ring embeds in the displayed extension, since its defining polynomial is monic, so this is an identity in R_q. There are $O(\log q)$ steps and no divisions. □

5.3 Combining the prime degrees

Substitution $Z \mapsto Y^{r/q}$ defines a homomorphism $R_q \to C_n$: the polynomial $\Phi_q(Y^{r/q})$ is divisible by $\Phi_r(Y)$ over $\mathbb{Z}$. Form

$$b(Y) = \prod_{q|r} \beta_q(Y^{r/q})^{r/q} \quad \text{in } C_n. \tag{23}$$

Each computation in Z takes place in a ring of rank $q-1$; the substitution combines its result with the other prime degrees in the common coefficient ring C_n.

Proposition 5.2 (Completeness on prime inputs)**.** *If n is prime, the construction (23) satisfies all three equalities (3)–(5).*

Proof. Put $N = n^D$. In R_q, Nth powering fixes every coefficient, because $n^D \equiv 1 \pmod q$ and the scalar field is $\mathbb{F}_n$. For the Gauss sum from Lemma 5.1, Frobenius and reindexing give

$$\tau_1^N = \sum_{u \neq 0} \chi_q(u) T^{uN} = \chi_q(N)^{-1} \tau_1 = Z^{-Ds_q} \tau_1.$$

The scalar ℓ_q is invertible modulo n, so (22) makes τ_1 a unit. Since $\beta_q = \tau_1^q$ and $q \mid N-1$, cancellation gives

$$\beta_q^{(N-1)/q} = Z^{-Ds_q}. \tag{24}$$

This identity holds in R_q, by its injection into the monic extension used in the proof. Substituting into (23),

$$b^{(N-1)/r} = Y^{-D\sum_{q|r} s_q(r/q)} = Y.$$

Indeed, modulo each prime $q \mid r$, all but its own summand vanish, and (18) makes the remaining exponent 1. The Chinese remainder theorem gives the exponent 1 modulo r. This proves (3). Finally, nth powering is Frobenius in every commutative algebra of characteristic the prime n. It gives $b(Y)^n = b(Y^n)$ and $(1+X)^n = 1 + X^n$, proving the other two equalities. □

6 The algorithm and its bit complexity

Here is the complete algorithm, with $\delta = 1/32$ and an effective constant C_δ from Lemma 4.2 fixed in advance. One may take C_δ to be an integer, so the search bound (17) is computed by integer powering.

1. Reject integers below 2; accept 2 and 3; reject even inputs greater than 2. Reject nontrivial perfect powers.
2. Construct D, r as in Proposition 3.2. For every prime $q \mid r$, if $q \mid n$, accept when $q = n$ and otherwise reject. Construct $\Phi_r(Y)$ modulo n.
3. Sieve the primes up to B in (17). A prime in the sieve dividing n permits the same immediate decision. For every $q \mid r$, select a prime $\ell_q \leq B$ with $q \mid \ell_q - 1$ and $n^{(\ell_q-1)/q} \not\equiv 1 \pmod{\ell_q}$. Reject if any such search fails.
4. Compute the tables j_q, the residues s_q, and the Jacobi-sum coefficients β_q using the binary recurrence. Form b by (23).
5. Check (3), (4), and (5). Accept if and only if all three hold.

Proof of Theorem 1.2. If the input is prime, preprocessing cannot reject it. Lemma 4.2, using Theorem 1.1, ensures all searches succeed, and Proposition 5.2 proves acceptance. A composite input accepted at the last step would be a prime power by Theorem 2.3, contrary to the preprocessing. The earlier acceptance branches identify the input with a known prime. This proves correctness on every input.

We give the cost bounds in some detail, including the construction of the coefficient. The degree search costs $L^{4+o(1)}$ by Proposition 3.2. Elementary integer-root methods for exponents up to L detect nontrivial perfect powers within $L^{4+o(1)}$ as well.

The sieve up to B uses $\widetilde{O}(B)$ bit operations. Compute n modulo all its primes with a product tree and a remainder tree [5]. The total bit length S of these moduli is at most $O(B \log B)$. With fast multiplication and division, the trees cost $\widetilde{O}(S + L) = \widetilde{O}(B + L)$: at every tree level the node lengths sum to $O(S)$, and there are $O(\log B)$ levels. This avoids an extra factor L from reducing n separately for each candidate.

Each small-prime modular exponentiation costs a polynomial in $\log B$. There are $O(\log r)$ primes $q \mid r$, all of size $L^{o(1)}$. Testing the candidates for all q consequently costs $L^{1/\delta+o(1)}$ in total. The character tables $j_q(u)$ are computed by modular exponentiation and lookup among q possibilities. Each needed Jacobi sum is accumulated by scanning $u = 2, \dots, \ell_q - 1$ and counting its exponent modulo q. These counts have $O(\log \ell_q)$ bits; the scan does not require an L-bit modular addition for each term. All scans, including the $O(\log q)$ sums for each q, therefore fit the same $L^{1/\delta+o(1)}$ bound. Arithmetic in the local rings of rank $q - 1 = L^{o(1)}$, after reduction of the counts, costs at most $L^{2+o(1)}$ over all q.

Put $m = \varphi(r) \le r = L^{2+o(1)}$. Fast polynomial multiplication and monic reduction give multiplication costs

$$\widetilde{O}(mL) \quad \text{in } C_n, \qquad \widetilde{O}(mrL) \quad \text{in } \mathcal{A}_n.$$

These bounds apply over $\mathbb{Z}/n\mathbb{Z}$ without assuming it is a field. For the second, polynomial multiplication in X over C_n, followed by $X^r = b$, gives the stated bound; equivalently one may use bivariate Kronecker substitution and monic reductions. Forming (23) costs $L^{3+o(1)}$. The coefficient checks cost $L^{4+o(1)}$, because the exponents have at most $O(DL)$ bits. Substitution $Y \mapsto Y^n$ is performed using $Y^r = 1$ followed by reduction modulo Φ_r.

The main congruence needs $O(L)$ multiplications in $\mathcal{A}_n$, for total cost

$$\widetilde{O}(mrL^2) = L^{6+o(1)}.$$

Finally, Φ_r is constructible by exact monic divisions from the polynomials $Y^d - 1$ for the known divisors $d \mid r$. There are $r^{o(1)}$ such divisors. Even classical polynomial division with elementary L-bit coefficient arithmetic costs at most $r^{2+o(1)}L^2 = L^{6+o(1)}$. This also shows that no polynomial-factorization subroutine is hidden in the construction. Combining the bounds gives

$$L^{\max\{6,1/\delta\}+o(1)} = L^{32+o(1)},$$

which proves the theorem. □

The auxiliary-prime search determines the exponent in the total bound. More generally, a uniform zero-free width δ gives $L^{\max\{6,1/\delta\}+o(1)}$ by the same analysis. OpenAI's width 10^{-6} yields a polynomial bound after abelian zeta factorization; Theorem 1.1 gives the exponent $32 + o(1)$ stated here. The algebraic verification remains $L^{6+o(1)}$, independently of the zero-free width. The construction does not factor $n - 1$, $n^D - 1$, or any $\ell_q - 1$.

Remark 6.1 (A two-equality form). If retaining the exponent n is unnecessary, one may replace (4) and (5) by

$$(1+X)^{n^D} = 1 + YX \quad \text{in } \mathcal{A}_n.$$

Together with (3), this gives the rotation used in Theorem 2.3 directly. Prime inputs satisfy it, and the same proof applies. Its asymptotic verification bound is unchanged because $D = L^{o(1)}$, although its exponent is longer.

7 A fixed-base conjecture

The coefficient $b(Y)$ in the proved construction enforces the normalization needed for the cyclic rotation. A simpler possibility is to fix the coefficient at 2 and choose the degree directly from the input. The following conjecture proposes such a test.

Agrawal's conjecture, as recorded in [2, Conjecture 6.1], asserts that if r is prime, $r \nmid n$, and

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

then n is prime or $n^2 \equiv 1 \pmod{r}$. The conjecture below is a modification of that proposal: it uses roots of 2 in place of roots of unity, the shift $+1$, and the least nondivisor of $n(n-1)$ as the degree. The two conjectures are not asserted to be equivalent.

Conjecture 7.1 (Fixed-base test)**.** *Let $n > 3$ be odd, and let r be the least positive integer not dividing $n(n-1)$. If*

$$(1+X)^n \equiv 1 + X^n \pmod{n, X^r - 2}, \tag{25}$$

then n is prime.

The degree r need not be prime. It is necessarily a prime power: otherwise it would be the least common multiple of its proper prime-power factors, each of which divides $n(n-1)$ by minimality.

Proposition 7.2 (Consequence of the fixed-base conjecture)**.** *If Conjecture 7.1 holds, its test is a deterministic primality algorithm using $\widetilde{O}(L^3)$ bit operations.*

Proof. Handle inputs at most 3 and even inputs directly. By the choice of r,

$$\operatorname{lcm}(1, \ldots, r-1) \mid n(n-1).$$

Chebyshev's estimate $\log \operatorname{lcm}(1, \ldots, m) = \Theta(m)$ therefore gives $r = O(\log n) = O(L)$. Testing consecutive integers for divisibility finds r within the claimed bound. Primes pass (25) by Frobenius, and the conjecture excludes composites. Multiplication in $(\mathbb{Z}/n\mathbb{Z})[X]/(X^r - 2)$ costs $\widetilde{O}(rL)$, and binary powering uses $O(L)$ multiplications, for total $\widetilde{O}(L^3)$. □

The open step is to obtain a comparable restriction on composite inputs from the fixed coefficient 2 and this degree rule. The normalization and cyclic rotation used in Theorem 2.3 are supplied by our coefficient construction; they have not been deduced from the congruence in Conjecture 7.1.

AI Assistance Disclosure

OpenAI's GPT-6 Astra developed and wrote the proofs, including the deterministic parameter construction and complexity analysis, through an extended mathematical dialogue with the author. The author supplied the fixed-base test, conjectural framework, research notes, and references; proposed applying OpenAI's recent analytic number-theoretic results to deterministic parameter selection; and directed the investigation of power nonresidues, composite degrees, multivariate quotient rings, and finite-field root counting.

References

[1] L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Annals of Mathematics **117** (1983), 173–206. Theorem 3 records the Odlyzko–Pomerance parameter construction. https://math.dartmouth.edu/~carlp/PDF/paper37.pdf.

[2] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Annals of Mathematics **160** (2004), 781–793. doi:10.4007/annals.2004.160.781. Agrawal's conjecture is stated in Section 6; see also the authors' version at https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf.

[3] Axiom Math, D. Cureton, and J. Thorner, *Dedekind Zeta Zero-Free Region*, Lean 4 formalization, October 2026. The declaration `DedekindZetaZeroFree.main` in `Solution/DedekindZetaSolution.lean` proves the Dedekind-zeta statement; the repository reports verification using only Lean's standard axioms. https://github.com/AxiomMath/DedekindZetaZeroFree.

[4] D. J. Bernstein, *Proving primality in essentially quartic random time*, Mathematics of Computation **76** (2007), 389–403. doi:10.1090/S0025-5718-06-01786-8. Section references are to the December 3, 2004 draft: https://cr.yp.to/papers/quartic-20041203.pdf.

[5] D. J. Bernstein, N. Heninger, and T. Lange, *FactHacks: Remainder tree*. https://facthacks.cr.yp.to/remainder.html.

[6] P. Berrizbeitia, *Sharpening "PRIMES is in P" for a large family of numbers*, Mathematics of Computation **74** (2005), 2043–2059. doi:10.1090/S0025-5718-05-01727-8.

[7] Q. Cheng, *Primality proving via one round in ECPP and one iteration in AKS*, preprint, 2003. https://arxiv.org/abs/math/0301179.

[8] K. Conrad, *Gauss and Jacobi sums on finite fields and $\mathbb{Z}/m\mathbb{Z}$*, expository notes. https://kconrad.math.uconn.edu/blurbs/gradnumthy/Gauss-Jacobi-sums.pdf.

[9] D. Cureton and J. Thorner, *A quasi-Riemann hypothesis for Dedekind zeta functions*, Hexagon preprint 2610.00200, version 2, October 12, 2026. Theorem 1.1 and Section 15. https://hexagonmath.org/2610.00200v2.

[10] H. W. Lenstra, Jr., and C. Pomerance, *Primality testing with Gaussian periods*, Journal of the European Mathematical Society **21** (2019), 1229–1269. doi:10.4171/JEMS/861.

[11] OpenAI, *Primitive roots for every admissible integer base*, preprint, October 4, 2026. Theorem 1.2 and Section 9. https://github.com/openai/math/blob/main/preprints/Primitive-roots-for-every-admissible-integer-base-October-4-2026/primitive-roots-all-integer-bases.pdf.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il