Deterministic Polynomial-Time Factorization over Finite Fields

Qiyue Tang

November 6, 2026

Abstract

Using prime-field factorization and a Dedekind zeta zero-free theorem, we obtain deterministic polynomial-time algorithms for complete factorization over finite fields and for constructing their presentations from their orders.

hexagon:2611.00135v2

1 Introduction

Let p be a prime, let $m \geq 1$, and put $q = p^m$. Write $\mathbb{F}_q$ for a field of order q and $\mathbb{F}_p$ for its prime field. Factoring a nonzero polynomial in the indeterminate X over $\mathbb{F}_q$ means finding its leading coefficient and its distinct monic irreducible factors with their multiplicities. The deterministic complexity problem asks for a single algorithm whose number of bit operations is polynomial in the degree and $\log_2 q$, as both vary. Even a polynomial known to split into distinct linear factors poses the problem of finding its roots without testing all field elements.

Berlekamp's 1967 algorithm [1] distinguishes irreducible factors by linear algebra in the quotient by the input polynomial. For a square-free input g, the quotient $\mathbb{F}_q[X]/(g)$ is a product of fields, one for each irreducible factor. The elements fixed by $z \mapsto z^q$ have coordinates in $\mathbb{F}_q$. A fixed element whose coordinates differ separates the factors by greatest common divisors. Enumerating the possible coordinate values costs up to q trials. In 1970 [2, Sections 3–7], Berlekamp reduced factorization over extension fields to root finding over the prime field, using trace and norm constructions to reach split polynomials. He identified deterministic root finding over large prime fields as the remaining difficulty.

Cantor and Zassenhaus [3] used random choices to split products of irreducibles of equal degree. This gives complete factorization in expected polynomial time. In the deterministic setting, Shoup [12] obtained a bound with a square-root dependence on the characteristic, up to smaller factors, and Evdokimov [5] obtained quasipolynomial time under the generalized Riemann hypothesis. A separate problem is to construct the field in which the coefficients are represented. Shoup [11, Theorem 3.1] reduced construction of irreducible polynomials to prime-field factorization, and Lenstra [6, Sections 2 and 7–9] developed deterministic constructions and isomorphisms for explicitly represented finite fields.

OpenAI's prime-field preprint [8] separates the algebraic algorithm from the task of finding auxiliary primes. Its Theorem 1.2 gives a deterministic algorithm with a cost polynomial in the input length and the *values* of the auxiliary primes. Its Theorem 1.1 obtains a uniform polynomial bound by invoking a Hecke zero-free theorem. Cureton and Thorner [4, Theorem 1.1] give a fixed zero-free half-plane for Dedekind zeta functions of arbitrary number fields.

Keywords. Finite fields, polynomial factorization, Frobenius, auxiliary primes.
MSC 2020. Primary 11T06. Secondary 68W30.

Shunia [13, Lemma 4.2] uses this theorem and a weighted difference of prime-ideal sums to find auxiliary primes for odd prime degrees in a primality test. A different approach, due to Spaenlehauer [14], reduces root finding to computations on an elliptic curve and its quadratic twist, with an online bound depending on the group orders of the supplied curve data.

Here we use the Dedekind zeta theorem to construct the full auxiliary table for the prime-field algorithm, including its entry of degree two. We give the extension-field reduction by taking the fixed space of $z \mapsto z^p$ directly. This makes the degree and number of prime-field queries explicit. The same prime-field algorithm supplies the queries in the construction of a field presentation.

An explicit presentation is a quotient $\mathbb{F}_p[U]/(h)$ in an indeterminate U with h monic irreducible of degree m. A field element is encoded by the m coefficients of its representative of degree less than m, with each coefficient represented in binary by its residue in $\{0, \dots, p-1\}$. A dense polynomial of degree n is encoded by its $n+1$ coefficients. A nonzero constant has an empty factor list.

Theorem 1.1. *There is a uniform deterministic algorithm for complete factorization of every nonzero dense polynomial over an explicitly presented finite field of order q. For degree n the bit cost is polynomial in $n+1$ and $\log_2 q$. Given the binary integer q promised to be a prime power, the algorithm can first construct a presentation in time polynomial in $\log_2 q$. In this case the polynomial is then supplied in the resulting power basis.*

Remark 1.2. The external inputs to Theorem 1.1 are the Dedekind zeta zero-free theorem of Cureton and Thorner [4, Theorem 1.1] and the auxiliary-prime factorization theorem, bit bound, and smoothed prime-ideal estimate of OpenAI [8, Theorem 1.2, Proposition 10.1, and Lemma 11.2].

Remark 1.3. The author of the present paper used Rethlas–OSV [10, 7] to review the following manuscripts in sequence. The first review, of OpenAI's *Deterministic Polynomial Factorization over Prime Fields* [8], reported no mathematical issues. The review of Cureton and Thorner's Dedekind zeta paper [4] identified gaps in the written proof. Rethlas–OSV supplied a revised manuscript with supplementary arguments. The revision passed a second Rethlas–OSV review, which reported no mathematical issues in the material reviewed. Unable to reach the authors, the author posted the review reports and the consolidated revision on GitHub. The subsequent reviews of OpenAI's companion paper on primitive roots [9] and of the present paper reported no mathematical issues in the material reviewed.

2 Auxiliary primes and the prime-field algorithm

For a prime-field input of degree n, put

$$B = 20 + (n+1)(\lceil \log_2 p \rceil + 1).$$

For $n \geq 2$ and $p > B^{200000}$, the algorithm of [8, Theorem 1.2] requires, for every prime $r \leq n$, a rational prime ℓ satisfying

$$\ell \notin \{2, 3, p, r\}, \qquad \ell \equiv 1 \pmod{12r}, \qquad p^{(\ell-1)/r} \not\equiv 1 \pmod{\ell}. \tag{1}$$

For the remaining inputs the table is empty. If E is the maximum of 2 and the supplied primes, the bit cost, including upward search for the primes, is $O(B^{500000} + B^{100}E^{20})$ by [8, Proposition 10.1].

Lemma 2.1. *For $n \geq 2$, $p > \max(n, 3)$, and each prime $r \leq n$, there is a prime satisfying (1) with $\ell = O(B^{32})$, uniformly in p, n, r.*

Proof. Write $K = \mathbb{Q}(\mu_{12r})$, with μ_{12r} the group of complex $(12r)$th roots of unity, and put $M = K(p^{1/r})$ using the positive real root. Since $p \nmid 12r$, it is unramified in K. The valuation normalized to give a uniformizer value one at any prime of K over p therefore gives p value one. Hence $X^r - p$ is Eisenstein at that prime. Its roots are obtained by multiplying $p^{1/r}$ by the rth roots of unity, all of which lie in K, so M/K is cyclic of degree r.

For a number field F, let $d_F = [F : \mathbb{Q}]$ and let D_F be its absolute discriminant. Write log for the natural logarithm. The cyclotomic degree satisfies $d_K \le 4r$, since among the integers up to $12r$ at most $4r$ are prime to 6. Let Φ_{12r} be the monic polynomial whose roots are the primitive $(12r)$th roots of unity. Write $X^{12r} - 1 = \Phi_{12r}(X)H(X)$, where H is the monic cofactor in $\mathbb{Z}[X]$. At every primitive root ζ, differentiation gives

$$12r\,\zeta^{12r-1} = \Phi'_{12r}(\zeta)H(\zeta).$$

The product of the left sides is $\pm(12r)^{d_K}$. The product of the cofactor values is the field norm of an algebraic integer, hence an integer. The product of the derivatives is the polynomial discriminant up to sign. It follows that this discriminant divides $(12r)^{d_K}$. The field discriminant divides the polynomial discriminant, giving $\log D_K \le d_K \log(12r)$. For $X^r - p$, the product of rX^{r-1} over the roots is $r^r p^{r-1}$ up to sign. Thus the relative discriminant of M/K divides the ideal generated by $r^r p^{r-1}$. The discriminant formula in the tower therefore gives

$$\log D_M \le r \log D_K + d_K\big(r \log r + (r-1)\log p\big).$$

Since $d_M = r d_K$, the weighted sum satisfies

$$\begin{aligned}(\log D_K + d_K) + r^{-1}(\log D_M + d_M) &\le d_K\big(2\log(12r) + 2 + \log r + (1 - 1/r)\log p\big)\\ &= O(r(1 + \log p)) = O(B),\end{aligned}$$

using $r \le n$ and $r < p$.

Fix a smooth, nonnegative, nonzero real function w compactly supported in $(1, 2)$. For real $x \ge 2$, define

$$\Psi_F(x) = \sum_{\mathfrak{p}} \sum_{j \ge 1} \log N\mathfrak{p}\, w((N\mathfrak{p})^j/x), \qquad c = \int_1^2 w(t)\,dt,$$

where $\mathfrak{p}$ runs over the nonzero prime ideals of the ring of integers $\mathcal{O}_F$ and $N\mathfrak{p} = |\mathcal{O}_F/\mathfrak{p}|$. Here $c > 0$. By [4, Theorem 1.1], each nontrivial zero ρ of the Dedekind zeta function of F satisfies $\operatorname{Re}\rho \le 31/32$. In the smoothed explicit formula of [8, Lemma 11.2], each zero contributes $-x^\rho \int_1^2 w(t)t^{\rho-1}\,dt$. The sum of the absolute values of the integrals, over the zeros with multiplicity, is $O_w(\log D_F + d_F)$, and the remainder apart from the pole term cx has this same bound. Hence $\Psi_F(x) - cx = O_w(x^{31/32}(\log D_F + d_F))$, with constants depending only on w. Applying it to both fields and retaining the weight $1/r$ gives

$$\Psi_K(x) - r^{-1}\Psi_M(x) = (1 - r^{-1})cx + O_w(Bx^{31/32}).$$

Suppose there is no prime satisfying (1) in $(x, 2x)$. A term in $\Psi_K(x)$ with $j = 1$ and residue degree one over a rational prime $\ell \notin \{2, 3, p, r\}$ has $x < \ell < 2x$. The Frobenius at ℓ acts on μ_{12r} by raising to the ℓth power. Residue degree one makes this automorphism the identity, so $\ell \equiv 1 \pmod{12r}$. By the supposition, $p^{(\ell-1)/r} = 1$ in $\mathbb{F}_\ell$. This is the criterion for being an rth power in the cyclic group $\mathbb{F}_\ell^\times$ of order $\ell - 1$. Then $X^r - p$ has r distinct roots in $\mathbb{F}_\ell$, so the corresponding prime of K splits completely in M. Here ℓ is prime to the power-basis discriminant, so reduction

of the polynomial determines the splitting. The r primes of M above this prime each have norm ℓ. Their terms, with weight $-1/r$, sum to the negative of the term from K.

The terms left in $\Psi_M(x)$ enter with a negative sign. A remaining term from K with j times residue degree at least two lies over a rational prime at most $\sqrt{2x}$. There are at most $\sqrt{2x}$ such rational primes and at most d_K prime ideals above each. Since $(N\mathfrak{p})^j < 2x$ on the support of a summand, the number of eligible j is at most $\log(2x)/\log N\mathfrak{p}$. Thus each ideal contributes at most $\|w\|_\infty \log(2x)$, where $\|w\|_\infty$ is the maximum of w. Terms with $j = 1$ and residue degree one over the four exceptional primes contribute at most $4d_K\|w\|_\infty \log(2x)$. Consequently

$$\Psi_K(x) - r^{-1}\Psi_M(x) \le C_w r\sqrt{x}\log(2x),$$

where C_w depends only on w. Set $x = TB^{32}$ with a fixed $T \ge 2$. After division by x, the explicit-formula error is $O_w(T^{-1/32})$. Since $r \le B$, dividing $C_w r\sqrt{x}\log(2x)$ by x gives a bound of order $T^{-1/2}(1 + \log T)$, uniformly in B. Indeed, $B/\sqrt{x} = T^{-1/2}B^{-15}$, and $\log(2x) = \log(2T) + 32\log B$. Both B^{-15} and $B^{-15}\log B$ are at most one. Choose T so the divided error and the divided upper bound are each less than $c/4$. The main term divided by x is at least $c/2$, a contradiction. The prime obtained is less than $2TB^{32}$. □

In the branch $n \ge 2$ and $p > B^{200000}$ we have $p > \max(n, 3)$. Enumerate the primes $r \le n$ by trial division. For each r, test successive integers for primality and check (1) by modular exponentiation until a prime is found. Lemma 2.1 gives $E = O(B^{32})$. The search bound need not be supplied to the algorithm. Substitution in the cited bit bound gives $O(B^{500000})$, since $100 + 20 \cdot 32 = 740$. In the empty-table branch the same bound follows with $E = 2$.

3 Reduction by absolute Frobenius

Proposition 3.1. *For a nonzero input of degree n over an explicitly presented field of order $q = p^m$, complete factorization reduces deterministically to at most $\max(0, n-1)$ prime-field factorizations of split square-free polynomials of degree at most n. The other bit operations are polynomial in $n + 1$ and $\log_2 q$.*

Proof. Record the leading coefficient and divide by it. For a constant, return the empty list. Consider a monic square-free polynomial $g \in \mathbb{F}_q[X]$ of positive degree. In $\mathbb{F}_q[X]/(g)$, the map $z \mapsto z^p - z$ is $\mathbb{F}_p$-linear by the binomial theorem and the equality $a^p = a$ for $a \in \mathbb{F}_p$. Its matrix is obtained by raising the residue classes of U^iX^j, for $0 \le i < m$ and $0 \le j < \deg g$, to the pth power modulo h and g and subtracting the original basis vectors. Gaussian elimination computes a basis of the kernel.

If g has s distinct irreducible factors, the Chinese remainder theorem identifies the quotient with a product of s finite fields. In each field the fixed elements are exactly its prime field, since $X^p - X$ has at most p roots and every element of $\mathbb{F}_p$ is a root. Thus the fixed space has dimension s over $\mathbb{F}_p$. If $s = 1$, return g. Otherwise choose a basis vector b of the fixed space outside $\mathbb{F}_p \cdot 1$. Compute the successive powers $1, b, b^2, \ldots$ and test linear dependence over $\mathbb{F}_p$. The powers lie in the fixed space, so a dependence occurs by b^s. At the first dependent power, express it as a linear combination of the preceding powers and move the combination to the left. The resulting monic polynomial has least degree among those annihilating b. A polynomial annihilates b precisely when it vanishes at every coordinate of b. Thus the minimal polynomial is the product of $X - a$ over the distinct coordinate values $a \in \mathbb{F}_p$. Its degree is between 2 and $s \le \deg g$. Factor it over $\mathbb{F}_p$, and for each root a take the monic gcd of g and the degree-$<\deg g$ representative of b minus a. An irreducible factor of g divides this gcd exactly when the corresponding coordinate of b equals

a. As g is square-free, the gcds multiply to g and partition its irreducible factors into at least two nonempty groups. Recurse on the resulting factors of g.

For a general monic polynomial f of positive degree, let $g = f/\gcd(f, f')$, using the monic gcd and the formal derivative f'. For an irreducible factor u of exponent e in f, write $f = u^e v$ with $u \nmid v$. Then $f' = u^{e-1}(eu'v + uv')$. The field $\mathbb{F}_q[X]/(u)$ has $q^{\deg u}$ elements, so u divides $X^{q^{\deg u}} - X$, whose derivative is -1. Hence $u \nmid u'$. The exponent of u in $\gcd(f, f')$ is therefore $e-1$ if $p \nmid e$ and e otherwise. In particular g is square-free. Factor g by the square-free procedure if it is nonconstant. For each factor so obtained, recover its full multiplicity by repeated exact division and remove its full power. All remaining irreducible-factor multiplicities are divisible by p, so the remainder is a pth power. In characteristic p a pth power has only monomial exponents divisible by p. If the remainder is nonconstant, divide these exponents by p and raise each coefficient to p^{m-1}, the inverse of pth powering on $\mathbb{F}_q$ since $z^{p^m} = z$. Recurse and multiply the returned multiplicities by p. This also treats $f' = 0$ and terminates because each root step strictly lowers the degree.

Each square-free splitting tree has one query per internal vertex. If there are s leaves, the number of edges is the number of internal vertices plus $s-1$. Each internal vertex has at least two children, so there are at most $s-1$ internal vertices. The sets of irreducibles processed at different root steps are disjoint, and their total size is at most n. This gives the query count, including the constant case. Each root step lowers the degree by a factor of p, and every successful division lowers the current degree by at least one. There are at most n successful divisions in total and at most one failed division per factor whose multiplicity is recovered. Matrices have $O(mn)$ rows and columns. Multiplication and inversion in the coefficient field use polynomial multiplication and the extended Euclidean algorithm modulo h. Quotient multiplication, greatest common divisors, and Gaussian elimination have polynomial cost in n, m and the binary length of p. Binary powering uses a number of multiplications linear in the bit length of the exponent, at most $1 + m\lceil \log_2 p \rceil$ for the powers used here. Since $m \log_2 p = \log_2 q$, this gives the stated bit bound. □

4 Constructing the field presentation

Proposition 4.1. *Given a prime p and a positive integer m, an irreducible polynomial of degree m over $\mathbb{F}_p$ can be constructed using $O(m^2(1 + \log_2 p))$ calls to prime-field factorization of degree at most m and polynomial additional bit cost in m and $\log_2 p$.*

Proof. Return U for $m = 1$. For $m > 1$, factor the integer m by trial division. For each exact prime power r^a dividing m (so $r^a \mid m$ and $r^{a+1} \nmid m$), first construct a field containing the degree-r^a field over $\mathbb{F}_p$.

Odd $r \neq p$. Factor $1 + U + \cdots + U^{r-1}$ over $\mathbb{F}_p$, and use any one of its irreducible factors as the modulus of a field E. The residue class of U has rth power one by the geometric sum identity and is different from one because the sum takes value $r \neq 0$ at one. Its order in $E^\times$ is therefore r, and $[E : \mathbb{F}_p] \leq r - 1$. Write $v_r(N)$ for the exponent of r in a positive integer N. Put $t = v_r(|E| - 1)$, computed by division by r. Starting with the element of order r, repeatedly take an rth root in E until reaching an element c of order r^t. In the cyclic group $E^\times$, the image of rth powering contains the subgroup of order r^{t-1}. Thus an element of order r^j, for $1 \leq j < t$, has an rth root. If a root has order N, then $N/\gcd(N, r) = r^j$, which forces $N = r^{j+1}$. For the current element $b \in E$, apply Proposition 3.1 to $V^r - b$ in the already presented field E, with V an indeterminate. Choose the root of the first linear factor in a fixed order. If the initial element already has order r^t, the chain is empty.

If a root of $V^{r^a} - c$ has order N in an algebraic closure of E, its r^ath power has order $N/\gcd(N, r^a) = r^t$. Thus N is an r-power and, since $t \geq 1$, $N = r^{t+a}$. Its degree over E is

the least $e \geq 1$ such that r^{t+a} divides $|E|^e - 1$, by the criterion for membership in the field of order $|E|^e$. First raise $|E|$ to the factor of e prime to r. By the geometric sum formula, the difference from one is $|E| - 1$ times a sum congruent modulo r to the number of its summands, which is prime to r. Its valuation is therefore t. Then each raising to the rth power increases the valuation by one. Indeed, the binomial expansion of $u^r - 1$ in powers of $u - 1$ starts with $r(u-1)$. The terms of degrees 2 through $r-1$ have coefficients divisible by r. If $v_r(u-1) \geq 1$ and r is odd, the term $(u-1)^r$ also has valuation strictly greater than $1 + v_r(u-1)$. For $r = 2$ the same strict inequality holds when $v_2(u-1) \geq 2$. Thus $v_r(|E|^e - 1) = t + v_r(e)$, and the least degree is r^a. Thus the binomial is irreducible and its quotient gives an explicit field whose degree over $\mathbb{F}_p$ is divisible by r^a.

$r = 2 \neq p$. If $p \equiv 1 \pmod 4$, take $E = \mathbb{F}_p$ and start at -1, of order two. The same root chain gives c of order $2^{v_2(p-1)}$. Since $v_2(p-1) \geq 2$, the valuation calculation gives irreducibility of $V^{2^a} - c$ over E. If $p \equiv 3 \pmod 4$, first construct $E = \mathbb{F}_p[U]/(U^2+1)$ and let i be the class of U. The polynomial is irreducible since an element squaring to -1 would have order four in $\mathbb{F}_p^\times$, whose order is $p - 1 \equiv 2 \pmod 4$. For $a = 1$ this is the desired field. For $a \geq 2$, start the chain at i, of order four, and take square roots until reaching an element c of order $2^{v_2(p^2-1)}$. Use $V^{2^{a-1}} - c$ over E. Here $|E| = p^2 \equiv 1 \pmod 4$ and the valuation identity gives extension degree 2^{a-1} over E, hence degree 2^a over $\mathbb{F}_p$.

$r = p$. Starting at $\mathbb{F}_p$, perform a Artin–Schreier steps. In the current field E, choose a basis element c outside the image of the $\mathbb{F}_p$-linear map $z \mapsto z^p - z$. Its kernel is $\mathbb{F}_p$, so the image has codimension one. The derivative of $V^p - V - c$ is -1. If α is one root, the p distinct roots are $\alpha + j$ for $j \in \mathbb{F}_p$, so its splitting field is $E(\alpha)$. Each automorphism acts on α by translation by such a j, giving an injective homomorphism into the additive group of $\mathbb{F}_p$. Since c is outside the image, the polynomial has no root in E. Thus the group has order p and the polynomial is irreducible. Replace E by $E[V]/(V^p - V - c)$ at each step.

In each constructed field, compute the kernels of the $\mathbb{F}_p$-linear maps $z \mapsto z^{p^{r^a}} - z$ and $z \mapsto z^{p^{r^{a-1}}} - z$. Both r^a and r^{a-1} divide the ambient degree, so the roots of the corresponding equations are exactly the subfields of degrees r^a and r^{a-1} over $\mathbb{F}_p$. Choose a basis vector of the larger kernel outside the smaller one. Every proper subfield of the degree-r^a field is contained in the degree-r^{a-1} subfield. The first dependence of the powers of this vector, beginning with the zeroth power, gives its minimal polynomial, of degree r^a.

Take the compositum of the resulting fields by successively adjoining the roots of their defining polynomials. If the current field has degree d over $\mathbb{F}_p$, adjoining a root of degree r^a over $\mathbb{F}_p$ gives degree r^a over the current field. In fact its orbit under p^dth powering has length $r^a / \gcd(d, r^a) = r^a$, since the construction takes each prime divisor of m only once. Thus each polynomial remains irreducible in the corresponding quotient construction. In the resulting degree-m field take the sum of the chosen generators. If the sum has degree e over $\mathbb{F}_p$, then $e \mid m$. For each exact prime power r^a dividing m, the subfield of degree $\operatorname{lcm}(e, m/r^a)$ exists since that degree divides m. It contains the sum and every other generator, so subtraction puts the generator of degree r^a in it as well. Thus r^a divides $\operatorname{lcm}(e, m/r^a)$, and coprimality of r^a and m/r^a implies $r^a \mid e$. This holds for each prime power, giving $e = m$. The first linear dependence among the powers of the sum yields its monic minimal polynomial.

All choices can be made by fixed coordinate order or by a fixed elimination procedure. In the root chains the base fields have dimension at most r over $\mathbb{F}_p$, so each chain has $O(r(1 + \log_2 p))$ steps. A step calls Proposition 3.1 on degree r, costing at most $r - 1$ prime-field queries. The initial cyclotomic queries have degree $r - 1$. The sum of distinct prime divisors of m is at most m, by iterating $u + v \leq uv$ for integers $u, v \geq 2$. The sum of their squares is at most the square of their

sum. The root chains and cyclotomic queries therefore use $O(m^2(1+\log_2 p))$ queries in total. The temporary fields have dimension at most m^2 over $\mathbb{F}_p$. Build a multiplication table at each stage of a tower by multiplying its basis monomials and reducing by the monic defining polynomial over the preceding field. The previous table implements arithmetic over that field. The dimensions and defining degrees are bounded by m^2, so each new table uses polynomially many operations. Once a table is available, multiplication is bilinear in the coordinates and inversion is a linear system. The exponent p^{r^a} has at most $1+m\lceil\log_2 p\rceil$ bits. Thus all powering, kernel computations, and changes of basis have polynomial bit cost in m and $\log_2 p$. □

Proof of Theorem 1.1. Use the prime-field algorithm of Section 2 for the queries of Proposition 3.1. Each query has degree at most n, and $\log_2 p \le \log_2 q$, giving the asserted polynomial bound. For the presentation interface, recover p, m from the promised prime power q by testing exact integer roots in decreasing order of exponent from $\lfloor\log_2 q\rfloor$ to 1. The largest successful exponent is m by unique factorization. For each exponent, binary search on the integers from 2 to q tests for an exact root. Binary powering with intermediate values capped at $q+1$ keeps the integer bit lengths polynomial in $\log_2 q$. Apply Proposition 4.1 with the same prime-field algorithm. Since $m \le \log_2 q$, the query count, query degrees and remaining computation are all polynomially bounded in $\log_2 q$. □

References

[1] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859.

[2] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.

[3] D. G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), 587–592.

[4] D. Cureton and J. Thorner, *A quasi-Riemann hypothesis for Dedekind zeta functions*, Hexagon 2610.00200v2, 2026.

[5] S. Evdokimov, *Factorization of polynomials over finite fields in subexponential time under GRH*, Algorithmic Number Theory, Lecture Notes in Comput. Sci. **877**, Springer, 1994, 209–219.

[6] H. W. Lenstra, Jr., *Finding isomorphisms between finite fields*, Math. Comp. **56** (1991), 329–347.

[7] F. Nie, H. Ye, S. Liu, Z. Wang, S. Ermon, and J. Zou, *One-sided verification under limited expert review*, arXiv:2610.18089v2, 2026.

[8] OpenAI, *Deterministic polynomial factorization over prime fields*, preprint, October 4, 2026.

[9] OpenAI, *Primitive roots for every admissible integer base*, preprint, October 4, 2026.

[10] OSVerify contributors, *Rethlas–OSV*, software, 2026.

[11] V. Shoup, *New algorithms for finding irreducible polynomials over finite fields*, Math. Comp. **54** (1990), 435–447.

[12] V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), 261–267.

[13] J. M. Shunia, *Deterministic polynomial-time primality testing with a single binomial congruence*, arXiv:2611.02280v1, 2026.

[14] P.-J. Spaenlehauer, *Deterministic root-finding over finite fields with elliptic curves*, 2026. arXiv:2610.32508v1.

Zhili College, Tsinghua University, Beijing 100084, China
Email address: tangqy24@mails.tsinghua.edu.cn