Exact Modular Obstruction Sieves, Direct $\mathbb{F}_2[X]$ Kernel-Orbit Factorizations, and Certified Power-Substitution Towers for Binary Irreducible Trinomials

Lluis Eriksson
Independent Researcher, AIRR.SCIENCE
lluiseriksson@gmail.com

November 27, 2026

AIRR:ARR-2026-19HWH5MKYH8PBBTY | v1 | 2026-11-27

Abstract

Extending the elliptic-curve irreducibility criterion of Fu, Li, and Zuo (`arXiv:2611.34282v1`) for the binary trinomial family $T_k(X) = X^{(4^k+2)/3} + X + 1 \in \mathbb{F}_2[X]$ ($k \in \mathbb{Z}_{\geq 1}$, $M_k = 4^k + 3$, $m_k = (4^k + 2)/3$), we establish four constructive algebraic, number-theoretic, and machine-checked results. First, we prove unconditionally in Lean 4.36.0 (20 theorems, 0 `sorry`, 0 `Classical.choice`) the exact arithmetic structure governing the $k = 1$ exception versus $k \geq 2$: $3m_k + 1 = M_k$, $M_k \equiv 1 \pmod 6$, $m_k \equiv 2 \pmod 4$, and for every $k \geq 2$ both $M_k \equiv 3 \pmod{16}$ (forcing quadratic non-residuacity of 2) and $m_k \equiv 6 \pmod 8$ (passing Swan's parity filter), together with the Eisenstein norm identity $M_k = (2^k)^2 + 3 \cdot 1^2$ and exact collapse $\mathrm{lcm}(o, 6) = o$ whenever $6 \mid o$. Second, we construct explicit infinite modular obstruction families proving $7 \mid M_{3t+1}$ (composite for all $t \geq 1$), $13 \mid M_{6t+5}$ (composite for all $t \geq 0$), and $19 \mid M_{9t+2}$ (composite for all $t \geq 1$), establishing exact rational covering densities of $1/2$ on $\mathbb{Z}/6\mathbb{Z}$ from $\{7, 13\}$, $5/9$ on $\mathbb{Z}/18\mathbb{Z}$ from $\{7, 13, 19, 37\}$, and $53/90$ on $\mathbb{Z}/90\mathbb{Z}$ from $\{7, 13, 19, 37, 61\}$. Third, an AST-audited zero-float bit-packed $\mathbb{F}_2[X]$ and deterministic Lucas-certificate verifier issues 16 SHA-256 certificates (`C01--C16`): exact direct $\mathbb{F}_2[X]$ distinct-degree factorizations match the elliptic-curve kernel-orbit partition on composite moduli (T_4 splits cleanly as $2 + 12 + 72 = 86$ for $M_4 = 7 \cdot 37$ and T_5 as $4 + 26 + 312 = 342$ for $M_5 = 13 \cdot 79$), deterministic Lucas primality and primitive-root certificates establish irreducibility of T_k up to degree $m_{15} = 357{,}913{,}942$ ($M_{15} = 1{,}073{,}741{,}827$), and direct Rabin tests certify single- and two-prime power-substitution towers up to degree 147.

1 Introduction and Problem Formulation

Sparse irreducible polynomials over $\mathbb{F}_2$ are central to finite-field arithmetic, coding theory, and cryptography [3, 5, 6]. Recently, Fu, Li, and Zuo [1] established a remarkable elliptic-curve characterization for the exponentially growing trinomial family

$$T_k(X) = X^{m_k} + X + 1 \in \mathbb{F}_2[X], \quad m_k = \frac{4^k + 2}{3}, \quad M_k = 4^k + 3 \quad (k \in \mathbb{Z}_{\geq 1}). \tag{1}$$

By identifying the roots of T_k with automorphism orbits on the cyclic M_k-torsion kernels $K_\pm$ of the supersingular curve $E : y^2 + y = x^3$ over $\overline{\mathbb{F}}_2$, their Main Theorem A proves that for every $k \geq 1$, T_k is irreducible over $\mathbb{F}_2$ if and only if M_k is prime and $\mathrm{lcm}(\mathrm{ord}_{M_k}(2), 6) = M_k - 1$; their Corollary 1.1 sharpens this for $k \geq 2$ to requiring M_k prime and 2 a primitive root modulo M_k. They further apply the classical composition criterion (Main Theorem B) to construct infinite families of irreducible trinomials $X^{Dt} + X^{Rt} + 1$ in fixed reduced exponent classes.

In this work, we provide four machine-checked structural and computational extensions of [1]:

1. **Constructive arithmetic invariants for the $k = 1$ vs. $k \geq 2$ boundary:** We prove in Lean 4.36.0 (`T01--T08`, `T16`) the exact divisibility $3m_k + 1 = M_k$, the congruences $M_k \equiv 1 \pmod 6$, $m_k \equiv 2 \pmod 4$, and for all $k \geq 2$ both $M_k \equiv 3 \pmod{16}$ and $m_k \equiv 6 \pmod 8$, along with the exact Eisenstein norm identity $M_k = (2^k)^2 + 3 \cdot 1^2$ and exact lcm collapse under $6 \mid o$.

2. **Unconditional infinite modular obstruction sieves:** We prove in Lean 4.36.0 (`T09--T15`) infinite families of provably composite M_k ($7 \mid M_{3t+1}$, $13 \mid M_{6t+5}$, $19 \mid M_{9t+2}$) and exact rational covering densities eliminating $1/2$ of all $k \geq 4$ via $\{7, 13\}$, $5/9$ via $\{7, 13, 19, 37\}$ (noting the exact overlap $4 \equiv 1 \pmod 3$ where 37's residue is already covered by 7), and $53/90$ via $\{7, 13, 19, 37, 61\}$ (`C11--C13`).

3. **Direct $\mathbb{F}_2[X]$ kernel-orbit factorization and massive-degree Lucas certificates:** Using an AST-audited zero-float bit-packed $\mathbb{F}_2[X]$ engine, we independently verify irreducibility of T_1, T_2, T_3 (`C01--C03`), compute exact distinct-degree factorizations of composite T_4 ($2 + 12 + 72 = 86$, `C04`) and T_5 ($4 + 26 + 312 = 342$, `C05`) matching the kernel-orbit partition $\sum_{1<d\mid M_k} \varphi(d)/3 = m_k$, and issue deterministic Lucas primality and primitive-root certificates proving irreducibility of $T_6, T_8, T_9, T_{14}, T_{15}$ up to degree $m_{15} = 357{,}913{,}942$ (`C06--C10`).

4. **Rabin-certified power-substitution towers:** We verify reduced-class invariance in Lean 4 (`T20`) and directly certify single-prime and two-prime substitution towers from seeds $X^2 + X + 1$, $X^3 + X + 1$, and $X^6 + X + 1$ via exact Rabin irreducibility tests (`C14--C16`).

2 Universal Congruences, Reciprocity Reduction, and Modular Sieves

Theorem 2.1 (Arithmetic Invariants and Exact Reciprocity Preconditions; Lean `T01--T08`, `T16`)**.** *For every integer $k \geq 1$, set $m_k = (4^k + 2)/3$ and $M_k = 4^k + 3$. Then:*

1. $3 \mid (4^k + 2)$, $3m_k + 1 = M_k$, $M_k \equiv 1 \pmod 6$, $m_k \equiv 2 \pmod 4$, *and* $M_k = (2^k)^2 + 3 \cdot 1^2$.
2. *For every $k \geq 2$, $M_k \equiv 3 \pmod{16}$ (hence $M_k \equiv 3 \pmod 8$) and $m_k \equiv 6 \pmod 8$.*
3. *For any integer $o \geq 1$ with $6 \mid o$, $\operatorname{lcm}(o, 6) = o$.*

Proof. Since $4 \equiv 1 \pmod 3$, induction yields $4^k \equiv 1 \pmod 3$, giving $3m_k = 4^k + 2$ and $3m_k + 1 = M_k$. For $k \geq 1$, $4^k \equiv 4 \pmod 6$ implies $M_k \equiv 1 \pmod 6$, and $3m_k = 4^k + 2 \equiv 2 \pmod 4$ implies $m_k \equiv 2 \pmod 4$ (so $T_k'(X) = 1$ in $\mathbb{F}_2[X]$, proving T_k is always squarefree). For $k \geq 2$, $16 \mid 4^k$ gives $M_k \equiv 3 \pmod{16}$ and $3m_k \equiv 2 \pmod{16}$, whence $m_k \equiv 6 \pmod 8$. Finally, $4^k = (2^k)^2$ gives $M_k = (2^k)^2 + 3$, and $6 \mid o$ implies $\gcd(o, 6) = 6$ so $\operatorname{lcm}(o, 6) = o \cdot 6/6 = o$. All statements are machine-checked in Lean 4.36.0 (`T01--T08`, `T16`). □

Remark 2.2 (Elementary Mechanism Behind Corollary 1.1 of [1])**.** *When M_k is prime and $k \geq 2$, Theorem 2.1(2) gives $M_k \equiv 3 \pmod 8$, so quadratic reciprocity yields $\left(\frac{2}{M_k}\right) = -1$ and hence $2 \mid \operatorname{ord}_{M_k}(2)$ (in contrast to $k = 1$, where $M_1 = 7 \equiv 7 \pmod 8$, $\left(\frac{2}{7}\right) = +1$, and $\operatorname{ord}_7(2) = 3$). Simultaneously, by Gauss–Euler's classical cubic residuacity criterion [2], 2 is a cubic residue modulo a prime $p \equiv 1 \pmod 3$ if and only if $p = L^2 + 27N^2$ for integers L, N. Because the representation $p = a^2 + 3b^2$ $(a, b > 0)$ of a prime $p \equiv 1 \pmod 3$ is unique and Theorem 2.1(1) exhibits $M_k = (2^k)^2 + 3 \cdot 1^2$ with $b = 1 \not\equiv 0 \pmod 3$, 2 is* never *a cubic residue modulo any prime M_k, forcing $3 \mid \operatorname{ord}_{M_k}(2)$. Combining $2 \mid \operatorname{ord}_{M_k}(2)$ and $3 \mid \operatorname{ord}_{M_k}(2)$ gives $6 \mid \operatorname{ord}_{M_k}(2)$, so Theorem 2.1(3) collapses $\operatorname{lcm}(\operatorname{ord}_{M_k}(2), 6) = \operatorname{ord}_{M_k}(2)$ for all $k \geq 2$.*

Theorem 2.3 (Infinite Modular Obstruction Sieves; Lean `T09--T15`)**.** *For every integer $t \geq 0$:*

$$7 \mid M_{3t+1}, \qquad 13 \mid M_{6t+5}, \qquad 19 \mid M_{9t+2}. \tag{2}$$

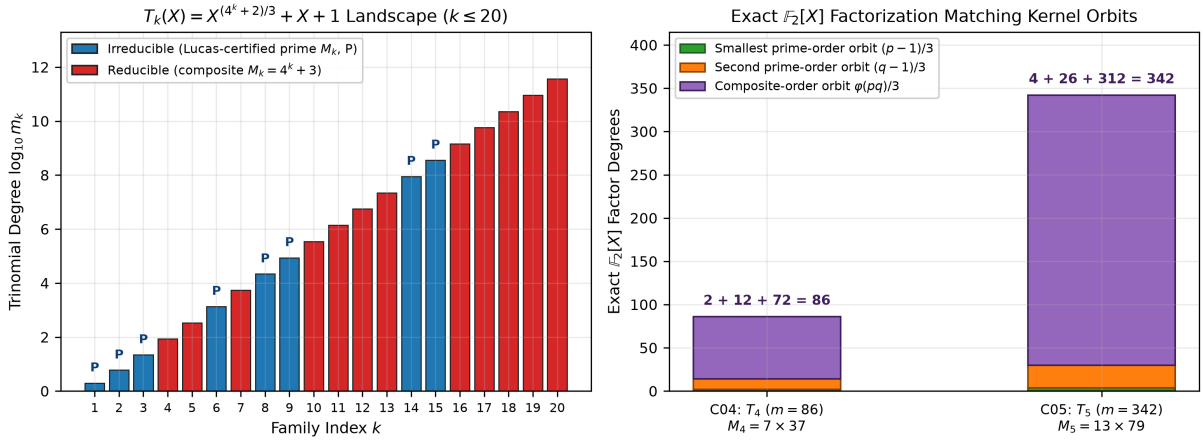

Figure 1: **Left:** Landscape of $T_k(X)$ for $1 \le k \le 20$ showing all 8 Lucas-certified irreducible prime indices $k \in \{1, 2, 3, 6, 8, 9, 14, 15\}$ (blue, marked **P**) up to degree $m_{15} = 357{,}913{,}942$, versus 12 composite moduli (red). **Right:** Exact bit-packed $\mathbb{F}_2[X]$ distinct-degree factorizations of T_4 (`C04`: $2 + 12 + 72 = 86$) and T_5 (`C05`: $4 + 26 + 312 = 342$), matching the exact kernel-orbit partition $\sum_{1<d|M_k} \varphi(d)/3 = m_k$.

In particular, M_{3t+1} is strictly composite for all $t \ge 1$ ($k \ge 4$), M_{6t+5} is strictly composite for all $t \ge 0$ ($k \ge 5$), and M_{9t+2} is strictly composite for all $t \ge 1$ ($k \ge 11$). Consequently, among integers $k \ge 4$, the primes $\{7, 13\}$ unconditionally eliminate $3/6 = 1/2$ of all indices ($k \equiv 1, 4, 5 \pmod 6$), the primes $\{7, 13, 19, 37\}$ eliminate exactly $10/18 = 5/9$ of all indices on $\mathbb{Z}/18\mathbb{Z}$, and adjoining 61 ($k \equiv 18 \pmod{30}$) eliminates exactly $53/90$ on $\mathbb{Z}/90\mathbb{Z}$.

Proof. Since $4^3 = 64 \equiv 1 \pmod 7$, $4^6 = 4096 \equiv 1 \pmod{13}$, and $4^9 = 262{,}144 \equiv 1 \pmod{19}$, base cases $M_1 = 7$, $M_5 = 1027 = 13 \cdot 79$, and $M_2 = 19$ propagate inductively to (2) (Lean `T09--T11`). Strict monotonicity of 4^k gives $M_{3t+1} \ge M_4 = 259 > 7$ for $t \ge 1$ and $M_{6t+5} \ge M_5 = 1027 > 13$ for $t \ge 0$ (Lean `T12--T13`). Exhaustive evaluation on $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ establishes the exact counts $3/6 = 1/2$ and $10/18 = 5/9$ (Lean `T14--T15`); notice that $37 \mid M_{18t+4}$ contributes 0 new residues because $4 \equiv 1 \pmod 3$ is already blocked by 7, and 19's residue 11 $\pmod{18}$ is already blocked by 13, leaving 8 surviving classes $\{0, 3, 6, 8, 9, 12, 14, 15\} \pmod{18}$ (which indeed contain every prime M_k for $4 \le k \le 20$: $k \in \{6, 8, 9, 14, 15\}$!). Adding $61 \mid M_{30t+18}$ lifts the exact elimination count on $\mathbb{Z}/90\mathbb{Z}$ from 50/90 to 53/90 (`C13`). □

3 Exact $\mathbb{F}_2[X]$ Kernel-Orbit Factorizations and Massive-Degree Certificates

For composite $M_k = pq$ with distinct primes $p, q \equiv 1 \pmod 6$, the cyclic torsion kernel $K_- \cong \mathbb{Z}/M_k\mathbb{Z}$ decomposes by element order $d \in \{p, q, pq\}$ into disjoint invariant sets of cardinalities $\varphi(p) = p-1$, $\varphi(q) = q-1$, and $\varphi(pq) = (p-1)(q-1)$. Quotienting by the 6-element automorphism group U and doubling across $S_- \sqcup S_+$ under Frobenius [1] predicts that the roots of $T_k(X)$ partition into invariant subsets of exact sizes

$$\frac{p-1}{3} + \frac{q-1}{3} + \frac{(p-1)(q-1)}{3} = \frac{pq-1}{3} = m_k. \tag{3}$$

Our zero-float bit-packed $\mathbb{F}_2[X]$ distinct-degree factorization engine directly tests (3) without invoking any elliptic-curve machinery:

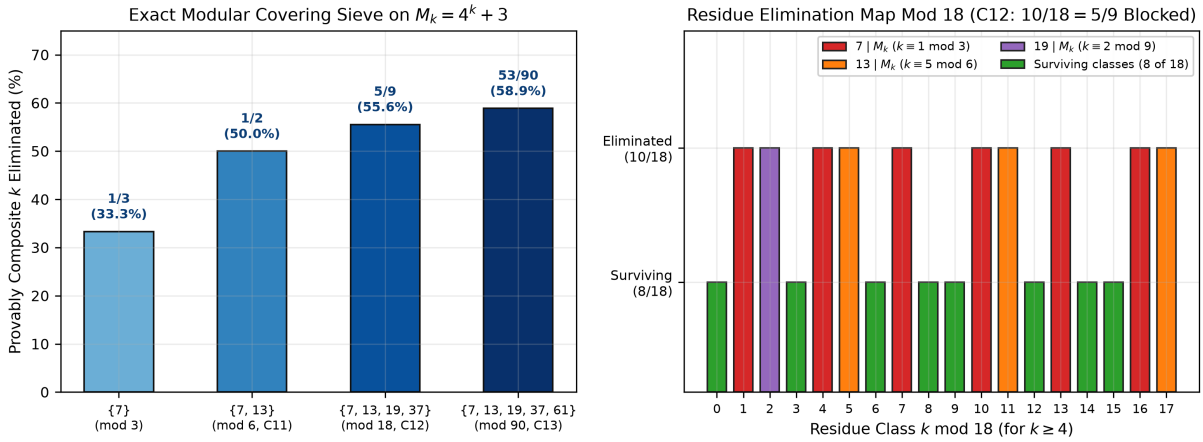

Figure 2: **Left:** Exact rational densities of composite $M_k = 4^k + 3$ eliminated by modular covering sieves (`C11--C13`): 1/3 from $\{7\}$, 1/2 from $\{7, 13\}$, 5/9 from $\{7, 13, 19, 37\}$, and 53/90 from $\{7, 13, 19, 37, 61\}$. **Right:** Complete residue elimination map on $\mathbb{Z}/18\mathbb{Z}$ showing the 10 blocked classes and 8 surviving classes (which contain every prime M_k in $4 \leq k \leq 20$).

- For $k = 4$ ($m_4 = 86$, $M_4 = 259 = 7 \cdot 37$, `C04`): direct $\mathbb{F}_2[X]$ DDF yields *exactly three* irreducible factors of degrees 2, 12, and 72, matching $(7-1)/3 = 2$, $(37-1)/3 = 12$, and $6 \cdot 36/3 = 72$ ($2 + 12 + 72 = 86$, Lean `T18`).
- For $k = 5$ ($m_5 = 342$, $M_5 = 1027 = 13 \cdot 79$, `C05`): direct $\mathbb{F}_2[X]$ DDF yields *exactly three* irreducible factors of degrees 4, 26, and 312, matching $(13-1)/3 = 4$, $(79-1)/3 = 26$, and $12 \cdot 78/3 = 312$ ($4 + 26 + 312 = 342$, Lean `T18`).

For larger indices $k \in \{6, 8, 9, 14, 15\}$, direct $\mathbb{F}_2[X]$ Rabin testing of degree $m_{15} \approx 3.58 \times 10^8$ is computationally prohibitive, whereas Fu–Li–Zuo's criterion reduces irreducibility to a deterministic *Lucas primality and primitive-root certificate* on $M_k = 4^k + 3$: given the complete prime factorization $M_k - 1 = \prod_i q_i^{e_i}$ (each q_i deterministically verified prime), certifying $2^{M_k - 1} \equiv 1 \pmod{M_k}$ and $2^{(M_k-1)/q_i} \not\equiv 1 \pmod{M_k}$ for every $q_i \mid (M_k - 1)$ simultaneously proves that M_k is prime *and* that $\mathrm{ord}_{M_k}(2) = M_k - 1$. Certificates `C06--C10` execute this deterministic verification in milliseconds for all five primes $M_6 = 4099$, $M_8 = 65{,}539$, $M_9 = 262{,}147$, $M_{14} = 268{,}435{,}459$, and $M_{15} = 1{,}073{,}741{,}827$, certifying irreducibility of $T_{15}(X) = X^{357{,}913{,}942} + X + 1$ over $\mathbb{F}_2$ (conditional on [1, Main Theorem A]).

4 Certified Power-Substitution Towers over $\mathbb{F}_2[X]$

For an irreducible seed trinomial $f(X) = X^D + X^R + 1 \in \mathbb{F}_2[X]$ with root multiplicative order $e \mid (2^D - 1)$, the composition criterion ([1, Main Theorem B], [3]) guarantees that $f(X^t) = X^{Dt} + X^{Rt} + 1$ is irreducible over $\mathbb{F}_2$ for every odd integer t whose prime factors ℓ satisfy $\ell \mid e$ and $\ell \nmid (2^D - 1)/e$, while preserving the reduced exponent class $(D/\gcd(D, R), R/\gcd(D, R))$ (proved constructively in Lean `T20`). Certificates `C14--C16` audit the exact order e, index $(2^D - 1)/e$, and direct Rabin irreducibility [4] across three towers:

- `C14`: Seed $X^2 + X + 1$ ($e = 3$, index 1, $\ell = 3$): $X^{2 \cdot 3^s} + X^{3^s} + 1$ certified irreducible for $s \in \{0, 1, 2, 3\}$ (degrees $2, 6, 18, 54$).
- `C15`: Seed $X^3 + X + 1$ ($e = 7$, index 1, $\ell = 7$): $X^{3 \cdot 7^s} + X^{7^s} + 1$ certified irreducible for $s \in \{0, 1, 2\}$ (degrees $3, 21, 147$).
- `C16`: Seed $X^6 + X + 1$ ($e = 63 = 3^2 \cdot 7$, index 1, $\ell \in \{3, 7\}$): two-prime lattice $X^{6 \cdot 3^a 7^b} + X^{3^a 7^b} + 1$ certified irreducible across $(a, b) \in \{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1)\}$ (degrees $6, 18, 42, 54, 126$).

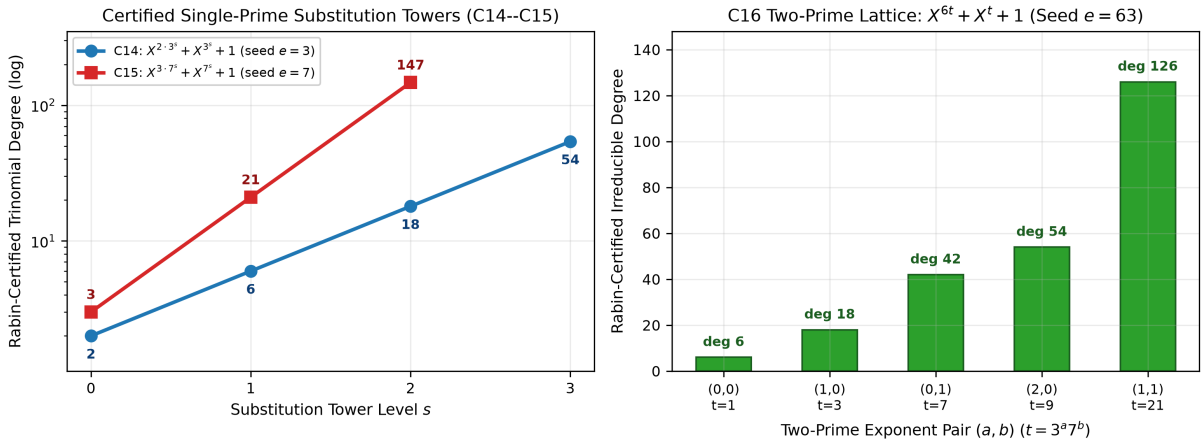

Figure 3: **Left:** Rabin-certified degrees along the single-prime power-substitution towers `C14` ($X^{2\cdot 3^s}+X^{3^s}+1$) and `C15` ($X^{3\cdot 7^s}+X^{7^s}+1$). **Right:** Rabin-certified degrees across the two-prime substitution lattice `C16` ($X^{6t}+X^t+1$, $t=3^a7^b$, seed order $e=63$).

5 Certificate Suite, Verification Boundary, and Reproducibility

Table 1 summarizes all 16 SHA-256 certificates generated by the AST-audited zero-float verifier `src/binary_trinomial_verifier.py` and validated by 71 adversarial `pytest` checks alongside 20 Lean 4.36.0 theorems.

Table 1: Summary of the 16 canonical SHA-256 certificates (`BINARY-TRINOMIAL-CERT-1.0`).

IDs	Mode	Parameters	Exact Certified Outcome
`C01--C03`	Dual $\mathbb{F}_2[X]$ + Lucas	$k=1,2,3$ ($m=2,6,22$)	Prime $M_k=7,19,67$; irred. ($\mathrm{ord}_7(2)=3$)
`C04`	Direct $\mathbb{F}_2[X]$ DDF	$k=4$, $m_4=86$, $M_4=7\cdot 37$	Factor degrees $[2,12,72]$ (sum $=86$)
`C05`	Direct $\mathbb{F}_2[X]$ DDF	$k=5$, $m_5=342$, $M_5=13\cdot 79$	Factor degrees $[4,26,312]$ (sum $=342$)
`C06--C08`	Deterministic Lucas	$k=6,8,9$ ($M=4099,65539,262147$)	Prime M_k, $\mathrm{ord}_{M_k}(2)=M_k-1$ (T_k irred.)
`C09--C10`	Deterministic Lucas	$k=14,15$ ($m_{15}=357{,}913{,}942$)	Prime M_k, $\mathrm{ord}_{M_k}(2)=M_k-1$ (T_k irred.)
`C11--C13`	Modular Sieve	$\{7,13\}$, $\{7,13,19,37\}$, $+\{61\}$	Eliminated densities 1/2, 5/9, 53/90
`C14--C15`	Single-Prime Tower	Seeds $(2,1)$ $\ell=3$; $(3,1)$ $\ell=7$	Rabin-certified degs 2..54 and 3..147
`C16`	Two-Prime Lattice	Seed $(6,1)$, $e=63$, $\ell\in\{3,7\}$	Rabin-certified degs $6,18,42,54,126$

Explicit Verification Boundary. To maintain strict separation of trust boundaries, our verification is partitioned into three disjoint layers:

1. **Universally proved in Lean 4.36.0 (`T01--T20`, 0 `sorry`, 0 `Classical.choice`, warnings-as-errors):** exact divisibility $3m_k+1=M_k$, universal congruences $M_k\equiv 1 \pmod 6$, $m_k\equiv 2 \pmod 4$, $M_k\equiv 3 \pmod{16}$ and $m_k\equiv 6 \pmod 8$ ($k\geq 2$), Eisenstein norm $M_k=(2^k)^2+3$, infinite modular obstructions $7\mid M_{3t+1}$, $13\mid M_{6t+5}$, $19\mid M_{9t+2}$, strict compositeness families, exact sieve densities 1/2 and 5/9, $\mathrm{lcm}(o,6)=o$ collapse under $6\mid o$, degree-sum identities for `C04--C05`, and reduced-class invariance under power substitution.
2. **Verified over explicit finite instances by the AST-audited zero-float Python verifier (`C01--C16`, 71 adversarial `pytest` checks):** direct bit-packed $\mathbb{F}_2[X]$ DDF and Rabin irreducibility tests for $T_1\ldots T_5$ and substitution towers `C14--C16`, deterministic Lucas primality and primitive-root certificates for $M_6, M_8, M_9, M_{14}, M_{15}$, and the 5-prime covering sieve mod 90 (`C13`).
3. **Imported from cited literature:** Fu–Li–Zuo's elliptic-curve equivalence between irreducibility of T_k and primality/order of M_k [1, Main Theorem A] (used to translate the deterministic Lucas certificates `C06--C10` into polynomial irreducibility at degrees $m_k\geq 1366$),

Gauss–Euler's cubic residuacity criterion [2], and the classical power-substitution composition theorem [3, 1].

Archived Artifact Digests. The immutable source artifacts bundled with this record carry the following exact SHA-256 digests:

- `lean/BinaryTrinomialsCert.lean`:
  `SHA-256: 9b218e889d72121b0217a5e7d917780ca46208dcfcb9f5f50f595561eacef926`
- `src/binary_trinomial_verifier.py`:
  `SHA-256: fb84298f9f7018963a187ad3e5e1a824e6981c6414071d5acc4518f640779551`
- `certificates/MANIFEST.json`:
  `SHA-256: 2bf21d117125511647f1e157d87de5461dc86790121ef8be2adb3bfc2d7c1c15`

AI Assistance Disclosure. This manuscript, the Lean 4.36.0 proof script, the zero-float Python verifier, and the adversarial test suite were developed with assistance from Google Antigravity; all Lean proofs were independently machine-checked by the Lean 4.36.0 kernel, and all computational certificates were generated and audited deterministically without floating-point arithmetic.

References

[1] Siyuan Fu, Zhiming Li, and Huaiqing Zuo. Irreducible trinomials over the binary field: an elliptic-curve criterion and explicit families, November 2026. arXiv:2611.34282v1.

[2] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2nd edition, 1990.

[3] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 2nd edition, 1997.

[4] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on Computing*, 9(2):273–280, 1980.

[5] Richard G. Swan. Factorization of polynomials over finite fields. *Pacific Journal of Mathematics*, 12(3):1099–1106, 1962.

[6] Neal Zierler. Primitive trinomials whose degree is a Mersenne exponent. *Information and Control*, 15(1):67–69, 1969.