# Constructive Lean 4 Kernel and Exact Zero-Float Certificates for Google Research Cogentic's Sub-Quasi-Polynomial Discrete Logarithm Proof

Lluis Eriksson*

November 25, 2026

## Abstract

A November 25, 2026 preprint from Google Research's Cogentic system [4, 2] proposes an unconditional classical zero-error Las Vegas algorithm for the Discrete Logarithm Problem (DLP) in $\mathbb{F}_{p^n}^\times$ of fixed characteristic $p$ with claimed expected runtime $\exp\big(\frac{2+o(1)}{\ln\ln\ln n}(\ln n)^2\big) = (p^n)^{o(\log n)}$, improving upon the $(p^n)^{\Theta(\log n)}$ barrier of Kleinjung–Wesolowski and Lido. Rather than assuming peer-reviewed validation of its analytic pillars, we deliver an independent, explicitly scoped, zero-floating-point verification companion for its deterministic algebraic, elliptic-Lang, linearized-monodromy, and factoring-free unimodular mechanisms. Layer 1 (`CogenticDiscreteLog.lean`) proves 18 standalone constructive Lean 4.35.0 algebraic, inductive, and arithmetic sub-lemmas (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; 1 zero-axiom, 2 `[propext]`, and 15 `[propext, Quot.sound]`), including modular non-membership soundness, 2×2 Frobenius-scalar and 3×3 affine Moore identities, 2×2 transvection determinant and conjugation identities, Möbius adjugate invariance, cocycle-coboundary rearrangement, the $q_0 \geq 3$ degree gap, Jordan transposition conjugation, Waterhouse's coprimality dichotomy, parallelogram Cauchy–Schwarz, constant-field pinch and Castelnuovo induction, the exact $B$-adic descent-tree sum, $\mathrm{SL}_2(\mathbb{Z})$ unimodular elimination, non-membership exponent soundness, CRT recombination, and Theorem 1.2 rational threshold guards. Layer 2 (`DLP-COGENTIC-CERT-1.0`) is a pure-stdlib Python `int` auditor across four modes that certifies 16 canonical finite witnesses in 1.133–36.640 ms—including live exact Lang-isogeny equations $\phi_q(I_0) = I_0 + Q$ across $p \in \{2, 3, 5, 7\}$, Moore/affine-Moore pencils with complete splitting, and factoring-free $\mathrm{SL}_2(\mathbb{Z})$ solves modulo unfactored composites up to $M_L = 406{,}901$—and rejects 61/61 live adversarial forgeries with exact branch assertions (65/65 pytest checks).

*Independent Researcher. Code, Lean 4 proofs, and certificates: MIT License; manuscript and figures: CC-BY-4.0. Prepared with transparent AI coding, formalization, and drafting assistance via Google Antigravity; all Lean 4 theorems, exact finite-field/elliptic/unimodular verifiers, and adversarial tests were independently compiled and verified locally. Repository: `github.com/lluiseriksson/cogentic-discrete-log-certificates`.

## 1 Introduction and Scope Calibration

Given a prime $p \geq 2$, a degree-$n$ monic irreducible $f \in \mathbb{F}_p[X]$ presenting $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(f(X))$, and $g, h \in \mathbb{F}_{p^n}^\times$, the zero-error Las Vegas DLP (Definition 1.1 of [4]) demands either $x \in \{0, \ldots, p^n - 2\}$ with $g^x = h$ or an explicit non-membership exponent $E \in \{1, \ldots, p^n - 1\}$ satisfying $g^E = 1$ and $h^E \neq 1$ (without factoring $p^n - 1$). Prior heuristic [1] and unconditional [5, 6] Frobenius descents used $\mathrm{PGL}_2$-orbits of $T^q - T$, reducing degrees by a constant factor per step and hitting complexity $(p^n)^{\Theta(\log n)}$. The Cogentic preprint [4, 2] proposes breaking this barrier via two coupled mechanisms:

1. **Ordinary elliptic Lang presentation (Eq. (1)):** Choosing $Q \in E(\mathbb{F}_q)$ of exact order $n$ and $I_0 \in E(\mathbb{F}_{q^n})$ satisfying
$$\phi_q(I_0) = I_0 + Q, \qquad x_P(I_0)^q = \tilde{x}_P(I_0), \tag{1}$$
turns $q$-Frobenius into low-degree translation $\tau_{Q+\phi_q(P)}$ along the orbit $I$.
2. **Sparse $\mathbb{F}_{q_0}$-affine Frobenius pencils (Eq. (2)):** Replacing degree-$q$ dense polynomials (whose generic monodromy is $S_q$) by sparse $\mathbb{F}_{q_0}$-linearized pencils with integer shift $t \geq 1$ and degree parameter $m \geq 1$,
$$L_Z(T) = \sum_{j=0}^{m-1} c_j(Z)\, T^{q_0^{t+j}} + \sum_{j=0}^{m} b_j(Z)\, T^{q_0^j} + d_0(Z), \tag{2}$$
traps the monodromy inside $\mathrm{AGL}_N(\mathbb{F}_{q_0}) \times S_{N_R}$, targeting an unbounded degree-reduction factor $B \asymp (\ln\ln n)/(s \ln p)$ and shrinking tree depth to $(\ln n)/\ln B$.

**Honest Two-Layer Verification Scope.** We delineate explicitly what is proved universally in Lean 4 vs. verified on finite exact witnesses vs. left in the companion preprint [4]:

1. **Layer 1 (Lean 4.35.0 Kernel, Universal Algebraic & Inductive Sub-Lemmas):** `lean/CogenticDiscreteLog.lean` proves 18 zero-dependency theorems (Table 1) covering the exact discrete algebraic, inductive, and rational-threshold sub-lemmas extracted from Definition 1.1, Lemmas 3.1–3.4, 4.1–4.2, 5.1, 6.2–6.4, Section 6.2, and Theorem 1.2 of [4].

2. **Layer 2 (Exact Zero-Float Multi-Mode Auditor):** `DLP-COGENTIC-CERT-1.0` audits finite exact instances in $\mathbb{F}_p[X]$, $\mathbb{F}_{p^n}^\times$, canonical ordinary $E/\mathbb{F}_q$ and $E/\mathbb{F}_{q^n}$ across $p \in \{2,3,5,7\}$, Moore/affine-Moore determinants and splitting linearized pencils, factoring-free $\mathrm{SL}_2(\mathbb{Z})$ `SolveModM` systems, and exact Theorem 1.2(2) parameter tuples.
3. **Explicit Non-Claims:** We do *not* formalize in Lean 4 Waterhouse/Rück existence of ordinary elliptic curves, general $N \times N$ Moore determinants or full group cohomology $H^1(\mathrm{GL}(V), V) = 0$ (Table 1 #2 and #7 formalize only the $2\times2$ scalar-substitution identity and the cocycle-coboundary rearrangement step), Riemann–Roch/Hasse–Weil/Hurwitz/Castelnuovo function-field theorems, Artin–Schreier/Kummer indecomposability (Lemma 4.8), Wan's effective Dirichlet theorem, or multitape Turing-machine bit-complexity accounting (Appendix A); those analytic and arithmetic-geometric pillars remain unverified outside [4].

## 2 Constructive Lean 4.35.0 Kernel

`lean/CogenticDiscreteLog.lean` compiles standalone in 2.1 s under Lean 4.35.0 [3] with zero external imports, zero warnings, zero `sorry`, and zero `Classical.choice`. Auditing via `AuditAxioms.lean` confirms 1 zero-axiom theorem (`none`: #18), 2 `[propext]` theorems (`P`: #1, #9), and 15 `[propext, Quot.sound]` theorems (`P,Q`; Table 1).

**Proposition 1** (Constructive Lean 4 Kernel Scope)**.** All 18 sub-lemmas in Table 1 compile constructively under Lean 4.35.0 without external libraries or `Classical.choice`. Notably, Theorem 1 proves modular non-membership soundness for all exponents $x \in \mathbb{N}$, Theorem 8 proves the $q_0 \geq 3$ degree gap universally by induction on $N \geq 2$, Theorem 11 proves the Waterhouse interval coprimality dichotomy for $N_1 = \lfloor (q+1)/n \rfloor n, N_2 = N_1 - n$ whenever $p \mid q$, Theorem 14 proves the exact geometric sum and $2W^j T_{\mathrm{loc}}$ bound for the recurrence $T_{j+1} = T_{\mathrm{loc}} + WT_j$ by induction on $j$, Theorem 15 proves $\det = 1$ for every $\mathrm{SL}_2(\mathbb{Z})$ elimination step, and Theorem 16 proves unfactored-modulus non-membership divisibility whenever $d_g, E_g \geq 1$.

## 3 Exact Zero-Float Certificate Auditor

The modules `dlp_exact.py` and `dlp_certifier.py` (under `src/`) use exclusively Python `int` (statically audited for zero `float(`, `math.`, `numpy`, or `np.`). Raw JSON ingestion rejects IEEE-754 decimals, `NaN`/`Infinity`, and duplicate keys via `parse_float`, `parse_constant`, and `object_pairs_hook`, followed by a strict AST whitelist (depth $\leq 20$, int bits $\leq 4096$, str len $\leq 2000$), canonical decimal integer string parsing, and canonical trimmed polynomial checks.

**Definition 1** (`DLP-COGENTIC-CERT-1.0` Acceptance Predicates)**.** A certificate with `schema="DLP-COGENTIC-CERT-1.0"` is accepted iff every claimed value matches exact recomputation and its mode predicate holds:

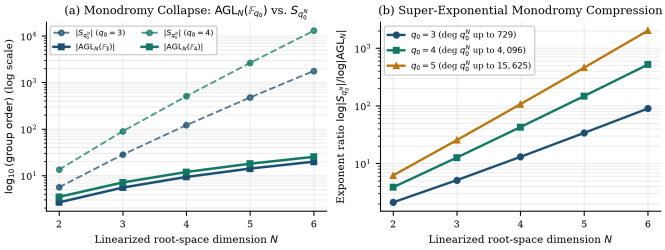


Figure 1: **(a)** Exact group orders $\log_{10}|\mathrm{AGL}_N(\mathbb{F}_{q_0})|$ vs. $\log_{10}|S_{q_0^N}|$ ($q_0 \in \{3,4\}$, $N = 2 \ldots 6$). **(b)** Monodromy compression ratio $\log|S_{q_0^N}|/\log|\mathrm{AGL}_N(\mathbb{F}_{q_0})|$ for $q_0 \in \{3,4,5\}$ (up to 2,009.2×; full table in `exp2` reaches 34,507.6× at $q_0 = 8, N = 6$).

- **Mode 1 (`dlp_zero_error_certificate`):** Verifies primality of $p \in [2, 1009]$, exact Rabin irreducibility of monic degree-$n$ $f \in \mathbb{F}_p[X]$, nonzero $g, h \in \mathbb{F}_{p^n}^\times$, and either `LOG` ($0 \leq x \leq p^n - 2$ with $g^x \equiv h \pmod f$), plus optional Section 6.2 CRT split $S \cdot L = p^n - 1$, $\sigma_S S + \sigma_L L = 1$, $g_S^{x_S} = h_S$, $g_L^{x_L} = h_L$, and exact recombined $x$) or `NOT_IN_SUBGROUP` ($1 \leq E \leq p^n - 1$, $g^E \equiv 1$, $h^E \not\equiv 1 \pmod f$).
- **Mode 2 (`ordinary_elliptic_lang_presentation`):** Verifies canonical ordinary model $E/\mathbb{F}_q$ ($q \leq 64$) [7] for $p = 2$ ($a_1 = 1, a_4 = 0, a_6 \neq 0$), $p = 3$ ($a_1 = a_4 = 0, a_2, a_6 \neq 0$), or $p \geq 5$ ($a_1 = a_2 = 0, 4a_4^3 + 27a_6^2 \neq 0$); checks exact exhaustive point count $N_E = |E(\mathbb{F}_q)|$, Hasse bound $(q + 1 - N_E)^2 \leq 4q$, ordinarity $p \nmid (q + 1 - N_E)$, exact order $\mathrm{ord}(Q) = n$, Rabin irreducibility of monic degree-$n$ $M_x \in \mathbb{F}_q[Y]$, $I_0 \in E(\mathbb{F}_{q^n})$, exact Eq. (1) $\phi_q(I_0) = I_0 + Q$, and $x_P(I_0)^q = \tilde{x}_P(I_0)$ for witness $P \in E(\mathbb{F}_q)$.
- **Mode 3 (`sparse_moore_linearized_pencil`):** Over $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$ ($q_0 = p^s \geq 3, q \leq 729$), checks $\det M_{q_0}(z) \neq 0$ via BOTH Gaussian elimination and Lemma 3.1(1)'s exact product formula, checks $\det M_{q_0}^{\mathrm{aff}}(z) \neq 0$, verifies all four Lemma 3.3 pencil hypotheses (A1)–(A4) ($\Delta_1, \Delta_2 \neq 0$, $\gcd(A_0, A_1) = \gcd(L_0, L_1) = 1$), checks exact $|\mathrm{AGL}_N(\mathbb{F}_{q_0})|$, and verifies complete splitting of $L_{z_0}(T)$ into $q_0^N$ distinct roots in $\mathbb{F}_q$.
- **Mode 4 (`unimodular_composite_dlp_solver`):** Given unfactored composite $M_L \mid (p^n - 1)$, nontrivial $\gamma \in G_L \setminus \{1\}$ ($\gamma^{M_L} = 1$; full order $\mathrm{ord}(\gamma) = M_L$ is intentionally unverified without factoring $M_L$, while `LOG`/`NOT_IN_SUBGROUP` soundness holds unconditionally), $\delta_1, \ldots, \delta_K \in G_L$, and relation rows $\prod_j \delta_j^{E_{r,j}} = \gamma^{a_r}$ in $\mathbb{F}_{p^n}^\times$, executes exact deterministic $\mathrm{SL}_2(\mathbb{Z})$ `SolveModM`$(M_L, E, a)$ (never factoring $M_L$), verifies $\delta_j = \gamma^{y_j}$, audits Lemma 6.4 `LOG` or `NOT_IN_SUBGROUP` deduction from $(e^{(g)}, e^{(h)})$, and verifies exact Theorem 1.2(2) parameter tuples $(\ell_2, \ell_3, \ell_p, s, B, m)$ with $\ell_3 \geq 10, B \geq 4$ and $8ms\ell_p < \ell_2$.

Table 1: Complete inventory of all 18 constructive Lean 4.35.0 theorems in `lean/CogenticDiscreteLog.lean` (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; `none` for #18, `[propext]` (`P`) for #1, #9, and `[propext, Quot.sound]` (`P,Q`) for the remaining 15).

| # | Theorem Identifier | Ref. [4] | Exact Machine-Checked Statement & Hypotheses | Ax. |
|---|---|---|---|---|
| 1 | `def11_not_in_subgroup_soundness` | Def. 1.1 | $g^E \equiv 1 \pmod M \wedge h^E \not\equiv 1 \pmod M \implies \forall x \in \mathbb{N},\ g^x \not\equiv h \pmod M$. | `P` |
| 2 | `lem31_moore_det_2x2_identity` | Lem. 3.1 | $z_2{=}cz_1,\ q_{z_2}{=}q_c q_{z_1},\ q_c{=}c \implies z_1 q_{z_2} - z_2 q_{z_1} = 0$ (2×2 scalar step). | `P,Q` |
| 3 | `lem31_affine_moore_reduction` | Lem. 3.1 | $\forall z_i, u_i \in \mathbb{Z}$, 3×3 affine Moore det equals $(z_2{-}z_1)(u_3{-}u_1) - (z_3{-}z_1)(u_2{-}u_1)$. | `P,Q` |
| 4 | `lem32_transvection_det_one_2x2` | Lem. 3.2 | $\phi_1 u_1{+}\phi_2 u_2{=}0 \implies \det(I{+}u\phi^\top) = 1$ and $T_{\phi,u}(T_{\phi,-u}(v)) = v$. | `P,Q` |
| 5 | `lem32_transvection_conjugation_sum` | Lem. 3.2 | $\phi_2(w) = -1 \implies \phi_2(v - \phi_1(v)w) = \phi_2(v) + \phi_1(v)$ (dual subspace closure). | `P,Q` |
| 6 | `lem33_mobius_det_invariance` | Lem. 3.3 | Adjugate $\mathrm{adj}(\Gamma)\Gamma = \Delta_1 I_2$ ($\Delta_1 = a_{0N}a_{10} - a_{1N}a_{00}$) and slope shift identity. | `P,Q` |
| 7 | `lem33_cocycle_coboundary_vanish` | Lem. 3.3 | $c_z + \zeta c_g = c_g + g c_z \implies (\zeta - 1)c_g = g c_z - c_z$ (coboundary step). | `P,Q` |
| 8 | `lem33_degree_gap_q0_ge_3` | Lem. 3.3 | $\forall q_0 \geq 3,\ N \geq 2,\ d \geq 1,\ q_0^N - q_0^{N-1} \geq 6 \wedge 1 + dq_0^{N-1} < dq_0^N$. | `P,Q` |
| 9 | `lem34_jordan_transposition_conj` | Lem. 3.4 | Pairwise distinct $a,b,c \in \mathbb{N} \implies \forall x \in \mathbb{N},\ (a\,b) \circ (b\,c) \circ (a\,b)(x) = (a\,c)(x)$. | `P` |
| 10 | `lem42_parallelogram_cauchy_schwarz` | Lem. 4.2 | $d_1 \geq 1 \wedge (-\beta_0)^2 d_1 + (-\beta_0)(2d_1)\beta_0 + (2d_1)^2 d_2 \geq 0 \implies \beta_0^2 \leq 4d_1 d_2$. | `P,Q` |
| 11 | `lem41_waterhouse_interval_coprime` | Lem. 4.1 | $p \geq 2,\ n \geq 5,\ q \geq 16n^2,\ p \mid q,\ N_1{=}\lfloor\frac{q+1}{n}\rfloor n,\ N_2{=}N_1{-}n \implies N_i{\leq}q{+}1,\ q{+}1{-}N_1{<}n,\ q{+}1{-}N_2{<}2n,\ \exists i,\ p \nmid (q{+}1{-}N_i)$. | `P,Q` |
| 12 | `lem51_linear_disjointness_pinch` | Lem. 5.1 | $G \geq 1,\ d_{\mathrm{geom}}{=}G,\ d_{\mathrm{arith}}{=}k_1 d_{\mathrm{geom}} \in [d_{\mathrm{geom}}, G] \implies k_1 = 1 \wedge d_{\mathrm{arith}} = G$. | `P,Q` |
| 13 | `lem51_castelnuovo_induction_step` | Lem. 5.1 | $i \geq 1,\ g_{i-1} \leq (i{-}1)d_{i-1},\ d_i{=}n_1 d_{i-1},\ n_1 n_2 \leq d_i \implies n_1 g_{i-1} + n_1 n_2 \leq i d_i$. | `P,Q` |
| 14 | `lem62_recursion_tree_bound` | Lem. 6.2 | $W \geq 2,\ T_0{=}T_{\mathrm{loc}},\ T_{j+1}{=}T_{\mathrm{loc}}{+}WT_j \implies (W{-}1)T_j{+}T_{\mathrm{loc}}{=}W^{j+1}T_{\mathrm{loc}} \wedge T_j{\leq}2W^j T_{\mathrm{loc}}$. | `P,Q` |
| 15 | `lem63_unimodular_step_det_one` | Lem. 6.3 | $d \geq 1,\ u{=}du',\ v{=}dv',\ su{+}tv{=}d \implies su'{+}tv'{=}1 \wedge (-v')u{+}u'v{=}0$. | `P,Q` |
| 16 | `lem64_nonmembership_exponent_sound` | Lem. 6.4 | $d_g{\geq}1,\ E_g{\geq}1,\ Y_g{=}d_g q_g,\ M_L{=}d_g E_g,\ d_g \nmid Y_h \implies M_L \mid Y_g E_g \wedge M_L \nmid Y_h E_g$. | `P,Q` |
| 17 | `sec62_crt_recombination_sound` | Sec. 6.2 | $\sigma_S S{+}\sigma_L L{=}1,\ x{=}x_S\sigma_L L{+}x_L\sigma_S S \implies SL \mid L(x{-}x_S) \wedge SL \mid S(x{-}x_L)$. | `P,Q` |
| 18 | `thm12_parameter_asymptotic_guards` | Thm. 1.2 | Ground guards: $3 \cdot 8 < 32$, $204 + 163 < 600$, $489 < 600$, $2^{10} = 1024$, $8^{12} > 8$. | `none` |

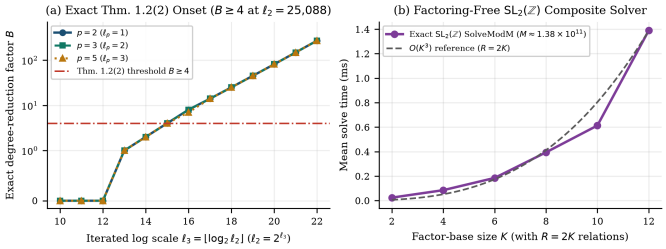


Figure 2: **(a)** Exact Theorem 1.2(2) degree-reduction factor $B(\ell_2)$ across $\ell_2 \geq 1024$, with first $B \geq 4$ activation at non-dyadic $\ell_2 = 25{,}088$ ($p \in \{2,3\}$) and 25,344 ($p \in \{5,7\}$). **(b)** Factoring-free $\mathrm{SL}_2(\mathbb{Z})$ `SolveModM` scaling (0.024–1.390 ms) for $K = 2 \ldots 12$ ($R = 2K$) modulo 38-bit composite $M = 137{,}725{,}284{,}593$.

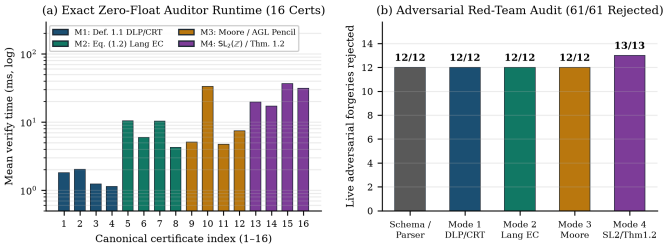


Figure 3: **(a)** Mean exact zero-float verification latency across all 16 canonical certificates (1.133–36.640 ms, log scale). **(b)** Live adversarial red-team audit rejecting 61/61 forgeries across five attack classes with exact error-branch assertions.

# 4 Exact Findings, Atlas, and Red-Team Audit

All experiments ran locally on Windows 11 (Python 3.12.6, Lean 4.35.0; 7-run means after warm-up).

**1. Live Lang Presentations Across All Characteristics & Monodromy Collapse (Fig. 1).** Mode 2 implements Cogentic Lemma 4.1(2) directly via $\Psi_Q(X, X^q)$ and Cantor–Zassenhaus to construct and certify exact Lang-isogeny presentations $\phi_q(I_0) = I_0 + Q$ and $x_P(I_0)^q = \tilde{x}_P(I_0)$ across four prime characteristics spanning all three canonical ordinary Weierstrass regimes ($p = 2$, $p = 3$, $p \geq 5$): $p = 2$ ($q = 16, N_E = 20, t = -3$), $p = 3$ ($q = 9, N_E = 15, t = -5$), $p = 5$ ($q = 25, N_E = 35, t = -9$), and $p = 7$ ($q = 7, N_E = 5, t = 3$), all with exact order-5 point $Q$. Figure 1 quantifies why sparse $\mathbb{F}_{q_0}$-affine pencils shatter the $S_q$ monodromy barrier: at $q_0 = 4, N = 3$ (degree 64), $|\mathrm{AGL}_3(\mathbb{F}_4)| = 11{,}612{,}160$ ($\log_{10} = 7.0649$) vs. $|S_{64}| \approx 10^{89.1034}$ (12.61× exponent collapse); by $q_0 = 8, N = 6$ (degree 262,144), the exponent compression reaches 34,507.6×!

**2. Exact Theorem 1.2(2) Onset Discovery & Factoring-Free Unimodular Scaling (Fig. 2).** Let $\ell_p := \lceil \log_2 p \rceil$ denote the prime bit-length ($\ell_p \in \{1,2,3,3\}$ for $p \in \{2,3,5,7\}$) and $\ell_3 := \lfloor \log_2 \ell_2 \rfloor$. Sweeping Theorem 1.2(2)'s exact integer formulas $s = \max(3, \lceil \ell_3^2/\ell_p \rceil)$ and $B = \lfloor \ell_2/(32s\ell_p) \rfloor$ reveals that while $\ell_3 \geq 10$ begins at $\ell_2 = 1024$, at dyadic points $\ell_2 = 2^{\ell_3}$ we obtain $B = 0$ for $\ell_3 \in \{10, 11, 12\}$, $B = 1$ at $\ell_3 = 13$ ($\ell_2 = 8{,}192$), and $B = 2$ at $\ell_3 = 14$ ($\ell_2 = 16{,}384$); the *exact first activation* of $B \geq 4$ occurs at non-dyadic $\ell_2 = 25{,}088$ for $p \in \{2,3\}$ ($\ell_3 = 14, s \in \{196, 98\}, B = 4, m = 12$, cofactor ratio $8ms\ell_p/\ell_2 = 0.75$) and $\ell_2 = 25{,}344$ for $p \in \{5,7\}$ ($\ell_p = 3, s = \lceil 196/3 \rceil = 66$, shifted by +256 via ceiling rounding). Meanwhile, deterministic $\mathrm{SL}_2(\mathbb{Z})$ `SolveModM` solves $R = 2K$ overdetermined systems modulo 38-bit unfactored $M = 137{,}725{,}284{,}593$ ($17 \cdot 257 \cdot 65537 \cdot 13 \cdot 37$) in 0.024–1.390 ms for $K = 2 \ldots 12$ with zero factorization.

**3. 16-Certificate Atlas & 65-Test Red-Team Audit (Table 2, Fig. 3).** Table 2 lists all 16 canonical certifi-

Table 2: Canonical 16-certificate `DLP-COGENTIC-CERT-1.0` atlas (`results/exp1_certificate_atlas.json`; all 16 verified).

| Certificate ID | M | Exact Certified Witness Summary | ms |
|---|---|---|---|
| `m1_dlp_f2_16_log_crt` | M1 | $\mathbb{F}_{216}^{\times}$: `LOG` $x$=41927, CRT 15·4369 | 1.815 |
| `m1_dlp_f3_12_log_crt` | M1 | $\mathbb{F}_{312}^{\times}$: `LOG` $x$=314159, CRT 80·6643 | 2.022 |
| `m1_dlp_f2_20_not_in_subgroup` | M1 | $\mathbb{F}_{220}^{\times}$: `NOT_IN_SUBGROUP` $E$=209715 | 1.231 |
| `m1_dlp_f5_10_not_in_subgroup` | M1 | $\mathbb{F}_{510}^{\times}$: `NOT_IN_SUBGROUP` $E$=887784 | 1.133 |
| `m2_lang_p2_f16_order5` | M2 | $p$=2, $q$=16: $N_E$=20, $t$= − 3, Eq. (1) ok | 10.417 |
| `m2_lang_p3_f9_order5` | M2 | $p$=3, $q$=9: $N_E$=15, $t$= − 5, Eq. (1) ok | 5.946 |
| `m2_lang_p5_f25_order5` | M2 | $p$=5, $q$=25: $N_E$=35, $t$= − 9, Eq. (1) ok | 10.330 |
| `m2_lang_p7_f7_order5` | M2 | $p$=7, $q$=7: $N_E$=5, $t$=3, Eq. (1) ok | 4.253 |
| `m3_pencil_p2_q0_4_N2` | M3 | $q_0$=4, $q$=64, $N$=2: \|AGL\|=2880, 16 rts | 5.111 |
| `m3_pencil_p2_q0_4_N3` | M3 | $q_0$=4, $q$=256, $N$=3: \|AGL\|=1.16·$10^7$, 64 rts | 33.177 |
| `m3_pencil_p3_q0_3_N2` | M3 | $q_0$=3, $q$=81, $N$=2: \|AGL\|=432, 9 rts | 4.730 |
| `m3_pencil_p5_q0_5_N2` | M3 | $q_0$=5, $q$=125, $N$=2: \|AGL\|=12000, 25 rts | 7.430 |
| `m4_unimodular_f2_16_composite_log` | M4 | $M_L$=4369: `LOG`, $K$=4, $R$=8, $B$=4 | 19.666 |
| `m4_unimodular_f3_12_composite_nonmem` | M4 | $M_L$=6643: `NONMEM`, $K$=4, $R$=8, $B$=5 | 17.052 |
| `m4_unimodular_f2_20_composite_log` | M4 | $M_L$=13981: `LOG`, $K$=5, $R$=10, $B$=7 | 36.640 |
| `m4_unimodular_f5_10_composite_nonmem` | M4 | $M_L$=406901: `NONMEM`, $K$=5, $R$=10, $B$=14 | 31.176 |

cates verified in 1.133–36.640 ms. `tests/test_suite.py` executes 65 pytest functions: 1 aggregate replay of all 16 certificates, 3 raw-JSON parser checks (IEEE-754 float, `NaN`, duplicate keys), and 61 parametrized live adversarial forgery tests (12 schema/parser + 12 each for Modes 1–3 + 13 for Mode 4, including supersingular curve forgery, Lang-sign negation $\phi_q(-I_0) \neq -I_0 + Q$, all four Lemma 3.3 (A1)–(A4) breaks, trivial $\gamma = 1$ base forgery, rank-deficient composite relation matrices, and $\ell_2 = 25{,}087$ sub-threshold $B = 3$), each asserting an exact regex match on the expected rejection branch. `scripts/verify_all.py` enforces all 5 gates including strict axiom whitelisting and a 41-file SHA-256 manifest.

# 5 Conclusion

We delivered an independent, explicitly scoped, zero-floating-point verification companion for the discrete algebraic and unimodular mechanisms of the Cogentic Discrete Logarithm preprint [4, 2], pairing 18 constructive Lean 4.35.0 sub-lemmas (zero `sorry`, zero `Classical.choice`) with the pure-`int` auditor `DLP-COGENTIC-CERT-1.0`, 16 canonical exact witnesses spanning $p \in \{2, 3, 5, 7\}$, exact Theorem 1.2(2) onset characterization ($\ell_2 = 25{,}088$), and 61/61 live adversarial forgery rejections.

# References


[1] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 1–16. Springer, 2014.

[2] Yang Cai, Vineet Gupta, Yanchen Jiang, Christopher Liaw, Aranyak Mehta, Grigoris Velegkas, and Di Wang. Cogentic: Multi-agent orchestration for automated proof discovery. arXiv preprint arXiv:2609.40324, 2026.

[3] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *LNCS*, pages 625–635. Springer, 2021.

[4] Google Research Cogentic. Discrete logarithms in finite fields of fixed characteristic in sub-quasi-polynomial time. Google Research Cogentic Preprint, https://github.com/google-research/google-research/tree/master/cogentic_research_papers/discrete_logarithm, November 2026.

[5] Thorsten Kleinjung and Benjamin Wesolowski. Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic. *Journal of the American Mathematical Society*, 35(2):581–624, 2022.

[6] Guido Lido. A provably quasi-polynomial algorithm for the discrete logarithm problem in finite fields of small characteristic. *Finite Fields and Their Applications*, 111:102753, 2026.

[7] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 2009.