Constructive Lean 4 Kernel and Exact Zero-Float Certificates for Unconditional $L_N[1/3, 105]$ Las Vegas Integer Factorization

Lluis Eriksson*

November 25, 2026

Abstract

A November 25, 2026 companion preprint from Google Research's Cogentic framework [6, 3] proposes the first unconditional uniform zero-error Las Vegas integer factorization algorithm running in expected time $L_N[1/3, 105]$ and deterministic workspace $L_N[1/3, 40]$, targeting the 34-year gap between Lenstra–Pomerance's unconditional $L_N[1/2, 1]$ bound and the heuristic $L_N[1/3, c]$ Number Field Sieve. Rather than assuming peer-reviewed validation of its analytic sieve pillars, we deliver an independent, explicitly scoped, zero-floating-point verification companion for its discrete lattice, mod-3 discrete Laplace ensemble, deterministic 3-adic Newton–Hensel square-root, Dixon splitting, and strong-induction mechanisms. Layer 1 (`CogenticL13Factorization.lean`) proves 18 standalone constructive Lean 4.35.0 algebraic, lattice, and arithmetic sublemmas (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; 4 zero-axiom `none` and 14 `[propext, Quot.sound]`). Layer 2 (`L13FACT-COGENTIC-CERT-1.0`) is a pure-stdlib Python `int`/`Fraction` 4-mode auditor certifying 16 canonical finite witnesses in 0.081–0.609 ms and rejecting 68/68 live adversarial forgeries with exact branch assertions (74/74 pytest checks).

1 Introduction and Scope Calibration

For more than three decades, unconditional Las Vegas general integer factorization stood at Lenstra–Pomerance's $L_N[1/2, 1]$ [8], while the General Number Field Sieve (GNFS) [2] achieved $L_N[1/3, (64/9)^{1/3}]$ only under unproved smoothness and algebraic heuristics. The November 25, 2026 Cogentic companion preprint [6, 3] proposes an unconditional uniform zero-error Las Vegas multitape Turing machine achieving expected time $L_N[1/3, 105]$ and deterministic space $L_N[1/3, 40]$ by coupling four discrete-algebraic engines with Siegel-zero-free analytic sieves:

1. **Mod-N LLL Lattices & 2D Lagrange–Gauss Smooth Ratio Splitting (Props. 2.2–2.3):** (3/4)-LLL reduction [7] on $\Lambda_n = \{h \in \mathbb{Z}^n : \sum h_s m_N^s \equiv 0 \pmod N\}$ ($g_1 m_N \equiv g_0 \pmod N$, $g_1^{n-1} > N/2$) supports exact layer-cake box sampling, while Lagrange–Gauss reduction on $L_z = \{(x, y) \in \mathbb{Z}^2 : x \equiv zy \pmod N\}$ splits blinded squares $w_m \equiv z_m^2 \pmod N$ into disjoint r_0-prime ratios x_1/y_1 below $\frac{1}{2}\sqrt{N}$.
2. **Mod-3 Discrete Laplace Ensemble & Geometric Ladder (Defs. 2.7, 4.1, Lem. 4.2):** Pinning $f_{\tilde{c}}(X, 1) \equiv h_0(X) \pmod 3$ to a monic odd-degree irreducible $h_0 \in \mathbb{F}_3[X]$ enforces $3 \nmid f_{\tilde{c}}(a, b)$ on all primitive pairs and enables step-2 geometric descent across $Y_0 > Y_1 > \cdots > Y_J = B$.
3. **Deterministic 3-Adic Newton–Hensel Square Roots (Lem. 5.2):** Odd degree d forces $4 \mid (3^d + 1)$, giving explicit initialization $\beta_0 = \alpha_0^{(3^d+1)/4}$ in $\mathbb{F}_{3^d}^\times$ and quadratic lifting modulo $(3^{2^k}, \tilde{f}_\iota)$ to exact global roots $\hat{\beta}_\iota(X)^2 \equiv \tilde{\Gamma}_\iota(X) \pmod{\tilde{f}_\iota}$.
4. **Adleman Characters, Blinded Dixon Splitting & Strong Induction (Lems. 5.1, 5.3, Thm. 1.1):** Degree-1 quadratic characters cut the obstruction kernel to $\dim_{\mathbb{F}_2}(E_1 \times E_2) \le 2 < 3$, unsealing z_m splits N via $\gcd(Z - Y, N)$ [5], and recursive calls on $[2, \lfloor \frac{1}{2}\sqrt{N} \rfloor]$ contract via $21.15 + 104 \cdot 2^{-1/3} < 103.72 < 104 < 105$.

Honest Two-Layer Verification Scope.

1. **Layer 1 (Lean 4.35.0 Kernel, Standalone Sub-Lemmas):** `lean/CogenticL13Factorization.lean` proves 18 standalone constructive algebraic, lattice, 3-adic Hensel, and rational-contraction sub-lemmas (Table 1) extracted from Propositions 2.2–2.3, Lemmas 2.8, 4.2, 5.1–5.3, and Theorem 1.1 of [6].
2. **Layer 2 (Exact Zero-Float Auditor):** `L13FACT-COGENTIC-CERT-1.0` audits 16 finite exact witnesses across mod-N (3/4)-LLL lattices and Lagrange–Gauss ratio splits ($N \le 100{,}160{,}063$), mod-3-pinned forms ($d \in \{3, 5\}$) with geometric ladders and smooth special-q points, 3-adic Newton–Hensel lifting traces ($K \le 5$), and end-to-end two-field blinded Dixon splits ($N \le 64{,}507$).
3. **Explicit Non-Claims:** We do *not* formalize in Lean 4 Gevrey-2 Mellin cutoffs, hybrid large sieves, truncated Brun sieves, Siegel-zero-free local Euler cancellation (Section 3), discrete Laplace sub-averaging and backward path telescoping (Lemmas 4.3–4.6), Stark–Chebotarev/Landau–Page density bounds (Lemma 5.1(3)), AKS pri-

*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 zero-float verifiers, and adversarial tests were independently compiled and verified locally. Repository: github.com/lluiseriksson/cogentic-l13-factorization-certificates.

mality [1], or multitape Turing-machine bit-cost accounting (Section 6); those analytic pillars remain unverified outside the companion preprint [6].

2 Constructive Lean 4.35.0 Kernel

`lean/CogenticL13Factorization.lean` compiles standalone under Lean 4.35.0 [4] with zero external imports, zero warnings, zero `sorry`, and zero `Classical.choice`. Auditing via `AuditAxioms.lean` confirms 4 zero-axiom theorems (`none`: #9, #15, #17, #18) and 14 `[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, Theorems 4–6 prove Lagrange–Gauss quadratic-form coercivity, determinant bounds, and ratio-split injectivity over $\mathbb{Z}$; Theorems 8 and 11 prove the exact geometric ladder identity $7\sum 9^t 16^{r-1-t} + 9^r = 16^r$ and layer-cake telescoping universally by induction; Theorems 12–14 prove $4 \mid (3^{2k+1}+1)$ and quadratic Newton–Hensel convergence ($M \to M^2$); Theorem 15 constructively exhibits a nonzero kernel vector in $\mathbb{F}_2^3 \to \mathbb{F}_2^2$ with zero axioms; and Theorems 17–18 certify Theorem 1.1's strong-induction runtime ($103.70 < 104 < 105$) and workspace ($37.40 < 38 < 40$) contractions via exact integer cubes.

3 Exact Zero-Float Certificate Auditor

The modules `l13fact_exact.py` and `l13fact_certifier.py` (under `src/`) use exclusively Python `int`, `fractions.Fraction`, and exact `math.gcd` (statically audited via `ast.walk` for zero float/complex literals, true division `/`, or floating-point `math.*` calls). Deterministic primality uses 13-base Miller–Rabin (bases $2 \ldots 41$, exact below 3.317×10^{24}). Strict JSON parsing rejects floats, `NaN`/`Infinity`, and duplicate keys via `parse_float`, `parse_constant`, and `object_pairs_hook`.

Definition 1 (`L13FACT-COGENTIC-CERT-1.0` Predicates)**.** A certificate with `protocol="L13FACT-COGENTIC-CERT-1.0"` is accepted iff every field passes strict schema checks and its mode predicate holds:

- **Mode 1 (`mod_n_lattice_and_lagrange_split_cert`):** Audits odd $N \geq 15$, $g_1 m_N \equiv g_0 \pmod N$, $g_1^{n-1} > N/2$, exact Λ_n membership of every column of B_{lat}, Bareiss $|\det B_{\text{lat}}| = N$, integer adjugate $A_{\text{adj}} B_{\text{lat}} = N I_n$, exact rational (3/4)-LLL reduction and Prop. 2.2(1) bound $\|b_j\|_2^2 \leq 2^{n+3} G^2$, plus 2D Lagrange–Gauss reduction (v_1, v_2) on L_z ($z \equiv st^2 \pmod N$) and smooth split $(x_1, y_1) = (\prod_{p \in A} p, \prod_{q \in B} q)$ on disjoint r_0-prime sets $A, B \subseteq [2, Q]$ with $4Q^{2r_0} \leq N$.
- **Mode 2 (`mod3_laplace_ladder_and_smooth_cert`):** Audits $\gcd(N, 6) = 1$, $3 \mid M$, $6W \leq M$, Rabin irreducibility of monic odd-degree $h_0 \in \mathbb{F}_3[X]$, mod-3-pinned form $f_{\tilde{c}}(g_0, g_1) \equiv 0 \pmod N$, strictly decreasing ladder $Y_0 > \cdots > Y_J \geq 2$, special-$q$ root $f_{\tilde{c}}(r_q, 1) \equiv 0 \pmod q$, primitive lattice point $(a, b) \in \Lambda_{q, r_q}$ with $3 \nmid f_{\tilde{c}}(a, b)$ and non-vacuously smooth cofactor $f_{\tilde{c}}(a, b)/q$ ($2 \leq \text{cap} < \text{cofactor}$), and exact layer-cake telescoping.
- **Mode 3 (`adic3_newton_hensel_sqrt_cert`):** Audits monic odd-degree $\tilde{f} \in \mathbb{Z}[X]$ irreducible mod 3, $4 \mid (3^d + 1)$, $\tilde{\Gamma} = \tilde{f}'(\theta)^2 \prod (c_d a_\nu - b_\nu \theta)$, independent Euler square check and lifting trace (β_k, γ_k) satisfying $\beta_k^2 \equiv \tilde{\Gamma} \pmod{3^{2^k}, \tilde{f}}$ and $2\beta_k\gamma_k \equiv 1 \pmod{3^{2^{\max(0,k-1)}}, \tilde{f}}$, balanced bound $|\hat{b}_j| \leq (3^{2^K} - 1)/2$, and exact global square $\hat{\beta}(X)^2 \equiv \tilde{\Gamma}(X) \pmod{\tilde{f}}$ in $\mathbb{Z}[X]$.
- **Mode 4 (`dixon_character_and_induction_split_cert`):** Audits odd composite N, canonical $0 \leq m_N, Y, Z < N$, two mod-3-pinned forms (f_1, f_2) vanishing at $(g_0, g_1) \pmod N$, degree-1 Adleman characters (ℓ, s) with $\tilde{f}_\iota(s) \equiv 0 \pmod \ell$, per-relation nonempty algebraic factor lists and Eq. (6.1) congruences with $w_m \equiv z_m^2 \pmod N$, $\mathbb{F}_2$ right-nullspace mask, both Lemma 5.2 3-adic roots $(\hat{\beta}_1, \hat{\beta}_2)$, exact $Y^2 \equiv Z^2 \equiv \prod_{T_x} w_m \pmod N$, nontrivial split $1 < \gcd(Z - Y, N) < N$, and Theorem 1.1 integer-cube contraction guards.

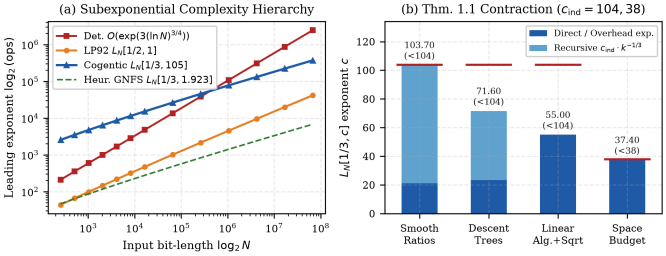

Figure 1: **(a)** Leading-term bit-operation exponents comparing deterministic $O(\exp(3(\ln N)^{3/4}))$, Lenstra–Pomerance $L_N[1/2, 1]$, Cogentic $L_N[1/3, 105]$, and heuristic GNFS $L_N[1/3, 1.923]$. **(b)** Theorem 1.1 strong-induction exponent contraction budgets ($103.70 < 104 < 105$ runtime; $37.40 < 38 < 40$ deterministic workspace).

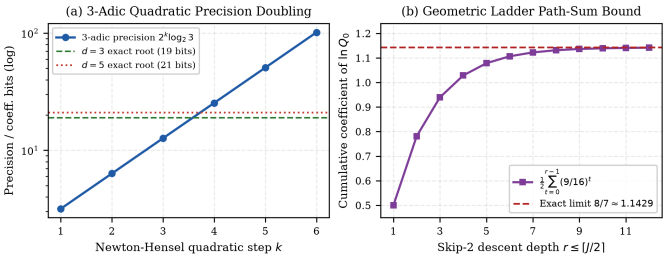

Figure 2: **(a)** Deterministic 3-adic Newton–Hensel quadratic precision doubling $2^k \log_2 3$ recovering exact global square roots at $k = 4$ (25.36 bits) for $d = 3$ (19-bit root) and $d = 5$ (21-bit root). **(b)** Exact skip-2 geometric ladder path sum $\frac{1}{2}\sum_{t=0}^{r-1} (9/16)^t$ monotonically bounded by $8/7 \approx 1.1429$.

Table 1: Complete inventory of all 18 constructive Lean 4.35.0 sub-lemmas in `lean/CogenticL13Factorization.lean` (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; `none` for #9, #15, #17, #18 and `[propext, Quot.sound]` (`P,Q`) for the remaining 14).

#	Theorem Identifier	Ref. [6]	Exact Machine-Checked Statement & Hypotheses	Ax.
1	`prop22_lll_basis_norm_bound`	Prop. 2.2	$1 \le j \le n \implies (4 \cdot 2^{n-j} + (2^n - 2^{n-j+1}))S \le 4 \cdot 2^{n-1} S$.	P,Q
2	`prop22_dual_lattice_gap`	Prop. 2.2	$0 < t$, $2t < N$, $N < 2g_1^{n-1}$, $g_1^{n-1} \mid t \implies$ False (dual gap).	P,Q
3	`prop22_box_inclusion_margin`	Prop. 2.2	$\eta \ge 2$, $W_{\min} \le W_i$, $6\eta \le W_{\min} \implies (W_i{+}1)(W_{\min}{-}6\eta) \le (W_i{+}1{-}(4\eta{+}2))W_{\min}$.	P,Q
4	`prop23_lagrange_gauss_quad_form`	Prop. 2.3	$0 \le n_1 \le n_2$, $\lvert 2g\rvert \le n_1 \implies x_1^2 n_1 + x_2^2 n_2 \le 2(x_1^2 n_1 + 2x_1 x_2 g + x_2^2 n_2)$.	P,Q
5	`prop23_lagrange_det_bounds`	Prop. 2.3	$0 \le n_1 \le n_2$, $4g^2 \le n_1^2 \implies 3n_1 n_2 \le 4(n_1 n_2 - g^2) \le 4 n_1 n_2$.	P,Q
6	`prop23_ratio_split_injective`	Prop. 2.3	$0 \le H$, $4H^2 \le N$, $u_i, v_i \in [1, H]$, $N \mid (u_1 v_2 - u_2 v_1) \implies u_1 v_2 = u_2 v_1$.	P,Q
7	`prop23_alternating_sign_nonneg`	Prop. 2.3	$2K \le M_Q$, $4r_0^2 M_Q \le (s{-}2r_0)^2$, $j < r_0 \implies 2(K{-}j)(2r_0{-}2j)(2r_0{-}2j{-}1) \le (j{+}1)(s{-}2r_0{+}2j{+}2)(s{-}2r_0{+}2j{+}1)$.	P,Q
8	`lem28_ladder_geometric_sum`	Lem. 2.8	$\forall r \in \mathbb{N}$, $7\sum_{t=0}^{r-1} 9^t 16^{r-1-t} + 9^r = 16^r$ (certifies $\frac{8}{7} \ln Q_0$).	P,Q
9	`lem28_exponent_ratio_identities`	Lem. 2.8	Ground schedule ratios: $8+1+8=17$, $3 \cdot 6 - 1 = 17$, $17 \cdot 6 = 102 < 108$.	none
10	`lem42_mod3_irreducible_nondiv`	Lem. 4.2	$\neg(3 \mid a \wedge 3 \mid b)$, $(3 \mid b \Rightarrow f\%3 = a^d\%3)$, $(3 \nmid b \Rightarrow f\%3 \ne 0) \implies 3 \nmid f$.	P,Q
11	`lem42_laplace_layer_cake_telescope`	Lem. 4.2	$\forall z \in \mathbb{Z}$, $a, m \in \mathbb{N}$, $(1-z)\,\mathrm{tail}(z,a,m) = (2a+1)z^a(1-z) + 2(z^{a+1} - z^{a+m+1})$.	P,Q
12	`lem52_three_pow_odd_div_four`	Lem. 5.2	$\forall k \in \mathbb{N}$, $4 \mid (3^{2k+1} + 1)$ (exact $\mathbb{F}^{\times}_{3^d}$ root exponent).	P,Q
13	`lem52_newton_inv_quad_step`	Lem. 5.2	$\forall M, b, g \in \mathbb{Z}$, $M \mid (1 - 2bg) \implies M^2 \mid (1 - 2b(g(2 - 2bg)))$.	P,Q
14	`lem52_newton_sqrt_quad_step`	Lem. 5.2	$M \mid (b^2 - G)$, $M \mid (1 - 2bg') \implies M^2 \mid ((b + (G - b^2)g')^2 - G)$.	P,Q
15	`lem51_kernel_dim_pigeonhole`	Lem. 5.1	$\forall v_1, v_2, v_3 \in \mathbb{F}_2^2$, $\exists \lambda \in \mathbb{F}_2^3 \setminus \{0\}$, $\lambda_1 v_1 \oplus \lambda_2 v_2 \oplus \lambda_3 v_3 = (0,0)$.	none
16	`lem53_dixon_congruence_split`	Lem. 5.3	$Y \le Z$, $N \mid (Z{-}Y)(Z{+}Y)$, $N \nmid (Z{-}Y)$, $N \nmid (Z{+}Y) \implies \neg\mathrm{Cop}(N, Z{-}Y) \wedge \neg\mathrm{Cop}(N, Z{+}Y)$.	P,Q
17	`thm11_runtime_contraction_105`	Thm. 1.1	$104^3 \cdot 100^3 < 2 \cdot 8255^3$, $2115{+}8255 < 10372 < 10400 < 10500$, $104^3 \cdot 100^3 < 10 \cdot 4828^3$, $7160 < 10400$.	none
18	`thm11_workspace_and_phase_success`	Thm. 1.1	$38^3 \cdot 100^3 < 2 \cdot 3017^3$, $3740 < 3800 < 4000$, and $3 \cdot 29106 > 80000$ ($> 1/3$).	none

4 Exact Findings, Worked Witnesses, and Audit

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

1. Complexity Regimes, 3-Adic Convergence & Ladder Geometry (Figs. 1–2). Figure 1(b) confirms Theorem 1.1's strong-induction margins: recursive calls on $[2, \lfloor \frac{1}{2}\sqrt{N} \rfloor]$ shrink the $c_{\text{ind}} = 104$ exponent by $2^{-1/3}$ to $82.5448\cdots < 82.55$, so smooth-ratio collection sums to $21.15 + 82.55 = 103.70 < 103.72 < 104 < 105$, while descent-tree recursion on $[2, N^{1/10}]$ shrinks by $10^{-1/3}$ to $48.2725\cdots < 48.28$ (total $71.60 < 104$), and workspace contracts via $38 \cdot 2^{-1/3} < 30.17$ ($37.40 < 38 < 40$). In Figure 2(a), deterministic 3-adic quadratic lifting doubles precision from 3.17 to 101.44 bits in $k = 6$ steps (0.159 ms for $d = 3$, 0.393 ms for $d = 5$), crossing both 19-bit and 21-bit global roots cleanly at $k = 4$ (25.36 bits). Figure 2(b) verifies exact rational convergence of $\frac{1}{2}\sum_{t=0}^{r-1}(9/16)^t$ to 8/7 across depths $r = 1 \ldots 12$.

2. Hand-Verifiable Worked Exact Witnesses (One per Mode).

- **Mode 1 (`C01`, $N = 101 \cdot 103 = 10{,}403, G = 50, g_0 = 79, g_1 = 83, n = 3$):** $83 \cdot 1505 \equiv 79 \pmod{10403}$, $83^2 = 6889 > 5201.5$; (3/4)-LLL basis columns $(-8,-10,-9)^\top, (7,12,-12)^\top, (-34,17,-2)^\top$ have $|\det B_{\text{lat}}| = 10{,}403$, $\max \|b_j\|_2^2 = 1449 \le 2^6 \cdot 50^2 = 160{,}000$, and $A_{\text{adj}} B_{\text{lat}} = 10{,}403 I_3$; for $s = 8934, t = 17$, $z = 1982 \equiv 10 \cdot 21^{-1} \pmod{10403}$, Lagrange–Gauss returns $v_1 = (10, 21) = (2 \cdot 5, 3 \cdot 7)$ ($Q = 7, 4 \cdot 7^4 = 9604 \le 10403$).
- **Mode 2 (`C05`, $N = 323, d = 3, M = 180, W = 25, h_0 = X^3 + 2X + 1$):** With $\tilde{c} = (-15, -25, -18, 0)$, $f_{\tilde{c}}(X, Y) = 256X^3 - 54X^2Y - 73XY^2 - 44Y^3$ satisfies $f_{\tilde{c}}(7, 11) = -61{,}693 = 323 \cdot (-191) \equiv 0 \pmod{323}$ and $f_{\tilde{c}}(10, 1) \equiv 0 \pmod{23}$; primitive point $(33, 1) \in \Lambda_{23,10}$ gives $f_{\tilde{c}}(33, 1)/23 = 397{,}331 = 11 \cdot 41 \cdot 881$ (2500-smooth, $3 \nmid 397{,}331$).
- **Mode 3 (`C09`, $\tilde{f} = X^3 + 2X + 1$, $K = 3$, $3^8 = 6561$):** Pairs $(2,1)^2(3,1)^2$ yield $\beta_0 = \theta^2 + \theta$, $\beta_1 = 4\theta^2 + \theta$, $\beta_2 = 67\theta^2 + 64\theta + 54$, $\beta_3 = 6547\theta^2 + 6544\theta + 6534 \pmod{6561}$, balancing to exact $\hat{\beta}(X) = -14X^2 - 17X - 27 \in \mathbb{Z}[X]$ with $\hat{\beta}(\theta)^2 \equiv \tilde{\Gamma}(\theta) \pmod{\tilde{f}}$.
- **Mode 4 (`C13`, $N = 17 \cdot 19 = 323, g_0 = 7, g_1 = 11, m_N = 30$):** Mod-3-pinned forms (ascending coefficients) $f_1 = (-44, -73, -54, 256)$ and $f_2 = (-37, -73, -69, 259)$ with 6 Adleman characters and 4 blinded relations yield $\mathbb{F}_2$-nullspace mask $[1, 1, 0, 0]$ ($w_0 = 254 = 106^2, w_1 = 172 = 227^2 \pmod{323}$); $K = 5$ 3-adic roots (ascending) $\hat{\beta}_1 = (18219008, 92672, -1482)$ and $\hat{\beta}_2 = (-22136730, -145040, 2262)$ assemble $Y = 27$, while unsealing gives $Z = 106 \cdot 227 \equiv 160 \pmod{323}$

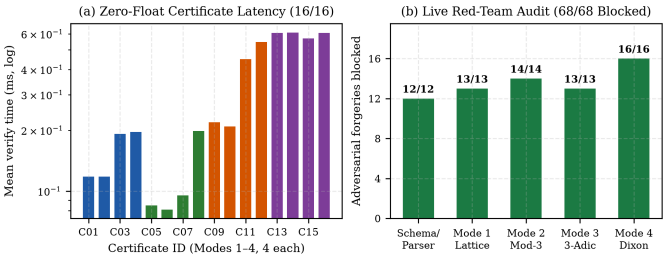

Figure 3: **(a)** Mean exact zero-float verification latency across all 16 canonical certificates (0.081–0.609 ms, log scale). **(b)** Live adversarial red-team audit rejecting 68/68 forgeries across five attack classes with exact error-branch assertions.

Table 2: Canonical 16-certificate `L13FACT-COGENTIC-CERT-1.0` atlas (`exp1_certificate_atlas.json`; all 16 verified).

Certificate ID	M	Exact Certified Witness Summary	ms
`m1_lattice_lagrange_n10403_d3`	M1	N=10403, n=3: r_0=2, (10, 21), λ_1^2=541	0.118
`m1_lattice_lagrange_n64507_d3`	M1	N=64507, n=3: r_0=2, (33, 35), λ_1^2=2314	0.118
`m1_lattice_lagrange_n256027_d4`	M1	N=256027, n=4: r_0=2, (26, 55), λ_1^2=3701	0.192
`m1_lattice_lagrange_n100160063_d4`	M1	N=100160063, n=4: r_0=3, (238, 429)	0.196
`m2_mod3_laplace_n323_d3`	M2	N=323, d=3: q=23, P^+=881 $\leq$ 2500	0.085
`m2_mod3_laplace_n1763_d3`	M2	N=1763, d=3: q=29, P^+=233 $\leq$ 8000	0.081
`m2_mod3_laplace_n10403_d3`	M2	N=10403, d=3: q=37, P^+=3989 $\leq$ 25000	0.095
`m2_mod3_laplace_n1763_d5`	M2	N=1763, d=5: q=47, P^+=56489 $\leq$ 60000	0.198
`m3_adic3_sqrt_d3_p2_k3`	M3	d=3, 4 pairs, K=3: max $\lvert\dot{b}_j\rvert$=27	0.219
`m3_adic3_sqrt_d3_p3_k4`	M3	d=3, 6 pairs, K=4: max $\lvert\dot{b}_j\rvert$=408320	0.209
`m3_adic3_sqrt_d5_p2_k4`	M3	d=5, 4 pairs, K=4: max $\lvert\dot{b}_j\rvert$=47	0.450
`m3_adic3_sqrt_d5_p3_k5`	M3	d=5, 6 pairs, K=5: max $\lvert\dot{b}_j\rvert$=1761280	0.547
`m4_dixon_split_n323_17x19`	M4	17·19: 6 chars, K=5, Y=27, Z=160 $\to$ 19	0.606
`m4_dixon_split_n1763_41x43`	M4	41·43: 6 chars, 3-adic roots $\to$ 43	0.609
`m4_dixon_split_n10403_101x103`	M4	101·103: 6 chars, 3-adic roots $\to$ 103	0.570
`m4_dixon_split_n64507_251x257`	M4	251·257: 6 chars, 3-adic roots $\to$ 257	0.607

$(27^2 \equiv 160^2 \equiv 83 \pmod{323})$ and $\gcd(160-27, 323) = \gcd(133, 323) = 19$.

3. 16-Certificate Atlas & 74-Test Red-Team Audit (Table 2, Fig. 3). Table 2 lists all 16 canonical certificates verified in 0.081–0.609 ms. `tests/test_suite.py` runs 74 pytest checks: 1 full 16-certificate replay, 3 raw-JSON parser guards (float, `NaN`, duplicate keys), 2 exact regressions (rejecting the 12-base Sorenson–Webster strong pseudoprime 318,665,857,834,031,151,167,461 and rejecting non-squares in $\mathbb{F}_{3^d}^{\times}$), and 68 parametrized live adversarial forgeries (12 schema/parser + 13 Mode 1 + 14 Mode 2 + 13 Mode 3 + 16 Mode 4), each asserting an exact regex on its intended `CertificateError` branch. `scripts/verify_all.py` enforces all 5 gates including strict axiom whitelisting and a 41-file SHA-256 manifest.

5 Conclusion

We built an independent, explicitly scoped, zero-floating-point verification companion for the discrete lattice, mod-3 Laplace ensemble, deterministic 3-adic Newton–Hensel square-root, blinded Dixon splitting, and strong-induction mechanisms of the Cogentic $L_N[1/3, 105]$ integer factorization preprint [6, 3], pairing 18 constructive Lean 4.35.0 sub-lemmas (zero `sorry`, zero `Classical.choice`) with the pure-`int`/`Fraction` 4-mode auditor `L13FACT-COGENTIC-CERT-1.0`, 16 canonical exact finite witnesses, and 68/68 live adversarial forgery rejections.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] J. P. Buhler, H. W. Lenstra, Jr., and Carl Pomerance. Factoring integers with the number field sieve. In *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, pages 50–94. Springer-Verlag, 1993.

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

[4] 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.

[5] John D. Dixon. Asymptotically fast factorization of integers. *Mathematics of Computation*, 36(153):255–260, 1981.

[6] Google Research Cogentic. Unconditional subexponential integer factorization in time $L_N[1/3, 105]$. Unrefereed Companion Preprint (Google Research Cogentic), November 2026. Proposes a uniform zero-error Las Vegas multitape Turing machine factoring every integer $N \geq 2$ in expected time $L_N[1/3, 105]$ and deterministic space $L_N[1/3, 40]$.

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[8] H. W. Lenstra, Jr. and Carl Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3):483–516, 1992.