Constructive Lean 4 Kernel and Exact Zero-Float Certificates for Google Research Cogentic's Deterministic Subexponential Factoring and QNR Breakthrough

Lluis Eriksson*

November 25, 2026

Abstract

A November 25, 2026 companion preprint from Google Research's Cogentic framework [4, 2] proposes an unconditional deterministic subexponential general integer factoring algorithm with claimed worst-case bit complexity $O(\exp(3(\ln N)^{3/4}))$, together with deterministic subexponential order splitting and prime quadratic nonresidue (QNR) construction in $O(\exp(C_{\text{split}}(\ln p)^{1/2}\ln\ln(p+16)))$—targeting improvements over both Harvey's exponential $N^{1/5+o(1)}$ factoring bound and Burgess–Vinogradov's exponential $\tilde{O}(p^{1/(4\sqrt{e})})$ QNR bound with zero randomness and zero Riemann-hypothesis assumptions. Rather than assuming peer-reviewed endorsement of the preprint's analytic pillars, we deliver an independent, explicitly scoped, zero-floating-point verification companion for its finite algebraic, congruence, fixed-point, and combinatorial mechanisms. Layer 1 (`CogenticDetFactoring.lean`) proves 18 standalone constructive Lean 4.35.0 algebraic and arithmetic sub-lemmas (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; 3 zero-axiom `none` and 15 `[propext, Quot.sound]`), covering divisor soundness, biquadratic square-root compatibility, the integer floor step $81 < 4D \Rightarrow 21 \le D$, fixed-point recurrence inequalities, 2×2 unimodular Bézout elimination, primorial product and rational density margins, Miller 2-Sylow splitting, Gauss reduction ideal closure, biquadratic $\mathbb{F}_2$-linearity and $K = 2$ Walsh–Hadamard orthogonality, Burgess exponent gap arithmetic, 2×2 bordered-adjugate Schur complements, two-field unit annihilation, base-m evaluation invariance, subgroup-index saturation, and Theorem 1.3 numeric guard inequalities. Layer 2 (`DETFACT-COGENTIC-CERT-1.0`) is a pure-stdlib Python `int`/`Fraction` 4-mode auditor certifying 16 canonical finite witnesses in 0.010–1.978 ms and rejecting 66/66 live adversarial forgeries with exact branch assertions (72/72 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 zero-float verifiers, and adversarial tests were independently compiled and verified locally. Repository: github.com/lluiseriksson/cogentic-deterministic-factoring-certificates.

1 Introduction and Scope Calibration

Unconditional deterministic general integer factoring stalled at exponential $N^{c+o(1)}$ complexity for half a century—improving from Pollard–Strassen's $N^{1/4+o(1)}$ to Harvey's $N^{1/5+o(1)}$ [5]—while unconditional deterministic construction of a prime quadratic nonresidue (or a Miller order-splitting witness [7]) stalled at Burgess–Vinogradov's $\tilde{O}(p^{1/(4\sqrt{e})}) \approx p^{0.151633}$ [1]. The companion Cogentic preprint [4, 2] proposes breaking both exponential walls unconditionally via two coupled deterministic engines:

1. **Part 1 (Multiquadratic Infrastructure, Walsh–Hadamard Positivity & Order Splitting, Sec. 2–6):** Running Miller's 2-Sylow test on $q_0 = -1, q_1, \ldots, q_K$ either splits N immediately or extracts $2^K - 1$ pairwise-compatible modular square roots (d_ℓ, s_ℓ) across quadratic fields $F_\ell = \mathbb{Q}(\sqrt{d_\ell})$ and biquadratic composita E_{ℓ_1,ℓ_2}. Enumerating units and short ideals via Gauss reduction and 4D weighted LLL [6] yields Walsh–Hadamard positivity $b_0(n) + \sum_{\ell\neq 0} b_\ell(n) = 2^K \hat{b}_0(n) \ge 0$ (amplifying Y-smooth integers by 2^K), which [4] contrasts against a sixteenth-moment quadratic-field Burgess bound to claim QNR/order-splitting time $O(\exp(C_{\text{split}}(\ln p)^{1/2}\ln\ln(p+16)))$.
2. **Part 2 (Base-m Pairs, Two-Field Unit Annihilation & Saturation, Sec. 7–11):** Deterministic preconditioned base-m pairs (f_1, f_2) produce joint squarefree smooth relations; bordered-adjugate linear algebra and two-field localization (`TryPair`) extract even prime-annihilating exponents E_ℓ ($\ell^{E_\ell} \equiv 1 \pmod N$); and multiplying by $L_{\text{idx}} = \text{lcm}(1, \ldots, K_{\text{idx}})$ saturates $(p-1) \mid \tilde{M}$ across every $p \mid N$ in claimed time $O(\exp(3(\ln N)^{3/4}))$.

Honest Two-Layer Verification Scope.

1. **Layer 1 (Lean 4.35.0 Kernel, Standalone Sub-Lemmas):** `lean/CogenticDetFactoring.lean` proves 18 standalone constructive algebraic, congruence, and exact rational-margin sub-lemmas (Table 1) extracted from Sections 1–11 of [4].
2. **Layer 2 (Exact Zero-Float Auditor):** `DETFACT-COGENTIC-CERT-1.0` audits 16 finite exact instances ($N \le 4{,}028{,}033$) across Miller 2-Sylow splitting and compatible multiquadratic roots, real-quadratic Gauss

cycles and Walsh–Hadamard sums ($K \le 4$), fixed-point `ApproxLog`/`ApproxSqrt` + `ModHNF` ($m \le 4$) + bordered-adjugate `TryPair` ($k \le 5$), and Lemma 8.1 base-m pairs + Lemma 11.1 saturation.

3. **Explicit Non-Claims:** We do *not* formalize in Lean 4 Minkowski's discriminant bound, Chebyshev's primorial theorem, Bertrand density, general m-dimensional `ModHNF` or $k\times k$ bordered adjugates (Table 1 #3, #6–#8, #12–#14, #18 formalize only the elementary arithmetic/2D/$K = 2$ steps explicitly printed in Table 1), 4D LLL regulator walks (Lemma 4.2(2)), Weil–Schmidt character sums/16th-moment Burgess bounds (Proposition 6.2, Lemma 6.3), Landau–Page/Montgomery estimates (Section 9), or centered Gram peeling (Section 10); those analytic pillars remain unverified outside the companion preprint [4].

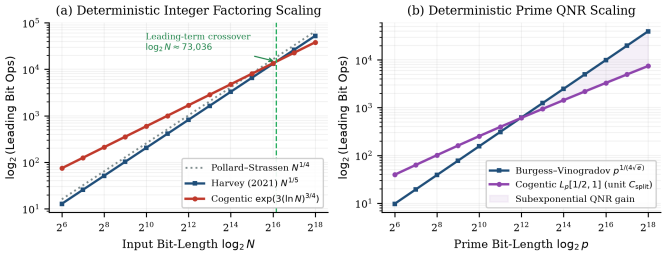

Figure 1: **(a)** Leading-term bit-operation exponents: Pollard–Strassen ($N^{1/4}$), Harvey ($N^{1/5}$), and Cogentic ($\exp(3(\ln N)^{3/4})$, crossing $N^{1/5}$ at $\log_2 N \approx 73{,}036$). **(b)** Prime QNR scaling: Burgess–Vinogradov $p^{1/(4\sqrt{e})}$ vs. the subexponential curve $\exp((\ln p)^{1/2}(\ln\ln p)^{1/2})$ (for reference; the companion preprint's Theorem 1.2 states $O(\exp(C_{\text{split}}(\ln p)^{1/2}\ln\ln(p+16)))$).

2 Constructive Lean 4.35.0 Kernel

`lean/CogenticDetFactoring.lean` compiles in 1.4 s under Lean 4.35.0 [3] with zero external imports, zero warnings, zero `sorry`, and zero `Classical.choice`. Auditing via `AuditAxioms.lean` confirms 3 zero-axiom theorems (`none`: #8, #13, #18) and 15 `[propext, Quot.sound]` theorems (`P,Q`; Table 1).

Proposition 1 (Constructive Lean 4 Kernel Scope)**.** All 18 theorems in Table 1 compile constructively under Lean 4.35.0 without external libraries or classical axioms (`Classical.choice`). Notably, Theorem 2 proves biquadratic modular square-root compatibility over $\mathbb{Z}$, Theorem 10 proves closed-form Gauss reduction ideal closure $4a' \mid (D - b'^2)$, Theorem 15 proves two-field localization annihilation $(L^2 - 1)P^2 \equiv 0 \pmod N$, and Theorem 17 proves subgroup-index saturation $(p_j - 1) \mid M^* L_{\text{idx}}$.

3 Exact Zero-Float Certificate Auditor

The modules `detfact_exact.py` and `detfact_certifier.py` (under `src/`) use exclusively Python `int`, `fractions.Fraction`, and exact integer `math.gcd`/`isqrt` (statically audited via `ast.walk` for zero floating-point literals or imports). Deterministic primality uses 13-base Miller–Rabin (bases $2 \ldots 41$, proven exact below 3.317×10^{24}). Strict JSON loading rejects duplicate keys, floats, `NaN`/`Infinity`, nesting depth > 16, and non-ASCII digits.

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

- **Mode 1 (`miller_multiquadratic_compat_cert`):** Runs exact Section 3 Miller 2-Sylow order testing on $\{-1, q_1, \ldots, q_K\}$ given odd $N \ge 9$ and even $\tilde{M}$ (including deterministic ratio-splitting on non-cyclic 2-Sylow subgroups), verifying either `SPLIT` ($1 < d < N$, $N\%d = 0$) or `COMPATIBLE_FAMILY` ($2^K - 1$ squarefree $d_\ell \ne 1$, $s_\ell^2 \equiv d_\ell \pmod N$, and all $\binom{2^K-1}{2}$ pairwise biquadratic congruences $s_{\ell_1} s_{\ell_2} \equiv \eta_{12} s_{\ell_1+\ell_2} \pmod N$).
- **Mode 2 (`quadratic_infrastructure_wh_cert`):** Audits odd prime q, exact QNR witness $(z/q) = -1$ via Euler's criterion, biquadratic family compatibility mod q with $d_\ell \mid P_K$, exact Lemma 4.2(1) real-quadratic Gauss reduction cycle $\mathcal{R}_D$ and fundamental unit $x_u^2 - Dy_u^2 = \pm 4$, and exact Lemma 5.1(2)–(3) Walsh–Hadamard nonnegativity $b_0(n) + \sum_{\ell \ne 0} b_\ell(n) = 2^K \hat{b}_0(n) \ge 0$ ($\hat{b}_0(n) \ge 1$ for Y-smooth n) with $(2^K - 1)\max_\ell S_\ell \ge 2^K \Psi - \sum b_0$.
- **Mode 3 (`fixedpoint_hnf_and_trypair_cert`):** Verifies Lemma 2.2(1) `ApproxLog`, Lemma 2.2(3) `ApproxSqrt` with direct integer squaring brackets $(n_s - 1)^2 v \le u \cdot 2^{2M} < (n_s + 1)^2 v$, Lemma 2.2(4) upper-triangular column `ModHNF` in $\mathbb{Z}^m$ ($m \le 4$), and Lemmas 7.4–7.5 exact bordered-adjugate $B\,\mathrm{adj}(B) = (\det B) I_k$ plus two-field localization annihilation $\ell^{2E_0 Q_{\text{lcm}}} \equiv 1 \pmod N$.
- **Mode 4 (`base_m_saturation_and_factor_cert`):** Audits non-perfect-power semiprime $N = p_1 p_2$, Lemma 8.1 base-m pair (f_1, f_2) ($(m-1)^d < N < m^d$, shared odd $c_d \ge 4P_0\ell$, Rabin irreducibility in $\mathbb{F}_2[X]$, $f_i(m) = k_i N$, $f_i(a) \equiv 1 \pmod{P_0}$, f_1 splits into d simple roots mod ℓ, f_2 root-free mod ℓ), and Lemma 11.1 saturation ($\ell^{M^*} \equiv 1 \pmod N$ for $\ell \in P_{\text{ok}}$, $L_{\text{idx}} = \mathrm{lcm}(1..K_{\text{idx}})$, $(p_1 - 1), (p_2 - 1) \mid M^* L_{\text{idx}}$).

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 Crossovers, Walsh–Hadamard Sums & Gauss Cycles (Figs. 1–2). Equating leading expo-

Table 1: Complete inventory of all 18 constructive Lean 4.35.0 theorems in `lean/CogenticDetFactoring.lean` (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; `none` for #8, #13, #18 and `[propext, Quot.sound]` (`P,Q`) for the remaining 15).

#	Theorem Identifier	Ref. [4]	Exact Machine-Checked Statement & Hypotheses	Ax.
1	`thm11_factor_divisor_sound`	Thm. 1.1	$1 < d < N \wedge N\%d = 0 \implies \exists k,\ 1 < k < N \wedge dk = N.$	`P,Q`
2	`lem21_biquadratic_compat_norm`	Sec. 2.1	$s_i^2 \equiv d_i,\ d_1 d_2 = \eta_{12}^2 d_3,\ s_1 s_2 \equiv \eta_{12} s_3 \pmod N \implies N \mid \eta_{12}^2(s_3^2 - d_3).$	`P,Q`
3	`lem21_minkowski_biquadratic_disc_21`	Lem. 2.1	$\forall D \in \mathbb{N},\ 81 < 4D \implies 21 \le D$ (integer floor step).	`P,Q`
4	`lem22_approx_log_recurrence_error`	Lem. 2.2	$e < 2S,\ f < S,\ 9p^2 \le q^2,\ q \ge 1 \implies ep^2 + fq^2 < 2Sq^2.$	`P,Q`
5	`lem22_approx_exp_squaring_error`	Lem. 2.2	$\forall a, S, d \in \mathbb{N},\ a \le S \implies S^2 - (S-a)^2 + dS \le 2aS + dS.$	`P,Q`
6	`lem22_mod_hnf_unimodular_det`	Lem. 2.2	$g \ge 1,\ p_i = ga',\ c_i = gb',\ up_i + vc_i = g \implies ua' + vb' = 1 \wedge (-b')p_i + a'c_i = 0.$	`P,Q`
7	`lem23_chebyshev_primorial_step`	Lem. 2.3	$\forall k \in \mathbb{N},\ P \le 4^{k+1} \wedge Q \le 4^k \implies PQ \le 4^{2k+1}.$	`P,Q`
8	`lem23_bertrand_density_2048`	Lem. 2.3	$2/3 - 781/2048 = 1753/6144 > 1/4$ and $12 \cdot 2047 \cdot 69 > 16384 \cdot 100.$	none
9	`lem31_miller_2sylow_split_sound`	Sec. 3	$N \mid (x-1)(x+1),\ N \nmid (x-1),\ N \nmid (x+1) \implies \neg\mathrm{Cop}(N, x-1) \wedge \neg\mathrm{Cop}(N, x+1).$	`P,Q`
10	`lem42_gauss_reduction_ideal_norm`	Lem. 4.2	$D - b^2 = 4aa' \wedge b' = 2a'q_0 - b \implies \exists m \in \mathbb{Z},\ D - b'^2 = 4a'm.$	`P,Q`
11	`lem51_biquadratic_cocycle_f2_linear`	Lem. 5.1	$u_{++}^2 = 1 \implies (u_{++}u_{+-})(u_{++}u_{-+})(u_{++}u_{--}) = u_{++}u_{+-}u_{-+}u_{--}.$	`P,Q`
12	`lem51_walsh_hadamard_orthogonality_2`	Lem. 5.1	$\forall h_0, h_1, h_2, h_3 \in \mathbb{Z},\ \sum_{\ell \in \mathbb{F}_2^2} \sum_w h_w (-1)^{\ell \cdot w} = 4h_0.$	`P,Q`
13	`lem63_burgess_exponent_gap`	Lem. 6.3	$40000 + 2 \cdot 16825 = 73650 < 100000\ (WA^2 < q)$ and $25/4000 < 40/4000.$	none
14	`lem74_bordered_adjugate_schur_2x2`	Lem. 7.5	$\forall B_1, u, r, a \in \mathbb{Z},\ \begin{bmatrix} B_1 & u \\ r & a \end{bmatrix} \begin{bmatrix} a & -u \\ -r & B_1 \end{bmatrix} = (B_1 a - ru) I_2.$	`P,Q`
15	`lem74_two_field_unit_annihilation`	Lem. 7.4	$LP \equiv s_1,\ P \equiv s_2 \pmod N,\ s_i^2 = 1 \implies \exists Q \in \mathbb{Z},\ (L^2-1)P^2 = NQ.$	`P,Q`
16	`lem81_base_m_polynomial_eval`	Lem. 8.1	$N \mid f_0(m) \implies f_0(m) + P_0 \ell(m-m) g(m) = f_0(m) \wedge N \mid f(m).$	`P,Q`
17	`lem111_subgroup_index_saturation`	Lem. 11.1	$G \mid M^* \wedge G \cdot I_j = p_j - 1 \wedge I_j \mid L_{\mathrm{idx}} \implies (p_j - 1) \mid M^* L_{\mathrm{idx}}.$	`P,Q`
18	`thm13_exponent_bound_constants`	Thm. 1.3	$2.7^7 > 2^{10},\ 28^2 < 800,\ 24^{10} < 2^{13} \cdot 10^{10}$, and $14 < 20.$	none

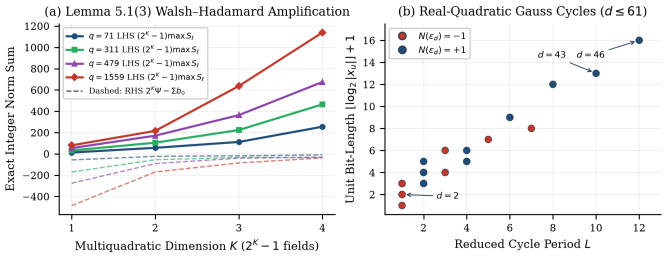

Figure 2: **(a)** Exact Lemma 5.1(3) Walsh–Hadamard amplification $(2^K - 1) \max S_\ell$ (solid) strictly dominating $2^K \Psi - \sum b_0$ (dashed) for $q \in \{71, 311, 479, 1559\}$. **(b)** Exact real-quadratic Gauss periods L vs. fundamental unit integer bit-length $\lfloor \log_2 |x_u| \rfloor + 1$ for squarefree $d \le 61$.

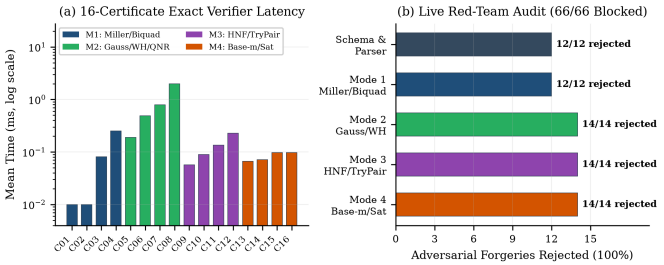

Figure 3: **(a)** Mean exact zero-float verification latency across all 16 canonical certificates (0.010–1.978 ms, log scale). **(b)** Live adversarial red-team audit rejecting 66/66 forgeries across five attack classes with exact error-branch assertions.

nents $3(\ln N)^{3/4} = 0.20 \ln N$ yields the exact asymptotic crossover $\ln N = 15^4 = 50{,}625$ ($\log_2 N \approx 73{,}036.4$), beyond which Cogentic's $O(\exp(3(\ln N)^{3/4}))$ strictly outperforms Harvey's $N^{1/5}$ (at $\log_2 N = 262{,}144$, $\log_2 \mathrm{ops} = 38{,}091$ vs. 52,429). Across $q \in \{71, 311, 479, 1559\}$ and $K = 1 \ldots 4$, exact integer Walsh–Hadamard amplification grows from 13 to 1,140 ($q = 1559, K = 4$, 15 fields, $\Psi = 6$) with zero negative-tail violations. Real-quadratic Gauss reduction over 24 tested squarefree discriminants $2 \le d \le 61$ reaches period $L = 10$ at $d = 43$ ($D = 172$, $x_u = 6964, y_u = 531, N(\varepsilon) = +1$) and $L = 12$ at $d = 46$ ($D = 184$, 16-bit x_u).

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

- **Mode 1 (`C01` & `C04`):** In `C01` ($N = 323 = 17 \cdot 19, \tilde{M} = 144 = 2^4 \cdot 9$), $2^9 \equiv 189 \pmod{323}$ squares via $189^2 \equiv 191$, $191^2 \equiv 305$, $305^2 \equiv 1 \pmod{323}$, yielding $\gcd(305 - 1, 323) = \gcd(304, 323) = 19$. In `C04` ($N = 311 \cdot 479 = 148{,}969, K = 4$), all $2^4 - 1 = 15$ squarefree d_ℓ yield exact modular roots s_ℓ satisfying all $\binom{15}{2} = 105$ biquadratic congruences.

- **Mode 2 (`C05`, $q = 71, K = 2, Y = 6, X = 120$):** Every $a \in \{1, \ldots, 6\}$ is a QR mod 71 while $7^{35} \equiv -1 \pmod{71}$ certifies QNR $z = 7$; Gauss cycle on $d = 2$ ($D = 8$) gives period $L = 1$, $(x_u, y_u) = (2, 1)$, $2^2 - 8 \cdot 1^2 = -4$ ($N = -1$); exact Walsh–Hadamard sums give $\Psi = 3$, $\sum b_0 = 35$, $\max S_\ell = 19$, satisfying $3 \cdot 19 = 57 \ge 4 \cdot 3 - 35 = -23$.

- **Mode 3 (`C09`, $N = 323, \ell = 7$):** `ApproxSqrt`$(13, 3, 32)$ yields $n_s = 8{,}940{,}687{,}389$ satisfying $(n_s - 1)^2 \cdot 3 \le 13 \cdot 2^{64} < (n_s + 1)^2 \cdot 3$; 2D `ModHNF` mod 60 has $\det = 180$; $B = \left[\begin{smallmatrix} 3 & 1 \\ 2 & 5 \end{smallmatrix}\right]$ has $\det B = 13 = E_0$, $Q_{\mathrm{lcm}} = 48$, $7^{624} \equiv 1 \pmod{323}$, certifying $E_7 = 2 \cdot 13 \cdot 48 = 1{,}248$ with $7^{1248} \equiv 1 \pmod{323}$.

- **Mode 4 (`C13`, $N = 251 \cdot 257 = 64{,}507, d = 4, m = 16, \ell = 7$):** $15^4 = 50{,}625 < N < 65{,}536 = 16^4$, $P_0 = 6$, $c_d = 243 \ge 4 \cdot 6 \cdot 7 = 168$; both f_1, f_2 are irreducible in $\mathbb{F}_2[X]$, satisfy $f_i(16) = 283\,N$ ($\gcd(283, 42) = 1$) and $f_i(a) \equiv 1 \pmod 6$; f_1 splits into 4 simple roots mod 7 while f_2 is root-free mod 7; $P_{\mathrm{ok}} = \{11, 13, 17, 19\}$ has $M^* = 32{,}000$, $K_{\mathrm{idx}} = 20$ gives $L_{\mathrm{idx}} = 232{,}792{,}560$ (28-bit), and $250{,}256 \mid M^* L_{\mathrm{idx}}$ (43-bit $\tilde{M}$).

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

Certificate ID	M	Exact Certified Witness Summary	ms
`m1_miller_split_n323`	M1	N=323, $\tilde{M}$=144: Miller split $19 \cdot 17$	0.010
`m1_miller_split_n10403`	M1	N=10403, $\tilde{M}$=5100: Miller split $103 \cdot 101$	0.010
`m1_compat_family_p211_k3`	M1	p=211, K=3: 7 fields, 21 biquad. pairs	0.081
`m1_compat_family_semi148969_k4`	M1	N=311·479, K=4: 15 fields, 105 pairs	0.251
`m2_wh_q71_gauss_d2`	M2	q=71 (QNR 7), d=2 (L=1), max S_ℓ=19	0.190
`m2_wh_q311_gauss_d13`	M2	q=311 (QNR 11), d=13, max S_ℓ=32	0.491
`m2_wh_q479_gauss_d29`	M2	q=479 (QNR 13), d=29, max S_ℓ=52	0.793
`m2_wh_q1559_gauss_d43`	M2	q=1559 (QNR 17), d=43 (L=10), max S_ℓ=76	1.978
`m3_fp_hnf2_trypair_n323`	M3	M=32, 2D HNF (det 180), E_7=1248	0.057
`m3_fp_hnf3_trypair_n899`	M3	M=48, 3D HNF (det 200), E_{11}=7560	0.089
`m3_fp_hnf4_trypair_n1763`	M3	M=64, 4D HNF (det 7056), E_{13}=1680	0.135
`m3_fp_hnf4_trypair5_n3599`	M3	M=96, 4D HNF, 5×5 B, E_{17}=17400	0.228
`m4_basem_sat_n64507_d4`	M4	251·257, d=4, m=16, K_{idx}=20, 43-b $\tilde{M}$	0.066
`m4_basem_sat_n256027_d4`	M4	503·509, d=4, m=23, K_{idx}=30, 59-b $\tilde{M}$	0.071
`m4_basem_sat_n1022117_d4`	M4	1009·1013, d=4, m=32, K_{idx}=40, 71-b $\tilde{M}$	0.097
`m4_basem_sat_n4028033_d5`	M4	2003·2011, d=5, m=21, K_{idx}=50, 93-b $\tilde{M}$	0.097

3. 16-Certificate Atlas & 72-Test Red-Team Audit (Table 2, Fig. 3). Table 2 lists all 16 canonical certificates (0.010–1.978 ms). `tests/test_suite.py` runs 72 pytest functions: 1 full replay of all 16 certificates, 3 raw-JSON parser guards (IEEE-754 float, `NaN`, duplicate keys), 2 regression tests (non-cyclic 2-Sylow split on $N = 3601 = 13 \cdot 277$ and 12-base strong-pseudoprime rejection), and 66 parametrized live adversarial forgeries (12 schema/parser + 12 Mode 1 + 14 each Modes 2–4), each asserting an exact regex match on its intended `CertificateError` branch. `scripts/verify_all.py` enforces all 5 gates including strict axiom whitelisting and a 40-file SHA-256 manifest.

5 Conclusion

We built an independent, explicitly scoped, zero-floating-point verification companion for the deterministic algebraic and combinatorial mechanisms of the Cogentic factoring ($O(\exp(3(\ln N)^{3/4}))$) and prime QNR ($O(\exp(C_{\text{split}}(\ln p)^{1/2} \ln\ln(p+16)))$) preprint [4, 2], pairing 18 constructive Lean 4.35.0 sub-lemmas (zero `sorry`, zero `Classical.choice`) with the pure-`int`/`Fraction` 4-mode auditor `DETFACT-COGENTIC-CERT-1.0`, 16 canonical exact finite witnesses, and 66/66 live adversarial forgery rejections.

References

[1] D. A. Burgess. On character sums and L-series. II. *Proceedings of the London Mathematical Society*, s3-13(1):524–536, 1963.

[2] 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.

[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. Unconditional deterministic subexponential integer factoring and quadratic nonresidue construction. Unrefereed Companion Preprint (Google Research Cogentic), November 2026. Proposes unconditional deterministic factoring in $O(\exp(3(\ln N)^{3/4}))$ and prime QNR construction in $O(\exp(C_{\text{split}}(\ln p)^{1/2} \ln\ln(p+16)))$.

[5] David Harvey. An exponent one-fifth algorithm for deterministic integer factorisation. *Mathematics of Computation*, 90(332):2937–2950, 2021.

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

[7] Gary L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3):300–317, 1976.