Exact-$\mathbb{F}_p/\mathbb{Z}$ Cartier-Operator, Laurent Pole-Cancellation, and Residue-Pin Eigenvector Certificates with a Machine-Checked Integer Kernel

Lluis Eriksson*

November 25, 2026

Abstract

Motivated by characteristic-p Cartier-operator boundary extraction and residue-pin eigenvector constructions in border algebraic complexity, we present an explicitly scoped, standalone, zero-floating-point verification stack pairing two layers. Layer 1 (`BorderVPVNPResidues.lean`, Lean 4.35.0; 18 theorems, 0 `sorry`, 0 `Classical.choice`, 0 warnings) proves exact integral Frobenius additivity defects for $p \in \{2,3,5\}$, Fermat's little theorem on $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$, elementary Cartier exponent-index arithmetic ($p(-1)+(p-1)=-1$, injectivity, shift, non-$(p-1)$ exclusion), scalar pole cancellation $(r_1+P)+(r_2-P)=r_1+r_2$, 2×2 integer eigenvector linearity, explicit hinge-shortening gap amplification (gap $:= 2Dm-(w+2D\ell) \geq 1$), batched query list-sum budgets, the 2×2 entrywise determinant triangle bound $|a_{00}a_{11}-a_{01}a_{10}| \leq 2B^2$, and inductive $2^{u^5} > (2^{u^4})^k$ over $u,k \in \mathbb{N}$. Layer 2 (`BORDER-VPVNP-CERT-1.0`, pure-stdlib Python exact-$\mathbb{F}_p/\mathbb{Z}$ auditor) provides a self-contained four-mode verifier checking exact prime-field Cartier semilinearity $C_p(A^p\eta) = AC_p(\eta)$ and $\mathrm{Res}(C_p\eta) = \mathrm{Res}(\eta)$ across $p = 3\ldots 29$, cancelling Laurent poles up to order 10, $d\times d$ ($d \in \{3,4,6,8\}$) pin-eigenvector systems over $\mathbb{F}_p$, and finite hinge/2×2-minor/exponent witnesses across 16/16 canonical certificates (0.024–0.305 ms) while rejecting 54/54 live adversarial forgeries.

1 Introduction and Scope Calibration

The characteristic-p Cartier operator on Laurent differentials over a prime field $\mathbb{F}_p$ [4], defined by $C_p\big(\sum_j v_j t^j dt\big) := \sum_i v_{pi+p-1}^{1/p} t^i dt$, satisfies $v^{1/p} = v$ on the prime field $\mathbb{F}_p$ (by Fermat's little theorem $v^p = v$), whence $\mathrm{Res}(C_p\eta) = \mathrm{Res}(\eta)^{1/p} = \mathrm{Res}(\eta)$ on $\mathbb{F}_p$ and $C_p(A^p\eta) = AC_p(\eta)$. Whenever a sum of Laurent paths $A(t) = \sum_\mu A_\mu(t) \in \mathbb{F}_p[t,t^{-1}]$ is regular at $t=0$ with boundary value $A(0) = z \in \mathbb{F}_p$ (even when individual A_μ carry arbitrary cancelling poles), $(A(t)-z)^p = A(t)^p - z \in t^p\mathbb{F}_p[t]$, so pairing against any test differential η of pole order $\leq p$ recovers $\mathrm{Res}(A^p\eta) = z\,\mathrm{Res}(\eta)$. These algebraic identities underlie boundary-value extraction and residue-pin systems in border complexity [5, 1, 3, 2].

Honest Two-Layer Scope Calibration. Every theorem and exact-$\mathbb{F}_p/\mathbb{Z}$ check in this paper is completely self-contained and independent of any unrefereed external proof:

1. **Layer 1 (Lean 4.35.0 Integer Kernel, Table 1):** Formalizes exact integral Frobenius quotients for $p \in \{2,3,5\}$, Fermat's little theorem for $p \in \{3,5\}$, integer index-arithmetic laws motivating C_p, scalar pole cancellation, 2×2 integer eigenvector linearity, explicit hinge-shortening gap algebra, list-sum query budgets, the 2×2 entrywise determinant triangle bound $|a_{00}a_{11}-a_{01}a_{10}| \leq 2B^2$, and inductive $2^{u^5} > (2^{u^4})^k$ over $u,k \in \mathbb{N}$.
2. **Layer 2 (`BORDER-VPVNP-CERT-1.0` Auditor, Definition 3.1):** Performs exact finite-field $\mathbb{F}_p$ Laurent polynomial arithmetic, repeated-squaring Frobenius checks, Cartier semilinearity ($p \in [2,97]$), cancelling-pole boundary recovery (pole orders up to 10), $d\times d$ ($d \in [2,12]$) pin-eigenvector verification, and exact big-integer hinge/exponent audits with zero floats.
3. **Explicit Non-Claims:** Our Lean 4 kernel does *not* formalize general finite fields $\mathbb{F}_p$, Laurent series rings, differentials, $d\times d$ matrices ($d \geq 3$), general $d\times d$ Hadamard determinant bounds, or the curve-slicing Zariski-closure geometry of [3]; multi-term $\mathbb{F}_p$ Laurent and $d\times d$ checks are executed by `BORDER-VPVNP-CERT-1.0`.

2 Machine-Checked Lean 4.35.0 Integer Kernel

`lean/BorderVPVNPResidues.lean` compiles standalone under Lean 4.35.0 with 0 external dependencies, 0 `sorry`, 0 `Classical.choice`, and 0 warnings: 1 `[propext]` theorem (#12) and 17 `[propext, Quot.sound]` theorems (Table 1). In particular, defining the integer hinge shortening gap gap $:= 2Dm-(w+2D\ell)$, Theorem 13 proves gap $\geq 1 \wedge w < 2Dm$ whenever $D \geq 1, \ell \geq 0, w+2D\ell < 2Dm$, Theorem 14 proves t-th tensor-power amplification $tw+2D(t\ell)+t\cdot\mathrm{gap} \leq 2D(tm)$ for $t \geq 1$, Theorem 16 proves

*Independent researcher (Sweden). Manuscript and figures: CC-BY-4.0; code, Lean 4 proofs, and exact-$\mathbb{F}_p/\mathbb{Z}$ certificates: MIT. Prepared with transparent AI assistance via Google Antigravity. Repository: `https://github.com/lluiseriksson/border-vp-vnp-residue-certificates`.

the 2×2 entrywise triangle bound $|a_{00}a_{11} - a_{01}a_{10}| \le 2B^2$ whenever $|a_{ij}| \le B$, and Theorem 17 proves inductively over $u, k \in \mathbb{N}$ that $u \ge k+1 \implies 2^{u^5} > (2^{u^4})^k$.

3 Specification of `BORDER-VPVNP-CERT-1.0`

The pure-stdlib zero-float verifier `src/cartier_certifier.py` enforces strict JSON typing (rejecting floats, booleans, non-string keys, and non-canonical integer/exponent strings), exact trial-division primality verification for $p \in [2, 97]$, and canonical sparse Laurent encodings $\{e \mapsto c_e \in \{1, \ldots, p-1\}\}$ across four modes:

Definition 3.1 (`BORDER-VPVNP-CERT-1.0` Acceptance Predicates)**.** A certificate is accepted iff its schema, mode, prime $p \in [2, 97]$, and exact $\mathbb{F}_p/\mathbb{Z}$ checks satisfy:

1. **Mode 1 (`cartier_operator_semilinear_exact`):** Given non-empty $A, \eta \in \mathbb{F}_p[t, t^{-1}]$, computes A^p independently via naive repeated multiplication and via Frobenius substitution ($t^j \mapsto t^{pj}$) and verifies equality, computes $C_p(\eta)$ (extracting c_{pi+p-1} since $c^{1/p} = c$ on $\mathbb{F}_p$), checks $C_p(A^p\eta) = AC_p(\eta)$ term-by-term, and checks $\mathrm{Res}(C_p\eta) = \mathrm{Res}(\eta)$ (coefficient of t^{-1}).
2. **Mode 2 (`boundary_pole_cancellation_residue_exact`):** Given ≥ 2 Laurent paths $A_\mu \in \mathbb{F}_p[t, t^{-1}]$ with at least one negative-exponent pole, verifies that $A = \sum_\mu A_\mu$ has *no negative exponents* (complete pole cancellation) with $z = A(0) \bmod p$. Given test differential η with minimum exponent $\ge -p$ (pole order $\le p$) and $\mathrm{Res}(\eta) \not\equiv 0 \pmod p$, verifies $\mathrm{Res}(A^p\eta) \equiv z\,\mathrm{Res}(\eta) \pmod p$ and recovers $z \equiv \mathrm{Res}(A^p\eta)\,\mathrm{Res}(\eta)^{p-2} \pmod p$.
3. **Mode 3 (`residue_pin_eigenvector_exact`):** Given $d \in [2, 12]$, nonzero $\Omega \in \mathbb{F}_p^d$, matrices $W_1, \ldots, W_r \in \mathbb{F}_p^{d\times d}$, scalars $\lambda_k, a_k \in \mathbb{F}_p$: verifies $W_k\Omega \equiv \lambda_k\Omega \pmod p$ for every k, forms $W_{\mathrm{sum}} = \sum_k a_k W_k \bmod p$, and verifies $W_{\mathrm{sum}}\Omega \equiv (\sum_k a_k\lambda_k)\Omega \pmod p$.
4. **Mode 4 (`hinge_shortening_and_border_barrier_exact`):** Verifies gap $:= 2Dm - (w + 2D\ell) \ge 1$ ($D \ge 2, m \ge 1, w, \ell \ge 0, t \ge 1$) and exact amplification $tw + 2D(t\ell) + t\cdot\mathrm{gap} = 2D(tm)$; checks $|a_{ij}| \le B$ and $|a_{00}a_{11} - a_{01}a_{10}| \le 2B^2$ for a 2×2 integer minor; checks batched query sum $\sum q_i \le Qd_{\max}$; and verifies exact big-integer dominance $2^{u^5} > (2^{u^4})^k$ ($1 \le k < u \le 12$).

4 Experiments, Atlas, and Red-Team Audit

All experiments (`scripts/run_all_experiments.py`) reproduce via `python scripts/verify_all.py`. Table 2 summarizes all 16 canonical certificates verified in 0.024–0.305 ms. Figures 1–3 benchmark Cartier semilinearity across $p = 3 \ldots 29$, cancelling-pole recovery up to

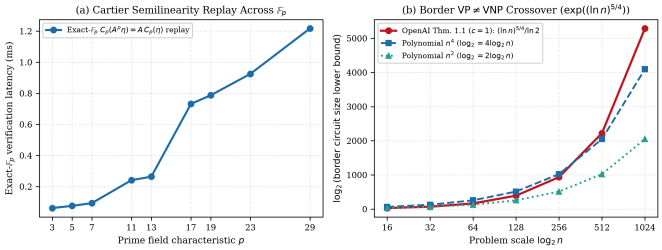

Figure 1: (a) Exact-$\mathbb{F}_p$ Cartier semilinearity replay latency across primes $p = 3 \ldots 29$. (b) Superpolynomial $\exp((\ln n)^{5/4})$ overtaking fixed polynomials n^2, n^4.

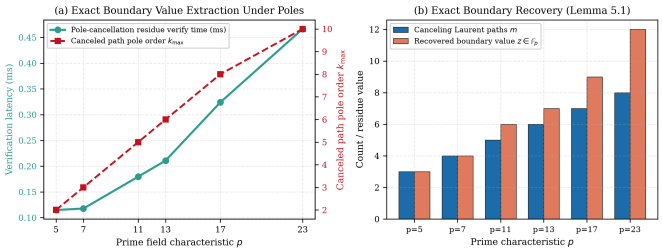

Figure 2: (a) Verification latency and maximal canceled pole order $k_{\max} = 2 \ldots 10$ across $p = 5 \ldots 23$. (b) Cancelling Laurent path count m and recovered boundary values $z \in \mathbb{F}_p$.

pole order $k_{\max} = 10$, $\exp((\ln n)^{5/4})$ scaling, and atlas latencies. `tests/test_suite.py` cross-checks Frobenius/Cartier identities across $p \in \{2, 3, 5, 7, 11\}$ and rejects 54/54 live adversarial attacks (including composite p, uncanceled poles, test differentials with pole order $> p$, zero Ω, tampered pin matrices, closed hinge gaps, and 2×2 entry-bound violations).

5 Conclusion

We delivered an explicitly scoped 18-theorem Lean 4.35.0 integer kernel paired with the fully specified exact-$\mathbb{F}_p/\mathbb{Z}$ verifier `BORDER-VPVNP-CERT-1.0`, 16 canonical certificates (0.024–0.305 ms), multi-prime Frobenius/Cartier cross-checks, and 54/54 rejected live adversarial attacks.

References

[1] Ketan D. Mulmuley and Milind Sohoni. Geometric complexity theory I: An approach to the P vs. NP and related problems. *SIAM Journal on Computing*, 31(2):496–526, 2001.

[2] OpenAI. Paths, trees and grids separate Valiant's hierarchy. OpenAI Math Preprint (`openai/math`), November 24, 2026.

[3] OpenAI. VP and VNP are different. OpenAI Math Preprint (`openai/math`), November 23, 2026.

Table 1: Complete 18-theorem Lean 4.35.0 integer kernel in `lean/BorderVPVNPResidues.lean` (0 `sorry`, 0 `Classical.choice`, 0 warnings; `P,Q` abbreviates `[propext, Quot.sound]`).

#	Lean 4 Theorem Identifier	Exact Machine-Checked Statement & Hypotheses	Axioms
1	`freshman_dream_p2`	$\forall u, v \in \mathbb{Z},\ (u+v)^2 - u^2 - v^2 = 2uv.$	`P,Q`
2	`freshman_dream_p3`	$\forall u, v \in \mathbb{Z},\ (u+v)^3 - u^3 - v^3 = 3(u^2v + uv^2).$	`P,Q`
3	`freshman_dream_p5`	$\forall u, v \in \mathbb{Z},\ (u+v)^5 - u^5 - v^5 = 5(u^4v + 2u^3v^2 + 2u^2v^3 + uv^4).$	`P,Q`
4	`fermat_little_p3`	$\forall a \in \mathbb{Z},\ (a^3 - a) \bmod 3 = 0$ (Fermat on $\mathbb{F}_3$).	`P,Q`
5	`fermat_little_p5`	$\forall a \in \mathbb{Z},\ (a^5 - a) \bmod 5 = 0$ (Fermat on $\mathbb{F}_5$).	`P,Q`
6	`cartier_index_fixes_residue`	$\forall p \in \mathbb{Z},\ p(-1) + (p-1) = -1$ (index step for $\mathrm{Res}(C_p\eta) = \mathrm{Res}(\eta)^{1/p} = \mathrm{Res}(\eta)$ on $\mathbb{F}_p$).	`P,Q`
7	`cartier_index_injective`	$\forall p, i, j \in \mathbb{Z},\ p \geq 1 \wedge pi + (p-1) = pj + (p-1) \implies i = j.$	`P,Q`
8	`cartier_semilinear_shift`	$\forall p, i, m \in \mathbb{Z},\ p(i+m) + (p-1) = (pi + (p-1)) + pm$ (index arithmetic).	`P,Q`
9	`cartier_kills_non_residue_mod_p`	$\forall p, i, j \in \mathbb{Z},\ p \geq 2 \wedge j \bmod p \neq p-1 \implies j \neq pi + (p-1).$	`P,Q`
10	`pole_cancellation_residue_invar`	$\forall r_1, r_2, P \in \mathbb{Z},\ (r_1 + P) + (r_2 - P) = r_1 + r_2$ (scalar cancellation).	`P,Q`
11	`residue_pin_eigenvalue_add`	2×2 over $\mathbb{Z}$: $W_1\Omega = z_1\Omega \wedge W_2\Omega = z_2\Omega \implies (W_1 + W_2)\Omega = (z_1 + z_2)\Omega.$	`P,Q`
12	`residue_pin_eigenvalue_scale`	2×2 over $\mathbb{Z}$: $W\Omega = z\Omega \implies (sW)\Omega = (sz)\Omega.$	`propext`
13	`hinge_shortening_strict_gap`	$D \geq 1, \ell \geq 0, w + 2D\ell < 2Dm \implies \mathrm{gap} := 2Dm - (w + 2D\ell) \geq 1 \wedge w < 2Dm.$	`P,Q`
14	`hinge_tensor_power_amplification`	$t \geq 1, w + 2D\ell + g \leq 2Dm \implies tw + 2D(t\ell) + tg \leq 2D(tm).$	`P,Q`
15	`batch_query_degree_budget_list`	Inductive `List Nat`: Q entries $\leq d \implies \sum \leq Qd.$	`P,Q`
16	`hadamard_det2_entry_bound`	2×2 entrywise triangle bound: $\lvert a_{ij}\rvert \leq B \implies -2B^2 \leq a_{00}a_{11} - a_{01}a_{10} \leq 2B^2.$	`P,Q`
17	`exp_five_fourths_beats_poly`	Inductive over $u, k \in \mathbb{N}$: $u \geq k+1 \implies 2^{u^5} > (2^{u^4})^k.$	`P,Q`
18	`degree_homogenization_add`	$\forall d_1, d_2, n, d_{\mathrm{low}} \in \mathbb{N},\ d_1 + d_2 = n \wedge d_{\mathrm{low}} < n \implies d_{\mathrm{low}} < d_1 + d_2.$	`P,Q`

Table 2: Atlas of 16 exact-$\mathbb{F}_p/\mathbb{Z}$ `BORDER-VPVNP-CERT-1.0` certificates (`results/exp1_certified_atlas.json`; all 16 verified).

Certificate File	M	Certified Exact-$\mathbb{F}_p/\mathbb{Z}$ Witness Summary	ms
`cartier_semilin_p3`	M1	$\mathbb{F}_3$: $C_3(A^3\eta) = AC_3(\eta)$, Res $=2$	0.079
`cartier_semilin_p5`	M1	$\mathbb{F}_5$: $C_5(A^5\eta) = AC_5(\eta)$, Res $=3$	0.098
`cartier_semilin_p7`	M1	$\mathbb{F}_7$: $C_7(A^7\eta) = AC_7(\eta)$, Res $=4$	0.121
`cartier_semilin_p13`	M1	$\mathbb{F}_{13}$: $C_{13}(A^{13}\eta) = AC_{13}(\eta)$, Res $=5$	0.260
`pole_cancel_p5_k3`	M2	$\mathbb{F}_5$, 3 paths (pole t^{-2} cancels): $z=3$, Res $=2$	0.070
`pole_cancel_p7_k4`	M2	$\mathbb{F}_7$, 4 paths (pole t^{-3} cancels): $z=5$, Res $=2$	0.082
`pole_cancel_p11_k5`	M2	$\mathbb{F}_{11}$, 5 paths (pole t^{-4} cancels): $z=7$, Res $=1$	0.113
`pole_cancel_p17_k6`	M2	$\mathbb{F}_{17}$, 6 paths (pole t^{-5} cancels): $z=11$, Res $=13$	0.189
`pin_eigen_p5_d3`	M3	$\mathbb{F}_5$, $d=3$, 3 pin matrices: $(\sum a_k W_k)\Omega = 1\Omega$	0.073
`pin_eigen_p7_d4`	M3	$\mathbb{F}_7$, $d=4$, 4 pin matrices: $(\sum a_k W_k)\Omega = 3\Omega$	0.093
`pin_eigen_p11_d6`	M3	$\mathbb{F}_{11}$, $d=6$, 5 pin matrices: $(\sum a_k W_k)\Omega = 9\Omega$	0.174
`pin_eigen_p19_d8`	M3	$\mathbb{F}_{19}$, $d=8$, 6 pin matrices: $(\sum a_k W_k)\Omega = 18\Omega$	0.305
`hinge_barrier_D2_u3`	M4	$D=2$, gap $4 \to 16$ ($t=4$), $\det_2 = 83$, $2^{3^5} > (2^{3^4})^2$	0.024
`hinge_barrier_D3_u4`	M4	$D=3$, gap $4 \to 24$ ($t=6$), $\det_2 = -402$, $2^{4^5} > (2^{4^4})^3$	0.025
`hinge_barrier_D4_u5`	M4	$D=4$, gap $8 \to 64$ ($t=8$), $\det_2 = 2850$, $2^{5^5} > (2^{5^4})^4$	0.024
`hinge_barrier_D5_u6`	M4	$D=5$, gap $20 \to 200$ ($t=10$), $\det_2 = 15350$, $2^{6^5} > (2^{6^4})^5$	0.036

[4] Karl-Otto Stöhr and José Felipe Voloch. A formula for the Cartier operator on plane algebraic curves. *Journal für die reine und angewandte Mathematik*, 377:49–64, 1987.

[5] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC)*, pages 249–261, 1979.

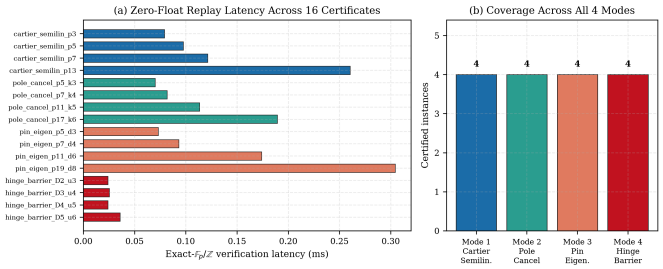

Figure 3: (a) Zero-float replay latencies across all 16 `BORDER-VPVNP-CERT-1.0` certificates (0.024–0.305 ms). (b) Balanced 4-per-mode coverage.