ECC RESEARCH PROGRAM · P4.2

Pairing-Friendly Cycles of Elliptic Curves: A Complete Low-Cyclotomic-Degree Classification and a 28-Bit Census

Every prime-order 2-cycle with both exact embedding degrees in {3, 4, 5, 6, 8, 10, 12} is MNT or one of two tiny exceptions

math.st [1] **@math__street** [1]

with GPT 5.6 Sol · Claude Fable 5

[1]Independent research collective, math.st · July 2026

ABSTRACT

A 2-cycle of elliptic curves is a pair with $\#E_1(\mathbb{F}_p) = q$ and $\#E_2(\mathbb{F}_q) = p$; an m-cycle is the analogous closed chain. Cycles in which every curve is pairing-friendly are the arithmetic backbone of recursive proof composition, and essentially the only known construction is the MNT family with embedding degrees $(6, 4)$. Problem P4.2 asks whether pairing-friendly 2-cycles exist outside the MNT degree pattern, whether cycles of length at least 3 exist, and whether a cycle-level $\rho < 2$ criterion can be met. We give a two-part answer. **Globally**, we prove that every prime-order 2-cycle whose two exact embedding degrees lie in $\{3, 4, 6\}$ is MNT — a self-contained parameter-level converse of the MNT classification — and, pushing the same quotient-remainder method through the quartic cyclotomic degrees $\{5, 8, 10, 12\}$, that the **only** non-MNT cycles with both degrees in $\{3, 4, 5, 6, 8, 10, 12\}$ are the two tiny cycles $(7, 11; 10, 3)$ and $(11, 13; 12, 10)$. The quartic case reduces to 750 genus-one equations, which local sieves, exact sign analysis, Hensel lifting, and exact Magma computations (integral points, fake 2-Selmer sets, one rank-0 curve) close completely. We further prove that the consecutive MNT 3-chain never closes to a directed 3-cycle with degrees at most 12. **Empirically**, a candidate-complete census of all prime fields below 2^{28} (proved complete via exact-order cyclotomic-root enumeration) finds exactly 333 2-cycles — 328 MNT and the five known tiny exceptions, all with fields at most 31 — and exactly five directed 3-cycles, all with fields at most 43. Every hit through 24 bits is realized by explicit, independently point-counted curve equations. Under the standard per-curve definition the $\rho < 2$ criterion is automatic for every prime-order 2-cycle, which we flag as a gap in the problem statement rather than a result. The degree pairs involving 7, 9, and 11 and the general length-3 question remain open beyond the stated bounds.

Keywords. elliptic curve cycles · pairing-friendly curves · MNT curves · embedding degree · genus-one Diophantine equations · recursive SNARKs

1 Introduction

Proof-carrying data and recursive SNARK composition need two elliptic curves that alternately host each other's verifier arithmetic: the scalar field of one must be the base field of the other. This

is exactly a **2-cycle** of curves, and if both curves must also be pairing-friendly, the only known constructions come from the MNT curves of embedding degrees 4 and 6 [1], [2]. Chiesa, Chua, and Weidner proved that within the MNT families the possible cycle degree patterns are $(6, 4)$ and $(6, 4, 6, 4)$, and ruled out several degree pairs unconditionally [2]; Belles-Munoz, Jimenez Urroz, and Silva extended the family-based exclusions [3]. What has been missing is a classification that does not assume membership in a named family, and any census of what actually exists at small scale.

Problem P4.2 poses three questions: (1) do pairing-friendly 2-cycles exist outside the MNT degree pattern? (2) do pairing-friendly cycles of length at least 3 exist? (3) can a cycle meet a clearly specified cycle-level $\rho < 2$ criterion? This paper reports the completed three-session record: four global classification theorems, one global obstruction for length 3, and a candidate-complete verified census of all prime fields below 2^{28}.

Main results. **(i) Global classification.** PROVED Every prime-order 2-cycle whose two exact embedding degrees lie in $\{3, 4, 5, 6, 8, 10, 12\}$ is either one of the two MNT orientations — with the explicit parameterization $p = 4x^2 + 1$, $q = 4x^2 \pm 2x + 1$ — or one of exactly two tiny exceptions: $(p, q; k_1, k_2) = (7, 11; 10, 3)$ and $(11, 13; 12, 10)$. The quartic/quartic case closes 750 genus-one Diophantine equations.

(ii) Length-3 obstruction. PROVED The consecutive MNT chain $(4x^2 - 2x + 1,\ 4x^2 + 1,\ 4x^2 + 2x + 1)$ never closes to a directed 3-cycle with all exact embedding degrees in $\{3, \ldots, 12\}$, in either orientation, for any $x \geq 1$.

(iii) 28-bit census. EMPIRICAL: distinct primes < 2^28, exact degrees 3–12 There are exactly 333 prime-order 2-cycles (164 + 164 MNT, five exceptions with largest field 31) and exactly five directed 3-cycles (largest field 43). Non-MNT 2-cycles with larger field at least 32 do not exist below 2^{28}; neither does any 3-cycle with a field above 43.

(iv) The ρ question is degenerate as posed. PROVED With the standard per-curve definition, every distinct prime-order 2-cycle over fields at least 5 satisfies $\rho_{\max} < 2$ automatically, and the geometric mean of per-curve ρ values is identically 1 for every prime-order cycle.

The claims carry the epistemic tags of the research record: PROVED for proved statements (several with machine-checked finite certificates), CITED for literature statements, and EMPIRICAL: scope for census facts that hold exactly in the stated finite range and are claimed nowhere else.

2 Cycle arithmetic

Definition 1 (m-cycle). Elliptic curves $E_i/\mathbb{F}_{p_i}$ ($i \in \mathbb{Z}/m\mathbb{Z}$, p_i distinct primes) form an **m-cycle** if $\#E_i\left(\mathbb{F}_{p_i}\right) = p_{i+1}$ for every i. The cycle has **prime order** if every p_i is prime (which the definition already forces). A **2-cycle** is the case $m = 2$.

Proposition 2 (trace identities). PROVED Write $t_i = p_i + 1 - p_{i+1}$ for the Frobenius trace of E_i. Then an m-cycle satisfies

$$\sum_{i=1}^{m} t_i = m, \tag{1}$$

and for $m = 2$, additionally $t_1 + t_2 = 2$ and the two Frobenius discriminants agree:

$$t_2^2 - 4p_2 = t_1^2 - 4p_1. \tag{2}$$

Proof. The defining identity $\#E_i\left(\mathbb{F}_{p_i}\right) = p_i + 1 - t_i = p_{i+1}$ gives $t_i = p_i + 1 - p_{i+1}$; summing over the cycle telescopes the field sizes, leaving $\sum t_i = m$. For $m = 2$ put $p_1 = p$, $p_2 = q = p + 1 - t, t_1 = t, t_2 = 2 - t$; then $4q - t_2^2 = 4(p + 1 - t) - (2 - t)^2 = 4p - t^2$. Consequently the unique decompositions $t_i^2 - 4p_i = D_K f_i^2$ with D_K fundamental give the **same** CM field and conductor for both ordinary isogeny classes. □

Proposition 3 (exact embedding degree). PROVED In a prime-order cycle, the exact embedding degree of $E_i/\mathbb{F}_{p_i}$ (with respect to its full group of order p_{i+1}) is the multiplicative order $\mathrm{ord}_{p_{i+1}}(p_i)$. A claimed degree k_i therefore requires $p_i^{k_i} \equiv 1 \bmod p_{i+1}$ and $p_i^j \not\equiv 1 \bmod p_{i+1}$ for every $1 \le j < k_i$.

Every stored hit in this paper checks both conditions; a degree above the search ceiling is recorded as "> 12", never guessed.

2.1 The ρ conventions, and a gap in the problem statement

PROVED For a prime-order cycle we use the per-curve values $\rho_i = \log p_i / \log p_{i+1}$ and the cycle statistic $\rho_{\max} = \max_i \rho_i$. The product of the ρ_i telescopes, so their geometric mean is **identically** 1 — it carries no information. Moreover Hasse's bound $q \le p + 1 + 2\sqrt{p} < p^2$ (for $p \ge 5$) forces $\log q / \log p < 2$, so:

Proposition 4 ($\rho_{\max} < 2$ is automatic). PROVED Every 2-cycle over distinct prime fields at least 5 satisfies $\rho_{\max} < 2$. The published MNT cycle over fields 37 and 43 has $\rho_{\max} = 1.041618836729$.

Remark 5 (gap Q010). PROVED Question (3) of the problem statement asks whether a cycle can achieve "$\rho < 2$", but under the standard per-curve definition this is automatic for every object in scope. Resolving the **intended** question would require a different explicit definition; the record keeps this as open question Q010 rather than inventing one.

3 The published MNT anchor, reproduced

CITED Chiesa–Chua–Weidner parameterize an MNT6/MNT4 2-cycle by field sizes $4x^2 + 1$ and $4x^2 + 2x + 1$ with traces $1 - 2x$ and $2x + 1$, and give at $x = 3$ the explicit curves $y^2 = x^3 + 24x + 16$ over $\mathbb{F}_{37}$ and $y^2 = x^3 + 36x + 5$ over $\mathbb{F}_{43}$ (Table 4.1, Example 4.9) [2].

EMPIRICAL: published x=3 curves Direct equation enumeration and an independent Hasse/BSGS twist-based counter both return orders 43 and
37. The traces are -5 and 7, the common CM radicand is

$4 \cdot 37 - 25 = 123$, and the exact embedding degrees are 6 and 4. This is the known-answer regression for every counter used below.

4 Census methodology

4.1 Frozen search space

PROVED The primary search enumerates every unordered pair of distinct primes $5 \le p < q < 2^{16}$ (later extended to 2^{28}), retaining a pair as a 2-cycle isogeny-class candidate exactly when both traces $t_1 = p + 1 - q$, $t_2 = q + 1 - p$ satisfy the Hasse bounds $t_1^2 \le 4p$, $t_2^2 \le 4q$. CITED Every retained trace is ordinary and realized by an elliptic curve over the corresponding field [4] (ordinarity because distinct primes force $t_i \neq 0$ and $|t_i| < p_i$). A **hit** requires both exact degrees in $\{3, \ldots, 12\}$; degrees 1 and 2 are the fixed non-pairing-friendly baseline; one-sided rows are stored as near-misses. The search space file was frozen before the first run.

4.2 Candidate-complete cyclotomic-root enumeration

Scanning all $\sim 10^{14}$ prime pairs at 28 bits is infeasible; the census instead **generates** target-degree edges and proves nothing is lost.

> **Theorem 6** (root enumeration is candidate-complete). PROVED For a prime q and $k \mid q - 1$, the residues of exact multiplicative order k modulo q are exactly the $\varphi(k)$ generators power-classes z^j, $\gcd(j, k) = 1$, of the unique order-k subgroup of $\mathbb{F}_q^*$, and there are none if $k \nmid q - 1$. Moreover, every directed Hasse edge $p \to q$ satisfies $p < 2q$, so $p = z$ or $p = q + z$ where $z = p \bmod q$. Consequently, enumerating exact-order residues generates every target-degree Hasse edge; taking unordered endpoints retains every reportable 2-cycle row, and joining the directed target graph with itself retains every reportable directed 3-cycle row (any full hit or two-of-three near-miss contains two consecutive target edges after rotation).

Proof. Cyclicity of $\mathbb{F}_q^*$ gives the subgroup structure; a generator is found by raising elements to $(q - 1)/k$ and rejecting z with $z^{k/\ell} = 1$ for a prime $\ell \mid k$. For the edge bound: $(p + 1 - q)^2 \le 4p$ with $p \ge 2q$ would force $p + 1 - q \ge p/2 + 1 > 2\sqrt{p}$ for $p \ge 11$, a contradiction. The implementation retains only prime p satisfying the Hasse inequality and **recomputes** the exact order of every generated edge, so the generated set equals the target set. □

EMPIRICAL: complete 24-bit ledgers The root-generated and exhaustively Hasse-scanned candidate CSVs are byte-identical (equal SHA-256) at every overlapping bound, while the runtime at 24 bits drops from 404.6 to 20.4 seconds for 2-cycles and from 405.3 to 28.4 seconds for 3-cycles. At 28 bits the root method processes 14,630,841 primes in 301.0 and 427.7 seconds respectively.

4.3 Independent verification of every hit

EMPIRICAL: all full hits through 24 bits Every arithmetic hit is converted to explicit curve equations by seeded coefficient search; each curve's order is confirmed by BSGS **and**, through 22 bits, by direct equation enumeration. At 24 bits the second check is the prime-order certificate: PROVED a nonidentity point annihilated by the prime q, together with uniqueness of q as a multiple of the point order in the Hasse interval, certifies the exact curve order. All 108 new 24-bit equations carry this certificate. Above 24 bits every newly appearing hit is MNT-pattern and is covered by the global classification of §6 plus exact arithmetic checks; individual equations were not redundantly re-searched there, and we state this rather than imply otherwise.

5 The census

5.1 2-cycles

EMPIRICAL: 5 <= p < q < 2^16, exact degrees 3–12 The primary 16-bit census covers 6,540 primes, 21,382,530 unordered prime pairs, and 204,074 Hasse-valid pairs; it stores 26 full hits and 219 one-sided near-misses. The hits are 13 copies of $(6, 4)$, eight of $(4, 6)$, and one each of $(10, 3)$, $(12, 10)$, $(9, 8)$, $(7, 11)$, $(10, 11)$ — the last five over the tiny field pairs listed in Table 1.

Table 1: EMPIRICAL: verified by two point counters The five exceptional (non-MNT-pattern) 2-cycles below 2^{28}. All were explicitly constructed and independently point-counted. No novelty is claimed for any single tiny instance.

fields (p, q)	degrees (k_1, k_2)	status in this paper	prior record
(7, 11)	(10, 3)	unique in its class (Thm. 9)	MNT3 $x = 1$ exception, [3] Table 2
(11, 13)	(12, 10)	unique in its class (Thm. 10)	—
(17, 19)	(9, 8)	class open (deg. 9)	—
(23, 29)	(7, 11)	class open (deg. 7, 11)	—
(23, 31)	(10, 11)	class open (deg. 11)	—

EMPIRICAL: primes < 2^28, exact degrees 3–12 Extending the bound stepwise to 28 bits (14,630,841 primes) grows the ledger to 333 hits: 164 of degree pair $(6, 4)$, 164 of $(4, 6)$, and the same five exceptions — **no new exceptional cycle appears after $q = 31$**. Figure 1 shows the growth. The precisely scoped negative statement is: below 2^{28} there is no 2-cycle outside degree pairs $\{(6, 4), (4, 6)\}$ whose larger field is at least 32.

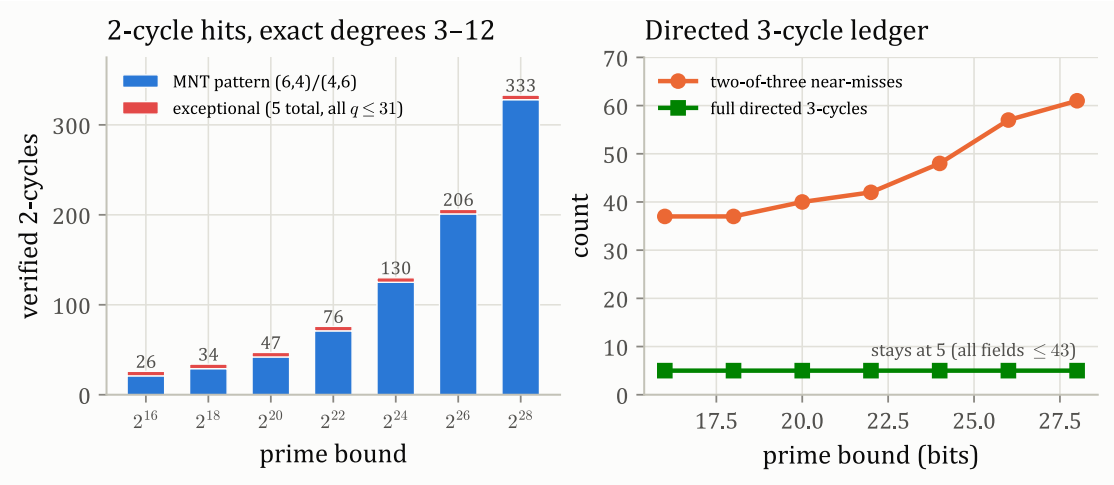

Figure 1: EMPIRICAL: seven candidate-complete censuses Left: the verified 2-cycle ledger from 2^{16} to 2^{28} — MNT-pattern hits grow steadily while the exceptional count is frozen at five. Right: the directed 3-cycle ledger — near-misses accumulate but the full-hit count never leaves

5. Data: the fourteen `search_*_summary.json` artifacts.

EMPIRICAL: all 328 MNT-pattern hits below 2^28 Every degree-$\{4, 6\}$ ledger row matches the integer parameter formula of Theorem 7 exactly: 164 rows in each orientation, at parameters recorded in `verify_mnt_parameterization_n328_20260627.csv`.

5.2 Directed 3-cycles

EMPIRICAL: three distinct primes < 2^16, exact degrees 3–12 The directed Hasse graph at 16 bits has 408,148 edges and 6,922,890 directed triangles up to rotation. Exactly five directed 3-cycles occur — and the count is **still five** at 28 bits:

Table 2: EMPIRICAL: all 15 curves constructed and independently counted The complete list of directed 3-cycles with distinct prime fields below 2^{28} and exact degrees in $\{3, \ldots, 12\}$.

fields (p_1, p_2, p_3)	exact degrees	largest field
(7, 13, 11)	(12, 10, 3)	13
(11, 13, 17)	(12, 4, 10)	17
(13, 17, 19)	(4, 9, 12)	19
(23, 29, 31)	(7, 10, 11)	31
(37, 41, 43)	(5, 7, 4)	43

This answers question (2) **at toy scale**: pairing-friendly cycles of length 3 exist, but every known one has fields at most 43, and the near-miss analysis of §7 shows the structured candidates that could have produced larger ones are globally obstructed. The scoped negative: below 2^{28} no directed 3-cycle hit contains a field greater than 43.

6 Global 2-cycle classification

We now replace the census's finite negatives, degree pair by degree pair, with theorems. Throughout, $p < q$ are primes at least 5 forming a prime-order 2-cycle, $c = q - p$ (a positive even integer), and Φ_k is the k-th cyclotomic polynomial; exact degree k_1 on the first curve gives $q \mid \Phi_{k_1}(p)$, hence $q \mid \Phi_{k_1}(-c)$, and exact degree k_2 gives $p \mid \Phi_{k_2}(q)$, hence $p \mid \Phi_{k_2}(c)$.

6.1 The MNT orientations

Theorem 7 (degree-$(6,4)$ and $(4,6)$ cycles are MNT). PROVED If the exact degree pair is $(6,4)$ then $p = 4x^2 + 1$, $q = 4x^2 + 2x + 1$ for an integer $x \geq 1$; if it is $(4,6)$ then $p = 4x^2 - 2x + 1$, $q = 4x^2 + 1$. Thus every such cycle is a specialization of the MNT6/MNT4 cycle polynomials [1], [2].

Proof. Take degrees $(6,4)$. Degree 4 on the second curve gives $p \mid \Phi_4(q) = q^2 + 1$; since $q \equiv c \bmod p$, write $c^2 + 1 = mp$ with $m \geq 1$. Degree 6 gives $q \mid \Phi_6(p) = p^2 - p + 1$, and $p \equiv -c \bmod q$ turns this into $q \mid c^2 + c + 1$. Now

$$c^2 + c + 1 = mp + c = m(p + c) - (m - 1)c = mq - (m - 1)c, \tag{3}$$

so $q \mid (m-1)c$. Hasse gives $(c-1)^2 \leq 4p$, hence for $p \geq 7$

$$(c^2 + 1)/p \leq 4 + 4/\sqrt{p} + 2/p < q, \tag{4}$$

so $0 < m < q$; also $0 < c < q$ and q prime give $q \nmid c$. Therefore $q \mid m - 1$ forces $m = 1$, i.e. $p = c^2 + 1$, $q = c^2 + c + 1$, and $c = 2x$ gives the first parameterization. (The boundary case $p = 5$ forces $q = 7$ and again $m = 1$ directly.) The $(4,6)$ orientation is symmetric: $q \mid c^2 + 1 = mq$-side and $p \mid c^2 - c + 1 = mp + (m-1)c$ force $m = 1$, giving $q = c^2 + 1$, $p = c^2 - c + 1$. □

This is a parameter-level **converse**: Chiesa–Chua–Weidner classify cycles **within** the MNT families [2]; Theorem 7 says any prime-order 2-cycle exhibiting the MNT degree pattern lies on the MNT polynomials. No novelty is claimed for the method, which is elementary.

6.2 Both degrees quadratic: $\{3, 4, 6\}$

Theorem 8 (classification for degrees in $\{3, 4, 6\}$). PROVED If both exact degrees lie in $\{3, 4, 6\}$, the ordered pair is $(6, 4)$ or $(4, 6)$ — hence the cycle is MNT by Theorem 7. No other ordered pair in $\{3, 4, 6\}^2$ occurs.

Proof. For $k \in \{3, 4, 6\}$, $\Phi_k(-c) = c^2 + ac + 1$ and $\Phi_k(c) = c^2 + bc + 1$ with $a \in \{-1, 0, 1\}$, $b = -a$ in degree order. Writing $\Phi_{k_1}(-c) = mq$ and $\Phi_{k_2}(c) = np$, Hasse bounds give $1 \le m \le 3$ and $1 \le n \le 6$. Eliminating p, q via $q - p = c$ yields the exact integer identity

$$(n - m)c^2 + (na - mb - mn)c + (n - m) = 0. \tag{5}$$

If $m = n = s$ this vanishes identically iff $s = a - b$, whose positive solutions are exactly $(k_1, k_2, s) = (6, 4, 1)$, $(4, 6, 1)$, and $(6, 6, 2)$; the first two are the MNT identities, and the third is impossible because $\Phi_6(-c) = c^2 + c + 1$ is odd while $2q$ is even. For $m \neq n$ the equation is a genuine quadratic over the finite multiplier box; exhausting it yields exactly eight positive integral roots, each rejected by parity of the gap, non-integral quotients, or fields smaller than 5. The full 11-row certificate is `classify_quadratic_degree_pairs_k3-4-6_20260718.csv`. □

6.3 Mixed quadratic/quartic degrees

Theorem 9 (mixed classification). PROVED If one exact degree lies in $Q_2 = \{3, 4, 6\}$ and the other in $Q_4 = \{5, 8, 10, 12\}$, the only prime-order 2-cycle is

$$(p, q; k_1, k_2) = (7, 11; 10, 3). \tag{6}$$

Proof. Suppose $k_2 \in Q_2$, so $\Phi_{k_2}(c) = np$ with $1 \le n \le 6$; then $nq = \Phi_{k_2}(c) + nc =: D_n(c)$ is a **monic** quadratic in c. The quartic condition $q \mid \Phi_{k_1}(-c)$ becomes $D_n(c) \mid n\Phi_{k_1}(-c)$, and polynomial division by the monic D_n leaves an integral **linear** remainder $R_n(c) = u_n c + v_n$; divisibility forces $D_n(c) \mid R_n(c)$. For $c > |d| + |u| + |v| + 2$ (writing $D = c^2 + dc + 1$) one has $D(c) > |R(c)|$, so only finitely many gaps survive — provided $R \neq 0$, which holds in **all** 108 bounded multiplier cases (largest surviving even-gap bound: 2,649). The orientation with $k_1 \in Q_2$ is symmetric. EMPIRICAL: complete 116-row certificate Exhausting every retained gap leaves exactly one row with prime Hasse fields and the prescribed exact degrees: $k_1 = 10$, $k_2 = 3$, $n = 3$, $c = 4$, $(p, q) = (7, 11)$. □

6.4 Both degrees quartic: the genus-one wall

Theorem 10 (quartic classification). PROVED If both exact degrees lie in $Q_4 = \{5, 8, 10, 12\}$, the only prime-order 2-cycle is

$$(p, q; k_1, k_2) = (11, 13; 12, 10). \tag{7}$$

The proof is the technical core of the record; we give its architecture and the exact bookkeeping.

Quotient-difference reduction. PROVED Write $F(c) = \Phi_{k_1}(-c) = mq$ and $H(c) = \Phi_{k_2}(c) = np$. Since every Φ_k with $k \in Q_4$ has constant term 1, both $F(c)$ and $H(c)$ are $\equiv 1 \bmod c$,

and $p \equiv q \bmod c$ with $\gcd(p, c) = 1$ forces $m \equiv n \bmod c$; write $n = m + hc$. The degree-≤ 2 polynomial $G(c) = (F(c) - H(c))/c$ satisfies $G = m - hp$, and substitution gives

$$hp^2 + (hc + G(c))p - H(c) = 0. \tag{8}$$

For $h \neq 0$ an integral solution requires the discriminant to be a square:

$$y^2 = D_{k_1,k_2,h}(c) := (hc + G(c))^2 + 4hH(c), \tag{9}$$

a quartic in c — a genus-one integral-point problem for each (k_1, k_2, h).

Bounding h. PROVED The two Hasse inequalities give the explicit decreasing bound $|h| \leq B(c)$ with $B(108) < 25$; hence $c \geq 108$ implies $|h| \leq 24$. The complementary gaps $c = 2, 4, \ldots, 106$ are a complete finite audit: for all 16 ordered degree pairs and all 53 gaps, every prime divisor $p \mid \Phi_{k_2}(c)$ is enumerated and both divisibilities, primality, Hasse, and exact orders are checked — 848 cases, whose only cycle is $(11, 13; 12, 10)$ at $c = 2$.

The 784 large-gap rows. EMPIRICAL: exact symbolic reduction, all 16 pairs, |h| <= 24 The 16×49 discriminant rows split into 750 genus-one equations, 10 nonsquare constants times polynomial squares, 8 genus-zero equations, 12 finite $h = 0$ divisibility cases, and 4 impossible $h = 0, G = 0$ cases; no discriminant is a square polynomial. PROVED The 34 degenerate rows are closed by integral-root and Cauchy-bound arguments; none yields a large-gap cycle.

Closing the 750 genus-one rows. PROVED Congruence conditions modulo powers of two and odd primes through 251 eliminate 630 rows; exact sign analysis on $c \geq 108$ eliminates 69 more; higher-power Hensel lifting kills four rows whose singular solutions modulo 3 and 13 do not lift modulo 9 or
169. The 47 survivors normalize to 29 curves. Figure 2 shows the

funnel.
Two independent closures finish: EMPIRICAL: every even gap 108 <= c <= 10^7, all 51 pre-Hensel curves an exact CRT-wheel search over 11,333,558 curve/gap candidates finds no integral point; and EMPIRICAL: exact Magma V2.29-8 computations of the 29 final curves, 22 have complete integral-point lists (only $c = 0$, once also $c = \pm 1$), five are everywhere locally soluble yet have **empty fake 2-Selmer sets**, and the last symmetric pair (one curve up to $c \mapsto -c$) has rank bounds $[0, 0]$ and torsion $\mathbb{Z}/2\mathbb{Z}$, so its only rational points sit at $c = \pm 1$ [5]. No surviving equation contributes a cycle.

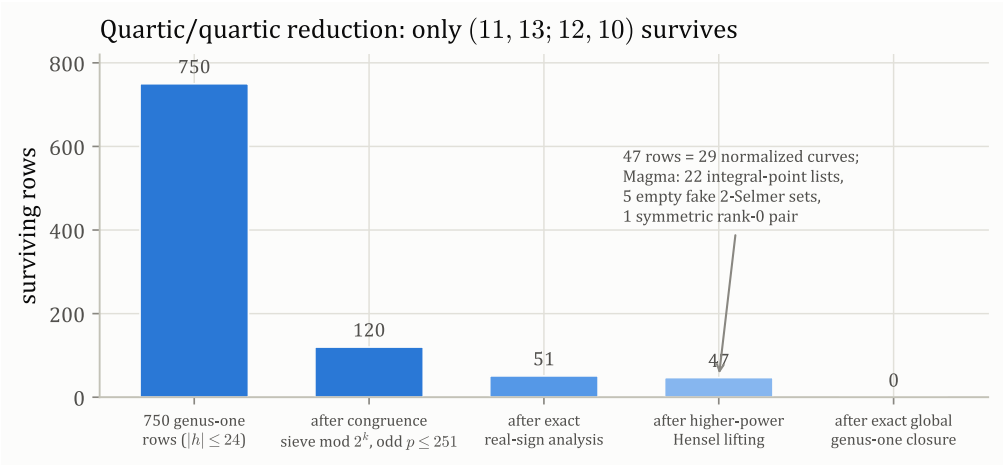

Figure 2: PROVED The quartic/quartic elimination funnel: 750 genus-one rows from the quotient-difference reduction are closed by congruence sieving, exact real-sign analysis, Hensel lifting, and exact global genus-one computations. The parallel small-gap ($c \leq 106$) and degenerate-row audits contribute the unique surviving cycle $(11, 13; 12, 10)$.

6.5 The classification map

Corollary 11 (complete low-cyclotomic-degree classification). PROVED Every prime-order 2-cycle whose two exact embedding degrees lie in $\{3, 4, 5, 6, 8, 10, 12\}$ is one of: an MNT cycle in one of the two orientations of Theorem 7, or the tiny cycles $(7, 11; 10, 3)$ and $(11, 13; 12, 10)$.

The set $\{3, 4, 5, 6, 8, 10, 12\}$ is exactly the set of $k \leq 12$ whose cyclotomic polynomial has degree at most 4 (with $k \neq 1, 2$). The remaining degrees 7, 9, 11 have $\deg \Phi_k \in \{6, 10\}$, where the quotient-remainder method meets genuinely higher-genus equations; they remain open globally, constrained below 2^{28} only by the census. Figure 3 draws the resulting map.

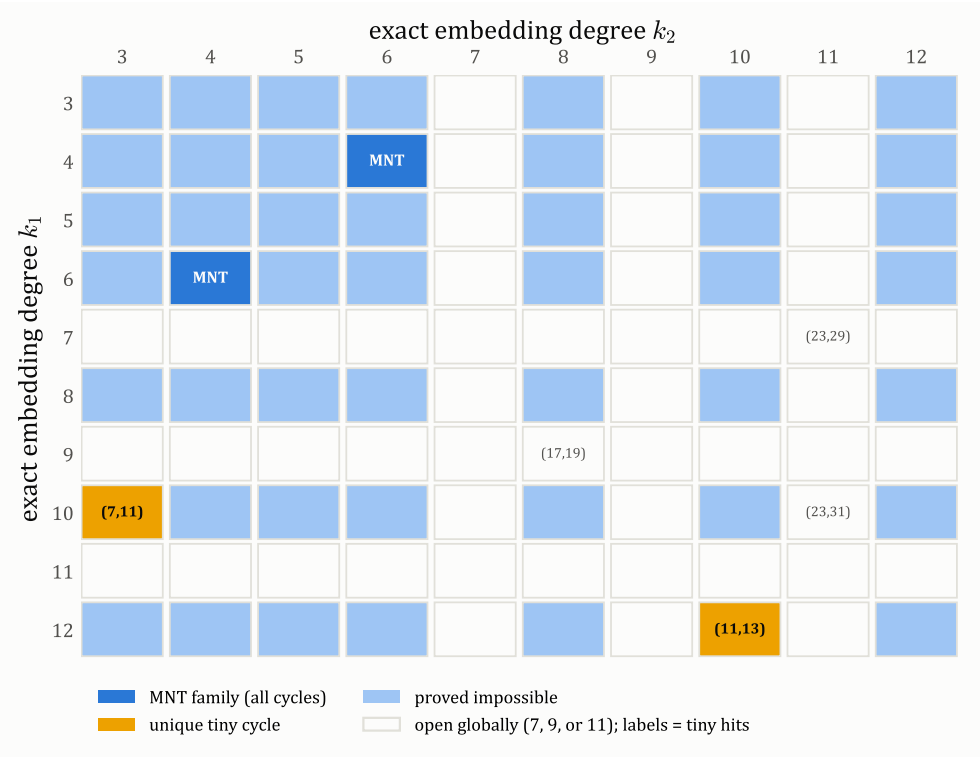

Figure 3: Status of every ordered exact-degree pair $(k_1, k_2) \in \{3, \ldots, 12\}^2$. Blue: the two MNT orientations (all cycles known, Theorem 7). Yellow: the two provably unique tiny cycles (Theorems 9, 10). Light blue: proved empty (Theorems 8–10). White: open globally — every such pair involves degree 7, 9, or 11; the three labels mark the tiny census hits in the open region, which are the only ones below 2^{28}.

7 Length-3 structure

The 3-cycle census's most conspicuous near-misses are **consecutive MNT chains**: prime triples $(A, B, C) = (4x^2 - 2x + 1, 4x^2 + 1, 4x^2 + 2x + 1)$, in which the four inner edges automatically carry degrees 4 and 6. Do they ever close?

> **Theorem 12** (the consecutive MNT chain never closes). PROVED For no integer $x \geq 1$ with A, B, C prime does either orientation of the chain close to a directed 3-cycle with all exact embedding degrees in $\{3, \ldots, 12\}$.

Proof. The closing edge requires $A \mid (4x)^k - 1$ (forward) or $C \mid (-4x)^k - 1$ (reverse) for some $k \leq 12$. Modulo A put $y = 4x$ (modulo C, $y = -4x$); in both cases $y^2 \equiv 2y - 4$. Writing $y^k \equiv a_k y + b_k$ gives the recurrence $a_{k+1} = 2a_k + b_k$, $b_{k+1} = -4a_k$, whose values for $k \leq 12$ satisfy $|a_k| \leq 1024$ and $|b_k - 1| \leq 4095$, with $\pm 4a_k x + b_k - 1$ never zero for integral $x \geq 1$. So the divisibility target is a **nonzero** integer of absolute value at most $4096x + 4095$, while $A - (4096x + 4095) = 4x^2 - 4098x - 4094 > 0$ for $x \geq 1026$: the divisibilities are impossible there. EMPIRICAL: deterministic exhaustion, 1 <= x <= 1025 Below the cutoff, exactly four all-prime triples occur ($x = 3, 45, 480, 987$) and neither orientation closes with degree at most 12. □

> **Theorem 13** (equal-gap (4,6) paths are MNT chains). PROVED If distinct primes $p, q, r \geq 5$ carry directed Hasse edges $p \to q$ and $q \to r$ with exact degrees 4 and 6 and equal signed gaps

> $q - p = r - q$, then (p, q, r) is one of the two orientations of the consecutive MNT chain. Consequently — combining with the previous theorem — no such path ever completes to a primary directed 3-cycle, **regardless of parameter size**.

Proof. Put $d = q - p = r - q > 0$ (the decreasing orientation is symmetric). Degree 4 gives $q \mid d^2 + 1 = mq$, and Hasse bounds force $1 \le m < 4$. Degree 6 gives $r \mid d^2 + d + 1 = mr - (m-1)d$, so $r \mid (m-1)d$ with $0 < d < r$ and $m < 4 < r$, forcing $m = 1$. Then $q = d^2 + 1$, $p = d^2 - d + 1$, $r = d^2 + d + 1$, and $d = 2x$. □

EMPIRICAL: all 61 near-misses below 2^28 The two theorems organize the near-miss ledger: of the 61 two-of-three near-misses, 26 are orientations of the globally excluded MNT chain (at $x = 3, 45, 480, 987$ and their larger analogues) and 35 are residual isolated rows — only **two** of which lie above 2^{16}, with target-degree pairs $(5, 11)$ and $(8, 9)$ and astronomically non-pairing closing degrees 483,882 and 12,053,055. Figure 4 shows the ledger.

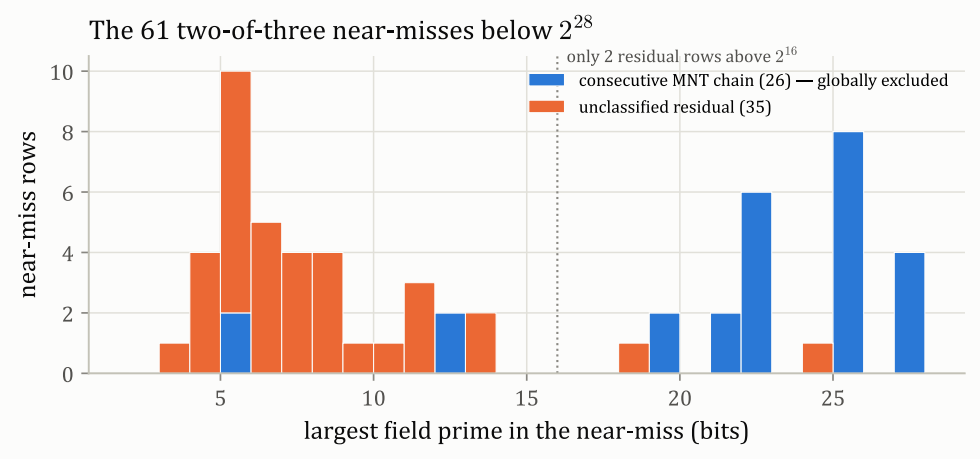

Figure 4: EMPIRICAL: classified ledger, n = 61 The 61 directed two-of-three near-misses below 2^{28} by largest field prime. The MNT-chain class (blue) is globally excluded by Theorems 12–13; the residual class (orange) thins out rapidly — two rows above 2^{16}, none above 2^{25}. Data: `classify_three_cycle_near_misses_n61_20260718.csv`.

8 One-axis relaxation: degrees up to 18

EMPIRICAL: 5 <= p_i < 2^16, exact degrees 3–18 Raising only the degree ceiling from 12 to 18 in the 16-bit space increases the 2-cycle count from 26 to 36 and the directed 3-cycle count from 5 to 12; all 72 2-cycle and 36 3-cycle curve equations were constructed and independently counted. The relaxed exceptional 2-cycles have larger field at most 271, and every relaxed 3-cycle has all fields at most 673. The pattern — a handful of tiny sporadic objects and then silence — matches the primary census, but this relaxation is only a 16-bit result and is not extended by any global theorem here.

9 Limitations

PROVED The finite negative statements cover exactly: distinct prime fields below 2^{28}, exact embedding degrees 3 through 12 (18 at 16 bits), prime-order (hence cyclic, distinct-field) cycles. They say nothing about fields at least 2^{28}, higher degrees, composite orders, repeated primes, or polynomial families with no instance inside the range. The global theorems are the stated-class exceptions: degree pairs inside $\{3, 4, 5, 6, 8, 10, 12\}^2$ and the consecutive-MNT-chain obstruction

hold without size bounds. Exact degrees 7, 9, and 11 — cyclotomic degrees 6 and 10 — are outside every global 2-cycle theorem here, and the general length-3 question is open outside the MNT-chain class. The near-miss ledgers store isogeny-class parameters only and are not full cycle candidates. SageMath was unavailable throughout; point counting uses the shared BSGS/enumeration routines, and the final quartic closures use exact Magma V2.29-8 computations with local parser regressions [5]. Two anomalous empty `IntegralQuarticPoints` outputs (QG012/QG013) are **not** relied upon; the independent rank-zero proof closes those curves.

10 Conclusion

Within the reach of quadratic and quartic cyclotomic arithmetic, the classification of prime-order pairing-friendly 2-cycles is now complete: MNT's two orientations plus exactly two tiny sporadic cycles, nothing else — and the 28-bit census confirms the picture empirically with five sporadic 2-cycles frozen since field 31 and five 3-cycles frozen since field 43. The first genuinely new algebra required to go further is explicit: degree pairs involving 7, 9, or 11 lead to higher-genus analogues of the genus-one wall closed here, and the length-3 problem beyond MNT chains has no comparable reduction yet. For applications, the practical reading is sobering: production-scale pairing-friendly cycles outside MNT remain unconstructed, every known non-MNT object is cryptographically tiny, and the standard $\rho < 2$ target is vacuous as usually stated (Proposition 4) — a sharper cycle-quality metric is needed before "cycles with good ρ" is even a well-posed goal.

Reproducibility

All census, construction, classification, and certificate artifacts are dated, seeded files in the research record: the seven two-cycle and seven three-cycle summary JSONs, the `construct_hit_cycles_*` and `construct_three_cycle_hits_*` equation ledgers, the `verify_mnt_parameterization_n328` and `classify_three_cycle_near_misses_n61` classification CSVs, the 848-case and 116-row finite certificates, and the Magma transcripts `magma_*_20260718.txt`. Search code is `code/search_two_cycles*.py` / `search_three_cycles*.py` (exhaustive and root-enumeration variants, byte-identical outputs at overlapping bounds), with 58 problem-local tests plus 70 shared tests passing on Python 3.13.4 / SymPy 1.14.0. The figures are regenerated from these artifacts by `papers/figures/P4.2/make.py`. Frozen protocol files (`SEARCH_SPACE.md`, `THREE_CYCLE_CONDITIONS.md`) predate the searches they govern. Every claim carries its epistemic tag; untagged sentences are exposition.

References

[1] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, vol. E84-A, no. 5, pp. 1234–1243, 2001.

[2] A. Chiesa, L. Chua, and M. Weidner, "On cycles of pairing-friendly elliptic curves," *SIAM Journal on Applied Algebra and Geometry*, vol. 3, no. 2, pp. 175–192, 2019.

[3] M. Belles-Munoz, J. J. Urroz, and J. Silva, "Revisiting cycles of pairing-friendly elliptic curves." 2022.

[4] W. C. Waterhouse, "Abelian varieties over finite fields," *Annales scientifiques de l'École Normale Supérieure*, vol. 2, no. 4, pp. 521–560, 1969.

[5] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system I: The user language,” *Journal of Symbolic Computation*, vol. 24, no. 3–4, pp. 235–265, 1997.