The Joux–Buchmann Bridge Revisited

Fixed-Degree Obstructions and Continued-Fraction Loophole Closures in Real Quadratic Semiprime Factoring

Project: Faktorisierung 1
Document type: consolidated research paper / revised technical manuscript
Status: revised draft
Language: English

Abstract

We revisit the proposed bridge from the Joux/BGJT quasi-polynomial descent for discrete logarithms in small-characteristic finite fields to Buchmann-style regulator and class-group computations in real quadratic fields

$$K = \mathbf{Q}(\sqrt{N}), \qquad N = pq.$$

The original motivating hope was that a sufficiently strong improvement in real quadratic regulator computation could yield an asymptotic factoring algorithm for semiprimes beyond the Number Field Sieve threshold $L[1/3]$.

The present paper sharpens the negative side of that program in three ways.

First, we isolate a fully rigorous **Frobenius obstruction**. The only intrinsic $\mathbf{Q}$-algebra endomorphisms of K are the identity and conjugation. Any public residue-level projector that separates the hidden p- and q-components of $\mathbf{Z}/N\mathbf{Z}$ produces a nontrivial CRT idempotent and therefore factors N. Thus a Joux-style Frobenius replacement is unavailable in the real quadratic semiprime setting.

Second, we isolate a fully rigorous **tower obstruction** in the bounded-degree, polynomial-norm principal-relation regime. Real quadratic fields have no nontrivial internal tower. Any public external tower of bounded degree has only bounded length, and any descent that remains in the fixed-degree smooth principal-relation regime keeps relation norms polynomial in the discriminant. Under the standard smoothness heuristic, this forces the familiar $L[1/2]$ balance. This structural theorem does **not** address towers whose degree grows with $\log N$ or more general NFS-style variable-degree constructions; it only rules out the bounded-degree, polynomial-norm principal-relation regime made explicit below.

Third, we reformulate the remaining loopholes via the exact near-square dynamics of continued fractions and reduced ideals. The rare-event states with small denominator Q_i are characterized exactly, assembled into a functional divisor graph, and shown to correspond to reduced narrow-class cycles. This yields several further negative results: graph-only cycle selection collapses to narrow-class selection; on the thin family of small split ideals, dynamic principal-cycle

membership is equivalent to static principality; and principal-genus admissibility does not remove the odd part of the narrow class group.

The resulting picture is structurally sharp. Within the Joux-style smooth-relation paradigm, no sub-$L[1/2]$ route is found. The only substantially different escape route isolated in this pass is conjectural and external to the proved negative results: an explicit real-multiplication reciprocity mechanism of Darmon–Vonk / Hilbert-12 type that would provide a finite principal-class separating signature. No theorem-level algorithm follows from this conjectural branch.

---

1. Introduction

Let

$$N = pq$$

be a balanced semiprime. Set

$$K = \mathbf{Q}(\sqrt{N}),$$

and let D_K denote the discriminant of K. The regulator R_K of K is the logarithm of a fundamental unit. A sufficiently fast algorithm for R_K, combined with the real quadratic class number formula and the usual regulator-to-factorization pipeline, would imply a faster factoring method for N.

The concrete question motivating this paper was whether the Joux/BGJT mechanism for discrete logarithms in finite fields of small characteristic admits an analogue in the Buchmann framework for real quadratic class groups and regulators. The target was an asymptotic factoring algorithm beating

$$L_N[1/3].$$

The present paper gives a revised and more rigorous account of the negative outcome. The theorem-level negative results are deliberately scoped: they rule out the Joux–Buchmann bridge in the **bounded-degree, polynomial-norm smooth principal-relation regime**, not every conceivable variable-degree or non-principal-relation construction. It replaces the earlier compact bridge note by combining the original K3/K4 obstruction analysis with a new exact continued-fraction/divisor-graph study of the remaining internal loopholes. The most important improvements are:

1. The main obstruction theorems are now stated and proved in paper-safe form.
2. The continued-fraction and infrastructure remainder has been reformulated through exact near-square identities and a functional divisor graph.
3. Several apparently independent loopholes are shown to collapse back to principality or narrow-class selection.

We emphasize what is and is not proved. We do **not** prove that no classical breakthrough exists. We do prove that the specific Joux–Buchmann bridge fails inside the fixed-degree smooth principal-relation world, and that several natural residual loopholes collapse to already understood class-group/principality problems.

---

2. The Joux skeleton and its real quadratic translation

We decompose the finite-field descent into five structural components.

ID	Component	Structural role
K1	Smoothness basis	A small generating family supporting relation collection and descent
K2	On-the-fly elimination	Target-specific relations that reduce complexity
K3	Frobenius symmetry	Large public fixed-locus identity plus low-complexity rewrite
K4	Recursive tower/subfield descent	Iterated complexity reduction with bounded branching
K5	Representation switching	Choice of coordinates where descent is cheap

For real quadratic fields:

- K1 survives in weak form: factor bases of prime ideals exist.
- K2 survives only weakly: targeted principal-ideal relations exist, but no BGJT-style elimination is known.
- K3 fails intrinsically.
- K4 fails internally and becomes structurally ineffective in bounded-degree external towers.
- K5 survives representationally, but not asymptotically in fixed degree.

The decisive obstructions therefore sit at K3/K4.

---

3. Main results

We separate the core statements into theorem-level structural obstructions and a conditional smoothness corollary. Taken together, Theorems T1–T5 support the

following single message: within the bounded-degree smooth principal-relation interpretation of the Joux–Buchmann bridge, every serious internal loophole either collapses to principality/narrow-class selection or remains outside theorem-level reach.

Theorem T1 (Frobenius obstruction)

Let

$$N = pq$$

with distinct odd primes, let

$$K = \mathbf{Q}(\sqrt{N}), \qquad R = \mathbf{Z}/N\mathbf{Z}.$$

Then:

1. every $\mathbf{Q}$-algebra endomorphism of K is either the identity or the nontrivial Galois involution;
2. any public residue-level projector separating the hidden p- and q-components of R produces a nontrivial idempotent in R, hence factors N.

In particular, there is no public Frobenius-like symmetry of the type required by Joux/BGJT unless factorization data is already present.

Theorem $\mathrm{T2}_{\mathrm{str}}$ (Structural tower obstruction in the bounded-degree polynomial-norm regime)

Let

$$K = \mathbf{Q}(\sqrt{N})$$

with $[K : \mathbf{Q}] = 2$. Consider any descent built from principal-ideal relations inside a public bounded-degree tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_t = L$$

with $[L : \mathbf{Q}] \le C$, where all relation elements satisfy

$$|N_{L/\mathbf{Q}}(\alpha)| \le |D_K|^A$$

for some absolute constant A. Then:

1. there is no nontrivial internal tower inside K;
2. any such external tower has bounded length $t = O(1)$;
3. no asymptotically growing Joux-style recursive depth can arise in this regime.

Scope note. Theorem $\mathrm{T2}_{\mathrm{str}}$ does **not** exclude external towers whose total degree grows with $\log N$ or with another asymptotic parameter, nor non-principal-relation methods. Its content is exactly the bounded-degree, polynomial-norm principal-relation regime formalized in Definitions 5.1–5.2.

Corollary T2$_{\mathrm{sm}}$ (Conditional $L[1/2]$ barrier)

Under the standard random-norm smoothness heuristic for these polynomial-size relation norms, the optimal relation-collection exponent in the fixed-degree principal-relation regime is

$$L_{D_K}[1/2].$$

Thus no $L[1/3]$-type behavior can emerge inside this paradigm.

Theorem T3 (Graph-only cycle selection collapses to narrow-class selection)

The exact near-square dynamics of $\sqrt{D}$ define a functional divisor graph whose directed cycles are exactly the reduced cycles of narrow ideal classes. The cycle through the base state $(0, 1)$ is the principal narrow class. Therefore any graph-only procedure that selects the principal cycle among all graph cycles is exactly a principal narrow-class selection procedure in different language.

Theorem T4 (Dynamic principality equals static principality on the thin small split family)

For a small split prime ℓ and a local root $s^2 \equiv D \pmod{\ell}$, the ideal

$$\mathfrak{a}_{\ell,s} = (\ell, \sqrt{D} + s)$$

is principal if and only if it appears on the principal cycle, and this is equivalent to the existence of a Pell-type solution

$$x^2 - Dy^2 = \pm\ell, \qquad x \equiv -sy \pmod{\ell}.$$

Thus dynamic principal-cycle membership supplies no extra filter beyond static principality on this thin family.

Theorem T5 (The odd part remains visible on the thin split family)

Let $C = \mathrm{Cl}^+(K)$. Every class in $2C$, hence in particular every odd class component, is realized by infinitely many split prime ideals of the form $(\ell, \sqrt{D}+s)$. Therefore principal-genus admissibility does not collapse principality to a purely 2-adic condition on the thin split family.

The proofs are given below.

---

4. Theorem T1: Frobenius obstruction

We first formalize "component separation".

Definition 4.1 (public component projector)

A **public component projector** on

$$R = \mathbf{Z}/N\mathbf{Z}$$

is a publicly computable ring endomorphism

$$\pi : R \to R$$

(not necessarily unital) such that under the Chinese remainder isomorphism

$$\chi : R \xrightarrow{\sim} \mathbf{F}_p \times \mathbf{F}_q$$

one has either

$$\chi \circ \pi \circ \chi^{-1}(x, y) = (x, 0)$$

for all (x, y), or

$$\chi \circ \pi \circ \chi^{-1}(x, y) = (0, y).$$

This is the precise meaning of "publicly separating the hidden p- and q-components".

Lemma 4.2

Every $\mathbf{Q}$-algebra endomorphism of $K = \mathbf{Q}(\sqrt{N})$ is a $\mathbf{Q}$-automorphism.

Proof A $\mathbf{Q}$-algebra endomorphism of a field is injective. Since $K/\mathbf{Q}$ is finite-dimensional, any injective $\mathbf{Q}$-linear endomorphism is surjective. □

Lemma 4.3

The only $\mathbf{Q}$-automorphisms of $K = \mathbf{Q}(\sqrt{N})$ are

$$\mathrm{id} \qquad \text{and} \qquad \iota : \sqrt{N} \mapsto -\sqrt{N}.$$

Proof The element $\sqrt{N}$ has minimal polynomial

$$X^2 - N$$

over $\mathbf{Q}$. Any $\mathbf{Q}$-automorphism sends $\sqrt{N}$ to another root of this polynomial, hence to $\pm\sqrt{N}$. Since $K = \mathbf{Q}(\sqrt{N})$, this determines the automorphism. □

Lemma 4.4

The idempotents in

$$R = \mathbf{Z}/N\mathbf{Z}$$

are exactly the CRT-images of

$$(0, 0),\ (1, 1),\ (1, 0),\ (0, 1)$$

in $\mathbf{F}_p \times \mathbf{F}_q$.

Proof Under CRT,

$$R \cong \mathbf{F}_p \times \mathbf{F}_q.$$

An element (a, b) is idempotent iff $a^2 = a$ and $b^2 = b$, hence iff $a, b \in \{0, 1\}$. $\square$

Lemma 4.5

Let $e \in R$ be a nontrivial idempotent. Then one can recover a nontrivial factor of N from

$$\gcd(\widetilde{e}, N) \qquad \text{or} \qquad \gcd(\widetilde{e} - 1, N),$$

where $\widetilde{e} \in \mathbf{Z}$ is any lift of e.

Proof Under CRT, e is either $(1, 0)$ or $(0, 1)$. In the first case,

$$e \equiv 1 \pmod{p}, \qquad e \equiv 0 \pmod{q},$$

so $\gcd(\widetilde{e}, N) = q$ and $\gcd(\widetilde{e} - 1, N) = p$. The second case is symmetric. $\square$

Lemma 4.6

If $\pi : R \to R$ is a public component projector, then

$$e := \pi(1_R)$$

is a nontrivial idempotent.

Proof Under CRT, e is either $(1, 0)$ or $(0, 1)$, hence nontrivial and idempotent. $\square$

Proof of Theorem T1

Part (1) follows from Lemmas 4.2 and 4.3.

For part (2), let π be a public component projector. By Lemma 4.6, $e = \pi(1_R)$ is a nontrivial idempotent. By Lemma 4.5, one then recovers a nontrivial factor of N. $\square$

Corollary 4.7

A public residue-level Frobenius substitute of projector type cannot exist in the semiprime real quadratic setting unless factorization data is already present.

---

5. Theorem T2$_{\mathrm{str}}$: structural tower obstruction

Definition 5.1 (public bounded-degree tower)

A **public bounded-degree tower over** K is a chain

$$K = K_0 \subset K_1 \subset \cdots \subset K_t = L$$

such that:

1. each field K_i is explicitly constructible from N alone;
2. the construction does not use the factorization $N = pq$;
3. there is an absolute constant C with

$$[L : \mathbf{Q}] \leq C.$$

Definition 5.2 (fixed-degree principal-relation regime)

A descent lies in the **fixed-degree principal-relation regime** if:

1. all relations are generated from principal ideals (α) in one of the K_i;
2. these relations are pushed back to K by the usual ideal-theoretic maps;
3. the relation elements satisfy

$$|N_{L/\mathbf{Q}}(\alpha)| \leq |D_K|^A$$

for some absolute constant A.

Lemma 5.3

If $[K : \mathbf{Q}] = 2$, then K has no proper intermediate field.

Proof Let

$$\mathbf{Q} \subseteq F \subseteq K.$$

By the tower law,

$$[K : \mathbf{Q}] = [K : F][F : \mathbf{Q}] = 2.$$

Since 2 is prime, either $F = \mathbf{Q}$ or $F = K$. □

Lemma 5.4

Let

$$K = K_0 \subset K_1 \subset \cdots \subset K_t = L$$

be a strict tower of number fields. Then

$$[L : K] \geq 2^t.$$

Proof Each strict inclusion satisfies $[K_i : K_{i-1}] \geq 2$. Multiplying gives the claim. □

Corollary 5.5

If $[L : \mathbf{Q}] \leq C$ and $[K : \mathbf{Q}] = 2$, then

$$t \leq \left\lfloor \log_2\left(\frac{C}{2}\right) \right\rfloor.$$

Proof By Lemma 5.4,

$$[L : \mathbf{Q}] = [L : K][K : \mathbf{Q}] \geq 2^t \cdot 2 = 2^{t+1}.$$

Thus $2^{t+1} \leq C$. □

Proof of Theorem T2$_{\mathrm{str}}$

Part (1) is Lemma 5.3.

Part (2) is Corollary 5.5, hence any public bounded-degree external tower has length $O(1)$.

Part (3) follows immediately: bounded tower length forbids asymptotically growing recursive depth. In addition, the polynomial-norm condition from Definition 5.2 is preserved throughout the tower, so the entire construction remains in the polynomial-norm world. Since Joux-style speedup requires many recursive complexity reductions, no analogous structural resource is available here. □

Corollary 5.6 (= Corollary T2$_{\mathrm{sm}}$, Conditional $L[1/2]$ barrier)

Assume the standard random-norm smoothness heuristic in the fixed-degree principal-relation regime. Then the optimal relation-collection exponent is $L_{D_K}[1/2]$.

Proof Let

$$y = L_{D_K}[a, c].$$

For polynomial-size relation norms $X = |D_K|^{\Theta(1)}$, the smoothness probability is

$$L_{D_K}[-(1-a), O(1)]$$

under the standard Dickman/CEP heuristic. The factor base has size

$$L_{D_K}[a, O(1)].$$

Hence the relation-collection complexity is

$$L_{D_K}[\max(a, 1-a), O(1)],$$

minimized at $a = 1/2$. □

5A. Why the continued-fraction remainder is the next place to look

The tower obstruction closes the Joux-style route only inside the bounded-degree polynomial-norm principal-relation regime. It does **not** by itself dispose of the classical real-quadratic infrastructure. In particular, one could still imagine that the principal cycle of reduced ideals has a semiprime-specific rare-event structure that is invisible to smoothness heuristics and to K3/K4 considerations.

The next sections therefore change viewpoint completely. Instead of asking for a new tower or a new relation family, we ask whether the continued-fraction dynamics of $\sqrt{D}$ contains an exact low-denominator skeleton whose geometry might distinguish the principal cycle from the other narrow-class cycles. The near-square identities below are the mechanism by which this remainder can be studied without returning to the original Joux-style framework.

---

6. Exact near-square dynamics and the functional divisor graph

We now turn to the only serious remainder inside the original real quadratic framework: continued fractions, reduced states, and rare low-denominator events.

Let

$$D > 0$$

be a nonsquare discriminant and write

$$m := \lfloor \sqrt{D} \rfloor, \qquad r := D - m^2, \qquad F_D(t) := D - (m-t)^2 = r + 2mt - t^2.$$

Let

$$\alpha_i = \frac{\sqrt{D} + P_i}{Q_i} \qquad (i \in \mathbf{Z}/\ell\mathbf{Z})$$

be the cyclic indexing of the complete quotients of $\sqrt{D}$, chosen so that

$$(P_0, Q_0) = (m, 1).$$

Set

$$t_i := m - P_i.$$

Then $(t_0, Q_0) = (0, 1)$.

Proposition 6.1 (exact near-square factorization)

For every complete quotient,

$$Q_{i-1}Q_i = D - P_i^2 = F_D(t_i).$$

Proof The standard identity is $Q_{i-1}Q_i = D - P_i^2$. Since $P_i = m - t_i$, one has

$$D - P_i^2 = D - (m - t_i)^2 = F_D(t_i).$$

□

Proposition 6.2 (exact (t_i, Q_i)-dynamics)

One has

$$t_{i+1} = (2m - t_i) \bmod Q_i, \qquad Q_{i+1} = \frac{F_D(t_{i+1})}{Q_i},$$

where t_{i+1} denotes the unique residue in $[0, Q_i)$.

Proof From

$$P_{i+1} = a_i Q_i - P_i$$

we get

$$t_{i+1} = m - P_{i+1} = 2m - t_i - a_i Q_i,$$

hence the congruence modulo Q_i. The formula for Q_{i+1} follows from Proposition 6.1 with index $i + 1$. □

Proposition 6.3 (local characterization of admissible denominators)

Fix $u \in \{0, \dots, m\}$. An integer q is the denominator of a reduced complete quotient of the form

$$\frac{\sqrt{D} + (m - u)}{q}$$

if and only if

$$q \mid F_D(u), \qquad u < q \leq 2m - u.$$

Proof Reduction requires

$$q \mid D - (m - u)^2 = F_D(u)$$

and

$$\sqrt{D} - (m - u) < q < \sqrt{D} + (m - u).$$

Since $\sqrt{D} - m \in [0, 1)$, these inequalities are equivalent for integer q to

$$u < q \leq 2m - u.$$

□

Theorem 6.4 (functional divisor graph realization)

Define

$$V_D := \{(u, q) : 0 \le u < q \le 2m - u,\ q \mid F_D(u)\}$$

and

$$T_D(u, q) := \left(v, \frac{F_D(v)}{q}\right), \qquad v \equiv 2m - u \pmod{q}, \quad 0 \le v < q.$$

Then the complete-quotient cycle of $\sqrt{D}$ is exactly the directed T_D-cycle

$$(t_i, Q_i)_{i \in \mathbf{Z}/\ell\mathbf{Z}}$$

through $(0, 1)$.

Proof By Proposition 6.2,

$$(t_i, Q_i) \mapsto (t_{i+1}, Q_{i+1}) = T_D(t_i, Q_i).$$

By cyclic indexing, $(t_0, Q_0) = (0, 1)$, and after one full period one returns to the same complete quotient. □

Proposition 6.5 (continuant bridge and exact denominator identity)

Let p_n/q_n be the n-th convergent to $\sqrt{D}$, and let the next complete quotient be

$$\alpha_{n+1} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}}.$$

Then:

1. $$\sqrt{D} = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}};$$
2. $$p_n = q_n P_{n+1} + q_{n-1} Q_{n+1}, \qquad D q_n = p_n P_{n+1} + p_{n-1} Q_{n+1};$$
3. $$p_n^2 - D q_n^2 = (-1)^{n+1} Q_{n+1}.$$

Proof The finite-tail continued-fraction identity gives (1). Substitute the complete quotient expression and compare coefficients of 1 and $\sqrt{D}$ to obtain (2). Then use

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$

and simplify as usual to obtain (3). □

Proposition 6.6 (exact prefix/future decomposition)

Define

$$x_n := \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, \dots, a_1].$$

Then:

1. $$p_n - \sqrt{D}\, q_n = \frac{(-1)^{n+1}}{q_n(\alpha_{n+1} + x_n)};$$

2. $$Q_{n+1} = \frac{p_n + \sqrt{D}\, q_n}{q_n(\alpha_{n+1} + x_n)};$$

3. $$q_{n+1} = (a_{n+1} + x_n)q_n, \qquad \log q_{n+1} - \log q_n = \log(a_{n+1} + x_n);$$

4. $$\frac{\sqrt{D}}{a_{n+1} + 2} < Q_{n+1} < \frac{2\sqrt{D} + 1}{a_{n+1}},$$

   hence

   $$Q_{n+1} \asymp \frac{\sqrt{D}}{a_{n+1}}$$

   with absolute constants.

Proof The first formula follows by dividing the standard determinant identity by $q_n\alpha_{n+1} + q_{n-1}$. The second follows by multiplying by $p_n + \sqrt{D}q_n$ and using Proposition 6.5(3). The third is the recurrence for convergent denominators rewritten using x_n. The final inequalities follow from

$$a_{n+1} < \alpha_{n+1} < a_{n+1} + 1, \qquad 0 \le x_n < 1,$$

and the bounds

$$\sqrt{D} < \frac{p_n + \sqrt{D}q_n}{q_n} < 2\sqrt{D} + 1.$$

□

Proposition 6.7 (isolation of low-Q events outside the Fermat zone)

Assume

$$r > M^2.$$

If

$$Q_i \le M,$$

then

$$Q_{i-1} > M \qquad \text{and} \qquad Q_{i+1} > M.$$

Proof If $Q_i \le M$, then $0 \le t_i, t_{i+1} < M$. For $0 \le t < M$, the assumption $r > M^2$ gives

$$F_D(t) = r + 2mt - t^2 > M^2.$$

By Proposition 6.1,

$$Q_{i-1}Q_i = F_D(t_i) > M^2, \qquad Q_iQ_{i+1} = F_D(t_{i+1}) > M^2,$$

so $Q_{i-1}, Q_{i+1} > M$. □

Proposition 6.8 (gcd kernel of low-Q spikes)

Suppose

$$Q_i = q \le M, \qquad u := t_i, \qquad v := t_{i+1}.$$

Then

$$0 \le u, v < q \le M,$$

and

$$q \mid F_D(u), \qquad q \mid F_D(v), \qquad q \mid (2m - u - v), \qquad q \mid (r + uv).$$

Proof From Proposition 6.2,

$$v \equiv 2m - u \pmod{q},$$

so $q \mid (2m - u - v)$. Also

$$F_D(u) = r + 2mu - u^2 = u(2m - u - v) + (r + uv).$$

Since $q \mid F_D(u)$ and $q \mid (2m - u - v)$, we get $q \mid (r + uv)$. □

---

7. Directed cycles and narrow classes

We now connect the exact divisor graph to ideal-class theory.

Proposition 7.1

Every vertex $(u, q) \in V_D$ corresponds to a reduced quadratic state, equivalently to a reduced ideal or reduced indefinite form of discriminant D.

Proof Put

$$s = m - u.$$

By the definition of V_D,

$$q \mid D - s^2$$

and

$$0 \le u < q \le 2m - u.$$

Thus

$$\alpha = \frac{\sqrt{D} + s}{q}$$

is a complete quotient satisfying the usual reduction inequalities

$$\alpha > 1, \qquad -1 < \alpha' < 0,$$

where α' denotes the conjugate. Conversely every reduced complete quotient of $\sqrt{D}$ has this form for a unique pair (u, q) satisfying the same divisibility and inequality conditions.

The standard dictionary between real quadratic continued fractions, primitive indefinite binary quadratic forms, and invertible ideals sends this quotient to the reduced form

$$[q, 2s, (s^2 - D)/q]$$

and to the corresponding reduced oriented ideal generated by q and $\sqrt{D} + s$, up to the harmless convention-dependent sign in s; see, for example, Buchmann–Vollmer [16, Chs. 5–6] or Mollin [17, Chs. 3–5]. This gives the claimed identification. □

Proposition 7.2

The map T_D is exactly the reduction successor map on these reduced states.

Proof Let $\alpha_i = (\sqrt{D} + P_i)/Q_i$ be the complete quotient corresponding to (t_i, Q_i). The ordinary continued-fraction reduction step sends α_i to α_{i+1}, where

$$P_{i+1} = a_i Q_i - P_i, \qquad Q_{i+1} = \frac{D - P_{i+1}^2}{Q_i}.$$

After writing $t_i = m - P_i$, these formulae are exactly

$$t_{i+1} = (2m - t_i) \bmod Q_i, \qquad Q_{i+1} = \frac{F_D(t_{i+1})}{Q_i},$$

which is the definition of T_D. Hence T_D is precisely the reduction successor. □

Theorem 7.3

The directed cycles of T_D are exactly the reduced cycles of the narrow ideal classes of K. The cycle through $(0, 1)$ is the principal narrow class.

Proof By Proposition 7.1, vertices of V_D are reduced oriented quadratic states. By Proposition 7.2, T_D is the ordinary reduction successor.

Reduction of indefinite primitive binary quadratic forms preserves proper equivalence, equivalently the narrow ideal class. Thus the T_D-orbit of a reduced state remains inside one narrow class. In a fixed narrow class there are only finitely

many reduced states: for reduced forms $[a, b, c]$ of fixed discriminant one has the standard reduction bounds on a, b, and c, hence only finitely many possibilities. Since the reduction successor is reversible on reduced states – the inverse is the preceding continued-fraction reduction step – it permutes the finite reduced states in that narrow class. Therefore each narrow class decomposes into directed cycles.

For indefinite forms the reduced states in a fixed proper narrow class form a single reduction cycle: applying the reduction successor repeatedly runs through all reduced forms properly equivalent to the initial one before returning to it; see again Buchmann–Vollmer [16, Ch. 6] or Cohn [18, Ch. 5]. Hence the directed cycles of T_D are exactly the reduced cycles of narrow ideal classes.

Finally, $(0, 1)$ corresponds to

$$\frac{\sqrt{D} + m}{1}$$

and to the principal oriented ideal state. Therefore its T_D-cycle is the principal narrow class. □

Corollary 7.4 (graph-only cycle selection is not a new mechanism)

Selecting the principal directed cycle in the functional divisor graph is exactly selecting the principal narrow class. Therefore graph-only cycle selection is not an independent shortcut beyond principality.

---

8. Dynamic principality on the thin split family

We now isolate the thin family of small split ideals and show that dynamic principal-cycle membership adds no extra power beyond static principality.

Let $\ell \nmid D$ be a rational prime with $\ell < \sqrt{D}$, and let

$$s^2 \equiv D \pmod{\ell}.$$

Define

$$\mathfrak{a}_{\ell,s} := (\ell, \sqrt{D} + s).$$

Theorem 8.1 (dynamic principality equals static principality)

Let $\ell \nmid D$ be prime with $\ell < \sqrt{D}$, and let $s^2 \equiv D \pmod{\ell}$. For

$$\mathfrak{a}_{\ell,s} := (\ell, \sqrt{D} + s),$$

the following are equivalent.

1. $\mathfrak{a}_{\ell,s}$ is principal.

2. There exist integers x, y with

$$x^2 - Dy^2 = \pm\ell, \qquad x \equiv -sy \pmod{\ell}.$$

3. The reduced oriented state attached to $\mathfrak{a}_{\ell,s}$ lies on the principal reduction cycle.

Moreover, when a generator in (2) is already in the continued-fraction orientation, the corresponding state is recorded by a convergent p_n/q_n with

$$p_n^2 - Dq_n^2 = \pm\ell.$$

If the generator is in the opposite real embedding, the same assertion holds for the conjugate split ideal, i.e. after replacing s by $-s$. Thus, up to the unavoidable conjugation of the two prime ideals above ℓ, dynamic principal-cycle membership is exactly static principality on this thin split family.

Proof For (1) $\Leftrightarrow$ (2), suppose first that $\mathfrak{a}_{\ell,s} = (\alpha)$ with $\alpha = x + y\sqrt{D}$. Since $N(\mathfrak{a}_{\ell,s}) = \ell$,

$$|N(\alpha)| = |x^2 - Dy^2| = \ell.$$

Moreover $\alpha \in (\ell, \sqrt{D} + s)$, so

$$x + sy \equiv 0 \pmod{\ell}.$$

Conversely, if such (x, y) exists, then $\alpha = x + y\sqrt{D} \in \mathfrak{a}_{\ell,s}$ and $|N(\alpha)| = \ell = N(\mathfrak{a}_{\ell,s})$. Hence $(\alpha) = \mathfrak{a}_{\ell,s}$.

For (1) $\Leftrightarrow$ (3), use the standard infrastructure fact that the principal reduction cycle is precisely the reduction cycle of principal oriented ideals. If $\mathfrak{a}_{\ell,s}$ is principal, reducing it gives a reduced state on the principal cycle. Conversely, every reduced state on the principal cycle represents a principal oriented ideal, hence the corresponding $\mathfrak{a}_{\ell,s}$ is principal.

To justify the final continued-fraction statement, assume $\alpha = x + y\sqrt{D}$ is a generator as in (2) in the continued-fraction orientation. Then x/y is a reduced approximation to $\sqrt{D}$; in the classical continued-fraction/ideal dictionary, the reduced principal ideal generated by α corresponds to the reduced complete quotient reached from the convergent attached to x/y. More concretely, writing the associated reduced form as

$$[\ell, 2s, (s^2 - D)/\ell],$$

its proper-equivalence class is principal, and the reduced state determined by this form is exactly the one attached to $\mathfrak{a}_{\ell,s}$. Proposition 6.5 then identifies the Pell residual of the corresponding convergent with the denominator/norm of that reduced state, so one obtains

$$p_n^2 - Dq_n^2 = \pm\ell.$$

If α is in the opposite real embedding, the same argument applies to $\bar{\alpha}$, which replaces s by $-s$ and exchanges the two split prime ideals above ℓ. See Buchmann–Vollmer [16, Chs. 5–6] and Mollin [17, Chs. 6–7] for the surrounding reduction theory; the present theorem sharpens the usual half-distance / SQUFOF viewpoint to an exact principality equivalence on the thin split family. □

Consequence 8.2

On the thin split family $\mathfrak{a}_{\ell,s}$, principal-cycle membership is exactly static principality; there is no extra dynamic filter. In particular, the usual half-distance / SQUFOF intuition can be upgraded here to an exact reduced-state/principal-cycle equivalence for the split ideals themselves.

---

9. The odd part remains visible

We now test the final static hope for the thin split family: perhaps principality collapses almost entirely to the 2-primary/genus side. The answer is negative in general.

Let

$$C = \mathrm{Cl}^+(K) = P \times O,$$

where P is the 2-primary part and O the odd part.

Proposition 9.1

The principal genus is

$$2C,$$

and the entire odd part satisfies

$$O \subseteq 2C.$$

Proof Multiplication by 2 is an automorphism on every odd-order group, hence on O. So $O = 2O \subseteq 2C$. □

Theorem 9.2 (the thin split family sees the full principal genus)

For every class

$$c \in C,$$

there exist infinitely many degree-one split prime ideals of class c. Equivalently, there are infinitely many rational primes ℓ splitting in K and root classes $s^2 \equiv D \pmod{\ell}$ such that

$$(\ell, \sqrt{D} + s)$$

represents c. In particular, this holds for every $c \in 2C$.

Proof Let H^+ be the narrow Hilbert class field. Narrow class field theory identifies

$$\mathrm{Gal}(H^+/K) \cong C.$$

For a class $c \in C$, let σ_c be the corresponding Artin element. Since $K/\mathbf{Q}$ is quadratic, the normal closure of H^+ over $\mathbf{Q}$ is Galois, and conjugation over $\mathbf{Q}$ acts on C by inversion. Apply Chebotarev to this Galois extension and to the conjugacy class of an element whose restriction to K is trivial and whose restriction to H^+/K is σ_c. Infinitely many rational primes ℓ have Frobenius in this conjugacy class. Such primes split in K, because the Frobenius restricts trivially to K. For either of the two primes $\mathfrak{l} \mid \ell$ of K, the Frobenius in H^+/K is σ_c or σ_c^{-1}; the two conjugate primes above ℓ therefore represent inverse narrow classes. Hence one of them has class c, so the Chebotarev primes produced here populate every narrow class by degree-one split primes.

Finally, if $\mathfrak{l} \mid \ell$ is a degree-one split prime, then D has a square root s modulo ℓ, and, after choosing the sign of s corresponding to $\mathfrak{l}$,

$$\mathfrak{l} = (\ell, \sqrt{D} + s).$$

Thus every class c is represented by infinitely many split prime ideals of the displayed form. □

Corollary 9.3

Principal-genus admissibility is only a first-stage condition. On the thin split family, the odd part O remains fully visible. Thus principality does not collapse in general to a purely genus/2-adic test.

---

10. What remains after the rigorous negative results

At this point the landscape is sharply reduced.

10.1 Eliminated routes

The following routes are closed or collapse to already understood problems.

1. **Intrinsic Frobenius replacement:** ruled out by Theorem T1.
2. **Bounded-degree towers in the polynomial-norm smooth principal-relation world:** ruled out by Theorem $\mathrm{T2}_{\mathrm{str}}$ and Corollary $\mathrm{T2}_{\mathrm{sm}}$.
3. **Graph-only cycle selection:** collapses to narrow-class selection by Theorem 7.3.
4. **Dynamic principality on the thin split family:** collapses to static principality by Theorem 8.1.
5. **Principal-genus / 2-adic collapse on the thin split family:** ruled out in general by Theorem 9.2.

10.2 The last internal real-quadratic remainder

Inside the original real-quadratic framework, the only genuinely different remainder identified in this pass is an **archimedean placement** problem: whether the principal-split prime angles associated to low-denominator rare events exhibit a non-generic geometric placement law on the infrastructure circle. Concretely, this asks whether the angles of principal-cycle low-Q states on the infrastructure circle are equidistributed, or instead exhibit a semiprime-specific bias or window structure. The additive and graph-theoretic simplifications tested in this pass do not supply such a law.

This remainder is not developed into a theorem here; it remains an open internal loophole.

---

11. Final conclusion

The revised paper supports the following conclusion.

> **Main conclusion.** The Joux–Buchmann bridge fails inside the fixed-degree smooth principal-relation regime. The Frobenius and tower layers do not transfer; the exact continued-fraction/divisor-graph remainder collapses several natural loopholes back to principality or narrow-class selection; and no sub-$L[1/2]$ mechanism is found there.

The strongest theorem-level content is therefore negative:

1. no intrinsic or residue-level Frobenius substitute exists without factorization data;
2. no bounded-degree tower can create Joux-style recursive depth in the fixed-degree principal-relation regime;
3. on the main continued-fraction/divisor-graph remainder, several natural "graphical" or "dynamic" hopes collapse to static principality or narrow-class theory.

A future positive result would have to come from a genuinely different source. In this pass, the only such source isolated is conjectural: explicit real-multiplication reciprocity of Darmon–Vonk / Hilbert-12 type.

Appendix A. Conjectural external branch: Darmon–Vonk real multiplication

The proved negative theorems T1–T5 do **not** address a qualitatively different, external route coming from explicit real-multiplication reciprocity. Recent work of Darmon and Vonk proposes rigid meromorphic cocycles and real quadratic singular moduli as class-field-theoretic invariants for real quadratic fields, together

with reciprocity laws and arithmetic intersection formulae for modular geodesics [11–13].

For the purposes of the present paper we record only the following minimal conjectural escape hatch: there may exist an anchored binary RM invariant

$$A \longmapsto J_p(\tau_0, \tau_A)$$

whose finitely many valuation/intersection tests separate the principal narrow class from the others. We make **no theorem-level claim** from this branch and derive **no** factoring algorithm from it here. Its role is solely to identify an external mechanism not contradicted by T1–T5.

References

1. Antoine Joux, *A new index calculus algorithm with complexity $L(1/4+o(1))$ in very small characteristic.* In: T. Lange, K. Lauter, P. Lisonek (eds.), **Selected Areas in Cryptography – SAC 2013**, Lecture Notes in Computer Science **8282**, Springer, 2014, pp. 355–379. DOI: 10.1007/978-3-662-43414-7_18.
2. Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thome, *A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic.* In: P.-Q. Nguyen, E. Oswald (eds.), **Advances in Cryptology – EUROCRYPT 2014**, Lecture Notes in Computer Science **8441**, Springer, 2014, pp. 1–16. DOI: 10.1007/978-3-642-55220-5_1.
3. Robert Granger, Thorsten Kleinjung, Jens Zumbragel, *On the discrete logarithm problem in finite fields of fixed characteristic.* **Transactions of the American Mathematical Society 370** (2018), no. 5, 3129–3145. DOI: 10.1090/tran/7038.
4. Antoine Joux, Cecile Pierrot, *The Special Number Field Sieve in $\mathbf{F}_{p^n}$. Application to Pairing-Friendly Constructions.* In: Z. Cao, F. Zhang (eds.), **Pairing-Based Cryptography – Pairing 2013**, Lecture Notes in Computer Science **8365**, Springer, 2014, pp. 45–61. DOI: 10.1007/978-3-319-06416-9_4.
5. Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields.* In: C. Goldstein (ed.), **Seminaire de Theorie des Nombres, Paris 1988–1989**, Progress in Mathematics **91**, Birkhauser, 1990, pp. 27–41.
6. Jean-Francois Biasse, Michael J. Jacobson Jr., *Practical Improvements to Class Group and Regulator Computation of Real Quadratic Fields.* In: G. Hanrot, F. Morain, E. Thome (eds.), **Algorithmic Number Theory – ANTS IX**, Lecture Notes in Computer Science **6197**, Springer, 2010, pp. 50–65. DOI: 10.1007/978-3-642-14518-6_8.
7. Jean-Francois Biasse, Claus Fieker, *Subexponential class group and unit group computation in large degree number fields.* **LMS Journal**

of Computation and Mathematics 17 (2014), 385–403. DOI: 10.1112/S1461157014000345.

8. Mark L. Bauer, Safuat Hamdy, *On Class Group Computations Using the Number Field Sieve*. In: C.-S. Laih (ed.), **Advances in Cryptology – ASIACRYPT 2003**, Lecture Notes in Computer Science **2894**, Springer, 2003, pp. 311–325. DOI: 10.1007/978-3-540-40061-5_20.
9. Friedrich Hirzebruch, Don Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus*. **Inventiones Mathematicae 36** (1976), 57–113. DOI: 10.1007/BF01390005.
10. Jan Hendrik Bruinier, Tonghai Yang, *CM-values of Hilbert modular functions*. **Inventiones Mathematicae 163** (2006), 229–288. DOI: 10.1007/s00222-005-0457-2.
11. Henri Darmon, Jan Vonk, *Singular moduli for real quadratic fields: A rigid analytic approach*. **Duke Mathematical Journal 170** (2021), no. 1, 23–93. DOI: 10.1215/00127094-2020-0035.
12. Henri Darmon, Jan Vonk, *Arithmetic intersections of modular geodesics*. **Journal of Number Theory 230** (2022), 89–111. DOI: 10.1016/j.jnt.2020.12.012.
13. Henri Darmon, Jan Vonk, *Real quadratic Borcherds products*. **Pure and Applied Mathematics Quarterly 18** (2022), no. 5, 1803–1865. DOI: 10.4310/PAMQ.2022.v18.n5.a1.
14. Samit Dasgupta, Mahesh Kakde, *On the Brumer–Stark conjecture*. **Annals of Mathematics 197** (2023), no. 1, 289–388. DOI: 10.4007/annals.2023.197.1.5.
15. Samit Dasgupta, Mahesh Kakde, *Brumer–Stark units and explicit class field theory*. **Duke Mathematical Journal 173** (2024), no. 8, 1477–1555. DOI: 10.1215/00127094-2023-0039. Preprint version: arXiv:2103.02516.
16. Johannes Buchmann, Ulrich Vollmer, *Binary Quadratic Forms: An Algorithmic Approach*. Algorithms and Computation in Mathematics **20**, Springer, 2007. DOI: 10.1007/978-3-540-46368-9.
17. Richard A. Mollin, *Quadratics*. CRC Press, Boca Raton, 1996.
18. Harvey Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*. Universitext, Springer, New York, 1978. DOI: 10.1007/978-1-4612-9950-9.