

NON-PRINCIPAL IDEAL CLASSES AND SELMER VANISHING OVER QUADRATIC FIELDS

YICHENG WANG

ABSTRACT. The study of rational points on elliptic curves has long been connected with descent, a method used by Fermat in the study of Diophantine equations. In 1922, Mordell proved that the group of rational points on an elliptic curve over $\mathbb{Q}$ is finitely generated, and Weil extended this theorem to number fields in 1928 [2, Chapter IV]. Isogeny descent provides a way to investigate these groups through square classes and local conditions. Over quadratic fields, non-principal ideal classes introduce an additional arithmetic obstruction that can be reflected in the coordinates of points.

We study the contribution of these ideal classes to the first isogeny descent of $E_{D,m} : y^2 = x^3 + (m + \sqrt{D})x^2 + x$ over $K = \mathbb{Q}(\sqrt{D})$, where D is fixed and squarefree, $D \equiv 2 \pmod{4}$, and $m \in \mathbb{Z}$. Both positive and negative D are included. The possible descent classes lie in a finite group determined by units and ideal classes.

We prove that the first isogeny Selmer group is trivial for density one of the parameters, uniformly over translated long intervals, and that its average size tends to one. We also determine the torsion groups exactly. They are C_2 on $E_{D,m}$ and C_2^2 on its associated curve.

The main step we take next is a local calculation showing that $m + \sqrt{D} \equiv -2$ at an odd prime forces the entire local first-descent image to be trivial. Chebotarev's theorem supplies sufficiently many degree-one primes detecting each non-square case, and a finite application of the Chinese Remainder Theorem gives the parameter results. Over $\mathbb{Q}(\sqrt{10})$, explicit local conditions prove vanishing whenever $m \equiv 3 \pmod{15}$. At $m = 1$, however, the point $(2, 2 + \sqrt{10})$ realizes the non-principal ideal class, and the torsion theorem proves that it has infinite order. This example showcases the nuanced effect non-principal classes have.

Key words and phrases. Elliptic curves; Quadratic fields; Isogeny descent; Selmer groups; Non-principal ideal classes.

CONTENTS

1. Introduction and main results	3
1.1. Parameter results	4
1.2. Literature summary	5
2. Descent and Ideal Classes	5
2.1. Map directions on the associated curves	5
2.2. Homomorphisms on the square-class and its kernel	7
2.3. Evaluation of ideals on the candidate group	8
2.4. Selmer Group as constraints	10
3. Local Exclusion and Primes	11
3.1. Hensel's Lemma	11
3.2. Application of Chebotarev	12
3.3. Primes as integer congruences	13
4. Density-one Vanishing	13
4.1. Application of Chinese Remainder Theorem	14
4.2. Limits on ordered sets	14
4.3. Progression sequences and signs	15
4.4. Average size	15
5. Vanishing Subprogressions	16
6. Consequences for Points and Ideal Classes	17
6.1. The Kummer-Selmer exact sequence	17
6.2. Isogeny verification	17
6.3. Proof of the results	18
7. An Example over $\mathbb{Q}(\sqrt{10})$	19
7.1. The ring of integers and the full ideal class group	19
7.2. The units and the eight virtual square classes	21
7.3. Conditions for the parameters	22
7.4. Progression on odd prime factors	23
7.5. The parameter $m = 1$ and its global points	24
8. Conclusion	25
9. Acknowledgements	26
Appendix A. Proof of the Torsion Classification	26
A.1. The square tests	27
A.2. The duplication formula	28
A.3. The unique dyadic primes	28
A.4. Excluding order three	30
A.5. Excluding odd torsion	31
References	33

1. INTRODUCTION AND MAIN RESULTS

Fix a squarefree integer $D \equiv 2 \pmod{4}$. Write

$$\begin{aligned} K &= \mathbb{Q}(w), & w &= \sqrt{D}, & a_m &= m + w, \\ E_m &= E_{D,m} : & y^2 &= x^3 + a_m x^2 + x. \end{aligned} \tag{1.1}$$

The letter D stays fixed over variable m . Since D is squarefree and even, w is irrational. The quadratic integral-basis theorem gives [1, Example 2.41]

$$\mathcal{O}_K = \mathbb{Z}[w], \quad \text{disc}(K) = 4D.$$

Here $\mathcal{O}_K$ is the ring of elements of K satisfying a monic polynomial with integer coefficients. In particular a_m is integral for every $m \in \mathbb{Z}$.

The associated curve of E and the directions of the two maps are

$$E'_m : Y^2 = X(X - a_m - 2)(X - a_m + 2), \quad E_m \xrightarrow{\phi_m} E'_m \xrightarrow{\hat{\phi}_m} E_m.$$

Their formulas and their composition [2] are shown in Section 2. The point at infinity is denoted as O .

Lemma 1.1 (Non-singularity). *For every D and m satisfying the previous conditions, both E_m and E'_m are elliptic curves.*

Proof. For $y^2 = x^3 + Ax^2 + Bx$, the discriminant is $16B^2(A^2 - 4B)$. This curve is nonsingular precisely when its discriminant is nonzero [2, Chapter II, Section 2]. Put $d_m = a_m^2 - 4$. Substitution gives

$$\begin{aligned} \Delta(E_m) &= 16d_m, \\ \Delta(E'_m) &= 16d_m^2(4a_m^2 - 4d_m) = 256d_m^2, \\ d_m = 0 &\implies a_m = 2 \text{ or } a_m = -2 \\ &\implies w = 2 - m \text{ or } w = -2 - m \in \mathbb{Q}, \end{aligned}$$

contradicting irrationality. Thus both discriminants are nonzero, and each projective curve has the rational point O . $\square$

This paper concerns the relationship between points and ideal classes. A nonzero coordinate x of a point on E_m has even valuation at every finite prime. Thus we know $(x) = \mathfrak{a}_x^2$ for a unique fractional ideal $\mathfrak{a}_x$. The ideal $\mathfrak{a}_x$ can be non-principal while its square is principal. Even when it is principal, a non-square unit can still satisfy the conditions. Section 2 proves that this generates a finite square-class group $V(K)$ which is independent of m .

We determine when non-principal classes contribute to first descent.

We impose the local conditions defining the first isogeny Selmer group

$$S_m = \text{Sel}^{\hat{\phi}_m}(E'_m/K) \subseteq V(K).$$

The notation is indexed by E'_m of $\hat{\phi}_m$. In this paper, 'first' refers to this. We write a multiplicative square class as $[c]$ and the trivial group as $\{[1]\}$. The definitions will show that a point gives a class in S_m , while a Selmer class could possibly not come from a point.

1.1. Parameter results. For $B \in \mathbb{Z}$ and positive integer X , put $\mathcal{I}(B, X) = \{B + 1, \dots, B + X\}$.

Theorem 1.2 (Density-one Selmer vanishing). *For each fixed squarefree $D \equiv 2 \pmod{4}$, let $\mathcal{B} = \{m \in \mathbb{Z} : S_m \neq \{[1]\}\}$. Then*

$$\lim_{X \rightarrow \infty} \sup_{B \in \mathbb{Z}} \frac{|\mathcal{B} \cap \mathcal{I}(B, X)|}{X} = 0, \quad (1.2)$$

$$\lim_{X \rightarrow \infty} \sup_{B \in \mathbb{Z}} \left| \frac{1}{X} \sum_{m \in \mathcal{I}(B, X)} |S_m| - 1 \right| = 0. \quad (1.3)$$

The same density-one and average-size conclusions hold for positive parameters, negative parameters, symmetric intervals, and every fixed arithmetic progression. In a progression $b + q\mathbb{Z}$, the convergence is uniform no matter what types of translations are used.

Uniformity means that all starting points have a vanishing proportion of exceptions as the interval length grows. Since the field is fixed, no uniformity as D varies is claimed.

Theorem 1.3 (Vanishing on a subprogression). *For every $b \in \mathbb{Z}$ and $q \geq 1$, there are integers m_0 and $M \geq 1$, with $q \mid M$ and $m_0 \equiv b \pmod{q}$, such that*

$$m \equiv m_0 \pmod{M} \implies S_m = \{[1]\}.$$

Section 5 gives a finite selection of primes and uses the Chinese Remainder Theorem to determine m_0 and M .

Theorem 1.4 (Consequences of Selmer vanishing). *For every $m \in \mathbb{Z}$, $S_m = \{[1]\}$ is equivalent to the following two conditions holding together:*

$$E_m(K) = \hat{\phi}_m(E'_m(K)), \quad \text{Sha}(E'_m/K)[\hat{\phi}_m] = 0. \quad (1.4)$$

Whenever these two conditions hold, each affine K -point has square x -coordinate, including $0 = 0^2$. For $x \neq 0$, its fractional half-ideal $\mathfrak{a}_x$ is principal. Thus these conclusions hold on the density-one set of Theorem 1.2 and on every member of the subprogressions constructed previously in Theorem 1.3.

Here $\text{Sha}(E'_m/K)[\hat{\phi}_m]$ denotes the kernel of the induced map from $\text{Sha}(E'_m/K)$ to $\text{Sha}(E_m/K)$. Section 6 defines this notation and states the canonical theorems used to show it. The result will concern mostly the kernel of this object.

Theorem 1.5 (Torsion in the restricted family). *For every squarefree $D \equiv 2 \pmod{4}$ and every $m \in \mathbb{Z}$,*

$$\begin{aligned} E_m(K)_{\text{tors}} &= \{O, (0, 0)\} \cong C_2, \\ E'_m(K)_{\text{tors}} &= \{O, (0, 0), (a_m + 2, 0), (a_m - 2, 0)\} \cong C_2 \times C_2. \end{aligned}$$

Here $C_2 = \mathbb{Z}/2\mathbb{Z}$ and the torsion subgroup consists of the points of finite order. Thus every point with nonzero ordinate on either curve has infinite order.

Appendix A proves this result at the unique prime above 2. Its hypotheses include negative D thus proving the claim across the entire definition.

Theorem 1.6 (An explicit example over $\mathbb{Q}(\sqrt{10})$). *Let $D = 10$, $w = \sqrt{10} > 0$, $\varepsilon = 3 + w$, and $\mathfrak{q}_2 = (2, w)$. Then*

$$\begin{aligned} \text{Cl}(K) &= \langle [\mathfrak{q}_2] \rangle \cong C_2, \\ V(K) &= \{[(-1)^i \varepsilon^j 2^k] : i, j, k \in \{0, 1\}\} \cong C_2^3, \\ \pi([(-1)^i \varepsilon^j 2^k]) &= [\mathfrak{q}_2]^k. \end{aligned}$$

Here π sends a square class to the class of its half-ideal. At every parameter, $S_m \subseteq \langle [-1], [2] \rangle$. The primes $(3, w-1)$ and $(5, w)$ give

$$m \equiv 3 \pmod{15} \implies S_m = \{[1]\}.$$

At $m = 1$, however,

$$\begin{aligned} P = (2, 2 + w) &\in E_1(K), & \alpha_{1,K}(P) &= [2], \\ \pi([2]) &= [\mathfrak{q}_2] \neq 1, & S_1 &= \{[1], [2]\}. \end{aligned}$$

The point P has infinite order. Its coset generates $E_1(K)/\widehat{\phi}_1(E'_1(K)) \cong C_2$, and $\text{Sha}(E'_1/K)[\widehat{\phi}_1] = 0$.

1.2. Literature summary. Zywinia [5] studies specializations for which both isogeny Selmer groups are generated by global points and obtains exact rank results. In contrast, we fix a quadratic field $K = \mathbb{Q}(\sqrt{D})$ and study the first $\widehat{\phi}_m$ -Selmer group in the integer family E_m . We prove that it vanishes for density one of the parameters and on a suitable subprogression. The local-obstruction strategy is related to that of Loughran–Smeets [6], but here the candidate group and the excluding congruences are obtained from the equation.

2. DESCENT AND IDEAL CLASSES

We supply the group maps and arithmetic definitions used in the proof and use the descent map to connect point coordinates with square classes and fractional ideals.

2.1. Map directions on the associated curves. Fix $m \in \mathbb{Z}$ and define $a = a_m$, $d = a^2 - 4$. By Lemma 1.1, $d \neq 0$ and both curves are elliptic. The chord-and-tangent law makes the points on each curve an abelian group, with inverse $(x, y) \mapsto (x, -y)$ [2, Chs. I–II]. In particular $T = (0, 0) \in E_m(K)$ and $T' = (0, 0) \in E'_m(K)$ have order two.

The following two maps, initially away from the displayed denominators, will be isogenies:

$$\phi_m : E_m \longrightarrow E'_m, \quad (x, y) \longmapsto \left(x + a + \frac{1}{x}, y \left(1 - \frac{1}{x^2} \right) \right), \quad (2.1)$$

$$\widehat{\phi}_m : E'_m \longrightarrow E_m, \quad (X, Y) \longmapsto \left(\frac{X - 2a + d/X}{4}, \frac{Y(1 - d/X^2)}{8} \right). \quad (2.2)$$

We extend them by $\phi_m(O) = \phi_m(T) = O$ and $\widehat{\phi}_m(O) = \widehat{\phi}_m(T') = O$.

Lemma 2.1 (Verification of the isogeny Pair). *The formulas define degree-two isogenies with kernels $\{O, T\}$ and $\{O, T'\}$, respectively. They satisfy*

$$\widehat{\phi}_m \phi_m = [2] \quad \text{on } E_m, \quad \phi_m \widehat{\phi}_m = [2] \quad \text{on } E'_m.$$

Proof. First set $X = x + a + 1/x = y^2/x^2$ and $Y = y(1 - 1/x^2)$. Direct calculation gives

$$\begin{aligned} (X - a)^2 - 4 &= \left(x - \frac{1}{x}\right)^2, \\ X((X - a)^2 - 4) &= \frac{y^2}{x^2} \left(x - \frac{1}{x}\right)^2 = Y^2. \end{aligned}$$

Hence ϕ_m fulfills the requirements. For the other direction, let $u = X - 2a + d/X = Y^2/X^2$ and $v = Y(1 - d/X^2)$. Then

$$\begin{aligned} (u + 2a)^2 - 4d &= \left(X - \frac{d}{X}\right)^2, \\ v^2 &= u((u + 2a)^2 - 4d) \\ &= u^3 + 4au^2 + 16u, \end{aligned}$$

where we use $a^2 - d = 4$. Setting $u = 4x$ and $v = 8y$ gives E_m , and the resulting map is exactly (2.2).

The rational maps extend to the nonsingular projective curves. [2, Proposition 4.18]. At the points with zero first coordinate the displayed first coordinate has a pole, so the image is O . The same is true at O . No other point maps to O meaning both maps preserve O and are therefore group homomorphisms [2, Proposition 1.5]. Their kernels are the two pairs previously stated. We also use the separable-fiber theorem which claims that a separable map of curves has a general geometric fiber with as many points as its degree [2, Proposition 4.24(a)]. In characteristic zero the maps are separable. Since each fiber of a group homomorphism is a coset of its kernel, the general fiber in this case has two points. Thus both maps have degree two.

Next we verify the composition. The tangent slope on E_m is $\lambda = (3x^2 + 2ax + 1)/(2y)$. For $y \neq 0$,

$$\begin{aligned} x(2P) &= \lambda^2 - a - 2x \\ &= \frac{(3x^2 + 2ax + 1)^2 - 4y^2(a + 2x)}{4y^2} = \frac{(x^2 - 1)^2}{4y^2}. \end{aligned}$$

Put $q = x^2 + ax + 1$, so $y^2 = xq$ and $X = q/x$. Using the equation of E'_m to write the first coordinate of $\widehat{\phi}_m$ as $Y^2/(4X^2)$ gives

$$\begin{aligned} x(\widehat{\phi}_m \phi_m(P)) &= \frac{(x^2 - 1)^2}{4y^2} = x(2P), \\ q^2 - dx^2 &= x^4 + 2ax^3 + 6x^2 + 2ax + 1, \\ y(\widehat{\phi}_m \phi_m(P)) &= \frac{(x^2 - 1)(q^2 - dx^2)}{8y^3} \\ &= \lambda \left(x - \frac{(x^2 - 1)^2}{4y^2} \right) - y = y(2P). \end{aligned}$$

These identities extend to the exceptional points, showing the first composition formula. A nonconstant map of projective curves is surjective over the algebraic closure [2, Chs. I-II]. Thus, from $\phi_m \widehat{\phi}_m \phi_m = \phi_m[2] = [2]\phi_m$, surjectivity of ϕ_m gives the second formula. $\square$

2.2. Homomorphisms on the square-class and its kernel. For a field F containing K , write $[c]$ for the class of $c \in F^\times$ in $F^\times/F^{\times 2}$. Two elements have the same class precisely when their ratio is a square and every class has order dividing two. Multiplication of classes therefore also defines addition in an $\mathbb{F}_2$ -vector space.

Lemma 2.2 (The First Descent Map). *The map*

$$\alpha_{m,F}(O) = \alpha_{m,F}(T) = [1], \quad \alpha_{m,F}(x, y) = [x] \quad (x \neq 0)$$

is a group homomorphism and has kernel $\widehat{\phi}_m(E'_m(F))$. So

$$E_m(F)/\widehat{\phi}_m(E'_m(F)) \cong \text{im } \alpha_{m,F}. \quad (2.3)$$

Proof. Step 1: Verify the homomorphism. The intersections of $y = \lambda x + \nu$ with E_m have first coordinates satisfying

$$x^3 + (a - \lambda^2)x^2 + (1 - 2\lambda\nu)x - \nu^2 = 0.$$

If $\nu \neq 0$, their product is ν^2 . Counting tangent with multiplicity, the three intersection points P, Q, R satisfy $P + Q + R = O$. Thus

$$[x(P)][x(Q)][x(R)] = [1] \implies \alpha_{m,F}(P + Q) = \alpha_{m,F}(P)\alpha_{m,F}(Q),$$

because negation leaves the first coordinate constant.

A line through T has $\nu = 0$. The line's equation factors as

$$x(x^2 + (a - \lambda^2)x + 1) = 0.$$

The two nonzero intersection coordinates have product 1, and $\alpha_{m,F}(T) = [1]$, so the previous identity holds. A vertical line gives $P + (-P) = O$ and $[x]^2 = [1]$ while also accounting for $T + T = O$. Thus homomorphism is proved.

Step 2: Show that points in the isogeny image have square class [1]. For $X \neq 0$, formula (2.2) and the curve equation give

$$x(\widehat{\phi}_m(X, Y)) = \frac{Y^2}{4X^2}.$$

If $Y \neq 0$, this is a nonzero square. If $Y = 0$, the image is T , whose class is $[1]$. The two kernel points map to O .

Step 3: Construct a preimage of every element in the kernel. Suppose $P = (r^2, y)$ with $r \in F^\times$, and let $s = y/r$. Then $s^2 = r^4 + ar^2 + 1$. Define

$$X = a + 2r^2 + 2s, \quad Y = 2rX.$$

The equality

$$\begin{aligned} (a + 2r^2 + 2s)(a + 2r^2 - 2s) &= (a + 2r^2)^2 - 4s^2 \\ &= a^2 - 4 = d \end{aligned}$$

shows that $X \neq 0$ and $d/X = a + 2r^2 - 2s$. It follows that

$$\begin{aligned} X^2 - 2aX + d &= 4r^2X, \\ X(X^2 - 2aX + d) &= 4r^2X^2 = Y^2, \\ x(\hat{\phi}_m(X, Y)) &= r^2, \\ y(\hat{\phi}_m(X, Y)) &= \frac{r}{4} \left(X - \frac{d}{X} \right) = rs = y. \end{aligned}$$

This proves that (X, Y) is a preimage. The point O has a preimage, and $(a + 2, 0) \in E'_m(F)$ maps to T . Here $a + 2 \neq 0$ because $d \neq 0$. This proves the kernel identity and thus also proves the quotient isomorphism. $\square$

2.3. Evaluation of ideals on the candidate group. A nonzero fractional ideal is an $\mathcal{O}_K$ -submodule $\mathfrak{a} \subset K$ for which some nonzero integer multiple is a nonzero integral ideal. Unique ideal factorization in $\mathcal{O}_K$ states that

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, \quad n_{\mathfrak{p}} \in \mathbb{Z}, \quad (2.4)$$

with finitely many nonzero exponents and a unique such expression [1, Theorem 3.7]. When $\mathfrak{p}$ runs over nonzero prime ideals we can write $v_{\mathfrak{p}}(\mathfrak{a}) = n_{\mathfrak{p}}$. For $c \in K^\times$, define $v_{\mathfrak{p}}(c)$ to be the exponent of $\mathfrak{p}$ in the principal fractional ideal (c) . In particular,

$$v_{\mathfrak{p}}(cd) = v_{\mathfrak{p}}(c) + v_{\mathfrak{p}}(d), \quad v_{\mathfrak{p}}(c^2) = 2v_{\mathfrak{p}}(c).$$

The ideal class group $\text{Cl}(K)$ is the group of nonzero fractional ideals modulo the subgroup of principal ideals. Its subgroup $\text{Cl}(K)[2]$ consists of classes whose squares are the identity.

A unit $u \in \mathcal{O}_K^\times$ is an algebraic integer with an inverse in $\mathcal{O}_K$. This means that

$$u \in \mathcal{O}_K^\times \iff (u) = \mathcal{O}_K \iff v_{\mathfrak{p}}(u) = 0 \text{ for every } \mathfrak{p}.$$

Now define

$$V(K) = \{[c] \in K^\times / K^{\times 2} : v_{\mathfrak{p}}(c) \in 2\mathbb{Z} \text{ for every finite } \mathfrak{p}\}. \quad (2.5)$$

Multiplying by a square changes every valuation by an even amount, so this definition is independent of the representative. In this case the condition is closed under multiplication and inverses, making $V(K)$ a group of square classes.

Proposition 2.3 (Units and Half-ideal Classes). *The group $V(K)$ fits into the following exact sequence*

$$0 \longrightarrow \mathcal{O}_K^\times / \mathcal{O}_K^{\times 2} \longrightarrow V(K) \xrightarrow{\pi} \text{Cl}(K)[2] \longrightarrow 0, \quad (2.6)$$

where $\pi([c]) = [\mathfrak{a}]$ if $(c) = \mathfrak{a}^2$. It is finite, with

$$|V(K)| = \begin{cases} 4|\text{Cl}(K)[2]|, & D > 0, \\ 2|\text{Cl}(K)[2]|, & D < 0. \end{cases} \quad (2.7)$$

Proof. Step 1: Construct and check π . For $[c] \in V(K)$, halving the exponents in (c) gives a unique fractional ideal $\mathfrak{a}$ with $(c) = \mathfrak{a}^2$. Its class has order dividing two. If c is replaced by cz^2 , then its half-ideal is $\mathfrak{a}(z)$, which has the same ideal class. Thus π is well-defined. Also

$$(c) = \mathfrak{a}^2, \quad (d) = \mathfrak{b}^2 \implies (cd) = (\mathfrak{a}\mathfrak{b})^2 \implies \pi([cd]) = \pi([c])\pi([d]).$$

So π is a homomorphism.

Step 2: Prove surjectivity. If $[\mathfrak{a}] \in \text{Cl}(K)[2]$, then by definition $\mathfrak{a}^2 = (c)$ for some $c \in K^\times$. This gives $[c] \in V(K)$ and $\pi([c]) = [\mathfrak{a}]$.

Step 3: Determine the kernel and injection. If $\pi([c]) = 1$, write $\mathfrak{a} = (z)$. Then

$$\begin{aligned} (c) = \mathfrak{a}^2 = (z)^2 &\implies (c/z^2) = \mathcal{O}_K \\ &\implies c/z^2 = u \in \mathcal{O}_K^\times \implies [c] = [u]. \end{aligned}$$

Conversely every unit has a trivial half-ideal class. If a unit is a square in K , let $u = z^2$, then $0 = v_{\mathfrak{p}}(u) = 2v_{\mathfrak{p}}(z)$ at every prime. Thus z is a unit. This proves that units modulo their own squares inject into $V(K)$, and proves exactness.

Step 4: Prove finiteness and count total possibilities. We use two arithmetic theorems, both for the number field K : the ideal class group is finite [1, Theorem 4.4], and Dirichlet's unit theorem states [1, Theorem 5.1]

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r, \quad r = 1 \ (D > 0), \quad r = 0 \ (D < 0).$$

The group $\mu(K)$ of roots of unity is finite cyclic. Its order is even since it contains -1 . A cyclic group of even order has two cosets modulo squares. The rank r is one for a real quadratic field (two real embeddings) and zero for an imaginary quadratic field (one pair of complex embeddings). Consequently

$$\begin{aligned} |\mathcal{O}_K^\times / \mathcal{O}_K^{\times 2}| &= 2^{r+1}, \\ |V(K)| &= 2^{r+1} |\text{Cl}(K)[2]| < \infty. \end{aligned}$$

The second equality is derived by counting the equal-size fibers of the surjective homomorphism π . This shows (2.7). $\square$

Thus there are two different possibilities to an element not being a square. If $(c) = \mathfrak{a}^2$ with $\mathfrak{a}$ non-principal, then c is a non-square. If $\mathfrak{a} = (z)$ is principal, then $c = uz^2$ for a unit u , and it remains to test the unit class.

2.4. Selmer Group as constraints. For a finite place v of K , write K_v for the completion, with valuation v , valuation ring $\mathcal{O}_v$, maximal ideal $\mathfrak{m}_v$, and residue field κ_v . We use the standard valuation identities and set $v(0) = +\infty$.

Definition 2.4. With res_v denoting the map on square classes induced by $K \hookrightarrow K_v$, define

$$S_m = \{[c] \in K^\times / K^{\times 2} : \text{res}_v[c] \in \alpha_{m, K_v}(E_m(K_v)) \text{ for every place } v\}. \quad (2.8)$$

This is the first isogeny Selmer group $\text{Sel}^{\hat{\phi}_m}(E'_m/K)$ in source notation.

It is a subgroup, since it is an intersection of preimages of subgroups. A global point gives a point at every completion, so

$$E_m(K)/\hat{\phi}_m(E'_m(K)) \hookrightarrow S_m. \quad (2.9)$$

Section 6 checks the square-class Kummer identification and relates this definition to Sha.

The local test also has a direct equation. If $x = c(U/V)^2$, write $y = cUW/V^3$. Substituting and cancelling gives

$$\begin{aligned} y^2 = x^3 + ax^2 + x &\iff c^2U^2W^2 = c^3U^6 + ac^2U^4V^2 + cU^2V^4 \\ &\iff cW^2 = c^2U^4 + acU^2V^2 + V^4 \quad (UV \neq 0). \end{aligned}$$

Thus a non-trivial class $[c]$ belongs to the local image exactly when this last equation has a solution with $UV \neq 0$ in K_v . Allowing $(U, V) \neq (0, 0)$ also includes $[1]$ as if $U = 0$ or $V = 0$, the equation forces c to be a square, and the trivial class has such a solution. These equations explain concretely what the local conditions mean. We do not infer a global solution merely because all the local tests pass.

Lemma 2.5 (The uniform finite candidate bound). *For every $m \in \mathbb{Z}$,*

$$S_m \subseteq V(K), \quad |S_m| \leq |V(K)|.$$

Moreover, the nonzero x -coordinate of a global point has a unique fractional half-ideal.

Proof. Work at a finite completion $F = K_{\mathfrak{p}}$ and put $a = m + w \in \mathcal{O}_F$. Suppose first that $xy \neq 0$, and set $n = v(x)$. If $n > 0$, then

$$\begin{aligned} v(x^2) > 0, \quad v(ax) > 0 &\implies v(x^2 + ax + 1) = 0 \\ &\implies 2v(y) = v(x(x^2 + ax + 1)) = n \implies n \in 2\mathbb{Z}. \end{aligned}$$

If $n < 0$, factor the equation in a different way:

$$\begin{aligned} y^2 = x^3(1 + a/x + 1/x^2), \quad v(a/x) > 0, \quad v(1/x^2) > 0 &\implies 2v(y) = 3n \\ &\implies n \in 2\mathbb{Z}. \end{aligned}$$

The case $n = 0$ already has even valuation. If $y = 0$ and $x \neq 0$, then $x^2 + ax + 1 = 0$. For $n > 0$ the constant term is the unique term of least valuation. For $n < 0$ the x^2 term is the unique such term. Neither can cancel, so $n = 0$ in this case as well. The two special points have class $[1]$.

Consequently every local image class has even valuation, including at primes above 2. Since multiplying by a local square changes valuation by an even integer,

$$[c] \in S_m \implies v_{\mathfrak{p}}(c) \in 2\mathbb{Z} \text{ for all } \mathfrak{p} \implies [c] \in V(K).$$

For a nonzero global coordinate x , define $\mathfrak{a}_x = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)/2}$. The exponents are integers, and unique ideal factorization proves $(x) = \mathfrak{a}_x^2$ and uniqueness. $\square$

The coefficient 1 of x makes the constant term in $x^2 + ax + 1$ a unit at every finite place. This is the reason for the even-valuation statement and for the candidate group defined using all finite primes, with no exceptional prime set.

3. LOCAL EXCLUSION AND PRIMES

Fix a non-trivial class $[c] \in V(K)$.

We only need to calculate $a \equiv -2$ at an odd prime.

3.1. Hensel's Lemma.

Theorem 3.1 (Hensel's lemma in simple-root form). *Let A be a complete discrete valuation ring with maximal ideal (ϖ) and residue field κ . If $f \in A[T]$ and $\bar{t} \in \kappa$ satisfy*

$$\bar{f}(\bar{t}) = 0, \quad \bar{f}'(\bar{t}) \neq 0,$$

then there is a unique $t \in A$ reducing to $\bar{t}$ with $f(t) = 0$.

This is [1, Proposition 7.31]. When $\text{char } \kappa \neq 2$ and $u \in A^\times$, apply it to $f(T) = T^2 - u$. A nonzero root $\bar{t}$ has derivative $2\bar{t} \neq 0$. Consequently

$$u \in F^{\times 2} \iff \bar{u} \in \kappa^{\times 2}, \quad F = \text{Frac}(A). \quad (3.1)$$

In particular, every element of $1 + (\varpi)$ is a square, so we use the root $\bar{t} = 1$.

Lemma 3.2 (The local exclusion rule). *Let $\mathfrak{p}$ be a prime of K above an odd rational prime, and put $F = K_{\mathfrak{p}}$. If $a_m \equiv -2 \pmod{\mathfrak{m}_F}$, then $\alpha_{m,F}(E_m(F)) = \{[1]\}$.*

Proof. Abbreviate $a = a_m$. The points O and $(0, 0)$ have trivial class. For a point with $x \neq 0$, Lemma 2.5's valuation calculation shows that $y = 0$ can occur only when $v(x) = 0$. Thus $y \neq 0$ in each of the following nonunit cases.

If $v(x) > 0$, write $y^2 = xu$ with $u = 1 + ax + x^2 \in 1 + \mathfrak{m}_F$. Hensel gives $u = z^2$, so

$$y^2 = xz^2 \implies x = (y/z)^2.$$

If $v(x) < 0$, write $y^2 = x^3u$ with $u = 1 + a/x + 1/x^2 \in 1 + \mathfrak{m}_F$. Again $u = z^2$, and

$$y^2 = x^3z^2 \implies x = (y/(xz))^2.$$

Both cases have trivial square class.

It remains to treat $v(x) = 0$. The equation makes y integral. Reducing it gives

$$\bar{y}^2 = \bar{x}(\bar{x}^2 - 2\bar{x} + 1) = \bar{x}(\bar{x} - 1)^2.$$

If $\bar{x} = 1$, it is a square. If $\bar{x} \neq 1$, division by $(\bar{x} - 1)^2$ gives $\bar{x} = (\bar{y}/(\bar{x} - 1))^2$. This is nonzero since x is a unit. Equation (3.1) now shows that x is a square in F . This also covers $y = 0$ in the unit case. All image classes are therefore trivial. $\square$

3.2. Application of Chebotarev. For a prime ideal $\mathfrak{p}$ above a rational prime p , put

$$N\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}| = p^{f_{\mathfrak{p}}}, \quad f_{\mathfrak{p}} = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p].$$

The integer $f_{\mathfrak{p}}$ is its residue degree over $\mathbb{Q}$. The prime-decomposition theorem gives $\sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} = 2$, where $e_{\mathfrak{p}}$ is the exponent of $\mathfrak{p}$ in (p) . Thus there are at most two primes above each p [1, Theorem 3.34].

Theorem 3.3 (Chebotarev in quadratic Dirichlet-density form). *For our fixed quadratic field K , let L/K be a quadratic extension. Let $\mathcal{T}$ be the prime ideals of K unramified and inert in L . Then*

$$\lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} (N\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = \frac{1}{2}. \quad (3.2)$$

Here inert means that $\mathfrak{p}$ stays prime in L and the relative residue extension has degree two. The statement is the quadratic case of the Chebotarev density theorem [3, Theorem 28.9]: in a finite Galois extension, primes with Frobenius in a union C of conjugacy classes have Dirichlet density $|C|/|\text{Gal}(L/K)|$. For a quadratic extension take C to be its single non-identity automorphism. Only this Dirichlet-density form, not an error estimate, is used below.

Lemma 3.4 (Enough degree-one primes). *For every non-square $c \in K^\times$, there is a set $\mathcal{P}_c$ of odd rational primes satisfying*

$$\sum_{p \in \mathcal{P}_c} \frac{1}{p} = \infty.$$

For each such p , one can choose $\mathfrak{p} | p$ with $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$ such that c is a unit at $\mathfrak{p}$ and has non-square residue. The set can avoid any preassigned finite set of rational primes.

Proof. Step 1: use the quadratic extension detecting c . Since c is non-square, $L = K(\sqrt{c})$ is quadratic over K . By (3.2), its inert prime ideals have a divergent reciprocal-norm sum:

$$\sum_{\mathfrak{p} \text{ inert in } L/K} \frac{1}{N\mathfrak{p}} = \infty.$$

Indeed, a finite sum at $s = 1$ would bound all the sums for $s > 1$, because $(N\mathfrak{p})^{-s} \leq (N\mathfrak{p})^{-1}$, contradicting their divergence as $s \downarrow 1$.

Step 2: remove higher residue degrees over $\mathbb{Q}$. Using the bound of two prime ideals above each rational prime, we have

$$\begin{aligned} \sum_{\substack{\mathfrak{p} \text{ of } K \\ f_{\mathfrak{p}} \geq 2}} \frac{1}{N\mathfrak{p}} &\leq 2 \sum_{p \text{ prime}} \frac{1}{p^2} \\ &\leq 2 \sum_{j=2}^{\infty} \frac{1}{j^2} < \infty. \end{aligned}$$

Thus deleting these primes leaves a divergent sum over inert prime ideals with residue degree one. The relative residue degree in L/K is still two. The degree now being restricted is the degree of $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{F}_p$.

Step 3: pass to distinct rational primes. Let $\mathcal{P}_c$ initially be the set of rational primes under those degree-one inert ideals. Each p is counted at most twice, so

$$\sum_{\substack{\mathfrak{p} \text{ inert} \\ f_{\mathfrak{p}}=1}} \frac{1}{N\mathfrak{p}} \leq 2 \sum_{p \in \mathcal{P}_c} \frac{1}{p}.$$

The right-hand sum must also diverge.

Step 4: ensure the needed local square test. Delete the primes dividing $2D$, all primes below the finitely many nonzero valuations of c , and any prescribed finite set. The sum still diverges. At a chosen remaining inert ideal $\mathfrak{p}$, c is a unit. If its residue were a square, Theorem 3.1 would give $\sqrt{c} \in K_{\mathfrak{p}}$. Then $T^2 - c$ has two distinct linear factors over $K_{\mathfrak{p}}$. The completion decomposition theorem says that the irreducible factors of the defining polynomial over $K_{\mathfrak{p}}$ correspond to the primes above $\mathfrak{p}$, with their degrees equal to the completion degrees [1, Propositions 8.1, 8.2]. It applies because L/K is finite and separable. The two linear factors would give two primes over $\mathfrak{p}$, contradicting inertness. Therefore c has non-square residue, as required. $\square$

3.3. Primes as integer congruences. Fix a non-trivial class $[c] \in V(K)$ and choose one representative $c \in K^{\times}$. For every $p \in \mathcal{P}_c$, choose a prime $\mathfrak{p}(c, p)$ as in Lemma 3.4. Since $\mathcal{O}_K = \mathbb{Z}[w]$ and the residue field is $\mathbb{F}_p$, the image $t_{c,p}$ of w satisfies $t_{c,p}^2 \equiv D \pmod{p}$, and $\mathfrak{p}(c, p) = (p, w - t_{c,p})$. Indeed, evaluation $A + Bw \mapsto A + Bt_{c,p}$ is a surjection onto $\mathbb{F}_p$ with this kernel. There is therefore a residue $r_{c,p} \in \mathbb{Z}/p\mathbb{Z}$ satisfying

$$r_{c,p} \equiv -2 - w \pmod{\mathfrak{p}(c, p)}.$$

For every parameter the local exclusion rule gives

$$\begin{aligned} m \equiv r_{c,p} \pmod{p} &\implies m + w \equiv -2 \pmod{\mathfrak{p}(c, p)} \\ &\implies \alpha_{m, K_{\mathfrak{p}(c, p)}}(E_m(K_{\mathfrak{p}(c, p)})) = \{[1]\} \\ &\implies [c] \notin S_m. \end{aligned} \tag{3.3}$$

The last implication uses that c remains non-square in this completion. A prime ideal of larger residue degree would not necessarily allow its residue $-2 - w$ to be represented by an integer. This explains exactly why degree one is needed.

4. DENSITY-ONE VANISHING

We prove Theorem 1.2. The key estimate uses only finitely many congruences at a time. This is what makes the argument uniform in the starting point of an interval.

4.1. Application of Chinese Remainder Theorem. We use the Chinese remainder theorem in its coprime-modulus form: if $d_1, \dots, d_h$ are pairwise coprime positive integers, then

$$\mathbb{Z}/(d_1 \cdots d_h)\mathbb{Z} \longrightarrow \prod_{i=1}^h \mathbb{Z}/d_i\mathbb{Z}$$

is a bijection, given by reduction in each coordinate [1, Theorem 1.14]. Thus imposing or avoiding residues in different coordinates gives an exact product count.

Fix $[c] \neq [1]$ in $V(K)$, with the separating set $\mathcal{P}_c$ from Lemma 3.4. For a finite subset $T \subset \mathcal{P}_c$, put

$$M_T = \prod_{p \in T} p, \quad \rho_T = \prod_{p \in T} \left(1 - \frac{1}{p}\right).$$

At each $p \in T$, condition (3.3) says that survival of $[c]$ requires avoiding the single residue $r_{c,p}$. There are $p - 1$ choices left. By the Chinese Remainder Theorem the number of permitted residues modulo M_T is exactly

$$\prod_{p \in T} (p - 1) = M_T \rho_T.$$

Each one of these residues occurs at most $X/M_T + 1$ times in any interval of X consecutive integers. Hence, for every B ,

$$\begin{aligned} & \#\{m \in \mathcal{I}(B, X) : [c] \in S_m\} \\ & \leq M_T \rho_T \left(\frac{X}{M_T} + 1 \right) = X \rho_T + M_T \rho_T \leq X \rho_T + M_T. \end{aligned} \quad (4.1)$$

The right side has no dependence on B .

4.2. Limits on ordered sets. For the fixed class $[c]$, define

$$\eta_c(X) = \sup_{B \in \mathbb{Z}} \frac{\#\{m \in \mathcal{I}(B, X) : [c] \in S_m\}}{X}.$$

Keep T fixed while taking $X \rightarrow \infty$. Equation (4.1) gives

$$\begin{aligned} \eta_c(X) & \leq \rho_T + \frac{M_T}{X} \\ & \implies \limsup_{X \rightarrow \infty} \eta_c(X) \leq \rho_T. \end{aligned}$$

We now enlarge the finite set T inside $\mathcal{P}_c$. The elementary inequality $\log(1 - u) \leq -u$ for $0 < u < 1$ follows, for example, by integrating $1/(1 - t) \geq 1$ from 0 to u .

It gives

$$\begin{aligned} \log \rho_T & = \sum_{p \in T} \log \left(1 - \frac{1}{p}\right) \\ & \leq - \sum_{p \in T} \frac{1}{p} \longrightarrow -\infty \quad \implies \quad \rho_T \longrightarrow 0. \end{aligned}$$

Since $\eta_c(X) \geq 0$, we conclude that

$$\eta_c(X) \longrightarrow 0. \quad (4.2)$$

The order of limits is important as the first X grows with the finite modulus fixed, and only afterwards do we add more primes. The argument does not give a claimed rate of convergence in X .

There are finitely many non-trivial classes in $V(K)$, by Proposition 2.3. A non-trivial S_m must contain at least one of them. Therefore

$$\begin{aligned} \sup_{B \in \mathbb{Z}} \frac{|\mathcal{B} \cap \{B+1, \dots, B+X\}|}{X} &\leq \sum_{\substack{[c] \in V(K) \\ [c] \neq [1]}} \eta_c(X) \\ &\longrightarrow 0. \end{aligned}$$

This is the uniform density assertion (1.2). If $V(K)$ has no non-trivial classes, the sum is empty and the conclusion is immediate.

4.3. Progression sequences and signs. Write the supremum in (1.2) as $\eta(X)$ where we have just proved $\eta(X) \rightarrow 0$. Choosing $B = 0$ counts the positive parameters $1, \dots, X$. Choosing $B = -X - 1$ counts the negative parameters $-X, \dots, -1$. Choosing $B = -X - 1$ and interval length $2X + 1$ counts $-X, \dots, X$. Each therefore has exceptional proportion tending to zero.

For a fixed progression $b + q\mathbb{Z}$, where $q \geq 1$, consider a block of X parameters

$$b + q(J+1), \dots, b + q(J+X).$$

It lies in the integer interval $\{b + qJ + 1, \dots, b + qJ + qX\}$. Consequently

$$\begin{aligned} \frac{1}{X} \#\{J < j \leq J+X : b + qj \in \mathcal{B}\} \\ \leq q\eta(qX) \longrightarrow 0. \end{aligned} \quad (4.3)$$

This estimate is even uniform in J , with b and q fixed. Thus the assertion for arithmetic progressions follows directly from the stronger interval statement.

4.4. Average size. Set $C_K = |V(K)|$. For every $m \in \mathbb{Z}$, Lemma 2.5 gives the pointwise bound

$$0 \leq |S_m| - 1 \leq (C_K - 1)\mathbf{1}_{\mathcal{B}}(m), \quad (4.4)$$

where the indicator is 1 for $m \in \mathcal{B}$ and 0 otherwise. For $X \geq 1$, averaging over $\mathcal{I}(B, X)$ gives

$$\begin{aligned} 0 &\leq \frac{1}{X} \sum_{m \in \mathcal{I}(B, X)} |S_m| - 1 \\ &\leq (C_K - 1) \frac{|\mathcal{B} \cap \{B+1, \dots, B+X\}|}{X} \\ &\leq (C_K - 1)\eta(X). \end{aligned}$$

The bound is independent of B and tends to zero. This proves (1.3), and in particular the symmetric average

$$\frac{1}{2X+1} \sum_{|m| \leq X} |S_m| \longrightarrow 1. \quad (4.5)$$

The same inequality applied to a progression block, followed by (4.3), proves its average-size limit. The bound by the fixed number C_K is essential to this deduction: density-one triviality alone would not control the average of arbitrarily large exceptional groups. This completes the proof of Theorem 1.2.

5. VANISHING SUBPROGRESSIONS

We now make a finite selection of one prime for each non-trivial candidate. This proves Theorem 1.3 and gives an explicit formula for the resulting progression once those primes are chosen.

Proof of Theorem 1.3. Step 1: choose the finitely many primes. Fix the prescribed progression $b + q\mathbb{Z}$ with $q \geq 1$. List the non-trivial classes of $V(K)$ as $[c_1], \dots, [c_h]$. Choose primes

$$p_i \in \mathcal{P}_{c_i} \quad (1 \leq i \leq h)$$

successively, requiring each p_i to be distinct from the earlier ones and not to divide q . Lemma 3.4 allows this, since removing any finite set leaves a divergent reciprocal sum and hence infinitely many choices. For each i , choose its indicated degree-one prime ideal and let $r_i = r_{c_i, p_i}$ be the forbidden residue in (3.3).

Step 2: combine the conditions inside the original progression. Write $m = b + qt$. Since q is invertible modulo p_i , the desired condition $m \equiv r_i \pmod{p_i}$ is equivalent to

$$t \equiv d_i := q^{-1}(r_i - b) \pmod{p_i}.$$

Put $P = \prod_{i=1}^h p_i$. For $h > 0$, choose integers u_i satisfying

$$u_i \frac{P}{p_i} \equiv 1 \pmod{p_i}.$$

They exist because P/p_i and p_i are coprime. The usual explicit Chinese Remainder Theorem is

$$t_0 = \sum_{i=1}^h d_i u_i \frac{P}{p_i}.$$

Indeed, reduction modulo p_i leaves only the i th summand, which is d_i . Hence every $t = t_0 + P\ell$ satisfies every condition. Set

$$m_0 = b + qt_0, \quad M = qP. \quad (5.1)$$

Then $m_0 + M\mathbb{Z} \subseteq b + q\mathbb{Z}$, and each member satisfies $m \equiv r_i \pmod{p_i}$ for every i . If $h = 0$, take the empty product $P = 1$ and $t_0 = 0$ to return to the original progression.

Step 3: exclude every non-trivial candidate. For any $m \equiv m_0 \pmod{M}$ and every i ,

$$\begin{aligned} m \equiv r_i \pmod{p_i} &\implies \alpha_{m, K_{\mathfrak{p}(c_i, p_i)}}(E_m(K_{\mathfrak{p}(c_i, p_i)})) = \{[1]\} \\ &\implies [c_i] \notin S_m. \end{aligned}$$

All non-trivial elements of $V(K)$ have been excluded. Since $S_m \subseteq V(K)$ and $[1] \in S_m$, we get $S_m = \{[1]\}$. This holds for every member of the constructed subprogression, not merely for almost all of them. $\square$

The construction uses only finitely many primes, so the modulus M is an ordinary positive integer. The proof gives no small upper bound on M . Its assertion is the existence of a full subprogression of vanishing, with every member included.

6. CONSEQUENCES FOR POINTS AND IDEAL CLASSES

We now state the classical descent theorem that translates $S_m = \{[1]\}$ into information about points and ideal classes.

6.1. The Kummer-Selmer exact sequence. We use the standard isogeny Kummer-Selmer exact sequence. Here $\text{Sha}(A/K)$ denotes the Tate-Shafarevich group of A .

Proposition 6.1 (Classical isogeny Kummer-Selmer theorem). *Let $\psi : A \rightarrow B$ be a degree-two isogeny of elliptic curves over our fixed field K , with $A[\psi]$ rational over K . For $F = K$ or a completion K_v , its Kummer map*

$$\delta_F : B(F) \longrightarrow F^\times / F^{\times 2}$$

is a homomorphism with kernel $\psi(A(F))$. The class $\delta_F(P)$ is the square class of the two-point fiber $\psi^{-1}(P)$ as it is $[c]$ when adjoining $\sqrt{c}$ separates its two points, with $[1]$ for a split fiber. Let $S^\psi(A/K)$ consist of the global square classes whose images lie in $\delta_{K_v}(B(K_v))$ at every place. Then there is an exact sequence

$$0 \longrightarrow B(K)/\psi(A(K)) \xrightarrow{\delta_K} S^\psi(A/K) \longrightarrow \text{Sha}(A/K)[\psi] \longrightarrow 0.$$

We use this proposition as a cited classical input. The square-class identification is Kummer theory [2, Example 1.8(b)], and the exact sequence is [4, Equation (2.1)]. Their Remark 2.2 explains that their Selmer notation names the target B , whereas our notation names the source A . In particular the last group belongs to the source curve.

6.2. Isogeny verification. Apply the proposition with

$$A = E'_m, \quad B = E_m, \quad \psi = \hat{\phi}_m.$$

Lemma 2.1 supplies the degree-two isogeny and its rational kernel $\{O, T'\}$, where $T' = (0, 0)$. The characteristic is zero, so its fibers are separable two-point fibers.

We check its Kummer map without introducing cocycles. Write $a = a_m$, $d = a^2 - 4$, and use (X, Y) on E'_m . Its equation and the formula for $\widehat{\phi}_m$ give the identity of rational functions

$$x \circ \widehat{\phi}_m = \frac{X - 2a + d/X}{4} = \frac{Y^2}{4X^2} = \left(\frac{Y}{2X} \right)^2. \quad (6.1)$$

To distinguish the two points of a fiber, compute translation by its non-identity kernel point T' . The joining line has slope $\lambda = Y/X$. If $(X_1, Y_1) = (X, Y) + T'$, the addition law gives

$$\begin{aligned} X_1 &= \lambda^2 + 2a - X = \frac{Y^2}{X^2} + 2a - X = \frac{d}{X}, \\ Y_1 &= \lambda(X - X_1) - Y = -\frac{dY}{X^2}, \\ \frac{Y_1}{2X_1} &= -\frac{Y}{2X}. \end{aligned}$$

For $P = (x, y)$ with $x \neq 0$, the two points over P therefore have respective values $\sqrt{x}$ and $-\sqrt{x}$ for this function. These two distinct values distinguish the two points, so an automorphism fixes either point exactly when it fixes its value. The points are therefore defined over $F(\sqrt{x})$, and their Kummer class is $[x]$. The point O has the rational preimage O , while $T = (0, 0)$ has the rational preimage $(a+2, 0)$. Both classes are $[1]$. Thus $\delta_F = \alpha_{m,F}$ over K and every completion K_v .

Definition 2.4 consequently gives $S_m = S^{\widehat{\phi}_m}(E'_m/K)$, and the theorem becomes

$$0 \longrightarrow \frac{E_m(K)}{\widehat{\phi}_m(E'_m(K))} \xrightarrow{\alpha_{m,K}} S_m \longrightarrow \text{Sha}(E'_m/K)[\widehat{\phi}_m] \longrightarrow 0. \quad (6.2)$$

The kernel of the final arrow is exactly the image of the global point quotient. This is the concrete obstruction measured by the last group.

6.3. Proof of the results.

Proof of Theorem 1.4. Exactness means that the middle group in (6.2) is trivial if and only if both outer groups are trivial. Hence

$$\begin{aligned} S_m = \{[1]\} &\iff E_m(K)/\widehat{\phi}_m(E'_m(K)) = 0 \text{ and } \text{Sha}(E'_m/K)[\widehat{\phi}_m] = 0 \\ &\iff E_m(K) = \widehat{\phi}_m(E'_m(K)) \text{ and } \text{Sha}(E'_m/K)[\widehat{\phi}_m] = 0. \end{aligned}$$

Suppose these conditions hold and take $(x, y) \in E_m(K)$. For $x \neq 0$, the global descent class belongs to S_m . Thus

$$\begin{aligned} [x] \in S_m = \{[1]\} &\implies x = z^2 \text{ for some } z \in K^\times \\ &\implies (x) = (z)^2. \end{aligned}$$

If $x = 0$, it is the square 0^2 . The descent map at $(0, 0)$ was defined separately, without assigning a square class to zero.

For $x \neq 0$, Lemma 2.5 gives the unique fractional ideal $\mathfrak{a}_x$ with $(x) = \mathfrak{a}_x^2$. For every nonzero prime ideal $\mathfrak{p}$,

$$\begin{aligned} \mathfrak{a}_x^2 = (z)^2 &\implies 2v_{\mathfrak{p}}(\mathfrak{a}_x) = 2v_{\mathfrak{p}}(z) \\ &\implies v_{\mathfrak{p}}(\mathfrak{a}_x) = v_{\mathfrak{p}}(z) \\ &\implies \mathfrak{a}_x = (z), \end{aligned}$$

where the last implication uses unique factorization of fractional ideals. Therefore the half-ideal is principal.

Theorem 1.2 makes these conclusions valid for a set of integer parameters of density one, with its stated uniformity. Theorem 1.3 makes them valid for every member of each constructed subprogression. $\square$

7. AN EXAMPLE OVER $\mathbb{Q}(\sqrt{10})$

We now specialize the family to $D = 10$, which is squarefree and satisfies $D \equiv 2 \pmod{4}$. Throughout this section, put

$$w = \sqrt{10} > 0, \quad K = \mathbb{Q}(w), \quad \varepsilon = 3 + w, \quad E_m = E_{10,m}.$$

Thus the equation under study is

$$E_m : y^2 = x^3 + (m + w)x^2 + x, \quad m \in \mathbb{Z}.$$

The choice $w > 0$ fixes one real embedding for the calculations of units. Both real embeddings will be stated explicitly when used. The earlier results also allow negative D as the sign arguments in this section concern only the present field $\mathbb{Q}(\sqrt{10})$. We abbreviate $\alpha_m = \alpha_{m,K}$ within this section. The notation $[c]$ denotes an element of $K^\times/K^{\times 2}$, while $[\mathfrak{a}]$ denotes an ideal class. These are different groups, connected by the half-ideal map π of Proposition 2.3.

We prove Theorem 1.6 by first computing the field arithmetic, then imposing local conditions. This will also explain why a non-principal candidate can be excluded for one parameter and realized by a point for another.

7.1. The ring of integers and the full ideal class group. The quadratic integral-basis formula [1, Example 2.41] gives

$$\mathcal{O}_K = \mathbb{Z}[w], \quad \text{disc}(K) = 40.$$

The two embeddings send w to w and $-w$, and the field norm is

$$N_{K/\mathbb{Q}}(a + bw) = (a + bw)(a - bw) = a^2 - 10b^2.$$

For a nonzero integral element β , the norm of the principal ideal (β) is $|N_{K/\mathbb{Q}}(\beta)|$. Ideal norms are multiplicative.

The ideal $\mathfrak{q}_2 = (2, w)$ has quotient $\mathbb{F}_2$, so its ideal norm is two. Its square can be checked by multiplying the generators:

$$\mathfrak{q}_2^2 = (4, 2w, w^2) = (4, 2w, 10) = (2).$$

Indeed all three generators are multiples of 2, while $10 - 2 \cdot 4 = 2$ belongs to the ideal. Thus $[\mathfrak{q}_2]^2 = 1$. If $\mathfrak{q}_2 = (a + bw)$ were principal, its generator would be integral, with $a, b \in \mathbb{Z}$, and

$$\begin{aligned} N\mathfrak{q}_2 = 2 &\implies |a^2 - 10b^2| = 2 \\ &\implies a^2 \equiv 2 \text{ or } 3 \pmod{5}. \end{aligned}$$

The squares modulo 5 are 0, 1, 4. This is impossible, proving

$$[\mathfrak{q}_2] \neq 1. \quad (7.1)$$

We must still show that there are no other ideal classes. Minkowski's ideal-class bound [1, Theorem 4.3] for a real quadratic field gives an integral representative of each class with norm at most

$$\frac{\sqrt{40}}{2} < 4.$$

Only norms 1, 2, 3 therefore need to be considered. Norm 1 gives the principal class, and $\mathfrak{q}_2$ is the only prime above 2, since $\mathfrak{q}_2^2 = (2)$.

Modulo 3, the polynomial of w factors as

$$T^2 - 10 \equiv (T - 1)(T + 1) \pmod{3}.$$

Thus the two primes of norm 3 are

$$\mathfrak{q}_3 = (3, w - 1), \quad \mathfrak{q}'_3 = (3, w + 1), \quad \mathfrak{q}_3\mathfrak{q}'_3 = (3).$$

These factorizations are instances of prime-ideal factorization from [1, Theorem 3.41]. They can also be checked here from the quotient maps $w \mapsto 1$ and $w \mapsto -1$ modulo 3. Now

$$N_{K/\mathbb{Q}}(2 + w) = -6, \quad 2 + w \in \mathfrak{q}_2 \cap \mathfrak{q}_3, \quad 2 + w \notin \mathfrak{q}'_3.$$

The ideals $\mathfrak{q}_2$ and $\mathfrak{q}_3$ are distinct primes, so their product divides $(2 + w)$. The product and $(2 + w)$ both have norm 6. Unique factorization of ideals [1, Theorem 3.7] therefore gives

$$\begin{aligned} (2 + w) &= \mathfrak{q}_2\mathfrak{q}_3 \\ &\implies [\mathfrak{q}_3] = [\mathfrak{q}_2]^{-1} = [\mathfrak{q}_2], \\ \mathfrak{q}_3\mathfrak{q}'_3 = (3) &\implies [\mathfrak{q}'_3] = [\mathfrak{q}_3]^{-1} = [\mathfrak{q}_2]. \end{aligned}$$

Every ideal of norm 2 or 3 is prime, because its quotient ring has prime order. We have accounted for all such ideals. The Minkowski bound therefore proves

$$\text{Cl}(K) = \{1, [\mathfrak{q}_2]\} \cong \mathbb{Z}/2\mathbb{Z}. \quad (7.2)$$

This determines the full class group, not just its subgroup of elements of order two.

7.2. The units and the eight virtual square classes. The element $\varepsilon = 3 + w$ is a unit because

$$N(\varepsilon) = 9 - 10 = -1, \quad \varepsilon^{-1} = w - 3 \in \mathcal{O}_K.$$

We verify explicitly that it generates the units up to sign. Suppose $u = a + bw$ is a unit with $1 < u < \varepsilon$ at the embedding where $w > 0$. Its conjugate is $u' = \pm 1/u$, since the norm of a unit is 1 or -1 . Thus

$$0 < b = \frac{u - u'}{2w} \leq \frac{u + 1/u}{2w} < \frac{\varepsilon + 1/\varepsilon}{2w} = 1.$$

The strict inequality holds because $t + 1/t$ is strictly increasing for $t > 1$. Equivalently, for $v > u > 1$ its difference is $(v - u)(1 - 1/(uv)) > 0$. We have contradicted $b \in \mathbb{Z}$. There is therefore no unit in the interval $(1, \varepsilon)$.

For an arbitrary unit u , choose $s \in \{1, -1\}$ so that $su > 0$ at this embedding, and take $j = \lfloor \log(su)/\log \varepsilon \rfloor$. Then

$$\varepsilon^j \leq su < \varepsilon^{j+1} \implies 1 \leq su\varepsilon^{-j} < \varepsilon.$$

The element $su\varepsilon^{-j}$ is a unit. The preceding argument forces it to equal 1, so $u = s\varepsilon^j$. Hence

$$\mathcal{O}_K^\times = \{\pm \varepsilon^j : j \in \mathbb{Z}\}. \quad (7.3)$$

Modulo squares, its four classes are represented by $1, -1, \varepsilon, -\varepsilon$. Here is the independence check. If $(-1)^i \varepsilon^j = z^2$ with $i, j \in \{0, 1\}$, then $v_p(z) = 0$ at every finite prime because its square is a unit. Thus z is itself a unit, and (7.3) gives $z = s\varepsilon^r$ for $s \in \{1, -1\}$ and $r \in \mathbb{Z}$. Consequently

$$\begin{aligned} (-1)^i \varepsilon^j = z^2 = \varepsilon^{2r} &\implies i = 0 \text{ by positivity at } w > 0, \\ \varepsilon^j = \varepsilon^{2r} &\implies j = 2r \text{ because } \varepsilon > 1 \\ &\implies j = 0. \end{aligned}$$

Thus the four unit square classes are distinct.

Apply Proposition 2.3. Its exact sequence becomes

$$0 \longrightarrow \langle [-1], [\varepsilon] \rangle \longrightarrow V(K) \xrightarrow{\pi} \langle [\mathfrak{q}_2] \rangle \longrightarrow 0.$$

The map in this exact sequence is the ordinary ideal-class map: if $(c) = \mathfrak{a}^2$, it sends $[c]$ to $[\mathfrak{a}]$. Since $(2) = \mathfrak{q}_2^2$, the class $[2]$ maps to the non-identity ideal class. In particular, $[2] \neq [1]$; a hypothetical square root $2 = z^2$ would imply $\mathfrak{q}_2^2 = (z)^2$, hence $\mathfrak{q}_2 = (z)$ by unique ideal factorization, contradicting (7.1). Therefore every class in $V(K)$ has a unique expression

$$[c] = [(-1)^i \varepsilon^j 2^k], \quad i, j, k \in \{0, 1\}. \quad (7.4)$$

For existence, use $[2]^k$ to remove the ideal-class image and then use the unit generators. For uniqueness, applying π first forces k , and the independence of the unit classes then forces i, j . In particular

$$V(K) = \{[1], [-1], [\varepsilon], [-\varepsilon], [2], [-2], [2\varepsilon], [-2\varepsilon]\}, \quad \pi([c]) = [\mathfrak{q}_2]^k.$$

Exactly four virtual classes map to the non-principal ideal class: those with $k = 1$. The local conditions still have to be checked. The class group alone does not decide whether these classes belong to S_m .

7.3. Conditions for the parameters. Let $F = K_{\mathfrak{q}_2}$, with normalized valuation v . The equality $\mathfrak{q}_2^2 = (2)$ gives $v(2) = 2$. Since 5 is a local unit and $w^2 = 2 \cdot 5$, we have

$$2v(w) = v(2) + v(5) = 2 \implies v(w) = 1.$$

Thus w is a uniformizer, and $(w^2) = (2)$ in $\mathcal{O}_F$. Completion preserves the quotients by powers of the maximal ideal: local integers can be approximated modulo any such power by global integers, with the same kernel of reduction. This is the finite quotient property of completion [1, Aside 7.30]. Applying it at the power $\mathfrak{q}_2^2$ gives the explicit calculation

$$\begin{aligned} \mathcal{O}_F/(w^2) &\cong \mathcal{O}_K/\mathfrak{q}_2^2 = \mathbb{Z}[w]/(2) \\ &\cong \mathbb{F}_2[t]/(t^2). \end{aligned}$$

The four elements of this quotient are $0, t, 1, 1+t$. Their squares are, respectively, $0, 0, 1, 1$. Its two units are 1 and $1+t$, and both are their own inverses.

Lemma 7.1. *For every integer m , every first local image class over F has a representative in $1 + w^2\mathcal{O}_F$. Consequently, if $[(-1)^i \varepsilon^j 2^k] \in S_m$, then $j = 0$.*

Proof. First, there is no local point with $v(x) = 0$. For such a point y is integral. Dividing the equation by x^2 gives

$$(y/x)^2 = x + (m+w)x^{-1}.$$

Modulo w^2 , the unit x equals its inverse, so $x + x^{-1} = 0$ in the quotient. The right side is therefore $(m \bmod 2) + t$, which is neither 0 nor 1. It cannot be a square. This is a contradiction.

For a point with $x \neq 0$ and $v(x) \neq 0$, the valuation calculation of Lemma 2.5 shows that $v(x)$ is even. To check that we may divide by y , observe that $y = 0$ would give $x^2 + (m+w)x + 1 = 0$. If $v(x) > 0$, the constant term would have uniquely smallest valuation. If $v(x) < 0$, the term x^2 would have uniquely smallest valuation. Neither sum can vanish. Thus $y \neq 0$. If $v(x) > 0$, then $v(x) \geq 2$ and

$$\begin{aligned} y^2 = x(1 + (m+w)x + x^2) &\implies [x] = [1 + (m+w)x + x^2], \\ 1 + (m+w)x + x^2 &\in 1 + w^2\mathcal{O}_F. \end{aligned}$$

If $v(x) < 0$, then $v(1/x) \geq 2$ and

$$\begin{aligned} y^2 = x^3(1 + (m+w)/x + 1/x^2) &\implies [x] = [1 + (m+w)/x + 1/x^2], \\ 1 + (m+w)/x + 1/x^2 &\in 1 + w^2\mathcal{O}_F. \end{aligned}$$

We used $[x]^3 = [x]$ in the second case. The special points have class $[1]$, which also has a representative of the required form.

Now take the representative $c = (-1)^i \varepsilon^j 2^k$ from (7.4). Dividing by the square w^{2k} gives the unit representative

$$c_0 = (-1)^i \varepsilon^j 5^{-k}.$$

If $[c] \in S_m$, the first part gives a unit $u \equiv 1 \pmod{w^2}$ in the same local square class. Thus $c_0/u = z^2$ for a local unit z . A unit square is 1 modulo w^2 , so $c_0 \equiv 1 \pmod{w^2}$. However,

$$-1 \equiv 1, \quad 5^{-1} \equiv 1, \quad \varepsilon = 3 + w \equiv 1 + w \pmod{w^2},$$

and hence $c_0 \equiv (1+w)^j$. The element w is nonzero modulo w^2 , so this is 1 exactly when $j = 0$. This proves the lemma. $\square$

The lemma proves the uniform restriction

$$S_m \subseteq \langle [-1], [2] \rangle. \quad (7.5)$$

It excludes the four candidates involving an odd power of ε for every parameter, before any odd-prime condition is imposed.

7.4. Progression on odd prime factors. Use the primes

$$\mathfrak{q}_3 = (3, w-1), \quad \mathfrak{q}_5 = (5, w).$$

Their residue fields are $\mathbb{F}_3$ and $\mathbb{F}_5$, respectively. The second prime is ramified in $K/\mathbb{Q}$. This causes no large difference because Lemma 3.2 requires odd residue characteristic, not an unramified extension. The basis representatives $-1, \varepsilon, 2$ are units at both primes. Their residues and quadratic characters are

prime	$\bar{w}$	-1	ε	2	$\chi(-1)$	$\chi(\varepsilon)$	$\chi(2)$
$\mathfrak{q}_3$	1	2	1	2	-1	1	-1
$\mathfrak{q}_5$	0	4	3	2	1	-1	-1

Here χ is 1 on nonzero squares and -1 on non-squares in the indicated residue field. The table follows just by listing the nonzero squares $\{1\}$ modulo 3 and $\{1, 4\}$ modulo 5.

We claim the following exact vanishing progression:

$$m \equiv 3 \pmod{15} \implies S_m = \{[1]\}. \quad (7.6)$$

Suppose $m \equiv 3 \pmod{15}$. The two congruences are

$$\begin{aligned} m \equiv 0 \pmod{3}, \quad w \equiv 1 \pmod{\mathfrak{q}_3} &\implies m + w \equiv 1 = -2 \pmod{\mathfrak{q}_3}, \\ m \equiv 3 \pmod{5}, \quad w \equiv 0 \pmod{\mathfrak{q}_5} &\implies m + w \equiv 3 = -2 \pmod{\mathfrak{q}_5}. \end{aligned}$$

Both local first-descent images are therefore trivial. If $[c] = [(-1)^i \varepsilon^j 2^k] \in S_m$, the dyadic lemma and the two rows of the character table give

$$\begin{aligned} \text{at } \mathfrak{q}_2: \quad &j = 0, \\ \text{at } \mathfrak{q}_3: \quad &i + k = 0 \text{ in } \mathbb{F}_2, \\ \text{at } \mathfrak{q}_5: \quad &j + k = 0 \text{ in } \mathbb{F}_2 \\ &\implies j = 0, \quad k = 0, \quad i = 0. \end{aligned}$$

Thus every one of the seven non-trivial candidates is excluded, and $S_m = \{[1]\}$. The Chinese Remainder Theorem construction is explicit by writing $m = 3t$, the requirement $m \equiv 3 \pmod{5}$ is $t \equiv 1 \pmod{5}$, so $m = 3 + 15\ell$. This proves (7.6) for every integer in the progression, including negative integers. Theorem 1.4 now yields

$$E_m(K) = \hat{\phi}_m(E'_m(K)), \quad \text{Sha}(E'_m/K)[\hat{\phi}_m] = 0 \quad (m \equiv 3 \pmod{15}).$$

Also, every point with $x \neq 0$ has $x = z^2$ for some $z \in K^\times$, so its fractional half-ideal is the principal ideal (z) .

7.5. The parameter $m = 1$ and its global points. At $m = 1$, direct substitution gives

$$(2 + w)^2 = 14 + 4w,$$

$$2^3 + (1 + w)2^2 + 2 = 8 + 4 + 4w + 2 = 14 + 4w.$$

Therefore $P = (2, 2 + w)$ lies on $E_1(K)$. The torsion classification in Theorem 1.5 applies because 10 is squarefree and $10 \equiv 2 \pmod{4}$. It gives

$$E_1(K)_{\text{tors}} = \{O, (0, 0)\}.$$

Since P has nonzero second coordinate, it is not one of these points and has infinite order. Its first descent class is $[2]$, and the already proved equality $(2) = \mathfrak{q}_2^2$ gives

$$\alpha_1(P) = [2], \quad (x(P)) = \mathfrak{q}_2^2, \quad \pi([2]) = [\mathfrak{q}_2] \neq 1. \quad (7.7)$$

In particular $[2] \in S_1$ and is non-trivial.

It remains to exclude the other candidates at this parameter. The dyadic lemma has already reduced them to

$$S_1 \subseteq \{[1], [-1], [2], [-2]\}.$$

For the remaining step we use that this particular field is real: $D = 10 > 0$. Consider its real embedding $\sigma_- : w \mapsto -\sqrt{10}$. The coefficient becomes $1 - \sqrt{10} < 0$. If a real point had $x < 0$, then

$$x^2 + (1 - \sqrt{10})x + 1 > 0,$$

$$x(x^2 + (1 - \sqrt{10})x + 1) < 0,$$

contradicting $y^2 \geq 0$. All nonzero x -coordinates at this real place are positive, so its first local image is trivial. The classes $[-1]$ and $[-2]$ are negative at this embedding and cannot belong to S_1 . We have proved

$$\{[1], [2]\} \subseteq S_1 \subseteq \{[1], [2]\}, \quad \text{hence } S_1 = \{[1], [2]\}.$$

Finally, the actual global point P supplies the non-identity element of S_1 . The global Kummer image is consequently the whole group S_1 . The isogeny Kummer exact sequence quoted and identified in Section 6 is

$$0 \longrightarrow E_1(K)/\widehat{\phi}_1(E'_1(K)) \longrightarrow S_1 \longrightarrow \text{Sha}(E'_1/K)[\widehat{\phi}_1] \longrightarrow 0.$$

The general isogeny form is described in [4, Equation (2.1) and Remark 2.2]. The latter explains the alternative source-versus-target convention for naming the Selmer group. Since the first arrow is now surjective as well as injective, exactness gives

$$E_1(K)/\widehat{\phi}_1(E'_1(K)) \cong S_1 \cong \mathbb{Z}/2\mathbb{Z},$$

$$\text{Sha}(E'_1/K)[\widehat{\phi}_1] = 0. \quad (7.8)$$

This proves (7.8) and completes the proof of Theorem 1.6. Thus this member has a non-trivial first Selmer group even though the specified Sha kernel is zero, meaning its non-identity Selmer class comes from the global point P .

Corollary 7.2 (Odd multiples; a consequence of descent). *For every odd integer n , the point nP has infinite order and there is $z_n \in K^\times$ such that*

$$x(nP) = 2z_n^2, \quad (x(nP)) = ((z_n)\mathfrak{q}_2)^2.$$

Its unique fractional half-ideal is $(z_n)\mathfrak{q}_2$, which is non-principal. Thus the single curve E_1 has infinitely many infinite-order points carrying the non-principal ideal class.

Proof. Since P has infinite order and n is a nonzero integer, nP also has infinite order. In particular it is neither O nor $(0, 0)$, so its x -coordinate is nonzero. The descent map is a homomorphism, and n is odd, giving

$$\begin{aligned} \alpha_1(nP) = [2]^n = [2] &\implies x(nP) = 2z_n^2 \text{ for some } z_n \in K^\times \\ &\implies (x(nP)) = (2)(z_n)^2 = (\mathfrak{q}_2(z_n))^2. \end{aligned}$$

Unique ideal factorization identifies this square root ideal. Its class is $[\mathfrak{q}_2] \neq 1$, because multiplication by the principal ideal (z_n) does not change an ideal class. The half-ideal is unique because all exponents in a fractional ideal factorization are integers. Thus $\mathfrak{a}^2 = \mathfrak{b}^2$ forces each exponent in $\mathfrak{a}$ and $\mathfrak{b}$ to agree. Distinct odd integers give distinct points as if $nP = n'P$, then $(n - n')P = O$, so $n = n'$ because P has infinite order. $\square$

In this example, the non-principal class does not produce an unaccounted-for Sha class. The progression $m \equiv 3 \pmod{15}$ shows how the same candidate can be removed by local conditions at other parameters. This distinguishes the fixed field arithmetic, encoded by $V(K)$ and $\text{Cl}(K)[2]$, from the parameter-dependent local conditions.

8. CONCLUSION

The fixed field supplies possible square classes, but each curve decides which of them remain. The coefficient 1 forces even valuations and places every first-descent class in $V(K)$. The map $\pi : V(K) \rightarrow \text{Cl}(K)[2]$ identifies the ideal-class part of a candidate. Its membership in S_m then asks whether it passes the local tests for that particular parameter.

The argument answering the frequency question has three steps:

$$\begin{aligned} [c] &\neq [1] \implies \text{many degree-one primes keep } c \text{ non-square,} \\ m \equiv -2 - w \pmod{\mathfrak{p}} &\implies \text{the local first image is trivial,} \\ \text{these two conditions together} &\implies [c] \notin S_m. \end{aligned}$$

The first step is the direct consequence of Chebotarev, the second is a family-specific calculation, and the third is the definition of the Selmer condition. Counting finitely many such congruences at a time gives uniform density-one vanishing and the average-size limit. Choosing one detecting prime per candidate gives a subprogression of guaranteed vanishing.

Over $\mathbb{Q}(\sqrt{10})$, the non-principal class is actually realized when $P = (2, 2 + \sqrt{10})$ at $m = 1$ has descent class $[2]$. The torsion theorem certifies that P has infinite

order, and its odd multiples supply infinitely many points with non-principal half-ideals. At every $m \equiv 3 \pmod{15}$, the first Selmer group is trivial, and all point half-ideals are principal. The class group of the field has not changed. What changes is whether a class contributes to the descent of the chosen curve.

Throughout the family, $E_m(K)_{\text{tors}} \cong C_2$ and $E'_m(K)_{\text{tors}} \cong C_2 \times C_2$. $S_m = \{[1]\}$ implies that $E_m(K) = \hat{\phi}_m(E'_m(K))$ and $\text{Sha}(E'_m/K) [\hat{\phi}_m] = 0$.

9. ACKNOWLEDGEMENTS

Over the past nine months, I worked under the guidance of my mentors to produce the paper on Non-principal ideal classes and Selmer vanishing over quadratic fields. I would like to take the time to thank my mentor Dr. Zhu and counselor Filippo for their guidance as detailed below.

My interest in the project originated from my PROMYS course titled: Projective Curves. The course built on my previous background of algebraic geometry by introducing more sophisticated proofs of theorems. After developing an interest in pursuing this field, subsequent extensive reading and discussions with my in-school teacher and mentor, Dr. Yating Zhu from the SHSID STEM Office, helped me locate this rather interesting problem.

Dr. Zhu recommended the works listed as references 1, 2, and 3 in the paper and guided my exploration of the literature, discussing the current structural knowledge of elliptic curves as well as possible cavities. I undertook the reading and further investigation needed to develop the project. The published sources supplied background results and context, while my work on the paper involved formulating the precise problem and developing the arguments presented in response to it.

After initial consolidation of the proofs, Dr. Zhu helped me organize the arguments into a more logical sequence and present the paper in a more formally accepted manner. Her guidance concerned how the research should be communicated clearly, including how to present consecutive statements in the proof.

I would also like to take the time to appreciate Filippo, my counselor at PROMYS 2026, for helping me understand course material and gain insight into practice problems, while unrelated to the problem in this specific paper, provided me with many problem solving tools specifically related to structures in algebraic geometry. His feedback also led me to investigate the possibility of pursuing a career in mathematics.

APPENDIX A. PROOF OF THE TORSION CLASSIFICATION

We use the assumptions of the paper that D is squarefree, $D \equiv 2 \pmod{4}$, $K = \mathbb{Q}(w)$ with $w^2 = D$, and $m \in \mathbb{Z}$. There is no restriction on the sign of D . Write

$$a = m + w, \quad d = a^2 - 4,$$

and abbreviate $E_{D,m}$ and $E'_{D,m}$ by E_m and E'_m :

$$E_m : y^2 = x^3 + ax^2 + x,$$

$$E'_m : Y^2 = X^3 - 2aX^2 + dX = X(X - a - 2)(X - a + 2).$$

The isogenies and their kernels were proved in Lemma 2.1. We establish the square and duplication tests first, exclude odd torsion at the unique prime above 2, and then assemble the result.

A.1. The square tests.

Lemma A.1 (A coefficient restriction). *If $A, B \in \mathbb{Z}$ and $A + Bw$ is a square in K , then every square root belongs to $\mathbb{Z}[w]$ and B is even. In particular, neither $a + 2$ nor $a - 2$ is a square in K .*

Proof. Suppose $z \in K$ satisfies $z^2 = A + Bw$. Then

$$(z^2 - A)^2 = B^2D \implies z^4 - 2Az^2 + (A^2 - B^2D) = 0.$$

The polynomial is monic with integer coefficients, so z is an algebraic integer. Because $D \equiv 2 \pmod{4}$, the quadratic integral-basis formula gives $\mathcal{O}_K = \mathbb{Z}[w]$ [1, Example 2.41]. We may therefore write $z = r + sw$ with $r, s \in \mathbb{Z}$. Coefficient comparison yields

$$z^2 = r^2 + Ds^2 + 2rs w = A + Bw \implies 2rs = B.$$

Thus B is even. The coefficient of w in each of $a + 2$ and $a - 2$ is 1, so neither can be a square. $\square$

Lemma A.2 (The quadratic factor does not split). *The element $d = (m + w)^2 - 4$ is not a square in K . Consequently $E_m(K)$ has precisely one non-identity point of order two, namely $T = (0, 0)$.*

Proof. If $d = z^2$, Lemma A.1 gives $z = r + sw$ for integers r, s . Comparing coefficients gives

$$\begin{aligned} r^2 + Ds^2 &= m^2 + D - 4, & rs &= m \implies r^2 + Ds^2 = r^2s^2 + D - 4 \\ & & &\implies (s^2 - 1)(r^2 - D) = 4. \end{aligned}$$

If s is odd, then $s^2 \equiv 1 \pmod{8}$. The left side is divisible by 8, whereas the right side is not. If s is even, then $s^2 - 1 \equiv -1 \pmod{4}$. Reducing the same equation modulo 4 gives

$$-(r^2 - D) \equiv 0 \pmod{4} \implies r^2 \equiv D \equiv 2 \pmod{4},$$

which is impossible because a square is 0 or 1 modulo 4. Both parity cases are excluded, so d is a non-square.

The inverse of an affine point is $(x, -y)$, so a non-identity point of order two has $y = 0$. On E_m this gives

$$x(x^2 + ax + 1) = 0.$$

The quadratic factor has discriminant d and has no root in K . Thus the only such point is $(0, 0)$. $\square$

A.2. The duplication formula.

Lemma A.3. *Let C be either E_m or E'_m , written as $y^2 = x^3 + Ax^2 + Bx$, with*

$$(A, B) = (a, 1) \quad \text{or} \quad (A, B) = (-2a, d),$$

respectively. For $Q = (x, y) \in C(K)$ with $y \neq 0$,

$$x(2Q) = \left(\frac{x^2 - B}{2y} \right)^2. \quad (\text{A.1})$$

Hence the first coordinate of every affine double on either curve is a square. The same formula holds over the completion used below.

Proof. The tangent slope is $\lambda = (3x^2 + 2Ax + B)/(2y)$, and the chord-and-tangent formula gives

$$\begin{aligned} x(2Q) &= \lambda^2 - A - 2x \\ &= \frac{(3x^2 + 2Ax + B)^2 - 4(A + 2x)(x^3 + Ax^2 + Bx)}{4y^2}. \end{aligned}$$

The numerator can be checked term by term:

$$\begin{aligned} (3x^2 + 2Ax + B)^2 &= 9x^4 + 12Ax^3 + (4A^2 + 6B)x^2 \\ &\quad + 4ABx + B^2, \\ 4(A + 2x)(x^3 + Ax^2 + Bx) &= 8x^4 + 12Ax^3 + (4A^2 + 8B)x^2 + 4ABx. \end{aligned}$$

Subtracting gives $x^4 - 2Bx^2 + B^2 = (x^2 - B)^2$, proving the formula. If a double is affine, its original point is neither O nor a point with $y = 0$, because those points double to O . Thus every affine double is covered. The calculation uses field operations alone and remains valid in the completion of K . $\square$

A.3. The unique dyadic primes. Let $\mathfrak{p} = (2, w) \subset \mathbb{Z}[w]$. Its quotient is $\mathbb{F}_2$, so it is a prime ideal. Also

$$\mathfrak{p}^2 = (4, 2w, D) = (2).$$

To verify the last equality, all three generators are divisible by 2, while

$$D - 4 \left(\frac{D-2}{4} \right) = 2$$

shows that 2 belongs to $\mathfrak{p}^2$. Here $(D-2)/4$ is an integer, including when $D < 0$. Unique ideal factorization therefore makes $\mathfrak{p}$ the only prime above 2. Put $F = K_{\mathfrak{p}}$ and normalize the valuation by $v(F^\times) = \mathbb{Z}$. Then

$$v(2) = 2, \quad \mathcal{O}_F/\mathfrak{m}_F = \mathbb{F}_2.$$

Write $D = 2D_0$ with D_0 odd. Since D_0 is a local unit,

$$2v(w) = v(w^2) = v(2D_0) = 2 \implies v(w) = 1.$$

Thus w is a uniformizer and $\mathfrak{m}_F = w\mathcal{O}_F$. We use the convention $v(0) = +\infty$.

An integral Weierstrass equation over F is *minimal* if its discriminant valuation is least among integral Weierstrass equations for the same pointed curve. To reduce a point, choose projective coordinates in $\mathcal{O}_F$ with at least one unit coordinate and reduce them modulo $\mathfrak{m}_F$.

Theorem A.4 (Local reduction). *For an elliptic curve C/F with a minimal integral Weierstrass equation, $v(\Delta) > 0$ and $v(c_4) > 0$ imply additive reduction. Let $C_0(F)$ be the subgroup reducing to nonsingular points and $C_1(F)$ the subgroup reducing to the identity. In the additive case,*

$$C_0(F)/C_1(F) \cong (\mathbb{F}_2, +), \quad |C(F)/C_0(F)| \leq 4.$$

The parameter $t = -x/y$, with $t(O) = 0$, identifies $C_1(F)$ with $\mathfrak{m}_F$ equipped with a formal group law. Multiplication by a positive integer n has a convergent expansion

$$[n](t) = nt + \sum_{j \geq 2} c_j t^j, \quad c_j \in \mathcal{O}_F.$$

The reduction criterion and nonsingular reduction group are in [2, Chapter II, Section 3]. The reduction filtration and formal-group description are in [2, Proposition 4.1]. Remark 4.3 includes residue characteristic two and finite ramified extensions. The component-group bound is stated for every finite extension of $\mathbb{Q}_p$ in [7, Introduction], so it applies to this ramified quadratic field above 2.

Lemma A.5 (The minimal equation at the dyadic prime). *The displayed equation of E_m is minimal over F and has additive reduction. More precisely,*

	$v(a)$	$\nu := v(a+2)$	$v(\Delta)$
m odd	0	0	8
m even	1	1	10

Proof. The invariant formulas give

$$\Delta = 16(a^2 - 4), \quad c_4 = 16(a^2 - 3)$$

[2, Chapter II, Section 2]. If m is odd, $v(m) = 0 < v(w) = 1$, so $v(a) = 0$. Both $a+2$ and $a-2$ are then units, giving

$$v(a^2 - 4) = 0, \quad \nu = 0, \quad v(\Delta) = 8.$$

If m is even, $v(m) \geq 2 > v(w) = 1$, where $m = 0$ is covered by $v(0) = +\infty$. The rule for a sum of unequal valuations gives

$$\begin{aligned} v(a) = v(m+w) = 1 < 2 = v(2) &\implies v(a+2) = v(a-2) = 1 \\ &\implies v(a^2 - 4) = 2 \\ &\implies \nu = 1, \quad v(\Delta) = 10. \end{aligned}$$

In either case $0 < v(\Delta) < 12$. An isomorphism of Weierstrass equations has discriminant transformation $\Delta = u^{12}\Delta'$, with $u \in F^\times$ [2, Theorem 2.4(b)]. A strictly smaller valuation would therefore satisfy

$$v(\Delta') = v(\Delta) - 12v(u), \quad v(u) \in \mathbb{Z}_{\geq 1},$$

and hence would be negative. This is impossible for an integral Weierstrass equation. Our equation is minimal. Finally a is integral, so

$$v(c_4) = 8 + v(a^2 - 3) \geq 8 > 0.$$

Theorem A.4 proves additive reduction. □

A.4. Excluding order three.

Lemma A.6. *The curve E_m has no K -rational point of order three.*

Proof. Suppose $P = (x, y)$ has order three. Then $x, y \neq 0$ and $2P = -P$. Using the duplication identity on E_m gives

$$x = x(2P) = \left(\frac{x^2 - 1}{2y} \right)^2.$$

Thus x is a square in K , and also in F . Clearing denominators in the same equality gives

$$\begin{aligned} 4xy^2 = (x^2 - 1)^2 &\implies 4x(x^3 + ax^2 + x) = x^4 - 2x^2 + 1 \\ &\implies \psi_3(x) := 3x^4 + 4ax^3 + 6x^2 - 1 = 0. \end{aligned}$$

This polynomial has been derived from duplication.

We first show that x is a unit in F . If $v(x) < 0$, the term $3x^4$ has valuation $4v(x)$, and the differences from the other three term valuations are

$$\begin{aligned} v(4ax^3) - 4v(x) &= 4 + v(a) - v(x) > 0, \\ v(6x^2) - 4v(x) &= 2 - 2v(x) > 0, \\ v(-1) - 4v(x) &= -4v(x) > 0. \end{aligned}$$

The uniquely smallest term cannot cancel. If $v(x) > 0$, all three nonconstant terms have positive valuation, so -1 is instead the uniquely smallest term. Thus $v(x) = 0$. Reduction of $\psi_3(x) = 0$ gives

$$\bar{x}^4 - 1 = (\bar{x} - 1)^4 = 0 \implies \bar{x} = 1.$$

Write $x = u^2$. The unit u has $\bar{u}^2 = 1$, so $\bar{u} = 1$. Since the residue field has characteristic two, both $u - 1$ and $u + 1$ lie in $\mathfrak{m}_F$. Putting $z = x - 1$, we obtain

$$z = (u - 1)(u + 1), \quad v(u - 1), v(u + 1) \geq 1 \implies v(z) \geq 2.$$

The case $z = 0$ is included by the convention $v(0) = +\infty$.

Expand at $x = 1$:

$$\begin{aligned} 0 = \psi_3(1 + z) &= 4(a + 2) + 12(a + 2)z + 12(a + 2)z^2 \\ &\quad + 4(a + 3)z^3 + 3z^4. \end{aligned}$$

By Lemma A.5, $\nu = v(a + 2)$ is zero or one. The constant term is nonzero and has valuation $4 + \nu \leq 5$. The remaining valuations satisfy

$$\begin{aligned} v(12(a + 2)z) &\geq 6 + \nu, \\ v(12(a + 2)z^2) &\geq 8 + \nu, \\ v(4(a + 3)z^3) &\geq 10, \\ v(3z^4) &\geq 8. \end{aligned}$$

Every one is strictly greater than $4 + \nu$. Again a uniquely smallest term cannot cancel, contradicting the equation. $\square$

A.5. Excluding odd torsion.

Proposition A.7. *Neither $E_m(K)$ nor $E'_m(K)$ has non-trivial odd torsion.*

Proof. Let G_0, G_1 be the reduction subgroups of $E_m(F)$ denoted by $C_0(F), C_1(F)$ in Theorem A.4. For an odd positive integer n and a nonzero parameter $t \in \mathfrak{m}_F$, that theorem gives

$$[n](t) = nt + \sum_{j \geq 2} c_j t^j.$$

Because n is a unit, $v(nt) = v(t)$. Every higher term has valuation at least $2v(t) > v(t)$:

$$v(nt) = v(t) < 2v(t) \leq jv(t) \leq v(c_j t^j) \quad (j \geq 2).$$

The higher terms form a convergent sum of valuation at least $2v(t)$ and cannot cancel nt . Hence $[n](t) \neq 0$, proving that G_1 has no non-trivial odd torsion.

The quotient $G_0/G_1 \cong (\mathbb{F}_2, +)$ has order two. An odd-order point of G_0 maps to an element of order dividing both two and an odd integer. Its image is therefore zero, so it lies in G_1 , where it must also be zero. Thus every finite odd-order subgroup of $E_m(F)$ injects into $E_m(F)/G_0$. Additive reduction and the component-group bound give

$$|E_m(F)/G_0| \leq 4.$$

If a non-trivial K -rational point had odd order, the order of its cyclic group would therefore be an odd integer greater than one and at most four. It would have order three, contradicting Lemma A.6. This excludes odd torsion on $E_m(K)$.

The map $\hat{\phi}_m : E'_m(K) \rightarrow E_m(K)$ has kernel of order two by Lemma 2.1. An odd-order subgroup meets this kernel trivially, so its restriction is injective. The absence of odd torsion on $E_m(K)$ therefore gives the same conclusion for $E'_m(K)$. $\square$

Proof of Theorem 1.5. There is no non-trivial odd torsion on either curve. Every torsion point therefore has order a power of two, since any other finite order would yield a non-trivial odd-order multiple.

On E_m , Lemma A.2 shows that $T = (0, 0)$ is the only non-identity point of order two. If a point Q had order four, we would have $2Q = T$ and $Q = (x, y)$ with $y \neq 0$. By the duplication identity,

$$\begin{aligned} x(2Q) = 0 &\implies x^2 = 1 \\ &\implies x = 1 \text{ or } x = -1 \\ &\implies y^2 = a + 2 \text{ or } y^2 = a - 2. \end{aligned}$$

Both alternatives are impossible by Lemma A.1. Thus $E_m(K)$ has no point of order four.

The factored equation of E'_m gives precisely the three non-identity points of order two

$$T' = (0, 0), \quad (a + 2, 0), \quad (a - 2, 0).$$

They are distinct because $a \neq \pm 2$ and $4 \neq 0$ in K . The last two cannot be doubles since every affine double has a square first coordinate, whereas $a + 2$ and $a - 2$

are non-squares. A half $Q = (X, Y)$ of T' would have $Y \neq 0$, and duplication on E'_m gives

$$0 = x(2Q) = \left(\frac{X^2 - d}{2Y} \right)^2 \implies X^2 = d.$$

This contradicts Lemma A.2. None of the three non-identity points of order two has a half, so $E'_m(K)$ also has no point of order four.

A point of order 2^j with $j \geq 2$ would have a multiple of order four. Therefore every torsion point on either curve is killed by two, and the lists just obtained are complete:

$$E_m(K)_{\text{tors}} = \{O, (0, 0)\} \cong \mathbb{Z}/2\mathbb{Z},$$

$$E'_m(K)_{\text{tors}} = \{O, (0, 0), (a + 2, 0), (a - 2, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

In particular every affine torsion point on either displayed model has ordinate zero. Every argument used only squarefreeness and $D \equiv 2 \pmod{4}$. $\square$

REFERENCES

- [1] J. S. Milne, *Algebraic Number Theory*, version 3.08 (2020). <https://www.jmilne.org/math/CourseNotes/ANT.pdf>.
- [2] J. S. Milne, *Elliptic Curves*, second edition, World Scientific (2021). <https://www.jmilne.org/math/Books/EC2.pdf>.
- [3] A. V. Sutherland, *Number Theory I*, MIT 18.785, Fall 2021, Lecture 28, Theorem 28.9 (lecture page 6), Chebotarev density theorem. https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/mit18_785f21_full_lec.pdf.
- [4] B. Creutz and R. L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, Journal of Algebra **372** (2012), 673–701. <https://www.math.canterbury.ac.nz/~b.creutz/Papers/sec-desc-bsd.pdf>.
- [5] D. Zywina, *On the infinitude of elliptic curves over a number field with prescribed small rank*, preprint (2026), arXiv:2602.10865. Lemmas 5.13–5.14. <https://davidzywina.github.io/papers/LowRanks.pdf>.
- [6] D. Loughran and A. Smeets, *Fibrations with few rational points*, Geometric and Functional Analysis **26** (2016), 1449–1482. Theorems 1.2 and 1.5; Section 5.5. doi:10.1007/s00039-016-0381-8.
- [7] J. E. Cremona, *Computing in component groups of elliptic curves*, Algorithmic Number Theory, ANTS VIII, Lecture Notes in Computer Science **5011** (2008), 118–124. Introduction. <https://johncremona.github.io/papers/component.pdf>.