GROSS VECTORS MODULO 2 AND ELLIPTIC CURVES OF PRIME CONDUCTOR

MATIJA KAZALICKI AND SINIŠA SLIJEPČEVIĆ

Abstract. Let $p > 3$ be a prime, and let S_p denote the geometric isomorphism classes of supersingular elliptic curves in characteristic p whose j-invariants lie in $\mathbb{F}_p$. For each negative fundamental discriminant $-D$ for which p is inert in $\mathbb{Q}(\sqrt{-D})$, let $m_i(D)$, $i \in S_p$, be the integral coefficients of the corresponding Gross vector. We prove that the vectors

$$\big(m_i(D) \bmod 2\big)_{i \in S_p}$$

span $\mathbb{F}_2^{S_p}$. The key step reduces the parity of the representation numbers of Gross's ternary lattices to representation by rank-two sublattices perpendicular to Frobenius. Using Ibukiyama's explicit maximal orders, these binary forms are identified with those occurring in the Xiao–Zhou–Deng–Qu parametrization of supersingular elliptic curves over $\mathbb{F}_p$. Class field theory and Chebotarev's theorem then allow the individual supersingular coordinates to be isolated.

As a consequence, if $E/\mathbb{Q}$ has prime conductor p and positive Mordell–Weil rank, then every coefficient of its Brandt eigenvector indexed by S_p is even, proving a conjecture of Kazalicki and Kohen. Thus an odd coefficient at a rational supersingular class is an algebraic certificate of rank 0. Combining this parity theorem with formulas of Mestre and Gross–Kudla, we also prove that the modular degree of every positive-rank elliptic curve of prime conductor and root number $+1$ is divisible by 4. Consequently, Watkins' conjecture holds for all such curves of rank 2.

1. Introduction

Let $p > 3$ be a prime, and let S denote the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. The Brandt module $X = \bigoplus_{i \in S} \mathbb{Z} e_i$ carries the usual Hecke operators. Let $E/\mathbb{Q}$ be an elliptic curve of conductor p, and let $f_E = \sum_{n \geq 1} a_n(E) q^n$ be its normalized newform. By the definite Jacquet–Langlands correspondence, f_E determines a one-dimensional simultaneous Hecke eigenspace in $X \otimes \mathbb{C}$ on which, for every prime $\ell \neq p$, the Hecke operator t_ℓ acts by multiplication by $a_\ell(E)$. This eigenspace contains a primitive vector with integer coefficients, unique up to sign, which we write as

$$v_E = \sum_{i \in S} c_i e_i;$$

see, for example, [4, Section 5]. We write

$$S_p = \{i \in S : j(E_i) \in \mathbb{F}_p\}$$

for the supersingular classes fixed by Frobenius. We prove that positive Mordell–Weil rank forces c_i to be even for every $i \in S_p$. Equivalently, a single odd coefficient at a rational supersingular class certifies that $\operatorname{rank} E(\mathbb{Q}) = 0$.

For $i \in S$, let $R_i = \operatorname{End}_{\overline{\mathbb{F}}_p}(E_i)$ and $w_i = \#R_i^\times/2$. By Deuring's correspondence, R_i is a maximal order in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞ [3]. We use the Brandt pairing $\langle e_i, e_j \rangle = w_i \delta_{ij}$. Let $-D$ be a negative fundamental discriminant satisfying $\left(\frac{-D}{p}\right) = -1$.

2020 *Mathematics Subject Classification.* Primary 11G05, 11F67; Secondary 11E16, 11R37, 14H52.

Key words and phrases. supersingular elliptic curves, Brandt modules, Gross vectors, binary quadratic forms, modular degree, Watkins' conjecture.

If $h_i(-D)$ denotes the number of optimal embeddings $\mathcal{O}_{-D} \hookrightarrow R_i$, modulo $R_i^\times$-conjugacy, and $u(-D) = \#\mathcal{O}_{-D}^\times$, Gross [4, Sections 12–13] defines the CM vector

$$b_D = \sum_{i \in S} \frac{h_i(-D)}{u(-D)} e_i.$$

We use the integral coefficients

$$m_i(D) = \langle e_i, b_D \rangle = \frac{w_i h_i(-D)}{u(-D)}.$$

Definition. A negative fundamental discriminant $-D$ is *admissible* for p if $\left(\frac{-D}{p}\right) = -1$, equivalently if p is inert in $\mathbb{Q}(\sqrt{-D})$. For such $-D$, the *Gross parity row* is

$$\mathbf{c}(D) = \big(m_i(D) \bmod 2\big)_{i \in S_p} \in \mathbb{F}_2^{S_p},$$

and the *Gross-row space* is

$$\mathcal{R}_p = \operatorname{span}_{\mathbb{F}_2}\{\mathbf{c}(D) : -D \text{ admissible}\}.$$

Our main result is the following.

Theorem 1.1 (Gross-row spanning)**.** *For every prime $p > 3$,*

$$\mathcal{R}_p = \mathbb{F}_2^{S_p}.$$

Suppose now that $E(\mathbb{Q})$ has positive rank. By Kolyvagin–Logachev [12, Theorem 0.3], $L(E,1) = 0$, and Gross's central-value formula [4, Proposition 13.5] gives $\langle v_E, b_D \rangle = 0$ for every admissible $-D$; see Proposition 2.3. If $\bar{i}$ denotes the Frobenius conjugate of i, then $m_{\bar{i}}(D) = m_i(D)$, while Lemma 2.1 gives $c_{\bar{i}} = \varepsilon(E) c_i$, where $\varepsilon(E)$ is the root number. In particular, $c_{\bar{i}} \equiv c_i \pmod 2$. The contributions of the nonrational supersingular classes therefore cancel in Frobenius pairs modulo 2, giving

$$\sum_{i \in S_p} c_i m_i(D) \equiv 0 \pmod 2$$

for every admissible $-D$. Hence $(c_i \bmod 2)_{i \in S_p} \in \mathcal{R}_p^\perp$, and Theorem 1.1 gives the following.

Corollary 1.2 (Kazalicki–Kohen parity)**.** *If $E/\mathbb{Q}$ has prime conductor $p > 3$ and positive Mordell–Weil rank, then*

$$c_i \equiv 0 \pmod 2 \qquad (i \in S_p).$$

Consequently, an odd coefficient c_i for some $i \in S_p$ forces $\operatorname{rank} E(\mathbb{Q}) = 0$. This is a one-sided criterion: the converse is false. For example, the rank-zero curve

$$E: \quad y^2 + y = x^3 + x^2 - 1873x - 31833$$

of conductor 37 has positive discriminant and no rational point of order 2, so [9, Theorem 1.4] shows that $c_i \equiv 0 \pmod 2$ for every $i \in S_{37}$.

This parity question arose from the study of divisor polynomials. Ono observed a connection between their zeros modulo p and supersingular j-invariants [14, p. 118]. Kazalicki and Kohen made this connection precise for elliptic curves of prime conductor by relating the supersingular zeros of the divisor polynomial to the coefficients of the corresponding Brandt eigenvector [9]. When the root number is -1, they proved that $c_i = 0$ for every $i \in S_p$. For root number $+1$, they conjectured that positive rank forces $c_i \equiv 0 \pmod 2$ for every $i \in S_p$, and proved this when the minimal discriminant is positive and E has no rational point of order 2. Corollary 1.2 removes both restrictions.

The connection with Watkins' conjecture was developed in [10, 11]. Watkins conjectured that, for an elliptic curve $E/\mathbb{Q}$,

$$2^{\operatorname{rank} E(\mathbb{Q})} \mid m_E,$$

where m_E denotes the modular degree [15, Conjecture 4.1]. Kazalicki and Kohen showed how parity on S_p, together with Mestre's norm formula [13, Section 3, formula (5), Theorem 3.2] and the Gross–Kudla cubic identity [5, Corollary 11.5], yields divisibility by 4 of the modular degree. Using their previously established parity theorem, this proved Watkins' conjecture for rank-two elliptic curves of prime conductor and positive discriminant. Corollary 1.2 removes the discriminant restriction and gives, for every positive-rank prime-conductor curve with root number $+1$, the divisibility statement proved below in Theorem 6.1.

Corollary 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor $p > 3$, positive Mordell–Weil rank, and root number $+1$. Then*

$$4 \mid m_E.$$

In particular, Watkins' conjecture holds for such curves of rank 2.

We briefly describe the proof of Theorem 1.1. Gross's coefficient $m_i(D)$ is half the number of norm-D vectors in the ternary Gross lattice

$$L_i = \{x \in \mathbb{Z} + 2R_i : \operatorname{tr}(x) = 0\}.$$

For $i \in S_p$, choose an $\mathbb{F}_p$-model of E_i with Frobenius π_i and consider the rank-two lattice

$$L_i^{\perp} = L_i \cap (\mathbb{Q}\pi_i)^{\perp}.$$

Conjugation by π_i, together with negation, groups the norm-D vectors outside $L_i^{\perp}$ into four-element orbits. It follows that, modulo 2, $m_i(D)$ is determined by representation by $L_i^{\perp}$. Thus Frobenius reduces the parity problem from a ternary to a binary quadratic form.

To identify these binary forms, we use Ibukiyama's explicit maximal-order models in $B_{p,\infty}$, keeping track of the quadratic order generated by Frobenius. The resulting marked-order identification sends π_i to the distinguished quadratic generator in the corresponding model, and hence identifies $L_i^{\perp}$ with its perpendicular lattice. A direct norm calculation then gives either a primitive positive-definite binary quadratic form of discriminant $-16p$, or four times a primitive form of discriminant $-p$. We refer to these as the discriminant $-16p$ and discriminant $-p$ branches.

For each nonexceptional i, let C_i denote the proper class of the primitive form obtained in this way. Thus the natural orientation-free object attached to i is the inverse orbit

$$\{C_i, C_i^{-1}\},$$

that is, the orbit of C_i under the involution $C \mapsto C^{-1}$. Comparing the formulas with the parametrization of Xiao–Zhou–Deng–Qu [16, Theorems 3.3, 3.5 and 3.7] shows that, within either branch, distinct geometric supersingular classes determine distinct inverse orbits:

$$i \neq j \qquad \Longrightarrow \qquad \{C_i, C_i^{-1}\} \neq \{C_j, C_j^{-1}\}.$$

In the discriminant $-16p$ branch, the classes C_i also lie in the nonprincipal genus.

The spanning theorem is then proved by applying Chebotarev's theorem in the corresponding ring class fields. The exceptional coordinates $j = 0$ and $j = 1728$, when supersingular, are handled separately by explicit Gross rows. For a nonexceptional coordinate i in the discriminant $-16p$ branch, we choose a rational prime ℓ that splits in the relevant quadratic order so that the two ideals above ℓ represent the classes C_i and C_i^{-1}. Since these are the only ideals of norm ℓ, the inverse orbit attached to i has odd representation parity, while every other nonexceptional inverse orbit has even parity. The genus conditions ensure that $-\ell$ is admissible, and the relation between Gross coefficients and binary representation numbers then shows that, modulo the exceptional

coordinates, the corresponding Gross row isolates i. Thus all coordinates in the discriminant $-16p$ branch lie in $\mathcal{R}_p$.

When $p \equiv 3 \pmod 4$, we next treat the discriminant $-p$ branch. For a coordinate i in this branch, Chebotarev is used with an additional congruence condition to choose a prime $q \equiv 1 \pmod 4$ whose two ideals above q represent C_i and C_i^{-1}. The discriminant $-4q$ is then admissible, and the corresponding Gross row isolates i on the discriminant $-p$ branch. It may also have support on the discriminant $-16p$ branch, but those coordinates have already been shown to lie in $\mathcal{R}_p$. Hence $e_i \in \mathcal{R}_p$ for every remaining coordinate, proving

$$\mathcal{R}_p = \mathbb{F}_2^{S_p}.$$

Products of two suitably chosen split primes give an additional support phenomenon: in the discriminant $-16p$ branch, a Gross row associated with such a product can realize any prescribed pair of nonexceptional coordinates. We record this after the proof of Theorem 1.1.

Section 2 fixes the Gross normalization and reduces the elliptic-curve parity statement to Theorem 1.1. Section 3 relates Gross coefficients modulo 2 to binary quadratic forms using Frobenius and identifies the resulting form classes. Section 4 develops the class-field-theoretic tools used to control their representation parities, and Section 5 proves the spanning theorem and records the additional support relations arising from products of two primes. Finally, Section 6 gives the modular-degree application, and Section 7 illustrates the argument for $p = 83$.

2. Gross relations and the mod-2 reduction

We retain the notation of the introduction. Most of the ingredients in this section are standard, and we record them in the precise normalization needed below, where factors of 2 are essential. The Frobenius symmetry of Brandt eigenvectors is recalled from [9, Propositions 18–19], the interpretation of Gross coefficients as ternary representation numbers comes from [4, Section 12, in particular Proposition 12.9], and the exact orthogonality relation follows from Gross's central-value formula. We then extract two elementary consequences needed for the proof: modulo 2 the Gross relations may be restricted to the Frobenius-fixed supersingular classes, and the exceptional coordinates $j = 0, 1728$ are supplied directly by the discriminants -3 and -4.

2.1. Frobenius on Brandt eigenvectors.

Write $\bar{i}$ for the Frobenius conjugate of $i \in S$.

Lemma 2.1 (Frobenius sign)**.** *Let $f \in S_2(\Gamma_0(p))$ be a newform with root number $\varepsilon(f)$, and write its Brandt eigenvector as $v_f = \sum_i c_i e_i$. Then*

$$c_{\bar{i}} = \varepsilon(f) c_i$$

for every i. In particular, $c_{\bar{i}} \equiv c_i \pmod 2$; if $\varepsilon(f) = +1$, then $c_{\bar{i}} = c_i$.

Proof. The degree-p Brandt operator sends e_i to $e_{\bar{i}}$. Under Jacquet–Langlands it corresponds to $-W_p$. Since the W_p-eigenvalue of a weight-two newform of prime level is $-\varepsilon(f)$, we have $t_p v_f = \varepsilon(f) v_f$. Comparing coefficients gives the result. This is the normalization used in [9, Propositions 18–19]. □

2.2. Gross coefficients as representation numbers.

For an admissible discriminant $-D$, let b_D and $m_i(D)$ be as in the introduction. We use throughout the full-unit convention $u(-D) = \#\mathcal{O}_{-D}^\times$. Define Gross's trace-zero lattice

$$L_i = \{x \in \mathbb{Z} + 2R_i : \mathrm{tr}(x) = 0\},$$

and let $N_i(D)$ be the number of vectors $x \in L_i$ with $\mathrm{Nr}(x) = D$.

Lemma 2.2 (Vector–embedding normalization)**.** *For every negative fundamental discriminant $-D$,*

$$N_i(D) = 2m_i(D).$$

In particular, $m_i(D) \in \mathbb{Z}$.

Proof. This is Gross's description of the coefficients of the ternary theta series associated with $\mathbb{Z} + 2R_i$; see [4, (12.7)–(12.8) and Proposition 12.9]. Indeed, Gross writes

$$\frac{1}{2}\sum_{x\in L_i} q^{\mathrm{Nr}(x)} = \frac{1}{2} + \sum_{D>0} a_i(D)q^D,$$

so that $a_i(D) = N_i(D)/2$. For $-D$ fundamental, Proposition 12.9 gives

$$a_i(D) = \frac{w_i}{2}\frac{h_i(-D)}{u_{\mathrm{Gross}}(-D)}.$$

Gross uses $u_{\mathrm{Gross}}(-D) = \#\mathcal{O}^\times_{-D}/2$, whereas our convention is $u(-D) = \#\mathcal{O}^\times_{-D}$. Hence

$$a_i(D) = \frac{w_i h_i(-D)}{u(-D)} = m_i(D),$$

which proves the assertion. □

2.3. **Gross orthogonality and the rational relation.**

Proposition 2.3 (Gross orthogonality)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor $p > 3$ and positive Mordell–Weil rank, and let v_E be its primitive integral Brandt eigenvector. Then, for every admissible $-D$,*

$$\langle v_E, b_D\rangle = 0.$$

Proof. Under the present fundamental-discriminant and inertness hypotheses, Gross's central-value formula gives

$$L(E,1)L(E\otimes\varepsilon_{-D},1) = C(E,D)\frac{\langle v_E, b_D\rangle^2}{\langle v_E, v_E\rangle}, \qquad C(E,D)\neq 0;$$

see [4, Proposition 13.5] and [9, Proposition 24]. By Kolyvagin–Logachev, $L(E,1)\neq 0$ implies that $E(\mathbb{Q})$ is finite [12, Theorem 0.3]. Thus positive Mordell–Weil rank implies $L(E,1) = 0$, and the formula forces $\langle v_E, b_D\rangle = 0$. □

Frobenius transports optimal embeddings in R_i bijectively to optimal embeddings in $R_{\bar{i}}$, and therefore

$$m_{\bar{i}}(D) = m_i(D).$$

Combining this symmetry with Lemma 2.1 turns the exact Gross relation into a relation supported only on S_p modulo 2.

Corollary 2.4 (Rational Gross relation)**.** *Under the hypotheses of Proposition 2.3,*

$$\sum_{i\in S_p} c_i m_i(D) \equiv 0 \pmod 2$$

for every admissible $-D$.

Proof. Expanding the exact pairing gives $0 = \sum_i c_i m_i(D)$. If $i \notin S_p$, then $i \neq \bar{i}$ and the pair $\{i,\bar{i}\}$ contributes

$$c_i m_i(D) + c_{\bar{i}} m_{\bar{i}}(D) \equiv 0 \pmod 2$$

by Lemma 2.1. Only the Frobenius-fixed classes remain. □

Two rational supersingular coordinates can be produced without class-field theory and will serve as exceptional coordinates in the prime and semiprime constructions.

Lemma 2.5 (Exceptional rows)**.** *If $j = 0$ is supersingular, then -3 is admissible and*

$$\mathbf{c}(3) = e_0.$$

If $j = 1728$ is supersingular, then -4 is admissible and

$$\mathbf{c}(4) = e_{1728}.$$

For a positive-rank prime-conductor elliptic curve, the corresponding exact Gross relations give $c_0 = 0$ and $c_{1728} = 0$ whenever these classes occur.

Proof. The class $j = 0$ is supersingular exactly when $p \equiv 2 \pmod 3$, and an embedding of $\mathcal{O}_{-3}$ into $R_i = \mathrm{End}(E_i)$ forces E_i to have an automorphism of order 3, hence $j(E_i) = 0$. There are two such oriented embeddings modulo $R_0^\times$-conjugacy, so

$$m_0(3) = \frac{3 \cdot 2}{6} = 1.$$

Thus $\mathbf{c}(3) = e_0$. Similarly, $j = 1728$ is supersingular exactly when $p \equiv 3 \pmod 4$; an embedding of $\mathcal{O}_{-4}$ occurs only at $j = 1728$, and the two oriented embeddings give

$$m_{1728}(4) = \frac{2 \cdot 2}{4} = 1.$$

Hence $\mathbf{c}(4) = e_{1728}$. The final assertions follow from Proposition 2.3. □

Corollary 2.4 says that $(c_i \bmod 2)_{i \in S_p}$ lies in $\mathcal{R}_p^\perp$. Hence Theorem 1.1 immediately implies Corollary 1.2. From this point on, the elliptic curve E no longer enters the proof: the remaining task is the purely quaternionic statement that the vectors $\mathbf{c}(D)$ span $\mathbb{F}_2^{S_p}$.

3. Frobenius reduction and binary quadratic forms

Section 2 reduced the elliptic-curve application to the parity of the integers $m_i(D)$. We now show that, at a rational supersingular class, this parity is controlled by a binary rather than a ternary quadratic form. We then show that distinct supersingular coordinates give distinct inverse orbits and record the genus-theoretic condition that will ensure admissibility of the discriminants used later.

3.1. **The Frobenius-perpendicular lattice.** Fix $i \in S_p$ and choose an $\mathbb{F}_p$-model of E_i. Its Frobenius $\pi_i \in R_i$ satisfies

$$\mathrm{tr}(\pi_i) = 0, \qquad \pi_i^2 = -p, \qquad \mathrm{Nr}(\pi_i) = p.$$

Orthogonality in the trace-zero quaternion space will always refer to the symmetric bilinear form obtained by polarizing the reduced norm:

$$(x, y) = \frac{1}{2}\big(\mathrm{Nr}(x + y) - \mathrm{Nr}(x) - \mathrm{Nr}(y)\big) = -\frac{1}{2}\,\mathrm{tr}(xy).$$

Definition. The *Frobenius-perpendicular lattice* attached to i is

$$L_i^\perp = L_i \cap (\mathbb{Q}\pi_i)^\perp.$$

For $D > 0$, write

$$N_i^\perp(D) = \#\{x \in L_i^\perp : \mathrm{Nr}(x) = D\}.$$

For $j(E_i) \neq 0, 1728$, the two $\mathbb{F}_p$-models in the geometric class i are quadratic twists. After identifying them over $\overline{\mathbb{F}}_p$, their Frobenius endomorphisms differ by sign. Hence the line $\mathbb{Q}\pi_i$, and therefore $L_i^\perp$, depends only on the nonexceptional geometric supersingular class i. For $j(E_i) \in \{0, 1728\}$, we retain the chosen $\mathbb{F}_p$-model; these coordinates are handled separately by Lemma 2.5.

Kaneko's calculations with Ibukiyama's explicit maximal orders implicitly produce the same binary norm forms, while He–Korpal–Tran–Vincent explicitly construct the corresponding rank-two sublattices of the Gross lattice; here we identify these sublattices intrinsically as the Frobenius-perpendicular lattices $L_i^\perp$ [8, 7, 6].

Here the key point is the following parity reduction.

Proposition 3.1 (Frobenius parity reduction)**.** *If $p \nmid D$, then*

$$m_i(D) \equiv \frac{N_i^\perp(D)}{2} \pmod 2.$$

Proof. Conjugation by Frobenius,

$$\Theta_i(x) = \pi_i x \pi_i^{-1},$$

is the Galois action on geometric endomorphisms. It preserves R_i, hence also L_i and the reduced norm. On the trace-zero quaternion space, its $+1$-eigenspace is the line $\mathbb{Q}\pi_i$ and its -1-eigenspace is $(\mathbb{Q}\pi_i)^\perp$; in particular, $\Theta_i(x) = -x$ is equivalent to $x \in (\mathbb{Q}\pi_i)^\perp$.

A norm-D vector cannot lie on the Frobenius line: if $x = t\pi_i$ with $t \in \mathbb{Q}$, then $D = pt^2$, so $v_p(D) = 1 + 2v_p(t)$ is odd, contradicting $p \nmid D$. If $x \notin L_i^\perp$, then x lies in neither eigenspace, and

$$x, \quad -x, \quad \Theta_i(x), \quad -\Theta_i(x)$$

are four distinct norm-D vectors in L_i. Hence

$$N_i(D) \equiv N_i^\perp(D) \pmod 4.$$

The involution $x \mapsto -x$ acts without fixed points on the norm-D vectors in $L_i^\perp$, so $N_i^\perp(D)$ is even. Lemma 2.2 gives $N_i(D) = 2m_i(D)$, and dividing the preceding congruence by two proves the result. □

Thus, modulo 2, all norm-D vectors outside the Frobenius anti-invariant plane cancel in four-element orbits. The problem has been reduced to the binary lattice $L_i^\perp$.

Remark 3.2 (Theta-series factorization modulo 4). Proposition 3.1 is an instance of a general mod-4 factorization of theta series. Let L be a positive-definite integral lattice equipped with a norm-preserving involution σ, and put

$$L^+ = \{x \in L : \sigma(x) = x\}, \qquad L^- = \{x \in L : \sigma(x) = -x\}.$$

Writing

$$\theta_M(q) = \sum_{x \in M} q^{\mathrm{Nr}(x)},$$

one has the coefficientwise congruence

$$\theta_L(q) \equiv \theta_{L^+}(q)\theta_{L^-}(q) \pmod 4.$$

Indeed, grouping the vectors outside $L^+ \cup L^-$ into four-element orbits under σ and negation gives

$$\theta_L \equiv \theta_{L^+} + \theta_{L^-} - 1 \pmod 4.$$

Moreover, every nonzero vector of L^+ and L^- occurs together with its negative, so every non-constant coefficient of $\theta_{L^+} - 1$ and $\theta_{L^-} - 1$ is even. Hence

$$(\theta_{L^+} - 1)(\theta_{L^-} - 1) \equiv 0 \pmod 4,$$

and therefore

$$\theta_L \equiv \theta_{L^+}\theta_{L^-} \pmod 4.$$

In the present setting, σ is conjugation by Frobenius,

$$L_i^+ = L_i \cap \mathbb{Q}\pi_i, \qquad L_i^- = L_i^\perp,$$

and hence

$$\theta_{L_i}(q) \equiv \theta_{L_i^+}(q)\theta_{L_i^\perp}(q) \pmod 4.$$

3.2. **Explicit Frobenius-compatible models.** To determine the norm form on $L_i^\perp$, it is not enough to know the abstract maximal order R_i: one must also keep track of the Frobenius line $\mathbb{Q}\pi_i$. The embedded quadratic order

$$\mathfrak{o}_i = R_i \cap \mathbb{Q}(\pi_i) = \mathrm{End}_{\mathbb{F}_p}(E_i)$$

is either $\mathbb{Z}[\pi_i]$ or $\mathbb{Z}[(1+\pi_i)/2]$, and this determines which of Ibukiyama's two explicit models applies.

Ibukiyama's models use an auxiliary prime $q \equiv 3 \pmod 8$ with $\left(\frac{p}{q}\right) = -1$. Write

$$B_{p,\infty} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta, \qquad \alpha^2 = -p, \quad \beta^2 = -q, \quad \alpha\beta = -\beta\alpha.$$

If $r^2 + p \equiv 0 \pmod q$, put

$$O(q,r) = \mathbb{Z} + \mathbb{Z}\frac{1+\beta}{2} + \mathbb{Z}\frac{\alpha(1+\beta)}{2} + \mathbb{Z}\frac{(r+\alpha)\beta}{q}.$$

When $p \equiv 3 \pmod 4$ and $(r')^2 + p \equiv 0 \pmod{4q}$, put

$$O'(q,r') = \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(r'+\alpha)\beta}{2q}.$$

Proposition 3.3 (Ibukiyama models preserving Frobenius)**.** *Assume $p > 5$ and $j(E_i) \neq 0, 1728$. For suitable q and r or r' as above, there is an inner automorphism of $B_{p,\infty}$ sending*

$$(R_i, \pi_i)$$

to

$$(O(q,r), \pm\alpha) \qquad \text{or} \qquad (O'(q,r'), \pm\alpha).$$

The first case occurs when $\mathfrak{o}_i = \mathbb{Z}[\pi_i]$, and the second when $\mathfrak{o}_i = \mathbb{Z}[(1+\pi_i)/2]$.

Proof. By Skolem–Noether we may first identify $\mathbb{Q}(\pi_i)$ with $\mathbb{Q}(\alpha)$ so that π_i is sent to $\pm\alpha$. Under this identification the optimal quadratic order

$$\mathfrak{o}_i = R_i \cap \mathbb{Q}(\pi_i)$$

becomes $\mathbb{Z}[\alpha]$ or $\mathbb{Z}[(1+\alpha)/2]$.

Ibukiyama's Theorems 1–2 give the corresponding standard maximal orders, and the relative classification in [7, Section 4, Propositions 4.1–4.2] allows the isomorphism to be chosen preserving the specified optimal quadratic order. Hence the distinguished Frobenius element is carried to $\pm\alpha$. Since every $\mathbb{Q}$-algebra automorphism of $B_{p,\infty}$ is inner, the assertion follows. □

The perpendicular norm forms can now be read off directly.

Proposition 3.4 (Perpendicular norm forms)**.** *Under the isomorphism of Proposition 3.3, the lattice $L_i^\perp$ has the following descriptions.*

(a) *In $O(q,r)$, a basis is*

$$\beta, \qquad \frac{2r\beta + 2\alpha\beta}{q},$$

and the norm form is

$$Q_{q,r}(x,y) = qx^2 + 4rxy + \frac{4(r^2+p)}{q}y^2.$$

It is primitive of discriminant $-16p$.

(b) *In $O'(q,r')$, a basis is*

$$2\beta, \qquad \frac{r'\beta + \alpha\beta}{q},$$

and the norm form is $4Q'_{q,r'}$, where

$$Q'_{q,r'}(x,y) = qx^2 + r'xy + \frac{(r')^2+p}{4q}y^2.$$

The form $Q'_{q,r'}$ is primitive of discriminant $-p$.

Proof. Consider first the order $O(q,r)$. From its displayed basis, a general trace-zero element of $\mathbb{Z} + 2O(q,r)$ can be written as

$$b\beta + c(\alpha + \alpha\beta) + d\,\frac{2r\beta + 2\alpha\beta}{q}, \qquad b,c,d \in \mathbb{Z}.$$

Since orthogonality to α is equivalent to vanishing of the α-component, we must have $c = 0$. Hence

$$L_i^{\perp} = \mathbb{Z}\beta + \mathbb{Z}\frac{2r\beta + 2\alpha\beta}{q}.$$

For $O'(q,r')$, a general trace-zero element of $\mathbb{Z} + 2O'(q,r')$ has the form

$$b\alpha + 2c\beta + d\,\frac{r'\beta + \alpha\beta}{q}, \qquad b,c,d \in \mathbb{Z}.$$

Orthogonality to α forces $b = 0$, and therefore

$$L_i^{\perp} = \mathbb{Z}(2\beta) + \mathbb{Z}\frac{r'\beta + \alpha\beta}{q}.$$

For $u, v \in \mathbb{Q}$, using

$$\alpha^2 = -p, \qquad \beta^2 = -q, \qquad \alpha\beta = -\beta\alpha,$$

one obtains

$$\mathrm{Nr}((u + v\alpha)\beta) = q(u^2 + pv^2).$$

Substitution of the two displayed bases gives respectively

$$Q_{q,r}(x,y) = qx^2 + 4rxy + \frac{4(r^2+p)}{q}\,y^2$$

and

$$4Q'_{q,r'}(x,y) = 4\left(qx^2 + r'xy + \frac{(r')^2+p}{4q}\,y^2\right).$$

Their primitive parts have discriminants

$$(4r)^2 - 4q\frac{4(r^2+p)}{q} = -16p$$

and

$$(r')^2 - 4q\frac{(r')^2+p}{4q} = -p.$$

Finally, since q is odd and $q \nmid r, r'$, the leading and middle coefficients of each form are coprime. Hence both forms are primitive. □

The factor 4 in the second case is important: every norm represented by $L_i^\perp$ in that branch is divisible by 4.

3.3. **Matching form classes with supersingular classes.** The primitive forms obtained in Proposition 3.4 are exactly the forms associated by Xiao–Zhou–Deng–Qu with the corresponding Ibukiyama orders; see [16, Section 3, especially Theorems 3.3 and 3.5]. We record the consequences of their parametrization that will be used below.

For a nonexceptional $i \in S_p$, let C_i denote the proper class of the primitive form obtained from $L_i^\perp$. Reversing the orientation of the binary lattice replaces a form $[a, b, c]$ by $[a, -b, c]$, and hence replaces its proper class by its inverse. Thus the natural orientation-free object attached to i is the inverse orbit

$$\{C_i, C_i^{-1}\}.$$

Proposition 3.5 (Supersingular/form-class matching)**.** *Let $i \in S_p \setminus \{0, 1728\}$. Under the Xiao–Zhou–Deng–Qu parametrization, the two classes*

$$C_i, \qquad C_i^{-1}$$

correspond to the two $\mathbb{F}_p$-isomorphism classes in the quadratic-twist pair with geometric supersingular class i. In particular, within either branch the map

$$i \longmapsto \{C_i, C_i^{-1}\}$$

is injective on the nonexceptional geometric supersingular classes, and $C_i \neq C_i^{-1}$.

The form classes arising from the $O(q, r)$ branch are exactly the nonexceptional classes in the nonprincipal genus of discriminant $-16p$. The $O'(q, r')$ branch occurs only when $p \equiv 3 \pmod 4$ and gives the nonexceptional form classes of discriminant $-p$.

Proof. By Proposition 3.3, the Frobenius-marked pair (R_i, π_i) is identified with the corresponding Ibukiyama model, and Proposition 3.4 shows that the primitive form obtained from $L_i^\perp$ is the form occurring in [16, Theorems 3.3 and 3.5]. Hence their parametrization associates this form to the original geometric supersingular class i.

By [16, Theorem 3.7], replacing a form class by its inverse corresponds to passing to the quadratic twist over $\mathbb{F}_p$. Hence the inverse orbit $\{C_i, C_i^{-1}\}$ corresponds precisely to the two $\mathbb{F}_p$-isomorphism classes with geometric class i, and distinct nonexceptional geometric supersingular classes give distinct inverse orbits. Moreover, [16, Remark 3.6] shows that the only self-inverse classes arising here are the exceptional classes corresponding to $j = 1728$; thus $C_i \neq C_i^{-1}$ for nonexceptional i. The description of the two branches follows from [16, Theorems 3.5 and 3.7]. □

Let $S_p^{(16)}$ denote the nonexceptional geometric supersingular classes arising from the discriminant $-16p$ branch, and let $S_p^{(p)}$ denote those arising from the discriminant $-p$ branch. Thus

$$S_p \setminus \{0, 1728\} = S_p^{(16)} \sqcup S_p^{(p)},$$

where absent exceptional classes are ignored, and $S_p^{(p)} = \varnothing$ unless $p \equiv 3 \pmod 4$.

For a primitive positive-definite binary form $C = [a, b, c]$, write

$$r_C(n) = \#\{(x, y) \in \mathbb{Z}^2 : ax^2 + bxy + cy^2 = n\}.$$

Since

$$r_C(n) = r_{C^{-1}}(n),$$

the representation number depends only on the inverse orbit $\{C, C^{-1}\}$. We may therefore translate the parity formula of Proposition 3.1 directly into the form-class language.

Corollary 3.6 (Representation-parity dictionary)**.** *Let $-D$ be admissible for p, and let $i \in S_p \setminus \{0, 1728\}$ correspond to the inverse orbit $\{C_i, C_i^{-1}\}$.*

(a) *If $i \in S_p^{(16)}$, then*

$$m_i(D) \equiv \frac{r_{C_i}(D)}{2} \pmod 2.$$

(b) *If $i \in S_p^{(p)}$ and $D = 4n$, then*

$$m_i(D) \equiv \frac{r_{C_i}(n)}{2} \pmod 2.$$

(c) *If $i \in S_p^{(p)}$ and D is odd, then*

$$m_i(D) \equiv 0 \pmod 2.$$

Proof. Proposition 3.1 reduces $m_i(D)$ modulo 2 to half the number of norm-D vectors in $L_i^{\perp}$. In the $-16p$ branch, Proposition 3.4 identifies this norm form with a representative of C_i, giving part (a). In the $-p$ branch the perpendicular norm form is $4Q'_{q,r'}$, which gives part (b) and represents no odd integer, proving part (c). □

3.4. **The genus condition and admissibility.** We record the genus-theoretic fact needed later to verify admissibility in the $-16p$ branch.

Lemma 3.7 (Admissibility from the nonprincipal genus)**.** *Let C lie in the nonprincipal genus of discriminant $-16p$. If n is squarefree, coprime to $2p$, and represented by C, then*

$$n \equiv 3 \pmod 4, \qquad \left(\frac{-n}{p}\right) = -1.$$

In particular, $-n$ is admissible for p.

Proof. By genus theory, the nonprincipal genus of discriminant $-16p$ has genus character

$$(-1)^{(n-1)/2} = -1$$

on represented integers prime to $2p$; see [2, Theorem 3.15]. Hence $n \equiv 3 \pmod 4$.

Since n is squarefree, its representation is primitive. By [2, Lemma 2.5], the discriminant $-16p$ is a quadratic residue modulo n, and therefore $\left(\frac{-p}{n}\right) = 1$. Quadratic reciprocity, together with $n \equiv 3 \pmod 4$, gives $\left(\frac{-n}{p}\right) = -1$.

Finally, $-n$ is a fundamental discriminant because n is squarefree and $n \equiv 3 \pmod 4$. □

Corollary 3.6 translates the parity of the Gross coefficients into representation parity by the corresponding binary form classes, while Lemma 3.7 ensures that the squarefree integers represented in the discriminant $-16p$ branch give admissible discriminants. The next section uses the form–ideal correspondence and Chebotarev's theorem to control these representation parities.

4. Form classes, ideals, and Chebotarev

Corollary 3.6 expresses the parity of a Gross coefficient in terms of representation by a binary form class. To control these representations, we pass from form classes to the corresponding ideal classes in quadratic orders, where class field theory and Chebotarev's theorem allow us to choose split primes with prime ideals in specified ideal classes. We collect here the standard facts needed for this purpose.

Let $\Delta < -4$ be a negative discriminant, put $K = \mathbb{Q}(\sqrt{\Delta})$, and let

$$G_\Delta = \mathrm{Pic}(\mathcal{O}_\Delta)$$

be the proper ideal class group of the quadratic order $\mathcal{O}_\Delta$ of discriminant Δ. Proper equivalence classes of primitive positive definite binary quadratic forms of discriminant Δ are identified with G_Δ via the usual form–ideal correspondence. Let H_Δ be the ring class field of $\mathcal{O}_\Delta$. Artin reciprocity gives

$$\mathrm{Gal}(H_\Delta/K) \simeq G_\Delta,$$

and $H_\Delta/\mathbb{Q}$ is generalized dihedral. If σ_C denotes the automorphism corresponding to $C \in G_\Delta$ and c denotes complex conjugation, then

$$c\sigma_C c^{-1} = \sigma_C^{-1}.$$

We also recall that the genera of discriminant Δ are the cosets of G_Δ^2 [2, Theorem 3.15].

Lemma 4.1 (Representations as ideal counts)**.** *Let $C \in G_\Delta$ and $(n, \Delta) = 1$. Then $r_C(n)/2$ is the number of proper integral $\mathcal{O}_\Delta$-ideals of norm n in the ideal class corresponding to C.*

Proof. This is the classical form–ideal correspondence; see [2, Theorem 7.7 and Chapter 9]. The two representations (x, y) and $(-x, -y)$ determine the same ideal, and for $\Delta < -4$ the only proper automorphisms of a primitive positive-definite form are $\pm I$. □

For a prime norm the preceding lemma is especially rigid: if $\ell \nmid \Delta$ splits in K, there are exactly two proper ideals of norm ℓ, and their classes are inverse to one another. Chebotarev therefore allows us to choose ℓ so that these two ideals represent any prescribed inverse orbit.

Lemma 4.2 (A prime in a prescribed inverse orbit)**.** *Let $C \in G_\Delta$ and let Σ be a finite set of rational primes. There are infinitely many primes $\ell \notin \Sigma$, unramified in H_Δ, such that ℓ splits in K and the two prime ideals above ℓ have classes C and C^{-1}. No form class outside $\{C, C^{-1}\}$ represents ℓ. Moreover,*

$$\frac{r_C(\ell)}{2} = \begin{cases} 1, & C \neq C^{-1}, \\ 2, & C = C^{-1}. \end{cases}$$

Proof. Via the Artin isomorphism, let $\sigma_C \in \mathrm{Gal}(H_\Delta/K)$ correspond to C. Its conjugacy class in $\mathrm{Gal}(H_\Delta/\mathbb{Q})$ is $\{\sigma_C, \sigma_C^{-1}\}$. Chebotarev, with the primes in Σ excluded, gives infinitely many rational primes with this Frobenius conjugacy class. Its image in $\mathrm{Gal}(K/\mathbb{Q})$ is trivial, so such a prime ℓ splits in K. After choosing one prime $\mathfrak{l}$ above ℓ, the two primes $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ have classes C and C^{-1}. They are the only ideals of norm ℓ, so the last assertions follow from Lemma 4.1. □

For the discriminant $-p$ branch, which occurs only when $p \equiv 3 \pmod 4$, a refined Chebotarev argument produces a prime $q \equiv 1 \pmod 4$ that splits in $\mathbb{Q}(\sqrt{-p})$ and whose prime ideals above q represent C_i and C_i^{-1}.

Lemma 4.3 (Adding the condition $q \equiv 1 \pmod 4$)**.** *Assume $p \equiv 3 \pmod 4$, put $K = \mathbb{Q}(\sqrt{-p})$, and let H be its Hilbert class field. For every $x \in \mathrm{Pic}(\mathcal{O}_K)$ and every finite set Σ, there are infinitely many primes $q \notin \Sigma$ with $q \equiv 1 \pmod 4$ such that one of the primes of K above q has class x.*

Proof. The extension H/K is unramified at every finite prime. Since $K \neq \mathbb{Q}(i)$ and the fundamental discriminant of K is odd, the nontrivial quadratic extension $K(i)/K$ is ramified above 2. If $H \cap K(i)$ were larger than K, then, because $K(i)/K$ is quadratic, one would have $K(i) \subseteq H$, contradicting the finite-prime unramifiedness of H/K. Hence

$$H \cap K(i) = K, \qquad \mathrm{Gal}(HK(i)/K) \simeq \mathrm{Gal}(H/K) \times \mathrm{Gal}(K(i)/K).$$

Choose an element of this product whose restriction to H corresponds under Artin reciprocity to x and whose restriction to $K(i)$ is trivial. Its conjugacy class over $\mathbb{Q}$ consists of this element and the element with first component x^{-1}. Chebotarev gives infinitely many rational primes outside Σ with this conjugacy class. Their image in $\mathrm{Gal}(K/\mathbb{Q})$ is trivial, so they split in K; their Frobenius on $\mathbb{Q}(i)$ is also trivial, so $q \equiv 1 \pmod 4$. Choosing one of the two primes above q, and conjugating it if necessary, gives ideal class x. □

Products of two split primes give a second, equally simple pattern. Choose prime ideals $\mathfrak{q}_1 \mid q_1$ and $\mathfrak{q}_2 \mid q_2$ with classes x and y. The four choices of a prime above each q_j give all ideals of norm q_1q_2.

Lemma 4.4 (Ideals of semiprime norm)**.** *Let $q_1 \neq q_2$ be rational primes prime to Δ that split in $K = \mathbb{Q}(\sqrt{\Delta})$, and choose proper invertible prime ideals above them with classes $x, y \in G_\Delta$. The four proper invertible ideals of norm q_1q_2 have classes*

$$xy, \qquad xy^{-1}, \qquad x^{-1}y, \qquad x^{-1}y^{-1}.$$

If the inverse orbits of xy and xy^{-1} are distinct and non-self-inverse, each has odd representation parity and every other inverse orbit has even representation parity. If xy is non-self-inverse and xy^{-1} is self-inverse, only the inverse orbit of xy has odd representation parity.

Proof. Write $q_j\mathcal{O}_\Delta = \mathfrak{q}_j\overline{\mathfrak{q}}_j$ with $[\mathfrak{q}_1] = x$ and $[\mathfrak{q}_2] = y$. Since the primes are distinct and prime to Δ, the four proper invertible ideals of norm q_1q_2 are obtained by choosing independently $\mathfrak{q}_j$ or $\overline{\mathfrak{q}}_j$; their classes are the four displayed products. Lemma 4.1 says that $r_C(q_1q_2)/2$ counts how many of these ideals lie in the class C. A non-self-inverse class occurring once therefore contributes odd parity, whereas a self-inverse class occurring twice contributes even parity. □

The genus condition needed for prescribed semiprime support is exactly what allows two inverse orbits to be realized by such a product.

Lemma 4.5 (Two classes in the same genus)**.** *If $A, B \in G_\Delta$ lie in the same genus, there are $x, y \in G_\Delta$ such that*

$$xy = A, \qquad xy^{-1} = B.$$

Moreover, x and y may be realized by chosen prime ideals above two distinct rational primes, avoiding any prescribed finite set.

Proof. Since A and B lie in the same genus, $AB^{-1} \in G_\Delta^2$. Hence

$$AB = (AB^{-1})B^2$$

is also a square. Choose $x \in G_\Delta$ with $x^2 = AB$ and put $y = Ax^{-1}$. Then $xy = A$ and $xy^{-1} = B$. Lemma 4.2, applied twice and with an enlarged avoidance set after the first choice, realizes x and y by prime ideals above distinct rational primes. If necessary, replace a chosen prime ideal by its conjugate to reverse the orientation. □

5. Proof of the spanning theorem: isolating coordinates with primes

We prove Theorem 1.1 by constructing, for each $i \in S_p$, a Gross parity row equal to e_i modulo coordinates already known to lie in $\mathcal{R}_p$. We first treat the discriminant $-16p$ branch using admissible discriminants $-\ell$ with ℓ prime; since ℓ is odd, the discriminant $-p$ branch contributes zero. We then treat the discriminant $-p$ branch using admissible discriminants of the form $-4q$.

Let

$$W_{\mathrm{exc}} = \mathrm{Span}_{\mathbb{F}_2}\{e_i : i \in \{0, 1728\} \cap S_p\}.$$

By Lemma 2.5, $W_{\mathrm{exc}} \subseteq \mathcal{R}_p$. For $p = 5, 7, 11$ one has respectively $S_5 = \{0\}$, $S_7 = \{1728\}$, and $S_{11} = \{0, 1728\}$, so all rational supersingular classes are exceptional and there is nothing more to prove. Assume henceforth that $p \geq 13$.

We begin with $S_p^{(16)}$. Fix $i \in S_p^{(16)}$ and choose a representative C_i of its inverse orbit. Proposition 3.5 shows that C_i is not self-inverse. By Lemma 4.2, we may choose a prime ℓ, avoiding the primes dividing $6p$, such that the only form classes of discriminant $-16p$ representing ℓ are C_i and C_i^{-1}. Since these classes lie in the relevant nonprincipal genus, Lemma 3.7 gives $\ell \equiv 3 \pmod 4$ and $\left(\frac{-\ell}{p}\right) = -1$; hence $-\ell$ is admissible.

Corollary 3.6 now shows that the restriction of $\mathbf{c}(\ell)$ to $S_p^{(16)}$ is e_i. Its restriction to $S_p^{(p)}$ is zero because ℓ is odd. Thus

$$\mathbf{c}(\ell) \equiv e_i \pmod{W_{\mathrm{exc}}}.$$

Both $\mathbf{c}(\ell)$ and W_{exc} lie in $\mathcal{R}_p$, so $e_i \in \mathcal{R}_p$. Varying i gives

$$W_{16} := W_{\mathrm{exc}} + \mathrm{span}_{\mathbb{F}_2}\{e_i : i \in S_p^{(16)}\} \subseteq \mathcal{R}_p.$$

It remains to treat $S_p^{(p)}$, which occurs only for $p \equiv 3 \pmod 4$. Fix $i \in S_p^{(p)}$ and choose a representative $C_i \in \mathrm{Pic}(\mathcal{O}_{-p})$ of its inverse orbit. By Proposition 3.5, C_i is not self-inverse. Lemma 4.3 gives a prime $q \equiv 1 \pmod 4$, with $q \nmid 2p$, such that a prime of $\mathbb{Q}(\sqrt{-p})$ above q has class C_i; the conjugate prime has class C_i^{-1}. Since these are the only ideals of norm q, Lemma 4.1 shows that $C_i^{\pm 1}$ is the unique inverse orbit with odd representation parity at q.

The discriminant $-4q$ is fundamental. Moreover q splits in $\mathbb{Q}(\sqrt{-p})$, so $\left(\frac{-p}{q}\right) = 1$. Since $q \equiv 1 \pmod 4$, this gives $\left(\frac{q}{p}\right) = 1$ by quadratic reciprocity; because $p \equiv 3 \pmod 4$, it follows that $\left(\frac{-4q}{p}\right) = -1$. Hence $-4q$ is admissible. By Corollary 3.6, the restriction of $\mathbf{c}(4q)$ to $S_p^{(p)}$ is e_i. The row may also have entries on the already treated $-16p$ branch, but all of those coordinates lie in W_{16}. Therefore

$$\mathbf{c}(4q) \equiv e_i \pmod{W_{16}},$$

and $e_i \in \mathcal{R}_p$. Varying i gives every remaining standard basis vector. Consequently

$$\mathcal{R}_p = \mathbb{F}_2^{S_p},$$

which proves Theorem 1.1.

5.1. **Semiprime rows.** Although products of two primes are not needed for the spanning theorem, they reveal additional structure in the family of Gross rows: the same class-group argument gives precise control over pairwise supports. We record this stronger support phenomenon here.

Proposition 5.1 (Semiprime support)**.** *Let $i, j \in S_p^{(16)}$ be distinct. Then there are distinct odd primes q_1, q_2 such that $-q_1q_2$ is admissible and*

$$\mathbf{c}(q_1q_2) \equiv e_i + e_j \pmod{W_{\mathrm{exc}}}.$$

Thus every pair of nonexceptional coordinates in the discriminant $-16p$ branch occurs as the support, modulo the exceptional coordinates, of a single admissible semiprime Gross row.

Proof. Choose representatives C_i, C_j of the inverse orbits attached to i and j. Since they lie in the same nonprincipal genus of discriminant $-16p$, Lemma 4.5 gives classes x, y and distinct split primes q_1, q_2, coprime to $2p$, such that

$$xy = C_i, \qquad xy^{-1} = C_j,$$

and chosen prime ideals above q_1, q_2 have classes x, y. If $n = q_1 q_2$, the four ideals of norm n have classes

$$C_i, \qquad C_j, \qquad C_j^{-1}, \qquad C_i^{-1}.$$

The two inverse orbits are distinct and non-self-inverse, so Lemma 4.4 and Corollary 3.6 give

$$\mathbf{c}(n) \equiv e_i + e_j \pmod{W_{\mathrm{exc}}}.$$

Moreover, n is represented by the nonprincipal genus, and Lemma 3.7 shows that $-n$ is admissible. Since n is odd, the discriminant $-p$ branch contributes nothing. □

6. Application to Watkins' conjecture

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let m_E denote its modular degree, namely the minimal degree of a modular parametrization

$$X_0(N) \longrightarrow E.$$

Watkins conjectured that

$$2^{\operatorname{rank} E(\mathbb{Q})} \mid m_E$$

[15, Conjecture 4.1].

The following argument is the prime-conductor argument of [10, Theorem 1.3], with Corollary 1.2 supplying the required parity of the Brandt coefficients. We state explicitly the root-number $+1$ hypothesis used in that argument.

Theorem 6.1. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor $p > 3$, positive Mordell–Weil rank, and root number $+1$. Then*

$$4 \mid m_E.$$

In particular, Watkins' conjecture holds for such curves of rank 2.

Proof. Let E_0 be the $\Gamma_0(p)$-optimal curve in the isogeny class of E. The curves E and E_0 have the same Brandt eigenvector, rank, and root number. By Corollary 1.2, its coefficients corresponding to the classes in S_p are even. Since the root number is $+1$, the proof of [10, Theorem 1.3] applies to E_0 and gives

$$4 \mid m_{E_0}.$$

It remains to pass from the optimal curve to the given curve E. Choose a modular parametrization $\psi : X_0(p) \to E$ of degree m_E. After translating ψ so that $\psi(\infty) = 0$, it factors through the optimal curve E_0; see [1, Remark 1.3]. Thus

$$\psi = \varphi \circ \pi_0$$

for the optimal parametrization $\pi_0 : X_0(p) \to E_0$ and a $\mathbb{Q}$-isogeny $\varphi : E_0 \to E$. Hence

$$\deg(\psi) = m_{E_0} \deg(\varphi),$$

so $m_{E_0} \mid m_E$, and therefore $4 \mid m_E$. □

7. The case $p = 83$

The prime 83 gives a small example in which both binary-form branches occur and the constructions used in the proof of Theorem 1.1 can be seen explicitly. The rational supersingular geometric classes are

$$S_{83} = \{0, 17, 28, 50, 67, 68\}, \qquad 68 \equiv 1728 \pmod{83}.$$

The corresponding $\mathbb{F}_{83}$-isomorphism classes occur in quadratic-twist pairs as in [16, Example 3.8]. Convenient reduced representatives of the relevant inverse orbits are

discriminant	j	form
-83	68	$[1,1,21]$
	50	$[3,1,7]$
-1328	68	$[4,0,83]$
	17	$[11,-6,31]$
	28	$[7,4,48]$
	67	$[16,-12,23]$
	0	$[3,-2,111]$

where inverse representatives are suppressed. Thus

$$S_{83}^{(16)} = \{17, 28, 67\}, \qquad S_{83}^{(p)} = \{50\},$$

while 0 and 68 are the exceptional coordinates supplied by $D = 3$ and $D = 4$.

The first stage of the spanning argument is already visible at $D = 7$. Among the nonexceptional classes of discriminant -1328, only $[7, 4, 48]$ has odd half-representation number at 7; indeed,

$$[7, 4, 48](\pm 1, 0) = 7.$$

Hence

$$\mathbf{c}(7) \equiv e_{28} \pmod{W_{\mathrm{exc}}}.$$

The second branch can be seen with

$$D = 68 = 4 \cdot 17.$$

At norm 68 in the discriminant--1328 branch, only the class $[7, 4, 48]$ has odd half-representation number, while at norm 17 in the discriminant--83 branch only $[3, 1, 7]$ does. For example,

$$[7, 4, 48](2, -1) = 68, \qquad [3, 1, 7](2, -1) = 17.$$

Thus the nonexceptional support of $\mathbf{c}(68)$ is

$$\{28, 50\}.$$

Since the coordinate e_{28} has already been generated, this row gives e_{50} modulo the previously generated subspace. This illustrates the two-stage structure of the proof of Theorem 1.1.

The additional semiprime relation recorded after the spanning theorem is also visible with small examples. Representation-parity computations give

D	factorization	nonexceptional support on $S_{83}^{(16)}$
51	$3 \cdot 17$	$\{28, 67\}$
123	$3 \cdot 41$	$\{17, 28\}$
259	$7 \cdot 37$	$\{17, 67\}$

For instance,

$$[7, 4, 48](1, -1) = [16, -12, 23](1, -1) = 51,$$

$$[11, -6, 31](1, 2) = [7, 4, 48](3, 1) = 123,$$

and

$$[11, -6, 31](3, -2) = [16, -12, 23](1, -3) = 259.$$

No other nonexceptional inverse orbit of discriminant -1328 has odd half-representation number at the corresponding value. Hence the restrictions of these three admissible semiprime rows to $S_{83}^{(16)}$ are, respectively,

$$e_{28} + e_{67}, \qquad e_{17} + e_{28}, \qquad e_{17} + e_{67}.$$

Thus, in this example, every pair of nonexceptional coordinates in the discriminant $-16p$ branch is realized by a single semiprime Gross row, as predicted by Proposition 5.1.

Acknowledgments

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026 institutional grants of the University of Zagreb Faculty of Science (IK IA 1.1.3 Impact4Math, PMF-CROFUND). M.K. was also supported by the Croatian Science Foundation under the project IP-2022-10-5008 (TEBAG) and by the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", Grant No. PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027.

During the development of this work, the authors used Aleph, a mathematical research assistant developed by Cantab Pi, and ChatGPT (OpenAI) for literature searches, exploratory work on proof strategies, and assistance with drafting and editorial review. The authors independently checked all mathematical statements, proofs, computations, and citations and take full responsibility for the contents of the paper.

References

[1] F. Calegari and M. Emerton, Elliptic curves of odd modular degree, *Israel J. Math.* **169** (2009), 417–444.
[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed., Wiley, Hoboken, NJ, 2013.
[3] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197–272.
[4] B. H. Gross, Heights and the special values of L-series, in *Number Theory (Montreal, 1985)*, CMS Conf. Proc. **7**, Amer. Math. Soc., Providence, RI, 1987, 115–187.
[5] B. H. Gross and S. S. Kudla, Heights and the central critical values of triple product L-functions, *Compos. Math.* **81** (1992), no. 2, 143–209.
[6] C. He, G. Korpal, H. T. N. Tran, and C. Vincent, *Gross lattices of supersingular elliptic curves*, arXiv:2503.03478v3 [math.NT], 2026.
[7] T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings, *Nagoya Math. J.* **88** (1982), 181–195.
[8] M. Kaneko, Supersingular j-invariants as singular moduli mod p, *Osaka J. Math.* **26** (1989), no. 4, 849–855.
[9] M. Kazalicki and D. Kohen, Supersingular zeros of divisor polynomials of elliptic curves of prime conductor, *Res. Math. Sci.* **4** (2017), Paper No. 10, 15 pp.
[10] M. Kazalicki and D. Kohen, On a special case of Watkins' conjecture, *Proc. Amer. Math. Soc.* **146** (2018), no. 2, 541–545.
[11] M. Kazalicki and D. Kohen, Corrigendum to "On a special case of Watkins' conjecture", *Proc. Amer. Math. Soc.* **147** (2019), no. 10, 4563.
[12] V. A. Kolyvagin and D. Yu. Logachev, Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties, *Leningrad Math. J.* **1** (1990), no. 5, 1229–1253.
[13] J.-F. Mestre, La méthode des graphes. Exemples et applications, in *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986)*, Nagoya University, 1986, 217–242.
[14] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-Series*, CBMS Regional Conference Series in Mathematics, vol. 102, American Mathematical Society, Providence, RI, 2004.
[15] M. Watkins, Computing the modular degree of an elliptic curve, *Experiment. Math.* **11** (2002), no. 4, 487–502.
[16] G. Xiao, Z. Zhou, Y. Deng, and L. Qu, Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$ and binary quadratic forms, *Adv. Math. Commun.* **19** (2025), no. 2, 698–715.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: matija.kazalicki@math.hr

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: slijepce@math.hr