ON A COMPARISON OF CASSELS PAIRINGS OF DIFFERENT ELLIPTIC CURVES

SHENXING ZHANG

Abstract. Let e_1, e_2, e_3 be nonzero integers satisfying $e_1 + e_2 + e_3 = 0$. Let (a, b, c) be a primitive triple of odd integers satisfying $e_1a^2 + e_2b^2 + e_3c^2 = 0$. Denote by $E : y^2 = x(x-e_1)(x+e_2)$ and $\mathcal{E} : y^2 = x(x-e_1a^2)(x+e_2b^2)$. Assume that the 2-Selmer groups of E and $\mathcal{E}$ are minimal. Let n be a positive square-free odd integer, where the prime factors of n are nonzero quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Then under certain conditions, the 2-Selmer group and the Cassels pairing of the quadratic twist $E^{(n)}$ coincide with those of $\mathcal{E}^{(n)}$. As a corollary, $E^{(n)}$ has Mordell-Weil rank zero without order 4 element in its Shafarevich-Tate group, if and only if these holds for $\mathcal{E}^{(n)}$. We also give some applications for the congruent elliptic curve.

1. Introduction

Let

$$E = \mathscr{E}_{e_1,e_2} : y^2 = x(x-e_1)(x+e_2)$$

be an elliptic curve defined over $\mathbb{Q}$ with full 2-torsion, where $e_1, e_2, e_3 = -e_1 - e_2$ are non-zero integers. Let $E^{(n)} = \mathscr{E}_{e_1n,e_2n}$ be a quadratic twist of E, where n is an odd positive square-free integer. We want to compare $E^{(n)}$ for different triples (e_1, e_2, e_3). For this purpose, we will assume that

$$\gcd(e_1, e_2, e_3) = 1 \text{ or } 2$$

for simplicity. By a translation of x, one can show that $E \cong \mathscr{E}_{e_2,e_3} \cong \mathscr{E}_{e_3,e_1}$. This gives a symmetry on (e_1, e_2, e_3). Without loss of generality, we may assume that $v_2(e_3)$ is maximal among $v_2(e_i)$, where v_2 is the normalized 2-adic valuation. Then $v_2(e_1) = v_2(e_2) < v_2(e_3)$.

Denote by $\mathrm{Sel}_2(E/\mathbb{Q})$ the 2-Selmer group of E. Then we have an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

If E has no rational point of order 4, then $E(\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$ since it has full 2-torsion. Therefore, $\mathrm{Sel}_2(E/\mathbb{Q})$ contains $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let (a, b, c) be a primitive triple of odd integers satisfying

$$e_1a^2 + e_2b^2 + e_3c^2 = 0.$$

Denote by $\mathcal{E} = \mathscr{E}_{e_1a^2,e_2b^2}$ and $\mathcal{E}^{(n)} = \mathscr{E}_{e_1na^2,e_2nb^2}$ its quadratic twist. The following theorems generalize the observations in [WZ22], which give a relation between $E^{(n)}$ and $\mathcal{E}^{(n)}$.

Date: April 8, 2022.

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11R11, 11R29.

Key words and phrases. elliptic curves; Selmer groups; 2-descent; Shafarevich-Tate groups; Cassels pairing; Gauss genus theory; class groups; full 2-torsion.

Write $2^{v_2(x)} \parallel x$.

Theorem 1.1 (= Theorem 3.5). *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Assume that*

- *e_1, e_2 are odd and $2 \parallel e_3$.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:

(1) $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(E^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
(2) $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(\mathcal{E}^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

When $\gcd(e_1, e_2, e_3) = 2$, $E^{(n)} = \mathscr{E}^{(2n)}_{e_1/2, e_2/2}$ is an even quadratic twist of an elliptic curve in Theorem 1.1. In which case, we require that some primes are congruent to 1 modulo 4.

Theorem 1.2 (= Theorem 4.6). *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Assume that*

- *$2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$;*
- *both E and $E^{(n)}$ have no rational point of order 4;*
- *if $e_2 > 0$ and $e_3 < 0$, then every prime factor of n is congruent to 1 modulo 4, or every odd prime factor of e_2e_3bc is congruent to 1 modulo 4;*
- *if $e_3 > 0$ and $e_1 < 0$, then every prime factor of n is congruent to 1 modulo 4, or every odd prime factor of e_1e_3ac is congruent to 1 modulo 4;*
- *if $e_1 > 0$ and $e_2 < 0$, then every prime factor of n is congruent to 1 modulo 4.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:

(1) $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(E^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
(2) $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(\mathcal{E}^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

For general triples (e_1, e_2, e_3), we require that the prime factors of n are congruent to 1 modulo 8.

Theorem 1.3 (= Theorem 2.7). *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *every prime factor of n is congruent to 1 modulo 8.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:

(1) $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(E^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
(2) $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}\big(\mathcal{E}^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

In each case, we will study the local solvability of homogeneous spaces and show the consistency of 2-Selmer groups. Then we will use Lemmas 2.8 and 2.9 to show the consistency of Cassels pairings. The main difference of these theorems is the local solvability and the Cassels pairing at the place 2. We will also give applications for the congruent elliptic curve, see Theorems 5.2 and 5.3.

The symbols we will use are listed here.

- v_p the normalized p-adic valuation.
- $\gcd(m_1, \dots, m_t)$ the greatest common divisor of integers $m_1, \dots, m_t$.

- $(\alpha,\beta)_v \in \{\pm 1\}$ the Hilbert symbol, $\alpha,\beta \in \mathbb{Q}_v^\times$.
- $[\alpha,\beta]_v \in \mathbb{F}_2$ the additive Hilbert symbol, i.e., $(\alpha,\beta)_v = (-1)^{[\alpha,\beta]_v}$.
- $\left(\frac{\alpha}{\beta}\right) = \prod_{p|\beta}(\alpha,\beta)_p \in \{\pm 1\}$ the Jacobi symbol, where α is coprime with $\beta > 0$.
- $\left[\frac{\alpha}{\beta}\right] = \sum_{p|\beta}[\alpha,\beta]_p \in \mathbb{F}_2$ the additive Jacobi symbol, where α is coprime with $\beta > 0$.
- $m^* = (-1,m)_2 m \equiv 1 \bmod 4$ for nonzero odd integer m.
- $\Lambda = (d_1,d_2,d_3)$ a triple of square-free integers, where $d_1d_2d_3$ is a square.
- D_Λ the homogeneous space associated to E and Λ, see (2.1).
- $\mathrm{Sel}_2'(\mathscr{E})$ the pure 2-Selmer group of $\mathscr{E}$, see (2.2). We will simply write $\Lambda \in \mathrm{Sel}_2'(\mathscr{E})$ the class of $\Lambda \in \mathrm{Sel}_2(\mathscr{E}/\mathbb{Q})$ for convention.
- $\mathbf{0} = (0,\dots,0)^{\mathrm{T}}$ and $\mathbf{1} = (1,\dots,1)^{\mathrm{T}}$.
- $\mathbf{I}$ the identity matrix and $\mathbf{O}$ the zero matrix.
- $\mathbf{A} = \mathbf{A}_n$ a matrix associated to n, see (2.5).
- $\mathbf{D}_u = \mathrm{diag}\left\{\left[\frac{u}{p_1}\right],\dots,\left[\frac{u}{p_k}\right]\right\}$, see (2.6).

2. The general case

2.1. **Classical 2-descent.** As shown in [Cas98], the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$ can be identified with

$$\left\{\Lambda = (d_1,d_2,d_3) \in \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)^3 : D_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset, d_1d_2d_3 \equiv 1 \bmod \mathbb{Q}^{\times 2}\right\},$$

where D_Λ is a genus one curve defined by

$$\begin{cases} H_1: & e_1t^2 + d_2u_2^2 - d_3u_3^2 = 0,\\ H_2: & e_2t^2 + d_3u_3^2 - d_1u_1^2 = 0,\\ H_3: & e_3t^2 + d_1u_1^2 - d_2u_2^2 = 0.\end{cases} \tag{2.1}$$

Under this identification, the points $O, (e_1,0), (-e_2,0), (0,0)$ and other point $(x,y) \in E(\mathbb{Q})$ correspond to

$$(1,1,1),\ (-e_3,-e_1e_3,e_1),\ (-e_2e_3,e_3,-e_2),\ (e_2,-e_1,-e_1e_2)$$

and $(x+e_2, x-e_1, x)$ respectively.

Denote by

$$\mathrm{Sel}_2'(E) := \frac{\mathrm{Sel}_2(E/\mathbb{Q})}{E(\mathbb{Q})_{\mathrm{tors}}/2E(\mathbb{Q})_{\mathrm{tors}}} \tag{2.2}$$

the pure 2-Selmer group of E defined over $\mathbb{Q}$.

Lemma 2.1 ([Ono96]). *$E(\mathbb{Q})$ has a point of order 4 if and only if one of the three pairs $(-e_1,e_2),(-e_2,e_3)$ and $(-e_3,e_1)$ consists of squares of integers.*

If E has no rational point of order 4, then $\mathrm{Sel}_2(E/\mathbb{Q})$ contains $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and therefore $\mathrm{Sel}_2'(E) = \mathrm{Sel}_2(E/\mathbb{Q})/E(\mathbb{Q})[2]$. Cassels in [Cas98] defined a skew-symmetric bilinear pairing $\langle -,- \rangle$ on the $\mathbb{F}_2$-vector space $\mathrm{Sel}_2'(E)$. We will write it additively. For any $\Lambda \in \mathrm{Sel}_2(E)$, choose $P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q})$. Since H_i is locally solvable everywhere, there exists $Q_i \in H_i(\mathbb{Q})$ by Hasse-Minkowski principle. Let L_i be a linear form in three variables such that $L_i = 0$ defines the tangent plane of H_i at Q_i. For any $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2(E)$, define

$$\langle \Lambda, \Lambda' \rangle_E = \sum_v \langle \Lambda, \Lambda' \rangle_{E,v} \in \mathbb{F}_2, \quad \text{where} \quad \langle \Lambda, \Lambda' \rangle_{E,v} = \sum_{i=1}^{3} \big[L_i(P_p), d_i' \big]_v.$$

This pairing is independent of the choice of P and Q_i, and is trivial on $E(\mathbb{Q})[2]$. We will omit the subscript E if there is no confusion.

Lemma 2.2 ([Cas98, Lemma 7.2])**.** *The local Cassels pairing $\langle \Lambda, \Lambda' \rangle_{E,p} = 0$ if*

- *$p \nmid 2\infty$,*
- *the coefficients of H_i and L_i are all integral at p, and*
- *modulo D_Λ and L_i by p, they define a curve of genus 1 over $\mathbb{F}_p$ together with tangents to it.*

Lemma 2.3 ([Wan16, p. 2157])**.** *If E has no rational point of order 4, then the following are equivalent:*

1. *$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ and $Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;*
2. *$\mathrm{Sel}_2'(E)$ has dimension $2t$ and the Cassels pairing on it is non-degenerate.*

2.2. **Homogeneous spaces.** Let's consider the quadratic twist $E^{(n)}$. The homogeneous space $D_\Lambda^{(n)}$ associated to $\Lambda = (d_1, d_2, d_3)$ is

$$\begin{cases} H_1: & e_1 n t^2 + d_2 u_2^2 - d_3 u_3^2 = 0, \\ H_2: & e_2 n t^2 + d_3 u_3^2 - d_1 u_1^2 = 0, \\ H_3: & e_3 n t^2 + d_1 u_1^2 - d_2 u_2^2 = 0. \end{cases}$$

By classical descent theory, if $p \nmid 2e_1e_2e_3n$, then $D_\Lambda^{(n)}(\mathbb{Q}_p)$ is non-empty if and only if $p \nmid d_1d_2d_3$, see [Sil09, Theorem X.1.1, Corollary X.4.4]. Hence we may assume that d_1, d_2, d_3 are square-free divisors of $2e_1e_2e_3n$ from now on.

Lemma 2.4. *Let $\Lambda = (d_1, d_2, d_3)$. Then $D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset$ if and only if*

- *$d_1 > 0$, if $e_2 > 0, e_3 < 0$;*
- *$d_2 > 0$, if $e_3 > 0, e_1 < 0$;*
- *$d_3 > 0$, if $e_1 > 0, e_2 < 0$.*

Proof. The proof is similar to [WZ22, Lemma 3.1(4)], which is easy to get. □

Lemma 2.5. *Let $\Lambda = (d_1, d_2, d_3)$ with square-free d_i. Let n be a positive square-free integer coprime with $e_1e_2e_3$ and p an odd prime factor of n. Then $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset$ if and only if*

- $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1$, *if $p \nmid d_1d_2d_3$;*
- $\left(\frac{-e_2e_3d_1}{p}\right) = \left(\frac{e_3n/d_2}{p}\right) = \left(\frac{-e_2n/d_3}{p}\right) = 1$, *if $p \nmid d_1, p \mid d_2, p \mid d_3$;*
- $\left(\frac{-e_3n/d_1}{p}\right) = \left(\frac{-e_3e_1d_2}{p}\right) = \left(\frac{e_1n/d_3}{p}\right) = 1$, *if $p \mid d_1, p \nmid d_2, p \mid d_3$;*
- $\left(\frac{e_2n/d_1}{p}\right) = \left(\frac{-e_1n/d_2}{p}\right) = \left(\frac{-e_1e_2d_3}{p}\right) = 1$, *if $p \mid d_1, p \mid d_2, p \nmid d_3$.*

Proof. Assume that $p \nmid d_1, p \nmid d_2, p \nmid d_3$. If $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset$, then each $H_i(\mathbb{Q}_p) \neq \emptyset$ and $\left(\frac{d_2d_3}{p}\right) = \left(\frac{d_1d_3}{p}\right) = \left(\frac{d_1d_2}{p}\right) = 1$. That's to say, $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) =$

1. Conversely, if $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1$, then $(0, \sqrt{1/d_1}, \sqrt{1/d_2}, \sqrt{1/d_3}) \in D_\Lambda^{(n)}(\mathbb{Q}_p)$.

Assume that $p \nmid d_1, p \mid d_2, p \mid d_3$. Then $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset$ if and only if $D_{\Lambda'}^{(n)}(\mathbb{Q}_p) \neq \emptyset$, where Hence this case can be reduced to the case $p \nmid d_1d_2d_3$. The rest cases can be obtained by symmetry. □

Let $n = p_1 \cdots p_k$ be a prime decomposition of n. For $\Lambda = (d_1, d_2, d_3)$ with square-free $d_i \mid 2e_1e_2e_3n$, denote by

$$x_i = v_{p_i}(d_1), \quad y_i = v_{p_i}(d_2), \quad z_i = v_{p_i}(d_3). \tag{2.3}$$

Then $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$, where

$$\mathbf{x} = (x_1, \dots, x_k)^{\mathrm{T}}, \quad \mathbf{y} = (y_1, \dots, y_k)^{\mathrm{T}}, \quad \mathbf{z} = (z_1, \dots, z_k)^{\mathrm{T}} \in \mathbb{F}_2^k.$$

Write

$$\begin{aligned} d_1 &= p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \\ d_2 &= p_1^{y_1} \cdots p_k^{y_k} \cdot \widetilde{d}_2, \\ d_3 &= p_1^{z_1} \cdots p_k^{z_k} \cdot \widetilde{d}_3. \end{aligned} \tag{2.4}$$

Then $\widetilde{d}_1\widetilde{d}_2\widetilde{d}_3 \in \mathbb{Q}^{\times 2}$.

Denote by

$$\mathbf{A} = \mathbf{A}_n = \left([p_j, -n]_{p_i}\right)_{i,j} \in M_k(\mathbb{F}_2) \tag{2.5}$$

and

$$\mathbf{D}_u = \mathrm{diag}\left\{\left[\frac{u}{p_1}\right], \cdots, \left[\frac{u}{p_k}\right]\right\} \in M_k(\mathbb{F}_2). \tag{2.6}$$

Theorem 2.6. *Let n be an odd positive square-free integer coprime with $e_1e_2e_3$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *every prime factor of n is congruent to 1 modulo 8.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the map $(d_1, d_2, d_3) \mapsto \begin{pmatrix}\mathbf{x}\\ \mathbf{y}\end{pmatrix}$ induces an isomorphism

$$\mathrm{Sel}_2'(E^{(n)}) \xrightarrow{\sim} \mathrm{Ker}\begin{pmatrix}\mathbf{A} & \\ & \mathbf{A}\end{pmatrix},$$

where $0 < d_i \mid n$.

Proof. Let $\Lambda = (d_1, d_2, d_3)$ with square-free $d_i \mid 2e_1e_2e_3n$ and denote by $\widetilde{\Lambda} = (\widetilde{d}_1, \widetilde{d}_2, \widetilde{d}_3)$. Then $D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset$ if and only if $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{R}) \neq \emptyset$ by Lemma 2.4 and the fact $\mathrm{sgn}(\widetilde{d}_i) = \mathrm{sgn}(d_i)$.

If q is a prime factor of $2e_1e_2e_3$, then $n, d_i/\widetilde{d}_i \in \mathbb{Q}_q^{\times 2}$. Therefore,

$$(t, u_1, u_2, u_3) \in D_\Lambda^{(n)}(\mathbb{Q}_q) \iff \left(t\sqrt{n}, u_1\sqrt{\frac{d_1}{\widetilde{d}_1}}, u_2\sqrt{\frac{d_2}{\widetilde{d}_2}}, u_3\sqrt{\frac{d_3}{\widetilde{d}_3}}\right) \in D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_q).$$

Hence $\Lambda \in \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})$ if and only if $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$ and $D_\Lambda^{(n)}$ is locally solvable at each $p \mid n$.

If $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$, then $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$. By our assumptions,

$$\widetilde{\Lambda} = (1,1,1),\ (-e_3,-e_1e_3,e_1),\ (-e_2e_3,e_3,-e_2) \text{ or } (e_2,-e_1,-e_1e_2)$$

is 2-torsion. If $\widetilde{\Lambda} = (-e_3,-e_1e_3,e_1)$, then

$$\Lambda\cdot(-e_3n,-e_1e_3,e_1n) = \Big(\prod_{i=1}^k p_i^{1-x_i}, \prod_{i=1}^k p_i^{y_i}, \prod_{i=1}^k p_i^{1-z_i}\Big).$$

The other cases are similar. Hence each element in $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has a unique representative (d_1,d_2,d_3) with $0<d_i \mid n$. Based on this, we can express $\mathrm{Sel}_2'\big(E^{(n)}\big)$ in terms of linear algebra by Lemma 2.5 after a translation of languages:

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \xrightarrow{\sim} \mathbf{M}_n, \quad \text{where} \quad \mathbf{M}_n = \begin{pmatrix} \mathbf{A}+\mathbf{D}_{-e_3} & \mathbf{D}_{-e_2e_3} \\ \mathbf{D}_{-e_1e_3} & \mathbf{A}+\mathbf{D}_{e_3}\end{pmatrix}.$$

Since $\left(\frac{p}{q}\right)=1$ for any odd primes $p\mid n, q\mid e_1e_2e_3$ and $\left(\frac{\pm1}{p}\right)=\left(\frac{\pm2}{p}\right)=1$, we have $\left(\frac{\pm e_i}{p}\right)=1$. Therefore, $\mathbf{D}_{\pm e_i}=\mathbf{O}$ and $\mathbf{M}_n=\mathrm{diag}\{\mathbf{A},\mathbf{A}\}$. □

2.3. **The Cassels pairing.** Let (a,b,c) be a primitive triple of odd integers satisfying

$$e_1a^2+e_2b^2+e_3c^2=0.$$

Denote by $\mathcal{E}=\mathscr{E}_{e_1a^2,e_2b^2}$ and $\mathcal{E}^{(n)}=\mathscr{E}_{e_1a^2n,e_2b^2n}$.

Theorem 2.7. *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *every prime factor of n is congruent to 1 modulo 8.*

If $\mathrm{Sel}_2(E/\mathbb{Q})\cong\mathrm{Sel}_2(\mathcal{E}/\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:

(1) $\mathrm{rank}_{\mathbb{Z}}\,E^{(n)}(\mathbb{Q})=0$ *and* $\text{Ш}\big(E^{(n)}/\mathbb{Q}\big)\cong(\mathbb{Z}/2\mathbb{Z})^{2t}$*;*
(2) $\mathrm{rank}_{\mathbb{Z}}\,\mathcal{E}^{(n)}(\mathbb{Q})=0$ *and* $\text{Ш}\big(\mathcal{E}^{(n)}/\mathbb{Q}\big)\cong(\mathbb{Z}/2\mathbb{Z})^{2t}$.

Lemma 2.8. *Assume that all prime factors of n are nonzero quadratic residues modulo each odd prime factor of $e_1e_2e_3$. If $a\equiv b\equiv c\equiv 1 \bmod 4$, then*

$$\frac{1}{8}(a+b)(b+c)(c+a)\equiv 1 \bmod 4$$

is a quadratic residue modulo each prime factor of n.

Proof. Let α,β be coprime integers satisfying

$$\frac{\beta}{\alpha}=\frac{e_1(a-c)}{e_2(b+c)}.$$

Then α is odd and β is even. It's not hard to show that

$$\begin{aligned}\lambda a &= e_1\alpha^2+2e_2\alpha\beta-e_2\beta^2\equiv e_1 \bmod 4,\\ \lambda b &= e_1\alpha^2-2e_1\alpha\beta-e_2\beta^2\equiv e_1 \bmod 4,\\ \lambda c &= e_1\alpha^2+e_2\beta^2\equiv e_1 \bmod 4,\end{aligned}$$

for some $\lambda \equiv e_1 \bmod 4$. Then

$$\begin{aligned}\lambda(a+b) &= 2(\alpha-\beta)(e_1\alpha+e_2\beta),\\ \lambda(b+c) &= 2e_1\alpha(\alpha-\beta),\\ \lambda(c+a) &= 2\alpha(e_1\alpha+e_2\beta)\end{aligned}$$

and

$$\frac{1}{8}(a+b)(b+c)(c+a) = e_1\lambda\big(\lambda^{-2}\alpha(\alpha-\beta)(e_1\alpha+e_2\beta)\big)^2 \equiv 1 \bmod 4.$$

Let q be a prime factor of λ. Then

$$q \mid \gcd\big(\lambda(a+b), \lambda(a+c)\big) = 2(e_1\alpha+e_2\beta).$$

If $q \nmid e_1$, then $q \mid \alpha(\alpha-\beta)$. If $q \mid \alpha$, then $q \mid e_2\beta$, $q \mid e_2$; if $q \mid (\alpha-\beta)$, then $q \mid e_2(\alpha-\beta)+(e_1\alpha+e_2\beta) = -e_3\alpha$, $q \mid e_3$. Hence $q \mid e_1e_2e_3$.

Let p be a prime factor of n. Since $e_1\lambda \equiv 1 \bmod 4$ and $\left(\frac{p}{q}\right) = 1$ for any odd prime $q \mid e_1e_2e_3$, we have

$$\left(\frac{e_1\lambda}{p}\right) = \left(\frac{p}{e_1\lambda}\right) = \prod_{q\mid e_1\lambda}\left(\frac{p}{q}\right)^{v_q(e_1\lambda)} = 1.$$

Hence $(a+b)(b+c)(c+a)/8$ is a quadratic residue modulo p. □

Lemma 2.9. *We have*

$$(ax+by+cz)(x+y+z) - \frac{1}{2}(a+b)(b+c)(c+a)\left(\frac{x}{b+c}+\frac{y}{c+a}+\frac{z}{a+b}\right)^2$$
$$= \frac{1}{2}(e_1a+e_2b+e_3c)\left(\frac{x^2}{e_1}+\frac{y^2}{e_2}+\frac{z^2}{e_3}\right).$$

Proof. The coefficient of x^2 on the left hand side is

$$a - \frac{(a+b)(a+c)}{2(b+c)} = \frac{a(b+c)-bc-a^2}{2(b+c)} = \frac{e_1a(b+c)-e_1bc-e_1a^2}{2e_1(b+c)}$$
$$= \frac{e_1a(b+c)+(e_2+e_3)bc+e_2b^2+e_3c^2}{2e_1(b+c)} = \frac{e_1a+e_2b+e_3c}{2e_1}$$

and the coefficient of yz on the left hand side is zero. The equality then follows by symmetry. □

Proof of Theorem 2.7. Since E has no rational point of order 4, none of $(-e_1, e_2)$, $(-e_2, e_3)$, $(-e_3, e_1)$ consists of squares by Lemma 2.1. Therefore, none of $(-e_1a^2, e_2b^2)$, $(-e_2b^2, e_3c^2)$, $(-e_3c^2, e_1a^2)$ consists of squares and $\mathcal{E}$ has no rational point of order 4. Similarly, $\mathcal{E}^{(n)}$ has no rational point of order 4.

By choosing suitable signs, we may assume that $a \equiv b \equiv c \equiv 1 \bmod 4$. Since the matrix in Theorem 2.6 does not depend on a, b, c, we have a canonical isomorphism

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \cong \mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big).$$

Let $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2'\big(E^{(n)}\big)$ with $0 < d_i, d_i' \mid n$. We will denote by D, H, Q, L, P the corresponding symbols for E and $\mathcal{D}, \mathcal{H}, \mathcal{Q}, \mathcal{L}, \mathcal{P}$ the corresponding symbols for $\mathcal{E}$ in the calculation of Cassels pairing. Then $\mathcal{D}_\Lambda^{(n)}$ is defined as

$$\begin{cases} \mathcal{H}_1: & e_1a^2nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ \mathcal{H}_2: & e_2b^2nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ \mathcal{H}_3: & e_3c^2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

Let $(\alpha_i, \beta_i, \gamma_i)$ be primitive triples of integers satisfying

$$e_1n\alpha_1^2 + d_2\beta_1^2 - d_3\gamma_1^2 = 0,$$
$$e_2n\alpha_2^2 + d_3\beta_2^2 - d_1\gamma_2^2 = 0,$$
$$e_3n\alpha_3^2 + d_1\beta_3^2 - d_2\gamma_3^2 = 0.$$

Choose

$$\begin{aligned} \mathcal{Q}_1 &= (\alpha_1, a\beta_1, a\gamma_1) \in \mathcal{H}_1(\mathbb{Q}), & \mathcal{L}_1 &= e_1an\alpha_1t + d_2\beta_1u_2 - d_3\gamma_1u_3, \\ \mathcal{Q}_2 &= (\alpha_2, b\beta_2, b\gamma_2) \in \mathcal{H}_2(\mathbb{Q}), & \mathcal{L}_2 &= e_2bn\alpha_2t + d_3\beta_2u_3 - d_1\gamma_2u_1, \\ \mathcal{Q}_3 &= (\alpha_3, c\beta_3, c\gamma_3) \in \mathcal{H}_3(\mathbb{Q}), & \mathcal{L}_3 &= e_3cn\alpha_3t + d_1\beta_3u_1 - d_2\gamma_3u_2. \end{aligned}$$

(i) The case $v \mid 2e_1e_2e_3abc$. Since each prime factor of n is a square in $\mathbb{Q}_v$, so is d_i'. Therefore, $[\mathcal{L}_i(\mathcal{P}_v), d_i']_v = 0 = [L_i(P_v), d_i']_v$.

(ii) The case $v = p \mid n$. Since $a \equiv 1 \bmod 4$ and p is a quadratic residue modulo every odd prime factor q of abc, we have

$$[a, p]_p = \left[\frac{a}{p}\right] = \left[\frac{p}{a}\right] = \sum_{q \mid a} v_q(a) \left[\frac{p}{q}\right] = 0.$$

Therefore $[a, d_i']_p = 0$. Similarly, $[b, d_i']_p = [c, d_i']_p = 0$.

(ii-a) The case $p \nmid d_1d_2d_3$. Take $\mathcal{P}_p = (0, 1/\sqrt{d_1}, 1/\sqrt{d_2}, 1/\sqrt{d_3}) = P_p$. Then

$$\mathcal{L}_1(\mathcal{P}_p) = \beta_1\sqrt{d_2} - \gamma_1\sqrt{d_3} = L_1(P_p).$$

Similarly, $\mathcal{L}_2(\mathcal{P}_p) = L_2(P_p)$ and $\mathcal{L}_3(\mathcal{P}_p) = L_3(P_p)$.

(ii-b) The case $p \nmid d_1, p \mid d_2, p \mid d_3$. Then $e_3n/d_2, -e_2n/d_3 \in \mathbb{Q}_p^{\times 2}$ by Lemma 2.5. Take $\mathcal{P}_p = (1, 0, cu, bv)$ where $u^2 = e_3n/d_2, v^2 = -e_2n/d_3$. Then $P_p = (1, 0, u, v)$ and

$$\mathcal{L}_1(\mathcal{P}_p) = ae_1n\alpha_1 - bd_3\gamma_1v + cd_2\beta_1u,$$
$$\mathcal{L}_2(\mathcal{P}_p) = be_2n\alpha_2 + bd_3\beta_2v = bL_2(P_p),$$
$$\mathcal{L}_3(\mathcal{P}_p) = ce_3n\alpha_3 - cd_2\gamma_3u = cL_3(P_p).$$

Since

$$\frac{(e_1n\alpha_1)^2}{e_1} + \frac{(-d_3\gamma_1v)^2}{e_2} + \frac{(d_2\beta_1u)^2}{e_3} = n(e_1n\alpha_1^2 - d_3\gamma_1^2 + d_2\beta_1^2) = 0,$$

we have

$$\mathcal{L}_1(\mathcal{P}_p)L_1(P_p) = \frac{1}{2}(a+b)(a+c)(b+c)\left(\frac{e_1n\alpha_1}{b+c} + \frac{d_2\beta_1u}{a+b} - \frac{d_3\gamma_1v}{a+c}\right)^2$$

by Lemma 2.9. Therefore,

$$\begin{aligned} [\mathcal{L}_1(\mathcal{P}_p), d_1']_p &= [L_1(P_p), d_1']_p + [2(a+b)(a+c)(b+c), d_1']_p = [L_1(P_p), d_1'], \\ [\mathcal{L}_2(\mathcal{P}_p), d_2']_p &= [L_2(P_p), d_2']_p + [b, d_2']_p = [L_2(P_p), d_2']_p, \\ [\mathcal{L}_3(\mathcal{P}_p), d_3']_p &= [L_3(P_p), d_3']_p + [c, d_3']_p = [L_3(P_p), d_3']_p \end{aligned}$$

by Lemma 2.8.

(ii-c) The case $p \mid d_1, p \nmid d_2, p \mid d_3$, and the case $p \mid d_1, p \mid d_2, p \nmid d_3$ can be proved similarly by the symmetry of e_i.

Now we have

$$\begin{aligned}\langle \Lambda, \Lambda' \rangle_{\mathcal{E}^{(n)}} &= \sum_{v \mid 2e_1e_2e_3abcn\infty} \sum_{i=1}^{3} \big[\mathcal{L}_i(\mathcal{P}_v), d_i'\big]_v = \sum_{p \mid n} \sum_{i=1}^{3} \big[\mathcal{L}_i(\mathcal{P}_p), d_i'\big]_p \\ &= \sum_{p \mid n} \sum_{i=1}^{3} \big[L_i(P_p), d_i'\big]_p = \langle \Lambda, \Lambda' \rangle_{E^{(n)}}\end{aligned}$$

by Lemma 2.2. In other words, the Cassels pairings on $\mathrm{Sel}_2'\big(E^{(n)}\big)$ and $\mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big)$ are same under the identity $\mathrm{Sel}_2'\big(E^{(n)}\big) \cong \mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big)$. Since both $E^{(}n)$ and $\mathcal{E}^{(n)}$ have no rational point of order 4, this theorem follows from Lemma 2.3. □

3. The odd case with $2 \parallel e_3$

Assume that e_1, e_2 are odd and $2 \parallel e_3$. Let n be an odd positive square-free integer. Let $\Lambda = (d_1, d_2, d_3)$ where d_1, d_2, d_3 are square-free integers dividing $2e_1e_2e_3n$.

3.1. **Homogeneous spaces.**

Lemma 3.1. *If $D_\Lambda^{(n)}(\mathbb{Q}_2) \neq \emptyset$, then d_3 is odd.*

Proof. The proof is similar to [WZ22, Lemma 3.1(2)]. Since we are dealing with homogeneous spaces, we may assume that t, u_1, u_2, u_3 are 2-adic integers and at least one of them is a 2-adic unit. Suppose that $D_\Lambda^{(n)}(\mathbb{Q}_2) \neq \emptyset$. If $2 \mid d_1, 2 \nmid d_2, 2 \mid d_3$, then u_2 is even by H_3 and t is even H_2. Therefore, u_3 is even by H_1 and u_1 is even by H_2, which is impossible. The case $2 \nmid d_1, 2 \mid d_2, 2 \mid d_3$ is similar. Hence d_3 is odd. □

Since the torsion $(-e_3n, -e_1e_3, e_1n)$ has 2-adic valuation $(1, 1, 0)$, any element in the pure 2-Selmer group $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has a representative $\Lambda = (d_1, d_2, d_3)$ with odd $d_i \mid e_1e_2e_3n$.

Lemma 3.2. *Let $\Lambda = (d_1, d_2, d_3)$ where d_1, d_2, d_3 are odd. If $D_\Lambda^{(n)}$ is locally solvable at all places $v \neq 2$, then $D_\Lambda^{(n)}$ is also locally solvable at $v = 2$.*

Proof. The proof is similar to [WZ22, Lemma 3.4]. Since $D_\Lambda^{(n)}(\mathbb{Q}_v) \neq \emptyset$ for all places $v \neq 2$, each H_i is locally solvable at $v \neq 2$. By the product formula of Hilbert symbols, H_i is also locally solvable at 2. In other words,

$$[e_1nd_3, d_1]_2 = [e_2nd_1, d_2]_2 = [e_3nd_2, d_3]_2 = 0.$$

(i) If $(d_1, d_2, d_3) \equiv (1, 1, 1) \bmod 4$, then $0 = [e_3nd_2, d_3]_2 = [2, d_3]_2$ and we have $d_3 \equiv 1 \bmod 8$. Therefore, $d_1 \equiv d_2 \bmod 8$. If $d_1 \equiv d_2 \equiv 1 \bmod 8$, take

$$t = 0,\ u_1 = \sqrt{d_3/d_1},\ u_2 = \sqrt{d_3/d_2},\ u_3 = 1.$$

If $d_1 \equiv d_2 \equiv 5 \bmod 8$, take

$$t = 2,\ u_1 = \sqrt{(d_3 + 4e_2n)/d_1},\ u_2 = \sqrt{(d_3 - 4e_1n)/d_2},\ u_3 = 1.$$

(ii) If $(d_1, d_2, d_3) \equiv (-1, -1, 1) \bmod 4$, then $d_3 \equiv 1 \bmod 8$ similarly. Since

$$[e_1n, -1]_2 = [e_1nd_3, d_1]_2 = 0 = [e_2nd_1, d_2]_2 = [-e_2n, -1]_2,$$

we have $e_1 n \equiv -e_2 n \equiv 1 \bmod 4$. This implies that $4 \mid (e_1 + e_2) = -e_3$, which is impossible.

(iii) If $d_3 \equiv -1 \bmod 4$, then $[e_3 n d_2, d_3]_2 = 0$, $e_3 n d_2 \equiv d_3 + 3 \bmod 8$ and

$$(d_1 - e_2 n) - (d_2 + e_1 n) = d_1 - d_2 + e_3 n \equiv 2(d_1 + d_2) \equiv 0 \bmod 8.$$

If $(d_1, d_2, d_3) \equiv (1, -1, -1) \bmod 4$, then $[e_2 n, -1]_2 = 0$ and $e_2 n \equiv d_1 \bmod 4$. If $(d_1, d_2, d_3) \equiv (-1, 1, -1) \bmod 4$, then $[-e_1 n, -1]_2 = 0$ and $e_1 n \equiv -d_2 \bmod 4$. If $d_2 + e_1 n \equiv d_1 - e_2 n \equiv 0 \bmod 8$, take

$$t = 1,\ u_1 = \sqrt{e_2 n / d_1},\ u_2 = \sqrt{-e_1 n / d_2},\ u_3 = 0.$$

If $d_2 + e_1 n \equiv d_1 - e_2 n \equiv 4 \bmod 8$, take

$$t = 1,\ u_1 = \sqrt{(4d_3 + e_2 n)/d_1},\ u_2 = \sqrt{(4d_3 - e_1 n)/d_2},\ u_3 = 2.$$

Hence $D_\Lambda^{(n)}$ is locally solvable at $v = 2$. □

Let $\Lambda = (d_1, d_2, d_3)$ with odd square-free $d_i \mid e_1 e_2 e_3 n$. We will use the notations $\mathbf{x}, \mathbf{y}, \mathbf{z}, \widetilde{d_i}$ in (2.3) and (2.4).

Theorem 3.3. *Let n be an odd positive square-free integer coprime with $e_1 e_2 e_3$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1 e_2 e_3$. If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the map $(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$ induces an isomorphism*

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \xrightarrow{\sim} \mathrm{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-e_3} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_3} & \mathbf{A} + \mathbf{D}_{e_3} \end{pmatrix},$$

where $0 < d_i \mid n$.

Proof. Since e_1, e_2 are odd and $2 \parallel e_3$, neither $(-ne_2, ne_3)$ nor $(-ne_3, ne_1)$ consists of squares. If $(-ne_1, ne_2)$ consists of squares, then $e_1 \equiv -e_2 \bmod 4$ and $4 \mid e_3$, which is impossible. Hence $E(\mathbb{Q})$ contains no point of order 4 by Lemma 2.1.

Let $\Lambda = (d_1, d_2, d_3)$ with odd square-free $d_i \mid e_1 e_2 e_3 n$ and denote by $\widetilde{\Lambda} = (\widetilde{d_1}, \widetilde{d_2}, \widetilde{d_3})$. Similar to the proof of Theorem 2.6, $D_\Lambda^{(n)}(\mathbb{Q}_v) \neq \emptyset$ if and only if $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_v) \neq \emptyset$ for $v = \infty$ or odd $v \mid e_1 e_2 e_3$. Hence $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$ if and only if $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$ and $D_\Lambda^{(n)}$ is locally solvable at each $p \mid n$ by Lemmas 3.1 and 3.2.

If $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$, then $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$. By our assumptions, $\widetilde{\Lambda}$ is 2-torsion, which should be $(1,1,1)$ or $(e_2, -e_1, -e_1 e_2)$. If $\widetilde{\Lambda} = (e_2, -e_1, -e_1 e_2)$, then

$$\Lambda \cdot (ne_2, -ne_1, -e_1 e_2) = \Big(\prod_{i=1}^k p_i^{1-x_i}, \prod_{i=1}^k p_i^{1-y_i}, \prod_{i=1}^k p_i^{z_i} \Big).$$

Hence each element in $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has a unique representative (d_1, d_2, d_3) with $0 < d_i \mid n$. Based on this, we can express $\mathrm{Sel}_2'\big(E^{(n)}\big)$ in terms of linear algebra by Lemma 2.5 after a translation of languages. □

Remark 3.4. Since $\left(\frac{p}{q}\right) = 1$ for any odd primes $p \mid n, q \mid e_1 e_2 e_3$, we have $\mathbf{D}_e = \mathbf{D}_u$, where $u \in \{\pm 1, \pm 2\}$ such that $e/u \equiv 1 \bmod 4$ for any square-free $e \mid e_1 e_2 e_3$.

3.2. **The Cassels pairing.** Let (a, b, c) be a primitive triple of integers satisfying

$$e_1a^2 + e_2b^2 + e_3c^2 = 0.$$

Then a, b, c are odd. Denote by $\mathcal{E} = \mathscr{E}_{e_1a^2,e_2b^2}$ and $\mathcal{E}^{(n)} = \mathscr{E}_{e_1a^2n,e_2b^2n}$.

Theorem 3.5. *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:*

(1) *$\mathrm{rank}_{\mathbb{Z}}\, E^{(n)}(\mathbb{Q}) = 0$ and $\text{Ш}\big(E^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;*

(2) *$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ and $\text{Ш}\big(\mathcal{E}^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.*

Proof. As shown in the proof of Theorem 3.3, both $E^{(n)}$ and $\mathcal{E}(\mathbb{Q})^{(n)}$ have no rational point of order 4. Since the matrix in Theorem 3.3 does not depend on a, b, c, we have a canonical isomorphism

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \cong \mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big).$$

By choosing suitable signs, we may assume that $a \equiv b \equiv c \equiv 1 \bmod 4$. Let $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2'\big(E^{(n)}\big)$ with $0 < d_i, d_i' \mid n$. We will use the notations $\mathcal{D}, \mathcal{H}, \mathcal{Q}, \mathcal{L}, \mathcal{P}, D, H, Q, L, P, \alpha_i, \beta_i, \gamma_i$ in the proof of Theorem 2.7.

(i) The case odd $v \mid e_1e_2e_3abcn$. The proof is similar to the proof of Theorem 2.7.

(ii) The case $v = 2$. As shown in Lemma 3.2, the case $(d_1, d_2, d_3) \equiv (-1, -1, 1) \bmod 4$ is impossible.

(ii-a) The case $(d_1, d_2, d_3) \equiv (1, 1, 1) \bmod 4$. As shown in Lemma 3.2, if $d_1 \equiv d_2 \equiv 1 \bmod 8$, take $\mathcal{P}_2 = (0, 1/\sqrt{d_1}, 1/\sqrt{d_2}, 1/\sqrt{d_3}) = P_2$. Then

$$\begin{aligned}
\mathcal{L}_1(\mathcal{P}_2) &= \beta_1\sqrt{d_2} - \gamma_1\sqrt{d_3} = L_1(P_2),\\
\mathcal{L}_2(\mathcal{P}_2) &= \beta_2\sqrt{d_3} - \gamma_2\sqrt{d_1} = L_2(P_2),\\
\mathcal{L}_3(\mathcal{P}_2) &= \beta_3\sqrt{d_1} - \gamma_3\sqrt{d_2} = L_3(P_2).
\end{aligned}$$

If $d_1 \equiv d_2 \equiv 5 \bmod 8$, denote by

$$\begin{aligned}
\mathcal{U} &= \sqrt{(d_3 + 4e_2b^2n)d_1}, & \mathcal{V} &= \sqrt{(d_3 - 4e_1a^2n)d_2},\\
U &= \sqrt{(d_3 + 4e_2n)d_1}, & V &= \sqrt{(d_3 - 4e_1n)d_2}
\end{aligned}$$

with $\mathcal{U} \equiv \mathcal{V} \equiv U \equiv V \equiv 1 \bmod 4$. Since $\mathcal{U}^2 \equiv U^2 \bmod 32$, we have $\mathcal{U} \equiv U \bmod 16$. Similarly, $\mathcal{V} \equiv V \bmod 16$. Take $\mathcal{P}_2 = (2, \mathcal{U}/d_1, \mathcal{V}/d_2, 1)$, then $P_2 = (2, U/d_1, V/d_2, 1)$ and

$$\begin{aligned}
\mathcal{L}_1(\mathcal{P}_2) &\equiv 2e_1an\alpha_1 + \beta_1V - d_3\gamma_1 \equiv L_1(P_2),\\
\mathcal{L}_2(\mathcal{P}_2) &\equiv 2e_2bn\alpha_2 + d_3\beta_2 - \gamma_2U \equiv L_2(P_2),\\
\mathcal{L}_3(\mathcal{P}_2) &\equiv 2e_3cn\alpha_3 + \beta_3U - \gamma_3V \equiv L_3(P_2)
\end{aligned}$$

modulo 8. If α_1 is odd, then exactly one of β_1 and γ_1 is odd. Thus $\mathcal{L}_1(\mathcal{P}_2)$ is odd. If α_1 is even, then both of β_1 and γ_1 are odd. By choosing a suitable sign of γ_1, we may assume that $2 \parallel (\beta_1 - \gamma_1)$. Therefore, $2 \parallel \mathcal{L}_1(\mathcal{P}_2)$. Similarly, we may assume that $2 \parallel \mathcal{L}_2(\mathcal{P}_2)$. Note that β_3, γ_3 are odd. By choosing a suitable sign of γ_3, we may assume that $2 \parallel \mathcal{L}_3(\mathcal{P}_2)$. Since $\mathcal{L}_i(\mathcal{P}_2) \equiv L_i(P_2) \bmod 8$, we have

$$[\mathcal{L}_i(\mathcal{P}_2), d_i']_2 = [L_i(P_2), d_i']_2.$$

(ii-b) The case $d_3 \equiv -1 \bmod 4$. As shown in Lemma 3.2,

$$e_1n + d_2 \equiv e_2n - d_1 \equiv 0 \bmod 4 \quad \text{and} \quad (e_1n + d_2) - (e_2n - d_1) \equiv 0 \bmod 8.$$

If $e_1n + d_2 \equiv e_2n - d_1 \equiv 0 \bmod 8$, take $\mathcal{P}_2 = (1, bu/d_1, av/d_2, 0)$ where $u^2 = e_2nd_1, v^2 = -e_1nd_2$. Then $P_2 = (1, u/d_1, v/d_2, 0)$ and

$$\begin{aligned}
\mathcal{L}_1(\mathcal{P}_2) &= ae_1n\alpha_1 + a\beta_1 v = aL_1(P_2),\\
\mathcal{L}_2(\mathcal{P}_2) &= be_2n\alpha_2 - b\gamma_2 u = bL_2(P_2),\\
\mathcal{L}_3(\mathcal{P}_2) &= -a\gamma_3 v + b\beta_3 u + ce_3n\alpha_3.
\end{aligned}$$

Since

$$\frac{(-\gamma_3 v)^2}{e_1} + \frac{(\beta_3 u)}{e_2} + \frac{(e_3n\alpha_3)^2}{e_3} = n(-d_2\gamma_3^2 + d_1\beta_3^2 + e_3n\alpha_3^2) = 0,$$

we have

$$\mathcal{L}_3(\mathcal{P}_2)L_3(P_2) = \frac{1}{2}(a+b)(a+c)(b+c)\left(\frac{e_3n\alpha_3}{a+b} + \frac{\beta_3 u}{a+c} - \frac{\gamma_3 v}{b+c}\right)^2$$

by Lemma 2.9. Therefore,

$$\begin{aligned}
[\mathcal{L}_1(\mathcal{P}_2), d_1']_2 &= [L_1(P_2), d_1']_2 + [a, d_1']_2 = [L_1(P_2), d_1']_2,\\
[\mathcal{L}_2(\mathcal{P}_2), d_2']_2 &= [L_2(P_2), d_2']_2 + [b, d_2']_2 = [L_2(P_2), d_2']_2,\\
[\mathcal{L}_3(\mathcal{P}_2), d_3']_2 &= [L_3(P_2), d_3']_2 + [2(a+b)(a+c)(b+c), d_3']_2 = [L_3(P_2), d_3']_2
\end{aligned}$$

by Lemma 2.8.

If $e_1n + d_2 \equiv e_2n - d_1 \equiv 4 \bmod 8$, denote by

$$\begin{aligned}
\mathcal{U} &= \sqrt{(4d_3b^{-2} + e_2n)d_1}, & \mathcal{V} &= \sqrt{(4d_3a^{-2} - e_1n)d_2},\\
U &= \sqrt{(4d_3 + e_2n)d_1}, & V &= \sqrt{(4d_3 - e_1n)d_2}
\end{aligned}$$

with $\mathcal{U} \equiv \mathcal{V} \equiv U \equiv V \equiv 1 \bmod 4$. Similar to (ii-a), we have $\mathcal{U} \equiv U, \mathcal{V} \equiv V \bmod 16$. Take $\mathcal{P}_2 = (1, b\mathcal{U}/d_1, a\mathcal{V}/d_2, 2)$, then $P_2 = (1, U/d_1, V/d_2, 2)$ and

$$\begin{aligned}
\mathcal{L}_1(\mathcal{P}_2) &\equiv ae_1n\alpha_1 + a\beta_1 V - 2d_3\gamma_1,\\
\mathcal{L}_2(\mathcal{P}_2) &\equiv be_2n\alpha_2 + 2d_3\beta_2 - b\gamma_2 U,\\
\mathcal{L}_3(\mathcal{P}_2) &\equiv -a\gamma_3 V + b\beta_3 U + ce_3n\alpha_3
\end{aligned}$$

modulo 16.

If γ_1 is odd, then exactly one of α_1 and β_1 is odd. Thus $\mathcal{L}_1(\mathcal{P}_2)$ is odd. If γ_1 is even, then both of α_1 and β_1 are odd. By choosing a suitable sign of α_1, we may assume that $4 \mid (\alpha_1 + \beta_1)$. Therefore, $2 \parallel \mathcal{L}_1(\mathcal{P}_2)$. Since $\mathcal{L}_1(\mathcal{P}_2) \equiv aL_1(P_2) \bmod 8$, we have

$$[\mathcal{L}_1(\mathcal{P}_2), d_1']_2 = [L_1(P_2), d_1']_2 + [a, d_1']_2 = [L_1(P_2), d_1']_2.$$

Similarly, we may assume that $2 \parallel \mathcal{L}_2(\mathcal{P}_2)$ by choosing a suitable sign of α_2. Since $\mathcal{L}_2(\mathcal{P}_2) \equiv aL_2(P_2) \bmod 8$, we have

$$[\mathcal{L}_2(\mathcal{P}_2), d_2']_2 = [L_2(P_2), d_2']_2 + [b, d_2']_2 = [L_2(P_2), d_2']_2.$$

Clearly, β_3 and γ_3 are odd. By choosing a suitable sign of γ_3, we may assume that $2 \parallel \mathcal{L}_3(\mathcal{P}_2)$ and $2 \parallel L_3(P_2)$. Since

$$\begin{aligned}&\frac{1}{4}\left(\frac{(-\gamma_3 V)^2}{e_1}+\frac{(\beta_3 U)^2}{e_2}+\frac{(e_3 n\alpha_3)^2}{e_3}\right)\\ =&d_3\left(\frac{d_1\beta_3^2}{e_2}+\frac{d_2\gamma_3^2}{e_1}\right)+\frac{1}{4}n(e_3n\alpha_3^2+d_1\beta_3^2-d_2\gamma_3^2)\\ \equiv&d_3(d_1e_2+d_2e_1)\equiv d_3\big((e_2n-4)e_2+(4-e_1n)e_1\big)\\ \equiv&4d_3(-e_2+e_1)\equiv 0 \bmod 8\end{aligned}$$

and $4 \mid (e_1a+e_2b+e_3c)$, the odd number

$$\frac{\mathcal{L}_3(\mathcal{P}_2)}{2}\cdot\frac{L_3(P_2)}{2}\equiv\frac{1}{8}(a+b)(a+c)(b+c)\left(-\frac{\gamma_3 V}{b+c}+\frac{\beta_3 U}{c+a}+\frac{e_3 n\alpha_3}{a+b}\right)^2 \bmod 8$$

is congruent to 1 modulo 4 by Lemmas 2.9 and 2.8. Therefore

$$[\mathcal{L}_3(\mathcal{P}_2), d_3']_2 = [L_3(P_2), d_3']_2.$$

The rest part is similar to the proof of Theorem 2.7. □

4. The even case

Assume that $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ and $E^{(n)}$ has no rational point of order 4. Write $e_i = 2f_i$. Let n be an odd positive square-free integer. Let $\Lambda = (d_1, d_2, d_3)$ where d_1, d_2, d_3 are square-free divisors of $2f_1f_2f_3n$.

4.1. **Homogeneous spaces.**

Recall that $D_\Lambda^{(n)}$ is defined as

$$\begin{cases} H_1: & 2f_1nt^2+d_2u_2^2-d_3u_3^2=0,\\ H_2: & 2f_2nt^2+d_3u_3^2-d_1u_1^2=0,\\ H_3: & 2f_3nt^2+d_1u_1^2-d_2u_2^2=0\end{cases}$$

and the 2-torsion points of $E^{(n)}$ correspond to

$$(1,1,1),\ (-2f_3n,-f_1f_3,2f_1n),\ (-f_2f_3,2f_3n,-2f_2n),\ (2f_2n,-2f_1n,-f_1f_2).$$

These triples have 2-valuations $(0,0,0),(0,1,1),(1,0,1),(1,1,0)$ (not correspondingly). Hence any element in the pure 2-Selmer group $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has a unique representative $\Lambda = (d_1, d_2, d_3)$ with odd $d_i \mid e_1e_2e_3n$.

Lemma 4.1. *Let $\Lambda = (d_1, d_2, d_3)$ where d_1, d_2, d_3 are odd. If $D_\Lambda^{(n)}(\mathbb{Q}_2) \neq \emptyset$, then $d_3 \equiv 1 \bmod 4$.*

Proof. Since $v_2(t) \geq v_2(u_3) = v_2(u_2)$ by H_1 and $v_2(t) \geq v_2(u_1) = v_2(u_3)$ by H_2, we may assume that u_1, u_2, u_3 are 2-adic units and t is a 2-adic integer. Then

$$2f_3nt^2 = d_2u_2^2 - d_1u_1^2 \equiv d_2 - d_1 \bmod 8.$$

This implies that $d_2 \equiv d_1 \bmod 4$ and then $d_3 \equiv 1 \bmod 4$. □

Lemma 4.2. *Let $\Lambda = (d_1, d_2, d_3)$ where d_1, d_2, d_3 are odd and $d_3 \equiv 1 \bmod 4$. If $D_\Lambda^{(n)}$ is locally solvable at all places $v \neq 2$, then $D_\Lambda^{(n)}$ is also locally solvable at $v = 2$.*

Proof. Similar to Lemma 3.2, we have

$$[2f_1nd_3, d_1]_2 = [2f_2nd_1, d_2]_2 = [2f_3nd_2, d_3]_2 = 0.$$

If $(d_1, d_2, d_3) \equiv (1, 1, 1) \bmod 4$, then $d_1 \equiv d_2 \equiv d_3 \equiv 1 \bmod 8$. Take

$$t = 0, u_1 = \sqrt{d_3/d_1},\ u_2 = \sqrt{d_3/d_2},\ u_3 = 1.$$

If $(d_1, d_2, d_3) \equiv (-1, -1, 1) \bmod 4$, then $2f_1nd_3 \equiv d_1 + 3$ and $2f_2nd_1 \equiv d_2 + 3 \bmod 8$. In other words, $2f_1n \equiv d_2 + 3d_3 \bmod 8$ and $2f_2n \equiv d_3 + 3d_1 \bmod 8$. Take $t = u_3 = 1$, then

$$u_1^2 = (d_3 + 2f_2n)/d_1 \equiv 2d_2 + 3 \equiv 1 \bmod 8$$

and

$$u_2^2 = (d_3 - 2f_1n)/d_2 \equiv -2d_1 - 1 \equiv 1 \bmod 8.$$

Hence $D_\Lambda^{(n)}$ is locally solvable at $v = 2$. □

Lemma 4.3. *Assume that n is coprime with $e_1e_2e_3$. If q is an odd prime factor of e_i, then $D_\Lambda^{(n)}(\mathbb{Q}_q) \neq \emptyset$ if and only if $q \nmid d_i$ and*

- $\left(\frac{d_i}{q}\right) = 1$, *if* $q \nmid d_{i+1}$;
- $\left(\frac{e_{i+1}nd_i}{q}\right) = 1$, *if* $q \mid d_{i+1}, q^2 \nmid e_i$;
- $\left(\frac{e_{i+1}n}{q}\right) = \left(\frac{d_i}{q}\right) = 1$, *if* $q \mid d_{i+1}, q^2 \mid e_i$.

Proof. By the symmetry, we only need to consider the case $i = 1$. Assume that $D_\Lambda(\mathbb{Q}_q) \neq \emptyset$. Since we are dealing with homogeneous spaces, we may assume that t, u_1, u_2, u_3 are q-adic integers and at least one of them is a q-adic unit. If $q \mid d_1, q \mid d_2, q \nmid d_3$, then $q \mid u_3$ by H_1 and $q \mid t$ by H_3. Therefore, $q \mid u_1$ by H_2 and $q \mid u_2$ by H_3, which is impossible. Similarly, the case $q \mid d_1, q \nmid d_2, q \mid d_3$ is also impossible. Hence $q \nmid d_1$.

If $q \nmid d_2d_3$, then $\left(\frac{d_1}{q}\right) = \left(\frac{d_2d_3}{q}\right) = 1$ by H_1. Conversely, if $\left(\frac{d_1}{q}\right) = 1$, then we take

$$\begin{aligned}
u_2 &= d_1d_3/d_2,\\
u_1^2 &= d_3 - e_3nt^2/d_1,\\
u_3^2 &= d_1 + e_1nt^2/d_3 \equiv d_1 \bmod q,
\end{aligned}$$

where $t \in \mathbb{Z}_q$ such that $d_3 - e_3nt^2/d_1$ is a square in $\mathbb{Z}_q$. In fact, if e_3nd_2 is quadratic residue modulo q, then we may take $t = \sqrt{\frac{d_1d_3}{e_3n}}$ and $u_1 = 0$; if not, then there exists $t \in \{0, 1, \dots, (q-1)/2\}$ such that $d_3 - e_3nt^2/d_1 \bmod q$ is a nonzero square. Hence $D_\Lambda(\mathbb{Q}_q)$ is non-empty.

If $q \mid d_2, q \mid d_3$ and $q^2 \nmid e_1$, then $\left(\frac{e_2nd_1}{q}\right) = 1$ by H_2. Conversely, if $\left(\frac{e_2nd_1}{q}\right) = 1$, then we take

$$\begin{aligned}
u_2^2 &= d_1d_3/d_2,\\
u_1^2 &= d_3 - e_3nt^2/d_1 \equiv e_2nt^2/d_1 \bmod q,\\
u_3^2 &= d_1 + e_1nt^2/d_3.
\end{aligned}$$

Similar to the previous case, there exists $t \in \mathbb{Z}_q$ such that $d_1 + e_1t^2/d_3$ is a square in $\mathbb{Z}_q$. Hence $D_\Lambda(\mathbb{Q}_q)$ is non-empty.

If $q \mid d_2, q \mid d_3$ and $q^2 \mid e_1$, then $\left(\frac{d_1}{q}\right) = \left(\frac{d_2 d_3}{q}\right) = 1$ by H_1 and $\left(\frac{e_2 n d_1}{q}\right) = 1$ by H_2. Conversely, if $\left(\frac{e_2 n}{q}\right) = \left(\frac{d_1}{q}\right) = 1$, then $\left(\frac{-e_3 n d_1}{q}\right) = 1$ and we take

$$\begin{aligned} u_2^2 &= d_1 d_3 / d_2, \\ u_1^2 &= d_3 - e_3 n t^2 / d_1 \equiv e_2 n t^2 / d_1 \bmod q, \\ u_3^2 &= d_1 + e_1 n t^2 / d_3 \equiv d_1 \bmod q. \end{aligned}$$

Hence $D_\Lambda(\mathbb{Q}_q)$ is non-empty. □

Let $\Lambda = (d_1, d_2, d_3) \in \mathrm{Sel}_2'\big(E^{(n)}\big)$ with odd $d_i \mid e_1 e_2 e_3 n$ and $d_3 \equiv 1 \bmod 4$. We will use the notations $\mathbf{x}, \mathbf{y}, \mathbf{z}$ in (2.3). If $e_2 > 0$ and $e_3 < 0$, or all $p_i \equiv 1 \bmod 4$, write

$$\begin{aligned} d_1 &= p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \\ d_2 &= p_1^{y_1} \left(\frac{-1}{p_1}\right)^{z_1} \cdots p_k^{y_k} \left(\frac{-1}{p_1}\right)^{z_k} \cdot \widetilde{d}_2, \\ d_3 &= (p_1^*)^{z_1} \cdots (p_k^*)^{z_k} \cdot \widetilde{d}_3 \end{aligned} \tag{4.1}$$

where $p^* = \left(\frac{-1}{p}\right) p$. Then $\widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}$.

Theorem 4.4. *Let n be an odd positive square-free integer coprime with $e_1 e_2 e_3$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1 e_2 e_3$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *$e_2 > 0$ and $e_3 < 0$, or all $p_i \equiv 1 \bmod 4$;*
- *$\left(\frac{p^*}{q}\right) = 1$ for any odd primes $p \mid n, q \mid e_2 e_3$.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the map $(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{z} \end{pmatrix}$ induces an isomorphism

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \xrightarrow{\sim} \mathrm{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{e_2} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_2} & \mathbf{A}^{\mathrm{T}} + \mathbf{D}_{e_2} \end{pmatrix},$$

where $d_i \mid n, d_1 > 0, d_3 \equiv 1 \bmod 4$.

Proof. Let $\Lambda = (d_1, d_2, d_3)$ with odd square-free $d_i \mid e_1 e_2 e_3 n$ and denote by $\widetilde{\Lambda} = (\widetilde{d}_1, \widetilde{d}_2, \widetilde{d}_3)$. If all $p_i \equiv 1 \bmod 4$, then $\mathrm{sgn}(d_i) = \mathrm{sgn}(\widetilde{d}_i)$. If $e_2 > 0, e_3 < 0$, then $\mathrm{sgn}(d_1) = \mathrm{sgn}(\widetilde{d}_1)$. Hence $D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset$ if and only if $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{R}) \neq \emptyset$ by Lemma 2.4.

One can show that $n, d_i / \widetilde{d}_i \in \mathbb{Q}_q^{\times 2}$ where q is an odd prime factor of e_i by our assumptions. Therefore, $D_\Lambda^{(n)}(\mathbb{Q}_q) \neq \emptyset$ if and only if $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_q) \neq \emptyset$ by Lemma 4.3. Hence $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$ if and only if $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$ and $D_\Lambda^{(n)}$ is locally solvable at each $p \mid n$ by Lemmas 4.1, 4.2 and the fact $d_3 \equiv \widetilde{d}_3 \equiv 1 \bmod 4$.

If $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$, then $\widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q})$. By our assumptions, $\widetilde{\Lambda} = (1, 1, 1)$. Hence each element in $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has a unique representative (d_1, d_2, d_3) with $d_i \mid n, d_1 > 0, d_3 \equiv 1 \bmod 4$. Based on this, we can express $\mathrm{Sel}_2'\big(E^{(n)}\big)$ in terms of linear algebra by Lemma 2.5 after a translation of languages. One need the fact that

$$\big([p_i^*, -n]_{p_j}\big)_{i,j} = \mathbf{A}^{\mathrm{T}} + \mathbf{D}_{-1}.$$

□

If $e_3 > 0$ and $e_1 < 0$, write

$$\begin{aligned} d_1 &= p_1^{x_1}\left(\frac{-1}{p_1}\right)^{z_1}\cdots p_k^{x_k}\left(\frac{-1}{p_1}\right)^{z_k}\cdot \widetilde{d}_1,\\ d_2 &= p_1^{y_1}\cdots p_k^{y_k}\cdot \widetilde{d}_2,\\ d_3 &= (p_1^*)^{z_1}\cdots (p_k^*)^{z_k}\cdot \widetilde{d}_3.\end{aligned}$$

Then $\widetilde{d}_1\widetilde{d}_2\widetilde{d}_3 \in \mathbb{Q}^{\times 2}$. Similar to Theorem 4.4, we have:

Theorem 4.5. *Let n be an odd positive square-free integer coprime with $e_1e_2e_3$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *$e_3 > 0$ and $e_1 < 0$;*
- *$\left(\frac{p^*}{q}\right) = 1$ for any odd primes $p \mid n, q \mid e_1e_3$.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the map $(d_1, d_2, d_3) \mapsto \begin{pmatrix}\mathbf{y}\\ \mathbf{z}\end{pmatrix}$ induces an isomorphism

$$\mathrm{Sel}_2'(E^{(n)}) \xrightarrow{\sim} \mathrm{Ker}\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-e_1} & \mathbf{D}_{-e_1e_3}\\ \mathbf{D}_{-e_1e_2} & \mathbf{A}^{\mathrm{T}}+\mathbf{D}_{-e_1}\end{pmatrix},$$

where $d_i \mid n, d_2 > 0, d_3 \equiv 1 \bmod 4$.

4.2. **The Cassels pairing.** Let (a, b, c) be a primitive triple of odd integers satisfying

$$e_1a^2 + e_2b^2 + e_3c^2 = 0.$$

Denote by $\mathcal{E} = \mathscr{E}_{e_1a^2, e_2b^2}$ and $\mathcal{E}^{(n)} = \mathscr{E}_{e_1a^2n, e_2b^2n}$.

Theorem 4.6. *Let n be an odd positive square-free integer coprime with $e_1e_2e_3abc$, whose prime factors are quadratic residues modulo each odd prime factor of $e_1e_2e_3abc$. Assume that*

- *both E and $E^{(n)}$ have no rational point of order 4;*
- *if $e_2 > 0$ and $e_3 < 0$, then $\left(\frac{p^*}{q}\right) = 1$ for any odd primes $p \mid n, q \mid e_2e_3bc$;*
- *if $e_3 > 0$ and $e_1 < 0$, then $\left(\frac{p^*}{q}\right) = 1$ for any odd primes $p \mid n, q \mid e_1e_3ac$;*
- *if $e_1 > 0$ and $e_2 < 0$, then $p \equiv 1 \bmod 4$ for any odd primes $p \mid n$.*

If $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then the following are equivalent:

1. *$\mathrm{rank}_\mathbb{Z} E^{(n)}(\mathbb{Q}) = 0$ and $Ш(E^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;*
2. *$\mathrm{rank}_\mathbb{Z} \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ and $Ш(\mathcal{E}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.*

Since $\left(\frac{p}{q}\right) = 1$, we have that $\left(\frac{p^*}{q}\right) = 1$ if and only if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$. Hence this theorem is the same as Theorem 1.2.

Proof. Similar to the proof of Theorem 2.7, both $E^{(n)}$ and $\mathcal{E}(\mathbb{Q})^{(n)}$ have no rational point of order 4. By choosing suitable signs, we may assume that $a \equiv b \equiv c \equiv 1 \bmod 4$.

Assume that $e_2 > 0$ and $e_3 < 0$, or all prime factors of n are congruent to 1 modulo 4. Since the matrix in Theorem 4.4 does not depend on a, b, c, we have a canonical isomorphism

$$\mathrm{Sel}_2'(E^{(n)}) \cong \mathrm{Sel}_2'(\mathcal{E}^{(n)}).$$

Let $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2'(\mathcal{E}^{(n)})$ with $d_i, d_i' \mid n, d_1, d_1' > 0, d_3 \equiv d_3' \equiv 1 \bmod 4$. If $d_2 < 0$ and $d_2' < 0$, we replace Λ' by $\Lambda + \Lambda'$. If $d_2 > 0$ and $d_2' < 0$, we switch Λ and Λ'. Since

$$\langle \Lambda, \Lambda' \rangle = \langle \Lambda, \Lambda + \Lambda' \rangle = \langle \Lambda', \Lambda \rangle,$$

these operations do not change $\langle \Lambda, \Lambda' \rangle$. Hence we may assume that $d_2' > 0$ and $d_3' > 0$. When $e_3 > 0$ and $e_1 < 0$, we may assume that $d_1' > 0$ and $d_3' > 0$ similarly.

We will denote by $\mathcal{D}, \mathcal{H}, \mathcal{Q}, \mathcal{L}, \mathcal{P}$ the corresponding symbols for $\mathcal{E}$ and D, H, Q, L, P the corresponding symbols for E in the calculation of Cassels pairing. Recall that $\mathcal{D}_\Lambda^{(n)}$ is defined as

$$\begin{cases} \mathcal{H}_1: & 2f_1a^2nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ \mathcal{H}_2: & 2f_2b^2nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ \mathcal{H}_3: & 2f_3c^2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

Let $(\alpha_i, \beta_i, \gamma_i)$ be primitive triples of integers satisfying

$$\begin{aligned} 2f_1n\alpha_1^2 + d_2\beta_1^2 - d_3\gamma_1^2 = 0, \\ 2f_2n\alpha_2^2 + d_3\beta_2^2 - d_1\gamma_2^2 = 0, \\ 2f_3n\alpha_3^2 + d_1\beta_3^2 - d_2\gamma_3^2 = 0. \end{aligned}$$

Choose

$$\begin{aligned} \mathcal{Q}_1 &= (\alpha_1, a\beta_1, a\gamma_1) \in \mathcal{H}_1(\mathbb{Q}), & \mathcal{L}_1 &= 2f_1an\alpha_1t + d_2\beta_1u_2 - d_3\gamma_1u_3, \\ \mathcal{Q}_2 &= (\alpha_2, b\beta_2, b\gamma_2) \in \mathcal{H}_2(\mathbb{Q}), & \mathcal{L}_2 &= 2f_2bn\alpha_2t + d_3\beta_2u_3 - d_1\gamma_2u_1, \\ \mathcal{Q}_3 &= (\alpha_3, c\beta_3, c\gamma_3) \in \mathcal{H}_3(\mathbb{Q}), & \mathcal{L}_3 &= 2f_3cn\alpha_3t + d_1\beta_3u_1 - d_2\gamma_3u_2. \end{aligned}$$

(i) The case odd $v = q \mid e_1e_2e_3abc$. Since $\left(\frac{p}{q}\right) = 1$ for any prime factor p of n, $d_i' > 0$ is a square modulo q. Therefore, $[\mathcal{L}_i(\mathcal{P}_q), d_i']_q = 0 = [L_i(P_q), d_i']_q$.

(ii) The case $v = p \mid n$. The proof is similar to the proof of Theorem 2.7.

(iii) The case $v = 2$. Note that $d_3 \equiv 1 \bmod 4$.

(iii-a) The case $(d_1, d_2, d_3) \equiv (1, 1, 1) \bmod 4$. As shown in Lemma 4.2, we have $d_1 \equiv d_2 \equiv d_3 \equiv 1 \bmod 8$, take $\mathcal{P}_2 = (0, 1/\sqrt{d_1}, 1/\sqrt{d_2}, 1/\sqrt{d_3}) = P_2$. Then

$$\begin{aligned} \mathcal{L}_1(\mathcal{P}_2) = \beta_1\sqrt{d_2} - \gamma_1\sqrt{d_3} = L_1(P_2), \\ \mathcal{L}_2(\mathcal{P}_2) = \beta_2\sqrt{d_3} - \gamma_2\sqrt{d_1} = L_2(P_2), \\ \mathcal{L}_3(\mathcal{P}_2) = \beta_3\sqrt{d_1} - \gamma_3\sqrt{d_2} = L_3(P_2). \end{aligned}$$

(iii-b) The case $(d_1, d_2, d_3) \equiv (-1, -1, 1) \bmod 4$. As shown in Lemma 4.2, we have $(d_3 + 2f_2b^2n)d_1 \equiv (d_3 - 2f_1a^2n)d_2 \equiv 1 \bmod 8$. Denote by

$$\begin{aligned} \mathcal{U} &= \sqrt{(d_3 + 2f_2b^2n)d_1}, & \mathcal{V} &= \sqrt{(d_3 - 2f_1a^2n)d_2}, \\ U &= \sqrt{(d_3 + 2f_2n)d_1}, & V &= \sqrt{(d_3 - 2f_1n)d_2} \end{aligned}$$

with $\mathcal{U} \equiv \mathcal{V} \equiv U \equiv V \equiv 1 \bmod 4$. Since $\mathcal{U}^2 \equiv U^2 \bmod 16$, we have $\mathcal{U} \equiv U \bmod 8$. Similarly, $\mathcal{V} \equiv V \bmod 8$.

Take $\mathcal{P}_2 = (1, \mathcal{U}/d_1, \mathcal{V}/d_2, 1)$, then $P_2 = (1, U/d_1, V/d_2, 1)$. Note that all β_i, γ_i are odd. By choosing suitable signs of γ_i, we may assume that $2 \parallel \mathcal{L}_i(\mathcal{P}_2)$. Since

$$\begin{aligned}\mathcal{L}_1(\mathcal{P}_2) &\equiv 2f_1 an\alpha_1 + \beta_1 V - d_3\gamma_1 \equiv L_1(P_2),\\ \mathcal{L}_2(\mathcal{P}_2) &\equiv 2f_2 bn\alpha_2 + d_3\beta_2 - \gamma_2 U \equiv L_2(P_2),\\ \mathcal{L}_3(\mathcal{P}_2) &\equiv 2f_3 cn\alpha_3 + \beta_3 U - \gamma_3 V \equiv L_3(P_2)\end{aligned}$$

modulo 8, we have

$$[\mathcal{L}_i(\mathcal{P}_2), d_i']_2 = [L_i(P_2), d_i']_2.$$

The rest part is similar to the proof of Theorem 2.7. □

5. Congruent elliptic curves

Assume that $n = p_1 \cdots p_k \equiv 1 \bmod 4$. Denote by

$$h_{2^s}(n) = \dim_{\mathbb{F}_2} \frac{2^{s-1}\mathrm{Cl}\big(\mathbb{Q}(\sqrt{-n})\big)}{2^s\mathrm{Cl}\big(\mathbb{Q}(\sqrt{-n})\big)}$$

the 2^s-rank of the class group of $\mathbb{Q}(\sqrt{-n})$. By Gauss genus theory and Rédei's work in [Rei34], we can characterize $h_2(n)$ and $h_4(n)$. See [Wan16, § 3] for more details.

Proposition 5.1. *We have $h_2(n) = k$ and $h_4(n) = k - \mathrm{rank}(\mathbf{A}, \mathbf{D}_2\mathbf{1})$.*

Denote by

$$E = \mathscr{E}_{1,1} : y^2 = x(x-1)(x+1)$$

the congruent elliptic curve and $E^{(n)} = \mathscr{E}_{n,n}$. Let (a, b, c) be a primitive triple of positive integers satisfying $a^2 + b^2 = 2c^2$. Then a, b, c are odd. Denote by $\mathcal{E} = \mathscr{E}_{a^2,b^2}, \mathcal{E}^{(n)} = \mathscr{E}_{a^n,b^2n}$.

Theorem 5.2 ([WZ22, Theorem 4.4])**.** *Let $n \equiv 1 \bmod 8$ be an positive square-free integer coprime with abc, where each prime factor of n is a quadratic residue modulo every odd prime factor of abc. Assume that*

- *$p \equiv 1 \bmod 4$ for all primes $p \mid n$;*
- *$\mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Then the following are equivalent:

1. *$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}^{(n)}(\mathbb{Q}) = 0$ and $Ш\big(\mathcal{E}^{(n)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^2$;*
2. *$h_4(n) = 1$ and $h_8(n) \equiv \frac{d-1}{4} \bmod 2$.*

Here $d \neq 1, n$ is a positive factor of n such that $(d, -n)_v = 1, \forall v$, or $(2d, -n)_v = 1, \forall v$.

Proof. Since $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, this result follows from Theorem 3.5 and [Wan16, Theorem 1.1] directly. □

Theorem 5.3. *Let $n \equiv 1 \bmod 8$ be a positive square-free integer coprime with abc, where each prime factor of n is a quadratic residue modulo every prime factor of abc. Assume that*

- *either n or a or b has no prime factor $\equiv 3 \bmod 4$;*
- *$p \equiv \pm 1 \bmod 8$ for all primes $p \mid n$;*
- *$\mathrm{Sel}_2\big(\mathcal{E}^{(2)}/\mathbb{Q}\big) \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Then the following are equivalent:

1. *$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}^{(2n)}(\mathbb{Q}) = 0$ and $Ш\big(\mathcal{E}^{(2n)}/\mathbb{Q}\big)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;*
2. *$h_4(n) = 1$ and $d \equiv 9 \bmod 16$.*

Here, d is the unique divisor of n such that $d \neq 1, d \equiv 1 \bmod 4$ and $(d,n)_v = 1, \forall v$.

Proof. For any prime $q \mid c$, we have $a^2 \equiv -b^2 \bmod q$. Therefore $q \equiv 1 \bmod 4$ and $\left(\frac{p^*}{q}\right) = \left(\frac{p}{q}\right) = 1$. If n or b has no prime factor $\equiv 3 \bmod 4$, then $\left(\frac{p^*}{q}\right) = \left(\frac{p}{q}\right) = 1$ for all primes $p \mid n, q \mid b$. We apply Theorem 4.4 to $(e_1, e_2, e_3) = (2a^2, 2b^2, -4c^2)$, the map $(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{z} \end{pmatrix}$ induces an isomorphism

$$\mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big) \xrightarrow{\sim} \mathrm{Ker}\,\mathbf{M} \quad \text{where} \quad \mathbf{M} = \begin{pmatrix} \mathbf{A} + \mathbf{D}_2 & \mathbf{D}_2 \\ \mathbf{D}_{-1} & \mathbf{A}^{\mathrm{T}} + \mathbf{D}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{A} & \\ \mathbf{D}_{-1} & \mathbf{A}^{\mathrm{T}} \end{pmatrix}$$

and $d_i \mid n, d_1 > 0, d_3 \equiv 1 \bmod 4$.

One can show that

$$\mathrm{Ker}\,\mathbf{M} \supseteq \left\{ \begin{pmatrix} \mathbf{0} \\ \mathbf{d} \end{pmatrix}, \begin{pmatrix} \mathbf{1} \\ \mathbf{d} + \mathbf{1} \end{pmatrix} : \mathbf{d} \in \mathrm{Ker}\,\mathbf{A}^{\mathrm{T}} \right\}.$$

Since $\mathbf{A}\mathbf{1} = \mathbf{0}$, we have $\mathrm{rank}\,\mathbf{A}^{\mathrm{T}} = \mathrm{rank}\,\mathbf{A} \leq k-1$ and then $\mathrm{Ker}\,\mathbf{M}$ has at least four vectors. Hence

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big) = 2 \iff \mathrm{rank}\,\mathbf{A} = k-1 \iff h_4(n) = 1$$

by Proposition 5.1.

Assume that $h_4(n) = 1$. Note that $(p_j, -n)_{p_i} = (p_i^*, n)_{p_j}$. Therefore, $\mathbf{A}^{\mathrm{T}}\mathbf{d} = 0$ if and only if $(d,n)_p = 1$ for all $p \mid n$, where $d = (p_1^*)^{s_1} \cdots (p_k^*)^{s_k}$, $\mathbf{d} = (s_1, \ldots, s_k)^{\mathrm{T}}$. Hence $\mathrm{Sel}_2'\big(\mathcal{E}^{(n)}\big)$ is generated by $\Lambda = (n, 1, n)$ and $\Lambda' = (1, d, d)$.

By Theorem 4.6, we may assume that $a = b = c = 1$. Recall that $D_\Lambda^{(n)}$ is defined as

$$\begin{cases} H_1: & 2nt^2 + u_2^2 - nu_3^2 = 0, \\ H_2: & 2t^2 + u_3^2 - u_1^2 = 0, \\ H_3: & -4nt^2 + nu_1^2 - u_2^2 = 0. \end{cases}$$

Choose

$$Q_2 = (0,1,1) \in H_2(\mathbb{Q}), \qquad L_2 = u_1 - u_3,$$
$$Q_3 = (1,0,-2) \in H_3(\mathbb{Q}), \qquad L_3 = 2t + u_1.$$

By Lemma 2.2, we have

$$\langle \Lambda, \Lambda' \rangle_{E^{(n)}} = \sum_{v \mid 2n\infty} \big[L_2L_3(P_v), d\big]_v$$

for any $P_v \in D_\Lambda^{(n)}(\mathbb{Q}_v)$.

For $v \mid n\infty$, take $P_v = (1, 2, 0, -\sqrt{2})$, then $L_2L_3(P_v) = 4(2+\sqrt{2})$ and $\langle \Lambda, \Lambda' \rangle_v = [2+\sqrt{2}, d]_v$. For $v = 2$, take $P_2 = (0, 1, \sqrt{n}, -1)$. Then $L_2L_3(P_2) = 2$ and $\langle \Lambda, \Lambda' \rangle_2 = [2, d]_2 = 0$. Hence $\langle \Lambda, \Lambda' \rangle_{E^{(n)}} = \left[\frac{2+\sqrt{2}}{|d|}\right] \equiv \frac{d-1}{8} \bmod 2$ by Lemma 5.4. Conclude the results by Lemma 2.3.

If a has no prime factor $\equiv 3 \bmod 4$, then $\left(\frac{p^*}{q}\right) = \left(\frac{p}{q}\right) = 1$ for all primes $p \mid n, q \mid a$. We apply Theorem 4.5 to $(e_1, e_2, e_3) = (-2b^2, -2a^2, 4c^2)$. Then we can prove the result similarly. □

Lemma 5.4. *Let $m \equiv 1 \bmod 8$ be a square-free integer with prime factors congruent to ± 1 modulo 8. Then $m \equiv 1 \bmod 16$ if and only if $\left(\frac{2+\sqrt{2}}{|m|}\right) = 1$.*

Proof. Write $m = u^2 - 2w^2 \equiv 1 \bmod 8$. Denote by $\mu = u + w$ and $\lambda = u + 2w$. Then $m = 2\mu^2 - \lambda^2$ and u, μ, λ are odd. Let w' be the positive odd part of w. Then
$$\left(\frac{w}{|m|}\right) = \left(\frac{m}{w'}\right) = \left(\frac{u^2 - 2w^2}{w'}\right) = 1, \quad \left(\frac{\lambda}{|m|}\right) = \left(\frac{m}{|\lambda|}\right) = \left(\frac{2\mu^2 - \lambda^2}{\lambda}\right) = \left(\frac{2}{|\lambda|}\right)$$
and $\lambda = u + 2w \equiv (2 \pm \sqrt{2})w \bmod m$. Hence
$$\left(\frac{2+\sqrt{2}}{|m|}\right) = \left(\frac{2}{|\lambda|}\right).$$
Since $m + \lambda^2 = 2\mu^2 \equiv 2 \bmod 16$, we have
$$m \equiv 1 \bmod 16 \iff \lambda \equiv \pm 1 \bmod 8 \iff \left(\frac{2}{|\lambda|}\right) = 1 \iff \left(\frac{2+\sqrt{2}}{|m|}\right) = 1. \quad \square$$

Acknowledgements

The author would like to thank Zhangjie Wang for his proof of Lemma 4.3. The author is partially supported by National Natural Science Foundation of China (Grant No. 12001510).

References

[Cas98] J. W. S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998. Dedicated to Martin Kneser on the occasion of his 70th birthday.

[Ono96] Ken Ono. Euler's concordant forms. *Acta Arith.*, 78(2):101–123, 1996.

[Rei34] L. Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wan16] Zhang Jie Wang. Congruent elliptic curves with non-trivial Shafarevich-Tate groups. *Sci. China Math.*, 59(11):2145–2166, 2016.

[WZ22] Zhangjie Wang and Shenxing Zhang. On the quadratic twist of elliptic curves with full 2-torsion. *preprint*, 2022.

School of Mathematics, Hefei University of Technology, Hefei, Anhui 230000, China
Email address: zhangshenxing@hfut.edu.cn