J. Korean Math. Soc. **60** (2023), No. 5, pp. 1087–1107
https://doi.org/10.4134/JKMS.j230085
pISSN: 0304-9914 / eISSN: 2234-3008

A CONJECTURE OF GROSS AND ZAGIER: CASE $E(\mathbb{Q})_{\mathbf{tor}} \cong \mathbb{Z}/2\mathbb{Z}$ OR $\mathbb{Z}/4\mathbb{Z}$

Dongho Byeon, Taekyung Kim, and Donggeon Yhee

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, c the Manin constant of E, and m the product of Tamagawa numbers of E at prime divisors of N. Let K be an imaginary quadratic field where all prime divisors of N split in K, P_K the Heegner point in $E(K)$, and $\mathrm{Ш}(E/K)$ the Shafarevich-Tate group of E over K. Let $2u_K$ be the number of roots of unity contained in K. Gross and Zagier conjectured that if P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\mathrm{Ш}(E/K)|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$. In this paper, we prove that this conjecture is true if $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$ except for two explicit families of curves. Further, we show these exceptions can be removed under Stein–Watkins conjecture.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, c the Manin constant of E and $m = \prod_{p|N} m_p$, where m_p is the Tamagawa number of E at a prime divisor p of N. Let K be an imaginary quadratic field where all prime divisors of N split in K, P_K the Heegner point in $E(K)$, and $\mathrm{Ш}(E/K)$ the Shafarevich-Tate group of E over K. Let $2u_K$ be the number of roots of unity contained in K. In [6], Gross and Zagier conjectured:

Conjecture 1.1 ([6, p. 311, (2.3) Conjecture])**.** *If P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\mathrm{Ш}(E/K)|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$.*

Rational torsion subgroups of elliptic curves E over $\mathbb{Q}$ are completely classified by Mazur [10]: $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \le n \le 10,\ n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} & \text{for } n = 2, 4, 6, 8. \end{cases}$$

Received February 15, 2023; Accepted July 11, 2023.
2020 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic curve, Manin constant, Tamagawa number, Shafarevich-Tate group.
This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2023R1A2C1002612).

From [9, Proposition 1.1] we know that the conjecture is true when $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $5 \leq n \leq 10$, $n = 12$ or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ (cf. [1, Theorem 1.1]). In [1, Theorem 1.2] and [2, Theorem 1.1], we proved that the conjecture is true when $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. So the only remaining cases for the validity of the conjecture are those when $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. In this paper, we prove the following theorems.

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let Δ be the discriminant of E and c_4, c_6 the usual invariants for E. Then Conjecture 1.1 is true except for the family $\mathcal{F}_1$ of elliptic curves having $\Delta = 16p$, $c_4 = 16p - 16$, and $c_6 = -32A(2p + 1)$, where $p = A^2 + 4$ is a prime.*

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Let Δ be the discriminant of E and c_4, c_6 the usual invariants for E. Then Conjecture 1.1 is true except for the family $\mathcal{F}_2$ of elliptic curves having $\Delta = p^n\ell$, $c_4 = p^{2n}+16p^n+1$, and $c_6 = -p^{3n}-24p^{2n}-120p^n+64$, where n is a positive even integer and $p \equiv 3 \pmod 4$ is a prime such that $p^n + 16 = \ell$ is a prime.*

For $i = 0, 1$, let $X_i(N) = \mathbb{H}^*/\Gamma_i(N)$ denote the modular curves of level N and $\mathcal{C}$ a rational isogeny class of elliptic curves of conductor N. Then there is a unique curve $E_i \in \mathcal{C}$ and a parametrization $\theta_i : X_i(N) \to E_i$ such that for any $E \in \mathcal{C}$ and parametrization $\theta_i' : X_i(N) \to E$, there is an isogeny $\pi_i : E_i \to E$ such that $\pi_i \circ \theta_i = \theta_i'$. The curve E_i is called the $X_i(N)$-optimal curve in $\mathcal{C}$. Let $\pi : E \to E'$ be an isogeny with $E, E' \in \mathcal{C}$. We say that π is étale if the extension $E_{\mathbb{Z}} \to E'_{\mathbb{Z}}$ to Néron models over $\mathbb{Z}$ is étale (cf. [15, Section 1]). Stevens [14] proved that there exists a unique curve $E_{\min} \in \mathcal{C}$ such that for every $E \in \mathcal{C}$, there is an étale isogeny $\pi : E_{\min} \to E$ and conjectured that $E_{\min} = E_1$. Based on numerical computation and the Stevens conjecture, Stein and Watkins made the following conjecture.

Conjecture 1.4 ([12, Section 4])**.** *For each curve E in the family $\mathcal{F}_1$ or $\mathcal{F}_2$, there is an étale isogeny $\pi : E \to E_0$ of degree 2^r $(r \geq 1)$, so E_1 differs from E_0 in $\mathcal{C} \ni E$.*

Theorem 1.5. *If we assume Conjecture 1.4, then Conjecture 1.1 is true for the two families $\mathcal{F}_1$ and $\mathcal{F}_2$.*

2. Preliminaries

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N having $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ given by the equation

$$y^2 = x^3 + Ax^2 + Bx \tag{1}$$

with $A, B \in \mathbb{Z}$. This curve has $\Delta = 16B^2(A^2 - 4B)$, $c_4 = 16(A^2 - 3B)$, $c_6 = 32A(-2A^2 + 9B)$ and has a 2-torsion point $(0, 0)$. Let d be 1 or a negative

square-free integer such that the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ satisfies the Heegner hypothesis: each prime divisor of N splits in K. Assume that the Heegner point P_K in $E(K)$ has infinite order. So the rank of $E(K)$ is 1 and $\mathrm{III}(E/K)$ is finite (cf. [7]).

In this section, we give some sufficient conditions for the divisibility $2 \mid |\mathrm{III}(E/K)|^{1/2}$. For each prime p (including ∞) of $\mathbb{Q}$, we define

$$i_p = \dim_{\mathbb{F}_2} E(\mathbb{Q}_p)/N_{K_\mathfrak{p}/\mathbb{Q}_p}(E(K_\mathfrak{p})),$$

where $K_\mathfrak{p}$ is the completion of K with respect to a prime $\mathfrak{p}$ lying over p and $N_{K_\mathfrak{p}/\mathbb{Q}_p}$ is the usual norm map. Let

$$\mathrm{Sel}^2(E/\mathbb{Q}) = \ker\Big(H^1(\mathbb{Q}, E[2]) \to \prod_p H^1(\mathbb{Q}_p, E)\Big)$$

be the 2-Selmer group. Let E_d be the quadratic twist of E with respect to d given by the equation $y^2 = x^3 + dAx^2 + d^2Bx$. Note that we can identify $E[2]$ with $E_d[2]$ and hence $H^1(\mathbb{Q}, E[2])$ with $H^1(\mathbb{Q}, E_d[2])$ via the Galois isomorphism $E[2] \to E_d[2]$ defined by $(t, 0) \mapsto (dt, 0)$. Now write

$$\Phi = \mathrm{Sel}^2(E/\mathbb{Q}) \bigcap \mathrm{Sel}^2(E_d/\mathbb{Q}) \tag{2}$$

(intersection taken inside $H^1(\mathbb{Q}, E[2]) \cong H^1(\mathbb{Q}, E_d[2])$). Note that originally the definition of the group Φ is different from (2) (for the original definition, see discussions just above [8, Theorem 1]). However, once we identify $E[2]$ with $E_d[2]$ as above, Φ can be given as in (2) (cf. [8, Proposition 7]).

Proposition 2.1. *Under the assumption of Conjecture 1.1, if*

$$\sum i_p + \dim_{\mathbb{F}_2} \Phi \geq 4,$$

where the sum is taken over all primes (including ∞), then $2 \mid |\mathrm{III}(E/K)|^{1/2}$.

Proof. By [8, Theorem 1], we have

$$\begin{aligned} \dim_{\mathbb{F}_2} \mathrm{III}(E/K)[2] &\geq \sum i_p + \dim_{\mathbb{F}_2} \Phi - \operatorname{rank} E(K) - 2\dim_{\mathbb{F}_2} E(\mathbb{Q})[2] \\ &\geq \sum i_p + \dim_{\mathbb{F}_2} \Phi - 3 \geq 1 \end{aligned}$$

since $\operatorname{rank} E(K) = \dim_{\mathbb{F}_2} E(\mathbb{Q})[2] = 1$. Because $\mathrm{III}(E/K)$ is finite, its order is a square, so $2 \mid |\mathrm{III}(E/K)|^{1/2}$ follows. □

Using the following proposition due to Kramer [8], we can compute i_p.

Proposition 2.2. *Let $\Delta_{\min}$ be the minimal discriminant of E.*

(i) $i_\infty = \begin{cases} 1 & \text{if } \Delta_{\min} > 0, \\ 0 & \text{if } \Delta_{\min} < 0. \end{cases}$

(ii) *If the prime 2 is ramified in K and E has ordinary good reduction modulo 2, then*

$$i_2 = \begin{cases} 2 & \text{if } (\Delta_{\min}, d)_{\mathbb{Q}_2} = +1, \\ 1 & \text{if } (\Delta_{\min}, d)_{\mathbb{Q}_2} = -1, \end{cases}$$

where $(-,-)_{\mathbb{Q}_2}$ *denotes the Hilbert norm-residue symbol.*

(iii) *If an odd prime* p *is ramified in* K *and* E *has good reduction modulo* p*, then*

$$i_p = \begin{cases} 2 & \text{if } (\frac{\Delta_{\min}}{p}) = +1, \\ 1 & \text{if } (\frac{\Delta_{\min}}{p}) = -1, \end{cases}$$

where $(\frac{\cdot}{\cdot})$ *denotes the Legendre symbol.*

Proof. It follows from [8, Propositions 3, 5, and 6]. □

Corollary 2.3. *Under the assumption of Conjecture 1.1, if* E *has positive minimal discriminant and there are at least* 3 *odd prime divisors in* d*, then we have* $\sum i_p \geq 4$*, so* $2 \mid |Ш(E/K)|^{1/2}$.

Proof. By Proposition 2.2(i), we have $i_\infty = 1$. Let p be an odd prime dividing d. By the Heegner hypothesis, E has good reduction modulo p. So $i_p \geq 1$ by Proposition 2.2(iii). Now the corollary follows from Proposition 2.1. □

Let $\phi : E \to E'$ be the isogeny with kernel $E[\phi] = E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and

$$\mathrm{Sel}^{\phi}(E/\mathbb{Q}) = \ker\Big(H^1(\mathbb{Q}, E[\phi]) \to \prod_p H^1(\mathbb{Q}_p, E)\Big)$$

the ϕ-Selmer group. Similarly, let us denote by $\phi_d : E_d \to E'_d$ the isogeny with kernel $E_d[\phi_d] = E_d(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Recall that we have identified the Galois modules $E[2]$ and $E_d[2]$, under which we also have $E[\phi] = E_d[\phi_d]$.

Proposition 2.4. *Let* G *be the subgroup of* $\mathbb{Q}^\times/{\mathbb{Q}^\times}^2 = H^1(\mathbb{Q}, E_d[\phi_d])$ *generated by the class of* $A^2 - 4B$*. Then* G *is the kernel of the homomorphism* $H^1(\mathbb{Q}, E_d[\phi_d]) \to H^1(\mathbb{Q}, E_d[2])$*. Thus,*

$$\ker\Big(\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q}) \to \mathrm{Sel}^{2}(E_d/\mathbb{Q})\Big) = G \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q}).$$

Proof. Consider the long exact sequence of cohomology groups:

$$\begin{aligned} 0 \to & E_d(\mathbb{Q})[\phi_d] \to E_d(\mathbb{Q})[2] \to E'_d(\mathbb{Q})[\phi'_d] \\ & \xrightarrow{\delta} H^1(\mathbb{Q}, E_d[\phi_d]) \to H^1(\mathbb{Q}, E_d[2]) \to H^1(\mathbb{Q}, E'_d[\phi'_d]) \to \cdots, \end{aligned}$$

where $\phi'_d : E'_d \to E_d$ is the dual isogeny of ϕ_d. Because the map $E_d(\mathbb{Q})[2] \to E'_d(\mathbb{Q})[\phi'_d]$ is the zero map, $\delta : E'_d(\mathbb{Q})[\phi'_d] \to H^1(\mathbb{Q}, E_d[\phi_d])$ is injective and the image $\delta(E'_d(\mathbb{Q})[\phi'_d])$ is the kernel of $H^1(\mathbb{Q}, E_d[\phi_d]) \to H^1(\mathbb{Q}, E_d[2])$.

We claim that this kernel is equal to G. Write $E_d[2] = \{O, P, Q, P+Q\}$, where O is the identity of E_d and $P \in E_d(\mathbb{Q})$, and similarly write $E'_d[\phi'_d] = \{O', T\}$, where O' is the identity of E'_d and $T \in E'_d(\mathbb{Q})$. Since $E_d[2] \to E'_d[\phi'_d]$ is surjective but $E_d(\mathbb{Q})[2] \to E'_d(\mathbb{Q})[\phi'_d]$ is the zero map, the point Q is mapped onto T under $E_d[2] \to E'_d[\phi'_d]$. Then, $\delta(T) \in H^1(\mathbb{Q}, E_d[\phi_d])$ is defined by the 1-cocyle

$$\sigma \mapsto \sigma(Q) - Q = \begin{cases} P & \text{if } \sigma(Q) = P + Q \neq Q, \\ 0 & \text{if } \sigma(Q) = Q. \end{cases}$$

However, this 1-cocycle corresponds to the 1-cocycle $\sigma \mapsto \sigma(\sqrt{b})/\sqrt{b}$ defining an element in $H^1(\mathbb{Q}, \mu_2)$, where $b = d^2(A^2 - 4B)$. The point Q corresponds to the point $\left(\frac{-A \pm d\sqrt{A^2-4B}}{2}, 0\right)$, so $\sigma(Q) = Q$ if and only if $\sigma\left(\sqrt{A^2 - 4B}\right) = \sqrt{A^2 - 4B}$. Clearly the 1-cocycle $\sigma \mapsto \frac{\sigma(\sqrt{A^2-4B})}{\sqrt{A^2-4B}}$ defining an element in $H^1(\mathbb{Q}, \mu_2)$ corresponds to $A^2 - 4B$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. □

From Proposition 2.4, if we find $b \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ such that $b \in \mathrm{Sel}^\phi(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ and check $b \notin G$, then we know that the image of b is a non-trivial element of Φ.

3. Proof of Theorem 1.2

First we give the proof of Theorem 1.2. Lemmas and propositions, which are used to prove Theorem 1.2, are stated and proved below the proof of Theorem 1.2.

Proof of Theorem 1.2. For an elliptic curve E defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z}$, we can find a Weierstrass model given by the equation (1) with $A, B \in \mathbb{Z}$. Note that A and B are not necessarily relatively prime. But if p is a prime dividing both A and B, then a simple change of variables guarantees that we have either $\mathrm{ord}_p A < 2$ or $\mathrm{ord}_p B < 4$. From Lemma 3.1(i), (ii), we may assume $B \in \{1, -1, 16, -16\}$ and from Lemma 3.1(iii), we may assume if p is an odd prime dividing $A^2 - 4B$, then $\mathrm{ord}_p(A^2 - 4B)$ is odd.

Suppose first that $B = 1$. When $A = 0, 1$ or -1, the corresponding curves are '64a4', '48a4' and '24a4'. First two curves have $c = 2$ and the last one has $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/4\mathbb{Z}$ (cf. [4]). So we may assume $A^2 - 4 > 0$. Suppose first that E has good reduction modulo 2. From Lemma 3.2(i), this is possible if and only if $\mathrm{ord}_2(A + 2) = 6$. If $A^2 - 4$ has at most one odd prime divisor, then $|A + 2| = 64$, hence $A \in \{-66, 62\}$. Ruling out the curve with $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/4\mathbb{Z}$ ($A = 62$), we have the curve '17a3' with $c = 2$ (cf. [4]). Thus we may assume the conditions of Proposition 3.3 and have $2 \mid c \cdot m \cdot u_K \cdot |\mathrm{Ш}(E/K)|^{1/2}$ in any case.

Now suppose that $B = 1$ with $A^2 - 4 > 0$ and E has bad reduction modulo 2. From Lemma 3.2(ii), we may assume that $s = 0$ with $A \equiv 1 \pmod 4$; $s = 1$; $s = 2$ with $A \equiv 10 \pmod{16}$ or $s \geq 5$ odd, where $s = \mathrm{ord}_2(A + 2)$. Suppose first that A is even, i.e., $s \geq 1$. If $A^2 - 4$ has no odd prime divisor, then $A + 2 = \pm 2^s$ with $|A - 2| = |\pm 2^s - 4|$ being a power of 2 as well; this is possible only if $A \in \{-6, 0, 6\}$. The case $A = 0$ is already excluded, the case $A = 6$ gives the curve '32a4' with $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/4\mathbb{Z}$ and the case $A = -6$ gives the curve '32a3' with $c = 2$ (cf. [4]). Now suppose that A is odd, i.e., $s = 0$ and $A \equiv 1 \pmod 4$. If $A^2 - 4$ has at most one odd prime divisor, then either $|A - 2| = 1$ or $|A + 2| = 1$, hence $A \in \{\pm 1, \pm 3\}$. Ruling out the already excluded cases and the case with $A \not\equiv 1 \pmod 4$, the case $A = -3$ solely remains. But this gives

the curve '80a2' with $c = 2$ (cf. [4]). Thus we may assume the conditions of Proposition 3.4 and have $2 \mid c \cdot m \cdot u_K \cdot |\text{Ш}(E/K)|^{1/2}$ in any case.

Suppose that $B = -1$. From Lemma 3.2(iii), we may assume $A \equiv 1, 2$ or 3 (mod 4). If $A \equiv 2 \pmod 4$, then write $A = 2A'$ for some odd A' and so $A^2 + 4 = 4(A'^2 + 1)$. This has no odd prime divisor if and only if $A'^2 + 1$ is a power of 2. By Mihailescu's theorem (cf. [11]), this is possible only if $A' = \pm 1$, i.e., $A = \pm 2$. These correspond to the curves '128b2' and '128d2', each with $c = 2$ (cf. [4]). If A is odd and $A^2 + 4 = p^k$ for some odd prime p and $k > 1$, then Nagell's theorem (cf. [3, Lemma 5.4]) forces that $A = 11$, $p = 5$ and $k = 3$, which corresponds to the curve '80b4' with $c = 2$ (cf. [4]). If $A^2 + 4 = p$ for some odd prime p, then these curves correspond to the curves in the family $\mathcal{F}_1$. Thus we may assume the conditions of Proposition 3.5 and have $2 \mid c \cdot m \cdot u_K \cdot |\text{Ш}(E/K)|^{1/2}$ in any case.

Suppose $B = 16$. If $A \equiv 0 \pmod 4$, then we can make a change of variables to (1) to reduce the 2-divisibility of A and B. Also in view of Lemma 3.2(iv), we may assume $A \equiv 1 \pmod 4$. Suppose moreover that $|A| \leq 9$, i.e., $A = -7, -3, 1, 5, 9$. Ruling out the curves with $E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/4\mathbb{Z}$ ($A = -7, 1$ and 9), we have two curves '39a4' and '55a4', each with $c = 2$ (cf. [4]). Hence we assume $A^2 - 64 > 0$. Moreover, since $\{A : |A - 8| = 1 \text{ or } |A + 8| = 1\} = \{\pm 7, \pm 9\}$, we also exclude these cases. Thus we may assume the conditions of Proposition 3.6 and have $2 \mid c \cdot m \cdot u_K \cdot |\text{Ш}(E/K)|^{1/2}$ in any case.

Finally, suppose $B = -16$. Similarly, we assume $A \equiv 1 \pmod 4$ as before. If $A^2 + 64 = p^k$ for some odd prime p and some $k > 1$, then [3, Lemma 5.5] forces that $A = \pm 15$, $p = 17$ and $k = 2$, which correspond to the curves '17a2' and '272b2', each with $E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (cf. [4]). If $A^2 + 64 = p$ for some odd prime p, then these curves correspond to the Neumann–Setzer curves having étale isogenies of degree 2 to the $X_0(p)$-optimal curves in their rational isogeny classes (cf. [13]) and have $c = 2$ by Lemma 5.1. Thus we may assume the conditions of Proposition 3.7 and have $2 \mid c \cdot m \cdot u_K \cdot |\text{Ш}(E/K)|^{1/2}$ in any case. □

Lemma 3.1. *Let E be an elliptic curve defined by the equation* (1).

(i) *Let p be a prime dividing both A and B and assume either* $\text{ord}_p A < 2$ *or* $\text{ord}_p B < 4$. *Then* $2 \mid m_p$.

(ii) *If p is a prime dividing B but not A, then $2 \mid m_p$ unless $p = 2$ with $A \equiv 1 \pmod 4$ and* $\text{ord}_2 B = 4$.

(iii) *If p is an odd prime such that* $\text{ord}_p(A^2 - 4B)$ *is even, then* $2 \mid m_p$.

Proof. (i) By Tate's algorithm, we see that E has reduction modulo p of type III, III*, or I_k^* for some k, all with even m_p.

(ii) If p is odd, then $\text{ord}_p c_4 = 0$ and $\text{ord}_p \Delta = 2\text{ord}_p B$, and hence E has multiplicative reduction modulo p of type $\text{I}_{2\text{ord}_p B}$. In particular, m_p is even. Suppose $p = 2$. Note that the equation

$$y^2 + 2xy = x^3 + (A - 1)x^2 + Bx$$

gives another Weierstrass model of the curve given by (1). If $\mathrm{ord}_2 B \geq 4$ and $A \equiv 1 \pmod 4$, we further reduce the equation into the form

$$y^2 + xy = x^3 + \frac{A-1}{4}x^2 + \frac{B}{16}x,$$

which has $\mathrm{ord}_2\Delta = 2\mathrm{ord}_2 B - 8$ and $\mathrm{ord}_2 c_4 = 0$. Hence in this case, m_2 is also even unless $\mathrm{ord}_2 B = 4$. When $1 \leq \mathrm{ord}_2 B \leq 3$ or $A \equiv 3 \pmod 4$, applying Tate's algorithm we see E has reduction of type III, III*, or I_k^* for some k as above.

(iii) From (i), we may assume $p \nmid AB$. In this case, E has reduction of type $\mathrm{I}_{\mathrm{ord}_p(A^2-4B)}$, and the parity of m_p and $\mathrm{ord}_p(A^2-4B)$ is the same. □

Lemma 3.2. *Let E be an elliptic curve defined by the equation* (1). *Write $s = \mathrm{ord}_2(A+2)$.*

(i) *Let $B = 1$. Then E has good reduction modulo* 2 *if and only if $s = 6$.*

(ii) *Let $B = 1$. Then E has bad reduction modulo* 2 *and m_2 is odd if and only if $s = 0$ with $A \equiv 1 \pmod 4$, $s = 1$, $s = 2$ with $A \equiv 10 \pmod{16}$ or $s \geq 5$ odd.*

(iii) *Let $B = -1$. If $A \equiv 0 \pmod 4$, then $m_2 = 2$.*

(iv) *Let $B = \pm 16$. If $A \equiv 2$ or $3 \pmod 4$, then $2 \mid m_2$.*

Proof. (i) and (ii). $s = 0$ if and only if A is odd. In this case, changing variables we have the equation:

$$y^2 + 2y = x^3 + (A+3)x^2 + 2(A+2)x + (A+1).$$

In this case, Tate algorithm tells us that if $A \equiv 1 \pmod 4$, then E has reduction of type II with $m_2 = 1$, and if $A \equiv -1 \pmod 4$, then E has reduction of type III with $m_2 = 2$.

Now assume A is even. If $s \geq 6$, then make a change of variables:

$$y^2 + xy = x^3 + 2^{-2}(A+2)x^2 + 2^{-3}(A+2)x + 2^{-6}(A+2).$$

This equation is minimal at 2 since $c_4 = A^2 - 3$ is odd. As the discriminant is $2^{-8}(A-2)(A+2)$, with 2-adic order $s-6$, in this case E has good reduction modulo 2 if and only if $s = 6$ and multiplicative reduction of type I_{s-6} when $s \geq 7$.

Finally, let $1 \leq s \leq 5$; we can make a change of variables:

$$y^2 + 2xy = x^3 + (A+2)x^2 + 2(A+2)x + (A+2).$$

Tate's algorithm shows that

- when $s = 1$, E has reduction of type II with $m_2 = 1$;
- when $s = 2$, E has reduction of type I_n^* for some n, and we have odd m_2 if and only if $A \equiv 10 \pmod{16}$;
- when $s = 3$, E has reduction of type I_0^* with $m_2 = 2$;
- when $s = 4$, E has reduction of type III* with $m_2 = 2$;
- finally, when $s = 5$, E has reduction of type II* with $m_2 = 1$.

(iii) and (iv) are also obtained by similar arguments. □

Proposition 3.3 ($B = 1$ and E has good reduction modulo 2)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (1) *with $B = 1$. Suppose*

- $A^2 - 4 > 0$,
- *if p is an odd prime dividing $A^2 - 4$, then* $\mathrm{ord}_p(A^2 - 4)$ *is odd,*
- *there are at least two distinct odd prime divisors in $A^2 - 4$, and*
- *E has good reduction modulo* 2.

Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.

Proof. In this case, we have $\mathrm{ord}_2(A + 2) = 6$ by Lemma 3.2(i). The equation (1) with $B = 1$ has $\Delta = 16(A^2 - 4) > 0$ and $\Delta_{\min} = 2^{-8}(A^2 - 4)$. We note that E has ordinary good reduction modulo 2.

First we compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$. For each prime p (including ∞), we denote by δ_p the map $E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \to H^1(\mathbb{Q}_p, E[\phi])$. Since $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[\phi]) \cong \mathbb{Q}^\times/{\mathbb{Q}^\times}^2$, the elements of $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$ are those classes of $b \in \mathbb{Q}^\times$ such that for each prime p (including ∞) of $\mathbb{Q}$, the restriction $b \in H^1(\mathbb{Q}_p, E[\phi]) \cong \mathbb{Q}_p^\times/{\mathbb{Q}_p^\times}^2$ is contained in the image $\mathrm{Im}\,\delta_p$. Using the method in [5], we can compute these local images as follows.

- $\mathrm{Im}\,\delta_\infty \supseteq \{1\}$.
- $\mathrm{Im}\,\delta_p = \mathbb{Q}_p^\times/{\mathbb{Q}_p^\times}^2$ for odd primes $p \mid \Delta$ such that $\mathrm{ord}_p\Delta$ is odd.
- $\mathrm{Im}\,\delta_p \supseteq \mathbb{Z}_p^\times{\mathbb{Q}_p^\times}^2/{\mathbb{Q}_p^\times}^2$ for other odd primes p.
- $\mathrm{Im}\,\delta_2 = \mathbb{Z}_2^\times{\mathbb{Q}_2^\times}^2/{\mathbb{Q}_2^\times}^2$.

So in particular, $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$ contains odd primes $p \mid \Delta$ with $\mathrm{ord}_p\Delta$ being odd in $\mathbb{Q}^\times/{\mathbb{Q}^\times}^2$.

Note that $\Delta_{\min} > 0$, i.e., $i_\infty = 1$ by Proposition 2.2(i). By the fact that $u_K = 2$ if $d = -1$ and Corollary 2.3, we only need to concern about the cases $d = -2$, $d = -q$, $-2q$ or $-qq'$ for some odd primes q and q'.

Assume that $d = -2$. If p is an odd prime dividing Δ, then $(\frac{-2}{p}) = 1$ by the Heegner hypothesis, so $p \equiv 1$ or $-5 \pmod 8$. This implies $(p, -2)_{\mathbb{Q}_2} = 1$. So $(\Delta_{\min}, d)_{\mathbb{Q}_2} = 1$ and we have $i_2 = 2$ by Proposition 2.2(ii). Thus $i_\infty + i_2 = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows: $\mathrm{Im}\,\delta_\infty^d \supseteq \{1\}$; $\mathrm{Im}\,\delta_p^d$ are the same as in $\mathrm{Im}\,\delta_p$ for odd primes p and $\mathrm{Im}\,\delta_2^d \supseteq \{1, 2, -5, -10\}$. If in particular, we let p be an odd prime such that $p \mid \Delta$ and $\mathrm{ord}_p\Delta$ is odd, then the image of $p \in \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4 (note that $\ker(\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \to \mathrm{Sel}^2(E/\mathbb{Q}))$ and $\ker(\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q}) \to \mathrm{Sel}^2(E_d/\mathbb{Q}))$ are generated by the class of $A^2 - 4$ and the existence of another odd prime dividing Δ in an odd power guarantees that the class of p does not vanish in the 2-Selmer group), so $\dim_{\mathbb{F}_2}\Phi \geq 1$. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d = -q$ with a prime $q \equiv 1 \pmod 4$, then $d \equiv -1 \pmod 4$. In this case, the prime 2 is ramified in K and we have $i_2 \geq 1$ by Proposition 2.2(ii). Because $i_\infty = 1$, we may assume $i_q = 1$, i.e., $(\frac{\Delta_{\min}}{q}) = -1$ by Proposition

2.2(iii). Thus $i_\infty+i_2+i_q \geq 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows: $\mathrm{Im}\,\delta_\infty^d \supseteq \{1\}$; $\mathrm{Im}\,\delta_p^d$ are the same as in $\mathrm{Im}\,\delta_p$ for odd primes p and $\mathrm{Im}\,\delta_2^d = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$. Thus the image of any odd prime $p \mid \Delta$ with $\mathrm{ord}_p\Delta$ being odd in $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a nontrivial element of Φ by Proposition 2.4, so $\dim_{\mathbb{F}_2}\Phi \geq 1$. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

Assume $d=-q$ with a prime $q \equiv 3 \pmod 4$, then $d \equiv 1 \pmod 4$. If p is an odd prime dividing Δ, then $(\frac{-q}{p}) = (\frac{-1}{p})(-1)^{\frac{q-1}{2}\frac{p-1}{2}}(\frac{p}{q}) = (\frac{p}{q}) = 1$ by the Heegner hypothesis, so $(\frac{\Delta_{\min}}{q}) = 1$, i.e., $i_q = 2$ by Proposition 2.2(iii). Thus $i_\infty + i_q = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows: $\mathrm{Im}\,\delta_q^d \supseteq \{1, qu\}$ for some representative u with $(\frac{u}{q}) = -1$; $\mathrm{Im}\delta_2^d = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ and the rest are the same. We note that if $p \mid \Delta$ is an odd prime, then $p \in \mathrm{Im}\,\delta_q^d$ because $(\frac{p}{q}) = 1$. Thus the image of any odd prime $p \mid \Delta$ with $\mathrm{ord}_p\Delta$ being odd in $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a nontrivial element of Φ by Proposition 2.4, so $\dim_{\mathbb{F}_2}\Phi \geq 1$. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d=-2q$ for some odd prime q. In this case, the prime 2 is ramified in K and we have $i_2 \geq 1$ by Proposition 2.2(ii). Because $i_\infty = 1$, we may assume $i_q = 1$, i.e., $(\frac{\Delta_{\min}}{q}) = -1$ by Proposition 2.2(iii). Thus $i_\infty + i_2 + i_q \geq 3$. Write $c = A^2 - 4$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows: $\mathrm{Im}\,\delta_q^d \supseteq \{1, qu\}$ for some representative u with $(\frac{u}{q}) = -1$;

$$\mathrm{Im}\,\delta_2^d = \begin{cases} \langle 2, -5, c\rangle & \text{when } q \equiv 1 \pmod 8, \\ \langle -1, 2, c\rangle & \text{when } q \equiv -1 \pmod 8, \\ \langle -2, -5, c\rangle & \text{when } q \equiv 5 \pmod 8, \\ \langle -1, 10, c\rangle & \text{when } q \equiv -5 \pmod 8; \end{cases}$$

and the rest are the same. Now we are going to do some case-by-case study. We note that $c = A^2 - 4$ is exactly divisible by 2^8. Let $c' = 2^{-8}c = \Delta_{\min}$.

- Suppose that $q \equiv 1 \pmod 8$. Then $d = -2$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.
  - If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\mathrm{Im}\,\delta_2^d = \langle 2, -5, -1\rangle = \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.
  - If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\mathrm{Im}\,\delta_2^d = \langle 2, -5, 5\rangle = \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.
  - If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
- Suppose that $q \equiv -1 \pmod 8$. Then $d = 2$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.

  - If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -1, 2, 5\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -1, 2, -5\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.

- Suppose that $q \equiv 5 \pmod 8$. Then $d = -10$ in $\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -2, -5, -1\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -2, -5, 5\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.

- Suppose that $q \equiv -5 \pmod 8$. Then $d = 10$ in $\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_p \geq 4$.
  - If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -1, 10, 5\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.
  - If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbb{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_p \geq 3$. In this case, $\operatorname{Im}\delta_2^d = \langle -1, 10, -5\rangle = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$.

Having these discussions, we can conclude that we have either $\sum i_p \geq 4$ or $\sum i_p \geq 3$ and $\operatorname{Im}\delta_2^d = \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2$. Suppose the latter. Let $\{p_1, \cdots, p_n\}$ be the set of all odd prime divisors $p_i \mid \Delta$ such that $\operatorname{ord}_{p_i}\Delta$ is odd. As $(\frac{p_1}{q})\cdots(\frac{p_n}{q}) = (\frac{\Delta_{\min}}{q}) = -1$, either we can find an $\lambda = p_i$ such that $(\frac{p_i}{q}) = 1$ or $(\frac{p_i}{q}) = -1$ for all i and n is odd. In the latter case, because $n \geq 3$, we take the product of two such primes $\lambda = p_i p_j$ with $i \neq j$. Then the image of $\lambda \in \operatorname{Sel}^\phi(E/\mathbb{Q}) \cap \operatorname{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4, so $\dim_{\mathbb{F}_2}\Phi \geq 1$. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

Finally, assume $d = -qq'$. If the prime 2 is ramified in $K = \mathbb{Q}(\sqrt{d})$, then we have $\sum i_p \geq 4$. Hence we may assume the prime 2 is unramified, which means that $d \equiv 1 \pmod 4$. Without loss of generality, we then assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover we further assume $i_q = i_{q'} = 1$, i.e., $(\frac{\Delta_{\min}}{q}) = (\frac{\Delta_{\min}}{q'}) = -1$ by Proposition 2.2(iii). Thus $i_\infty + i_q + i_{q'} = 3$. Now we consider the Selmer group $\operatorname{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows: $\operatorname{Im}\delta_q^d \supseteq \{1, qu\}$ for some representative u with $(\frac{u}{q}) = -1$; $\operatorname{Im}\delta_{q'}^d = \mathbb{Q}_{q'}^\times/{\mathbb{Q}_{q'}^\times}^2$;

$\operatorname{Im}\delta_2^d = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ and the rest are the same. If we take λ as above, then the image of $\lambda \in \mathrm{Sel}^\phi(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4, so $\dim_{\mathbb{F}_2}\Phi \geq 1$. Hence we have $\sum i_p + \dim_{\mathbf{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof. □

Proposition 3.4 ($B = 1$ and E has bad reduction modulo 2)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (1) *with $B = 1$. Write $s = \mathrm{ord}_2(A+2)$. Suppose*

- $A^2 - 4 > 0$,
- *if p is an odd prime dividing $A^2 - 4$, then $\mathrm{ord}_p(A^2-4)$ is odd,*
- *there is at least one odd prime divisor in $A^2 - 4$ if A is even and there are at least two distinct odd prime divisors in $A^2 - 4$ if A is odd,*
- *E has bad reduction modulo 2, and*
- *either one of the following holds: $s = 0$ and $A \equiv 1 \pmod 4$, $s = 2$ and $A \equiv 10 \pmod{16}$, or $s = 1, 4, 5$ or $s \geq 7$.*

(*In particular, all the cases where m_2 is odd (cf. Lemma 3.2) are contained in the last condition.*) *Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.*

Proof. First we consider the Selmer group $\mathrm{Sel}^\phi(E/\mathbb{Q})$. The local images are given as follows:

- $\operatorname{Im}\delta_\infty \supseteq \{1\}$.
- $\operatorname{Im}\delta_p = \mathbb{Q}_l^\times/{\mathbb{Q}_l^\times}^2$ for odd primes $p \mid \Delta$ such that $\mathrm{ord}_p(\Delta)$ is odd.
- $\operatorname{Im}\delta_p \supseteq \mathbb{Z}_\ell^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$ for other odd primes p.
- $\operatorname{Im}\delta_2 = \begin{cases} \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & \text{if } A \equiv 1 \pmod 4, \\ \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & \text{otherwise.} \end{cases}$

Since E has bad reduction modulo 2, the prime 2 splits completely in K by the Heegner hypothesis, and so we have $d \equiv 1 \pmod 8$. From Corollary 3.3 and by this fact, we only need to deal with the cases where $d = -q$ for some odd prime q ($q \equiv -1 \pmod 8$) or $d = -qq'$ for distinct odd primes q and q' with either $(q, q') \equiv (1, -1) \pmod 8$ or $(q, q') \equiv (5, -5) \pmod 8$ without loss of generality.

In both cases, we can prove that the images $\operatorname{Im}\delta_p^d$ are the same as the proof of Proposition 3.3 and $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ by the same argument as the proof of Proposition 3.3. We omit the detail. □

Proposition 3.5 ($B = -1$)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (1) *with $B = -1$. Suppose*

- *$A \equiv 1, 2$ or $3 \pmod 4$,*
- *if p is an odd prime dividing $A^2 + 4$, then $\mathrm{ord}_p(A^2+4)$ is odd, and*
- *there is at least one odd prime divisors in $A^2 + 4$ if $A \equiv 2 \pmod 4$ and there are at least two distinct odd prime divisors in $A^2 + 4$ if A is odd.*

Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.

Proof. The elliptic curve E given by the equation (1) with $B = -1$, i.e., $y^2 = x^3 + Ax^2 - 1$ has $\Delta = 2^4(A^2+4)$ and $c_4 = 2^4(A^2+3)$. We note that this equation is minimal for each prime. By Fermat's theorem of the sums of two squares, we have $p \equiv 1 \pmod 4$ for odd primes $p \mid (A^2+4)$.

First we compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$. The local images are given as follows:

- $\mathrm{Im}\,\delta_\infty \supseteq \{1\}$.
- $\mathrm{Im}\,\delta_p = \mathbb{Q}_l^\times/{\mathbb{Q}_l^\times}^2$ for odd primes $p \mid \Delta$.
- $\mathrm{Im}\,\delta_p = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$ for other odd primes p.
- $\mathrm{Im}\,\delta_2 = \begin{cases} \{1,5\} & \text{if } A \equiv 1,3 \pmod 4, \\ \{1,2,5,10\} & \text{if } A \equiv 2 \pmod 4. \end{cases}$

So $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$ in $\mathbb{Q}^\times/{\mathbb{Q}^\times}^2$ contains odd primes $p \mid \Delta$ because they all have $p \equiv 1 \pmod 4$, together with 2 whenever A is even.

Note that $\Delta_{\min} > 0$, i.e., $i_\infty = 1$ by Proposition 2.2(i). Since E has bad reduction modulo 2, the prime 2 splits completely in K by the Heegner hypothesis, and so we have $d \equiv 1 \pmod 8$. From Corollary 3.3 and by this fact, we only need to deal with the cases where $d = -q$ for some odd prime q ($q \equiv -1 \pmod 8$) or $d = -qq'$ for distinct odd primes q and q' with either $(q, q') \equiv (1, -1) \pmod 8$ or $(q, q') \equiv (5, -5) \pmod 8$ without loss of generality.

Assume that $d = -q$ with $q \equiv -1 \pmod 8$. If p is an odd prime dividing Δ, then $(\frac{p}{q}) = (\frac{-q}{p}) = 1$ by the Heegner hypothesis. From this, we have $(\frac{A^2+4}{q}) = 1$ for any cases of A. This implies $i_q = 2$ by Proposition 2.2(iii). Thus $i_\infty + i_q = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images $\mathrm{Im}\,\delta_p^d$ are the same as $\mathrm{Im}\,\delta_p$, except when $p = q$, we have $\mathrm{Im}\,\delta_q^d = \{1\}$. If $A \equiv 2 \pmod 4$, then $\mathrm{ord}_2(A^2+4) = 3$. Note that 2 is a square modulo q. Thus the image of $2 \in \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4. If $A \equiv 1$ or $3 \pmod 4$, then the image of any one of odd prime divisors of A^2+4 in $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d = -qq'$ with for distinct odd primes q and q' such that either $(q, q') \equiv (1, -1) \pmod 8$ or $(q, q') \equiv (5, -5) \pmod 8$. We may assume that $i_q = i_{q'} = 1$, i.e., $(\frac{A^2+4}{q}) = (\frac{A^2+4}{q'}) = -1$ by Proposition 2.2(iii). Thus $i_\infty + i_q + i_{q'} = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local image $\mathrm{Im}\,\delta_p^d$ are the same as the local image $\mathrm{Im}\delta_p$, except when $p = q$, $\mathrm{Im}\,\delta_q^d = \mathbb{Q}_q^\times/\mathbb{Q}_q^\times$. As above, if $A \equiv 2 \pmod 4$, then the image of 2 is a non-trivial element of Φ and if $A \equiv 1$ or $3 \pmod 4$, then the image of any one of odd prime divisors of A^2+4 is a non-trivial element of Φ. Hence we have $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof. □

Proposition 3.6 ($B = 16$)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (1) *with $B = 16$. Suppose*

- $A \equiv 1 \pmod 4$,
- $A^2 - 64 > 0$,
- *if p is an odd prime dividing $A^2 - 64$, then* $\mathrm{ord}_p(A^2 - 64)$ *is odd, and*
- *there is an odd prime divisor in each of $A - 8$ and $A + 8$.*

Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.

Proof. The elliptic curve E is given by the equation (1) with $B = 16$, i.e., $y^2 = x^3 + Ax^2 + 16x$ has $\Delta = 2^{12}(A^2 - 64)$ and $c_4 = 2^4(A^2 - 48)$. We note that this equation is minimal for each prime $\neq 2$, indeed, the minimal discriminant of such E is $\Delta_{\min} = A^2 - 64 > 0$, which is odd. In particular, E has ordinary good reduction modulo 2.

First we compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbb{Q})$. The local images are given as follows:

- $\mathrm{Im}\,\delta_\infty \supseteq \{1\}$.
- $\mathrm{Im}\,\delta_p = \mathbb{Q}_p^\times/{\mathbb{Q}_p^\times}^2$ for odd primes $p \mid \Delta$.
- $\mathrm{Im}\,\delta_p = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$ for other odd primes p.
- $\mathrm{Im}\,\delta_2 = \{1, 5\}$.

Note that $\Delta_{\min} > 0$, i.e., $i_\infty = 1$ by Proposition 2.2(i). By the fact that $u_K = 2$ if $d = -1$ and Corollary 2.3, we only need to concern about the cases $d = -2$, $d = -q$, $-2q$ or $-qq'$ for some odd primes q and q'.

Assume that $d = -2$. As $(\Delta_{\min}, d)_{\mathbb{Q}_2} = \big(A^2 - 64, -2\big)_{\mathbb{Q}_2} = (1, -2)_{\mathbb{Q}_2} = 1$, we have $i_2 = 2$ by Proposition 2.2(ii). Thus $i_\infty + i_2 = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images $\mathrm{Im}\,\delta_p^d$ are the same as $\mathrm{Im}\,\delta_p$, except when $p = 2$, we can only say $\mathrm{Im}\delta_2^d \supseteq \{1\}$. If p is an odd prime dividing Δ, then $(\frac{-2}{p}) = 1$ by the Heegner hypothesis, so $p \equiv 1$ or $-5 \pmod 8$. But as $A \pm 8 \equiv 1$ or $5 \pmod 8$, either we can find an odd prime $p \mid \Delta$ such that $p \equiv 1 \pmod 8$, in which case we take $\lambda = p$, or all odd primes $p \mid \Delta$ have $p \equiv -5 \pmod 8$ and there are even number of odd prime divisors in each of $A - 8$ and $A+8$. In the latter case, we take λ as the product of any two odd prime divisors. Then the image of $\lambda \in \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of $Ш$ by Proposition 2.4. Hence we have $\sum i_p + \dim_{\mathbb{F}_2} Ш \geq 4$ and Proposition 2.1 concludes the proof.

For the remaining cases, we can also prove that $\sum i_p + \dim_{\mathbb{F}_2} Ш \geq 4$ by similar arguments. We omit the detail. □

Proposition 3.7 ($B = -16$)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (1) *with $B = -16$. Suppose*

- $A \equiv 1 \pmod 4$,
- *if p is an odd prime dividing $A^2 + 64$, then* $\mathrm{ord}_p(A^2 + 64)$ *is odd, and*
- *there are at least two odd prime divisors in $A^2 + 64$.*

Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.

Proof. In this case, we can also prove that $\sum i_p + \dim_{\mathbb{F}_2}\Phi \geq 4$ by arguments similar to the proof of previous propositions. We omit the detail. □

4. Proof of Theorem 1.3

First we give the proof of Theorem 1.3. Lemmas and propositions, which are used to prove Theorem 1.3, are stated and proved below the proof of Theorem 1.3.

Proof of Theorem 1.3. For an elliptic curve E defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/4\mathbb{Z}$, we can find a Weierstrass model given by the equation

$$y^2 + xy - \lambda y = x^3 - \lambda x^2 \tag{3}$$

with $\lambda \in \mathbb{Q}$ (cf. the proof of [9, Proposition 2.4]). This equation has $\Delta = \lambda^4(1+16\lambda)$, $c_4 = 16\lambda^2+16\lambda+1$, and $c_6 = 64\lambda^3-120\lambda^2-24\lambda-1$. By Lemma 4.1(i), we may assume $\lambda = 1/\beta$ for some $\beta \in \mathbb{Z}\setminus\{0,-16\}$. Using the change of variables $x \mapsto x/\beta^2$, $y \mapsto y/\beta^3$, we can transform the equation (3) into the following form

$$y^2 + \beta xy - \beta^2 y = x^3 - \beta x^2 \tag{4}$$

with $\Delta = \beta^7(\beta+16)$, $c_4 = \beta^2(\beta^2+16\beta+16)$, and $c_6 = -\beta^3(\beta^3+24\beta^2+120\beta-64)$.

Suppose first that β has no odd prime factor. If $\beta = \pm 1$, then E is isomorphic to either '15a8' or '17a4', having $c = 4$ (cf. [4]). Assume $\beta = 2^t$. In view of Lemma 4.2(iii), (iv), we only need to consider the cases with $\beta = 4$ or $\beta = 16$. But these two cases correspond to the curves '40a3' and '32a4' respectively, all with $m_2 = c = 2$ (cf. [4]). Now assume $\beta = -2^t$. Again, by Lemma 4.2(iii) we assume $t = 2z$ for some $z \geq 1$. Noting that $z = 1$ gives the curve '24a4' with $m_2 = c = 2$ (cf. [4]) and $z = 2$ gives a singular curve, we further reduce to the case $z \geq 3$. By Lemma 4.2(ii), (v), if $z = 3$ or $z \geq 5$, then we have $2 \mid m_2$ and if $z = 4$, then the curve becomes '15a7', having $c = 2$ (cf. [4]). Now in any case, we can transform the equation (4) into the form (1) with $A = 2^{2z-2} - 2$ and $B = 1$. Note that $A^2 - 4 = 2^{2z}(2^{2z-4}-1) = -2^{2z-4}(\beta+16)$ has at least two distinct odd prime divisor (3 and 5) in the case $z = 4$, and has at least one odd prime divisor when $z = 3$ or $z \geq 5$. By Lemma 4.3(ii), we may assume that if ℓ is an odd prime dividing $\beta+16$, then $\mathrm{ord}_\ell(\beta+16)$ is odd. Hence by Proposition 3.3 (when E has good reduction modulo 2 which is the case if and only if $z = 4$) and by Proposition 3.4 (when E has bad reduction modulo 2, i.e., when $z = 3$ or $z \geq 5$), we have $4 \mid c \cdot m \cdot u_K \cdot |Ш(E/K)|^{1/2}$.

Now assume β has an odd prime divisor. In view of Lemmas 4.2 and 4.3, we only need to consider, for an odd prime p, (i) $\beta = p^n$ with even n, (ii) $\beta = -p^n$ with even n and finally (iii) $\beta = -2^8p^n$ with even n, all with the assumption that for any odd prime $\ell \mid (\beta+16)$, $\mathrm{ord}_\ell(\beta+16)$ is odd. Note also that in any case $m_p = 2$.

Suppose first that $\beta = p^n$ with $n = 2z$ ($z \geq 1$). If $p^{2z} + 16 = \ell^k$ for another odd prime ℓ with $k > 1$ and $p \equiv 3 \pmod 4$, then [3, Lemma 5.5] forces that $p = 3$, $z = 1$, $\ell = 5$ and $k = 2$, which corresponds to the curve '15a3' having the rational torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ (cf. [4]). If $p^{2z} + 16 = \ell$ for another odd prime ℓ and $p \equiv 3 \pmod 4$, then these curves correspond to the curves in the family $\mathcal{F}_2$ (note that in this case, we can transform the equation (3) into $y^2 + p^z xy - p^z y = x^3 - x^2$ with $\Delta = p^{2z}\ell$, $c_4 = p^{4z} + 16p^{2z} + 1$, and $c_6 = -p^{6z} - 24p^{4z} - 120p^{2z} + 64$). Thus we may assume the conditions of Proposition 4.4 and have $4 \mid c \cdot m \cdot u_K \cdot |Ш(E/K)|^{1/2}$.

If $\beta = -p^n$, then we are done by Proposition 4.5, except possibly for two curves '15a3' and '21a4'. For the curve '21a4', we have $4 \mid c \cdot m$ (cf. [4]).

If $\beta = -2^8 p^n$ with $n = 2z$ ($z \geq 1$), then the equation is transformed into $y^2 = x^3 + Ax^2 + x$ with $A = 64p^{2z} - 2$. In this case E has good reduction modulo 2 and we have $A^2 - 4 = 2^8 p^{2z}(16p^{2z} - 1) = -2^4 p^{2z}(\beta + 16) > 0$ and it has at least two odd prime divisors ℓ such that $\mathrm{ord}_\ell(A^2 - 4)$ is odd. Hence Proposition 3.3 shows $4 \mid c \cdot m \cdot u_K \cdot |Ш(E/K)|^{1/2}$. □

Lemma 4.1. *Let E be an elliptic curve given by the equation* (3).

(i) *If p is a prime such that $\mathrm{ord}_p\lambda > 0$, then E_λ has split multiplicative reduction of type I_{4n}. So $4 \mid m_p$.*

(ii) *If p is an odd prime such that $\mathrm{ord}_p\lambda < 0$, then E_λ has potentially multiplicative reduction. It has multiplicative reduction if and only if $\mathrm{ord}_p\lambda$ is even.*

Proof. This is proved in the proof of [9, Proposition 2.4]. □

Lemma 4.2. *Let E be an elliptic curve given by the equation* (4) *with $\beta = 2^t u$ for some $t \geq 0$ and odd u.*

(i) *If $t = 0$, then $m_2 = 1$.*

(ii) *If $t = 8$ and $u \equiv -1 \pmod 4$, then $m_2 = 1$.*

(iii) *If t is odd, then $m_2 = 4$.*

(iv) *If $t = 2z$ with $z \geq 3$ and if $u \equiv 1 \pmod 4$, then $m_2 = 4$.*

(v) *For all the other cases for t, we have even m_2.*

Proof. All of the statements can be checked by Tate's algorithm. For more details, see the proof of [9, Proposition 2.4]. □

Lemma 4.3. *Let E be an elliptic curve given by the equation* (4).

(i) *If p is an odd prime dividing β, then $2 \mid m_p$. Moreover, $4 \mid m_p$ if $\mathrm{ord}_p\beta$ is odd.*

(ii) *If ℓ is an odd prime dividing $\beta + 16$, then E has multiplicative reduction modulo ℓ. So m_ℓ has the same parity as $\mathrm{ord}_\ell(\beta + 16)$.*

Proof. (i) The first statement was proved in the proof of [9, Proposition 2.4]. If $\mathrm{ord}_p\beta$ is odd, then E has additive reduction modulo p by Lemma 4.1(ii), and hence by [2, Lemma 2.1(i)] we have $4 \mid m_p$.

(ii) After a suitable change of variables, we see that E has multiplicative reduction of type $\mathrm{I}_{\mathrm{ord}_\ell(\beta+16)}$. □

Proposition 4.4. *Under the assumption of Conjecture 1.1, let E be given by the equation* (4)*. Suppose that $\beta = p^n$ with an odd prime p and even n and that for each odd prime ℓ dividing $\beta + 16$, $\mathrm{ord}_\ell(\beta + 16)$ is odd. If either*

- $p \equiv 1 \pmod 4$*, or*
- *there are at least two odd prime divisors in $\beta + 16$,*

then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$.

Proof. Write $\beta = p^{2z}$ with $z \geq 1$ and we begin with the following equation:

$$y^2 + p^{2z}xy - p^{4z}y = x^3 - p^{2z}x^2.$$

By a suitable change of variables, the equation transformed into

$$y^2 = x^3 + (p^{2z} + 8)x^2 + 16x.$$

The last equation has $\Delta = 2^{12}(p^{2z} + 16)p^{2z}$ and $c_4 = 16p^{4z} + 256p^{2z} + 256$. We note that the minimal discriminant of E is given by $\Delta_{\min} = (p^{2z} + 16)p^{2z}$ and E has ordinary good reduction modulo 2.

First we compute the Selmer group $\mathrm{Sel}^\phi(E/\mathbb{Q})$. The local images are given as follows.

- $\mathrm{Im}\,\delta_\infty = \{1\}$.
- $\mathrm{Im}\,\delta_\ell = \mathbb{Z}_\ell^\times \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for odd primes $\ell \nmid \Delta$.
- $\mathrm{Im}\,\delta_\ell = \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for odd prime $\ell \mid (p^{2z} + 16)$.
- $\mathrm{Im}\,\delta_p = \begin{cases} \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $\mathrm{Im}\,\delta_2 = \{1, 5\}$.

Since $p^{2z} + 16$ is a sum of two squares, any prime divisor ℓ of $p^{2z} + 16$ satisfies $\ell \equiv 1 \pmod 4$. So $\mathrm{Sel}^\phi(E/\mathbb{Q})$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ contains odd primes $\ell \mid p^{2z} + 16$, together with p in case when $p \equiv 1 \pmod 4$.

Note that $\Delta_{\min} > 0$, i.e., $i_\infty = 1$ by Proposition 2.2(i). By the fact that $u_K = 2$ if $d = -1$ and Corollary 2.3, we only need to concern about the cases $d = -2$, $d = -q$, $-2q$ or $d = -qq'$ for some odd primes q and q'.

Assume that $d = -2$. As $(\Delta_{\min}, d)_{\mathbb{Q}_2} = \big((p^{2z} + 16)p^{2z}, -2\big)_{\mathbb{Q}_2} = (1, -2)_{\mathbb{Q}_2} = 1$, we have $i_2 = 2$ by Proposition 2.2(ii). Thus $i_\infty + i_2 = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows.

- $\mathrm{Im}\,\delta_\infty^d = \mathbb{R}^{\times 2}/\mathbb{R}^{\times 2}$.
- $\mathrm{Im}\,\delta_\ell^d = \mathbb{Z}_\ell^\times \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$.
- $\mathrm{Im}\,\delta_\ell^d = \mathbb{Q}_l^{\times 2}/\mathbb{Q}_l^{\times 2}$ for any odd prime $\ell \mid (p^{2z} + 16)$.
- $\mathrm{Im}\,\delta_p^d = \begin{cases} \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv \pm 1 \pmod 8, \\ \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv \pm 5 \pmod 8. \end{cases}$
- $\mathrm{Im}\,\delta_2^d = \{1, -2\}$.

By the Heegner hypothesis, for any odd prime $\ell \mid \Delta$, we have $(\frac{-2}{\ell}) = 1$, and so $\ell \equiv 1$ or $-5 \pmod 8$. However, by the sum of two squares theorem, we have $\ell \equiv 1 \pmod 8$ if $\ell \mid p^{2z} + 16$. From Proposition 2.4, we have that if

$p \equiv 1 \pmod 8$, then the image of $p \in \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ and if $p \equiv -5 \pmod 8$, then the image of any odd prime $\ell \mid p^{2z}+16$ in $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of $\Sh$. Hence we have $i_\infty + i_2 + \dim_{\mathbb{F}_2}\Sh \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d = -q$ with a prime $q \equiv 1 \pmod 4$, then $d \equiv 3 \pmod 4$. In this case, the prime 2 is ramified in K and we have $i_2 \geq 1$ by Proposition 2.2(ii). If ℓ is an odd prime dividing $p^{2z}+16$, then $(\frac{\ell}{q}) = (\frac{-q}{\ell}) = 1$ by the Heegner Hypothesis, so $(\frac{\Delta_{\min}}{q}) = 1$, i.e., $i_q = 2$ by Proposition 2.2(iii). Hence $i_\infty + i_2 + i_q \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d = -q$ with a prime $q \equiv 3 \pmod 4$, then $d \equiv 1 \pmod 4$. If ℓ is an odd prime dividing $p^{2z}+16$, then $(\frac{\ell}{q}) = (\frac{-q}{\ell}) = 1$ by the Heegner Hypothesis, so $(\frac{\Delta_{\min}}{q}) = 1$, i.e., $i_q = 2$ by Proposition 2.2(iii). Thus $i_\infty + i_q = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows.

- $\mathrm{Im}\,\delta_\infty^d = \mathbb{R}^{\times 2}/\mathbb{R}^{\times 2}$.
- $\mathrm{Im}\,\delta_\ell^d = \mathbb{Z}_\ell^\times \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{Im}\,\delta_\ell^d = \mathbb{Q}_l^{\times 2}/\mathbb{Q}_l^{\times 2}$ for any odd prime $\ell \mid (p^{2z}+16)$.
- $\mathrm{Im}\,\delta_p^d = \begin{cases} \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Z}_p\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $\mathrm{Im}\,\delta_q^d \supseteq \{1, qu\}$ for some u with $(\frac{u}{q}) = -1$.
- $\mathrm{Im}\,\delta_2^d = \{1, 5\}$.

From Proposition 2.4, we have that if $p \equiv 1 \pmod 4$, then the image of $p \in \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of $\Sh$ and if $p \equiv 3 \pmod 4$, then the image of any odd prime $\ell \mid p^{2z}+16$ in $\mathrm{Sel}^{\phi}(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of $\Sh$. Hence we have $i_\infty + i_q + \dim_{\mathbb{F}_2}\Sh \geq 4$ and Proposition 2.1 concludes the proof.

Assume that $d = -2q$ for some odd prime q. In this case, the prime 2 is ramified in K and we have $i_2 \geq 1$ by Proposition 2.2(ii). If ℓ is an odd prime dividing $p^{2z}+16$, then $(\frac{\ell}{q}) = (\frac{-q}{\ell}) = 1$ by the Heegner Hypothesis, so $(\frac{\Delta_{\min}}{q}) = 1$, i.e., $i_q = 2$ by Proposition 2.2(iii). Hence $i_\infty + i_2 + i_q \geq 4$ and Proposition 2.1 concludes the proof.

Finally, assume $d = -qq'$. If the prime 2 is ramified in $K = \mathbb{Q}(\sqrt{d})$, then we have $i_\infty + i_2 + i_q + i_{q'} \geq 4$. Hence we may assume that the prime 2 is unramified, which means that $d \equiv 1 \pmod 4$. Without loss of generality, we then assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, we further assume $i_q = i_{q'} = 1$, i.e., $(\frac{p^{2z}+16}{q}) = (\frac{p^{2z}+16}{q'}) = -1$ by Proposition 2.2(iii). Thus $i_\infty + i_q + i_{q'} = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows.

- $\mathrm{Im}\,\delta_\infty^d = \mathbb{R}^{\times 2}/\mathbb{R}^{\times 2}$.
- $\mathrm{Im}\,\delta_\ell^d = \mathbb{Z}_\ell^\times \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q, q'$.

- $\operatorname{Im}\delta_\ell^d = \mathbb{Q}_l^{\times 2}/\mathbb{Q}_l^{\times 2}$ for any odd prime $\ell \mid p^{2z}+16$.
- $\operatorname{Im}\delta_p^d = \begin{cases} \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Z}_p\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $\operatorname{Im}\delta_q^d \supseteq \{1, qu\}$ for some u with $(\frac{u}{q}) = -1$.
- $\operatorname{Im}\delta_{q'}^d = \mathbb{Q}_{q'}^{\times 2}/\mathbb{Q}_{q'}^{\times 2}$.
- $\operatorname{Im}\delta_2^d = \{1, 5\}$.

Suppose first that $p \equiv 1 \pmod 4$. From Proposition 2.4, we have that if $(\frac{p}{q}) = 1$, then the image of $p \in \mathrm{Sel}^\phi(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is non-trivial element of Φ and if $(\frac{p}{q}) = -1$, then the image of either p or pq is non-trivial element of Φ. Now suppose that $p \equiv 3 \pmod 4$. If there is an odd prime $\ell \mid p^{2z}+16$ such that $(\frac{\ell}{q}) = 1$, then we take $\lambda = \ell$. Otherwise, there are two distinct odd prims ℓ, $\ell' \mid p^{2z}+16$ such that $(\frac{\ell}{q}) = (\frac{\ell'}{q}) = -1$, in which case we take $\lambda = \ell\ell'$. Then the image of $\lambda \in \mathrm{Sel}^\phi(E/\mathbb{Q}) \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$ is a non-trivial element of Φ by Proposition 2.4. Hence $i_\infty + i_q + i_{q'} + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof. □

Proposition 4.5 ($\beta = -p^n$)**.** *Under the assumption of Conjecture 1.1, let E be given by the equation* (4)*. Suppose that $\beta = -p^n$ with an odd prime p and even n and that for each odd prime ℓ dividing $\beta+16$, $\mathrm{ord}_\ell(\beta+16)$ is odd. Then we have $2 \mid u_K \cdot |Ш(E/K)|^{1/2}$, except for '15a3' and '21a4'.*

Proof. Write $\beta = -p^{2z}$ and we begin with the following equation:

$$y^2 - p^{2z}xy - p^{4z}y = x^3 + p^{2z}x^2.$$

By a suitable change of variables, the equation transformed into

$$y^2 = x^3 + (p^{2z}-8)x^2 + 16x.$$

The last equation has $\Delta = 2^{12}(p^{2z}-16)p^{2z}$ and $c_4 = 16p^{4z} - 256p^{2z} + 256$. We note that the minimal discriminant of E is given by $\Delta_{\min} = (p^{2z}-16)p^{2z}$ and E has ordinary good reduction modulo 2. Since the only instance when $\Delta_{\min} < 0$ is the case $p = 3$ and $z = 1$, which gives the curve '21a4', we may assume $\Delta_{\min} > 0$, i.e., $i_\infty = 1$ by Proposition 2.2(i).

First we compute the Selmer group $\mathrm{Sel}^\phi(E/\mathbb{Q})$. The local images are given as follows.

- $\operatorname{Im}\delta_\infty = \{1\}$.
- $\operatorname{Im}\delta_\ell = \mathbb{Z}_\ell^\times\mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for odd primes $\ell \nmid \Delta$.
- $\operatorname{Im}\delta_\ell = \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for odd primes $\ell \mid \Delta$.
- $\operatorname{Im}\delta_2 = \{1, 5\}$.

So $\mathrm{Sel}^\phi(E/\mathbb{Q})$ contains odd primes ℓ dividing Δ such that $\ell \equiv 1 \pmod 4$, in $\mathbb{Q}^{\times 2}/\mathbb{Q}^{\times 2}$. We may assume that there are at least two distinct odd prime divisors in Δ other than p, except for the curve '15a3' (corresponding to the case when $p^z - 4 = 1$).

By the fact that $u_K = 2$ if $d = -1$ and Corollary 3.3, we only need to concern about the cases $d = -2$, $d = -q$, $-2q$ or $d = -qq'$ for some odd primes q and q'.

Assume $d = -2$. As $(\Delta_{\min}, d)_{\mathbb{Q}_2} = \big((p^{2z} - 16)p^{2z}, -2\big)_{\mathbb{Q}_2} = (1, -2)_{\mathbb{Q}_2} = 1$, we have $i_2 = 2$ by Proposition 2.2(ii). Thus $i_\infty + i_2 = 3$. Now we consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbb{Q})$. The local images are given as follows.

- $\operatorname{Im}\delta_\infty^d = \mathbb{R}^\times/\mathbb{R}^{\times 2}$.
- $\operatorname{Im}\delta_\ell^d = \mathbb{Z}_\ell^\times \mathbb{Q}_\ell^{\times 2}/\mathbb{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$.
- $\operatorname{Im}\delta_\ell^d = \mathbb{Q}_l^\times/\mathbb{Q}_l^{\times 2}$ for any odd prime $\ell \mid \Delta$.
- $\operatorname{Im}\delta_2^d = \{1, -2\}$.

By the Heegner hypothesis, for any odd prime $\ell \mid \Delta$, we have $(\frac{-2}{\ell}) = 1$, and so $\ell \equiv 1$ or $-5 \pmod 8$. From Proposition 2.4, we have if $p \equiv 1 \pmod 8$, then the image of p is a non-trivial element of Φ and if $p \equiv -5 \pmod 8$, then either one of the images of ℓ or ℓp is a non-trivial element of Φ. Hence we have $i_\infty + i_2 + \dim_{\mathbb{F}_2}\Phi \geq 4$ and Proposition 2.1 concludes the proof.

For the remaining cases, we can also prove that $i_\infty + i_2 + i_q + \dim_{\mathbb{F}_2}\Phi \geq 4$ or $i_\infty + i_2 + i_q + i_{q'} + \dim_{\mathbb{F}_2}\Phi \geq 4$ by similar arguments. We omit the detail. □

5. Proof of Theorem 1.5

To prove Theorem 1.5, we need the following lemma.

Lemma 5.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and E_0 the $X_0(N)$-optimal curve in its rational isogeny class. If there is an étale isogeny $\pi : E \to E_0$ of degree 2^r $(r \geq 1)$, then the Manin constant c of E is even.*

Proof. Let ω_E and ω_{E_0} be the Néron differentials on E and E_0, respectively. Since π is étale, we have $\pi^*(\omega_{E_0}) = \omega_E$, where π^* is the induced map on differentials (cf. [15, Section 1]). Let $\pi' : E_0 \to E$ be the dual isogeny of π. Then $\pi \circ \pi' = [2^r]$ is the multiplication by 2^r. So $\pi'^*(\omega_E) = \pi'^* \circ \pi^*(\omega_{E_0}) = (\pi \circ \pi')^*(\omega_{E_0}) = 2^r\omega_{E_0}$. Let $\theta_0 : X_0(N) \to E_0$ be the modular parametrization of E_0. Then $(\pi' \circ \theta_0)^*(\omega_E) = \theta_0^* \circ \pi'^*(\omega_E) = 2^r\theta_0^*(\omega_{E_0}) = 2^r c_0\omega_f$, where ω_f is the differential 1-form associated to a normalized newform f of level N and c_0 is the Manin constant of E_0. Thus the Manin constant $c = 2^r c_0$ of E is even. □

Now we can prove Theorem 1.5.

Proof of Theorem 1.5. If E is a curve in $\mathcal{F}_1$, then we have $2 \mid c$ by Conjecture 1.4 and Lemma 5.1. If E is a curve in $\mathcal{F}_2$, then we have $2 \mid m$ by the proof of Theorem 1.3 and $2 \mid c$ by Conjecture 1.4 and Lemma 5.1. Thus we complete the proof. □

References

[1] D. Byeon, T. Kim, and D. Yhee, *A conjecture of Gross and Zagier*: *case* $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$, Int. J. Number Theory **15** (2019), no. 9, 1793–1800. https://doi.org/10.1142/S1793042119501008

[2] D. Byeon, T. Kim, and D. Yhee, *A conjecture of Gross and Zagier*: *case* $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, Int. J. Number Theory **16** (2020), no. 7, 1567–1572. https://doi.org/10.1142/S1793042120500827

[3] Z. Cao, C. Chu, and W. C. Shiu, *The exponential Diophantine equation* $AX^2 + BY^2 = \lambda k^Z$ *and its applications*, Taiwanese J. Math. **12** (2008), no. 5, 1015–1034. https://doi.org/10.11650/twjm/1500574244

[4] J. Cremona, *Elliptic curve data*, available at http://johncremona.github.io/ecdata.

[5] T. Goto, *A study on the Selmer groups of elliptic curves with a rational* 2*-torsion*, Doctoral thesis, Kyushu University, 2002.

[6] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. https://doi.org/10.1007/BF01388809

[7] V. A. Kolyvagin, *Euler systems*, in The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.

[8] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. https://doi.org/10.2307/1998414

[9] D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 5, 1995–2037. https://doi.org/10.5802/aif.2664

[10] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33–186.

[11] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195. https://doi.org/10.1515/crll.2004.048

[12] W. A. Stein and M. Watkins, *A database of elliptic curves—first report*, in Algorithmic number theory (Sydney, 2002), 267–275, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002. https://doi.org/10.1007/3-540-45455-1_22

[13] W. A. Stein and M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. **2004** (2004), no. 27, 1395–1405. https://doi.org/10.1155/S1073792804133916

[14] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106. https://doi.org/10.1007/BF01388845

[15] V. Vatsal, *Multiplicative subgroups of* $J_0(N)$ *and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316. https://doi.org/10.1017/S147474800500006X

Dongho Byeon
Department of Mathematical Sciences
Research Institute of Mathematics
Seoul National University
Seoul 08826, Korea
Email address: dhbyeon@snu.ac.kr

Taekyung Kim
Cryptolab
Seoul 08826, Korea
Email address: Taekyung.Kim.Maths@gmail.com

Donggeon Yhee
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea
Email address: dgyhee@gmail.com