CLASS NUMBER PROBLEM FOR A FAMILY OF REAL QUADRATIC FIELDS

DONGHO BYEON AND JIGU KIM

Abstract. In this paper, we show that class number problem for a family of infinitely many real quadratic fields can be reduced to a finite computation by using an effectively computable lower bound for class numbers of real quadratic fields in [BK1].

1. Introduction

Let $d > 0$ be a fundamental discriminant of a real quadratic field. Let $h(d)$ be the class number and ε_d the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. In [BK1], we proved the following theorem.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ and $\mathcal{D}(g)$ the set of fundamental discriminants $d > 0$ of real quadratic fields such that the base change Hasse-Weil L-function $L_{E/\mathbb{Q}(\sqrt{d})}(s)$ has a zero of order $\geq g$ at $s = 1$. Then there are effectively computable positive constants c_1 and c_2 such that for any $d \in \mathcal{D}(g)$ greater than c_1,*

$$h(d) \log \varepsilon_d \geq c_2 (\log d)^{g-3} \prod_{p \in P(d)} \big(1 - \tfrac{\lfloor 2\sqrt{p} \rfloor}{p+1}\big),$$

where $P(d)$ is the set of primes p dividing d except for the largest of them.

Since $\log \varepsilon_d \gg \log d$, it is required that $L_{E/\mathbb{Q}(\sqrt{d})}(s)$ has a zero of order ≥ 5 at $s = 1$ to get a non-trivial lower bound from Theorem 1.1. But there is no known elliptic curve E whose Hasse-Weil L-function $L_{E/\mathbb{Q}}(s)$ has a zero of order ≥ 4 at $s = 1$.

2010 *Mathematics Subject Classification.* 11G05, 11R11, 11R29.

Key words and phrases. Class number, Real quadratic field, L-function, Elliptic curve.

The first and second authors were supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (Grant No. 2020R1F1A1A010534) and (Grant Nos. 2019R1A6A1A11051177 and 2020R1I1A1A01074746), respectively.

Let E be an elliptic curve over $\mathbb{Q}$ with a rational point of order 2 whose $L_{E/\mathbb{Q}}(s)$ has a zero of order $g(1) \geq 3$ at $s = 1$. We note that there are infinitely many such elliptic curves (cf. [RS], [ST]). If we assume by translating the x-coordinates that $(0,0)$ is a point of order 2, then we have the following Weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx.$$

Let $E(\delta) : \delta y^2 = x^3 + ax^2 + bx$ be the quadratic twist of E. If $v^2\delta_m = m^4 + am^2 + b = (m^2 + \frac{a}{2})^2 + b - \frac{a^2}{4}$ for a nonzero integer v, then $E(\delta_m)$ has a rational point (m^2, mv). If we can choose m such that (m^2, mv) has infinite order and $E(\delta_m)$ has the root number $W(E(\delta_m)) = (-1)^{g(\delta_m)} = 1$, where $g(\delta_m)$ is the order of zero of $L_{E(\delta_m)/\mathbb{Q}}(s)$ at $s = 1$, then $g(\delta_m) \geq 2$ (cf. [GM]). So $L_{E/\mathbb{Q}(\sqrt{\delta_m})}(s)$ has a zero of order $g(1) + g(\delta_m) \geq 5$ at $s = 1$.

Further, if D is a positive square-free integer and v be the least positive integer such that $v^2 D = n^2 + r$ holds with integers n, r satisfying $-n < r \leq n$ and $r \mid 4n$, then the fundamental unit ε_d of $\mathbb{Q}(\sqrt{D})$, where d is the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$, is of the following form (cf. [De], [Ku]):

$$\varepsilon_d = \begin{cases} n + v\sqrt{D} & \text{if } |r| = 1, \text{ (except for } D = 5,\ v = 1) \\ \frac{n+v\sqrt{D}}{2} & \text{if } |r| = 4, \\ \frac{2n^2+r+2nv\sqrt{D}}{|r|} & \text{if } |r| \neq 1, 4. \end{cases}$$

Thus, for an even integer a and a sufficiently small integer v, if we can chose m such that δ_m is a positive square-free integer and $(b - \frac{a^2}{4}) \mid 4(m^2 + \frac{a}{2})$, then the fundamental unit ε_{d_m} of the real quadratic field $\mathbb{Q}(\sqrt{\delta_m})$ satisfies $\log \varepsilon_{d_m} \ll \log d_m$, where d_m is the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{\delta_m})$. Thus we can obtain an effectively computable lower bound of the class number of the real quadratic field $\mathbb{Q}(\sqrt{\delta_m})$ by Theorem 1.1.

In this paper, for an example, we take the following elliptic curve E over $\mathbb{Q}$ with a rational point of order 2 whose $L_{E/\mathbb{Q}}(s)$ has a zero of order 3 at $s = 1$

$$E : y^2 = x^3 - 100x^2 + 2508x$$

of conductor $N = 80256 = 2^7 \cdot 3 \cdot 11 \cdot 19$ (cf. [Cr]) and prove the following theorem.

Theorem 1.2. *Let $\delta_m = ((2m^2-25)^2+2)/9$ be a square-free positive integer such that $m \equiv 1 \pmod{81}$. Then, for any fundamental discriminant $d_m = 4\delta_m$ of the real quadratic field $\mathbb{Q}(\sqrt{\delta_m})$ such that $(d_m, 11\cdot 19) = 1$, we have*

$$h(d_m) \geq \frac{1}{3600} \cdot \log d_m \prod_{p \in P(d_m)} \left(1 - \tfrac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right),$$

where $P(d_m)$ is the set of primes p dividing d_m except for the largest of them.

Thus the class number problem for the family of the real quadratic fields $\mathbb{Q}(\sqrt{\delta_m})$ in Theorem 1.2 is reduced to a finite computation. For the odd class number problem, we have the following corollary from Theorem 1.2.

Corollary 1.3. *Let $\delta_m = ((2m^2-25)^2+2)/9$ be a square-free positive integer such that $m \equiv 1 \pmod{81}$ and n an odd positive integer. If $h(d_m) = n$, then δ_m is a prime such that $d_m = 4\delta_m \leq e^{10800n}$.*

Remark. For the real quadratic fields of narrow Richaud-Degert type, that is, $\mathbb{Q}(\sqrt{m^2 \pm 1})$ or $\mathbb{Q}(\sqrt{m^2 \pm 4})$, we proved a theorem similar to Theorem 1.2 under the Birch and Swinnerton-Dyer conjecture (cf. [BK1, Theorem 3]). To get an explicit lower bound of class numbers for this family without the Birch and Swinnerton-Dyer conjecture by using the method in this paper, we need suitable elliptic curves for this family. But it is difficult to find a cubic polynomial $f(x)$, which has rational solutions (x, y) satisfying

$$(m^2 \pm 1)y^2 = f(x) \;\text{ or }\; (m^2 \pm 4)y^2 = f(x)$$

for any integer m. In [La] and [BK], there are similar works to Theorem 1.2 for subfamilies of narrow Richaud-Degert type. However, [La, Theorem 1.2] does not get an explicit lower bound and [BK, Theorem 1.6] is less effective.

For some families of real quadratic fields of known fundamental units, we can have explicit lower bounds of class numbers by using quadratic residue covers (cf. [LMW, Section 4]). But the family of real quadratic fields in Theorem 1.2 can not be dealt with this method, because we can show that there exist infinitely many δ_m in Theorem 1.2 such that $(\frac{\delta_m}{p}) = -1$ for all $p \in \mathcal{C}$, where $\mathcal{C}$ is any finite set of odd prime integers by using [MV, Theorem], the fact that $\delta_m = 9A^2+8A+2$, where $m = 81a+1$ and $A = 1458a^2+36a-3$, is a square-free polynomial of degree 4 modulo p for all prime $p \neq 2,3$, and direct computations for finite exceptional cases in [DKM, Theorem 1.1].

2. Preliminaries

In this section, we briefly explain how to compute c_1 and c_2 in Theorem 1.1. For more details, see [BK1].

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. We denote by $S_2^p(N)$ the set of normalized primitive holomorphic cusp forms for the congruence subgroup $\Gamma_0(N)$ of weight 2 with trivial nebentypus 1_N. From the Modularity Theorem, there exists $f = \sum_{n=1}^{\infty} a_n q^n$ $(q = e^{2\pi i\tau}) \in S_2^p(N)$ such that the associated L-function $L(f,s)$ satisfies

$$L_{E/\mathbb{Q}}(s) = L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

If necessary, we denote a_n by $a_n(f)$. Thus $L_{E/\mathbb{Q}}(s)$ has an analytic continuation to an entire function satisfying the functional equation

$$\Lambda(f,2-s) = W(f)\Lambda(f,s),$$

where $\Lambda(f,s) = \big(\frac{\sqrt{N}}{2\pi}\big)^s\Gamma(s)L(f,s)$ and $W(f) = \pm 1$ is the root number of f or $E/\mathbb{Q}$.

For a Dirichlet character χ_d, there exist an integer $N_{\chi_d} \geq 1$ and $f \otimes \chi_d \in S_2^p(N_{\chi_d})$ such that the p-th Fourier coefficient is given by

$$a_p(f \otimes \chi_d) = a_p(f)\chi_d(p)$$

for almost all primes p. This condition uniquely determines N_{χ_d} and $f \otimes \chi_d$. Let

$$M_d = \frac{\sqrt{NN_{\chi_d}}}{|d|}.$$

and

$$M = 2^{n_2} \cdot 3^{n_3} \cdot N,$$

where

$$\begin{cases} n_2 = \max_{\chi_d} \big\{0, \frac{\mathrm{ord}_2(N_{\chi_d}) - \mathrm{ord}_2(N)}{2} - 2\big\}, \\ n_3 = \max_{\chi_d} \big\{0, \frac{\mathrm{ord}_3(N_{\chi_d}) - \mathrm{ord}_3(N)}{2} - 1\big\}. \end{cases}$$

Let $L(\mathrm{sym}_i^2 E, s)$ be the imprimitive symmetric square L-function associated to $E/\mathbb{Q}$, B the symmetric square conductor of $E/\mathbb{Q}$ and

$$F_d(s) = \Big(\frac{M_d}{4\pi^2}\Big)^s \Gamma^2(s) \frac{L(\mathrm{sym}_i^2 E, 2s)}{(s-1)\zeta_N(2s-1)},$$

where the subscript N of ζ_N means that we have omitted the Euler factors at the primes dividing N. Let $F_d^{(k)}(s)$ be its k-th derivative and $\mathcal{F} = \{F_d \mid d \in \mathcal{D}(g)\}$.

Now we assume that $L_{E/\mathbb{Q}(\sqrt{d})}(s)$ has a zero of order $\geq g$ at $s = 1$. Let $W_d = W(f)W(f \otimes \chi_d)$, $\mu' \in \{1, 2\}$ such that $W_d = (-1)^{g-\mu'}$ and $\rho = g - \mu' - 1$. Let q_i be the i-th prime splitting in $\mathbb{Q}(\sqrt{d})$ (or the i-th prime). Then we can compute c_1 and c_2 in Theorem 1.1 as follows

$$\begin{aligned} c_1 &= \max_{\substack{F_d \in \mathcal{F},\\ 1 \leq k \leq \rho}} \left\{ c_3, \exp\big(2^{\rho-1}\rho!\sqrt{N}\big), \exp\big(L(\mathrm{Sym}_i^2 E, 2)\big), \exp\Big(2\rho \frac{|F_d^{(k)}(1)|}{|F_d(1)|}\Big) \right\}, \\ c_2 &= \frac{L(\mathrm{Sym}_i^2 E, 2)}{c_4 c_5 2^{\rho+1}\rho! 2^{n_2/2} 3^{n_3/2}\sqrt{N}} \prod_{p|N} \frac{p}{p-1} \prod_{i=1}^{\rho} \frac{(q_i - 1)(q_i + 1 - \lfloor 2\sqrt{q_i} \rfloor)}{(q_i + 1)(q_i + 1 + \lfloor 2\sqrt{q_i} \rfloor)}. \end{aligned}$$

Here, $c_3 \geq \exp(6\rho^{\rho+1})$ is a positive real number such that if $d \geq c_3$, then

$$\frac{1}{m}\log\frac{\sqrt{d}}{4} > \max\left\{ 2\left(\frac{(31/4)\sqrt{M}\log d}{2(\rho+1)L(\mathrm{Sym}_i^2 E, 2)\prod_{p|N}\frac{p}{p-1}} \right)^{\frac{1}{\rho+1}}, \log\left(\frac{Me^4}{16\pi^2}\right) \right\}, \tag{1}$$

where m is the largest integer such that

$$\frac{(\rho+1)L(\mathrm{Sym}_i^2 E, 2)\prod_{p|N}\frac{p}{p-1}}{(31/4)2^{2\rho+2}\sqrt{M}}(\log d)^{\rho} > (m-1)^{\rho+1},$$

$c_4 > (1 + e^{c_6} + e^{c_7} + e^{c_8})$, where

$$\begin{aligned}
c_6 &= \max_{\substack{d\in\mathcal{D}(g),\\ d>c_1}} \Bigg\{ \log \frac{12\binom{\rho+3}{3} L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}{\pi} - \frac{\log M + \log M_d}{2} \\
&\quad +(2\rho+3)\log\log d - \left(\frac{(31/4)\sqrt{M}\log d}{2(\rho+1)L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}} \Bigg\},\\
c_7 &= \max_{\substack{d\in\mathcal{D}(g),\\ d>c_1}} \Bigg\{ \log \frac{L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}{2^{\rho+1}\rho!} - \frac{\log M}{2} + \rho\log\log d \\
&\quad -2\left(\frac{(31/4)\sqrt{M}\log d}{2(\rho+1)L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}} \Bigg\},\\
c_8 &= \max_{\substack{d\in\mathcal{D}(g),\\ d>c_1}} \left\{ \log \frac{L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}{2^{2\rho+1}\rho!} + \rho\log\log d - \frac{\log d}{2} \right\},
\end{aligned}$$

and $c_5 > 1$ such that

$$\begin{aligned}
&2-\exp\left(\frac{2}{\log d}\Big(\frac{\log\log d}{\log 2}+1\Big)^2\right)\\
&-\frac{\rho\max_{\substack{F_d\in\mathcal{F}\\ 1\le k\le\rho}}\left\{\frac{|F_d^{(k)}(1)|}{|F_d(1)|}\right\}}{\log d}\cdot\exp\left(\frac{4}{\log d}\Big(\frac{\log\log d}{\log 2}+1\Big)^2\right)\\
&-\frac{280\pi\cdot 2^{5\rho}\cdot B^2\prod_{p\|N}\frac{\sqrt{p}}{\sqrt{p}-1}\prod_{p^2|N}\left(\frac{\sqrt{p}+1}{\sqrt{p}}\right)^2\frac{\sqrt{p}+1}{\sqrt{p}-1}\prod_{p|N}(\frac{p-1}{p})}{\sqrt[4]{M_d}}\frac{1}{d^{\frac{1}{4}}(\log d)}\\
&>\frac{1}{c_5}
\end{aligned}$$

for any $d\in\mathcal{D}(g)$ greater than c_1.

Remark. To get a better bound, we slightly change the assumption

$$h(d)\log\varepsilon_d \ge \frac{L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}{2^{\rho+1}\rho!\sqrt{M}}(\log d)^\rho$$

in [BK, Proposition 4] to

$$h(d)\log\varepsilon_d \ge \frac{L(\mathrm{Sym}_i^2 E,2)\prod_{p|N}\frac{p}{p-1}}{(31/4)2^{\rho+1}\rho!\sqrt{M}}(\log d)^\rho.$$

So only (31/4) is different for (1), c_6, c_7 here and (4.7.1), c_6, c_7 in [BK1].

3. Proof of Theorem 1.2 and Corollary 1.3

To prove Theorem 1.2, we need the following propositions.

Proposition 3.1. *Let* $\delta_m = ((2m^2-25)^2+2)/9$ *be a square-free positive integer such that* $m \equiv 1 \pmod{81}$ *and* $d_m = 4\delta_m$ *the fundamental discriminant of the real quadratic field* $\mathbb{Q}(\sqrt{\delta_m})$*. If* $(\frac{\delta_m}{p}) = 1$ *for some prime* p*, then we have*

$$h(d_m) \geq \frac{1}{2\log p} \cdot \log \frac{d_m}{4},$$

except for $m = 1$.

Proof. Let $m = 81a + 1$ for some nonzero integer a. Then we have $\delta_m = ((2m^2-25)^2+2)/9 = 19131876a^4 + 944784a^3 - 55404a^2 - 1656a + 59$. Let $A = 1458a^2 + 36a - 3$. Then $\delta_m = 9A^2 + 8A + 2$ and $\sqrt{\delta_m}$ has continued fraction $[3A+1, \overline{2, 1, 3A, 1, 2, 2(3A+1)}]$ of length 6. Let Q_i $(i = 0, \cdots, 6)$ be the usual invariants of the continued fraction of $\sqrt{\delta_m}$ (cf. [Mo, p. 42]). Then we have $Q_0 = 1$, $Q_1 = 2A+1$, $Q_2 = 4A+1$, $Q_3 = 2$, $Q_4 = 4A+1$, $Q_5 = 2A+1$ and $Q_6 = 1$. Thus $\{Q_i/Q_0 \mid i = 1, \cdots, 6\} = \{1, 2, 2A+1, 4A+1\}$. Suppose that $(\frac{\delta_m}{p}) = 1$ for some prime p. If $p^{h(d_m)} \leq \frac{1}{2}\sqrt{d_m}$, then $p^{h(d_m)} = 2A+1$ or $4A+1$ by [Lo, Lemma 1 and Proposition 2]. But it is impossible because $2A+1 = (18a+1)(162a-5)$ and $4A+1 \geq \frac{1}{2}\sqrt{d_m}$. Thus we have $p^{h(d_m)} \geq \frac{1}{2}\sqrt{d_m}$ (cf. [Lo, p. 171, Proof of (iii)]). □

Proposition 3.2. *Let* $\delta_m = ((2m^2-25)^2+2)/9$ *be a square-free positive integer such that* $m \equiv 1 \pmod{81}$ *and* $d_m = 4\delta_m$ *the fundamental discriminant of the real quadratic field* $\mathbb{Q}(\sqrt{\delta_m})$*. If* $(\frac{\delta_m}{11}) = -1$ *and* $(\frac{\delta_m}{19}) = -1$*, then we have*

$$h(d_m) \geq \frac{1}{3600} \cdot \log d_m \prod_{p \in P(d_m)} \left(1 - \tfrac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right),$$

where $P(d_m)$ *is the set of primes* p *dividing* d_m *except for the largest of them.*

Proof. Let $E : y^2 = x^3 - 100x^2 + 2508x$ be an elliptic curve over $\mathbb{Q}$ of conductor $N = 80256 = 2^7 \cdot 3 \cdot 11 \cdot 19$. It is known that $L_{E/\mathbb{Q}}(s)$ has a zero of order $g(1) = 3$ at $s = 1$ (cf. [Cr]). Let $\delta_m = ((2m^2-25)^2+2)/9$ be a square-free integer such that $m \equiv 1 \pmod{81}$. We note that $\delta_m \equiv 3 \pmod{8}$ and $\delta_m \equiv 5 \pmod{9}$.

Let $E(\delta_m) : \delta_m y^2 = x^3 - 100x^2 + 2508x$ be the quadratic twist of E. Then $E(\delta_m)$ has a rational point $(4m^2, 12m)$. By the substitution $(x, y) \to (x/\delta_m, y/{\delta_m}^2)$, we have the following Weierstrass equation

$$E(\delta_m) : y^2 = x^3 - 100\delta_m x^2 + 2508{\delta_m}^2 x$$

and this equation has a rational point $P = (4m^2\delta_m, 12m{\delta_m}^2)$. Let $c_4(\delta_m)$, $c_6(\delta_m)$ be the usual invariants of $E(\delta_m)$ and $\Delta(\delta_m)$ the discriminant of $E(\delta_m)$. Then we have $c_4(\delta_m) = 2^6 \cdot 619 \cdot {\delta_m}^2$, $c_6(\delta_m) = -2^9 \cdot 5^2 \cdot 643 \cdot {\delta_m}^3$ and $\Delta(\delta_m) = -2^{13} \cdot 3^2 \cdot 11^2 \cdot 19^2 \cdot {\delta_m}^6$.

Firstly we show that $P = (4m^2\delta_m, 12m{\delta_m}^2)$ has infinite order. By the substitution $(x, y) \to (\frac{x+1200}{36}, \frac{y}{216})$, we have $E(\delta_m) : y^2 = x^3 - 27c_4(\delta_m)x - 54c_6(\delta_m)$ (cf. [Si, p. 43]). Since $(216 \cdot 12m{\delta_m}^2)^2 = 2^{10} \cdot 3^8 \cdot m^2 \cdot {\delta_m}^4$ does not divide $4(-27c_4(\delta_m))^3 + 27(-54c_6(\delta_m))^2 = 2^{21} \cdot 3^{14} \cdot 11^2 \cdot 19^2 \cdot {\delta_m}^6$, P has infinite order (cf. [Si, p. 240, Corollary 7.2]).

Secondly we compute the root number of $E(\delta_m)$. Since $(N, d_m) \neq 1$, we directly compute the root number of $E(\delta_m)$ by using Rizzo's tables in [Ri]. Let (a, b, c) be the smallest triplet of nonnegative integers such that $a \equiv v_p(c_4(\delta_m)) \pmod 4$, $b \equiv v_p(c_6(\delta_m)) \pmod 6$ and $c \equiv v_p(\Delta(\delta_m)) \pmod{12}$. For any $x \in \mathbb{Q}_p$, we write $x'_p = x'$ for $x/p^{v_p(x)}$. Let $W_p(E(\delta_m))$ be the local root number at p. Then we have the following table.

p	(a, b, c)	$W_p(E(\delta_m))$
2	$(2, 3, 1)$	$-1\ (\because c_4(\delta_m)' + 4c_6(\delta_m)' \equiv 15\ (16)$ and $c_4(\delta_m)' \equiv 3\ (16))$
3	$(0, 0, 2)$	$-1\ (\because c_6(\delta_m)' \equiv 2\ (3))$
11	$(0, 0, 2)$	$-(\frac{-c_6(\delta_m)'}{11}) = -1\ (\because -c_6(\delta_m)' \equiv 2 \cdot {\delta_m}^3\ (11)$ and $(\frac{2}{11}) = -1)$
19	$(0, 0, 2)$	$-\frac{(-c_6(\delta_m)'}{19}) = -1\ (\because -c_6(\delta_m)' \equiv 18 \cdot {\delta_m}^3\ (19)$ and $(\frac{18}{19}) = -1)$
$p \mid \delta_m$	$(2, 3, 6)$	$(\frac{-1}{p})$

Thus $E(\delta_m)$ has the root number $W(E(\delta_m)) = W_\infty(E(\delta_m)) \cdot W_2(E(\delta_m)) \cdot W_3(E(\delta_m)) \cdot W_{11}(E(\delta_m)) \cdot W_{19}(E(\delta_m)) \cdot \prod_{p \mid \delta_m} W_p(E(\delta_m)) = (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) = 1$ and $L_{E(\delta_m)/\mathbb{Q}}(s)$ has a zero of order $g(\delta_m) \geq 2$ at $s = 1$. So $L_{E/\mathbb{Q}(\sqrt{\delta_m})}(s)$ has a zero of order $g(1) + g(\delta_m) \geq 5$ at $s = 1$.

Finally we compute c_1 and c_2 in Theorem 1.1. We note that $\delta_m \equiv 3 \pmod 4$ and $\delta_m \equiv 2 \pmod 3$. Therefore we have that $d_m = 4\delta_m$ and 2 (respectively, 3) ramifies (respectively, is inert) in $\mathbb{Q}(\sqrt{\delta_m})$. Since $\mathrm{ord}_2(N) = 7$ and $3 \nmid d_m$, we have $n_2 = 0$, $n_3 = 0$ and $M = N = 80256$. Since $N_{\chi_{-4}} = N$ and $-\delta_m$ is relatively prime to $3 \cdot 11 \cdot 19$, we have $M_{d_m} = N/4 = 20064$. Thus we have

$$\begin{aligned} F_{d_m}(s) &= L(\mathrm{Sym}_i^2 E, 2s)(\frac{N}{16\pi^2})^s \Gamma(s)^2 \frac{1}{(s-1)\zeta(2s-1)} \\ &\quad \cdot \frac{1}{1-2^{-2s+1}} \frac{1}{1-3^{-2s+1}} \frac{1}{1-11^{-2s+1}} \frac{1}{1-19^{-2s+1}}. \end{aligned}$$

Since $g = 5$ and $W_{d_m} = -1$ for $d_m = 4\delta_m$, we have $\mu' = 2$ and $\rho = 2$.

Let $c(E)$ be the Manin's constant of E, vol(E) the volume of a minimal period lattice Λ with $E \simeq \mathbb{C}/\Lambda$ and deg(E) the modular degree of E. These invariants can be calculated by Sage and we have

$$\begin{aligned} L(\mathrm{Sym}_i^2 E, 2) &= \frac{2\pi c(E)^2 \mathrm{vol(E)}\deg(\mathrm{E})}{N} \\ &= 2.840615.... \end{aligned}$$

The Laurent expansion of the Riemann zeta function can be written in the form,

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \frac{(-1)^n}{n!}\gamma_n (s-1)^n$$

where γ_n are the so-called Stieltjes constants. Then we have

$$(s-1)\zeta(2s-1) = \frac{1}{2} + \sum_{n=0}^{\infty} \frac{(-2)^n \gamma_n}{n!}(s-1)^{n+1}.$$

It is well known that $\Gamma^{(1)}(1) = -\gamma_0$ and $\Gamma^{(2)}(1) = \gamma_0^2 + \frac{\pi^2}{6}$. Thus we have

$$\begin{aligned} \left|\frac{F_{d_m}^{(1)}(1)}{F_{d_m}(1)}\right| &= \left| 2\frac{L^{(1)}(\mathrm{Sym}_i^2 E, 2)}{L(\mathrm{Sym}_i^2 E, 2)} + \log(\frac{N}{16\pi^2}) + 2\frac{\Gamma^{(1)}(1)}{\Gamma(1)} - 2\gamma_0 - \sum_{p|N} \frac{2\log p}{p-1} \right| \\ &< 2\frac{|L^{(1)}(\mathrm{Sym}_i^2 E, 2)|}{L(\mathrm{Sym}_i^2 E, 2)} + 0.7 \end{aligned}$$

and

$$\left|\frac{F_{d_m}^{(2)}(1)}{F_{d_m}(1)}\right| = \left| 4\frac{L^{(2)}(\mathrm{Sym}_i^2 E, 2)}{L(\mathrm{Sym}_i^2 E, 2)} + \Big(\log(\frac{N}{16\pi^2})\Big)^2 + 2\frac{\Gamma(1)\Gamma^{(2)}(1) + \Gamma^{(1)}(1)^2}{\Gamma(1)^2} \right.$$

$$
\begin{aligned}
&+8(\gamma_0^2+\gamma_1)+\sum_{p|N}\frac{4(p+1)(\log p)^2}{(p-1)^2}\\
&+4\frac{L^{(1)}(\mathrm{Sym}_i^2E,2)}{L(\mathrm{Sym}_i^2E,2)}\Big(\log\big(\frac{N}{16\pi^2}\big)+2\frac{\Gamma^{(1)}(1)}{\Gamma(1)}-2\gamma_0-\sum_{p|N}\frac{2\log p}{p-1}\Big)\\
&+2\log\big(\frac{N}{16\pi^2}\big)\Big(2\frac{\Gamma^{(1)}(1)}{\Gamma(1)}-2\gamma_0-\sum_{p|N}\frac{2\log p}{p-1}\Big)\\
&+4\frac{\Gamma^{(1)}(1)}{\Gamma(1)}\Big(-2\gamma_0-\sum_{p|N}\frac{2\log p}{p-1}\Big)+8\gamma_0\sum_{p|N}\frac{\log p}{p-1}\\
&+8\sum_{\substack{p_1|N,\,p_2|N\\ p_1<p_2}}\frac{\log p_1}{p_1-1}\frac{\log p_2}{p_2-1}\Bigg|\\
<\;& 4\frac{|L^{(2)}(\mathrm{Sym}_i^2E,2)|}{L(\mathrm{Sym}_i^2E,2)}+0.7\cdot 4\frac{|L^{(1)}(\mathrm{Sym}_i^2E,2)|}{L(\mathrm{Sym}_i^2E,2)}+16.5.
\end{aligned}
$$

By numerical computations with Magma, we have the following rough upper bounds

$$|L^{(1)}(\mathrm{Sym}_i^2E,2)|\le 8$$

and

$$|L^{(2)}(\mathrm{Sym}_i^2E,2)|\le 120.$$

We note that if $d_m\ge\exp(3600)$, then (1) holds. Therefore we can take

$$
\begin{aligned}
c_1=\max_{1\le k\le\rho}&\Big\{\exp(3600),\ \exp\big(2^{\rho-1}\rho!\sqrt{N}\big),\ \exp\big(L(\mathrm{Sym}_i^2E,2)\big),\ \exp\big(2\rho\frac{|F_{d_m}^{(k)}(1)|}{|F_{d_m}(1)|}\big)\Big\}\\
=\exp(3600)&.
\end{aligned}
$$

Further, we can take

$$c_5=1.29.$$

Since

$$
\begin{aligned}
&\frac{\partial}{\partial X}\left((2\rho+3)\log X-\left(\frac{(31/4)\sqrt{N}}{2(\rho+1)L(\mathrm{Sym}_i^2E,2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}}X^{\frac{1}{\rho+1}}\right)\\
&=\frac{1}{X}\left((2\rho+3)-\frac{1}{\rho+1}\left(\frac{(31/4)\sqrt{N}}{2(\rho+1)L(\mathrm{Sym}_i^2E,2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}}X^{\frac{1}{\rho+1}}\right)
\end{aligned}
$$

and

$$X=\log d_m\ge 3600\ge\frac{(\rho+1)^{\rho+2}(2\rho+3)^{\rho+1}L(\mathrm{Sym}_i^2E,2)\prod_{p|N}\frac{p}{p-1}}{(31/8)\sqrt{N}},$$

its primitive function of $X = \log d_m$ attains the maximum value at $\log d_m = 3600$. Therefore we can take

$$\begin{aligned}
& c_6 \\
\leq \ & \log \frac{12\binom{\rho+3}{3} L(\mathrm{Sym}_i^2 E, 2) \prod_{p|N} \frac{p}{p-1}}{\pi\sqrt{N}\sqrt{N/4}} + (2\rho+3)\log\log d_m \\
& -2\left(\frac{\sqrt{N}\log d_m}{2(\rho+1)L(\mathrm{Sym}_i^2 E, 2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}} \\
\leq \ & \log \frac{24\binom{\rho+3}{3} L(\mathrm{Sym}_i^2 E, 2) \prod_{p|N} \frac{p}{p-1}}{\pi N} + (2\rho+3)\log(3600) \\
& -2\left(\frac{\sqrt{N}(3600)}{2(\rho+1)L(\mathrm{Sym}_i^2 E, 2)\prod_{p|N}\frac{p}{p-1}}\right)^{\frac{1}{\rho+1}} \\
= \ & \log(4.906...).
\end{aligned}$$

Similarly, we can calculate c_7 and c_8 and so we can take

$$c_4 = 1 + e^{c_6} + e^{c_7} + e^{c_8} < 5.91.$$

Thus we have

$$2^{n_2/2} \cdot 3^{n_3/2} \cdot c_4 \cdot c_5 < 7.7.$$

By Proposition 3.1, we may assume that $q_1, q_2 > \exp(1000)$. Then we can take

$$\begin{aligned}
c_2 \ &= \ \frac{1}{7.7}\frac{L(\mathrm{Sym}_i^2, 2)}{2^{\rho+1}\rho!\sqrt{N}} \prod_{p|N}\frac{p}{p-1}\prod_{i=1}^{\rho}\frac{(q_i-1)(q_i+1-\lfloor\sqrt{2q_i}\rfloor)}{(q_i+1)(q_i+1+\lfloor\sqrt{2q_i}\rfloor)} \\
&> \ \frac{1}{3550}.
\end{aligned}$$

Since $\varepsilon_{d_m} = (2m^2-25)^2 + 1 + 3(2m^2-25)\sqrt{\delta_m} < 2\cdot 3^2 d_m$ (cf. [Ku]), we have for $d_m > c_1 = \exp(3600)$,

$$h(d_m) \geq c_2'(\log d_m) \prod_{p\in P(d_m)} \left(1 - \tfrac{\lfloor 2\sqrt{p}\rfloor}{p+1}\right), \tag{2}$$

where

$$c_2' = c_2 \frac{\log c_1}{\log c_1 + \log 18} \geq \frac{1}{3600}.$$

Since (2) is also true for $d_m \leq \exp(3600)$, we complete the proof. □

Proof of Theorem 1.2. Theorem 1.2 follows from Proposition 3.1 and Proposition 3.2. □

Proof of Corollary 1.3. By the genus theory of quadratic fields, if $h(d_m)$ is odd, then δ_m should be a prime. By Theorem 1.2, if $d_m = 4\delta_m > e^{10800n}$, then we have $h(d_m) > n$. □

Remark. We note that $h(d_m) > 2$ for all d_m, except for $m = 1$, because if p is a prime such that $p \mid 2A + 1 = (18a + 1)(162a - 5)$, where A and a are in the proof of Proposition 3.1, then p splits in $\mathbb{Q}(\sqrt{\delta_m})$ by the fact $\delta_m = 9A^2 + 8A + 2$ and $9A^2 + 8A + 2 - (3A + 1)^2 = 2A + 1$, so we have $h(d_m) \geq \frac{1}{2\log(|18a+1|)} \cdot \log \frac{d_m}{4} > 2$ by Proposition 3.1. If $m = 1$, then $\delta_m = 59$ and $h(4 * 59) = 1$ (cf. [Mo, p. 271, Table A1]). Here, we mention that, in general, dealing with the class number one problem for families of real quadratic fields of known fundamental units is a difficult problem (cf. [Bi], [Bi1], [BLK]).

Acknowledgment. The authors thank the referees for their careful readings and many valuable suggestions.

References

[Bi] A. Biró, *Yokoi's conjecture*, Acta Arith. **106** (2003), 85–104.

[Bi1] A. Biró, *Chowla's conjecture*, Acta Arith. **107** (2003), 179–194.

[BK] D. Byeon and J. Kim, *An explicit lower bound for special values of Dirichlet L-functions* , J. Number Th. **189** (2018), 272–303.

[BK1] D. Byeon and J. Kim, *Class numbers of real quadratic fields*, J. Number Th. (2021) https://doi.org/10.1016/j.jnt.2020.11.015.

[BKL] D. Byeon, M. Kim and J. Lee, *Mollin's Conjecture*, Acta Arith. **126** (2007), 99–114.

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

[De] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zhalkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97.

[DKM] S. Du, K. Kutnar and D. Marušič, *Polynomials of degree 4 over finite fields representing quadratic residues*, The Art of Discete and Applied Math. **2** (2019), #P1.10.

[GM] F. Gouvea and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.

[Ku] M. Kutsuna, *On the fundamental units of real quadratic fields*, Proc. Japan Acad. **50** (1974), 580–583.

[La] K. Lapkova, *Effective lower bound for the class number of a certain family of real quadratic fields*, J. Number Th. **132** (2012), 2736–2747.

[Lo] S. Louboutin, *Continued fractions and real quadratic fields*, J. Number Th. **30** (1988), 167–176.

[LMW] S. Louboutin, R.A. Mollin and H.C. Williams, *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers*, Can. J. Math. **44** (1992), 824–842.

[MV] D. J. Madden and W. Y. Vélez, *Polynomials that represent quadratic residues at promitive roots*, Pacific J. Math. **98** (1982), 123–137.

[Mo] R. Mollin, *Quadratics*, CRC Press, 1995.

[Ri] O. Rizzo, *Average root numbers for a nonconstant family of elliptic curves*, Compo. Math. **236** (2003), 1–23.

[RS] K. Rubin and A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), 559–569.

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 2009.

[ST] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

Department of Mathematical Sciences,
Seoul National University
Seoul, Korea,
E-mail: dhbyeon@snu.ac.kr

Institute of Mathematical Sciences,
Ewha Womans University,
Seoul, Korea,
E-mail: jigu.kim.math@gmail.com