Effective lower bound for the class number of a certain family of real quadratic fields

Kostadinka Lapkova

Central European University
Department of Mathematics and its Applications
Nador u. 9, 1051 Budapest, HUNGARY
Email: lapkova_kostadinka@ceu-budapest.edu

February 14, 2012

Abstract

In this work we establish an effective lower bound for the class number of the family of real quadratic fields $\mathbb{Q}(\sqrt{d})$, where $d = n^2 + 4$ is a square-free positive integer with $n = m(m^2 - 306)$ for some odd m, with the extra condition $\left(\frac{d}{N}\right) = -1$ for $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$. This result can be regarded as a corollary of a theorem of Goldfeld and some calculations involving elliptic curves and local heights. The lower bound tending to infinity for a subfamily of the real quadratic fields with discriminant $d = n^2 + 4$ could be interesting having in mind that even the class number two problem for these discriminants is still an open problem.

1 Introduction

In this paper we give a lower bound for the class number of the real quadratic fields of Yokoi type $d = n^2 + 4$ where n is a certain third degree polynomial. This is a special case of the extensively examined Richaud-Degert discriminants. There are already lower bounds for their class number described in [11]. They however depend on the number of divisors of n at least. We present an analytic lower bound depending on the discriminant and since Goldfeld's theorem and Gross-Zagier formula are applied the bound will be of the magnitude these theorems could provide: $(\log d)^{1-\epsilon}$. The result of this paper is also interesting bearing in mind that there is still no effective solution of the class number two problem for discriminants $d = n^2 + 4$.

We consider elliptic curves over the field of rational numbers given by the Weierstrass equation

$$E \ : \ y^2 = x^3 + Ax + B \tag{1.1}$$

with discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$ and conductor N. We denote the group of rational points with the usual $E(\mathbb{Q})$. By a quadratic twist of the elliptic curve we understand the curve

$$E^D \ : \ Dy^2 = x^3 + Ax + B\,. \tag{1.2}$$

Key words and phrases: class number, real quadratic fields, elliptic curves.
MSC2010: Primary 11R29; Secondary 11R11, 11G50, 14H52.

After replacing (x, y) by $(x/D, y/D^2)$ we get the Weierstrass equation of the twisted elliptic curve

$$E^{D,W} \; : \; y^2 = x^3 + (AD^2)x + (BD^3) \tag{1.3}$$

with discriminant $\Delta_D = D^6\Delta$. Note that $(x_0, y_0) \in E^D(\mathbb{Q})$ if and only if $(Dx_0, D^2y_0) \in E^{D,W}(\mathbb{Q})$.

The important result from [4] that we refer to in our work is explained in the remarks following Theorem 1 in [5]. We formulate it as

Theorem 1.1 (Goldfeld). *Let d be a fundamental discriminant of a real quadratic field. If there exists an elliptic curve E over $\mathbb{Q}$ whose associated base change Hasse-Weil L-function*

$$L_{E/\mathbb{Q}(\sqrt{d})}(s) = L(E, s)L(E^d, s)$$

has a zero of order $g \geq 5$ at $s = 1$, then for every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon(E) > 0$, depending only on ϵ and E, such that

$$h(d) \log \epsilon_d > c_\epsilon(E)(\log d)^{2-\epsilon} ,$$

where $h(d)$ is the class number of $\mathbb{Q}(\sqrt{d})$ and ϵ_d is the fundamental unit.

Note that after the Modularity theorem every elliptic curve over $\mathbb{Q}$ is modular, so we omitted the original condition on modularity of the elliptic curve in Goldfeld's theorem.

Let us look at Yokoi's discriminants $d = n^2 + 4$. In that case the fundamental unit is small, i.e.

$$\log d \ll \log \epsilon_d \ll \log d .$$

If we use this fact and we can find an elliptic curve as in Theorem 1.1 we could obtain an effective lower bound of the type

$$h(d) > c_\epsilon(E)(\log d)^{1-\epsilon} .$$

The question whether Goldfelds's theorem can be used for a possible extension of the class number one problem for Yokoi's discriminants solved in [1] was raised by Biró [2] . Unfortunately we can assure existence of such elliptic curve only for a small subset of $d = n^2+4$. More precisely, the main result of this paper is

Theorem 1.2. *Let $n = m(m^2 - 306)$ for a positive odd integer m, and $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$. If $d = n^2 + 4$ is square-free and $\left(\dfrac{d}{N}\right) = -1$, then for every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon > 0$, depending only on ϵ, such that*

$$h(d) = h(n^2 + 4) > c_\epsilon \, (\log d)^{1-\epsilon} \; .$$

Remark 1.3. We expect that there are infinitely many discriminants d satisfying the assumptions of Theorem 1.2. Let

$$d(x) = x^6 - 612x^4 + 93636x^2 + 4$$

be the polynomial defining the discriminant d for odd positive $x = m$. The polynomial is irreducible in $\mathbb{Z}[x]$ so there are not obvious reasons for it not to be square-free infinitely often. Something more, if we introduce

$$M(X) = \#\{0 < m \leq X \; : \; m \text{ is odd}\, , \mu\,(d(m)) \neq 0 \text{ and } \left(\frac{d(m)}{N}\right) = -1\} , \tag{1.4}$$

we check numerically that $M(X)/X \approx 0.221$, i.e. the odd positive integers m defining square-free discriminants $d(m)$, which are also quadratic nonresidues modulo N, seem to be of positive density.

Construction similar to the one in the present paper was already done in [6], where the quadratic twists of E from (1.1) are of the form $D = u.f(u, v)$ for the homogeneous binary polynomial $f(u, v) = u^3 + Au^2v + Bv^3$. In [6] by a 'square-free sieve' argument the authors give a density to a similar quantity as (1.4). However, we are strictly interested in discriminants $d = n^2 + 4 = d(m)$ where $d(m)$ is a polynomial in one variable of degree 6. There exists a lot of literature on estimating square-free /or k-free/ polynomials but there are no results on one-variable polynomials of degree higher than three.

2 Proof of Theorem 1.2

Recall that for the Hasse-Weil L-function associated to the elliptic curve E we consider a root number $\omega = (-1)^t$, where $\mathrm{ord}_{s=1}L(E, s) = t$. Let ω_D be the root number for E^D. If $(D, N) = 1$ for the conductor N, and $\chi = \chi_D = \left(\frac{D}{\cdot}\right)$ is the real quadratic character of $\mathbb{Q}(\sqrt{D})$, we have $\omega_D = \chi(-N)\omega$ (e.g. [9].(23.48)). The character χ is even, so $\omega_D = \chi(N)\omega$.

Let E be an elliptic curve with $\mathrm{ord}_{s=1}L(E, s) \geq 3$ and $\omega = -1$. Then $\omega_D = -\chi(N)$. If further we require $\chi(N) = -1$ we will have $\omega_D = 1$. If there is a rational point in $E^D(\mathbb{Q})$ that is not a torsion point, then the rank of the Mordell-Weil group $E^D(\mathbb{Q})$ is positive. Applying Kolyvagin and Gross-Zagier theorems like in [13].C.16.5.5 we get $L(E^D, 1) = 0$, i.e. $\mathrm{ord}_{s=1}L(E^D, s) \geq 1$. From $\omega_D = 1$ it will follow that $\mathrm{ord}_{s=1}L(E^D, s) \geq 2$ and the order is even.

We will construct such an elliptic curve for which certain quadratic twists of it satisfy the upper conditions. Then $\mathrm{ord}_{s=1}L(E, s)L(E^D, s) \geq 5$ and this would allow us to apply Theorem 1.1.

From now on $d = n^2 + 4$ is a square-free odd integer. Look at the twist (1.2) with $y = 1$ and assume that d satisfies the equation

$$d = x_0^3 + Ax_0 + B \tag{2.1}$$

for some $x_0 \in \mathbb{Z}$. Then we have $(x_0, 1) \in E^d(\mathbb{Q})$. The equation (2.1) reads as $n^2+4 = x_0^3+Ax_0+B$ or $n^2 = x_0^3 + Ax_0 + B - 4$. Let us choose the coefficients A and B in such a way that $g(x) = x^3 + Ax + B - 4 = (x - k)^2(x - l)$ for some integers k and l. This yields $g(k) = g(l) = 0$ and $g'(k) = 0$. Then $g'(k) = 3k^2 + A = 0$, so $A = -3k^2$ and therefore $0 = g(k) = k^3 - 3k^2 \cdot k + B - 4$. Thus $B = 2k^3 + 4$ and finally

$$g(x) = x^3 - 3k^2x + (2k^3 + 4) - 4 = x^3 - 3k^2x + 2k^3 = (x - k)^2(x + 2k)\,.$$

This means that d satisfies (2.1) if and only if

$$n^2 = g(x_0) = (x_0 - k)^2(x_0 + 2k) \tag{2.2}$$

for some integer x_0.

Look at the curve

$$C_k \ : \ y^2 = (x - k)^2(x + 2k)\,.$$

It is well-known/see [13].III.2.5/ that its non-singular points are in one-to-one correspondence with $\mathbb{Q}^*$. What can be easily seen is that if we put $m = y/(x-k)$, we have $m^2 = x + 2k$, so $x = m^2 - 2k$ and $y = m(x-k) = m(m^2 - 3k)$. Hence n satisfies (2.2) exactly when

$$\begin{aligned} x_0 &= m^2 - 2k \\ n &= m(m^2 - 3k)\,, \end{aligned}$$

where m is an odd integer.

We are led to the following claim.

Lemma 2.1. *Let*

$$E_k \;:\; y^2 = x^3 - 3k^2x + (2k^3 + 4) \tag{2.3}$$

be an elliptic curve over $\mathbb{Q}$ with $ord_{s=1}L(E_k, s) \geq 3$ and odd, and a conductor N_k. Let E_k^d be the quadratic twist of E_k with $d = n^2 + 4$ such that $\left(\frac{d}{N_k}\right) = -1$. If k is even, then for any $n = m(m^2 - 3k)$, where m is an odd integer, we have

$$ord_{s=1}L(E_k^d, s) \geq 2$$

with root number $\omega_d = 1$.

Proof. By the argument presented in the beginning of the section it is enough to find a point in $E_k^d(\mathbb{Q})$ which is not a torsion point. We take $Q = (x_0, 1) = (m^2 - 2k, 1) \in E_k^d(\mathbb{Q})$. Clearly, by (1.3), we have $P = (dx_0, d^2) = (d(m^2 - 2k), d^2) \in E_k^{d,W}(\mathbb{Q})$. By Lutz-Nagell theorem/see [13].VIII.7.2/ if P is a torsion point, both the $x(P)$ and $y(P)$ coordinates of P should be integers. We also use the simple fact that if P is a torsion point so is any multiple of it. Let us look at $[2]P$.

The duplication formula [13].III.2.3d, for an elliptic curve given with (1.1), reads

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{\phi(x)}{4\psi(x)}\,.$$

We are interested in

$$E_k^{d,W} \;:\; y^2 = x^3 + (-3k^2)d^2x + (2k^3 + 4)d^3 \tag{2.4}$$

and in this case $\psi(dx_0) = \psi\left(d(m^2 - 2k)\right) = d^3(x_0^3 - 3k^2x_0 + (2k^3 + 4)) = d^3 \cdot d = d^4$, where we used (2.1). On the other hand

$$\phi(dx_0) = d^4\left(x_0^4 - 2(-3k^2)x_0^2 - 8(2k^3 + 4)x_0 + (-3k^2)^2\right)$$

and clearly $\psi(dx_0)$ divides $\phi(dx_0)$. Note, however, that x_0 is an odd integer for m–odd, and when k is even, as d is also odd, we have $\phi(dx_0) \equiv 1 \pmod 4$. This means that $x([2]P)$ is not an integer, thus according to Lutz-Nagell theorem $[2]P$ is not a torsion point, so P is not torsion either. □

Remark 2.2. Note that $\phi(dx_0) \equiv 0 \pmod 4$ when k is odd, so we cannot use the same easy argument to prove that P is not torsion.

We can finalize the proof if we find an elliptic curve E_k with odd analytic rank not less than 3 and even k. In the last section we prove unconditionally that the analytic rank of E_{102} is odd and at least three by giving a lower bound for the canonical height of any non-torsion point on the curve. The conductor of E_{102} is $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$, therefore the statement of Theorem 1.2 follows from Lemma 2.1 and Goldfeld's theorem.

3 Analytic rank of E_{102}

All computer calculations in this section are made in SAGE if not stated otherwise. Through the function `analytic_rank`, which does not return a provably correct result in all cases, we run positive values for k smaller than 200. The data we find is presented in Table 1. Note that $k = 102$ is not the only good choice, since after Lemma 2.1 any even integer k that gives E_k with analytic rank three would work for us. Probably in the family given with (2.3) there are infinitely many even k for which $\mathrm{ord}_{s=1} L(E_k, s) = 3$.

k	conductor N_k
65	$2^5 \cdot 3^3 \cdot 11 \cdot 19 \cdot 73$
102	$2^3 \cdot 3^3 \cdot 103 \cdot 10303$
114	$2^3 \cdot 3^3 \cdot 5 \cdot 13 \cdot 23 \cdot 991$
129	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 337$
136	$2^2 \cdot 3^3 \cdot 7 \cdot 43 \cdot 61 \cdot 137$
141	$2^5 \cdot 3^3 \cdot 19 \cdot 71 \cdot 1039$
145	$2^5 \cdot 3^3 \cdot 7 \cdot 19 \cdot 73 \cdot 157$
162	$2^3 \cdot 3^3 \cdot 163 \cdot 26083$
184	$2^2 \cdot 3^3 \cdot 5 \cdot 37 \cdot 151 \cdot 223$
187	$2^4 \cdot 3^3 \cdot 7 \cdot 47 \cdot 4969$
191	$2^4 \cdot 3^3 \cdot 12097$

Table 1: Elliptic curves E_k of analytic rank 3

Assuming Birch and Swynnerton-Dyer conjecture, as one can see by examining the Mordell-Weil group $E_{102}(\mathbb{Q})$, the analytic rank is 3. However we want to show unconditional proof for the fact that this analytic rank is odd and at least 3. This can be achieved if we proceed in a similar way like in [3].

More precisely, SAGE unconditionally returns $\omega = -1$ and $L(E_{102}, 1) = 0$. It also gives $(-2.80575576483894 \cdot 10^{-13}, 4.32590860129513 \cdot 10^{-33})$ as the value of `L.deriv_at1(200000)`. Here the first value is an upper bound for $L'(E_{102}, 1)$, and the second term is the error size.

There are lower bounds for the canonical height of non-torsion points of elliptic curves like the bound of Hindry-Silverman given in Theorem 0.3 [8]. It says that if N is the conductor of E, Δ – the discriminant of its minimal model, and $\sigma = \log|\Delta| / \log N$, then for any non-torsion point $P \in E(\mathbb{Q})$ we have

$$\hat{h}(P) \geq \frac{2 \log|\Delta|}{(20\sigma)^8 10^{1.1+4\sigma}}.$$

The discriminant of E_{102} is $\Delta = -2^8 \cdot 3^3 \cdot 103 \cdot 10303$ so the Weierstrass equation (2.3) coincides with its minimal global model. We compute the Hindry-Silverman's bound in our case. It is $7.14186994767245 \cdot 10^{-16}$. Unfortunately it is 'too close' to zero compared to the approximate value of $L'(E_{102}, 1)$ to be able to use it with Gross-Zagier formula. What we do is to find a better lower bound for the rational points on $E_{102}(\mathbb{Q})$.

Lemma 3.1. *For all rational points $P \in E_{102}(\mathbb{Q})/\{0\}$ where*

$$E_{102} \ : \ y^2 = x^3 - 31212x + 2122420$$

we have

$$\hat{h}(P) \geq 0.38744\,,$$

in particular the torsion subgroup of $E_{102}(\mathbb{Q})$ is the trivial group. Something more, for all non-integral rational points $P \in E_{102}(\mathbb{Q})/\{0\}$ we have

$$\hat{h}(P) \geq 1.48606\,.$$

Note that we use the Silverman's definition for Néron-Tate height [13], which is normalized as being twice smaller than the height given in SAGE. We will denote the latter as $\hat{h}_S$.

Before we present the proof of Lemma 3.1 we show how to apply it to prove that $L'(E_{102},1) = 0$ and hence $\mathrm{ord}_{s=1}L(E_{102},s) \geq 3$. By list of the Heegner discriminants for E_{102} we take the point H corresponding to the imaginary quadratic field $\mathbb{Q}(\sqrt{-71})$. Recall that Gross-Zagier formula ([7] and Theorem 23.4 [9] for more elementary approach) claims that if $L(E,1) = 0$, then there are infinitely many twists with $d < 0$ satisfying certain conditions, such that for a Heegner point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ we have

$$L'(E,1)L(E^d,1) = c_{E,d}\hat{h}(P_d) \tag{3.1}$$

for some real non-zero constant $c_{E,d}$ depending on the elliptic curve E and d. Through the function `heegner_point_height`, which uses Gross-Zagier formula and computation of L-series with some precision, we see that the canonical height $\hat{h}_S$ of $H = P_{-71}$ is in the interval $[-0.00087635965, 0.00087636244]$:

```
E102.heegner_discriminants_list(4)
[-71, -143, -191, -263]
a71=E102.heegner_point_height(-71,prec=3)
a71.str(style='brackets')
    '[-0.00087635965 .. 0.00087636244]'
```

This means that $0 \leq \hat{h}_S(H) \leq 0.00087636244$. Also, by Corollary 3.3 [12] and $\omega = -1$, it follows that H equals its complex conjugate. Therefore not only H lies on $E_{102}(\mathbb{Q}(\sqrt{-71}))$ but it is a rational point: $H \in E_{102}(\mathbb{Q})$. By Lemma 3.1 it is clear that the Heegner point H is actually the infinite point, because $\hat{h}_S(H) = 2\hat{h}(H) \leq 0.00087636244$. We also check that $L(E_{102}^{-71},1) \neq 0$:

```
E71=E102.quadratic_twist(-71)
E71.lseries().at1(10^7)
```

gives $L(E_{102}^{-71},1) = 0.682040095555640 \pm 1.40979860223528 \cdot 10^{-20}$. Now from $\hat{h}(H) = 0$ and (3.1) it follows $L'(E_{102},1) = 0$.

We will use the Néron's definition of local heights (Theorem 18.1[13]) such that the canonical height is expressed like the sum $\hat{h}(P) = \sum_{\nu \in M_{\mathbb{Q}}} \lambda_\nu(P)$ (Theorem 18.2[13]) and the valuation ν arises from a rational prime or is the usual absolute value at the real field. We will write the finite primes with p and for any integer n and $x = x_1/x_2 \in \mathbb{Q}$ such that $(x_1,x_2) = (x_1,p) = (x_2,p) = 1$, we introduce $\mathrm{ord}_\nu(p^n x) = \mathrm{ord}_p(p^n x) := n$, $|p^n x|_\nu := p^{-n}$ and $\nu(p^n x) := n \log p$.

Let E is an elliptic curve defined over the field of rational numbers with the Weierstrass equation

$$E \;:\; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2}$$

and the quantities b_2, b_4, b_6, b_8, c_4 are the ones defined in III.1 [13]. In this notation the duplication formula for the point $P = (x,y) \in E(\mathbb{Q})$ reads

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}\,.$$

Let $t = 1/x$ and

$$z(x) = 1 - b_4 t^2 - 2b_6 t^3 - b_8 t^4 = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{x^4}.$$

Let also

$$\begin{aligned} \psi_2 &= 2y + a_1 x + a_3 \\ \psi_3 &= 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8 . \end{aligned} \tag{3.3}$$

We formulate Theorem 1.2 [14] into the following lemma

Lemma 3.2. *(Local Height at the Archimedean Valuation) Let $E(\mathbb{R})$ does not contain a point P with $x(P) = 0$. Then for all $P \in E(\mathbb{R})/\{O\}$*

$$\lambda_\infty(P) = \frac{1}{2}\log|x(P)| + \frac{1}{8}\sum_{n=0}^{\infty} 4^{-n}\log|z(2^n P)|.$$

The following lemma combines Theorem 4.2 [10] and Theorem 5.2b), c), d) [14]:

Lemma 3.3. *(Local Height at Non-Archimedean Valuations) Let $E/\mathbb{Q}$ be an elliptic curve given with a Weierstrass equation (3.2) which is minimal at ν and let $P \in E(\mathbb{Q}_\nu)$. Also let ψ_2 and ψ_3 are defined by (3.3).*

(a) If

$$ord_\nu(3x^2 + 2a_2 x + a_4 - a_1 y) \le 0 \text{ or } ord_\nu(2y + a_1 x + a_3) \le 0,$$

then

$$\lambda_\nu(P) = \frac{1}{2}\max(0, \log|x(P)|_\nu).$$

(b) Otherwise, if $ord_\nu(c_4) = 0$, then for $N = ord_\nu(\Delta)$ and $n = \min\left(ord_\nu(\psi_2(P)), N/2\right)$

$$\lambda_\nu(P) = \frac{n(N-n)}{2N^2}\log|\Delta|_\nu.$$

(c) Otherwise, if $ord_\nu\left(\psi_3(P)\right) \ge 3ord_\nu\left(\psi_2(P)\right)$, then

$$\lambda_\nu(P) = \frac{1}{3}\log|\psi_2(P)|_\nu.$$

(d) Otherwise

$$\lambda_\nu(P) = \frac{1}{8}\log|\psi_3(P)|_\nu.$$

The discussion in §5 of [14] verifies the correctness of all possible conditions in the different cases.

We see that in our case $a_1 = a_2 = a_3 = 0$, $a_4 = -3k^2$, $a_6 = 2k^3+4$ and $\Delta = (-16)(4(-3k^2)^3 + 27(2k^3+4)^2) = -16.16.27.(k^3+1) = -2^8 \cdot 3^3 \cdot 103 \cdot 10303$. We also need the quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 = 0, \\ b_4 &= 2a_4 + a_1 a_3 = -6k^2, \\ b_6 &= a_3^2 + 4a_6 = 8(k^3+2), \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 = -9k^4, \\ c_4 &= b_2^2 - 24b_4 = -24(-6k^2) = 2^4 \cdot 3^2 \cdot k^2 = 2^6 \cdot 3^4 \cdot 17^2 \end{aligned}$$

because $k = 102 = 2 \cdot 3 \cdot 17$. Also

$$\begin{aligned} \psi_2 &= 2y \\ \psi_3 &= 3x^4 - 18k^2x^2 + 24(k^3+2)x - 9k^4 \,. \end{aligned}$$

Now we are ready to present the proof of Lemma 3.1.

Proof. (Lemma 3.1) First we translate Lemma 3.3 for our curve E_{102} defined with (2.3) for $k = 102$. As we mentioned before by the form of the discriminant Δ, such that for any non-Archimedean valuation ν we have $\nu(\Delta) < 12$, and $a_i \in \mathbb{Z}$, it follows that the Weierstrass equation (2.3) is minimal at any ν/ see [13].VII.Remark 1.1/. Then we have

(a) If

$$\mathrm{ord}_\nu(3x^2 - 3k^2) \le 0 \text{ or } \mathrm{ord}_\nu(2y) \le 0\,,$$

then

$$\lambda_\nu = \frac{1}{2}\max(0, \log|x(P)|_\nu)\,.$$

(b) Otherwise we are in a case where P does not have a good reduction modulo p and we have $p \mid \Delta$. So, if $\mathrm{ord}_\nu(c_4) = \mathrm{ord}_\nu(2^6 \cdot 3^4 \cdot 17^2) = 0$, i.e. ν comes from 103 or 10303, then $N = \mathrm{ord}_\nu(\Delta) = 1$ and $n = \min(\mathrm{ord}_\nu\,(\psi_2(P))\,, N/2) = \min(\mathrm{ord}_\nu(2y), 1/2) = 1/2$. Therefore

$$\lambda_\nu(P) = \frac{1/2(1-1/2)}{2}\log|\Delta|_\nu = \frac{1}{8}\log|\Delta|_\nu\,.$$

(c) Otherwise, i.e. ν is the valuation at the primes 2 or 3 and P fails the conditions of (a), if $\mathrm{ord}_\nu\,(\psi_3(P)) \ge 3\mathrm{ord}_\nu\,(\psi_2(P))$, then

$$\lambda_\nu(P) = \frac{1}{3}\log|\psi_2(P)|_\nu = \frac{1}{3}\log|2y|_\nu\,.$$

(d) Otherwise

$$\lambda_\nu(P) = \frac{1}{8}\log|\psi_3(P)|_\nu\,.$$

For any non-torsion point P on $E_{102}(\mathbb{Q})$ let $x(P) = a/b$ for $(a,b) = 1$ and $b > 0$, and $y(P) = y = c/d$ with $(c,d) = 1$, $d > 0$. From equation (2.3) we have

$$\left(\frac{c}{d}\right)^2 = \left(\frac{a}{b}\right)^3 - 3k^2\frac{a}{b} + 2(k^3+2)$$

or the equivalent

$$b^3c^2 = d^2\left(a^3 - 3k^2ab^2 + 2(k^3+2)b^3\right)\,. \tag{3.4}$$

In (a) $\max(0, \log|x(P)|_\nu) = \max(0, \log|a/b|_\nu) > 0$ only if $\log|a/b|_\nu = \mathrm{ord}_\nu(b)\log p > 0$. If the local heights of P at the primes $p \mid \Delta$ are in cases (b),(c) and (d) we have $\mathrm{ord}_\nu\left(3(x^2-k^2)\right) = \mathrm{ord}_\nu\left(3(a^2-k^2)/b^2\right) > 0$. Let ν comes from 2 or 3 and consider cases (c) and (d). If $\mathrm{ord}_\nu(b) > 0$, then $\mathrm{ord}_\nu(a) = 0$, and since $2, 3 \mid k$, we will have $\mathrm{ord}_\nu(3(x^2-k^2)) < 0$ which is impossible. Thus $\mathrm{ord}_2(b) = \mathrm{ord}_3(b) = 0$.

If we are in case (b) ν comes from $q \in \{103, 10303\}$ and we also use that $\mathrm{ord}_\nu(2y) > 0$. This means that q divides c. If we assume that q divides b, i.e. $\mathrm{ord}_q(b) > 0$, after (3.4) it follows that q divides a as well - a contradiction. Hence in case (b) $\mathrm{ord}_{103}(b) = \mathrm{ord}_{10303}(b) = 0$.

In any case $\text{ord}_\nu(b) = 0$ if P is into (b), (c) or (d) , so in these cases we can add toward the local height expression $(\text{ord}_\nu(b)\log p)/2$. Combining these we get

$$\sum_{\nu\neq\infty} \lambda_\nu(P) = \frac{1}{2}\log b + \tilde{\lambda}_2 + \tilde{\lambda}_3 + \tilde{\lambda}_{103} + \tilde{\lambda}_{10303}\,, \tag{3.5}$$

where $\tilde{\lambda}_p$ for $p \mid \Delta$ are non-zero only if the point P falls into some of the corresponding cases (b), (c) or (d) and then $\tilde{\lambda}_p = \lambda_p(P)$.

Clearly for any $P \in E_{102}(\mathbb{Q})$ falling in case (b) we have

$$\lambda_{103}(P) = \frac{1}{8}\log|\Delta|_\nu = -\frac{1}{8}\log 103 \tag{3.6}$$

$$\lambda_{10303}(P) = \frac{1}{8}\log|\Delta|_\nu = -\frac{1}{8}\log 10303 \tag{3.7}$$

Next we estimate from below λ_2 and λ_3 from cases (c) or (d). Note that in these cases we have both $\text{ord}_\nu\big(3(x^2-k^2)\big) > 0$ and $\text{ord}_\nu(2y) > 0$.

$\underline{p=2}$ Here $\nu(3(a^2-k^2b^2)/b^2) > 0$ and $2 \mid k$, so we get $2 \mid a$. From $\nu(2y) > 0$ it follows that 2 does not divide d. If 2^2 divides c, then the right-hand side of the equality (3.4) should be divisible by 2^4. Note that $8 \mid a^3, 3k^2ab^2$ but $4 \parallel 2(k^3+2)b^3$. As $2 \nmid d$, then the right-hand side of (3.4) is $\equiv 4 \pmod 8$. Therefore we could have at most $2 \parallel c$. The left-hand side of (3.4) is surely divisible by 2 and hence $2 \mid c$. Then the only possibility is $\text{ord}_2(2y) = 2$.

Let us take a look at $\psi_3(P)$. As $2 \nmid b$ we are interested in the 2-order of $b^4\psi_3$:

$$3a^4 - 18k^2a^2b^2 + 24(k^3+2)ab^3 - 9k^4b^4\,. \tag{3.8}$$

The exact power of two dividing the summand $9k^4b^4$ is 4. If $2^2 \mid a$ we will have $2^5 \mid b^4\psi_3 + 9k^4b^4$, thus $2^4 \parallel \psi_3$. If $2 \parallel a$, then $2^4 \parallel 3a^4, 9k^4b^4$ and hence $2^5 \mid b^4\psi_3$. Therefore in any case $\text{ord}_2(\psi_3) \geq 4$. We conclude that for $\text{ord}_2(2y) = 2$ with $\text{ord}_2(\psi_3) \geq 6$ we are in case (c) and

$$\lambda_2(P) = \frac{1}{3}\log|\psi_2(P)|_\nu = \frac{1}{3}\log|2y|_\nu = -\frac{2}{3}\log 2\,.$$

If $\text{ord}_2(\psi_3)$ is 4 or 5, then according to (d)

$$\lambda_2(P) = \frac{1}{8}\log|\psi_3(P)|_\nu = -\frac{1}{8}\cdot 4\log 2 = -\frac{1}{2}\log 2$$

or

$$\lambda_2(P) = \frac{1}{8}\log|\psi_3(P)|_\nu = -\frac{1}{8}\cdot 5\log 2 = -\frac{5}{8}\log 2\,.$$

In any case we get

$$\lambda_2(P) \geq -\frac{2}{3}\log 2\,. \tag{3.9}$$

$\underline{p=3}$ Again from $\nu(3(a^2-k^2b^2)/b^2) > 0$ and $\nu(2c/d) > 0$ it follows that $3 \mid c$ and $3 \nmid b, d$. Look at $b^4\psi_3(P)$ at (3.8). We see that $\psi_3/3 \equiv a^4 + 16ab^3 \equiv a(a^3+b^3) \pmod 3$ because $3 \mid k$. If we use $3 \mid c$ in (3.4) we see that $3^2 \mid a^3 + 4b^3$. If $3 \mid a$ we should have $3 \mid b$ – a contradiction, hence $3 \nmid a$. If $3^2 \mid a^3 + b^3$, then as it already divides $a^3 + 4b^3$, it would follow

$3^2 \mid 3b^3$ which is impossible. Therefore at most $3 \parallel a^3+b^3$ and finally at most $3^2 \parallel \psi_3$, i.e. $\mathrm{ord}_3(\psi_3(P)) \leq 2$. In this case we always have $\mathrm{ord}_\nu(\psi_3(P)) < 3\mathrm{ord}_\nu(\psi_2(P))$, that is situation (d) with $\lambda_3(P) = \log|\psi_3(P)|_\nu/8 = -(\mathrm{ord}_3(\psi_3)\log 3)/8$. Then, since the 3-order of $\psi_3(P)$ is at most 2, in any case

$$\lambda_3(P) \geq -\frac{1}{4}\log 3\,. \tag{3.10}$$

When we combine the estimates (3.6), (3.7), (3.9) and (3.10) into equation (3.5) we come to

$$\sum_{\nu\neq\infty}\lambda_\nu(P) \geq \frac{1}{2}\log b - \frac{2}{3}\log 2 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq \frac{1}{2}\log b - 2.47112\,. \tag{3.11}$$

$\underline{p=\infty}$ For computing λ_∞ we apply Lemma 3.2. It can be seen from the graphic of E_{102} that there are points on $E_{102}(\mathbb{R})$ with $x(P)=0$. So we want to translate $x \to x+r$ such that $x+r>0$ for every $x \in E_{102}(\mathbb{R})$. On page 340 of [14] Silverman calls this transformation *the shifting trick*. Indeed, by Theorem 18.3.a)[13] it follows that the local height at Archimedean valuations depends only on the isomorphism class of $E/\mathbb{Q}_\nu$.

If after the translation with r we denote $E_{102} \to E'_{102}$ and $P \to P'$, by the above-mentioned property of the local height $\lambda_\infty(P) = \lambda_\infty(P')$. Note that with the change $x \to x+r$ the discriminant stays the same. Then

$$\lambda_\infty(P) = \frac{1}{2}\log(x+r) + \frac{1}{2}\sum_{n=0}^{\infty}\frac{\log\left(z(2^nP')\right)}{4^{n+1}}\,.$$

We take $r=516$ after we check numerically that with this r we achieve the best lower bound of $z(x)$ for $x \geq x_0$ where x_0 is the only real root of the equation $(x-r)^3 - 31212(x-r) + 2122420 = 0$. More precisely we run the MATHEMATICA procedure

```
Proc[r_] := (
  f[x_] := x^3 - 3*102^2*x + 2*102^3 + 4;
  f1[x_] := f[x - r];
  Clear[a];
  b2 := 4*Coefficient[f1[a], a, 2];
  b4 := 2*Coefficient[f1[a], a, 1];
  b6 := 4*Coefficient[f1[a], a, 0];
  b8 := 4*Coefficient[f1[a], a, 2]*Coefficient[f1[a], a, 0] -
    Coefficient[f1[a], a, 1]^2;
  P1[x_] := x^4 - b4*x^2 - 2*b6*x - b8;
  x0 = x /. Last[N[FindInstance[f1[x] == 0, x, Reals]]];
  minZ = Log[First[NMinimize[{P1[x]/x^4 , x >= x0}, x]]];
  Return [(minZ/3 + Log[x0])/2];
  ).
```

Then $r=516$ gives the best lower bound

$$\lambda_\infty(P) \geq \frac{1}{2}\left\{\log x_0 + \frac{1}{3}\log\left(\min_{x\geq x_0} z(x)\right)\right\} \geq 2.85856\,. \tag{3.12}$$

If we straight apply this estimate for any point $P \in E_{102}(\mathbb{Q})/\{0\}$ including the integral points, we have $b \geq 1$, so after (3.11)

$$\hat{h}(P) \geq \sum_{\nu\neq\infty}\lambda_\nu(P) + \lambda_\infty(P) \geq -2.47112 + 2.85856 \geq 0.38744\,.$$

This lower bound is already much better than Hindry-Silverman's bound. Note that it holds for all integral points as well, including the torsion points different from the infinite point. It follows that the only torsion point on $E_{102}(\mathbb{Q})$ is $0 = (0:1:0)$.

We still try to achieve better lower bound at the non-Archimedean local heights for non-integral points. Looking at (3.4), we see that for any prime power $q \parallel b$ we get $q^3 \parallel d^2$ and it follows that every q is on even power, i.e. b is a perfect square. If $2 \mid b$ we have $b \geq 4$. As from $2 \mid b$ it follows that the local height $\lambda_2(P)$ cannot fall into cases (c) and (d), it is given with case (a). Then

$$\sum_{\nu \neq \infty} \lambda_\nu(P) \geq \frac{1}{2}\log 4 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq -1.31587\,.$$

If $2 \nmid b$ we should have $b \geq 3^2$ and

$$\sum_{\nu \neq \infty} \lambda_\nu(P) \geq \frac{1}{2}\log 9 - \frac{2}{3}\log 2 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq -1.3725\,.$$

From the latter estimates and (3.12) we have

$$\hat{h}(P) \geq 2.85856 - 1.3725 = 1.48606$$

for any non-integral point $P \in E_{102}(\mathbb{Q})$. This proves the lemma. $\square$

We check that $L^{(3)}(E,1) \neq 0$ by `E102.analytic_rank(leading_coefficient=True)`, because the coefficient is far from zero: SAGE gives

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^3} \approx 264.870335957636575\,.$$

For our goal $\mathrm{ord}_{s=1}L(E_{102},s) \geq 3$ is enough so we do not delve more in the precision of the last computation. It suggests that $\mathrm{ord}_{s=1}L(E_{102},s) = 3$, as predicted by Birch and Swinnerton-Dyer conjecture.

Acknowledgements I am indebted to my supervisor András Biró for his guidance and constructive criticism and to Kumar Murty for discussions on Godlfeld's theorem while being a hospitable advisor during my stay at University of Toronto. I am also thankful to Central European University Budapest Foundation for supporting my visit in Toronto.

References

[1] A. Biró, *Yokoi's conjecture*, Acta Arith. 106 (2003), no. 1, 85–104

[2] A. Biró, *Yokoi-Chowla conjecture and related problems*, Proceedings of the 2003 Nagoya Conference,Held at Nagoya University, Nagoya, October 14–17, 2003, Ed.: S. Katayama, C. Levesque and T. Nakahara., Saga University, Faculty of Science and Engineering, Saga, 2004

[3] J. P. Buhler, B. H. Gross and D. B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. 44 (1985), 473–481

[4] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa (4) 3 (1976), 623–663

[5] D. Goldfeld, *The Gauss class number problem for imaginary quadratic fields*, Heegner Points and Rankin L-Series, Ed.: H. Darmon and S. Zhang, Cambridge University Press, 2004

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

[7] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320

[8] M. Hindry and J. H. Silverman, *The Canonical Height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450

[9] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS, 2004

[10] S. Lang, *Elliptic curves: Diophantine Analysis* , Springer, 1978

[11] R. A. Mollin, L.-C. Zhang and P. Kemp, *A lower bound for the class number of a real quadratic field of ERD type*, Canad. Math. Bull. 37 (1994), 90–96

[12] H. Nakazato, *Heegner points on modular elliptic curves*, Proc. Japan Acad. 72, Ser. A (1996), 223–225

[13] J. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Ed., Springer, 2010

[14] J. Silverman, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358