HEIGHT OF RATIONAL POINTS ON QUADRATIC TWISTS
OF A GIVEN ELLIPTIC CURVE

by

Pierre Le Boudec

Abstract. — We formulate a conjecture about the distribution of the canonical height of the lowest non-torsion rational point on a quadratic twist of a given elliptic curve, as the twist varies. This conjecture seems to be very deep and we can only prove partial results in this direction.

Contents

1. Introduction.......................... 1
2. Preliminaries.......................... 5
3. Proofs of Theorems 1 and 2............... 7
References.................................. 9

1. Introduction

1.1. Rational points on quadratic twists. — Let $E$ be the elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

where $(A, B) \in \mathbb{Z}^2$ satisfies $4A^3 + 27B^2 \neq 0$. For every squarefree integer $d \geq 1$, we denote by $E_d$ the quadratic twist of $E$ defined over $\mathbb{Q}$ by the equation

$$dy^2 = x^3 + Ax + B.$$  

(1.1)

From now on, we view $A$ and $B$ as being fixed, and $d$ as a varying parameter. In particular, the dependences on $A$ and $B$ of the constants involved in the notations $O$, $\ll$ and $\gg$ will not be specified.

The celebrated Mordell-Weil Theorem states that the abelian group $E_d(\mathbb{Q})$ is finitely generated. In other words, there exists a non-negative integer rank $\text{rank} E_d(\mathbb{Q})$, the algebraic rank of the curve $E_d$ over $\mathbb{Q}$, such that

$$E_d(\mathbb{Q}) \simeq E_d(\mathbb{Q})_{\text{tors}} \times 2^{\text{rank} E_d(\mathbb{Q})},$$

where $E_d(\mathbb{Q})_{\text{tors}}$ is a finite abelian group.

2010 Mathematics Subject Classification. — 11D45, 11G05, 14G05.

Key words and phrases. — Elliptic curves, quadratic twists, rational points, canonical height.
Let $\hat{h}_{E_d}$ be the canonical height on $E_d$. The goal of this article is to study the distribution, as $d$ varies, of the quantity $\eta_d(A, B)$ defined by
\[
\log \eta_d(A, B) = \min \{ \hat{h}_{E_d}(P), P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}} \},
\]
if rank $E_d(\mathbb{Q}) \geq 1$ and $\eta_d(A, B) = \infty$ if rank $E_d(\mathbb{Q}) = 0$.

Let us recall the conjecture of Goldfeld (see [Gol79]) about the average order of rank $E_d(\mathbb{Q})$ as $d$ varies. Let $\mathcal{S}(X)$ be the set of positive squarefree integers up to $X$. Goldfeld’s Conjecture states that
\[
(1.2) \quad \sum_{d \in \mathcal{S}(X)} \text{rank } E_d(\mathbb{Q}) \sim \frac{1}{2} \# \mathcal{S}(X).
\]

Let $L(E_d, s)$ denote the Hasse-Weil $L$-function associated to the curve $E_d$ and let rank$_{\text{an}} E_d(\mathbb{Q})$ be the order of the zero of $L(E_d, s)$ at the central point. Recall that the Parity Conjecture asserts that rank $E_d(\mathbb{Q}) = \text{rank}_{\text{an}} E_d(\mathbb{Q}) \pmod{2}$. Together with the conjectural estimate (1.2), it implies that, for $\varepsilon \in \{0, 1\}$, we have
\[
(1.3) \quad \# \{ d \in \mathcal{S}(X), \text{rank } E_d(\mathbb{Q}) = \varepsilon \} \sim \frac{1}{2} \# \mathcal{S}(X),
\]
and
\[
(1.4) \quad \# \{ d \in \mathcal{S}(X), \text{rank } E_d(\mathbb{Q}) \geq 2 \} = o(X).
\]

The estimates (1.3) and (1.4) are widely believed. In particular, they are supported by the Katz-Sarnak Philosophy (see [KS99]) about zeros of $L$-functions and also by Random Matrix Theory heuristics (see for instance [CKRS02]).

The conjectural estimate (1.4) states that the proportion of curves $E_d$ whose rank is at least 2 is negligible, and we work under the convention that $\eta_d(A, B) = \infty$ if rank $E_d(\mathbb{Q}) = 0$. As a result, in what follows, we restrict our investigation of $\eta_d(A, B)$ to the curves $E_d$ which have rank 1.

1.2. Analogy between quadratic twists and number fields - A Conjecture.

It is very instructive to describe the analogy between quadratic twists of a given elliptic curve and number fields (see for instance [Del07], Section 1]). According to this analogy, rank one quadratic twists correspond to real quadratic fields, and the equation (1.4) corresponds to the Pell equation.

Let $D \geq 1$ be a fundamental discriminant, and let $\text{Cl}(D)$ and $\varepsilon_D$ respectively denote the class group and the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Describing precisely the distribution of $\varepsilon_D$ is considered as being extremely difficult, in particular because it is linked to the celebrated Class Number One problem for real quadratic fields. Indeed, if we let $\mathcal{D}(X)$ be the set of positive fundamental discriminants up to $X$, then it is known (see [Dat93]) that there exists a constant $C > 0$ such that
\[
(1.5) \quad \sum_{D \in \mathcal{D}(X)} \# \text{Cl}(D) \log |\varepsilon_D| \sim CX^{3/2}.
\]

Let us note that the corresponding formula for positive discriminants (not necessarily fundamental) goes back to Siegel [Sie44]. In the asymptotic formula (1.5), the two quantities $\# \text{Cl}(D)$ and $\log |\varepsilon_D|$ are inextricably mixed and no one has ever been able to separate them.

At the beginning of the eighties, Hooley [Hoo84] and Sarnak [Sar82], [Sar85] have, at the same time but independently, studied this problem. Their investigations led people to believe that, most of the time, $\varepsilon_D$ should be huge compared to $D$. In particular, as recently remarked by Fouvry and Jouve (see [FJ13], Equation (3)), their conjectures would imply the following.
**Conjecture A.** — Let \( \varepsilon > 0 \) be fixed. For almost every fundamental discriminant \( D \geq 1 \), we have

\[
\varepsilon_D > e^{D^{1/2-\varepsilon}}.
\]

Let us note that Conjecture [A] and the asymptotic formula [LB] agree with the Cohen-Lenstra heuristics [CL84] which predict that \( \# \text{Cl}(D) \) should be small very often, and even equal to 1 for a positive proportion of \( D \)'s.

Let us now explain why \( \varepsilon_D \) and \( \eta_d(A, B) \) should have similar distributions. We recall that we are only concerned with the curves \( E_d \) whose rank is equal to 1.

An asymptotic formula analog of [LB] conjecturally arises from averaging over squarefree integers \( d \geq 1 \) the central values \( L'(E_d, 1/2) \). Indeed, it is known that the average order of \( L'(E_d, 1/2) \) has size \( \log d \) (see [BFH90], [MM91] and [twa90]).

In addition, recall that the full Birch and Swinnerton-Dyer Conjecture predicts that \( L'(E_d, 1/2) \) is essentially equal to \( d^{-3/2} \# \text{III}(E_d) \log \eta_d(A, B) \), where \( \text{III}(E_d) \) denotes the Tate-Shafarevich group of the curve \( E_d \). Therefore, it is reasonable to expect that there exists a constant \( C_E > 0 \) such that

\[
\sum_{d \in S(X)} \# \text{III}(E_d) \log \eta_d(A, B) \sim C_E X^{3/2} \log X.
\]

The similarities between the asymptotic formulas [LB] and [LB] are remarkable. In particular, the two quantities \( \# \text{III}(E_d) \) and \( \log \eta_d(A, B) \) also seem to be very hard to separate.

Delaunay [Del01] has carried out the Cohen-Lenstra heuristics to determine the distribution of \( \# \text{III}(E_d) \) for curves \( E_d \) which have rank 1. He obtained that \( \# \text{III}(E_d) \) should be small very often, and even equal to 1 for a positive proportion of \( d \)'s. In addition, it is to be noted that the recent work of Bhargava, Kane, Lenstra, Poonen and Rains [BKL+13], which uses different methods, leads to the same predictions.

These observations led Delaunay [Del05] to conjecture that the average order of \( \log \eta_d(A, B) \) for curves \( E_d \) with rank equal to 1 should be at least \( d^{1/2-\varepsilon} / \log \log d \) for some absolute constant \( c > 0 \). Guided by the analogy described above and Conjecture [A] we go further in this direction and conjecture that for any fixed \( \varepsilon > 0 \), almost every squarefree integer \( d \geq 1 \) for which rank \( E_d(\Q) = 1 \) satisfies

\[
\eta_d(A, B) > e^{d^{1/2-\varepsilon}}.
\]

As previously explained, the proportion of curves with rank at least 2 is conjectured to be negligible so we are led to the following analog of Conjecture [A]

**Conjecture 1.** — Let \( (A, B) \in \Z^2 \) be such that \( 4A^3 + 27B^2 \neq 0 \), and let \( \varepsilon > 0 \) be fixed. For almost every squarefree integer \( d \geq 1 \), we have

\[
\eta_d(A, B) > e^{d^{1/2-\varepsilon}}.
\]

Lang conjectured an upper bound for the canonical height of the lowest non-torsion rational point on an elliptic curve (see [Lan83] Conjecture 3), and it is implicit in his work that this upper bound should be almost optimal for most curves. It is worth noting that Conjecture [I] is in agreement with this general philosophy.

Conversely, Conjecture [I] gives conjectural information about the size of \( \# \text{III}(E_d) \) for curves \( E_d \) which have rank 1. More precisely, if we assume the full Birch and Swinnerton-Dyer Conjecture, and also that a positive proportion of curves \( E_d \) have rank 1, and finally Conjecture [I] then one can show that for any fixed \( \varepsilon > 0 \), almost every squarefree integer \( d \geq 1 \) such that rank \( E_d(\Q) = 1 \) satisfies

\[
\# \text{III}(E_d) < d^\varepsilon.
\]
1.3. Results towards Conjecture [A] and Conjecture [1] — Conjecture [A] is far out of reach. Indeed, Hooley [Hoo84, Corollary of Theorem 1] was only able to prove that for any fixed $\varepsilon > 0$, almost every discriminant (not necessarily fundamental) $D \geq 1$ satisfies $\varepsilon D > D^{3/2-\varepsilon}$. Then, Fouvry and Jouve [FJ13b, Corollary 1] improved the exponent $3/2$ to $7/4$ and recently, Reuss [Reu14, Corollary 6] improved it to $3$. This should be compared with the trivial lower bound $\varepsilon D \gg D^{1/2}$.

The modesty of these results is a good clue of how deep Conjecture [A] must lie. The goal of this article is to establish analogs of these results for our problem. It is easy to check that for every squarefree integer $d \geq 1$, we have $\eta_d(A, B) \gg d^{1/8}$ (see Section 2.2). In addition, we will see that this lower bound is best possible.

Note that Silverman has proved that we always have such a lower bound for twists of abelian varieties in general (see [Sil84, Theorem 6]).

In the general case, we can prove the following result.

**Theorem 1.** — Let $(A, B) \in \mathbb{Z}^2$ be such that $4A^3 + 27B^2 \neq 0$, and let $\varepsilon > 0$ be fixed. For almost every squarefree integer $d \geq 1$, we have $\eta_d(A, B) > d^{1/4-\varepsilon}$.

The main purpose of this article is to study an example for which Theorem [1] can be improved. More precisely, we consider the elliptic curve linked to the congruent number problem, that is to say the case $(A, B) = (-1, 0)$. However, it is worth pointing out that our method would actually apply to any elliptic curve with full rational 2-torsion. We obtain the following result.

**Theorem 2.** — Let $\varepsilon > 0$ be fixed. For almost every squarefree integer $d \geq 1$, we have $\eta_d(-1, 0) > d^{5/8-\varepsilon}$.

To establish Theorems [1] and [2] one is led to investigate the cardinalities

\begin{equation}
N_{\alpha}(A, B; X) = \#\{d \in S(X), \eta_d(A, B) \leq d^{1/8+\alpha}\},
\end{equation}

and

\begin{equation}
N_\alpha^*(A, B; X) = \sum_{d \in S(X)} \#\{P \in E_d(Q) \setminus E_d(Q)_{\text{tors}}, \exp E_d(P) \leq d^{1/8+\alpha}\},
\end{equation}

where $\alpha > 0$ is fixed.

A simple observation shows that $N_\alpha^*(A, B; X) \ll X^{1/2+4\alpha}$ for any fixed $\alpha > 0$, which suffices to prove Theorem [1].

In the case $(A, B) = (-1, 0)$, we use the fact that the curves $E_d$ have full rational 2-torsion to perform complete 2-descents. We then use geometry of numbers methods to prove that $N_\alpha^*(-1, 0; X) \ll X^{1/2+\alpha+\varepsilon}$ for any fixed $\alpha > 0$ and $\varepsilon > 0$, which suffices to prove Theorem [2].

1.4. Acknowledgements. — It is a great pleasure for the author to thank Peter Sarnak for his interest in this problem, and for generously sharing his thoughts and intuition. The author would also like to thank Joe Silverman for his enlightening comments on an earlier version of the manuscript.

This work was started while the author was a Postdoctoral Member of the Institute for Advanced Study, he is now a Postdoctoral Researcher at the École Polytechnique Fédérale de Lausanne. The financial support and the perfect working conditions provided by these two institutions are gratefully acknowledged.
2. Preliminaries

2.1. Descent arguments. — We start by proving the following result, which gives a parametrization of the rational points on the curves $E_d$ in the general case.

Lemma 1. — Let $(A, B) \in \mathbb{Z}^2$ be such that $4A^3 + 27B^2 \neq 0$. Let also $d \geq 1$ be a squarefree integer and let $(x, y, z) \in \mathbb{Z} \times \mathbb{Z}_{\geq 1}^2$ satisfying $\gcd(x, y, z) = 1$ and

$$dy^2z = x^3 + Axz^2 + Bz^3.$$ 

Then, there is a unique way to write $x = d_1b_1x_1$, $z = d_1^2b_1^3$ and $d = d_0d_1$ where $(d_0, d_1, b_1, x_1) \in \mathbb{Z}_{\geq 1}^2 \times \mathbb{Z}$ satisfy the conditions $|\mu(d_0d_1)| = 1$ and $\gcd(x_1, d_1b_1) = 1$, and the equation

$$(2.1) \quad d_0y^2 = x_1^3 + Ax_1d_1^2b_1^2 + Ba_1^6b_1^6.$$ 

Proof. — Let $d_1 = \gcd(d, z)$ and write $d = d_0d_1$ and $z = d_1z_0$ for some $(d_0, z_0) \in \mathbb{Z}_{\geq 1}^2$ satisfying $\gcd(d_0, z_0) = 1$. We see that $d_1 \mid x^3$ and since $d_1$ is squarefree, we actually have $d_1 \mid x$. We can thus write $x = d_1x_0$ for some $x_0 \in \mathbb{Z}$. The equation becomes

$$d_0z_0y^2 = d_1 \left( x_0^3 + Ax_0z_0^2 + Bz_0^3 \right).$$

Therefore, the coprimality condition $\gcd(d_1, d_0y) = 1$ implies $d_1 \mid z_0$, and we write $z_0 = d_1z_1$ for some $z_1 \in \mathbb{Z}_{\geq 1}$. We thus get

$$d_0z_1y^2 = x_1^3 + Ax_1d_1^2z_1^2 + Bz_1^3.$$ 

Let $b_1 = \gcd(x_0, z_1)$. We have $\gcd(b_1, d_0y) = 1$ so we see that $z_1 = b_1^3$. We also write $x_0 = b_1x_1$ for some $x_1 \in \mathbb{Z}$. We obtain the equation (2.1). Moreover, using this equation, it is easy to check that the coprimality conditions between the variables $d_0$, $d_1$, $b_1$, $x_1$ and $y$ can be summed up as $|\mu(d_0d_1)| = 1$ and $\gcd(x_1, d_1b_1) = 1$, which completes the proof. \hfill \Box

The following lemma describes the familiar process of complete 2-descent in the case $(A, B) = (-1, 0)$, and is the first key tool in the proof of Theorem 2.

Lemma 2. — Let $d \geq 1$ be a squarefree integer and let $(x, y, z) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}^2$ satisfying $\gcd(x, y, z) = 1$ and

$$dy^2z = x^3 - xz^2.$$ 

Then, there is a unique way to write $x = \nu d_1d_2d_3b_1b_2^2$, $y = b_2b_3b_4$, $z = d_1^2b_1^3$ and $d = d_1d_2d_3d_4$ where $\nu \in \{-1, 1\}$ and $(d_1, d_2, d_3, d_4, b_1, b_2, b_3, b_4) \in \mathbb{Z}_{\geq 1}^8$ satisfy the conditions $|\mu(d_1d_2d_3d_4)| = 1$ and $\gcd(d_1b_1, d_2b_2) = 1$, and the system of equations

$$(2.2) \quad d_2b_2^2 - \nu d_1b_1^2 = d_3b_3^2,$$ 

$$(2.3) \quad \nu d_2b_2^2 + d_1b_1^2 = d_4b_4^2.$$ 

Proof. — Using lemma 1 we get the equation

$$d_0y^2 = x_1(x_1 - d_1b_1^2)(x_1 + d_1b_1^2).$$

Let us write the three factors of the right-hand side as products of a squarefree number and a square. We set $x_1 = \nu d_2b_2^2$, $x_1 - d_1b_1^2 = \nu d_3b_3^2$ and $x_1 + d_1b_1^2 = d_4b_4^2$ where $\nu \in \{-1, 1\}$ and $(d_2, d_3, d_4, b_2, b_3, b_4) \in \mathbb{Z}_{\geq 1}^6$ satisfies $|\mu(d_i)| = 1$ for $i \in \{2, 3, 4\}$. We thus get

$$d_0y^2 = d_2d_3d_4b_2^2b_3^2b_4^2,$$ 

which implies $d_0 = d_2d_3d_4$ and $y = b_2b_3b_4$, and ends the proof. \hfill \Box
2.2. Heights. — Let \( h : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{R}_{\geq 0} \) be the logarithmic absolute Weil height and let \( h_x : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{R}_{\geq 0} \) be defined by
\[
h_x(x : y : z) = h(x : z)
\]
if \((x : y : z) \neq (0 : 1 : 0)\) and \( h_x(0 : 1 : 0) = 0 \). It is easier for our purpose to work with the height \( h_x \) so we need to find a link between the heights \( \hat{h}_{E_d} \) and \( h_x \). This is achieved by the following lemma.

**Lemma 3.** — For any \( P \in E_d(\mathbb{Q}) \), we have
\[
\hat{h}_{E_d}(P) = \frac{1}{2} h_x(P) + O(1),
\]
where the constant involved in the notation \( O \) may depend on \( E \) but neither on the point \( P \) nor on the integer \( d \).

**Proof.** — Let \( i : E_d(\mathbb{Q}) \to E(\mathbb{Q}(\sqrt{d})) \) be the isomorphism defined by
\[
i(x : y : z) = (x : d^{1/2} y : z),
\]
and let \( \hat{h}_E \) be the canonical height on \( E \). For any \( P \in E_d(\mathbb{Q}) \), we have the equality
\[
\hat{h}_{E_d}(P) = \hat{h}_E(i(P)).
\]
In addition, for any \( Q \in E(\mathbb{Q}) \), we have
\[
\hat{h}_E(Q) = \frac{1}{2} h_x(Q) + O(1),
\]
where the constant involved in the notation \( O \) does not depend on the point \( Q \). This completes the proof since we have \( h_x(i(P)) = h_x(P) \) for any \( P \in E_d(\mathbb{Q}) \). \(\square\)

Let \( P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}} \). Replacing \( P \) by \(-P\) if necessary, we can assume that the point \( P \) has coordinates as in lemma 4. We thus have
\[
h_x(P) = \log \max\{|x_1|, d_1 b_1^2\}.
\]
Now, we note that the equation (2.1) gives the lower bound
\[
\max\{|x_1|, d_1 b_1^2\} \gg d_0^{1/3} y^{2/3}.
\]
As a result, we have
\[
\max\{|x_1|, d_1 b_1^2\} \gg (d_1 b_1^2)^{1/4}(d_0^{1/3} y^{2/3})^{3/4}
\]
\[
\gg d_1^{1/4} b_1^{1/2} y^{1/2}
\]
\[
\gg d_1^{1/4},
\]
since \( b_1, y \geq 1 \). Therefore, lemma 3 gives the lower bound stated in the introduction
\[
\eta_d(A, B) \gg d_1^{1/8}.
\]
In addition, this lower bound is best possible since it is attained for all squarefree integers \( d \in \{d_1(x_1^2 + Ax_1d_2^2 + Bd_3^2), d_1, x_1 \geq 1\} \). Note that by the work of Greaves [Gre92], we know that there is about \( X^{1/2} \) such integers up to \( X \).
2.3. Geometry of numbers. — The following lemma was recently established by the author [11] using results of Browning and Heath-Brown based on geometry of numbers. It gives an upper bound for the number of integral solutions to a certain cubic diophantine equation, and is the second key tool in the proof of Theorem [2]

Lemma 4. — Let \( f = (f_1, f_2, f_3) \in \mathbb{Z}^3_{\neq 0} \) be a vector satisfying the conditions \( \gcd(f_i, f_j) = 1 \) for \( i, j \in \{1, 2, 3\}, i \neq j \). Let \( U_i, V_i \geq 1 \) for \( i \in \{1, 2, 3\} \). Let also \( N_f = N_f(U_1, U_2, U_3, V_1, V_2, V_3) \) be the number of vectors \((u_1, u_2, u_3) \in \mathbb{Z}^3_{\neq 0} \) and \((v_1, v_2, v_3) \in \mathbb{Z}^3_{\neq 0} \) satisfying \( |u_i| \leq U_i, |v_i| \leq V_i \) for \( i \in \{1, 2, 3\} \), and the equation

\[
f_1u_1v_1^2 + f_2u_2v_2^2 + f_3u_3v_3^2 = 0,
\]

and such that \( \gcd(u_i, v_i, u_j v_j) = 1 \) for \( i, j \in \{1, 2, 3\}, i \neq j \). Let \( \varepsilon > 0 \) be fixed. We have the bound

\[
N_f \ll_f (U_1U_2U_3)^{2/3+\varepsilon}(V_1V_2V_3)^{1/3}.
\]

3. Proofs of Theorems [1] and [2]

3.1. Proof of Theorem [1] — Recall the respective definitions \([1.7\text{ and }1.8\)] of \( N_\alpha(A, B; X) \) and \( N_\alpha^*(A, B; X) \). Our aim is to prove that \( N_\alpha(A, B; X) \sim o(X) \) for fixed \( 0 < \alpha < 1/8 \). Since we clearly have \( N_\alpha(A, B; X) \leq N_\alpha^*(A, B; X) \), Theorem [1] follows from the following lemma.

Lemma 5. — Let \((A, B) \in \mathbb{Z}^2\) be such that \( 4A^3 + 27B^2 \neq 0 \), and let \( \alpha > 0 \) be fixed. We have the upper bound

\[
N_\alpha^*(A, B; X) \ll X^{1/2+4\alpha}.
\]

Proof. — We have

\[
N_\alpha^*(A, B; X) \leq \sum_{d \in \mathcal{S}(X)} \# \{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}}, \exp h_d(P) \leq X^{1/8+\alpha}\}.
\]

By lemma [3] we also have

\[
N_\alpha^*(A, B; X) \leq \sum_{d \in \mathcal{S}(X)} \# \{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}}, \exp h_d(P) \ll X^{1/4+2\alpha}\}.
\]

We note that if \((x : y : z) \in \mathbb{P}^2(\mathbb{Q})\) is a representative of \( P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}} \) then necessarily \( yz \neq 0 \). Lemma [1] thus gives

\[
N_\alpha^*(A, B; X) \leq 2\# \left\{ (d_0, d_1, b_1, y, x_1) \in \mathbb{Z}_{\geq 1}^4 \times \mathbb{Z}, \begin{array}{l}
|\mu(d_0d_1)| = 1 \\
\gcd(x_1, d_1b_1) = 1 \\
d_0d_1 \leq X \\
|x_1|, d_1b_1^2 \ll X^{1/4+2\alpha}
\end{array}\right\}.
\]

This implies that

\[
N_\alpha^*(A, B; X) \leq 2 \sum_{|x_1|, d_1b_1^2 \ll X^{1/4+2\alpha}} \# \left\{ (d_0, y) \in \mathbb{Z}_{\geq 1}^2, |\mu(d_0)| = 1 \right\}.
\]

For fixed \((d_1, b_1, x_1) \in \mathbb{Z}_{\geq 1}^2 \times \mathbb{Z}, \) the cardinality in the right-hand side is at most 1, so we get

\[
N_\alpha^*(A, B; X) \ll X^{1/2+4\alpha},
\]
as wished. \( \square \)
3.2. Proof of Theorem 2 — We now treat the case $(A, B) = (-1, 0)$. Our aim is to prove that $N_\alpha(-1, 0; X) = o(X)$ for fixed $0 < \alpha < 1/2$. Hence, Theorem 2 follows from the following lemma.

**Lemma 6.** — Let $\alpha > 0$ and $\varepsilon > 0$ be fixed. We have the upper bound

$$N_\alpha^*(1, 0; X) \ll X^{1/2 + \alpha + \varepsilon}.$$

**Proof.** — As in the proof of lemma 5, we have

$$N_\alpha^*(1, 0; X) \leq \sum_{d \in S(X)} \# \{ P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}}, \exp h_x(P) \ll X^{1/4 + 2\alpha} \}.$$

Lemma 2 gives

$$N_\alpha^*(1, 0; X) \leq 2^\# \left\{ (\nu, d, b) \in \{-1, 1\} \times \mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1} : \begin{array}{l}
|\mu(d_1 d_2 d_3 d_4)| = 1 \\
gcd(d_1 b_1, d_2 b_2) = 1 \\
d_1^2 d_2^2 d_3^2 d_4^2 \leq X \\
d_1 b_1^2, d_2 b_2^2 \ll X^{1/4 + 2\alpha} \end{array} \right\},$$

where we have set $d = (d_1, d_2, d_3, d_4)$ and $b = (b_1, b_2, b_3, b_4)$.

In the following, we assume that $\nu = 1$ since the other case $\nu = -1$ can be treated similarly. For $i \in \{1, 2, 3, 4\}$, let $D_i, B_i \geq 1/2$ run over the set of powers of 2 and let $N = N(D_1, D_2, D_3, D_4, B_1, B_2, B_3, B_4)$ be the number of $(d, b) \in \mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1}^4$ such that $D_i < d_i \leq 2D_i, B_i \leq b_i \leq 2B_i$ for $i \in \{1, 2, 3, 4\}$, and satisfying the conditions $|\mu(d_1 d_2 d_3 d_4)| = 1$, $\gcd(d_1 b_1, d_2 b_2) = 1$, and the equations

\begin{align*}
&d_2 b_2^2 - d_1 b_1^2 = d_3 b_3^2, \\
&d_2 b_2^2 + d_1 b_1^2 = d_4 b_4^2.
\end{align*}

Note that these equations and the conditions $d_1 b_1^2, d_2 b_2^2 \ll X^{1/4 + 2\alpha}$ imply that we also have $d_3 b_3^2, d_4 b_4^2 \ll X^{1/4 + 2\alpha}$. Moreover, we have

\begin{align*}
&2d_2 b_2^2 = d_3 b_3^2 + d_4 b_4^2, \\
&2d_1 b_1^2 = -d_3 b_3^2 + d_4 b_4^2.
\end{align*}

We have

$$N_\alpha^*(1, 0; X) \ll \sum_{D_i, B_i \in \{1, 2, 3, 4\}} N,$$

where the sum is over the $D_i, B_i, i \in \{1, 2, 3, 4\}$, satisfying

\begin{align*}
&D_1 D_2 D_3 D_4 \leq X, \\
&D_i B_i^2 \ll X^{1/4 + 2\alpha},
\end{align*}

for $i \in \{1, 2, 3, 4\}$.

For fixed $(d_1, d_2, b_1, b_2) \in \mathbb{Z}_{\geq 1}^2$, there is at most one $(d_4, b_4) \in \mathbb{Z}_{\geq 1}^2$ satisfying the equation (5.2) since $d_4$ is squarefree. Note that the condition $\gcd(d_1 b_1, d_2 b_2) = 1$ and the equation (5.1) imply that we actually have $\gcd(d_i b_i, d_j b_j) = 1$ for $i, j \in \{1, 2, 3\}, i \neq j$. Applying lemma 4 to count the number of $(d_1, d_2, d_3, b_1, b_2, b_3) \in \mathbb{Z}_{\geq 1}^3$ satisfying $D_i < d_i \leq 2D_i, B_i \leq b_i \leq 2B_i$ for $i \in \{1, 2, 3\}$, $\gcd(d_i b_i, d_j b_j) = 1$ for $i, j \in \{1, 2, 3\}, i \neq j$, and the equation (5.1), we get

$$N \ll X^{\varepsilon}(D_1 D_2 D_3)^{2/3}(B_1 B_2 B_3)^{1/3}.$$

Similarly, using also the equations (5.3) and (5.4), we obtain

$$N \ll X^{\varepsilon}(D_1 D_2 D_3)^{2/3}(B_1 B_2 B_3)^{1/3},$$

for fixed $(d_1, d_2, b_1, b_2) \in \mathbb{Z}_{\geq 1}^2$.
and also
\[ N \ll X^{\varepsilon} (D_1 D_3 D_4)^{2/3} (B_1 B_3 B_4)^{1/3}, \]
and finally
\[ N \ll X^{\varepsilon} (D_2 D_3 D_4)^{2/3} (B_2 B_3 B_4)^{1/3}. \]
Note that we could have \( \gcd(d_3 b_3, d_4 b_4) = 2 \) but this does not change anything in the application of lemma 4. Combining the four upper bounds (3.7), (3.8), (3.9) and (3.10), we get
\[ N \ll X^{\varepsilon} (D_1 D_2 D_3 D_4)^{1/2} (B_1 B_2 B_3 B_4)^{1/4}. \]
Summing successively over \( B_i, i \in \{1, 2, 3, 4\} \), using the condition (3.6), and over \( D_4 \) using the condition (3.5), we obtain
\[ N^* (-1, 0; X) \ll X^{\varepsilon} \sum_{D_i, B_i \atop i \in \{1, 2, 3, 4\}} (D_1 D_2 D_3 D_4)^{1/2} (B_1 B_2 B_3 B_4)^{1/4} \]
\[ \ll X^{1/8 + \alpha + \varepsilon} \sum_{D_i \atop i \in \{1, 2, 3, 4\}} (D_1 D_2 D_3 D_4)^{3/8} \]
\[ \ll X^{1/2 + \alpha + \varepsilon} \sum_{D_1 \atop i \in \{1, 2, 3\}} 1 \]
\[ \ll X^{1/2 + \alpha + 2\varepsilon}, \]
as wished.

References

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives, Ann. of Math. (2) 131 (1990), no. 1, 53–127.

[BKL+13] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves, Preprint, arXiv:1304.3971v2 (2013).

[CKRS02] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–315.

[CL84] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[Dat93] B. A. Datskovsky, A mean-value theorem for class numbers of quadratic extensions, A tribute to Emil Grosswald: number theory and related analysis, Contemp. Math., vol. 143, Amer. Math. Soc., Providence, RI, 1993, pp. 179–242.

[Del01] C. Delaunay, Heuristics on Tate-Shafarevitch groups of elliptic curves defined over \( \mathbb{Q} \), Experiment. Math. 10 (2001), no. 2, 191–196.

[Del05] C. Delaunay, Moments of the orders of Tate-Shafarevitch groups, Int. J. Number Theory 1 (2005), no. 2, 243–264.

[Del07] C. Delaunay, Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340.

[FJ13a] É. Fouvry and F. Jouve, A positive density of fundamental discriminants with large regulator, Pacific J. Math. 262 (2013), no. 1, 81–107.

[FJ13b] É. Fouvry and F. Jouve, Size of regulators and consecutive square-free numbers, Math. Z. 273 (2013), no. 3-4, 869–882.
[Gol79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118.

[Gre92] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) **43** (1992), no. 169, 45–65.

[Hoo84] C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. Reine Angew. Math. **353** (1984), 98–131.

[Iwa90] H. Iwaniec, *On the order of vanishing of modular L-functions at the critical point*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 2, 365–376.

[Ka99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[Lan83] S. Lang, *Conjectured Diophantine estimates on elliptic curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 155–171.

[LeB13] P. Le Boudec, *Density of rational points on a certain smooth birational threefold*, Preprint, arXiv:1308.0033v1 (2013).

[MM91] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475.

[Reu14] T. Reuss, *Pairs of k-free numbers, consecutive square-full numbers*, Preprint, arXiv:1212.3150v2 (2014).

[Sar82] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Theory **15** (1982), no. 2, 229–247.

[Sar85] ______, *Class numbers of indefinite binary quadratic forms. II*, J. Number Theory **21** (1985), no. 3, 333–346.

[Sil84] J. H. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), no. 2, 395–403.

---

Pierre Le Boudec, EPFL SB MATHGEOM T AN, MA C3 604 (Bâtiment MA), Station 8, CH-1015 Lausanne, Switzerland • E-mail : pierre.leboudec@epfl.ch