International Journal of Number Theory
Vol. 7, No. 3 (2011) 611–621

DOI: 10.1142/S1793042111004149

ON THE NUMBER OF INTEGER POINTS ON THE ELLIPTIC CURVE $y^2 = x^3 + Ax$

KONSTANTINOS A. DRAZIOTIS

Kromnis 33, 54 454
Thessaloniki, Greece
drazioti@gmail.com

Received 1 May 2009
Accepted 24 May 2010

It is given an upper bound for the number of the integer points of the elliptic curve $y^2 = x^3 + Ax$ $(A \in \mathbb{Z})$ and a conjecture of Schmidt is proven for this family of elliptic curves.

Keywords: Elliptic curves; unit equation; canonical height.

Mathematics Subject Classification 2010: 11D25, 11D45, 11G05

1. Introduction and Statement of Results

Let K be a number field and $\mathbb{O}_K$ be its ring of integers. Let also $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{O}_K$, be an affine model of an elliptic curve given in Weierstrass form, defined over the number field K. We denote by d_K the degree of K over $\mathbb{Q}$ and $E(\mathbb{O}_K)$ the set of points on E with coordinates in $\mathbb{O}_K$. Also $\Delta_E = -16(4A^3+27B^2)$, is the discriminant of E. In [11] Schmidt, using the results of [8], proved that for the elliptic curve E/K and for every $\varepsilon > 0$ we have $\#E(\mathbb{O}_K) \ll_\varepsilon |\Delta_E|^{1/2+\varepsilon}$ (with the symbol $\ll_\varepsilon h$ we mean $< c(\varepsilon)h$, where $c(\varepsilon)$ is a constant which depends only on ε). In [9, Corollary 3.12], Venkatesh and Helfgott, managed to replace the exponent $1/2$ in $|\Delta_E|$, by a constant $\simeq 0.2008$. Schmidt conjectured, for the case $K = \mathbb{Q}$, that we do not need the exponent $1/2$.

Conjecture I (Schmidt). *Let $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Then given $\varepsilon > 0$ we have $\#E(\mathbb{Z}) \ll_\varepsilon |\Delta_E|^\varepsilon$.*

Furthermore, a weaker version of Schmidt's conjecture also stated in [1, Conjecture II] is the following.

Conjecture II (Bombieri–Zannier–Schmidt). *Let $E : y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$. Then given $\varepsilon > 0$ we have $\#E(\mathbb{Z}) \ll_\varepsilon H(E)^\varepsilon$.*

With $H(E)$ we denote the affine height of the vector $(1, A, B)$. This conjecture is an immediate consequence of Schmidt's conjecture, since $|\Delta_E| \leq cH(E)^3$, for some absolute positive constant c. In [1] Conjecture II is proved for elliptic curves of the form $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$, with e_1, e_2, e_3 rational integers.

For the case where $E : y^2 = x^3 + Ax,\ A \in \mathbb{Z} - \{0\}$, Conjecture I is connected with Lang's conjecture for integer points [13, Chap. VI, §2, p. 140], which asserts that, if $E/\mathbb{Q}$ is quasi-minimal, then the number $\#E(\mathbb{Z})$ should be bounded only in terms of $r = \mathrm{rank}(E(\mathbb{Q}))$ (in fact is stated for a general quasi-minimal elliptic curve $E/\mathbb{Q}$). If Lang's conjecture holds for the quasi-minimal elliptic curve $E : y^2 = x^3 + Ax$, we get $\#E(\mathbb{Z}) < c^{1+r}$, where c is an absolute positive constant, but since $r \ll_\varepsilon |\Delta_E|^\varepsilon$ (see [16, Proposition 6.1, p. 311]) we get that Schmidt's conjecture holds for $E/\mathbb{Q}$. In [10], Hindry and Silverman proved that the number of S-integer points of E/K is at most

$$c^{\#S+(1+r)\sigma_{E/K}}, \tag{1.1}$$

where c depends only on K and

$$\sigma_{E/K} = \frac{\log(\text{discriminant of } E)}{\log(\text{conductor of } E)},$$

is the Szpiro ratio. Conjecturally $\sigma_{E/K}$ is bounded and so (in the case $K = \mathbb{Q}$) we get

$$\text{Szpiro conjecture} \Rightarrow \text{Lang's conjecture} \Rightarrow \text{Schmidt's conjecture}. \tag{1.2}$$

These consequences hold under the assumption that $E : y^2 = x^3 + Ax$ is quasi-minimal. Note that the quasi-minimality of $E/\mathbb{Q}$ is not necessary for Schmidt's conjecture. Also, the second consequence in relation (1.2) does not hold for general elliptic curves $y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Z}$, since we do not have "sharp" upper bounds for the rank of the elliptic curve, but the first consequence remains true even in the general case (proved in [10]).

In [15] Silverman proved Lang's conjecture for elliptic curves having integral j-invariant, thus Schmidt's conjecture holds for $y^2 = x^3 + Ax, A \in \mathbb{Z} - \{0\}$ (under the assumption that it is quasi-minimal). In [12] Gross and Silverman presented the previous bound (1.1), explicitly and in [4] the bound was improved. Also in [5, §4, Theorem 2], it was recovered by another method and with supplementary precision.

In the present paper we consider only rational integer points on the elliptic curve $y^2 = x^3 + Ax,\ A \in \mathbb{Z} - \{0\}$, which from now on will be denoted by E (unless differently stated). The first result of our paper is the proof of Schmidt's conjecture for E, without using the strong machinery used in [15] in the proof of that special case of Lang's conjecture. We shall prove the following.

Theorem 1.1. *If $A \neq 0$ is fourth-power-free integer and $\mathrm{ord}_2(A) \leq 1$, then Schmidt's conjecture holds for the family $y^2 = x^3 + Ax$.*

This theorem uses the assumptions that A is fourth-power-free integer and $\mathrm{ord}_2(A) \leq 1$ (which come from the quasi-minimality of $E/\mathbb{Q}$). We shall show how to exploit this restriction in order to prove Conjecture I (and finally Conjecture II) for the elliptic curve $E/\mathbb{Q}$. In order to prove Theorem 1, we shall get a bound for the rational integer points of E, of the form $\kappa_1\kappa_2^{\omega(A)+r}$, where κ_1 and κ_2 are absolute positive constants and $\omega(A)$ is the number of distinct prime divisors of A. The assumptions for A are used in order to get a "good" upper bound for the rank and also to get a lower bound for the Néron–Tate height of a non-torsion point.

The second result of the present paper, given in the last section, is the proof of a bound of the form $\#E(\mathbb{Z}) < \kappa_3\kappa_4^{\omega(A)}$, for some absolute constants κ_3 and κ_4, which holds without the assumptions on A (remark that the constants κ_3 and κ_4 are given explicit). Among the two previous bounds the first one (even with the restrictions on A) gives more information about the shape of the bound. That is a reason why we present it.

The basic tools used for the proof are an estimate for the number of solutions of a S-unit equation over a number field, a bound for the rank of an elliptic curve and a lower bound for the Néron–Tate height of a non-torsion point.

We give a brief outline of the present paper. We use multiplication by 2 on the points of the elliptic curve E in order to construct a S-unit equation on a number field, (say) L. This idea goes back to Chabauty's paper [3] and is used in a series of paper [2, 6, 14]. Then we count the number fields L. Our bound comes from the product of the number of solutions of the unit equation with the number of the fields L and a constant representing how large is the torsion group of $E(\mathbb{Q})$. In the final section we show how to exploit the restriction of quasi-minimality.

2. Auxiliary Results

Let $A \in \mathbb{Z}$ be a non-zero integer and $E : y^2 = x^3 + Ax$. Let P be a point in $E(\mathbb{Z})$ and $R \in E(\overline{\mathbb{Q}})$ such that $2R = P$. With $\mathbb{Q}(R)$ we denote the number field extension of $\mathbb{Q}$, generated by the coordinates $(x(R), y(R))$ of R. We set $K = \mathbb{Q}(\sqrt{-A})$ and $M = K(R)$. Let

$$\{P_i : \ i = 1, 2, \dots, r = \operatorname{rank}(E(\mathbb{Q}))\}$$

be a basis of $E(\mathbb{Q})$ modulo torsion and $R_i \in E(\overline{\mathbb{Q}})$ such that $2R_i = P_i$. Finally, we set

$$\Re = \left\{ L/\mathbb{Q} : L = K\left(x\left(\sum_{1\le i\le j} (R_i + T') \right)\right), \ j = 1, 2, \dots, r \right\},$$

where $T' \in 2^{-1}(E_{\mathrm{tor}}(\mathbb{Q})) = \{T' \in E : 2T' = T, T \text{ rational torsion point}\}$. We shall prove the following proposition.

Proposition 2.1. *Let $P \in E(\mathbb{Q})$ and $2R = P$. Then $x(R) \in L$, for some L in $\Re$.*

First we need the following lemma.

Lemma 2.2. *If P, R are as in Proposition 2.1, then $K(R) = K(x(R)) = K(y(R))$.*

Proof. We set $R = (s, t)$ and $P = (a, b)$. From $2R = P$ we get the following relations (see [2] or [14] and set $B = 0$):

$$s^4 - 4as^3 - 2As^2 - 4aAs + A^2 = 0 \tag{2.1}$$

and

$$t^4 - 6at^2 - 8bt - 3a^2 - 4A = 0. \tag{2.2}$$

Also $s = (t^2 - a)/2$. So $\mathbb{Q}(s) \subseteq \mathbb{Q}(s,t) = \mathbb{Q}(t)$. In order to prove that $\mathbb{Q}(t) \subseteq \mathbb{Q}(s)$, we work as follows. From Eq. (2.1) we get

$$a = \frac{(s^2 - A)^2}{4s(s^2 + A)}.$$

Since $t^2 = s(s^2 + A)$, we get

$$t = \pm\frac{s^2 - A}{2\sqrt{a}} \in \mathbb{Q}(s^2, \sqrt{a}) \subseteq \mathbb{Q}(s, \sqrt{a}).$$

Finally, $\sqrt{a} \in \mathbb{Q}(s)$ (for details about this, see Lemma 3.1 below) so $t \in \mathbb{Q}(s)$. We conclude therefore that $\mathbb{Q}(s) = \mathbb{Q}(t) = \mathbb{Q}(s,t)$ and so $K(s) = K(t) = K(s,t)$. □

Proof of Proposition 2.1. Let $P \in E(\mathbb{Q})$ as in Proposition 2.1; then

$$P = n_1P_1 + \cdots + n_rP_r + T,$$

where T is a torsion point of $E(\mathbb{Q})$ and $n_1, n_2, \ldots, n_r$ are non-negative integers. Since $P_i = 2R_i, P = 2R$ and $T = 2T_1$, we get

$$2R = n_1 2R_1 + \cdots + n_r 2R_r + 2T_1.$$

Thus,

$$R = n_1R_1 + \cdots + n_rR_r + T_1 + T_2,$$

where T_2 is a rational 2-torsion point of E. We set $T' = T_1 + T_2$. Remark that $T' \in 2^{-1}E_{\rm tor}(\mathbb{Q})$. Indeed,

$$2T' = 2(T_1 + T_2) = 2T_1 + 2T_2 = 2T_1 = T,$$

where T is a rational torsion point. We rewrite R as

$$R = \sum_i 2k_iR_i + \sum_j (2m_j + 1)R_j + T',$$

where $i, j \in \{1, 2, \ldots, r\}$ and k_i, m_i are non-negative integers. The "even" part can be written as

$$\sum_i 2k_iR_i = \sum_i k_iP_i = \tilde{P}_1 \in E(\mathbb{Q})$$

and the "odd" part

$$\sum_j (2m_j + 1)R_j = \tilde{P}_2 + \tilde{R},$$

where $\tilde{P}_2 \in E(\mathbb{Q})$ and $\tilde{R} = \sum R_j$. From the previous we deduce that $R = \tilde{P} + \tilde{R} + T'$, where $\tilde{P} = \tilde{P}_1 + \tilde{P}_2 \in E(\mathbb{Q})$. Further we get

$$K(R) = K(\tilde{P} + \tilde{R} + T') \subseteq K(\tilde{P}, \tilde{R} + T') = K(\tilde{R} + T').$$

Indeed, from the addition formula on an elliptic curve we see that the sum $\tilde{P}+\tilde{R}+T'$ is written as a rational function of the coordinates of the points $\tilde{P}$ and $\tilde{R} + T'$. That is $x(\tilde{P} + \tilde{R} + T') = \Phi(x(\tilde{P}), x(\tilde{R} + T'))$, with $\Phi \in \mathbb{Q}[X, Y]$ and similar for $y(\tilde{P}+\tilde{R}+T')$. Moreover, $K(x(R)) = K(R)$ (since $2R \in E(\mathbb{Q})$, we apply Lemma 2.2) and $K(x(\tilde{R} + T')) = K(\tilde{R} + T')$ (since $2(\tilde{R} + T') = \sum m_j P_j + T \in E(\mathbb{Q})$). So we get $K(x(R)) \subseteq K(x(\tilde{R} + T'))$. We conclude that $x(R) \in L$, for some $L \in \Re$. $\square$

3. Properties of 2-Division Polynomials

We set $\Theta_a(T) = T^4 - 4aT^3 - 2AT^2 - 4aAT + A^2$. Remark that this is the 2-division polynomial (2.1).

Lemma 3.1. (i) *Let* $P = (a, b) \in E(\mathbb{Z})$ *and* $2R = P$. *Then*

$$\mathbb{Q}(x(R)) = \mathbb{Q}(\sqrt{2a(a \pm \sqrt{a^2 + A})}).$$

(ii) *If* $\Theta_a(T)$ *is irreducible over* $\mathbb{Q}$, *then* $a + A^2$ *is not a square.*
(iii) *If* $d = \gcd(a, a^2 + A)$, *then* $\mathbb{Q}(\sqrt{a^2 + A}) = \mathbb{Q}(\sqrt{d})$ *or* $\mathbb{Q}(\sqrt{-d})$.

Proof. (i) The element $x(R) = s$ is a root of the polynomial $\Theta_a(T)$. Then

$$\Theta_a(s)/s^2 = (s + A/s)^2 - 4a(s + A/s) - 4A = 0.$$

From this we get

$$s + A/s = 2a \pm 2\sqrt{a^2 + A},$$

whence $s^2 + A = 2s(a \pm \sqrt{a^2 + A})$. So the first part of lemma follows.

(ii) We set $Y = T + A/T$ and $G(Y) = Y^2 - 4aY - 4A$. If G is reducible over $\mathbb{Q}$, then there are linear monic polynomials $G_1(Y) = Y + A_1, G_2(Y) = Y + A_2$, with $A_1, A_2 \in \mathbb{Z}$ such that $G = G_1(Y)G_2(Y)$ (it may occur $A_1 = A_2$ so $G = G_1^2$, therefore the discriminant of G equals to 0). Substituting Y with $T + A/T$ and using that $\Theta_a(T) = T^2G(Y)$, we get

$$\Theta_a(T) = T^2G_1(T + A/T)G_2(T + A/T).$$

Hence,

$$\Theta_a(T) = (T^2 + A_1T + A)(T^2 + A_2T + A).$$

So $\Theta_a(T)$ is reducible over $\mathbb{Q}$. Thus, if $\Theta_a(T)$ is irreducible then G is irreducible, whence the discriminant of G is not a square and the same occurs for $a^2 + A$.

(iii) Let $d = \gcd(a, a^2 + A)$. Then from $b^2 = a(a^2 + A)$ we get $a = \pm dd_1^2$, $a^2 + A = \pm dd_2^2$, for some integers d_1, d_2. So $\mathbb{Q}(\sqrt{a^2 + A}) = \mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{-d})$. $\square$

3.1. $\Theta_a(T)$ is irreducible over $\mathbb{Q}$

Lemma 3.2. *Let $P=(a,b)\in E(\mathbb{Z})$ and $2R=P$. Put $K=\mathbb{Q}(\sqrt{-A})$. We assume that $\Theta_a(T)$ is irreducible over $\mathbb{Q}$. We set $u_{\pm}=s\pm\sqrt{-A}$. Then either the elements $u_{\pm}/\sqrt{-A}$ are $\overline{S}$-units in $M=K(R)$, or $u_{\pm}/A$ are $\overline{S}$-units in M, where $\overline{S}$ is the extension of the set $S=\{2\}\cup\{p \text{ prime}: p|A\}\cup\{\infty\}$ of primes of $\mathbb{Q}$ in M.*

Proof. We set $L=K(u_{\pm})$. Since $\Theta_a(T)$ is irreducible, then from Lemma 3.1(ii), a^2+A is not a square. We consider two cases.

(i) $K\not\subset\mathbb{Q}(s)$ and
(ii) $K\subset\mathbb{Q}(s)$. Since $\mathbb{Q}(\sqrt{a^2+A})$ is the unique quadratic subfield of $\mathbb{Q}(s)$ we get $K\subset\mathbb{Q}(\sqrt{a^2+A})$.

In the first case we get $[M:\mathbb{Q}]=8$. Since $L=K(s\pm\sqrt{-A})=K(s)$ we get $M/\mathbb{Q}=L/\mathbb{Q}$ thus $[L:\mathbb{Q}]=8$. A defining polynomial for the extension $L/\mathbb{Q}$ is given by the resultant

$$\mathrm{Res}_W(\Theta_a(T+W),W^2+A)=T^8+\cdots+16A^4.$$

So the norm $N_M(u_{\pm})=16A^4$. Also, $N_M(\sqrt{-A})=A^4$, and the element $u_{\pm}/\sqrt{-A}$ is $\overline{S}$-integer. Since $N_M(u_{\pm}/\sqrt{-A})=16$ and $2\in S$ we get that the element $u_{\pm}/\sqrt{-A}$ is $\overline{S}$-unit. So the result follows.

For case (ii) we consider two sub-cases.

(α) $K=\mathbb{Q}$, i.e. $-A=n^2$, for some integer n.
(β) $K=\mathbb{Q}(\sqrt{a^2+A})$.

For case (α) we work as previous. The resultant now is equal to

$$\mathrm{Res}_W(\Theta_a(T+W),W^2-n^2)=(T^4+8n^3T+\cdots+4n^4)(T^4-8n^3T+\cdots+4n^4).$$

Since $\Theta_a(T)$ is irreducible over $\mathbb{Q}$, we get

$$[M:\mathbb{Q}]=[\mathbb{Q}(s,\sqrt{-A}):\mathbb{Q}]=[\mathbb{Q}(s):\mathbb{Q}]=4.$$

Further, $L/\mathbb{Q}=M/\mathbb{Q}$ and a defining polynomial for the extension L over $\mathbb{Q}$ is one of the two factors of the resultant. So $u_{\pm}$ is a root of one of the two previous factors of the resultant, thus we get $N_M(u_{\pm})=4n^4=4A^2$. In addition, $N_M(\sqrt{-A})=A^2$, whence $N_M(u_{\pm}/\sqrt{-A})=4$. Since $u_{\pm}/\sqrt{-A}$ is $\overline{S}$-integer, the result follows.

For case (β), we have $d_M=4$. We set $v=s+A/s$. From Lemma 3.1(i), we note that $N_K(v)=-4A$, where $K=\mathbb{Q}(\sqrt{-A})=\mathbb{Q}(\sqrt{a^2+A})=\mathbb{Q}(v)$. We have $N_M(v)=N_K(v)^2=16A^2$ so $N_M(s^2+A)=16A^2N_M(s)$. Since $\Theta_a(T)$ is irreducible over $\mathbb{Q}$ and $\Theta_a(s)=0$, we get $N_M(s)=A^2$, thus $N_M(s^2+A)=16A^4$. Also $N_M(u_+)=N_M(u_-)=16A^4$. Therefore, $N_M(u_{\pm}/A)=16$. $\square$

3.2. $\Theta_a(T)$ is reducible over $\mathbb{Q}$

In this case $[\mathbb{Q}(s) : \mathbb{Q}] < 4$, so from Lemma 3.1(ii) necessarily $a^2 + A$ is a square therefore a is a square. Thus $a = d_1^2$, $a^2 + A = d_2^2$, for some integers d_1, d_2 (it may occur one of them to be zero but not both of them). Hence, we get the equation $d_1^4 - d_2^2 = -A$. We deduce that $d_1^2 = a \leq |A|$, so $h(a) \leq \log |A|$, where h is the Weil height on the projective line $\mathbb{P}^1(\mathbb{Q})$. In order to define the Weil height we consider $P \in \mathbb{P}^1(\mathbb{Q})$ and $(x_0 : x_1)$ denote projective coordinates of P. These coordinates can be selected to be integers and relatively prime. Then the Weil height is defined by the relation

$$h(P) = \log \max\{|x_0|, |x_1|\}.$$

With $\hat{h}$ we denote the canonical height on $E(\mathbb{Q})$, where E is as usual the elliptic curve defined by the equation $y^2 = x^3 + Ax$. The canonical height is defined by the following relation:

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h(x(2^n P))}{4^n}, \quad P \in E(\mathbb{Q}).$$

We need the following lemmas.

Lemma 3.3. *There is an absolute constant $c > 0$ such that if $P \in E(\mathbb{Q})$ is a non-torsion point, then*

$$\hat{h}(P) > c \log |\Delta_E|,$$

where Δ_E is the minimal discriminant of E.

Proof. Since the j-invariant is integral ($j = 1728$) the lemma follows from [17, Corollary 1]. □

Lemma 3.4. *We set $A_1 = \min\{\hat{h}(P) : P \in E(\mathbb{Q}), P$ non-torsion$\}$. If A_2 is a positive constant, then*

$$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) < A_2\} \leq 2(\sqrt{A_2/A_1} + 1)^r,$$

where $r = \mathrm{rank}(E(\mathbb{Q}))$.

Proof. For the proof, see [18, Lemma 6]. □

Lemma 3.5. *If A is fourth-power-free integer and $\mathrm{ord}_2(A) \leq 1$, then Δ_E is minimal over $\mathbb{Q}$.*

Proof. Since $\Delta_E = -2^6 A^3$ we get $\log |\Delta_E| = 6 \log 2 + 3 \log |A|$. In order Δ_E to be minimal, we must have $\mathrm{ord}_p(\Delta_E) < 12$, for every prime p. So the lemma follows. □

Lemma 3.6. *For every $P = (x, y) \in E(\mathbb{Q})$, we have*

$$\hat{h}(P) < \frac{1}{2}h(x) + \frac{1}{4}\log|A| + 2.038.$$

Proof. For the proof, see [19, Example 2.2]. □

Proposition 3.7. *If A is fourth-power-free integer and $\mathrm{ord}_2(A) \leq 1$, then there is an absolute constant $\kappa > 0$ such that*

$$\#\{(x, y) \in E(\mathbb{Q}) : h(x) < \log|A|\} < \kappa^r.$$

Proof. Let $P = (x, y) \in E(\mathbb{Q})$. From Lemma 3.6 we have $\hat{h}(P) < 0.5h(x) + 0.25\log|A| + 2.038$. Then

$$\begin{aligned}\sigma_A &= \#\{(x, y) \in E(\mathbb{Q}) : h(x) < \log|A|\}\\ &\leq \#\{(x, y) \in E(\mathbb{Q}) : \hat{h}(P) < 0.75\log|A| + 2.038\}.\end{aligned}$$

Since A is fourth-power-free integer and $\mathrm{ord}_2(A) \leq 1$, then from Lemma 3.5 Δ_E is minimal, so applying Lemma 3.3 we get

$$\hat{h}(P) > c\log|\Delta_E| = c(6\log(2) + 3\log|A|).$$

In order to apply Lemma 3.4 we set $A_1 = c(6\log(2) + 3\log|A|)$ and $A_2 = 2.038 + 0.75\log|A|$. Then

$$\sigma_A \leq 2\left(\sqrt{\frac{2.038 + 0.75\log|A|}{c(6\log(2) + 3\log|A|)}} + 1\right)^r.$$

The function

$$g(w) = \sqrt{\frac{2.038 + 0.75\log w}{c(6\log(2) + 3\log w)}}$$

for $w > 1$ and every positive c is decreasing so $g(w) < g(1)$. Therefore,

$$\sigma_A \leq 2(c_1 + 1)^r < \kappa^r.$$

□

An immediate consequence is the following.

Corollary 3.8. *There is a positive absolute constant κ such that*

$$\#\{(a, b) \in E(\mathbb{Z}) : \Theta_a(T) \textit{ is reducible over } \mathbb{Q}\} < \kappa^r.$$

4. Proof of Schmidt's Conjecture

Proof of Theorem 1.1. Let $P = (a, b)$ be a rational integer point of E and $R = (s, t) \in E(\overline{\mathbb{Q}})$ such that $2R = P$. We set $S = \{2\} \cup \{p \text{ prime} : p|A\} \cup \{\infty\}$,

$K = \mathbb{Q}(\sqrt{-A})$. We have $\#S \leq \omega(A) + 2$. Denote by $\overline{S}$ the extension of S in $K(R)$. Since the number of extensions of a valuation is at most the degree of the field extension we get $\#\overline{S} \leq 8(\omega(A) + 2)$. We consider two cases, whether $\Theta_a(T)$ is irreducible or not over $\mathbb{Q}$.

Case (i). $\boldsymbol{\Theta_a(T)}$ **is irreducible over** $\mathbb{Q}$**.** Set $r_{\pm} = (s \pm \sqrt{-A})/\sqrt{-A}$ and $\tilde{r}_{\pm} = (-s \pm \sqrt{-A})/A$. Then from Lemma 3.2, either $r_{\pm}$ or $\tilde{r}_{\pm}$ are $\overline{S}$-units in $K(R)$. Further,

$$r_+ - r_- = 2 \quad \text{and} \quad \sqrt{-A}(\tilde{r}_+ - \tilde{r}_-) = 2$$

and let n_1 be its number of solutions. Then from [7],

$$n_1 \leq 3 \cdot 7^{[K(R):\mathbb{Q}]+2\#\overline{S}} < 3 \cdot 7^{8+16(\omega(A)+2)}.$$

In advance, $K(R)$ belongs to the set $\Re$ and $\#\Re < 4\#E_{\mathrm{tor}}(\mathbb{Q}) \cdot 2^{r+1}$ (the number 4 comes from the fact that the equation $2T' = T$ has at most four solutions). From [16, Proposition 6.1, p. 311] we get $\#E_{\mathrm{tor}}(\mathbb{Q}) \leq 4$, so $\#\Re < 16 \cdot 2^{r+1}$. Thus,

$$\begin{aligned}&\#\{(a, b) \in E(\mathbb{Z}) : \Theta_a(T) \text{ is irreducible over } \mathbb{Q}\}\\ &\quad \leq 2\#\Re \cdot n_1 < 96 \cdot 7^{40} \cdot 7^{16\omega(A)} \cdot 2^{r+1} < \kappa_1 \cdot 7^{16\omega(A)+r},\end{aligned}$$

where $\kappa_1 = 192 \cdot 7^{40}$.

Case (ii). $\boldsymbol{\Theta_a(T)}$ **is reducible over** $\mathbb{Q}$**.** From Corollary 3.8 we get that the number of integer points is at most κ^r, for some positive absolute constant κ.

Since A is fourth-power-free integer from [16, Proposition 6.1, p. 311] we get

$$r < 2\omega(2A) - 1.$$

So $\#E(\mathbb{Z}) < \kappa_2 \kappa_3^{2\omega(2A)}$, for some absolute constants κ_2 and κ_3. Since $\omega(2A)$ is as large as

$$\frac{\log(|\Delta_{\mathrm{E}}|)}{\log\log(|\Delta_{\mathrm{E}}|)},$$

then for every $\varepsilon > 0$ we get $\kappa_3^{2\omega(2A)} \ll_{\varepsilon} |\Delta_E|^{\varepsilon}$. So $\#E(\mathbb{Z}) \ll_{\varepsilon} |\Delta_E|^{\varepsilon}$.

5. Exploiting the Assumption of Quasi-Minimality

For elliptic curves of the form $y^2 = x^3 + 2^k n^4 Ax$, where $n \in \mathbb{Z} - \{0\}$, $k \in \mathbb{Z}_{\geq 2}$ and A is fourth-power-free odd integer, our approach cannot prove Conjecture I. The problem comes from the use of Lemma 3.3 (which is a very deep result) since it demands the quasi-minimality of $E/\mathbb{Q}$. So we must reformulate the case (ii) of the proof of Theorem 1.1. We keep the notation of the previous sections. We set

$$\tilde{\sigma} = \#\{\mathbb{Q}(s)/\mathbb{Q} : \Theta_a(T) \text{ is reducible over } \mathbb{Q}\},$$

$$\sigma = \#\{K(s)/\mathbb{Q} : \Theta_a(T) \text{ is reducible over } \mathbb{Q}\},$$

where $K = \mathbb{Q}(\sqrt{-A})$. Set $u_\pm = s \pm \sqrt{-A}$. The elements $u_\pm$ are $\overline{S}$-units in $K(R) = K(s)$. Indeed, from [16, Sublemma 4.3, Chap. VIII, p. 204] and setting $Z = 1, X = s$ and $B = 0$, we get

$$(3s^2 + 4A)(s^4 - 2As^2 + A^2) - (3s^3 - 5As)(s^3 + As) = 4A^3$$

and since $\Theta_a(s) = 0$, i.e. $s^4 - 2As^2 + A^2 = 4a(s^3 + As)$ we get

$$N_{K(R)/\mathbb{Q}}(s^3 + As) | N_{K(R)/\mathbb{Q}}(4A^3).$$

Thus, (u_+, u_-) satisfy in $K(R)$ the $\overline{S}$-unit equation $X - Y = 2\sqrt{-A}$. If n_1 is its number of solutions we get

$$n_1 < 3 \cdot 7^{[K(R):\mathbb{Q}]+2\#\overline{S}} < 3 \cdot 7^{6+12(\omega(A)+2)} = 3 \cdot 7^{30} \cdot 7^{12\omega(A)}.$$

We conclude therefore that

$$\#\{(a,b) \in E(\mathbb{Z}) : \Theta_a(T) \text{ is reducible over } \mathbb{Q}\} \leq 6 \cdot 7^{30} \cdot 7^{12\omega(A)}\sigma. \tag{5.1}$$

Since we supposed that $\Theta_a(T)$ is reducible over $\mathbb{Q}$, then either it has a monic polynomial as divisor in $\mathbb{Z}[T]$ or a quadratic irreducible polynomial. In the first case there exists $s \in \mathbb{Z}$ such that $\Theta_a(s) = 0$. In the second case $s = \alpha + \beta\sqrt{d}$ with $\alpha, \beta \in \mathbb{Z}[1/2]$, $\beta \neq 0$ and d is non-zero squarefree integer. From [16, Proposition 1.5, p. 193] $K(s)/K$ is unramified outside $\overline{S}$ so $\mathbb{Q}(s)/\mathbb{Q}$ is unramified outside S, thus $d|2A$. If $\Theta_a(T)$ is divided by a third degree irreducible polynomial, then it has also a monic linear polynomial as divisor. Let (s_1, t_1) such that $2(s_1, t_1) = (a, b) \in E(\mathbb{Z})$ with s_1 be a root of the third-degree factor, then there exists also a rational integer s (the root of the linear polynomial divisor) with $2(s, t) = (a, b)$. So the integer point (a, b) of E comes also from the root of the linear divisor. Thus we conclude

$$\tilde{\sigma} \leq 1 + 4\tau_2(2A),$$

where $\tau_2(2A)$ equals to the number of squarefree divisors of $2A$. Then $\tau_2(2A) = 2^{\omega(2A)}$. So

$$\tilde{\sigma} \leq 1 + 2^{\omega(2A)+2} < 2^{\omega(2A)+3}.$$

If we add the element $\sqrt{-A}$ to all the number fields $\mathbb{Q}(s)$, then we get the number fields $K(s)$. So the number σ cannot be larger than $\tilde{\sigma}$. Thus, $\sigma \leq \tilde{\sigma}$. Hence from (5.1) we derive

$$\begin{aligned}\#\{(a,b) \in E(\mathbb{Z}) : \Theta_a(T) \text{ is reducible over } \mathbb{Q}\}\\ < 6 \cdot 7^{30} \cdot 2^{\omega(2A)+3} \cdot 7^{12\omega(A)} \ll_\varepsilon |\Delta_E|^\varepsilon.\end{aligned}$$

Since in the proof of part (i) of Theorem 1.1 we do not use the quasi-minimality of E, we conclude that Conjecture I is true and so Conjecture II for $E/\mathbb{Q}$.

Acknowledgment

The author is indebted to the referee for pointing him out a gap in Lemma 3.2 and proposing a number of suggestions.

References

[1] E. Bombieri and U. Zannier, On the number of rational points on certain elliptic curves, *Izv. Ross. Akad. Nauk Ser. Mat.* **68**(3) (2004) 5–14 (Russian); *Izv. Math.* **68**(3) (2004) 437–445 (English).

[2] Y. Bugeaud, On the size of integer solutions of elliptic equations, *Bull. Austral. Math. Soc.* **57**(2) (1998) 199–206.

[3] C. Chabauty, Démonstration de quelques lemmes de rehaussement, *C. R. Acad. Sci. Paris* **217** (1943) 413–415.

[4] W.-C. Chi, K. F. Lai and K.-S. Tan, Integer points on elliptic curves, *Pacific J. Math.* **222**(2) (2005) 237–252.

[5] P. Corvaja and U. Zannier, On the number of integral points on algebraic curves, *J. Reine Angew. Math.* **565** (2003) 27–42.

[6] K. Draziotis and D. Poulakis, Solving the Diophantine equation $y^2 = x(x^2 - n^2)$, *J. Number Theory* **129**(1) (2009) 102–121.

[7] J.-H. Evertse, On equations in S-units and the Thue–Mahler equation, *Invent. Math.* **75**(3) (1984) 561–584.

[8] J.-H. Evertse and J. H. Silverman, Uniform bounds for the number of solutions to $Y^n = f(X)$, *Math. Proc. Cambridge Philos. Soc.* **100**(2) (1986) 237–248.

[9] H. A. Helfgott and A. Venkatesh, Integral points on elliptic curves and 3-torsion in class groups, *J. Amer. Math. Soc.* **19**(3) (2006) 527–550.

[10] M. Hindry and J. H. Silverman, The canonical height and integral points on elliptic curves, *Invent. Math.* **93**(2) (1988) 419–450.

[11] W. M. Schmidt, Integer points on curves of genus 1, *Compos. Math.* **81** (1992) 33–59.

[12] R. Gross and J. Silverman, S-integer points on elliptic curves, *Pacific J. Math.* **167**(2) (1995) 263–288.

[13] S. Lang, *Elliptic Curves: Diophantine Analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Vol. 231 (Springer, Berlin, 1978), xi+261 pp.

[14] D. Poulakis, Integer points on algebraic curves with exceptional units, *J. Austral. Math. Soc. Ser. A* **63**(2) (1997) 145–164.

[15] J. H. Silverman, A quantitative version of Siegel's theorem: Integral points on elliptic curves and Catalan curves, *J. Reine Angew. Math.* **378** (1987) 60–100.

[16] ——, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106 (Springer, New York, 1986), xii+400 pp.

[17] ——, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48**(3) (1981) 633–648.

[18] ——, Integer points and the rank of Thue elliptic curves, *Invent. Math.* **66**(3) (1982) 395–404.

[19] ——, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55**(192) (1990) 723–743.