LOWER BOUNDS FOR THE HEIGHT OF RATIONAL POINTS OF ELLIPTIC CURVES

Dimitrios Poulakis
Department of Mathematics, Aristotle University of Thessaloniki, Thessaloniki, Greece
poulakis@math.auth.gr

Received: 12/30/24, Revised: 5/29/25, Accepted: 6/20/25, Published: 8/15/25

Abstract

In this paper, we study elliptic curves E defined over $\mathbb{Q}$ by equations of the form $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$, and compute explicit constants C, depending only on E, such that there exists at most one pair of points $\pm(x, y) \in E(\mathbb{Q})$, with $xy \neq 0$, whose naive height is less than C. Moreover, this point (x, y) can be efficiently computed. We also identify a family of elliptic curves that admit no such points. Using these bounds, we verify Lang's height conjecture for a subclass of these curves.

1. Introduction and Statement of Results

Let E be an elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \mathbb{Z}$. The discriminant and the j-invariant of E are the quantities $\Delta_E = -16(4a^3 + 27b^2)$ and $j_E = -1728(4a)^3/\Delta_E$, respectively. We denote by $E(\mathbb{Q})$, the set of rational points of E, that is, the set of points $P = (u, v)$ in the affine plane $\mathbb{A}^2_{\mathbb{Q}}$ with $v^2 = u^3 + au + b$ and the point at infinity $O = (0 : 1 : 0)$ (written in projective coordinates). Furthermore, we denote by $E(\mathbb{Q})_{tors}$ the torsion subgroup of $E(\mathbb{Q})$.

1.1. Lang's Height Conjecture

If the discriminant Δ_E has minimal absolute value (subject to the condition that $a, b \in \mathbb{Z}$) among all models of E of the form (1), then Equation (1) is called *quasi-minimal*. Since $\mathbb{Z}$ is a unique factorization domain, it is easily seen that for every elliptic curve defined by an equation of the form (1), there is a model of E over $\mathbb{Q}$ defined by an equation of the same form, (1), which is quasi-minimal.

DOI: 10.5281/zenodo.16881736

Let P be a point of the projective space $\mathbb{P}^n_{\mathbb{Q}}$ over $\mathbb{Q}$. Then, there are integers $a_1, \ldots, a_{n+1}$ with $\gcd(a_1, \ldots, a_{n+1}) = 1$ such that $P = (a_1 : \ldots : a_{n+1})$. The naive height of P is defined to be the quantity

$$H(P) = \max\{|a_1|, \ldots, |a_{n+1}|\},$$

and the logarithmic naive height the quantity $h(P) = \log H(P)$. Furthermore, if $Q = (b_1, \ldots, b_n)$ is a point of the affine space $\mathbb{A}^n_{\mathbb{Q}}$ over $\mathbb{Q}$, then we put $H(Q) = H(b_1 : \ldots : b_n : 1)$, and $h(Q) = \log H(Q)$.

Let $P \in E(\mathbb{Q}) \setminus \{O\}$. We denote by $x(P)$ and $y(P)$ the x-coordinate and the y-coordinate of P, respectively; that is, we write $P = (x(P), y(P))$. The canonical height of P, as defined in [11, Chapter VIII, Section 9], is given by

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h(x(2^n P))}{4^n}.$$

Note that some authors omit the factor of $1/2$ in this definition. A detailed discussion of the various normalizations used for both canonical and local heights can be found in [1, Section 4].

The difference $\hat{h}(P) - \frac{1}{2}h(P)$ remains bounded as the point P varies over $E(\mathbb{Q})$. Explicit upper and lower bounds for this difference, expressed in terms of the coefficients of the Weierstrass equation, are given in [10]. Further estimates for the difference between the canonical height and the naive height have been developed in [1, 12, 16]. These results highlight the close relationship between the canonical and naive heights of points on an elliptic curve.

The canonical height satisfies $\hat{h}(P) \geq 0$ for all $P \in E(\mathbb{Q})$, and $\hat{h}(P) = 0$ if and only if $P \in E(\mathbb{Q})_{\text{tors}}$. Thus, $\hat{h}$ defines a positive definite quadratic form on the lattice $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$, and in particular, it attains a smallest positive value on non-torsion points. On page 92 of [7], Serge Lang formulated the following conjecture concerning this minimal positive value of the canonical height.

Conjecture. Let E be an elliptic curve defined by a quasi-minimal equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. Then, there is an absolute constant $C > 0$ such that for any point $P \in E(\mathbb{Q})$ of infinite order, we have:

$$\hat{h}(P) \geq C \log |\Delta_E|.$$

Lang's conjecture admits a broader formulation than the one stated above. Specifically, it applies to the global minimal Weierstrass equation of any rational elliptic curve (for the definition of a global minimal Weierstrass equation, see [11, Chapter VII, Section 8]). Generalizations of Lang's height conjecture to elliptic curves defined over number fields are presented in [9, page 402] and [5, Conjecture 0.1, page 419]. In these versions, the discriminant of the global minimal Weierstrass equation is replaced by the minimal discriminant [11, page 224].

Several special cases of this conjecture have been proven; see [2, 5, 8, 9]. Additionally, the sharpest known lower bounds for the cases $a = 0$ and $b = 0$ are given in [14, 15]. These bounds have notable applications in various problems, such as counting integral points on elliptic curves [5], studying elliptic divisibility sequences [3, 4, 13], and more.

1.2. Our Contribution

In this paper, we consider elliptic curves E defined over $\mathbb{Q}$ by equations of the form $y^2 = x^3 + ax + b$, which are not necessarily quasi-minimal. We compute an explicit constant C, depending only on the polynomial $y^2 - x^3 - ax - b$, such that there exists at most one pair of points $\pm P \in E(\mathbb{Q})$, with $x(P)y(P) \neq 0$, whose naive height is less than C. Furthermore, we identify a class of elliptic curves that possess no such points.

By using a lower bound for the difference $\hat{h}(P) - \frac{1}{2}h(P)$, we derive corresponding lower bounds for the canonical height of rational points on a subclass of these curves, thereby confirming Lang's height conjecture in these cases. Moreover, when such an exceptional pair of points exists, it can be efficiently computed using the LLL algorithm.

1.3. Our Results

To present our results, we begin by introducing some fundamental concepts from lattice theory.

Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ be a basis of $\mathbb{R}^m$. The m-dimensional lattice generated by $\mathcal{B}$ is the set

$$\mathcal{L} = \{z_1\mathbf{b}_1 + \cdots + z_m\mathbf{b}_m \mid z_1, \ldots, z_m \in \mathbb{Z}\}.$$

For a vector $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{R}^m$, the Euclidean norm is defined as

$$\|\mathbf{v}\| = \sqrt{v_1^2 + \cdots + v_m^2}.$$

For a polynomial $f \in \mathbb{R}[x_1, \ldots, x_m]$, its Euclidean norm, denoted $\|f\|$, refers to the Euclidean norm of the vector of its coefficients.

The Gram-Schmidt orthogonalization of the basis $\mathcal{B}$ yields an orthogonal basis $\mathcal{B}^* = \{\mathbf{b}_1^*, \ldots, \mathbf{b}_m^*\}$ of $\mathbb{R}^m$, defined recursively by

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*, \quad \text{where} \quad \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}, \quad \text{for } 1 \leq j < i \leq m.$$

A basis $\mathcal{B}$ is called LLL-reduced if it satisfies the following two conditions:

1. $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq m$,

2. $\|\mathbf{b}_i\|^2 \leq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{b}_{i-1}^*\|^2$ for all $2 \leq i \leq m$.

We now proceed to state our main results.

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$p(x, y) = y^2 - x^3 - ax - b = 0,$$

where $a, b \in \mathbb{Z}$, with $ab \neq 0$ and $a \neq \pm b$. Define

$$n = \left\lfloor \frac{\|p\|^{3/2}}{2^{3/4} \cdot 1.001} \right\rfloor.$$

Let $\mathcal{L} \subset \mathbb{R}^3$ be the lattice spanned by the rows of the matrix

$$A = \begin{pmatrix} 1 & a & b \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix}.$$

Let L denote the length of the shortest vector in an LLL-reduced basis of $\mathcal{L}$. Then the curve E admits at most one pair of rational points $\pm P \in E(\mathbb{Q}) \setminus \{O\}$, with $x(P)y(P) \neq 0$, satisfying the height bound

$$H(P) < \left(\frac{n}{\sqrt{6}\, L}\right)^{1/3}.$$

Moreover, such a point P, if it exists, can be computed in $O((\log \|p\|)^3)$ bit operations using the LLL algorithm. Finally, if the inequality

$$1 + |a| < \frac{n^{1/3}}{\sqrt{2}}$$

holds, then no such pair of rational points $\pm P$ exists.

Corollary 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$p(x, y) = y^2 - x^3 - ax - b = 0,$$

where $a, b \in \mathbb{Z}$, with $ab \neq 0$, and suppose that

$$1 + |a| < \frac{\|p\|^{1/2}}{1.782}.$$

Then, for every point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that $x(P)y(P) \neq 0$, the following inequality holds:

$$H(P) > \frac{\|p\|^{1/6}}{1.634}.$$

In the following corollary, a class of elliptic curves is presented verifying Lang's height conjecture.

Corollary 2. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$p(x, y) = y^2 - x^3 - ax + b = 0,$$

where $a, b \in \mathbb{Z}$. Assume that $b > 0$, $a \neq 0$, $1 + |a| < \|p\|^{1/4}$, $\gcd(a, 3b) = \gcd(2, b) = 1$, and that $4a^3 + 27b^2$ is square-free. Then, for every point $P \in E(\mathbb{Q})$ of infinite order, the canonical height satisfies

$$\hat{h}(P) > \frac{1}{144} \log |\Delta_E| - 2.019.$$

Remark 1. According to [9], Lang's height conjecture holds for elliptic curves E with integer modular invariant j_E. However, the curves satisfying the assumptions of Corollary 2 do not have integer j-invariants. Assume, for contradiction, that $j_E \in \mathbb{Z}$. Then $4a^3+27b^2 \mid 108 \cdot 4a^3$, so there exists $C \in \mathbb{Z}$ such that $(4a^3+27b^2)C = 108 \cdot 4a^3$. This implies $4a^3 \mid 27b^2C$. Since $\gcd(a, 3b) = \gcd(2, b) = 1$, it follows that $4a^3 \mid C$, and thus $(4a^3 + 27b^2)C_1 = 108$ for some $C_1 \in \mathbb{Z}$. If $|4a^3 + 27b^2| > 1$, then either 2 or 3 divides it. If $2 \mid 4a^3+27b^2$, then b is even, contradicting $\gcd(2, b) = 1$. If $3 \mid 4a^3+27b^2$, then $3 \mid 4a^3$, contradicting $\gcd(a, 3b) = 1$. Therefore, $4a^3+27b^2 = \pm 1$. If $a > 0$, this is impossible. If $a < 0$, then $27b^2 = 4|a|^3 \pm 1$. However, the inequality $1 + |a| < \|p\|^{1/4}$ implies $4|a|^3 < b^2$, hence $27b^2 < b^2 \pm 1$, a contradiction.

Thus, $j_E \notin \mathbb{Z}$, and Corollary 2 identifies a new class of elliptic curves for which Lang's conjecture holds.

In the following theorem, we present a class of elliptic curves satisfying the assumptions of Theorem 1, and establish a sharper lower bound for the naive height of their rational points.

Theorem 2. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$. Then the following statements hold:

(a) If $a = \pm 1$ and $b \notin \{0, \pm 1\}$, then there exists no point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that

$$H(P) < \left(\frac{|b|}{5} \right)^{1/3}.$$

(b) If $a \notin \{0, \pm 1\}$ and $b = -1$, then there exists no point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that

$$H(P) < \left(\frac{|a|}{5} \right)^{1/3}.$$

(c) If $a \notin \{0, \pm 1\}$ and $b = 1$, then the only points $P \in E(\mathbb{Q}) \setminus \{O\}$ satisfying

$$H(P) < \left(\frac{|a|}{5}\right)^{1/3}$$

are $P = (0, \pm 1)$.

In the following corollary, we present a class of elliptic curves satisfying the assumptions of Corollary 2, and we obtain a better lower bound for the canonical height of their rational points.

Corollary 3. *Let $E_\pm$ be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$y^2 = x^3 \pm x - b,$$

where b is an odd integer ≥ 3, and suppose that the quantity

$$-\frac{\Delta_{E_\pm}}{16} = 27b^2 \pm 4$$

is square-free. Then, for every point $P \in E_\pm(\mathbb{Q})$ of infinite order, the canonical height satisfies

$$\hat{h}(P) > \frac{1}{9}\log b - 1.923.$$

Theorem 1 does not include the cases where either $a = 0$, $b = 0$, or $b = \pm a$. The following theorem addresses these cases.

Theorem 3. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation*

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$. We have the following cases:

(a) $b = a$. There is no point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that

$$H(P) < \left(\frac{|a|}{4}\right)^{1/3}.$$

(b) $b = -a$. The only points $P \in E(\mathbb{Q})$ with

$$H(P) < \left(\frac{|a|}{4}\right)^{1/3}$$

are O and $(1, \pm 1)$, which form a subgroup of order three.

(c) $b = 0$. The only point $P \in E(\mathbb{Q}) \setminus \{O\}$ with

$$H(P) < \left(\frac{|a|}{4}\right)^{1/3}$$

is $P = (0, 0)$.

(d) $a = 0$. *There is no point* $P \in E(\mathbb{Q}) \setminus \{O\}$ *such that*

$$H(P) < \left(\frac{|b|}{3}\right)^{1/3}.$$

By Theorem 3(b), every curve defined by an equation of the form $y^2 = x^3 + ax - a$ passes through the point $P = (1, 1)$, which has naive height $H(P) = 1$. However, the discriminant of these curves increases with $|a|$. This example illustrates that there is no analogue of Lang's conjecture when the naive height is used.

The proofs of Theorems 1, 2 and, 3 are based on the construction of a cubic curve distinct from E that intersects E in at most one rational point $Q \neq O$. In Theorem 1, the LLL algorithm was used to construct this cubic curve and identify the point of intersection with E, if it exists. For Theorems 2 and 3, arguments based on integer divisibility were applied. Using an upper bound for the shortest vector of an LLL-reduced basis for the lattice $\mathcal{L}$ in the proof of Theorem 1, Corollary 1 is derived. Combining Theorems 2 and 3 with a lower bound for the quantity $\hat{h}(P) - h(P)/2$, we obtain Corollaries 2 and 3.

1.4. The Structure of the Paper

The paper is organized as follows. In Section 2, we present some auxiliary lemmas that will be used in the proofs of our main results. Section 3 provides the proofs of Theorem 1 and Corollaries 1 and 2. Section 4 is dedicated to proving Theorem 2 and Corollary 3. The proof of Theorem 3 is given in Section 5. The final section outlines a polynomial-time algorithm for computing the pair of exceptional points $\pm P$, if they exist, which are smaller than the lower bound established by Theorem 1. Additionally, we present three examples: two where the pair of points exists and one where it does not.

2. Auxiliary Lemmas

In this section, we give some auxiliary lemmas that we will need to prove our results.

Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ be a basis of $\mathbb{R}^m$, and $\mathcal{L}$ the lattice generated by $\mathcal{B}$. Let $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,m})$ $(i = 1, \ldots, m)$, and consider the matrix $M(\mathcal{B}) = (b_{i,j})$. The quantity $\det \mathcal{L} = |\det M(\mathcal{B})|$ is independent of the particular basis used to compute it, and is called the determinant of $\mathcal{L}$.

Lemma 1 ([6]). *Let* $B = \max\{\|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_m\|\}$. *Then, the LLL-algorithm computes in time* $O(m^6(\log B)^3)$ *bit operations a reduced LLL-basis for* $\mathcal{L}$.

Lemma 2 ([6]). *Let* $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *be an LLL-reduced basis of* $\mathcal{L}$. *Then, the vector* $\mathbf{v}_1$ *satisfies*

$$\|\mathbf{v}_1\| \leq 2^{(m-1)/4} \det(\mathcal{L})^{1/m}.$$

An explicit estimate for the difference of the naive height and the canonical height of points on elliptic curves is given below.

Lemma 3 ([10])**.** *Let E be an elliptic curve over $\mathbb{Q}$ given by the equation*

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$. Suppose that $4a^3 + 27b^2$ is square-free, $\gcd(a, 3b) = 1$ and b is odd. Then, for every $P \in E(\mathbb{Q})$ we have

$$\frac{1}{2}h(x(P)) \leq \hat{h}(P) + \frac{1}{8}\max(\log|j_E|, 0) + 1.205.$$

Lemma 4. *Let E be an elliptic curve over $\mathbb{Q}$ given by the equation*

$$y^2 = x^3 + ax - b,$$

where $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b > 0$. Then, for every $P \in E(\mathbb{Q}) \setminus \{O\}$ we have:

$$H(P) < \sqrt{1 + |a|}\; H(x(P))^{3/2}.$$

Proof. Let $P \in E(\mathbb{Q}) \setminus \{O\}$. Then, there are $s, t, u \in \mathbb{Z}$ with $\gcd(s, t) = \gcd(t, u) = \gcd(s, u) = 1$ and $t \geq 1$ such that $x(P) = s/t^2$ and $y(P) = u/t^3$. It follows that $u^2 = s^3 + ast^4 - bt^6$ and $(x(P) : y(P) : 1) = (st : u : t^3)$. We distinguish the following two cases:

`Case 1:` $a > 0$. If $s > 0$, then $u^2 + bt^6 = s^3 + ast^4$, and since $b > 0$, we have $u^2 < (1 + a)\max\{|s|, t^2\}^3$. If $s \leq 0$, then we obtain

$$0 \leq u^2 + |s|^3 + a|s|t^4 + bt^6 = 0,$$

whence $s = t = u = 0$ which is a contradiction. Thus, we get:

$$|u| < \sqrt{1 + a}\, H(s/t^2)^{3/2}.$$

`Case 2:` $a < 0$. If $s > 0$, then we have $u^2 + |a|st^4 + bt^6 = s^3$, whence we get $|u|^2 < |s|^3$. If $s \leq 0$, then we deduce $u^2 + bt^6 + |s|^3 = |a||s|t^4$, whence we have $u^2 < |a|\max\{|s|, t^2\}^3$. It follows that

$$|u| < \sqrt{|a|}\, H(s/t^2)^{3/2}.$$

□

3. Proofs of Theorem 1 and Corollaries 1 and 2

Proof of Theorem 1. Set $p_h(x, y, z) = y^2z - x^3 - axz^2 - bz^3$. We denote by $\mathcal{L}$ the lattice spanned by the rows of the matrix

$$A = \begin{pmatrix} 1 & a & b \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix}.$$

The determinant of A is $\det A = n^{2/3}$. By Lemma 2, the LLL algorithm computes an LLL-reduced basis $\mathcal{B}$ for $\mathcal{L}$. The initial vector $\mathbf{v} = (v_1, v_2, v_3)$ of $\mathcal{B}$ satisfies

$$\|\mathbf{v}\| \leq \sqrt{2}\, n^{2/3} \leq \frac{\|p\|}{1.001} < \|p\|. \tag{2}$$

Furthermore, there are integers l_1, l_2, l_3 such that

$$v_1 = l_1, \quad v_2 = l_1 a + l_2 n, \quad v_3 = l_1 b + l_3 n. \tag{3}$$

We consider the polynomial:

$$f(x, y, z) = v_1(y^2 z - x^3) - v_2 x z^2 - v_3 z^3. \tag{4}$$

Replacing v_1, v_2, v_3 from the formulas above, we have:

$$f(x, y, z) = l_1 p_h(x, y, z) - n z^2 (l_2 x + l_3 z).$$

Let $P = (x_0/z_0, y_0/z_0) \in E(\mathbb{Q}) \setminus \{O\}$, where $(x_0, y_0, z_0) \in \mathbb{Z}^3$ with $x_0 y_0 z_0 \neq 0$ and $\gcd(x_0, y_0, z_0) = 1$, be a rational point of E satisfying

$$H(P) < \left(\frac{n}{\sqrt{6}\, \|\mathbf{v}\|} \right)^{1/3}. \tag{5}$$

We have $p_h(x_0, y_0, z_0) = 0$, and so, we deduce:

$$f(x_0, y_0, z_0) = l_1 p_h(x_0, y_0, z_0) - n z_0^2 (l_2 x_0 + l_3 z_0) \equiv 0 \pmod{n}.$$

On the other hand, using (4) and (5), we get

$$|f(x_0, y_0, z_0)| < \frac{n}{\sqrt{6}\, \|\mathbf{v}\|} (2|v_1| + |v_2| + |v_3|). \tag{6}$$

Applying the Cauchy-Schwarz Inequality, we have:

$$2|v_1| + |v_2| + |v_3| \leq \sqrt{6}\, \|\mathbf{v}\|. \tag{7}$$

Finally, using (6) and (7), we obtain

$$|f(x_0, y_0, z_0)| < \frac{n}{\sqrt{6}\, \|\mathbf{v}\|} \sqrt{6}\, \|\mathbf{v}\| \leq n.$$

Then, the relations $f(x_0, y_0, z_0) \equiv 0 \pmod{n}$ and $|f(x_0, y_0, z_0)| < n$ imply that $f(x_0, y_0, z_0) = 0$.

Suppose now that there are integers α and β with $\gcd(\alpha, \beta) = 1$, $\beta > 0$ such that $\alpha p_h(x, y, z) = \beta f(x, y, z)$ (in $\mathbb{Z}[x, y, z]$). Then, comparing the coefficients of $\alpha p_h(x, y, z)$ and $\beta f(x, y, z)$, we have:

$$\alpha = \beta v_1, \quad \alpha a = \beta v_2, \quad \alpha b = \beta v_3.$$

It follows that β divides α, and since $\gcd(\alpha, \beta) = 1$, we get $\beta = 1$. Thus, we have $\alpha p_h(x, y, z) = f(x, y, z)$, and so, (2) implies that

$$\|\alpha\|\|p_h\| = \|f\| < \|p_h\|,$$

which is a contradiction. Hence, $p_h(x, y, z)$ and $f(x, y, z)$ are linearly independent, and therefore define two distinct algebraic curves.

From the equality $p_h(x_0, y_0, z_0) = 0$, we obtain

$$y_0^2 z_0 - x_0^3 = a x_0 z_0^2 + b z_0^3.$$

Substituting this into the equation $f(x_0, y_0, z_0) = 0$ and cancelling out z_0^2 (since $z_0 \neq 0$), we deduce:

$$v_1(a x_0 + b z_0) = v_2 x_0 + v_3 z_0.$$

Replacing v_1, v_2, v_3 using their expressions from (3), we obtain:

$$l_1(a x_0 + b z_0) = (l_1 a + l_2 n) x_0 + (l_1 b + l_3 n) z_0.$$

Rearranging, it follows that

$$l_2 x_0 + l_3 z_0 = 0. \tag{8}$$

Thus, we conclude that

$$\frac{x_0}{z_0} = -\frac{l_3}{l_2}.$$

Equalities (3) yield

$$l_2 = \frac{v_2 - v_1 a}{n} \quad \text{and} \quad l_3 = \frac{v_3 - v_1 b}{n}.$$

Furthermore, we remark that

$$|l_2| \leq \frac{|v_2| + |v_1||a|}{n} \leq \frac{\sqrt{2}\,(1 + |a|)}{n^{1/3}}.$$

Thus, if $1 + |a| < n^{1/3}/\sqrt{2}$, then we deduce that $l_2 = 0$. If $l_3 = 0$, then the polynomials $f(x, y, z)$ and $p_h(x, y, z)$ are linearly dependent which is a contradiction. Then $l_3 \neq 0$, and therefore (8) implies that $z = 0$ which is a contradiction. Hence, such a point P does not exist.

The maximum Euclidean norm of the row vectors of matrix A that form a basis of $\mathcal{L}$ is n. Consequently, Lemma 1 yields that the overall computation of l_2 and l_3 requires $O((\log \|p\|)^3)$ bit operations. Furthermore, if a point $P = (x_0/z_0, y_0/z_0)$ satisfies (5), then the point $-P = (x_0/z_0, -y_0/z_0)$ also satisfies (5). The proof of Theorem 1 follows. □

Proof of Corollary 1. It is easily seen that

$$n = \left\lfloor \frac{\|p\|^{3/2}}{2^{3/4}\,1.001} \right\rfloor > \frac{\|p\|^{3/2}}{2}. \tag{9}$$

Thus, we have

$$1 + |a| < \frac{\|p\|^{1/2}}{1.782} < \frac{n^{1/3}}{\sqrt{2}}.$$

By Inequality (2), we have $\|\mathbf{v}\| \leq \sqrt{2}\, n^{2/3}$. Then, combining Theorem 1 with this inequality and (9), we obtain the result. □

Proof of Corollary 2. Let $P \in E(\mathbb{Q}) \setminus \{O\}$. By Lemma 4, we have

$$H(P) < \sqrt{1 + |a|}\, H(x(P))^{3/2}.$$

It follows that

$$h(P) < \frac{1}{2}\log(1 + |a|) + \frac{3}{2}\, h(x(P)) < \frac{1}{8}\log\|p\| + \frac{3}{2}\, h(x(P)).$$

By Corollary 1, we have

$$\frac{1}{6}\log\|p\| - 0.492 \leq h(P).$$

Combining the two previous inequalities, we obtain

$$\frac{1}{24}\log\|p\| - 0.492 \leq \frac{3}{2}\, h(x(P)).$$

Since $1 + |a| < \|p\|^{1/4}$, we deduce that $|j_E| < 1728/26$. Then, Lemma 3 yields

$$\frac{1}{72}\log\|p\| - 1.976 < \hat{h}(P). \tag{10}$$

On the other hand, the inequality $1 + |a| < \|p\|^{1/4}$ implies $4|a|^3 < b^2$, and therefore we get $|\Delta_E| < 448b^2 < 448\|p\|^2$. Then, using this inequality and (10), we get

$$\frac{1}{144}\log|\Delta_E| - 2.019 < \hat{h}(P).$$

□

4. Proof of Theorem 2 and Corollary 3

Proof of Theorem 2. First, suppose that $a = \pm 1$ and $b \neq 0, \pm 1$. Set $p_h(x, y, z) = y^2z - x^3 \mp xz^2 - bz^3$. Let $P = (x_0/z_0, y_0/z_0) \in E(\mathbb{Q}) \setminus \{O\}$, where $x_0, y_0, z_0 \in \mathbb{Z}^3$ with $x_0y_0 \neq 0$, $z_0 > 0$, and $\gcd(x_0, y_0, z_0) = 1$, satisfying

$$H(P) = \max\{|x_0|, |y_0|, |z_0|\} < (|b|/5)^{1/3}. \tag{11}$$

Let n be a positive integer such that $4b^2/3 \geq n > b^2$ and $\gcd(n, b) = 1$. Then, there are integers q and r such that $n = bq + r$ and $0 \leq r < |b|$. Since $\gcd(n, b) = 1$, we have $r > 0$. Furthermore, we have

$$|q| = \lfloor n/|b| \rfloor \leq 4|b|/3. \tag{12}$$

Consider the polynomial

$$\begin{aligned} f(x, y, z) &= nz^3 + qp_h(x, y, z) \\ &= q(y^2z - x^3 \mp xz^2) + (n - qb)z^3 \\ &= qy^2z - qx^3 \mp qxz^2 + rz^3. \end{aligned}$$

Then, we have $f(x_0, y_0, z_0) \equiv 0 \pmod{n}$. Furthermore, Inequalities (11) and (12) yield

$$|f(x_0, y_0, z_0)| < (3|q| + |b|)H(P)^3 \leq 5|b|H(P)^3 < |b|^2 < n.$$

Combining the congruence $f(x_0, y_0, z_0) \equiv 0 \pmod{n}$ with the above inequality, we obtain that $f(x_0, y_0, z_0) = 0$. Since $f(x, y, z) = nz^3 + qp_h(x, y, z)$, we obtain that $z_0 = 0$, and hence $P = O$ which is a contradiction.

Suppose that $x_0 = 0$. Then, $P = (0, \sqrt{b})$ and b is a perfect square. Since $H(P) = \sqrt{b} > (|b|/5)^{1/3}$, we have a contradiction. So, $x_0 \neq 0$. If $y_0 = 0$, then z_0^2 divides x_0^3, and so, $z_0 = 1$, because $\gcd(x_0, y_0, z_0) = 1$. Then $x_0^3 \pm x_0 + b = 0$, whence we get $|b| \leq |x_0|^3 + |x_0| < 2|b|/5$ which is a contradiction. Therefore, there is no point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that $H(P) < (|b|/5)^{1/3}$.

Suppose next that $a \neq 0$ and $b = \pm 1$. Let $P = (x_0/z_0, y_0/z_0) \in E(\mathbb{Q}) \setminus \{O\}$, where $x_0, y_0, z_0 \in \mathbb{Z}^3$ with $x_0y_0z_0 \neq 0$, $\gcd(x_0, y_0, z_0) = 1$ and

$$H(P) = \max\{|x_0|, |y_0|, |z_0|\} < (|a|/5)^{1/3}.$$

We put $p_h(x, y, z) = y^2z - x^3 - axz^2 \mp z^3$, and proceeding as previously we construct a polynomial of the form

$$f(x, y, z) = nxz^2 + qp_h(x, y, z)$$

satisfying $f(x_0, y_0, z_0) = 0$. The equalities $f(x_0, y_0, z_0) = 0$ and $p_h(x_0, y_0, z_0) = 0$ yield $x_0z_0 = 0$. If $z_0 = 0$, then $P = O$ which is a contradiction. If $z_0 \neq 0$, then $x_0 = 0$. It follows that $(y_0/z_0)^2 = \pm 1$. Thus, for $b = -1$ we have $(y_0/z_0)^2 = -1$ which is a contradiction. For $b = 1$, we have $(y_0/z_0)^2 = 1$, whence $y_0/z_0 = \pm 1$ and hence $P = (0, \pm 1)$. □

Proof of Corollary 3. Let $P = (x(P), (y(P)) \in E_{\pm}(\mathbb{Q}) \setminus \{O\}$. By Lemma 4, we have

$$H(P) < \sqrt{2}\, H(x(P))^{3/2}.$$

It follows that

$$h(P) < 0.347 + \frac{3}{2}\, h(x(P)). \tag{13}$$

Combining Theorem 2(a) and Inequality (13), we have

$$\frac{1}{3}\log|b| - 0.89 < \frac{3}{2}\, h(x(P)). \tag{14}$$

The modular invariant of $E_{\pm}$ is equal to

$$|j_{E_{\pm}}| = \frac{6912}{27b^2 \pm 4}.$$

Then, $|j_{E_{\pm}}|$ takes the larger value for $b = 3$. Thus, we have $\log|j_{E_{\pm}}| < 3.365$. It follows that Lemma 3 and Inequality (14) imply

$$\frac{1}{9}\log b - 1.923 < \hat{h}(P).$$

□

5. Proof of Theorem 3

Proof of Theorem 3. (a) Set $p_h(x, y, z) = y^2z - x^3 - axz^2 - az^3$. Let $P = (x_0/z_0, y_0/z_0) \in E(\mathbb{Q})\backslash\{O\}$, where $x_0, y_0, z_0 \in \mathbb{Z}^3$ with $x_0y_0z_0 \neq 0$ and $\gcd(x_0, y_0, z_0) = 1$, such that

$$H(P) = \max\{|x_0|, |y_0|, |z_0|\} < (|a|/4)^{1/3}. \tag{15}$$

Consider a positive integer n such that $n > a^2$ and $\gcd(n, a) = 1$. Then, there are integers q and r such that $n = aq + r$ and $0 \leq r < |a|$. Since $\gcd(n, a) = 1$, we have $r > 0$. Furthermore, we have $|q| = \lfloor n/|a| \rfloor$.

We set

$$\begin{aligned} f(x, y, z) &= nz^2(x + z) + qp_h(x, y, z) \\ &= q(y^2z - x^3) + (n - qa)(xz^2 + z^3) \\ &= qy^2z - qx^3 + rxz^2 + rz. \end{aligned}$$

Then, we have

$$f(x_0, y_0, z_0) = nz^2(x_0 + y_0) \equiv 0 \pmod{n}.$$

Furthermore, using (15), we obtain:

$$|f(x_0, y_0, z_0)| \leq 2q\frac{|a|}{4} + 2r\frac{|a|}{4} < 2\frac{n}{|a|}\frac{|a|}{4} + 2|a|\frac{|a|}{4} < n.$$

Since $f(x_0, y_0, z_0) \equiv 0 \pmod{n}$ and $|f(x_0, y_0, z_0)| < n$, we get $f(x_0, y_0, z_0) = 0$. Then, we have

$$0 = f(x_0, y_0, z_0) = nz^2(x_0 + z_0) + qp_h(x_0, y_0, z_0) = nz^2(x_0 + z_0).$$

Therefore, we get $x_0/z_0 = -1$, whence we deduce $(y_0/z_0)^2 = -1$ which is a contradiction.

Suppose now that $x_0 = 0$. Then, $(y_0/z_0)^2 = a$. If $a < 0$, then we have a contradiction. Suppose that $a > 0$. It follows that $y_0/z_0 = \pm\sqrt{a}$ and a is a perfect square. But in this case, we have $H(P) = \sqrt{a} > (|a|/4)^{1/3}$ which is a contradiction. Finally, suppose that $y_0 = 0$. Then $\rho = x_0/z_0$ is a root of equation $g(x) = x^3 + ax + a = 0$. It follows that $\rho \in \mathbb{Z}$ with $\rho \mid a$. Then, we have $a = a_1\rho$, where $a_1 \in \mathbb{Z}$, and so, we get $\rho^2 + a_1\rho + a_1 = 0$. Let σ be the second root of the previous equation. Then, we have $\rho + \sigma = -a_1$ and $\rho\sigma = a_1$, whence we get $\sigma \in \mathbb{Z}$ and $\rho + \sigma + \rho\sigma = 0$. It follows that $(\rho + 1)(\sigma + 1) = 1$, and therefore we have $\rho + 1 = \sigma + 1 = \pm 1$. If $\rho + 1 = 1$, then $\rho = 0$, and therefore $g(0) = 0$, whence $a = 0$ which is a contradiction. Then, $\rho + 1 = -1$, and so, $\rho = -2$. Therefore, we have $g(-2) = 0$, and we obtain $a = -8$. The solutions of the equation $x^3 - 8x - 8 = 0$ are -2 and $1 \pm \sqrt{5}$. Furthermore, we have $H(-2, 0) = 2 < (|a|/4)^{1/3} = 2^{1/3}$ which is a contradiction. The result follows.

(b) Set $p_h(x, y, z) = y^2z - x^3 - axz^2 + az^3$. Let $P = (x_0/z_0, y_0/z_0) \in E(\mathbb{Q}) \setminus \{O\}$, where $x_0, y_0, z_0 \in \mathbb{Z}^3$ with $x_0y_0z_0 \neq 0$, $\gcd(x_0, y_0, z_0) = 1$ and $H(P) < (|a|/4)^{1/3}$. Proceeding as in case (a), we construct a a polynomial of the form

$$f(x, y, z) = nz^2(x - z) + qp_h(x, y, z) = qy^2z - qx^3 + rxz^2 - rz^3$$

(where q, r as in case (a)) such that $f(x_0, y_0, z_0) = 0$. Thus, the equalities $p_h(x_0, y_0, z_0) = f(x_0, y_0, z_0) = 0$ imply $n(x_0 - z_0) = 0$, whence $x_0/z_0 = 1$. It follows that $(y_0/z_0)^2 = 1$, and so, we get $y/z_0 = \pm 1$. Hence $P = (1, \pm 1)$. Furthermore, it is easily seen that the order of the point P is 3, and so, the set $\{O, P, -P\}$ is a subgroup of order 3 of $E(\mathbb{Q})$.

Suppose next that $x_0 = 0$. Then, we deduce, as in the previous case, a contradiction. If $y_0 = 0$, then $\rho = x_0/z_0$ is a root of equation $h(x) = x^3 + ax - a = 0$. Then, we have $a = a_1\rho$, and so, we get $\rho^2 + a_1\rho - a_1 = 0$. If σ is the second root of this equation, then, we have $\rho + \sigma = -a_1$ and $\rho\sigma = -a_1$, whence we obtain $\sigma \in \mathbb{Z}$ and $\rho + \sigma - \rho\sigma = 0$. It follows that $(\rho - 1)(\sigma - 1) = 1$, and therefore we deduce $\rho - 1 = \sigma - 1 = \pm 1$. If $\rho - 1 = -1$, then $\rho = 0$, and we have, as in the previous case, $a = 0$, which is a contradiction. If $\rho - 1 = 1$, then $\rho = 2$. It follows that $a = -8$. The solutions of the equation $x^3 - 8x + 8 = 0$ are 2 and $-1 \pm \sqrt{5}$. Furthermore, we have $H(2, 0) = 2 < (|a|/4)^{1/3} = 2^{1/3}$ which is a contradiction. The result follows.

Finally, the proofs of (c) and (d) are similar to the previous ones and are thus omitted. □

6. An Algorithm

The proof of Theorem 1 leads to the following algorithm, which computes the unique pair of points $\pm P \in E(\mathbb{Q}) \setminus \{O\}$ with $x(P)y(P) \neq 0$ (if it exists), with naive height below the bound established in Theorem 1.

Algorithm 1.
Input: An elliptic curve E defined by an equation $p(x, y) = y^2 - x^3 - ax - b = 0$, where $a, b \in \mathbb{Z}$, with $ab \neq 0$ and $a \neq \pm b$.
Output: The points $\pm P \in E(\mathbb{Q}) \setminus \{O\}$ with $x(P)y(P) \neq 0$ such that

$$H(P) < \left(\frac{n}{\sqrt{6}\, L}\right)^{1/3},$$

where $n = \lfloor \|p\|^{3/2}/(2^{3/4} \cdot 1.001) \rfloor$ and L is the length of the shortest vector of an LLL-reduced basis of the lattice $\mathcal{L}$ generated by the vectors $(1, a, b)$, $(0, n, 0)$ and $(0, 0, n)$. If such a point does not exist the algorithm returns "Ø".

1. Compute
$$n = \left\lfloor \frac{\|p\|^{3/2}}{2^{3/4} \cdot 1.001} \right\rfloor.$$

2. Consider the lattice $\mathcal{L}$ spanned by the rows of the matrix
$$A = \begin{pmatrix} 1 & a & b \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix},$$
and using the LLL algorithm compute a reduced basis of $\mathcal{L}$ with smaller vector $\mathbf{u} = (u_1, u_2, u_3)$.

3. Compute
$$z_0 = \frac{u_2 - u_1 a}{n} \quad \text{and} \quad x_0 = \frac{u_1 b - u_3}{n}.$$

4. Output the points $\pm P \in E(\mathbb{Q}) \setminus \{O\}$ with $x(P) = x_0/z_0$. If such a point P does not exist, then output "Ø".

Below we give three examples in two of which the pair of points exists, while in the third it does not. Note that in all cases the inequality of Corollary 1, $1 + |a| < \|p\|^{1/2}/1.782$, does not hold.

Example 1. Consider the elliptic curve E defined by the equation

$$y^2 = x^3 + 1125899906842625x + 100205091709713235.$$

We have

$$n = 188815387445966929533540 98.$$

We consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$A = \begin{pmatrix} 1 & 1125899906842625 & 100205091709713235 \\ 0 & 1888153874459669295335 4098 & 0 \\ 0 & 0 & 1888153874459669295335 4098 \end{pmatrix}.$$

The LLL algorithm provides the following reduced basis for $\mathcal{L}$:

$$\begin{aligned} \mathbf{u} &= (268322803897, -2162850937955943, 594039434241243), \\ \mathbf{v} &= (-150931577192, 1286972396777882, 5928671050096378), \\ \mathbf{w} &= (-26238571527289063122, -3245326396338224, -989839033970258). \end{aligned}$$

The smallest vector of the above basis is $\mathbf{u}$ with length

$$L = 2242946076312956.20365866254680.$$

We shall compute the only rational point P (if it exists) with

$$H(P) \leq \lfloor (n/\sqrt{6}\, L)^{1/3} \rfloor = 1509.$$

We compute:

$$z_0 = \frac{-2162850937955943 - 268322803897 \times 1125899906842625}{1888153874459669295335 4098} = -16,$$

$$x_0 = \frac{268322803897 \times 100205091709713235 - 594039434241243}{1888153874459669295335 4098} = 1424.$$

Thus, we have $x_0/z_0 = -89$, and therefore $P = (-89, 121)$ is a point on E. Hence, we have found the points $(-89, \pm 121)$. Furthermore, we easily see (using for example SAGE) that the torsion group of E over $\mathbb{Q}$ is trivial. Hence, the points $(-89, \pm 121)$ are the only points, P, on the elliptic curve E with height $H(P) \leq 1509$, and their order is infinite.

Example 2. Let E be the elliptic curve defined by the equation

$$y^2 = x^3 + 9007199254740997x + 1648317463623779779.$$

We have

$$n = 1257084413730500663948905724.$$

We consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$A = \begin{pmatrix} 1 & 9007199254740997 & 1648317463623779779 \\ 0 & 1257084413730500663948905724 & 0 \\ 0 & 0 & 1257084413730500663948905724 \end{pmatrix}.$$

By applying the LLL algorithm (using for example the computational package SAGE), we compute the following reduced basis for $\mathcal{L}$:

$$\begin{aligned}\mathbf{u} &= (-976950842011, 33435944770715101, 83832102062736875),\\ \mathbf{v} &= (2651723714030, -89467964484120846, 7929646347397022),\\ \mathbf{w} &= (-203499702802419166527, -8873334237657355, -6381886666290097).\end{aligned}$$

The smaller vector of this basis is $\mathbf{u}$ with length

$$L = 90253995700588656.3643105596067.$$

We shall examine if there is a rational point P with $x(P)y(P) \neq 0$ with

$$H(P) \leq \lfloor (n/\sqrt{6}L)^{1/3} \rfloor = 1784.$$

We compute:

$$z_0 = \frac{33435944770715101 - (-976950842011) \times 9007199254740997}{125708441373050066394890572 4} = 7,$$

$$x_0 = \frac{-976950842011 \times 1648317463623779779 - 83832102062736875}{125708441373050066394890572 4} = -1281.$$

Thus, we have the point $P = (-183, 221)$ of E. Furthermore, the torsion group of E is trivial. Hence, the points $\pm P = (-183, \pm 221)$ are the only rational points of the elliptic curve with height at most 1784, and have infinite order.

Example 3. Consider the elliptic curve E defined by the equation

$$y^2 = x^3 - 1125900980584453x + 2033993457891049.$$

We have

$$n = 66585104598419215253253.$$

We consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$A = \begin{pmatrix} 1 & -1125900980584453 & 2033993457891049 \\ 0 & 66585104598419215253253 & 0 \\ 0 & 0 & 66585104598419215253253 \end{pmatrix}.$$

The LLL algorithm provides the following reduced basis for $\mathcal{L}$:

$$\begin{aligned}\mathbf{u} &= (315226585822314, -508511982146052, 45781937662197),\\ \mathbf{v} &= (-630453171644627, -108877016292349, 19424295825666558),\\ \mathbf{w} &= (-3046001647457609 - 1876781804548744 - 667038003994697).\end{aligned}$$

The smallest vector of the above basis is $\mathbf{u}$ with length

$$L = 600040183830553.713219321927951.$$

We shall compute the only rational point P (if it exists) with

$$H(P) \leq \lfloor (n/\sqrt{6}L)^{1/3} \rfloor = 356.$$

We compute:

$$z_0 = \frac{-508511982146052 - 315226585822314 \times (-1125900980584453)}{66585104598419215253253} = 5330230,$$

$$x_0 = \frac{315226585822314 \times 2033993457891049 - 45781937662197}{66585104598419215253253} = 9629313.$$

We easily verify that the quantity $x_0/z_0 = 5330230/9629313$ is not the x-coordinate of a rational point of E. Furthermore, the torsion group of E over $\mathbb{Q}$. Therefore, the elliptic curve E has not a rational point of height ≤ 356.

Acknowledgements. The author sincerely thanks the anonymous referee for useful and helpful suggestions and comments.

References

[1] J. E. Cremona, M. Prickett, and S. Siksek, Height difference bounds for elliptic curves over number fields, *J. Number Theory* **116** (2006), 42-68.

[2] S. David, Points de petite hauteur sur les courbes elliptiques, *J. Number Theory* **64** (1997), 104-129.

[3] G. Everest, P. Ingram, and S. Stevens, Primitive divisors on twists of the Fermat cubic, *LMS J. Comput. Math.* **12** (2009), 54-81.

[4] G. Everest, G. Mclaren, and T. Ward, Primitive divisors of elliptic divisibility sequences, *J. Number Theory* **118** (2006), 71-89.

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

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Undergraduate Texts in Mathematics, Springer, New York, 2008.

[7] S. Lang, *Elliptic Curves, Diophantine Analysis,* Springer, Berlin - Heidelberg - New York, 1978.

[8] C. Petsche, Small rational points on elliptic curves over number fields, *New York J. Math.* **12** (2006), 257-268.

[9] J. H. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48** (1981), 633-648.

[10] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55** (192) (1990), 723-743.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[12] Y. Uchida, The difference between the ordinary height and the canonical height on elliptic curves, *J. Number Theory* **128** (2) (2008), 263-279.

[13] P. Voutier and M. Yabuta, Primitive divisors of certain elliptic divisibility sequences, *Acta Arith.* **151** (2012), 165-190.

[14] P. Voutier and M. Yabuta, Lang's conjecture and sharp height estimates for the elliptic curves $y^2 = x^3 + ax$, *Int. J. Number Theory* **9** (5) (2013), 1141-1170.

[15] P. Voutier and M. Yabuta, Lang's conjecture and sharp height estimates for the elliptic curves $y^2 = x^3 + b$, *Acta Arith.* **173** (3) (2016), 197-224.

[16] H. G. Zimmer, On the difference of the Weil height and the Néron-Tate height, *Math. Z.* **147** (1976), 35-51.