Journal of Number Theory **80**, 187–208 (2000)
Article ID jnth.1999.2430, available online at http://www.idealibrary.com on IDEAL®

Integral Points in Arithmetic Progression on $y^2 = x(x^2 - n^2)$

A. Bremner

Department of Mathematics, Arizona State University, Tempe, Arizona 85287
E-mail: bremner@asu.edu

J. H. Silverman

Department of Mathematics, Brown University, Providence, Rhode Island 02912
E-mail: jhs@math.brown.edu

and

N. Tzanakis

Department of Mathematics, University of Crete, Iraklion, Greece
E-mail: tzanakis@itia.cc.uch.gr

Communicated by A. Granville

Received July 27, 1998

1. INTRODUCTION

Let $n \geqslant 1$ be an integer, and let E be the elliptic curve

$$E\colon\ y^2 = x(x^2 - n^2). \tag{1}$$

In this paper we consider the problem of finding three integral points P_1, P_2, P_3 whose x-coordinates $x_i = x(P_i)$ form an arithmetic progression with $x_1 < x_2 < x_3$.

Let $T_1 = (-n, 0)$, $T_2 = (0, 0)$, and $T_3 = (n, 0)$ denote the two-torsion points of E. As is well known [Si1, Proposition X.6.1(a)], the full torsion subgroup of $E(\mathbf{Q})$ is $E(\mathbf{Q})_{\text{tors}} = \{\mathcal{O}, T_1, T_2, T_3\}$.

One obvious solution to our problem is $(P_1, P_2, P_3) = (T_1, T_2, T_3)$. It is natural to ask whether there are further obvious solutions, say of the form

$$(T_1, Q, T_2) \qquad \text{or} \qquad (T_2, T_3, Q') \qquad \text{or} \qquad (T_1, T_3, Q''). \tag{2}$$

0022-314X/00 $35.00

This is equivalent to asking whether there exist integral points having x-coordinates equal to $-n/2$ or $2n$ or $3n$, respectively. As is easily checked, this occurs if and only if $n = 6N^2$ for some positive integer N, in which case

$$Q = (-3N^2, 9N^3), \quad Q' = (12N^2, 36N^3), \quad \text{and} \quad Q'' = (18N^2, 72N^3)$$

provide solutions. (Notice that T_1, T_2, T_3, Q', Q'' actually provides an example of five integral points in arithmetic progression.)

DEFINITION. Let $E/\mathbf{Q}$ be an elliptic curve given by a Weierstrass equation. For example, E might be the curve (1). An *arithmetic progression on* E is a sequence of at least three points $P_1, P_2, ..., P_s \in E(\mathbf{Q})$ whose x-coordinates $x_i = x(P_i)$ form an arithmetic progression with $x_1 < x_2 < \cdots < x_s$. An arithmetic progression is called *integral* if all of the x_i's are integers. Notice that the definition of arithmetic progression is independent of the choice of Weierstrass equation for E, since any other x coordinate is related to the original x by a transformation of the form $x' = u^2x + r$. On the other hand, integrality clearly depends on the choice of a particular equation.

DEFINITION. Let $E/\mathbf{Q}$ be the title elliptic curve (1). With notation as above, we call the triple (T_1, T_2, T_3) a *trivial* arithmetic progression in $E(\mathbf{Q})$. If in addition n has the form $6N^2$, then the following progressions are also considered *trivial*, where Q, Q' and Q'' are as above, and in the last case, the two $\pm$ signs are independent of one another:

$$(T_1, \pm Q, T_2), \quad (T_1, T_3, \pm Q''), \quad (T_2, T_3, \pm Q'), \quad (T_3, \pm Q', \pm Q''). \tag{3}$$

Our interest in the problem of arithmetic progressions on (1) arose in the study of three-by-three magic squares of integers where one desires all entries of the square to be perfect squares. Robertson [Ro] observed that the existence of such an object is equivalent to the existence of an elliptic curve (1) containing an integral arithmetic progression of three points in $2E(\mathbf{Q})$. The first author has exploited this idea to produce infinitely many parametrized families of "almost" magic squares; see [Br].

Our principal goal in this paper is the proof of the following theorem.

THEOREM 1.1. *Let $n \geqslant 1$ be a squarefree integer, let E be the elliptic curve*

$$E: y^2 = x(x^2 - n^2), \tag{4}$$

and let $\Gamma \subset E(\mathbf{Q})$ be a subgroup of rank 1. *Then Γ contains no non-trivial integral arithmetic progressions.*

Remark. For curves of the form (4), we are aware of only one example of an integral arithmetic progression where none of the points is a torsion point. The curve

$$E\colon y^2 = x(x^2 - 1254^2)$$

has the integral arithmetic progression

$$(-528, 26136), \qquad (-363, 22869), \qquad (-198, 17424)$$

consisting of three non-torsion points. In fact, these three points are independent, so $E(\mathbf{Q})$ has rank at least 3; and using Cremona's **mrank** program, one can check that the rank is exactly 3. Further, the tables of Wada and Taira [WaTa] show that $n = 1254$ is the smallest n such that the rank of (4) equals 3.

The proof of Theorem 1.1 requires very delicate height computations to deal with the cases $n \geqslant 72$, explicit computations using both elementary methods and ideas of Stroeker and Tzanakis [StTz] to deal with the finitely many instances $1 \leqslant n < 72$, and a detailed analysis of arithmetic progressions (P_1, P_2, P_3) on (4) in which exactly *one* of the points is a torsion point. (Progressions with two or three torsion points are trivial by definition.) The torsion case is covered by the following two results.

THEOREM 1.2. *There are no arithmetic progressions* (P_1, P_2, P_3) *on the curve* (4) *when one of the points* P_i *is equal to the torsion point* $T_2 = (0, 0)$, *and the other two points are non-torsion.*

THEOREM 1.3. *Suppose* (P_1, P_2, P_3) *is an arithmetic progression on the curve* (4) *consisting of one of the torsion points* $T_1 = (-n, 0)$ *or* $T_3 = (n, 0)$ *together with two non-torsion points. This can occur if and only if*

$$n = 3(r^2 + s^2)(r^2 - 2s^2)(2r^2 - s^2)\, t^2$$

for coprime integers r, s, $(rs \neq 0)$ *and a rational number* t. *The progressions containing* T_1 *occur when* $r^2 > 2s^2$ *or* $r^2 < s^2/2$, *while the progressions containing* T_3 *occur when* $s^2/2 < r^2 < 2s^2$. *In both cases the points* P_1, P_2, P_3 *are given by*

$$P_1 = [-3(r^2 + s^2)(r^2 - 2s^2)(2r^2 - s^2)\, t^2, 0], \tag{5}$$

$$P_2 = [3(r^2 + s^2)^2 (2r^2 - s^2)\, t^2, 9s(r^2 + s^2)^2 (2r^2 - s^2)^2\, t^3], \tag{6}$$

$$P_3 = [9(r^2 + s^2)(2r^2 - s^2)\, r^2 t^2, 18r(r^2 + s^2)^2 (2r^2 - s^2)^2\, t^3]. \tag{7}$$

In the final section, we will use much coarser arguments to prove the following weak generalization of Theorem 1.1. (Note that in Theorem 1.4, the subgroup Γ, is required to be free of rank 1, that is, Γ is torsion free, while in Theorem 1.1, it is only required that $\Gamma/\Gamma_{\text{tors}}$ have rank 1.)

THEOREM 1.4. *Let the elliptic curve $E/\mathbf{Q}$ be given by a Weierstrass equation*

$$E\colon y^2 = x^3 + ax + b, \tag{8}$$

and for each integer A, let E_A be the quadratic twist of E by A,

$$E_A\colon y^2 = x^3 + A^2ax + A^3b. \tag{9}$$

There is a constant $A_0(E)$ so that the following holds: If $A \geqslant A_0(E)$ is a square-free integer and if $\Gamma \subset E_A(\mathbf{Q})$ is a subgroup with $\Gamma \cong \mathbf{Z}$ (i.e., Γ is free of rank 1*), then Γ does not contain an integral progression.*

2. HEIGHT ESTIMATES FOR RATIONAL POINTS ON $y^2 = x^3 - n^2x$

In this section we shall prove the following estimates for the canonical height on the elliptic curve given in the title.

PROPOSITION 2.1. *Fix a positive squarefree integer n and consider the elliptic curve*

$$E\colon y^2 = x^3 - n^2x. \tag{10}$$

Let $P \in E(\mathbf{Q})$ be a rational point on E such that $2P \neq \mathcal{O}$, and write the x-coordinate of P as $x = a/d^2$. Then,

$$\hat{h}(P) \geqslant \frac{1}{16}\log(2n^2), \tag{11}$$

$$\hat{h}(P) \geqslant \frac{1}{4}\log\left(\frac{a^2 + n^2d^4}{2n^2}\right), \tag{12}$$

$$\hat{h}(P) \leqslant \frac{1}{4}\log(a^2 + n^2d^4) + \frac{1}{12}\log 2. \tag{13}$$

Remark. The inequalities (12) and (13) in Proposition 2.1 involve the quantity $\frac{1}{4}\log(a^2+n^2d^4)$ rather than the more usual height $\frac{1}{2}h(x)=\frac{1}{2}\log\max\{|a|,|d^2|\}$. However, observe that these quantities are related by the elementary inequalities

$$\tfrac{1}{2}h(x)\leqslant\tfrac{1}{4}\log(a^2+n^2d^4)\leqslant\tfrac{1}{2}h(x)+\tfrac{1}{4}\log(n^2+1), \tag{14}$$

so a weaker form of Proposition 2.1 says that

$$-\tfrac{1}{2}\log n-\tfrac{1}{4}\log 2\leqslant\hat{h}(P)-\tfrac{1}{2}h(x)\leqslant\tfrac{1}{4}\log(n^2+1)+\tfrac{1}{12}\log 2. \tag{15}$$

Remark. A number of other authors have given explicit estimates, in varying degrees of generality, for the difference between the canonical height and the Weil height on elliptic curves. See, for example, [BrCa, BGZ, De, Sik, Si7, Zi]. However, the inequalities (12) and (13) are sharper than any of these results, albeit for the very special family of curves $y^2=x^3-n^2x$ with which we are concerned in this paper.

Remark. The lower bound (11) is a special case of a conjecture of Serge Lang [La], which says that the canonical height of a non-torsion point on an elliptic curve should satisfy

$$\hat{h}(P)\gg\log|\Delta|.$$

Lang's conjecture was proven for elliptic curves with integral j-invariant [Si4, Si3] using a pigeon-hole argument, for elliptic curves which are twists [Si5] using Galois theory, and for elliptic curves with bounded Szpiro ratio [HiSi] using a Fourier averaging method. The curves E which we are studying happen to fit into all three of these categories, but none of the cited papers contains an explicit evaluation of constants. Thus (11) is an explicit, and probably close to sharp, version of Lang's conjecture for the curves $y^2=x^3-n^2x$. (Note that the discriminant of this curve is $\Delta=64n^6$, so the lower bound in (11) can equally well be expressed in terms of the discriminant of E.)

Proof of Proposition 2.1. The proof involves a detailed analysis of local height functions

$$\hat{\lambda}_p\colon E(\mathbf{Q}_p)\backslash\{O\}\to\mathbf{R}. \tag{16}$$

We will consider in turn the archimedean local height $\hat{\lambda}_\infty$, the local heights $\hat{\lambda}_p$ with $p\geqslant 3$, and the 2-adic local height $\hat{\lambda}_2$. Then the proof of Proposition 2.1 will be a simple matter of combining the various local estimates. For the definition of local heights and a description of their basic properties, see for example [Si2, Chap. VI].

Archimedean Estimates. We will estimate the archimedean contribution to the canonical height by using Tate's series (cf. [BGZ], where a similar method is used to analyze a specific curve of conductor 5077). In order to describe Tate's series for our curve E (see [Si6, Zi]), let

$$t = 1/x, \qquad w = 4t - 4n^2t^2, \qquad z = (1 + n^2t^2)^2.$$

We also note that the discriminant of E is $\Delta = 64n^6$. Then the archimedean local height of a point $P \in E(\mathbf{R})$ is given by the series

$$\hat{\lambda}_\infty(P) = \tfrac{1}{2} \log |x(P)| + \tfrac{1}{8} \sum_{k=0}^{\infty} 4^{-k} \log |z(2^k P)| - \tfrac{1}{12} \log |\Delta|,$$

where the series will converge provided the multiples $2^k P$ are uniformly bounded away from $(0, 0)$.

The real locus $E(\mathbf{R})$ has two components, and every point on the identity component $E^0(\mathbf{R})$ satisfies $x \geqslant n$. Further, we know that $2E(\mathbf{R}) \subset E^0(\mathbf{R})$, so if $Q \in E^0(\mathbf{R})$, then

$$x(Q) \geqslant n, \qquad 0 \leqslant t(Q) \leqslant \frac{1}{n}, \qquad 1 \leqslant z(Q) \leqslant 4. \tag{17}$$

Notice this applies in particular to $2^k P$ for every $P \in E(\mathbf{R})$ and every $k \geqslant 1$. Hence

$$\hat{\lambda}_\infty(P) = \tfrac{1}{2} \log |x(P)| + \tfrac{1}{8} \log |z(P)| + \tfrac{1}{8} \sum_{k=1}^{\infty} 4^{-k} \begin{pmatrix} \text{quantity between} \\ 0 \text{ and } \log 4 \end{pmatrix} - \tfrac{1}{12} \log |\Delta|, \tag{18}$$

so using the definition of z, we get

$$0 \leqslant \hat{\lambda}_\infty(P) - (\tfrac{1}{4} \log(x(P)^2 + 2) - \tfrac{1}{12} \log |\Delta|) \leqslant \tfrac{1}{12} \log 2. \tag{19}$$

Remark. It is possible to improve the upper bound by using the fact that if $2P$ is close to $(n, 0)$, then $2^k P$ will be close to $\mathcal{O}$ for $k \geqslant 2$. For example, just considering $2P$ and $4P$, the upper bound may be improved to $(13/12 \cdot 16) \log 2$. This is close to best possible, since if $2P$ is close to $(n, 0)$, then the series (with $k \geqslant 1$) actually gives $(1/16) \log 2$. We have chosen not to pursue this further, since in any case, it is generally the lower bound in (19) which is most useful in practice.

Non-Archimedean Estimates—Generalities. The canonical local height $\hat{\lambda}_p$ is a function

$$\hat{\lambda}_p : E(\mathbf{Q}_p) \backslash \{\mathcal{O}\} \to \mathbf{R} \tag{20}$$

TABLE I

Reduction Types and Local Heights

Type	$E(\mathbf{Q}_p)/E^0(\mathbf{Q}_p)$	$\varepsilon_p(P)$ for $P \notin E^0$
III	$\mathbf{Z}/2\mathbf{Z}$	3
I_0^*	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	6
I_2^*	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	6 or 9

satisfying certain growth and transformation properties (see, e.g., [Si2, VI, Sect. 1] for details). If $P \in E(\mathbf{Q}_p)$ lies on the identity component $E^0(\mathbf{Q}_p)$ of the Néron model (equivalently, if the reduction of P modulo p is non-singular), then the local height of P is given by the simple formula

$$\hat{\lambda}_\infty(P) = \tfrac{1}{2}\max\{0, -v_p(x(P))\} + \tfrac{1}{12}\, v_p(\Delta), \tag{21}$$

where we write $v_p(x) = \mathrm{ord}_p(x)\log(p)$. (See, for example, [Si2, VI.4.1].)

In general, define a quantity $\varepsilon_p(P)$ by writing the local height as

$$\hat{\lambda}_p(P) = \frac{1}{2}\max\{0, -v_p(x(P))\} + \frac{1}{12}\, v_p(\Delta) - \frac{\varepsilon_p(P)}{12}\log(p). \tag{22}$$

If P is not in $E^0(\mathbf{Q}_p)$, then the special fiber of E is necessarily of type I_N, *III*, *IV*, I_N^*, *IV**, or *III**. A complete description of the possible values of $\varepsilon_p(P)$ for all reduction types can be found in [Si3], but we will be content here to cite the three cases shown in Table I, which is all that we need for analyzing the curves $y^2 = x^3 - n^2x$. (For Type I_2^* reduction, one of the non-identity components is "close" to the identity component, and the other two are further away, which accounts for the two possibilities for $\varepsilon_p(P)$ in this case.)

Non-Archimedean Estimates ($p \geqslant 3$). We now fix an odd prime p and take a (non-zero) point $P \in E(\mathbf{Q}_p)$. As noted above, if P lies on the identity component $E^0(\mathbf{Q}_p)$ of the Néron model (equivalently, if the reduction of P modulo p is non-singular), then the local height P is given by the simple formula (21), with $\Delta = 64n^6$. If $P \notin E^0(\mathbf{Q}_p)$, then necessarily $p \mid n$, and using Tate's algorithm ([Si2, IV.9.4], [Ta]), we find that E has Type I_0^* reduction at p. Then Table I tells us that $\varepsilon_p(P) = 6$. To summarize, we have

$$\begin{aligned}\hat{\lambda}_p(P) = {} & \tfrac{1}{2}\max\{0, -v_p(x(P))\} \\ & + \tfrac{1}{12}\, v_p(\Delta) - \begin{cases} 0 & \text{if} \quad P \in E^0(\mathbf{Q}_p), \\ \tfrac{1}{2}v_p(n) & \text{if} \quad P \notin E^0(\mathbf{Q}_p). \end{cases}\end{aligned} \tag{23}$$

Non-Archimedean Estimates ($p=2$). We now consider the local height for $p=2$. Note that n^2 satisfies one of the two congruences

$$n^2 \equiv 1 \pmod 4 \qquad \text{or} \qquad n^2 \equiv 4 \pmod{16},$$

depending on whether n is odd or even respectively. A lengthy, but straightforward, computation using Tate's algorithm [Si2, IV.9.4; Ta] reveals that E has Type *III* reduction if n is odd, and Type I_2^* reduction if n is even. Note that in both cases the group of components is killed by 2, so $2E(\mathbf{Q}_2) \subset E^0(\mathbf{Q}_2)$. Reading off the various values from Table I, we find the following possibilities for $\hat{\lambda}_2$,

$$\hat{\lambda}_2(P) = \tfrac{1}{2}\max\{0,\, -v_2(x(P))\} + \tfrac{1}{12}\, v_2(\Delta)$$

$$- \begin{cases} 0 & \text{if} \quad P \in E^0(\mathbf{Q}_2), \\ \tfrac{1}{4}\log 2 & \text{if} \quad P \notin E^0(\mathbf{Q}_2),\ n \text{ odd}, \\ \tfrac{1}{2}\log 2 \text{ or } \tfrac{3}{4}\log 2 & \text{if} \quad P \notin E^0(\mathbf{Q}_2),\ n \text{ even}. \end{cases} \tag{24}$$

Completion of the Proof of Proposition 2.1. To prove the lower bound (11), we let $Q=2P$ and first derive a lower bound for $\hat{h}(Q)$. The fact that $Q \in 2E(\mathbf{Q})$ means that $Q \in E^0(\mathbf{Q}_p)$ for every prime p, including $p=2$, as shown above. Hence we can use (21) for every finite prime,

$$\hat{\lambda}_p(Q) = \tfrac{1}{2}\max\{0,\, -v_p(x(Q))\} + \tfrac{1}{12}\, v_p(\Delta). \tag{25}$$

Writing $x(Q) = \alpha/\delta^2$ as a fraction in lowest terms and summing over all finite primes gives the exact formula

$$\sum_{p \neq \infty} \hat{\lambda}_p(Q) = \log|\delta| + \tfrac{1}{12}\log|\Delta|. \tag{26}$$

Next, add this to the lower bound (19) for $\hat{\lambda}_\infty(Q)$ to obtain

$$\hat{h}(Q) \geqslant \tfrac{1}{4}\log(\alpha^2 + n^2\delta^4). \tag{27}$$

Since $\delta \geqslant 1$, we trivially obtain the lower bound $\frac{1}{2}\log n$. However, we can do a little better by observing that since $Q \in E^0(\mathbf{R})$, then $\alpha/\delta^2 \geqslant n$, so in fact $\alpha^2 + n^2\delta^4 \geqslant 2n^2\delta^4 \geqslant 2n^2$. This gives the lower bound

$$\hat{h}(Q) \geqslant \tfrac{1}{4}\log(2n^2), \tag{28}$$

and then the formula $\hat{h}(Q) = \hat{h}(2P) = 4\hat{h}(P)$ gives the desired inequality (11).

In order to prove the upper and lower bounds which relate the canonical height to the naive height, rewrite the inequalities (19), (23), and (24) respectively, as

$$0 \leqslant \hat{\lambda}_\infty(P) - \frac{1}{4}\log\left(\frac{a^2+n^2d^4}{d^4}\right) + \frac{1}{12}\log|\Delta| \leqslant \frac{1}{12}\log 2$$

$$-\frac{1}{2}v_p(n) \leqslant \hat{\lambda}_p(P) - v_p(d) - \frac{1}{12}v_p(\Delta) \leqslant 0 \qquad (p \geqslant 3)$$

$$-\frac{1}{4}\log 2 - \frac{1}{2}v_2(n) \leqslant \hat{\lambda}_2(P) - v_2(d) - \frac{1}{12}v_2(\Delta) \leqslant 0.$$

Adding these estimates over all places yields

$$-\tfrac{1}{4}\log(2n^2) \leqslant \hat{h}(P) - \tfrac{1}{4}\log(a^2+n^2d^4) \leqslant \tfrac{1}{12}\log 2. \tag{29}$$

These are exactly the lower bound (12) and the upper bound (13) which we wanted to prove, which completes the proof of Proposition 2.1. ∎

3. HEIGHT ESTIMATES FOR INTEGRAL POINTS ON $y^2 = x^3 - n^2x$

In this section we apply Proposition 2.1 to integral points P on the elliptic curve E given in the title. We assume throughout that n is a positive square-free integer.

PROPOSITION 3.1. (i) *For any integral point P on E,*

$$\hat{h}(P) - \tfrac{1}{2}\log|x(P)| > -\tfrac{1}{2}\log n - \tfrac{1}{4}\log 2. \tag{30}$$

(ii) *For any integral point P on the identity component of E,*

$$\hat{h}(P) - \tfrac{1}{2}\log(x(P)) \leqslant \tfrac{1}{3}\log 2. \tag{31}$$

(iii) *Let P_2 and P_3 be integral points on the identity component of E which satisfy $2x(P_2) > x(P_3) > x(P_2)$. Then*

$$-\tfrac{1}{2}\log n - \tfrac{7}{12}\log 2 < \hat{h}(P_3) - \hat{h}(P_2) < \tfrac{1}{2}\log n + \tfrac{13}{12}\log 2. \tag{32}$$

Proof. (i) This is a straightforward application of (12).

(ii) Since $x(P) \geqslant n$, the claimed inequality results immediately from (13).

(iii) Write $x(P_i) = x_i$. By (30) and the fact that $0 < x_2 < x_3$, we have

$$-\tfrac{1}{2}\log n - \tfrac{1}{4}\log 2 < \hat{h}(P_3) - \tfrac{1}{2}\log x_3 < \hat{h}(P_3) - \tfrac{1}{2}\log x_2.$$

On the other hand, by (31) and $2x_2 > x_3 > 0$,

$$\begin{aligned}\tfrac{1}{3}\log 2 \geqslant \hat{h}(P_3) - \tfrac{1}{2}\log x_3 &> \hat{h}(P_3) - \tfrac{1}{2}\log(2x_2) \\ &= \hat{h}(P_3) - \tfrac{1}{2}\log x_2 - \tfrac{1}{2}\log 2,\end{aligned}$$

and hence

$$-\tfrac{1}{2}\log n - \tfrac{1}{4}\log 2 < \hat{h}(P_3) - \tfrac{1}{2}\log x_2 < \tfrac{5}{6}\log 2.$$

For the point P_2, in view of (30) and (31),

$$-\tfrac{1}{2}\log n - \tfrac{1}{4}\log 2 < \hat{h}(P_2) - \tfrac{1}{2}\log x_2 \leqslant \tfrac{1}{3}\log 2.$$

Eliminating $\log x_2$ from the last two relations gives the required inequality. ∎

COROLLARY 3.2. *Let $Q \in E(\mathbf{Q})$ be a point of infinite order, and let P_2 and P_3 be integral points on the identity component of E belonging to the group generated by Q and $E(\mathbf{Q})_{\text{tors}}$. Assume further that $x(P_2) < x(P_3) < 2x(P_2)$, and write $P_i = m_i Q$ modulo torsion for $i = 2, 3$. If $n \geqslant 72$, then*

$$|m_3^2 - m_2^2| \leqslant 4 \qquad \text{and} \qquad m_3 \neq 0.$$

Proof. Replacing Q by $Q + T_1$ if necessary, we may assume that Q belongs to the identity component of E. Using $\hat{h}(P_i) = \hat{h}(m_i Q) = m_i^2 \hat{h}(Q)$ and (32), we find that

$$-\frac{(1/2)\log n + (7/12)\log 2}{\hat{h}(Q)} < m_3^2 - m_2^2 < \frac{(1/2)\log n + (13/12)\log 2}{\hat{h}(Q)}.$$

Using (11) and $n \geqslant 72$, we can estimate the upper and lower bounds, obtaining

$$-4 \leqslant m_3^2 - m_2^2 \leqslant 4.$$

Finally, observe that $m_3 = 0$ implies $x_3 = n$; but, since P_2 belongs to the zero-component of E, then $x_2 \geqslant n$, which contradicts the assumption $x_2 < x_3$. ∎

4. INTEGRAL ARITHMETIC PROGRESSIONS ON $y^2 = x^3 - n^2x$

In this section we shall prove Theorem 1.1. The proof splits into two cases depending on whether $n \geqslant 72$ or $n < 72$.

4.1. *The Case* $n \geqslant 72$

Without loss of generality, fix a non-torsion point $Q \in E(\mathbf{Q})$ belonging to the identity component of E, and assume that P_1, P_2, P_3 is a non-trivial integral arithmetic progression lying in the subgroup $\langle Q \rangle \oplus E(\mathbf{Q})_{\text{tor}}$. Write $P_i = m_i Q$ modulo torsion for each $i = 1, 2, 3$. Our goal is to show that necessarily $n < 72$.

PROPOSITION 4.1. *With the above notation and under the above assumptions, suppose that P_2 and P_3 lie on the identity component, and further suppose that $m_2 = \pm m_3$. If $n \geqslant 3$, then $|m_2| = |m_3| \leqslant 2$.*

Proof. Let $m = |m_2| = |m_3|$. Since the progression is non-trivial, we know that $m \neq 0$; and since P_i and $-P_i$ have the same x-coordinate, we may assume that $m_2 = m_3 = m$. We distinguish two cases:

(i) $P_3 = mQ$ and $P_2 = mQ + T_3$.

(ii) $P_2 = mQ$ and $P_3 = mQ + T_3$.

In both cases, mQ is an integral point on the identity component of E, so $a = x(mQ)$ satisfies $a > n$. In case (i) we have

$$x_3 - x_2 = \frac{a^2 - 2na - n^2}{a - n} = x_2 - x_1 \leqslant x_2 + n = \frac{2an}{a - n}.$$

Hence $a^2 - 4an - n^2 \leqslant 0$, from which we conclude that $a \leqslant (2 + \sqrt{5})\, n$.

In case (ii), $x_2 < x_3$ implies $a < n(a+n)/(a-n)$, and hence $a < (1 + \sqrt{2})\, n$. Thus, in any case, $n < a \leqslant (2 + \sqrt{5})\, n$, so applying (13) yields

$$m^2 \hat{h}(Q) = \hat{h}(mQ) \leqslant \tfrac{1}{2} \log(2 + \sqrt{5})\, n + \tfrac{1}{3} \log 2.$$

Since (11) gives $\hat{h}(Q) \geqslant \log(2n^2)/16$, we finally obtain

$$m^2 \leqslant \frac{8 \log(2 + \sqrt{5})\, n + 16/3 \log 2}{\log(2n^2)},$$

which, for $n \geqslant 3$, implies $|m| \leqslant 2$. ∎

For the points that belong to the non-identity component of E, we prove the following useful estimate.

LEMMA 4.2. *Let $P \in \langle Q \rangle \oplus E(\mathbf{Q})_{\text{tor}}$ be an integral point that belongs to the non-identity component of E. If $P = mQ$ modulo torsion, then $|m| \leqslant 2$. (We remark that this lemma is valid for every n.)*

Proof. Put $x(P) = x$. From (13) we have

$$\begin{aligned}\hat{h}(P) &\leqslant \tfrac{1}{4}\log(x^2 + n^2) + \tfrac{1}{12}\log 2 \\ &\leqslant \tfrac{1}{4}\log(2n^2) + \tfrac{1}{12}\log 2 = \tfrac{1}{12}\log(16n^6).\end{aligned}$$

On the other hand, by (11),

$$\hat{h}(P) = \hat{h}(mQ) = m^2\hat{h}(Q) \geqslant \frac{m^2}{16}\log(2n^2).$$

Combining the two inequalities gives

$$m^2 \leqslant \frac{4\log(16n^6)}{3\log(2n^2)} \leqslant \frac{40}{9} \approx 4.444,$$

(valid for $n \geqslant 2$), and hence $|m| \leqslant 2$. ∎

In order to complete the proof of Theorem 1.1 for $n \geqslant 72$, we now distinguish three cases, depending on whether three, two or none of the points P_1, P_2, P_3 belong to the identity component of E. Under the assumption that $n \geqslant 72$, in all three cases we shall arrive at a contradiction. Note that a non-trivial solution with exactly one point P_i on the non-identity component cannot exist. For in such a case, $x_3 \geqslant n$ and $-n \leqslant x_1 \leqslant x_2 \leqslant 0$, hence $n \geqslant x_2 - x_1 = x_3 - x_2 \geqslant x_3$. This is possible only if $(x_1, x_2, x_3) = (-n, 0, n)$, i.e., only in case of a trivial solution.

4.1.1. *P_1, P_2, P_3 Belong to the Identity Component of E.* For $i = 1, 2, 3$ put $P_i = m_i Q + \varepsilon_i T_3$, where $\varepsilon_i \in \{0, 1\}$. As noted above, we may assume that $m_i \geqslant 0$. Note that Corollary 3.2 can be applied, since $2x_2 = x_1 + x_3 > x_3$. Hence $0 \leqslant m_2, m_3 \leqslant 2$.

LEMMA 4.3. *With the above notation, $0 \leqslant m_1 \leqslant 2$.*

Proof. Suppose that $m_1 \geqslant 3$. Then $\hat{h}(P_1) = \hat{h}(m_1 Q) \geqslant 9\hat{h}(Q)$, and by (31),

$$\log x_1 \geqslant 2\hat{h}(P_1) - \tfrac{2}{3}\log 2 \geqslant 18\hat{h}(Q) - \tfrac{2}{3}\log 2.$$

In view of (30), we find that

$$\begin{aligned}\log x_2 &< 2\hat{h}(P_2) + \log n + \tfrac{1}{2}\log 2 \\ &= 2m_2^2\hat{h}(Q) + \log(2^{1/2}n) \\ &\leqslant 8\hat{h}(Q) + \log(2^{1/2}n).\end{aligned}$$

Since $x_1 < x_2$, combining the above two inequalities yields $10\hat{h}(Q) < \log(2^{7/6}n)$. Further, (11) tells us that $\hat{h}(Q) \geqslant (1/16)\log(2n^2)$, from which it follows that $2^{5/8}n^{5/4} < 2^{7/6}n$. Therefore, $n < 2^{13/6} \approx 4.49$, contradicting our assumption that $n \geqslant 72$. ∎

We know from Corollary 3.2 that $|m_3^2 - m_2^2| \leqslant 4$, and if $m_2^2 = m_3^2$, then Proposition 4.1 tells us that $|m_3| = |m_2| \leqslant 2$. It thus remains to treat the following cases:

$$P_i = m_i Q + \varepsilon_i T_3 \qquad \text{with} \quad 0 \leqslant m_i \leqslant 2 \quad \text{and}$$
$$\varepsilon_i \in \{0, 1\} \quad \text{for each} \quad i = 1, 2, 3.$$

To ease notation, let $q = x(Q) > n$. Observe now that

$$x(Q + T_3) = \frac{n(q+n)}{q-n},$$

$$x(2Q) = \frac{(q^2+n^2)^2}{4q(q^2-n^2)},$$

$$x(2Q + T_3) = n\left(\frac{q^2+2nq-n^2}{q^2-2nq-n^2}\right)^2.$$

Substituting these formulas into

$$2x(m_2 Q + \varepsilon_2 T_3) = x(m_1 Q + \varepsilon_1 T_3) + (m_3 Q + \varepsilon_3 T_3)$$

gives, for each particular choice of $m_1, m_2, m_3, \varepsilon_1, \varepsilon_2, \varepsilon_3$, an integral binary form in the variables n and q of degree varying between 4 and 8. For example, if $(P_1, P_2, P_3) = (2Q + T_3, Q + T_3, 2Q)$, then the relation $2x_2 = x_1 + x_3$ implies (after some calculation) that

$$n^8 - 8n^7q - 28n^6q^2 - 88n^5q^3 - 58n^4q^4 + 40n^3q^5 + 36n^2q^6 - 8nq^7 + q^8 = 0.$$

Hence if there is an arithmetic progression of the form $(2Q + T_3, Q + T_3, 2Q)$, then the polynomial

$$z^8 - 8z^7 - 28z^6 - 88z^5 - 58z^4 + 40z^3 + 36z^2 - 8z + 1$$

would have the rational root $z = n/q$. However, this polynomial has no rational roots, so we can rule out arithmetic progressions of the form $(2Q + T_3,\ Q + T_3,\ 2Q)$.

In a similar manner, we can rule out most of the other possibilities. However, in a few cases we obtain a polynomial which has $z = \pm 1$ as a root, which means that $q = \pm n$. But this implies that $Q = T_1$ or $Q = T_3$, contradicting our assumption that Q is non-torsion.

There are also a few cases where $z = 2$ or $z = 3$ appears as a root. For example, when $(P_1, P_2, P_3) = (T_3, Q + T_3, Q)$, the condition $2x_2 = x_1 + x_3$ is equivalent to $q^2 - 2qn - 3n^2$, and hence $q = -n$ or $3n$. The first possibility gives $Q = T_1$, so is rejected, while as explained in the introduction, the second implies that $n = 6N^2$ and that $Q = Q'' = (18N^2, 72N^3)$. We thus obtain the trivial progression $(T_3, \mp Q', \pm Q'')$.

Another example arises from setting $(P_1, P_2, P_3) = (T_3, Q, Q + T_3)$, which leads to the polynomial $q - 2n$. Then $n = 6N^2$, $Q = Q'$, and the resulting progression $(T_3, \pm Q', \mp Q'')$ is again trivial.

In a similar manner all of the other possibilities can be checked (Maple V was used for our symbolic computations), and no non-trivial arithmetic progressions are obtained. This completes the proof of Theorem 1.1 for $n \geqslant 72$ in the case that P_1, P_2, P_3 all belong to the identity component of E.

4.1.2. *Only P_2, P_3 Belong to the Identity Component of E.* In this case we have

$$-n \leqslant x_1 \leqslant 0 < n \leqslant x_2 < x_3.$$

We begin with some elementary estimates.

LEMMA 4.4. *With assumptions as above,*

$$2x_2 \leqslant x_3 < 4x_2 \qquad \text{and} \qquad x_3 > 2n.$$

Proof. Substituting $x_1 = 2x_2 - x_3$ into $-n \leqslant x_1 \leqslant 0$, we obtain

$$2x_2 \leqslant x_3 \leqslant 2x_2 + n.$$

Since $x_2 \geqslant n \geqslant 1$, this is stronger than the stated result. Finally, observe that

$$x_3 = 2x_2 - x_1 \geqslant 2n,$$

with equality if and only if $x_2 = n$ and $x_1 = 0$. Since we have ruled out the trivial solution $(x_1, x_2, x_3) = (0, n, 2n)$, we see that $x_3 > 2n$. ∎

Now use (13) and the inequality $0 < n/x_3 < 1/2$ from Lemma 4.4 to compute

$$\begin{aligned}\hat{h}(P_3) &\leqslant \frac{1}{4}\log(x_3^2+n^2)+\frac{1}{12}\log 2\\ &= \frac{1}{2}\log x_3+\frac{1}{4}\log\left(1+\left(\frac{n}{x_3}\right)^2\right)+\frac{1}{12}\log 2\\ &< \frac{1}{2}\log x_3+\frac{1}{4}\log\frac{5}{4}+\frac{1}{12}\log 2\\ &= \frac{1}{2}\log x_3+\frac{1}{4}\log 5-\frac{5}{12}\log 2.\end{aligned}$$

Combining this with (12) gives

$$-\tfrac{1}{2}\log n-\tfrac{1}{4}\log 2<\hat{h}(P_3)-\tfrac{1}{2}\log x_3<\tfrac{1}{4}\log 5-\tfrac{5}{12}\log 2.$$

From (12) and (13) we also have

$$-\tfrac{1}{2}\log n-\tfrac{1}{4}\log 2<\hat{h}(P_2)-\tfrac{1}{2}\log x_2<\tfrac{1}{3}\log 2.$$

Combining the above inequalities gives

$$\begin{aligned}-\tfrac{1}{2}\log n-\tfrac{7}{12}\log 2<\hat{h}(P_3)-\hat{h}(P_2)-\tfrac{1}{2}(\log x_3-\log x_2)\\ <\tfrac{1}{2}\log n+\tfrac{1}{4}\log 5-\tfrac{1}{6}\log 2.\end{aligned}$$

We combine this with the estimate $2 \leqslant x_3/x_2 < 4$ obtained in Lemma 4.4 to compute

$$-\tfrac{1}{2}\log n-\tfrac{1}{12}\log 2<\hat{h}(P_3)-\hat{h}(P_2)<\tfrac{1}{2}\log n+\tfrac{1}{4}\log 5+\tfrac{5}{6}\log 2.$$

In view of $\hat{h}(P_i)=m_i^2\hat{h}(Q)$ for $i=2, 3$ and the lower bound for $\hat{h}(Q)$ given by (11), we finally get a lower and an upper bound for $m_3^2-m_2^2$, expressed in terms of $\log n$. When $n \geqslant 72$, this yields $-3 \leqslant m_3^2-m_2^2 \leqslant 6$. Since we may assume $m_2 \geqslant 0$ and $m_3 > 0$, the only possibilities are $(m_2, m_3) = (2, 3), (0, 2), (0, 1), (2, 1), (1, 2)$.

On the other hand, in view of Lemma 4.2, we may assume $0 \leqslant m_1 \leqslant 2$. Thus

$$\begin{aligned}&P_1 = m_1 Q + T, \qquad T \in \{T_1, T_2\}, \quad m_1 \in \{0, 1, 2\};\\ &P_i = m_i Q + \varepsilon_i T_3, \qquad i = 2, 3, \quad \varepsilon_i \in \{0, 1\}, \quad (m_2, m_3) \text{ as above.}\end{aligned}$$

Then the condition

$$2x(m_2Q+\varepsilon_2T_3)=x(m_1Q+T)+x(m_3Q+\varepsilon_3T_3)$$

leads to polynomials with integral coefficients having n/q as a rational root, exactly as in Section 4.1.1. Going through the possibilities case-by-case, we find that the only rational numbers appearing as roots are -1, $1/2$, -3, 2, and 3. If -1 is a root, then $Q=T_1$, a contradiction, while $1/2$ and -3 being roots means that the x-coordinate of Q is $n/2$ or $-3n$, clearly impossible. The last two possibilities, namely 2 and 3, lead to trivial progressions, exactly as in Section 4.1.1. This completes the proof of Theorem 1.1 for $n\geqslant 72$ in the case that only P_2 and P_3 belong to the identity component of E.

We note that, for the symbolic computations needed in this case, use was made of three further formulas: If $P\in E$ and $x(P)=u$, then

$$x(P+T_2)=-\frac{n^2}{u},$$

$$x(P+T_1)=-\frac{n(u-n)}{u+n},$$

$$x(3P)=x\left(\frac{u^4+6n^2u^2-3n^4}{3u_4-6n^2u^2-n^4}\right)^2.$$

4.1.3. *P_1, P_2, P_3 Belong to the Non-identity Component of E.* In this case put

$$P_i=m_iQ+S_i \qquad \text{with} \quad s_i\in\{T_1,T_2\} \quad \text{and} \quad m_i\in\mathbf{Z} \quad (i=1,2,3).$$

Making the usual assumption that the m_i's are all positive, we see from Lemma 4.2 that it suffices to check all possible cases $(m_i,S_i)\in\{0,1,2\}\times\{T_1,T_2\}$. In each case, the condition

$$2x(m_2Q+S_2)=x(m_1Q+S_1)+x(m_3Q+S_3)$$

leads to the condition that n/q is a rational root of a polynomial equation with integer coefficients. A case-by-case analysis shows that the resulting polynomial either has no rational roots, or else it has a rational root in the set $\{1,-1,2,3,-3,1/3\}$. Then, just as in Subsections 4.1.1 and 4.1.2, we are led either to a contradiction or to a trivial progression (P_1,P_2,P_3). This completes the proof of Theorem 1.1 for $n\geqslant 72$ in the case that P_1, P_2, P_3 all belong to the non-identity component of E, and thus Theorem 1.1 is proved for all $n\geqslant 72$.

4.2. *The Case* $1 \leqslant n < 72$

For the finitely many squarefree values of n in the range $1 \leqslant n < 72$, we find explicitly all integer points on the curves (4), and in consequence all arithmetic progressions on (4) in the range $1 \leqslant n < 72$ are discovered to be trivial. It is only necessary to treat those values of n for which the rank of (4) is positive, and such n are easily found using Cremona's "mrank" program. For many of these n, all integer points on (4) may be determined by a straightforward application of theorems of Bennett and Walsh [BeWa] and of Cohn [Co]. We give one typical illustration, but omit full details.

EXAMPLE 4.5. Suppose p is a prime, $p \equiv 3 \bmod 8$.
Then all integer solutions of (4) for $n = 2p$ are straightforwardly found.

We first check directly all integer values in the interval $-n < x < 0$. Then for positive values of x, we consider the following cases:

(1) $x = a^2$, $x^2 - 4p^2 = b^2$, then $a^4 - b^2 = 4p^2$, and a trivial computation suffices.

(2) $x = 2pa^2$, $x^2 - 4p^2 = 8p^3b^2$, then $a^4 - 1 = 2pb^2$ and Cohn's Theorem [Co] applies to show that there is at most one non-trivial solution in integers, which is effectively (and easily) computable.

(3) $x = 2a^2$, $x^2 - 4p^2 = 8b^2$, then $a^4 - p^2 = 2b^2$, and since $(2/p) = -1$, it follows that $a \equiv b \equiv 0 \bmod p$. Now $p^2(a/p)^4 - 1 = 2(b/p)^2$ and the theorem of Bennett and Walsh [BeWa] applies to show that again there is at most one effectively computable solution in integers.

(4) $x = pa^2$, $x^2 - 4p^2 = p^3b^2$, then $a^4 - 4 = pb^2$. If a is odd, then b is odd and $1 - 4 \equiv 3 \bmod 8$, a contradiction. So a is even, and thus b is even, and $4(a/2)^4 - 1 = p(b/2)^2$, and the Bennett–Walsh Theorem applies again.

The values of n in the range that resist this elementary analysis are $n = 14$, 21, 30, 34, 46, 62, 69, 70, where the corresponding curves are of rank 1, except in the instance $n = 34$, where the rank is 2 (these ranks are known unconditionally using Connell's Apecs program under Maple V, which also provided respective bases for the Mordell–Weil groups over $\mathbf{Q}$).

To find all the integer points on these eight remaining curves, we applied the *Elliptic Logarithm Method*, explained in detail in Stroeker and Tzanakis [StTz] and also in Gebell *et al.* [GPZ1]. An analogous, but far more difficult, task was accomplished in Stroeker [Str], and also in [BST], see also Gebel *et al.* [GPZ2] for the simultaneous treatment of a large number of elliptic curves. The application of the method here proved routine, with no unexpected computational difficulties, and so details are suppressed. For

TABLE II

Non-trivial Integer Points $(x, \pm y)$ on (4)

n	$(x, \pm y)$ on $y^2 = x^3 - n^2x$
5	$(-4, 6), (45, 300)$
6	$(-3, 9), (-2, 8), (12, 36), (18, 72), (294, 5040)$
7	$(25, 120)$
14	$(18, 48), (112, 1176)$
15	$(-9, 36), (25, 100), (60, 450)$
21	$(-3, 6), (28, 98), (147, 1764)$
22	$(2178, 101640)$
29	$(284229, 151531380)$
30	$(-20, 100), (-6, 72), (45, 225), (150, 1800)$
34	$(-16, 120), (-2, 48), (162, 2016), (578, 13872)$
39	$(-36, 90), (975, 30420)$
41	$(-9, 120), (841, 24360)$
46	$(242, 3696)$
65	$(-25, 300), (-16, 252), (169, 2028)$
69	$(1083, 35568)$
70	$(-20, 30), (126, 1176), (245, 3675)$

completeness, in Table II we list all the integer points on the curves (4) in the range $1 \leqslant n < 72$, excluding the torsion points $(\pm n, 0), (0, 0)$.

Putting together the results of Subsections 4.1 and 4.2 completes the proof of Theorem 1.1 for all values of n. ∎

5. ARITHMETIC PROGRESSIONS CONTAINING A TORSION POINT

In this section we prove Theorems 1.2 and 1.3 which describe arithmetic progressions in which one of the points is a torsion point.

Proof of Theorem 1.2. Suppose (P_1, P_2, P_3) is an arithmetic progression on (4) with precisely one of the P_i being a torsion point, equal to T_2. The three points have x-coordinates equal to one of the following, for some positive rational a: $\{-a, 0, a\}$, $\{0, a, 2a\}$, $\{-2a, -a, 0\}$. The former case clearly implies $a = n$, so that the progression contains more than one torsion point. The latter two cases imply

$$\pm a(a^2 - n^2) = \square, \qquad \pm 2a(4a - n^2) = \square,$$

with respective signs, which implies that

$$A(A-2)(A-8) = \square,$$

where $A = 8a^2/n^2$. The elliptic curve $y^2 = x(x-2)(x-8)$ has rational rank 0 and torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and hence $A = 2$ or 8 with $a = n/2$ or n; and the progressions that result either do not correspond to three points on E, or else contain more than one torsion point. This completes the proof of Theorem 1.2. ▮

Proof of Theorem 1.3. Assume that the first case occurs. Then $P_1 = (-n, 0)$ and the three points have x-coordinates equal to $\{-n, a, 2a+n\}$ for some rational $a > -n$, $a \notin \{-n/2, 0n\}$. It follows that

$$a(a^2 - n^2) = \square, \qquad (2a+n)(4a^2 + 4an) = \square; \tag{33}$$

so multiplying these equalities, we get

$$(a-n)(2a+n) = \square.$$

This quadratic is parametrized by $[a : n] = [1 + \lambda^2 : 1 - 2\lambda^2]$, so

$$a = \mu(r^2 + s^2), \qquad n = \mu(r^2 - 2s^2),$$

where without loss of generality r, $s \in \mathbf{Z}$, $(r, s) = 1$, and $\mu \in \mathbf{Q}$, and since $a \notin \{-n/2, n\}$, both r and s are non-zero. Then from (33),

$$3\mu(r^2 + s^2)(2r^2 - s^2) = \square$$

giving

$$\mu = 3(r^2 + s^2)(2rp2 - s^2)\, t^2$$

for some $t \in \mathbf{Q}$. Finally,

$$a = 3(r^2 + s^2)^2\,(2r^2 - s^2)\, t^2, \qquad n = 3(r^2 + s^2)(r^2 - 2s^2)(2r^2 - s^2)\, t^2,$$

and the progression is as given at (5)–(7). The conditions $a > -n$ and $a \notin \{-n/2, 0, n\}$ are satisfied for the above values of a and n as is easily checked.

In the second case, suppose that T_3 is the only torsion point of an arithmetic progression of three points P_1, P_2, P_3. Then T_3 coincides with either P_1 or with P_2. In the first instance the analysis is, *mutatis mutandis*, the same as in the first case, on replacing n by $-n$, because the x-coordinates of the three points are $\{n, 0, 2a-n\}$ for some rational $a > n$. In the second instance the x-coordinates are $\{n-a, n, n+a\}$ for some rational a satisfying $n < a < 2n$. Then $a(n-a)(a-2n) = \square$ and $a(n+a)(a+2n) = \square$, from which $a^2(n^2 - 4n^2) = \square$, so that the elliptic curve $A(A+1)(A+4) = \square$ has a rational point with $A = -a^2/n^2$. The rank of this elliptic curve is zero

and the A-coordinates of its torsion points are $-4, -2, -1, 0, 2$. We conclude therefore that the only possibilities for arithmetic progressions are given by $a = \pm 2n, \pm n, 0$, all of which, however, must be rejected in view of the condition $n < a < 2n$. This completes the proof of Theorem 1.3. ∎

We remark that the curve E in the instance of Theorem 1.3 takes the form

$$E\colon\ y^2 = x(x^2 - 9(r^2+s^2)^2\,(r^2-2s^2)^2\,(2r^2-s^2)^2\,t^4),$$

which is isomorphic to

$$E\colon\ Y^2 = X(X^2 - 9(\lambda^2+1)^2\,(\lambda^2-2)^2\,(2\lambda^2-1)^2),$$

and the latter curve has rank at least 2 over $\mathbf{Q}(\lambda)$, with independent points

$$Q_0 = [\,3(\lambda^2+1)^2\,(2\lambda^2-1),\ 9(2\lambda^2-1)^2\,(\lambda^2+1)^2\,],$$
$$Q_1 = [\,-3(\lambda^2+1)^2\,(\lambda^2-2),\ 9\lambda(\lambda^2-2)^2\,(\lambda^2+1)^2\,].$$

6. RANK ONE ARITHMETIC PROGRESSIONS ON TWISTS

In this section we give the proof of Theorem 1.4. We use various height estimates. First, since there is an isomorphism (over $\bar{\mathbf{Q}}$) from E_A to E given by $(x, y) \mapsto (x/A,\ y/A^{3/2})$ and since the canonical height is invariant under $\bar{\mathbf{Q}}$-isomorphism, we have

$$\hat{h}(P) = \tfrac{1}{2}h(x(P)/A) + O(1) \qquad \text{for all} \quad P \in E_A(\mathbf{Q}). \tag{34}$$

(Here and in what follows, all constants may depend on the initial curve E, but they are independent of the twisting value A.)

Next, use the fact that E_A has Type I_0^* reduction at almost every prime dividing A. (Note that this is where we use the fact that A is square-free.) More precisely, this is true for all primes not dividing $6\Delta(E)$. Since the group of components of a fiber of Type I_0^* has exponent 2, we find that

$$\hat{h}(2P) \geqslant \tfrac{1}{12}\log(A^6) + O(1) \qquad \text{for all} \quad P \in E_A(\mathbf{Q}) \quad \text{with} \ \ 2P \neq O.$$

Hence

$$\hat{h}(P) \geqslant \tfrac{1}{8}\log|A| + O(1) \qquad \text{for all} \quad P \in E_A(\mathbf{Q}) \quad \text{with} \ \ 2P \neq O. \tag{35}$$

Now suppose that $\Gamma \subset E_A(\mathbf{Q})$ is a free rank 1 subgroup and that $P_1, P_2, P_3 \in \Gamma$ is an integral arithmetic progression, say with $x_1 < x_2 < x_3$, where

for notational convenience we write $x_i = x(P_i)$. Observe that for any integer x, the (multiplicative) height $H(x/A)$ trivially satisfies

$$|x/A| \leqslant H(x/A) \leqslant \max\{|x|, |A|\},$$

so combining this with the height estimate (34) given above yields.

$$|x(P)/A| \ll \hat{H}(P)^2 \ll \max\{|x(P)|, |A|\}.$$

(Here we are writing $\hat{H}(P) = \exp(\hat{h}(P))$.)

Let Q be a generator for Γ, and write $P_i = n_i Q$ for $i = 1, 2, 3$. Then

$$\begin{aligned}
\hat{H}(Q)^{2n_3^2} &= \hat{H}(P_3)^2 \\
&\ll \max\{|x_3|, |A|\} \qquad \text{from above} \\
&= \max\{|2x_2 - x_1|, |A|\} \qquad \text{since} \quad x_2 - x_1 = x_3 - x_2 \\
&\leqslant \max\{2|x_2| + |x_1|, |A|\} \\
&\ll \max\{2|A|\,\hat{H}(P_2)^2 + |A|\,\hat{H}(P_1)^2, |A|\} \qquad \text{from above} \\
&= |A| \max\{2\hat{H}(Q)^{2n_2^2} + \hat{H}(Q)^{2n_1^2}, 1\}.
\end{aligned}$$

Since $1 \leqslant n_1 < n_2 < n_3$ and $\hat{H}(Q) > 1$, adjusting the constants gives

$$\hat{H}(Q)^{2n_3^2} \ll |A|\,\hat{H}(Q)^{2n_2^2}.$$

Now use the height lower bound $\hat{H}(Q) \ll |A|^{1/8}$ described above (35) to get

$$|A|^{(n_3^2 - n_2^2 - 4)/4} \ll 1.$$

Finally observe that since $n_3 > n_2 > n_1 \geqslant 1$, then $n_3^2 - n_2^2 \geqslant 3^2 - 2^2 = 5$, so that $|A|^{1/4} \ll 1$. In other words, the existence of an integral arithmetic progression implies that $|A|$ is bounded by a constant depending only on the original curve E. This completes the proof of Theorem 1.4.

REFERENCES

[BeWa] M. A. Bennett and P. G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, *Amer. Math. Soc.*, in press.

[Br] A. Bremner, On squares of squares, preprint.

[BrCa] A. Bremner and J. W. S. Cassels, On the equation $Y^2 = X(X^2 + p)$, *Math. Comp.* **42** (1982), 257–264.

[BST] A. Bremner, R. Stroeker, and N. Tzanakis, On sums of consecutive squares, *J. Number Theory* **62** (1997), 39–70.

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

[Co] J. H. E. Cohn, The Diophantine equation $x^4 - Dy^2 = 1$, II, *Acta Arith.* **78** (1997), 403–409.

[De] V. A. Dem'janenko, An estimate of the remainder term in Tate's formula, *Mat. Zametki* **3** (1968) 271–278. [In Russian]

[GPZ1] J. Gebel, A. Pethö, and H. G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.* **68** (1994), 171–192.

[GPZ2] J. Gebel, A. Pethö, and H. G. Zimmer, On Mordell's equation, *Compositio Math.* **110** (1998), 335–367.

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

[La] S. Lang, "Elliptic Curves: Diophantine Analysis," Springer-Verlag, Berlin/New York, 1978.

[Ro] J. P. Robertson, Magic squares of squares, *Math. Mag.* **69**, No. 4 (1996), 289–293.

[Si1] J. H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Math., Vol. 106, Springer-Verlag, Berlin/New York, 1986.

[Si2] J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," Graduate Texts in Math., Vol. 151, Springer-Verlag, Berlin/New York, 1994.

[Si3] J. H. Silverman, "The Néron–Tate Height on Elliptic Curves," Ph.D. thesis, Harvard, 1981.

[Si4] J. H. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48** (1981), 633–648.

[Si5] J. H. Silverman, Lower bounds for height functions, *Duke Math. J.* **51** (1984), 395–403.

[Si6] J. H. Silverman, Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339–358.

[Si7] J. H. Silverman, The difference between the Weil and the canonical height on elliptic curves, *Math. Comp.* **55** (1990), 723–743.

[Sik] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), 1501–1538.

[Str] R. Stroeker, On the sum of consecutive cubes being a perfect square, *Compositio Math.* **97** (1995), 295–307.

[StTz] R. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* **67**, No. 2 (1994), 177–196.

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, *in* "Modular Functions of One Variable IV, Antwerp, 1972" (B. J. Birch and W. Kuyk, Eds.), Lecture Notes in Math., Vol. 272, Springer-Verlag, Berlin, 1975.

[WaTa] H. Wada and M. Taira, Computations of the rank of the elliptic curve $y^2 = x^3 - n^2x$, *Proc. Japan Acad. Ser. A* **70** (1994), 154–157.

[Zi] H. Zimmer, On the difference of the Weil height and the Néron–Tate height, *Math. Z.* **174** (1976), 35–51.