BULL. AUSTRAL. MATH. SOC. 11G05, 11G50, 11G07, 11G35
VOL. 72 (2005) [177–186]

HEIGHT ESTIMATES ON CUBIC TWISTS OF THE FERMAT ELLIPTIC CURVE

TOMASZ JEDRZEJAK

We give bounds for the canonical height of rational and integral points on cubic twists of the Fermat elliptic curve. As a corollary we prove that there is no integral arithmetic progression on certain curves in this family.

1. INTRODUCTION

A classical question in number theory is to describe the numbers m that can be written as the sum of two rational cubes. This leads to the family of elliptic curves

$$E_m : x^3 + y^3 = m, \tag{1.1}$$

which are cubic twists of the Fermat curve $x^3 + y^3 = 1$. Clearly E_{m_1} and E_{m_2} are isomorphic (over $\mathbb{Q}$) if m_1/m_2 is a cube, so we can and will assume that m is cubefree positive integer. The substitutions

$$X = \frac{12m}{y+x}, \qquad Y = 36m\frac{y-x}{y+x}$$

lead to a Weierstrass equation

$$E'_m : Y^2 = X^3 - 432m^2. \tag{1.2}$$

It is well known that $\left|E_m(\mathbb{Q})\right| \leqslant 3$, for $m = 1, 2$ and $E_m(\mathbb{Q})_{\text{tors}} = \{O\}$, for $m \geqslant 3$.

In this paper we consider the problem of finding three integral points P_0, P_1, P_2 on the global minimal model of E'_m, whose x-coordinates $x_i = x(P_i)$ form an increasing arithmetic progression (we say that P_0, P_1, P_2 form an integral arithmetic progression). This problem was investigated in [2] for congruent elliptic curves.

Note that the integrality of x-coordinates may depend on the choice of a particular equation. It does not depend, however, on the choice of a global minimal equation. Below we shall use $E_m^{\min}$, the global minimal Weierstrass model described in Lemma 1.

Our principal result is the following theorem

THEOREM 1. *Let $m \equiv 0, \pm 3, \pm 4 \pmod 9$; assume that any prime factor $p > 3$ of m is of the form $p \equiv 5 \pmod 6$. Let $A \subset E_m^{\min}(\mathbb{Q})$ be a subgroup of rank 1. Then A contains no integral arithmetic progressions.*

Unfortunately our method does not work for other m's (see discussion in Section 4).

Received 10th January, 2005

2. Height estimates

Lang [5] has formulated the conjecture which says that the canonical height of a non-torsion point P on an elliptic curve E should satisfy $\widehat{h}(P) >> \log|\Delta_E|$. Put

$$\beta_E := \frac{\log|\Delta_E|}{\log N_E}.$$

Hindry and Silverman [4] proved the explicit estimates

$$\widehat{h}(P) \geqslant c(\beta_E)\log|\Delta_E|.$$

where

$$c(\beta_E) = (20\beta_E)^{-8}10^{-1.1-4\beta_E}.$$

Hence Lang's conjecture holds true for elliptic curves with universally bounded β_E.

One immediately checks that $\beta_{E_m} \leqslant 2.91$, hence

$$\widehat{h}_{E_m}(P) \geqslant 1.38 \times 10^{-27} \times \log|\Delta_m|.$$

Below we prove much sharper inequalities (Corollary to Proposition 1).

In the proof we shall use the global minimal Weierstrass model (note, however, that our height estimates do not depend of the choice of Weierstrass model).

Lemma 1. *The global minimal Weierstrass model $E_m^{\min}$ for $E'_m : Y^2 = X^3 - 432m^2$ can be described as follows:*

(i) $y^2 = x^3 - (27/4)m^2$ *if* $2 \mid m$ *and* $9 \nmid m$,

(ii) $y^2 + y = x^3 - (27m^2+1)/4$ *if* $2 \nmid m$ *and* $9 \nmid m$,

(iii) $y^2 = x^3 - (3m'^2/4)$ *if* $2 \mid m$ *and* $9 \mid m$,

(iv) $y^2 + y = x^3 - (3m'^2+1)/4$ *if* $2 \nmid m$ *and* $9 \mid m$,

where $m' = m/9$.

Proof: The substitutions

$$X = u^2x + r, \qquad Y = u^3y + su^2x + t,$$

with $[u,r,s,t] = [2,0,0,0]$, $[2,0,0,4]$, $[6,0,0,0]$, $[6,0,0,108]$, respectively, lead to the equations in (i)-(iv). Let Δ_m denote the discriminant. In cases (i) and (ii) we have $\Delta_m = -3^9m^4$, so for any prime $p \neq 3$ the discriminant is 12th powerfree. The minimality at $p = 3$ follows from Tate's algorithm (see [7] or [6]). In cases (iii) and (iv) $\Delta_m = -3^5m'^4$ is 12th powerfree, hence the model is global minimal. ∎

Definition: We say that m satisfies condition (*), if every prime factor of m greather than 3 is congruent to 5 modulo 6.

https://doi.org/10.1017/S0004972700034997 Published online by Cambridge University Press

Proposition 1. *For $P \in E_m(\mathbb{Q}) \setminus \{O\}$ ($m > 2$ cubefree) we have*

$$(2.1)\quad \widehat{h}_{E_m}(P) \geqslant \begin{cases} \frac{1}{3}\log\frac{m}{2} + \frac{3}{4}\log 3 & \text{if } m \equiv \pm 3, \pm 4 \pmod 9 \text{ and } m \text{ satisfies } (*) \\ \frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3 & \text{if } m \equiv \pm 2 \pmod 9 \text{ and } m \text{ satisfies } (*) \\ \frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3 & \text{if } m \equiv \pm 1, \pm 3, \pm 4 \pmod 9 \\ \frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3 & \text{if } m \equiv 0 \pmod 9 \text{ and } m \text{ satisfies } (*), \end{cases}$$

and in general

$$(2.2)\quad \widehat{h}_{E_m}(P) \geqslant \begin{cases} \frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3 & \text{if } 9 \nmid m \\ \frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3 & \text{if } m \equiv 0 \pmod 9). \end{cases}$$

Corollary 1. *For $P \in E_m(\mathbb{Q}) \setminus \{O\}$ ($m > 2$ cubefree), we have*

$$\widehat{h}_{E_m}(P) \geqslant \left(\frac{1}{432} - \frac{\log 2}{108 \log 3^{13}}\right) \log \left|\Delta_m^{\min}\right|.$$

Proof: [Proof of Proposition 1] The proof involves an analysis of local height functions $\widehat{h}_p : E(\mathbb{Q}_p) \to \mathbb{R}$. Definition and basic properties of local heights may be found in [**6**]. We shall consider two cases.

Archimedean case. We shall estimate the archimedean contribution $\widehat{h}_\infty$ to the canonical height by using Tate's series. Assume first $9 \nmid m$. The group $E_m^{\min}(\mathbb{R})$ is connected, and if $P = (x, y) \in E_m^{\min}(\mathbb{R})$, then $x \geqslant 3\sqrt[3]{m^2/4}$. If we take

$$t = 1/x, \qquad w = 4t - 27m^2t^4, \qquad z = 1 + 54m^2t^3,$$

then the archimedean local height of P is given by the series

$$\widehat{h}_\infty(P) = \frac{1}{2}\log\left|x(P)\right| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log\left|z(2^kP)\right| - \frac{1}{12}\log\left|\Delta_m^{\min}\right|.$$

This series converges because no point on $E_m^{\min}(\mathbb{R})$ has x-coordinate 0. Now

$$0 \leqslant t \leqslant \frac{1}{3}\sqrt[3]{\frac{4}{m^2}}$$

implies $0 \leqslant \log z \leqslant \log 9$. Hence

$$\widehat{h}_\infty(P) = \frac{1}{2}\log\left|x(P)\right| + \frac{1}{8}\log\left|z(P)\right| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}c - \frac{1}{12}\log\left|\Delta_m^{\min}\right|,$$

where $0 \leqslant c \leqslant \log 9$. So using the definition of z, we obtain

$$(2.3)\qquad 0 \leqslant \widehat{h}_\infty(P) - \left(\frac{1}{8}\log\left|x(P)^4 + 54m^2x(P)\right| - \frac{1}{12}\log\left|\Delta_m^{\min}\right|\right) \leqslant \frac{1}{12}\log 3.$$

When $9 \mid m$ we take

$$t = 1/x, \qquad w = 4t - 3m'^2 t^4, \qquad z = 1 + 6m'^2 t^3,$$

where $m' = m/9$. Arguing as above, we obtain:

$$(2.4) \qquad 0 \leqslant \widehat{h}_\infty(P) - \Big(\frac{1}{8}\log\big|x(P)^4 + 6m'^2 x(P)\big| - \frac{1}{12}\log|\Delta_m^{\min}|\Big) \leqslant \frac{1}{12}\log 3.$$

NON-ARCHIMEDEAN CASE. If P belongs to the identity component $E_m^{\min}(\mathbb{Q}_p)^0$ of the Néron model (equivalently, if reduction of P modulo p is nonsingular), then the local height of P is given by formula

$$(2.5) \qquad \widehat{h}_p(P) = \frac{1}{2}\max\Big(0, -v_p\big(x(P)\big)\Big) + \frac{1}{12}v_p(\Delta_m^{\min}),$$

where $v_p(x) = \operatorname{ord}_p(x)\log p$. $E_m^{\min}(\mathbb{Q}_p)^0$ is a subgroup of finite index in $E_m^{\min}(\mathbb{Q}_p)$ and by using Tate's algorithm [**7**] we can find the order of the quotient group $E_m^{\min}(\mathbb{Q}_p)/E_m^{\min}(\mathbb{Q}_p)^0$ (that is, the Tamagawa number c_p). Of course, $E_m^{\min}(\mathbb{Q}_p) = E_m^{\min}(\mathbb{Q}_p)^0$, when $E_m^{\min}$ has good reduction at p, i e. if $p \neq 3$ and $p \nmid m$. $E_m^{\min}$ has bad reduction at 2 (for an even m), but $E_m^{\min}(\mathbb{Q}_2)^0 = E_m^{\min}(\mathbb{Q}_2)$ (the Kodaira symbols are IV^* or IV according as $4 \mid m$ or $2 \parallel m$). The case $p = 3$ is more complicated. If $m \equiv 0, \pm 3, \pm 4 \pmod 9$, then reduction types at 3 are II, II^*, IV^* respectively and Tamagawa number $c_3 = 1$. For $m \equiv \pm 1 \pmod 9$ we have type IV^*, but $c_3 = 3$, so $3E_m^{\min}(\mathbb{Q}_3) \subset E_m^{\min}(\mathbb{Q}_3)^0$. Finally, for $m \equiv \pm \pmod 9$ the reduction type is III^* and $E_m^{\min}(\mathbb{Q}_3)/E_m^{\min}(\mathbb{Q}_3)^0 \cong \mathbb{Z}/2\mathbb{Z}$. In the case $p \mid m$, $p > 3$ we have two possibilities. If $p \equiv 5 \pmod 6$ (equivalently $(-3/p) = -1$), then the Kodaira symbol is IV or IV^* according as $p^2 \nmid m$ or $p^2 \mid m$, and $E_m^{\min}(\mathbb{Q}_p)^0 = E_m^{\min}(\mathbb{Q}_p)$. If $p \equiv 1 \pmod 6$ (that is, $(-3/p) = 1$), then the Kodaira symbols are the same, but $c_p = 3$. Another way to decide when $E_m^{\min}(\mathbb{Q}_p)^0 = E_m^{\min}(\mathbb{Q}_p)$ is based on [**6**, Exercise 6.7a)], which says that $P = (x, y) \in E(\mathbb{Q}_p)^0$ if and only if

$$v_p(3x^2 + 2a_2x + a_4 - a_1y) \leqslant 0 \quad \text{or} \quad v_p(2y + a_1x + a_4x + a_6) \leqslant 0,$$

where E is given by minimal at p Weierstrass equation. We have checked our results using this method for primes p for which $c_p = 1$.

Let us summarise the above considerations:

(a) if $m \equiv 0, \pm 3, \pm 4 \pmod 9$ satisfies $(*)$, then $E_m^{\min}(\mathbb{Q}_p) = E_m^{\min}(\mathbb{Q}_p)^0$ for all p,

(b) if $m \equiv 0, \pm 2, \pm 3, \pm 4 \pmod 9$ satisfies $(*)$, then $2E_m^{\min}(\mathbb{Q}_p) \subset E_m^{\min}(\mathbb{Q}_p)^0$ for all p,

(c) if $m \equiv 0, \pm 1, \pm 3, \pm 4 \pmod 9$, then $3E_m^{\min}(\mathbb{Q}_p) \subset E_m^{\min}(\mathbb{Q}_p)^0$ for all p,

(d) for all m and any prime p we have $6E_m^{\min}(\mathbb{Q}_p) \subset E_m^{\min}(\mathbb{Q}_p)^0$.

The next step is to estimate the canonical height. Let $Q=(x,y)\in E_m^{\min}(\mathbb{Q})$ be any point satisfying $Q\in E_m^{\min}(\mathbb{Q}_p)^0$ for every prime p. We may write $x=a/d^2$ as a fraction in lowest terms. Hence

$$\widehat{h}_p(Q)=\frac{1}{2}\max\left(0,-v_p\left(\frac{a}{d^2}\right)\right)+\frac{1}{12}v_p(\Delta_m^{\min}),$$

and after summing over all finite primes we obtain the formula

$$\sum_{p\neq\infty}\widehat{h}_p(Q)=\log|d|+\frac{1}{12}\log|\Delta_m^{\min}|.$$

Adding this to the lower bound for $\widehat{h}_\infty(Q)$ we get

$$\widehat{h}_{E_m}(Q)\geqslant\begin{cases}\frac{1}{8}\log\left|\frac{a^4}{d^8}+54m^2\frac{a}{d^2}\right|+\log|d| & \text{if } 9\nmid m,\\ \frac{1}{8}\log\left|\frac{a^4}{d^8}+6m'^2\frac{a}{d^2}\right|+\log|d| & \text{if } 9\mid m.\end{cases}$$

Next, using the fact that $(a/d^2)\geqslant 3\sqrt[3]{m^2/4}$ (respectively $a/d^2\geqslant\sqrt[3]{3m'^2/4}$) we obtain

$$\widehat{h}_{E_m}(Q)\geqslant\begin{cases}\frac{1}{3}\log\frac{m}{2}+\frac{3}{4}\log 3 & \text{if } 9\nmid m,\\ \frac{1}{3}\log\frac{m}{2}-\frac{1}{4}\log 3 & \text{if } 9\mid m.\end{cases}$$

Let $P\in E_m^{\min}(\mathbb{Q})$ be an arbitrary point. Then, for some $k\in\{1,2,3,6\}$ (which depends on m) the reduction of kP is nonsingular modulo every prime p, so we can use the above estimations for $Q=kP$. Now $\widehat{h}_{E_m}(kP)=k^2\widehat{h}_{E_m}(P)$, and the assertions follows. ∎

The next proposition gives an estimate of the canonical height of non-torsion point P in terms of the coordinates P.

NOTATION. For the remaining part of this paper we set $M=m/9$ or m according as 9 divides m or not.

PROPOSITION 2. *Let $m>2$ be cubefree, and let $P\in E_m^{\min}(\mathbb{Q})\setminus\{O\}$. Let $x(P)=a/d^2$, where $(a,d)=1$. Then*

$$\frac{2}{3}\log M+\frac{3}{2}\log 3\leqslant\widehat{h}_{E_m}(P)-\frac{1}{8}\log\left|a^4+54\frac{M^3ad^6}{m}\right|\leqslant\frac{1}{12}\log 3.$$

PROOF: As previously we shall the use local height function. But in this cases we must evaluate the local p-adic height at points which after the reduction modulo p are singular. To do this, we shall use [**6**, Excercises 6.7a) and 6.8] (note that E_m has good or additive reduction). Of course, it is enough to consider the cases $p=3$ (with $m\equiv\pm1,\pm2 \pmod 9$), and p a prime factor of m which is congruent to 1 modulo 6 (in remaining cases we can use the formula (2.5))

https://doi.org/10.1017/S0004972700034997 Published online by Cambridge University Press

Let $P \in E_m^{\min}(\mathbb{Q}) \setminus \{O\}$ and let $x(P) = a/d^2$, with $(a,d) = 1$. We obtain for $P \notin E_m^{\min}(\mathbb{Q}_3)^0$:

$$\widehat{h}_3(P) = \begin{cases} -\frac{2}{3}\log 3, & \text{if } m \equiv \pm 1 \pmod 9 \\ -\frac{3}{4}\log 3, & \text{if } m \equiv \pm 2 \pmod 9. \end{cases}$$

Note, that for those points $v_3(d) = 0$. For m not divisible by 3, we have

$$\frac{1}{12} v_3(\Delta_m^{\min}) = (3/4)\log 3,$$

so after some calculation we get

$$\widehat{h}_3(P) = v_3(d) + \frac{1}{12}v_3(\Delta_m^{\min}) - \begin{cases} 0, & \text{if } P \in E_m^{\min}(\mathbb{Q}_3)^0, \\ \frac{17}{12}\log 3, & \text{if } P \notin E_m^{\min}(\mathbb{Q}_3)^0 \text{ and } m \equiv \pm 1 \pmod 9 \\ \frac{3}{2}\log 3, & \text{if } P \notin E_m^{\min}(\mathbb{Q}_3)^0 \text{ and } m \equiv \pm 2 \pmod 9. \end{cases}$$

Hence

$$-\frac{3}{2}\log 3 \leqslant \widehat{h}_3(P) - v_3(d) - \frac{1}{12}v_3(\Delta_m^{\min}) \leqslant 0, \tag{2.6}$$

for all m and any $P \in E_m^{\min}(\mathbb{Q}) \setminus \{O\}$.

Next, assume that $P \notin E_m^{\min}(\mathbb{Q}_p)^0$, where $p > 3$ and $p \mid m$. We obtain

$$\widehat{h}_p(P) = \begin{cases} -\frac{1}{3}\log p, & \text{if } p \parallel m \\ -\frac{2}{3}\log p, & \text{if } p^2 \mid m \end{cases} = -\frac{1}{3}v_p(m).$$

As before we can write

$$\widehat{h}_p(P) = v_p(d) + \frac{1}{12}v_p(\Delta_m^{\min}) - \begin{cases} 0, & \text{if } P \in E_m^{\min}(\mathbb{Q}_p)^0, \\ \frac{2}{3}v_p(m), & \text{if } P \notin E_m^{\min}(\mathbb{Q}_3)^0. \end{cases}$$

Of course, $E_m^{\min}(\mathbb{Q}_2)^0 = E_m^{\min}(\mathbb{Q}_2)$. Hence the above formula is true for every prime $p \neq 3$, and we obtain

$$-\frac{2}{3}v_p(m) \leqslant \widehat{h}_p(P) - v_p(d) - \frac{1}{12}v_p(\Delta_m^{\min}) \leqslant 0. \tag{2.7}$$

Now, adding the estimates (2.4), (2.6), (2.7) over $2 \leqslant p \leqslant \infty$ we obtain the bounds (i) and (ii). □

Corollary 2. *Let P, as in Proposition 2, be an integral point (that is, $x(P) = a$). Then*

$$\widehat{h}_{E_m}(P) > \frac{1}{2}\log a - \frac{2}{3}\log M - \frac{3}{2}\log 3 \tag{2.8}$$

and

$$\widehat{h}_{E_m}(P) \leqslant \frac{1}{2}\log a + \frac{1}{3}\log 3. \tag{2.9}$$

https://doi.org/10.1017/S0004972700034997 Published online by Cambridge University Press

PROOF: The first estimation is a straightforward application of the lower bound for $\widehat{h}_{E_m}(P)$ in Proposition 2. Since $a \geqslant \sqrt[3]{(27m^2)/4}$ if $9 \nmid m$ and $a \geqslant \sqrt[3]{(3m'^2)/4}$ if $9 \mid m$, the second inequality follows immediately from the upper bound of the canonical height in the Proposition 2. ∎

3. INTEGRAL ARITHMETIC PROGRESSION ON $E_m^{\min}$

In this section we shall prove the main theorem. We start with estimates for the difference between heights of two points satisfying certain relations.

LEMMA 2. *Let P_1, P_2 be integral points on $E_m^{\min}(\mathbb{Q})$. Assume that $x(P_1) < x(P_2) < 2x(P_1)$. Then*

$$(3.1)\qquad -\frac{2}{3}\log M - \frac{11}{6}\log 3 < \widehat{h}_{E_m}(P_2) - \widehat{h}_{E_m}(P_1) < \frac{2}{3}\log M + \frac{11}{6}\log 3 + \frac{1}{2}\log 2.$$

PROOF: We consider only the case $M = m$ (the second is similar). Write $x_i = x(P_i)$, $i = 1, 2$. By (2.8) and the fact that $0 < x_1 < x_2$, we have

$$-\frac{2}{3}\log m - \frac{3}{2}\log 3 < \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log x_2 < \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log x_1.$$

On other hand, by (2.9) and $2x_1 > x_2 > 0$,

$$\begin{aligned}\frac{1}{3}\log 3 \geqslant \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log x_2 &> \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log 2x_1\\ &= \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log x_1 - \frac{1}{2}\log 2,\end{aligned}$$

and hence

$$(3.2)\qquad -\frac{2}{3}\log m - \frac{3}{2}\log 3 < \widehat{h}_{E_m}(P_2) - \frac{1}{2}\log x_1 < \frac{1}{3}\log 3 + \frac{1}{2}\log 2.$$

Now using (2.8), (2.9) for P_1, together with (3.2) we obtain the required inequality. ∎

COROLLARY 3. *Let $Q \in E_m^{\min}(\mathbb{Q})$ be a point of infinite order (notice that then $|E_m^{\min}(\mathbb{Q})_{\text{tors}}| = 1$), and let P_1, P_2 be integral points belonging to the group $\langle Q\rangle$ generated by Q. Assume that $x(P_1) < x(P_2) < 2x(P_1)$, and write $P_i = n_iQ$, $i = 1, 2$. Then*

$$(3.3)\qquad \frac{-2\log M - \frac{11}{2}\log 3}{A\log m - A\log 2 + B\log 3} < n_2^2 - n_1^2 < \frac{2\log M + (11/2)\log 3 + (3/2)\log 2}{A\log m - A\log 2 + B\log 3},$$

where

$A = 1, B = 9/4$	*if* $m \equiv \pm 3, \pm 4 \pmod 9$ *satisfies* $(*)$	*(case 1)*
$A = 1/4,\ B = 9/16$	*if* $m \equiv \pm 2 \pmod 9$ *satisfies* $(*)$	*(case 2)*
$A = 1/9,\ B = 1/4$	*if* $m \equiv \pm 1, \pm 3, \pm 4 \pmod 9$	*(case 3)*
$A = 1/36,\ B = 1/16$	*if* $m \equiv \pm 2 \pmod 9$ *does not satisfy* $(*)$	*(case 4)*
$A = 1,\ B = -3/4$	*if* $m \equiv 0 \pmod 9$ *satisfies* $(*)$	*(case 5)*
$A = 1/9,\ B = -1/12$	*if* $m \equiv 0 \pmod 9$ *does not satisfy* $(*)$.	*(case 6)*

https://doi.org/10.1017/S0004972700034997 Published online by Cambridge University Press

PROOF: Using $\widehat{h}_{E_m}(kQ) = k^2\widehat{h}_{E_m}(Q)$ and (3.1) we find that

$$\frac{-(2/3)\log M - (11/6)\log 3}{\widehat{h}_{E_m}(Q)} < n_2^2 - n_1^2 < \frac{(2/3)\log M + (11/6)\log 3 + (1/2)\log 2}{\widehat{h}_{E_m}(Q)}.$$

The assertion now follows from Proposition 1. ∎

Notice that, when $m \to \infty$ the right hand side of (3.3) goes to $2/A$. Similarly, the left hand side goes to $-2/A$. Since $n_2^2 - n_1^2 \in \mathbb{Z}$, we can in each case find m_0 such that, for all $m \geqslant m_0$,

$$\left|n_2^2 - n_1^2\right| \leqslant g,$$

with choices $g \in \{2, 8, 18, 72\}$. Unfortunately, the bound m_0 is rather big. Below we write down our evaluation of m_0

(3.4)

g	m_0	*case*
2	6	1
8	224085	2
18	$\approx 10^{13}$	3
72	$\approx 10^{54}$	4
2	1395	5
18	$\approx 10^{23}$	6

In cases 2 and 5 we can reduce m_0 by taking slightly bigger bound than g, for example

(3.5) $$\left|n_2^2 - n_1^2\right| \leqslant 10 \text{ for } m \geqslant 20 \text{ as in case 2}$$

(3.6) $$\left|n_2^2 - n_1^2\right| \leqslant 4 \text{ for } m \geqslant 36 \text{ as in case 5}$$

PROOF OF THEOREM 1: Suppose that x–coordinates of three integral points P_0, P_1, P_2, belonging to the group $\langle Q\rangle$ generated by a fixed non-torsion point $Q \in E_m^{\min}(\mathbb{Q})$, form an increasing arithmetic progression. Write $x(P_i) = x_i$ and $P_i = n_iQ$, $i = 0, 1, 2$. We may assume that $n_i \in \mathbb{N}$ ($x(P) = x(-P)$) and $n_0 < n_1 < n_2$ (group $E_m^{\min}(\mathbb{Q})$ is torsionfree). Notice that P_1, P_2 satisfy the assumption of the last Corollary because $2x_1 = x_0 + x_2 > x_2$ (remember that $x_i > 0$ on these curves). Therefore, we have a bound for n_2 (and hence for n_0, n_1 too); more precisely, if $|n_2^2 - n_1^2| \leqslant 2k$, then $n_2 \leqslant k$.

Suppose that $m \equiv \pm 3, \pm 4 \pmod 9$ satisfies $(*)$. By the above calculation and (3.4), we obtain $n_2^2 - n_1^2 \leqslant 2$ for $m \geqslant 6$, which is impossible because $n_1 \neq n_2$. For $m \leqslant 5$ we have $\operatorname{rank}(E_m^{\min}(\mathbb{Q})) = 0$ (use Cremona's mwrank [**3**]). Hence, for such m's there is no integral arithmetic progression in a subgroup of rank 1 of $E_m^{\min}(\mathbb{Q})$.

Suppose that $m \equiv 0 \pmod 9$ satisfies $(*)$. Then, by (3.6) and the beginning of the proof, for $m \geqslant 36$ we obtain $0 < n_0 < n_1 < n_2 \leqslant 2$; a contradition. Therefore to complete the proof we have to consider the cases $m = 9, 18$. Again, using mwrank we obtain $\operatorname{rank}(E_{18}^{\min}(\mathbb{Q})) = 0$. On the other hand $\operatorname{rank}(E_9^{\min}(\mathbb{Q})) = 1$, but the only integer

https://doi.org/10.1017/S0004972700034997 Published online by Cambridge University Press

solutions of $y^2 + y = x^3 - 1$ are $(1, 0)$, $(1, -1)c$ $(7, -19)$, $(7, 18)$ tht is, P, $-P$, $2P$, $-2P$. Indeed, $x^3 = y^2 + y + 1 = (y - \omega)(y - \overline{\omega})$, where $\omega = e^{2\pi i/3}$ is a primitive root of unity. One can check that $y - \omega$ and $y - \overline{\omega}$ are relatively prime in $\mathbb{Z}[\omega]$. Since $\mathbb{Z}[\omega]$ is a UFD, we obtain $y - \omega = u \times (a + b\omega)^3$, where $a, b \in \mathbb{Z}$ and is u is an unit (that is, $u = \pm 1, \pm\omega, \pm\omega^2$). Therefore the problem of finding all integer solutions of $y^2+y = x^3-1$ is reduced to the problem of determining all representations of unity by the binary cubic form: $x^3 - 3xy^2 + y^3$. It is known (see for example, [1]) that 1 has only six representations by this form, so we can easily find all of them. And the assertion follows. □

4. Concluding Remarks

It turns out that our method does not work for other m's. Take for example $m \equiv \pm 2 \pmod 9$ satisfying (*). Then $n_2^2 - n_1^2 \leqslant 10$, (for every $m \geqslant 20$) so $n_2 \leqslant 5$ and

$$(n_0, n_1, n_2) \in \{(1,2,3), (1,3,4), (2,3,4), (1,4,5), (2,4,5), (3,4,5)\}.$$

Since $2x_1 = x_0 + x_2$ that is,

$$2x(n_1Q) = x(n_0Q) + x(n_2Q), \tag{4.1}$$

so puting $Q = (t, s) \in E_m^{\min}(\mathbb{Q})$ and substituting multiplication formulas for nQ into (4.1) we obtain, for each particular choice of n_0, n_1, n_2, an integral polynomial equation in two variables t and m (we have used Mathematica for our symbolic computations). Now it is suggested to test whether it has rational solution $(t, m) \in \mathbb{Q} \times \mathbb{Z}$. Unfortunately, in comparison with [2] our polynomial is non-homogeneous, hence investigation of its roots is more complicated. For m like in cases 3, 4, 6 the situation is even worse; first of all the bound m_0 is very large, so even after investigation of E_m for $m \geqslant m_0$ we shall still have enormous number (at level of 10^{54}) curves, that are to be checked with difference methods; for example, find all integral points. Secondly when the bound for $|n_2 - n_1|$ is 18 or 72 we have to use the formula for nQ with $n \leqslant 9$ or $n \leqslant 36$, respectively, which introduces polynomials of high degree consisting of many elements.

References

[1] M.A. Bennet, 'On the representation of unity by binary cubic forms', (preprint).

[2] A. Bremner, J.H. Silverman and N. Tzanakis, 'Intergral points in arithmetic progression on $y^2 = x(x^2 - n^2)$', *J. Number Theory* **80** (2000), 187–208.

[3] J.E. Cremona, http://www.maths.nott.ac.uk/personal/jec/ftp/progs.

[4] M. Hindry and J.H. Silverman, 'The cannonical heights and integral points on elliptic curves', *Invent. Math.* **93** (1998), 419–450.

[5] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Math. Wiss (Springer-Verlag, Berlin, New York, 1978).

[6] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math. **151** (Springer-Verlag, New York, 1994).

[7] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', in *Modular Functions of One Variable IV*, Lecture Notes in Math. **476** (Springer-Verlag, Berlin, Heidelberg, New York, 1975).

Institute of Mathematics
University of Szczecin
ul. Wielkopolska 15
70-451 Szczecin
Poland
e-mail: tjedr@sus.univ.szczecin.pl