INTEGRAL POINTS AND ARITHMETIC PROGRESSIONS ON HUFF CURVES

SZ. TENGELY

Abstract. In this paper we provide bounds for the size of the integral points on generalized Huff curves

$$H_{a,b}: \quad x(ay^2-1)=y(bx^2-1)$$

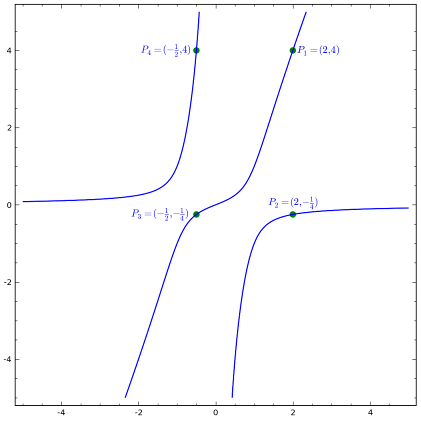
with $a,b\in\mathbb{Z}$ and

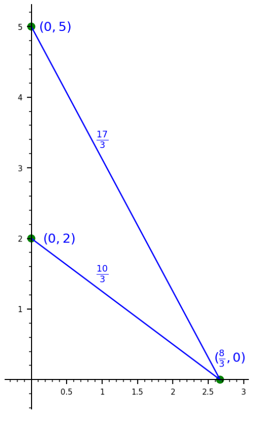
$$H_{a,b}^{c,d}: \quad ax(y^2-c)=by(x^2-d)$$

with $a,b,c,d\in\mathbb{Z}$. We also deal with integral points on these types of curves with x-coordinates forming arithmetic progressions.

1. introduction

In 1948 Huff [21] studied a geometric problem and related to it a family of curves now called Huff curves. He considered rational distance sets. Given $a,b\in\mathbb{Q}^*$ such that $a^2\neq b^2$. Determine the set of points $(x,0)\in\mathbb{Q}^2$ satisfying that $d((0,\pm a),(x,0))$ and $d((0,\pm b),(x,0))$ are rational numbers, where d denotes the usual Euclidean distance. Consider the Huff curve $ax(y^2-1)=by(x^2-1)$. If there is a rational point (x,y) on the curve, then the point $P=\left(\frac{2by}{y^2-1},0\right)$ is in the distance set.





2000 *Mathematics Subject Classification.* Primary 11D61; Secondary 11Y50.

Key words and phrases. Diophantine equations, arithmetic progressions, elliptic curves.

The point $(2, 4)$ is on the curve $2x(y^2 - 1) = 5y(x^2 - 1)$, hence

$$\left(\frac{2 \cdot 5 \cdot 4}{4^2 - 1}, 0\right) = \left(\frac{8}{3}, 0\right)$$

is in the distance set.

Elliptic curves were introduced in cryptography [23, 26]. Elliptic curves can be represented in different forms having different arithmetic properties. Many models have been studied recently: Edwards curves, Huff curves, Montgomery curves, Weierstrass curves, Hessian curves, Jacobi quartic curves and generalizations. In this paper we deal with arithmetic properties of two generalized Huff models introduced by Wu and Feng [42] and by Ciss and Sow [15]. We provide bounds for the size of integral solutions using Runge's method [31] combined with reduction method from [37]. In case of the family $H_{a,b}$ all integral solutions are classified and in case of $H_{a,b}^{c,d}$ the obtained bound is polynomial in a, b, c, d and in case of many concrete equations the largest integral point is very close to this bound.

Siegel [32] in 1926 proved that the equation $y^2 = a_0x^n + a_1x^{n-1} + \ldots + a_n =: f(x)$ has only a finite number of integer solutions if f has at least three simple roots. In 1929 Siegel [33] classified all irreducible algebraic curves over $\mathbb{Q}$ on which there are infinitely many integral points. These curves must be of genus 0 and have at most 2 infinite valuations. These results are ineffective, that is, their proofs do not provide any algorithm for finding the solutions. In the 1960's Baker [4, 6] gave explicit lower bounds for linear forms in logarithms of the form

$$\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i \neq 0$$

where $b_i \in \mathbb{Z}$ for $i = 1, \ldots, n$ and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers ($\neq 0, 1$), and $\log \alpha_i, \ldots, \log \alpha_n$ denote fixed determinations of the logarithms. Baker [5] used his fundamental inequalities concerning linear forms in logarithms to derive bounds for the solutions of the elliptic equation $y^2 = ax^3 + bx^2 + cx + d$. This bound were improved by several authors see e.g. [9, 20]. Baker and Coates [7] extended this result to general genus 1 curves. Lang proposed [24] proposed a different method to prove the finiteness of integral points on genus 1 curves. This method makes use of the group structure of the genus 1 curve. Stroeker and Tzanakis [34] and independently Gebel, Pethő and Zimmer [17] worked out an efficient algorithm based on this idea to determine all integral points on elliptic curves. The elliptic logarithm method for determining all integer points on an elliptic curve has been applied to a variety of elliptic equations (see e.g. [35, 36, 38, 39, 40]). The disadvantage of this approach is that there is no known algorithm to determine the rank of the so-called Mordell-Weil group of an elliptic curve, which is necessary to determine all integral points on the curve. There are other methods that can be used in certain cases to determine all integral solutions of genus 1 curves. Poulakis [30] provided an elementary algorithm to determine all integral solutions of equations of the form $y^2 = f(x)$, where $f(x)$ is quartic monic polynomial with integer coefficients. Using the theory of Pellian equations, Kedlaya [22] described a method to solve the system of equations

$$\begin{cases} x^2 - a_1 y^2 = b_1, \\ P(x, y) = z^2, \end{cases}$$

where P is a given integer polynomial.

An arithmetic progression on a curve $F(x, y) = 0$, is an arithmetic progression in either the x or y coordinates. One can pose the following natural question. What is the longest arithmetic progression in the x coordinates? In case of linear polynomials, Fermat claimed and Euler proved that four distinct squares cannot form an arithmetic progression. Allison [2] found an infinite family of quadratics containing an integral arithmetic progression of length eight. The curve is $y^2 = \frac{1}{2}(k^2 - l^2)x^2 - \frac{5}{2}(k^2 - l^2)x + (3k^2 - 2l^2)$, and the arithmetic progression is as follows $(-1, 6k^2 - 5l^2), (0, 3k^2 - 2l^2), (1, k^2), (2, l^2), (3, l^2), (4, k^2), (5, 3k^2 - 2l^2), (6, 6k^2 - 5l^2)$. Arithmetic progressions on Pellian equations $x^2 - dy^2 = m$ have been considered by many mathematicians. Dujella, Pethő and Tadić [16] proved that for any four-term arithmetic progression, except $\{0, 1, 2, 3\}$ and $\{-3, -2, -1, 0\}$, there exist infinitely many pairs (d, m) such that the terms of the given progression are y-components of solutions. Pethő and Ziegler [29] dealt with 5-term progressions on Pellian equations. Aguirre, Dujella and Peral [1] constructed 6-term arithmetic progression on Pellian equations parametrized by points on elliptic curve having positive rank. Pethő and Ziegler posed several open problems. One of them is as follows: "Can one prove or disprove that there are d and m with $d > 0$ and not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$?" Recenlty, González-Jiménez [18] answered the question: there is not m and d not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$. He constructed the related diagonal genus 5 curve and he applied covering techniques and the so-called elliptic Chabauty's method. Bremner [10] provided an infinite family of elliptic curve of Weierstrass form with 8 points in arithmetic progression. González-Jiménez [18] showed that these arithmetic progressions cannot be extended to 9 points arithmetic progressions. Bremner, Silverman and Tzanakis [12] dealt with the congruent number curve $y^2 = x^3 - n^2x$, they considered integral arithmetic progressions. If F is a cubic polynomial, then the problem is to determine arithmetic progressions on elliptic curves. Bremner and Campbell [13] found distinct infinite families of elliptic curves, with arithmetic progression of length eight. Campbell [13] produced infinite families of quartic curves containing an arithmetic progression of length 9. Ulas [41] constructed an infinite family of quartics containing a progression of length 12. Restricting to quartics possessing central symmetry MacLeod [25] discovered four examples of length 14 progressions (e.g. $y^2 = -17x^4 + 3130x^2 + 8551, x = -13, -11, \dots, 13.$) Alvarado [3] extended MacLeod's list by determining 11 more examples of length 14 progressions (e.g. $y^2 = 627x^4 - 87870x^2 + 3312859$) Moody [27] proved that there are infinitely many Edwards curves with 9 points in arithmetic progression. Bremner [11] and independently González-Jiménez [18, 19] proved using elliptic Chabauty's method that Moody's examples cannot be extended to longer arithmetic progressions. Moody [28] produced six infinite families of Huff curves having the property that each has rational points with x-coordinate $x = -4, -3, \dots, 3, 4$. That is he obtained arithmetic progressions of length 9. Choudhry [14] improved the result of Moody, he found infinitely many parametrized families of Huff curves on which there are arithmetic progressions of length 9, as well as several Huff curves on which there are arithmetic progressions of length 11.

In this article we characterize the arithmetic progressions in case of the curve $H_{a,b}$ and we provide infinite families of curves $H_{a,b}^{c,d}$ containing arithmetic progressions of length 9. It is important to note that we only consider arithmetic progressions related to integral points.

2. MAIN RESULTS

In the following theorem we characterize the integral points on the curve $H_{a,b}$.

Theorem 1. *The Diophantine equation*

$$H_{a,b}: \quad x(ay^2 - 1) = y(bx^2 - 1)$$

with $a, b, x, y \in \mathbb{Z}$ has the following solutions

$$\begin{aligned}
(a,b,x,y) &= (a,a,x,x) \text{ with } a,x \in \mathbb{Z},\\
(a,b,x,y) &= (1,1,-1,1),\\
(a,b,x,y) &= (1,1,1,-1),\\
(a,b,x,y) &= (-1,-1,-1,1),\\
(a,b,x,y) &= (-1,-1,1,-1),\\
(a,b,x,y) &= (a,2-a,-1,1) \text{ with } a \in \mathbb{Z},\\
(a,b,x,y) &= (a,2-a,1,-1) \text{ with } a \in \mathbb{Z}.
\end{aligned}$$

A direct consequence of the above theorem is as follows.

Corollary 1. *Let $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ be solutions of the equation $H_{a,b}$ for some $a, b \in \mathbb{Z}$ such that (x_1, x_2, x_3) forms an arithmetic progression and at most one solution (x_i, y_i) satisfies the condition $x_i = y_i$. Then $(x_1, x_2, x_3) = (-3, -1, 1), (-1, 0, 1), (1, 0, -1)$ or $(1, -1, -3)$.*

In case of the second family $H_{a,b}^{c,d}$ we have the following result.

Theorem 2. *Let $a, b, c, d \in \mathbb{Z}$ such that $abcd(a^2c - b^2d) \neq 0$. Define L_1, L_2, U_1, U_2 as follows*

$$\begin{aligned}
L_1 &= -\frac{1}{9}\sqrt{a^4c^2 - a^2b^2cd - 162\,a^2c + 81\,b^2d + 6561},\\
L_2 &= -\frac{1}{9}\sqrt{-a^4c^2 + a^2b^2cd - 162\,a^2c + 81\,b^2d - 6561},\\
U_1 &= \frac{1}{9}\sqrt{a^4c^2 - a^2b^2cd - 162\,a^2c + 81\,b^2d + 6561},\\
U_2 &= \frac{1}{9}\sqrt{-a^4c^2 + a^2b^2cd - 162\,a^2c + 81\,b^2d - 6561}.
\end{aligned}$$

Let $m_0 = \min(\{0\} \cup \{L_i : i = 1, 2, L_i \in \mathbb{R}\})$ and $M_0 = \max(\{0\} \cup \{L_i : i = 1, 2, L_i \in \mathbb{R}\})$. If (x, y) is an integral point on $H_{a,b}^{c,d}$, then we have that either

$$x = \pm\frac{\sqrt{\frac{2\,a^4c^2}{t} - \frac{2\,a^2b^2cd}{t} - 2\,a^2c + b^2d + \frac{1}{2}\,t}}{b} \qquad t \in \{-161, \ldots, 161\}$$

or

$$\begin{aligned}
\frac{m_0}{b} \leq x \leq \frac{M_0}{b} \ \text{if } b > 0,\\
\frac{M_0}{b} \leq x \leq \frac{m_0}{b} \ \text{if } b < 0.
\end{aligned}$$

Remark. In case of the curve $H_{5,2}^{-17,-6}$ there is no solution coming from the formula for x, the bound is $-29 \leq x \leq 29$. The integral solutions are given by $(x, y) \in \{(-27, -9), (0, 0), (27, 9)\}$, that is the largest solution is just 2 away from the bound. We determined all integral solutions on the curves $H_{a,b}^{c,d}$ with $-5 \leq a, b, c, d \leq 5$ and $abcd(a^2c - b^2d) \neq 0$. In 1976 cases there exist solution different from $(0, 0)$. Only in 36 cases there exist solutions with $|x| > 10$, in the table below we provide complete set of solutions for the corresponding curves.

(a, b, c, d)	solutions	(a, b, c, d)	solutions
$(-5, -4, -3, 4)$	$[(0, 0), (12, 9), (-12, -9)]$	$(3, -2, -5, 4)$	$[(0, 0), (16, -10), (-16, 10)]$
$(-5, -4, 2, -3)$	$[(0, 0), (-12, -10), (12, 10)]$	$(3, -1, -5, 4)$	$[(0, 0), (16, -4), (-16, 4)]$
$(-5, -2, -5, 4)$	$[(0, 0), (12, 3), (-12, -3)]$	$(3, 1, -5, 4)$	$[(0, 0), (16, 4), (-16, -4)]$
$(-5, -2, -3, -4)$	$[(0, 0), (16, 6), (-16, -6)]$	$(3, 2, -5, 4)$	$[(0, 0), (16, 10), (-16, -10)]$
$(-5, -1, 2, 4)$	$[(0, 0), (12, 3), (-12, -3)]$	$(4, -1, -2, 5)$	$[(0, 0), (15, -3), (-15, 3)]$
$(-5, -1, 3, -4)$	$[(0, 0), (-16, -4), (16, 4)]$	$(4, 1, -2, 5)$	$[(0, 0), (15, 3), (-15, -3)]$
$(-5, 1, 2, 4)$	$[(0, 0), (12, -3), (-12, 3)]$	$(5, -4, -3, 4)$	$[(0, 0), (12, -9), (-12, 9)]$
$(-5, 1, 3, -4)$	$[(0, 0), (-16, 4), (16, -4)]$	$(5, -4, 2, -3)$	$[(0, 0), (-12, 10), (12, -10)]$
$(-5, 2, -5, 4)$	$[(0, 0), (12, -3), (-12, 3)]$	$(5, -2, -5, 4)$	$[(0, 0), (12, -3), (-12, 3)]$
$(-5, 2, -3, -4)$	$[(0, 0), (16, -6), (-16, 6)]$	$(5, -2, -3, -4)$	$[(0, 0), (16, -6), (-16, 6)]$
$(-5, 4, -3, 4)$	$[(0, 0), (12, -9), (-12, 9)]$	$(5, -1, 2, 4)$	$[(0, 0), (12, -3), (-12, 3)]$
$(-5, 4, 2, -3)$	$[(0, 0), (12, -10), (-12, 10)]$	$(5, -1, 3, -4)$	$[(0, 0), (-16, 4), (16, -4)]$
$(-4, -1, -2, 5)$	$[(0, 0), (15, 3), (-15, -3)]$	$(5, 1, 2, 4)$	$[(0, 0), (12, 3), (-12, -3)]$
$(-4, 1, -2, 5)$	$[(0, 0), (15, -3), (-15, 3)]$	$(5, 1, 3, -4)$	$[(0, 0), (-16, -4), (16, 4)]$
$(-3, -2, -5, 4)$	$[(0, 0), (16, 10), (-16, -10)]$	$(5, 2, -5, 4)$	$[(0, 0), (12, 3), (-12, -3)]$
$(-3, -1, -5, 4)$	$[(0, 0), (16, 4), (-16, -4)]$	$(5, 2, -3, -4)$	$[(0, 0), (16, 6), (-16, -6)]$
$(-3, 1, -5, 4)$	$[(0, 0), (16, -4), (-16, 4)]$	$(5, 4, -3, 4)$	$[(0, 0), (12, 9), (-12, -9)]$
$(-3, 2, -5, 4)$	$[(0, 0), (16, -10), (-16, 10)]$	$(5, 4, 2, -3)$	$[(0, 0), (12, 10), (-12, -10)]$

On the curves $H_{a,b}^{c,d}$ we consider the question of long arithmetic progressions, we have the following statement.

Theorem 3. *There exist infinitely many tuples $(a, b, c, d), a, b, c, d \in \mathbb{Z}$ such that on the curve $H_{a,b}^{c,d}$ there is a length 9 arithmetic progression formed by x-coordinates of integral points of the curve.*

3. Proof of the results

Proof of Theorem 1. Consider the case $a = b$. We obtain that

$$axy(y - x) = x - y.$$

Therefore $x = y$ is a solution for all $x \in \mathbb{Z}$. Assume that $x \neq y$. We get that $axy = -1$. Hence $(a, b, x, y) \in \{(-1, -1, \mp 1, \pm 1), (1, 1, \mp 1, \pm 1)\}$ are the possible solutions of the equation, and one can check that these are in fact solutions.

We may assume that $|a| > |b|$. We rewrite the equation in the form

$$byx^2 + (1 - ay^2)x - y = 0.$$

Thus there exists an integer t such that

$$F(y) := a^2y^4 + (4b - 2a)y^2 + 1 = t^2. \tag{1}$$

This equation satisfies Runge's condition so we apply Runge's method to determine all the integral solutions. Define $P(y) = ay^2 + \frac{2b-a}{a}$. We have that

$$\begin{aligned} F(y) - \left(P(y) - \frac{1}{a}\right)^2 &= 2y^2 + \frac{4b}{a} - \frac{2}{a} - \frac{4b^2}{a^2} + \frac{4b}{a^2} - \frac{1}{a^2}, \\ F(y) - \left(P(y) + \frac{1}{a}\right)^2 &= -2y^2 + \frac{4b}{a} + \frac{2}{a} - \frac{4b^2}{a^2} - \frac{4b}{a^2} - \frac{1}{a^2}. \end{aligned}$$

These two quadratic polynomials have opposite signs if $|y| \geq 3$, since $|a| > |b|$. Therefore one has that

$$\left(P(y) - \frac{1}{a}\right)^2 < F(y) = t^2 < \left(P(y) + \frac{1}{a}\right)^2$$

if $|y| \geq 3$. It yields that $t = ay^2 + \frac{2b-a}{a}$. Equation (1) implies that $b = 0$. In this case

$$y \in \left\{ \frac{-1}{2ax} \pm \sqrt{\frac{1}{4a^2x^2} + \frac{1}{a}} \right\}$$

and we obtain that $|y| \leq 1$. It remains to check the cases $y \in \{0, \pm 1, \pm 2\}$. One gets that $(x, y) = (\mp 1, \pm 1)$ and $b = 2 - a$. □

Proof of Theorem 2. Rewrite the equation of $H_{a,b}^{c,d}$ as follows

$$axy^2 - b(x^2 - d)y - acx = 0.$$

Hence there exists an integer u for which

$$G(X) := X^4 + (4a^2c - 2b^2d)X + b^4d^2 = u^2,$$

where $X = bx$. Let $R(X) = X^2 + 2a^2c - b^2d$. Let $R(X) = X^2 + 2a^2c - b^2d$. We obtain that

$$\begin{aligned} G(X) - (R(X) - 162)^2 &= 324\,x^2 - 4\,a^4c^2 + 4\,a^2b^2cd + \\ &\ 648\,a^2c - 324\,b^2d - 26244, \\ G(X) - (R(X) + 162)^2 &= -324\,x^2 - 4\,a^4c^2 + 4\,a^2b^2cd - \\ &\ 648\,a^2c + 324\,b^2d - 26244. \end{aligned}$$

The roots of the above polynomials are defined in Theorem 2 as L_1, U_1 and L_2, U_2. If x is not an element of the interval $[\min(L_1, L_2), \max(U_1, U_2)]$, then

$$G(X) > (R(X) - 162)^2 \quad \text{and } G(X) < (R(X) + 162)^2.$$

Since $G(X)=u^2$ we get that $u=\pm(R(X)+t)$ for some integer $|t|<162$. It follows that

$$x=\pm\frac{\sqrt{\frac{2\,a^4c^2}{t}-\frac{2\,a^2b^2cd}{t}-2\,a^2c+b^2d+\frac{1}{2}\,t}}{b}\quad t\in\{-161,\dots,161\}.$$

It remains to bound the "small" solutions, that is to compute $\min(L_1,L_2)$ and $\max(U_1,U_2)$, these are roots of the above defined polynomials. □

Proof of Theorem 3. Based on numerical experience we fix $b=ma$ and $d=a+1$ for some integer m. The integral point $(0,0)$ is on the curve $H_{a,b}^{c,d}$ for any integral tuple (a,b,c,d). If we have an integral solution with $x=1$, then

$$c=\frac{n^2-m^2a^2}{4}$$

for some integer n. In a similar way $x=2$ corresponds to an integral solution if $2y^2-m(3-a)y-\frac{n^2-m^2a^2}{2}=0$. Hence $4n^2-3m^2(a^2+2a-3)$ is a square. We look for solutions of the form $n=ua+v$ for some $u,v\in\mathbb{Z}$. We get that

$$(v-u)^2-4u^2+3m^2=0.$$

Parametric solution of the above equation is given by

$$\begin{aligned} v-u &= \frac{-2p^2+6q^2}{G_{p,q}},\\ u &= \frac{p^2+3q^2}{G_{p,q}},\\ m &= \frac{4pq}{G_{p,q}}, \end{aligned}$$

for some integers p,q, where $G_{p,q}=\gcd(-2p^2+6q^2,p^2+3q^2,4pq)$. We deal with the case given by $G_{p,q}=1$. To obtain an integral solution with $x=3$ the polynomial

$$9(a^2-2a+1)p^4-2(37a^2+74a-431)p^2q^2+81(a^2+6a+9)q^4$$

has to be a square. Computing discriminant we have that $2560(a+7)(a+4)(a-2)(a-5)=0$, therefore $a\in\{-7,-4,2,5\}$. Using the above formulas we obtain that if $a=-7$, then

$$(x,y)=(3,4p^2+10pq-6q^2)$$

is a point on the curve, if $a=-4$, then

$$(x,y)=(3,\frac{5}{2}\,p^2+8\,pq+\frac{3}{2}\,q^2)$$

is a point, if $a = 2$, then

$$(x, y) = \left(3, \frac{1}{2}\,p^2 + 4\,pq + \frac{15}{2}\,q^2\right)$$

is a point on the curve and if $a = 5$, then

$$(x, y) = (3, 2p^2 + 2pq - 12q^2)$$

is a solution. We handle the latter two cases, the first two can be treated in a similar way. If $p^4 + 135p^2q^2 + 225q^4$ is a square, then we get a rational point on the curve with $a = 2, x = 4$. Hence we have a genus 1 curve which can be transformed to the elliptic curve

$$E_1 : \quad Y^2 = X^3 - 60750X^2 + 877078125X.$$

We use the computer algebra software Magma [8] to compute the maps between curves and ranks of elliptic curves. The rank of the Mordell-Weil group is 2. The points $(0, 0), (37125, 0)$ generate the torsion subgroup and the free part is generated by

$$(18900, 1275750), (39375, -1181250).$$

These points map to $+\infty, (0, -15)$ and $(20/3, -815), (-15, 285)$. It remains to provide infinitely many rational points on E_1 which map to rational points having an x-coordinate with odd numerator and denominator. The points $(2k + 1)(39375, -1181250)$ have this property for $k \in \mathbb{Z}$. To avoid cases with $abcd(a^2c - b^2d) = 0$ we need points with x-coordinate different from $\pm1, \pm3, \pm5, \pm15$. As examples we compute the cases with $k = 3, 5$.

(p, q)	$(-182745, 68681)$	$(-2384753104425, 47115188177959)$
points	$(0, 0)$ $(\pm1, \pm102280403100)$ $(\pm2, \pm6129121350)$ $(\pm3, \pm1871528340)$ $(\pm4, \pm1164860400)$	$(0, 0)$ $(\pm1, \pm171010830666100118328193072200)$ $(\pm2, \pm16533605562876168234812883720)$ $(\pm3, \pm16202218336426365555936358620)$ $(\pm4, \pm15931270770270530449534665405)$

We note that instead of odd multiples of the point $(39375, -1181250)$ one may use points of the form

$$(2k + 1)(18900, 1275750) + (2l + 1)(39375, -1181250)$$

to obtain appropriate rational points.

If $4p^4 - 27p^2q^2 + 144q^4$ is a square, then we get an integral point on the curve with $a = 5, x = 4$. Again we obtain an elliptic curve. It is given by

$$E_2 : \quad Y^2 = X^3 + 1990656X^2 - 2140353331200X.$$

The rank of the Mordell-Weil group of E_2 is 1. The torsion subgroup is generated by the points $(0,0),(774144,0)$ and the free part by the point $(-552960,1274019840)$. Any point of the form

$$k_1(-552960,1274019840)+k_2(0,0)+k_3(774144,0),$$

where $k_1\in\mathbb{Z},k_2,k_3\in\{0,1\}$ maps to appropriate rational point on the quartic model. We note that in this case $abcd(a^2c-b^2d)\neq 0$ if $\frac{p}{q}\neq\pm1,\pm2,\pm3,\pm6$. Let us consider the cases with $(k_1,k_2,k_3)=(3,0,0)$ and $(4,0,0)$. We have that $(p,q)=(16,3)$ and in the latter case $(-66,35)$.

(p,q)	$(16,3)$	$(-66,35)$
points	$(0,0)$	$(0,0)$
	$(\pm1,\pm140)$	$(\pm1,\pm46512)$
	$(\pm2,\pm308)$	$(\pm2,\pm10608)$
	$(\pm3,\mp500)$	$(\pm3,\pm1368)$
	$(\pm4,\mp700)$	$(\pm4,\pm612)$

We note that if $a=-7,-4$, then the corresponding elliptic curves have positive rank as well (1 and 2). □

Acknowledgement. Szabolcs Tengely was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 "National Excellence Program".

References

[1] J. Aguirre, A. Dujella, and J. C. Peral. Arithmetic progressions and Pellian equations. *Publ. Math. Debrecen*, 83(4):683–695, 2013.

[2] D. Allison. On certain simultaneous diophantine equations. *Math. Colloq. Univ. Cape Town*, 11:117–133, 1977.

[3] A. Alvarado. Arithmetic progressions on quartic elliptic curves. *Ann. Math. Inform.*, 37:3–6, 2010.

[4] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[5] A. Baker. The Diophantine equation $y^2=ax^3+bx^2+cx+d$. *J. London Math. Soc.*, 43:1–9, 1968.

[6] A. Baker. Linear forms in the logarithms of algebraic numbers. IV. *Mathematika*, 15:204–216, 1968.

[7] A. Baker and J. Coates. Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602, 1970.

[8] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[9] V. Bosser and A. Surroca. Upper bounds for the height of S-integral points on elliptic curves. *Ramanujan J.*, 32(1):125–141, 2013.

[10] A. Bremner. On arithmetic progressions on elliptic curves. *Experiment. Math.*, 8(4):409–413, 1999.

[11] A. Bremner. Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 16(8):article 13.8.5, 5, 2013.

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

[13] G. Campbell. A note on arithmetic progressions on elliptic curves. *J. Integer Seq.*, 6(1):Article 03.1.3, 5 pp. (electronic), 2003.

[14] A. Choudhry. Arithmetic progressions on Huff curves. *J. Integer Seq.*, 18(5):article 15.5.2, 9, 2015.

[15] A. A. Ciss and D. Sow. On a new generalization of Huff curves. https://eprint.iacr.org/2011/580.pdf, 2011.

[16] A. Dujella, A. Pethő, and P. Tadić. On arithmetic progressions on Pellian equations. *Acta Math. Hungar.*, 120(1-2):29–38, 2008.

[17] J. Gebel, A. Pethő, and H. G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.*, 68(2):171–192, 1994.

[18] E. González-Jiménez. Covering techniques and rational points on some genus 5 curves. In *Trends in number theory. Fifth Spanish meeting on number theory, Universidad de Sevilla, Sevilla, Spain, July 8–12, 2013. Proceedings*, pages 89–105. Providence, RI: American Mathematical Society (AMS); Madrid: Real Sociedad Matemática Española (RSME), 2015.

[19] E. González-Jiménez. On arithmetic progressions on Edwards curves. *Acta Arith.*, 167(2):117–132, 2015.

[20] L. Hajdu and T. Herendi. Explicit bounds for the solutions of elliptic equations with rational coefficients. *J. Symb. Comput.*, 25(3):361–366, art. no. sy970181, 1998.

[21] G. B. Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15:443–453, 1948.

[22] K. S. Kedlaya. Solving constrained Pell equations. *Math. Comp.*, 67(222):833–842, 1998.

[23] N. Koblitz. Elliptic curve cryptosystems. *Math. Comput.*, 48:203–209, 1987.

[24] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1978.

[25] A. J. MacLeod. 14-term arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 9(1):Article 06.1.2, 4 pp. (electronic), 2006.

[26] V. S. Miller. Use of elliptic curves in cryptography. Advances in cryptology - CRYPTO '85, Proc. Conf., Santa Barbara/Calif. 1985, Lect. Notes Comput. Sci. 218, 417-426 (1986)., 1986.

[27] D. Moody. Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 14(1):Article 11.1.7, 4, 2011.

[28] D. Moody. Arithmetic progressions on Huff curves. *Ann. Math. Inform.*, 38:111–116, 2011.

[29] A. Pethő and V. Ziegler. Arithmetic progressions on Pell equations. *J. Number Theory*, 128(6):1389–1409, 2008.

[30] D. Poulakis. A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$. *Elem. Math.*, 54(1):32–36, 1999.

[31] C. Runge. Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. *J. Reine Angew. Math.*, 100:425–435, 1887.

[32] C. L. Siegel. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$. *J. Lond. Math. Soc.*, 1:66–68, 1926.

[33] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Pr. Akad. Wiss.*, 1:41–69, 1929.

[34] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

[35] R. J. Stroeker and N. Tzanakis. Computing all integer solutions of a general elliptic equation. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 551–561. Springer, Berlin, 2000.

[36] R. J. Stroeker and N. Tzanakis. Computing all integer solutions of a genus 1 equation. *Math. Comp.*, 72(244):1917–1933, 2003.

[37] Sz. Tengely. On the Diophantine equation $F(x) = G(y)$. *Acta Arith.*, 110(2):185–200, 2003.

[38] N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. *Acta Arith.*, 75(2):165–190, 1996.

[39] N. Tzanakis. Effective solution of two simultaneous Pell equations by the elliptic logarithm method. *Acta Arith.*, 103(2):119–135, 2002.

[40] N. Tzanakis. *Elliptic Diophantine equations. A concrete approach via the elliptic logarithm.* Berlin: de Gruyter, 2013.

[41] M. Ulas. A note on arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 8(3):Article 05.3.1, 5 pp. (electronic), 2005.

[42] H. Wu and R. Feng. Elliptic curves in Huff's model. *Wuhan Univ. J. Nat. Sci.*, 17(6):473–480, 2012.

Mathematical Institute
University of Debrecen
P.O.Box 12
4010 Debrecen
Hungary
E-mail address: `tengely@science.unideb.hu`