Publ. Math. Debrecen
92/3-4 (2018), 441–452
DOI: 10.5486/PMD.2018.8018

Integral points and arithmetic progressions on Huff curves

By SZABOLCS TENGELY (Debrecen)

Abstract. In this paper, we provide bounds for the size of the integral points on some generalized Huff curves. We also deal with integral points on these types of curves with one of the coordinates forming arithmetic progressions.

1. Introduction

In 1948, Huff [22] 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. For example, with $(a, b) = (2, 5)$, the curve $2x(y^2 - 1) = 5y(x^2 - 1)$ contains the point $(2, 4)$, and so

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

lies in the distance set.

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 the arithmetic properties

Mathematics Subject Classification: Primary: 11D61; Secondary: 11Y50.
Key words and phrases: Diophantine equations, arithmetic progressions, elliptic curves.

of two generalized Huff models introduced by Wu and Feng [41] and by Ciss and Sow [15]. These models are as follows:

$$H_{a,b}: \quad x(ay^2-1) = y(bx^2-1), \qquad \text{with } a,b \in \mathbb{Z},$$

and

$$H_{a,b}^{c,d}: \quad ax(y^2-c) = by(x^2-d), \qquad \text{with } a,b,c,d \in \mathbb{Z}.$$

We provide bounds for the size of integral solutions using Runge's method [30] combined with reduction method from [36]. In case of the family $H_{a,b}$ all integral solutions are classified and in the case of $H_{a,b}^{c,d}$ the obtained bound is polynomial in a,b,c,d and in the case of many concrete equations the largest integral point is very close to this bound.

Siegel [31] in 1926 proved that the equation $y^2 = a_0x^n + a_1x^{n-1} + \cdots + a_n =: f(x)$ has only a finite number of integer solutions if f has at least three simple roots. In 1929, Siegel [32] 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 (see [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 $y^2 = ax^3 + bx^2 + cx + d$. These bounds were improved by several authors, see, e.g., [9], [21]. Baker and Coates [7] extended this result to general genus 1 curves. Lang [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 [33], 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., [34], [35], [37], [38], [39]). 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 [29] provided an elementary algorithm to determine all integral solutions of equations of the form $y^2 = f(x)$, where $f(x)$ is a quartic monic polynomial with integer coefficients. Using the theory of Pellian equations, Kedlaya [23] 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 the 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, and González-Jiménez and Xarles [20] proved that this family has no examples of length longer than eight. 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 [28] 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 $x^2 - dy^2 = m$?" Recently, González-Jiménez [18] answered the question: there do not exist m and d, where d is 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 curves 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 $y^2 = x^3 - n^2 x$, 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 [40] 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. Alvarado [3] extended MacLeod's list by determining 11 more examples of length-14 progressions. Moody [26] 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 [27] produced six infinite families of Huff curves having the property that each has rational points with x-coordinate $x = -4, -3, \ldots, 3, 4$, 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 the 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* $H_{a,b} : x(ay^2 - 1) = y(bx^2 - 1)$ *with* $a, b, x, y \in \mathbb{Z}$ *has precisely the following solutions:*

$$
\begin{aligned}
&(a, b, x, y) = (a, b, 0, 0) \text{ with } a, b \in \mathbb{Z},\\
&(a, b, x, y) = (a, a, x, x) \text{ with } a, x \in \mathbb{Z},\\
&(a, b, x, y) = (1, 1, -1, 1),\\
&(a, b, x, y) = (1, 1, 1, -1),\\
&(a, b, x, y) = (-1, -1, -1, 1),\\
&(a, b, x, y) = (-1, -1, 1, -1),\\
&(a, b, x, y) = (a, 2 - a, -1, 1) \text{ with } a \in \mathbb{Z},\\
&(a, b, x, y) = (a, 2 - a, 1, -1) \text{ with } a \in \mathbb{Z}.
\end{aligned}
$$

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 the case of the second family $H^{c,d}_{a,b}$, we have the following result. Define $\phi(a, b, c, d) = (a^2c - 81)(a^2c - 81 - b^2d)$.

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:*

$$L_1 = -\tfrac{1}{9}\sqrt{\phi(a,b,c,d)}, \qquad U_1 = \tfrac{1}{9}\sqrt{\phi(a,b,c,d)},$$
$$L_2 = -\tfrac{1}{9}\sqrt{-\phi(a,b,-c,-d)}, \qquad U_2 = \tfrac{1}{9}\sqrt{\phi(a,b,-c,-d)}.$$

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

$$x = \pm\frac{\sqrt{(2a^2c - t)(2a^2c - t - 2b^2d)}}{b\sqrt{2t}} \quad t \in \{-161, \ldots, 161\}$$

or

$$\frac{m_0}{b} \leq x \leq \frac{M_0}{b} \quad \text{if } b > 0, \qquad \frac{M_0}{b} \leq x \leq \frac{m_0}{b} \quad \text{if } b < 0.$$

Remark. In the case of the curve $H^{-17,-6}_{5,2}$, 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.

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

Theorem 3. *There exist infinitely many tuples $(a, b, c, d) \in \mathbb{Z}^4$ such that there is a length-9 arithmetic progression formed by x-coordinates of integral points on the curve $H^{c,d}_{a,b}$.*

3. Proof of the results

In the proofs of the results, we use several times that the discriminant of a degree-2 polynomial (in some variable) must be a rational square. This is a necessary condition to obtain integer solutions.

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

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

A necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in x must be a rational square. Thus there exists an integer t such that

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

We apply Runge's method [30] to determine all the integral solutions. Define $P(y) = ay^2 + \frac{2b-a}{a}$. We have that

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

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 $t = \pm\left(ay^2 + \frac{2b-a}{a}\right)$. 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 $|y| \leq 1$. Therefore, we have that $|y| < 3$. It remains to check the cases $y \in \{0, \pm 1, \pm 2\}$. If $y = 0$, it follows that $x = 0$. If $y = \pm 1$, then

$$\pm bx^2 - (a - 1)x \mp 1 = 0.$$

Hence $x = \pm 1$ and $b = a$ or $b = 2 - a$. If $y = \pm 2$, then we get that

$$\pm 2bx^2 - (4a - 1)x \mp 2 = 0.$$

Therefore $x \in \{\pm 1, \pm 2\}$. If $x = \pm 2$, then we get that $a = b$, a case that has been considered. If $x = \pm 1$, then no solution exists. □

PROOF OF THEOREM 2. Rewrite the equation of $H_{a,b}^{c,d}$ as follows:

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

A necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in y must be a rational square. Hence there exists an integer u for which

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

where $X = bx$. Let $R(X) = X^2 + 2a^2c - b^2d$, which is the polynomial part of the Puiseux expansion of $\sqrt{G(X)}$. We obtain that

$$G(X) - (R(X) - 162)^2 = 324X^2 - 4a^4c^2 + 4a^2b^2cd + 648a^2c - 324b^2d - 26244,$$
$$G(X) - (R(X) + 162)^2 = -324X^2 - 4a^4c^2 + 4a^2b^2cd - 648a^2c + 324b^2d - 26244.$$

The roots of the above polynomials are defined in Theorem 2 as L_1, U_1 and L_2, U_2, respectively. If X is not an element of the interval

$$[\min(L_1, L_2), \max(U_1, U_2)],$$

then

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

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

$$x = \frac{X}{b} = \pm\frac{\sqrt{(2a^2c - t)(2a^2c - t - 2b^2d)}}{b\sqrt{2t}} \quad t \in \{-161, \ldots, 161\}.$$

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. We note that we fixed the number 162 appearing in the above computation based on numerical experiences. It can be replaced by an other constant, say T. If a and b are large, then a baby step–giant step type algorithm can be used to find a near optimal value for T, for which the number of integers in the intervals $[\min(L_1, L_2), \max(U_1, U_2)]$ and $[-T + 1, T - 1]$ is almost as small as possible. □

PROOF OF THEOREM 3. First notice that if $(x, y) \in H_{a,b}^{c,d}$, then $(-x, -y) \in H_{a,b}^{c,d}$. 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 $y^2 + amy - c = 0$ and a necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in y must be a rational square. Hence

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

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

$$(v - u, u, m) = \left(\frac{-2p^2 + 6q^2}{G_{p,q}}, \frac{p^2 + 3q^2}{G_{p,q}}, \frac{4pq}{G_{p,q}}\right),$$

for some integers p, q, where $G_{p,q} = \gcd(-2p^2 + 6q^2, p^2 + 3q^2, 4pq)$. To obtain an integral solution with $x = 3$, an argument similar to the case $x = 1$ gives us that 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. The quartic is singular when its discriminant is 0, so for $a = -7, -4, 2$ or 5. Using the above formulas, we obtain for $x = 3$ and each values of a the corresponding y-coordinate of the point in $H^{c,d}_{a,b}$, where a, b, c, d are as above:

a	y
-7	$2(2p - q)(p + 3q)$
-4	$\frac{1}{2}(5p + q)(p + 3q)$
2	$\frac{1}{2}(p + 5q)(p + 3q)$
5	$2(p - 2q)(p + 3q)$

We handle the case with $a = 2$, the other three can be treated in a similar way. When $a = 2$, then a point on the curve with $x = 4$ demands

$$p^4 - 34p^2q^2 + 225q^4 + 52pqy - 4y^2 = 0,$$

so that necessarily its discriminant, $p^4 + 135p^2q^2 + 225q^4$, is a square. Hence we have a genus 1 curve, which has an affine model of the form

$$C : v^2 = u^4 + 135u^2 + 225, \qquad \text{where } u = p/q.$$

The quartic curve C has the rational point $[0:1:0]$, then it is an elliptic curve defined over $\mathbb{Q}$. A Weierstrass model for C is

$$E_2 : Y^2 = X^3 + 45X^2 - 6300X,$$

and the isomorphism is given in affine coordinates by

$$\phi : C \longrightarrow E_2\,, \qquad \phi(u,v) = (30 + 2u^2 + 2v, 270u + 4u^3 + 4uv).$$

We use the computer algebra software Magma [8] to compute the generator of the Mordell–Weil group of E_2. The points $(60,0)$, $(0,0)$ generate the torsion subgroup and the free part is generated by

$$(-30, 450), (-90, 450).$$

The point $(x,y) = \left(3, \frac{1}{2}(p+5q)(p+3q)\right) \in H_{a,b}^{c,d}$ is supposed to be an integral point, therefore we need to scale p and q so that they have the same parity. To avoid cases with $abcd(a^2c - b^2d) = 0$, we need points in C with a u-coordinate different from $\pm 1, \pm 3, \pm 5, \pm 15$, that is, the points that are not coming from the following points on E_2:

$$(70, \pm 350), (-6, \pm 198), (126, \pm 1386), (-30, \pm 450), (210, \pm 3150),$$
$$(-50, \pm 550), (1050, \pm 34650), (-90, \pm 450), (6, 0), (0, 0), (-105, 0).$$

As examples, we compute the cases corresponding to the points $3(-90, 450)$ and $2(-30, 450)$. From $3(-90, 450)$ we get that $p/q = 182745/68681$, so we do not need to scale. From $2(-30, 450)$ we obtain that $p/q = 8/13$, so we fix $(p, q) = (16, 26)$ to make the y-coordinate corresponding with the point with x-coordinate equal to 3 an integer.

(p,q)	$(182745, 68681)$	$(16, 26)$
points on $H_{2,b}^{c,3}$	$(0,0)$	$(0,0)$
	$(\pm 1, \pm 1871528340)$	$(\pm 1, \pm 3534)$
	$(\pm 2, \pm 31231340040)$	$(\pm 2, \pm 5358)$
	$(\pm 3, \pm 102280403100)$	$(\pm 3, \pm 6862)$
	$(\pm 4, \pm 164329281885)$	$(\pm 4, \pm 8322)$
b	100408874760	3328
c	191420673028273854000	24250308

We note that for $a = -7, -4, 5$, the corresponding elliptic curve E_a have positive ranks as well (1, 2 and 1, respectively). Moreover, E_2 and E_{-4} (and E_5 and E_{-7}) are isomorphic over $\mathbb{Q}$. □

Acknowledgements. The author is grateful for the helpful comments of the anonymous reviewers which improved the quality of this publication. The author 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** (2013), 683–695.

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

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

[4] A. Baker, Units of algebraic number fields, *Mathematika* **13** (1966), 204–216; *ibid.* **14** (1967), 102–107; *ibid.* **14** (1967), 220-228.

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

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

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

[8] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

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

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

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

[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** (2000), 187–208.

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

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

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

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

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

[18] E. González-Jiménez, Covering techniques and rational points on some genus 5 curves, In: Trends in Number Theory, Contemporary Mathematics, Vol. **649**, *American Mathematical Society*, *Providence, RI*, 2015, 89–105.

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

[20] E. González-Jiménez and X. Xarles, On symmetric square values of quadratic polynomials, *Acta Arith.* **149** (2011), 145–159.

[21] L. Hajdu and T. Herendi, Explicit bounds for the solutions of elliptic equations with rational coefficients, *J. Symbolic Comput.* **25** (1998), 361–366.

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

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

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

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

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

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

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

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

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

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

[32] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss. Phys.-Math.* **1** (1929), 41–69.

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

[34] R. J. Stroeker and N. Tzanakis, Computing all integer solutions of a general elliptic equation, In: Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Computer Science, Vol. **1838**, *Springer*, *Berlin*, 2000, 551–561.

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

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

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

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

[39] N. Tzanakis, Elliptic Diophantine Equations. A Concrete Approach via the Elliptic Logarithm, *Walter de Gruyter*, *Berlin*, 2013.

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

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

SZABOLCS TENGELY
MATHEMATICAL INSTITUTE
UNIVERSITY OF DEBRECEN
P. O. BOX 400
4002 DEBRECEN
HUNGARY

E-mail: tengely@science.unideb.hu

(Received April 24, 2017; revised August 1, 2017)