RATIONAL SEQUENCES ON DIFFERENT MODELS OF ELLIPTIC CURVES

Gamze Savas Celik, Mohammad Sadek and Gokhan Soydan
Bursa Uludag University, Turkey and Sabanci University, Turkey

Abstract. Given a set $S$ of elements in a number field $k$, we discuss the existence of planar algebraic curves over $k$ which possess rational points whose $x$-coordinates are exactly the elements of $S$. If the size $|S|$ of $S$ is either 4, 5, or 6, we exhibit infinite families of (twisted) Edwards curves and (general) Huff curves for which the elements of $S$ are realized as the $x$-coordinates of rational points on these curves. This generalizes earlier work on progressions of certain types on some algebraic curves.

1. Introduction

An algebraic (affine) plane curve $C$ of degree $d$ over some field $k$ is defined by an equation of the form

$$\{(x, y) \in k^2 : f(x, y) = 0\}$$

where $f$ is a polynomial of degree $d$. The algebraic affine plane curve $C$ can also be extended to the projective plane by homogenising the polynomial $f$. If $P = (x, y)$, then we write $x = x(P)$ and $y = y(P)$.

Studying the set of $k$-rational points on $C$, $C(k)$, has been subject to extensive research in arithmetic geometry and number theory, especially when $k$ is a number field. For example, if $f$ is a polynomial of degree 2, then one knows that $C$ is of genus 0, and so if $C$ possesses one rational point then it contains infinitely many such points. If $f$ is of degree 3, then $C$ is a genus 1 curve if it is smooth. In this case, if $C(k)$ contains one rational point, then it is an elliptic curve, and according to Mordell-Weil Theorem, $C(k)$ is a finitely

2010 Mathematics Subject Classification. 11D25, 11G05, 14G05.

Key words and phrases. Elliptic curve, Edwards curve, Huff curve, rational sequence, rational point.
generated abelian group. In particular, $C(k)$ can be written as $T \times \mathbb{Z}^r$ where $T$ is the subgroup of points of finite order, and $r \geq 0$ is the rank of $C$ over $k$.

In enumerative geometry, one may pose the following question. Given a set of points $S$ in $k^2$, how many algebraic plane curves $C$ of degree $d$ satisfy that $S \subseteq C(k)$? It turns out that sometimes the answer is straightforward. For example, given 10 points in $k^2$, in order for a cubic curve to pass through these points, a system of 10 linear equations will be obtained by substituting the points of $S$ in

$$a_1x^3 + a_2x^2y + a_3x^2 + a_4xy^2 + a_5xy + a_6x + a_7y^3 + a_8y^2 + a_9y + a_{10} = 0$$

and solving for $a_1, \ldots, a_{10}$. Therefore, there exists a nontrivial solution to the system if the determinant of the corresponding matrix of coefficients is zero, hence a cubic curve through the points of $S$. Thus, one needs linear algebra to check the existence of algebraic curves of a certain degree through various specified points in $k^2$.

In this article, we address the following, relatively harder, question. Given $S \subset k$, are there algebraic curves $C$ of degree $d$ such that for every $x \in S$, $x = x(P)$ for some $P \in C(k)$? In other words, $S$ constitutes the $x$-coordinates of a subset of $C(k)$. The latter question can be reformulated to involve $y$-coordinates instead of $x$-coordinates. It is obvious that linear algebra cannot be utilized to attack the problem as substituting with the $x$-values of $S$ will not yield linear equations.

Given a set $S = \{x_1, x_2, \ldots, x_n\} \subset k$, if $(x_i, y_i), i = 1, \ldots, n,$ are $k$-rational points on an algebraic curve $C$, then these rational points are said to be an $S$-sequence of length $n$. In what follows, we summarize the current state of knowledge for different types of $S$.

We first describe the state-of-art when the elements of $S \subset \mathbb{Q}$ are chosen to form an arithmetic progression, Lee and Vélez ([10]) found infinitely many curves described by $y^2 = x^3 + a$ containing $S$-sequences of length 4. Bremner ([2]) showed that there are infinitely many elliptic curves with $S$-sequences of length 7 and 8. Campbell ([5]) gave a different method to produce infinite families of elliptic curves with $S$-sequences of length 7 and 8. In addition, he described a method for obtaining infinite families of quartic elliptic curves with $S$-sequences of length 9, and gave an example of a quartic elliptic curve with an $S$-sequence of length 12. Ulas ([17]) first described a construction method for an infinite family of quartic elliptic curves on which there exists an $S$-sequence of length 10. Secondly he showed that there is an infinite family of quartics containing $S$-sequences of length 12. Macleod ([11]) showed that simplifying Ulas’ approach may provide a few examples of quartics with $S$-sequences of length 14. Ulas ([18]) found an infinite family of genus two curves described by $y^2 = f(x)$ where $\deg(f(x)) = 5$ possessing $S$-sequences of length 11. Alvarado ([1]) showed the existence of an infinite family of such curves with $S$-sequences of length 12. Moody ([12]) found an infinite number of
Edwards curves with an $S$-sequence of length 9. He also asked whether any such curve will allow an extension to an $S$-sequence of length 11. Bremner ([3]) showed that such curves do not exist. Also, Moody ([14]) found an infinite number of Huff curves with $S$-sequences of length 9, and Choudhry ([6]) extended Moody's result to find several Huff curves with $S$-sequences of length 11.

Now we consider the case when the elements of $S$ form a geometric progression, Bremner and Ulas ([4]) obtained an infinite family of elliptic curves with $S$-sequences of length 4, and they also pointed out infinitely many elliptic curves with $S$-sequences of length 5. Ciss and Moody ([13]) found infinite families of twisted Edwards curves with $S$-sequences of length 5 and Edwards curves with $S$-sequences of length 4. When the elements of $S \subset \mathbb{Q}$ are consecutive squares, Kamel and Sadek ([9]) constructed infinitely many elliptic curves given by the equation $y^2 = ax^3 + bx + c$ with $S$-sequences of length 5. When the elements of $S \subset \mathbb{Q}$ are consecutive cubes, Çelik and Soydan ([7]) found infinitely many elliptic curves of the form $y^2 = ax^3 + bx + c$ with $S$-sequences of length 5.

In the present work, we consider the following families of elliptic curves due to the symmetry enjoyed by the equations defining them: (twisted) Edwards curves and (general) Huff curves. Given an arbitrary subset $S$ of a number field $k$, we tackle the general question of the existence of infinitely many such curves with an $S$-sequence when there is no restriction on the elements of $S$. We provide explicit examples when the length of the $S$-sequence is 4, 5, or 6. This is achieved by studying the existence of rational points on certain quadratic and elliptic surfaces.

2. Edwards curves with $S$-sequences of length 6

Throughout this work, $k$ will be a number field unless otherwise stated. An Edwards curve over $k$ is defined by

$$E_d : x^2 + y^2 = 1 + dx^2y^2,$$

where $d$ is a non-zero element in $k$. It is clear that the points $(x, y) = (-1, 0), (0, \pm 1), (1, 0) \in E_d(k)$. We show that given any set

$$S = \{s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3, s_4\} \subset k,$$

$s_i \neq s_j$ if $i \neq j$, there are infinitely many Edwards curves $E_d$ that possess rational points whose $x$-coordinates are $s_i$, $-1 \leq i \leq 4$, i.e., the set $S$ is realized as $x$-coordinates in $E_d(k)$. In other words, there are infinitely many Edwards curves that possess an $S$-sequence.

We start with assuming that $s_2$ is the $x$-coordinate of a point in $E_d(k)$, then one must have $y^2 = \frac{s_2^2 - 1}{s_2^2d - 1}$, or $s_2^2d - 1 = (s_2^2 - 1)p^2$ for some $p = 1/y \in k$. 
Similarly, if $s_3$ is the $x$-coordinate of a point in $E_d(k)$, then $y^2 = \frac{s_3^2 - 1}{s_3^2 d - 1}$, or $s_3^2 d - 1 = (s_3^2 - 1)q^2$. So

$$d = \frac{(s_2^2 - 1)p^2 + 1}{s_2^2} = \frac{(s_3^2 - 1)q^2 + 1}{s_3^2}.$$  

Thus we have the following quadratic curve

$$s_3^2 [(s_2^2 - 1)p^2 + 1] - s_2^2 [(s_3^2 - 1)q^2 + 1] = 0$$

on which we have the rational points on the latter quadratic curve yields

$$p = \frac{2ts_2^2 - t^2s_2^2 - s_3^2 + 2ts_3^2 s_1^2 + t^2s_3^2 s_1^2}{-t^2s_2^2 + s_3^2 - s_3^2 s_1^2 + t^2s_3^2 s_1^2},$$

$$q = -\frac{(-1 + s_2^2)s_3^2 - 2t(-1 + s_2^2)s_3^2 + t^2s_2^2(-1 + s_3^2)}{-(-1 + s_2^2)s_3^2 + t^2s_2^2(-1 + s_3^2)}.$$

Therefore, fixing $s_2$ and $s_3$ in $k$, one sees that $p$ and $q$ lie in $k(t)$. Now we obtain the following result.

**Theorem 2.1.** Let $s_{-1} = -1$, $s_0 = 0$, $s_1 = 1$, $s_2$, $s_3$ and $s_4$, $s_i \neq s_j$ if $i \neq j$, be a sequence in $\mathbb{Z}$ such that

$$h(s_2, s_3) = -3 + 4s_2^2 + s_3^4 + s_2^2 (4 - 6s_2^2) \neq 0$$

where either $g_1(s_2, s_3)/h(s_2, s_3)^2$ or $g_2(s_2, s_3)/h(s_2, s_3)^3$ are not integers, $g_1$ and $g_2$ are defined in (2.3). There are infinitely many Edwards curves described by

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \quad d \in \mathbb{Q}$$

on which $s_i$, $-1 \leq i \leq 4$, are the $x$-coordinates of rational points in $E_d(Q)$. In other words, there are infinitely many Edwards curves that possess an $S$-sequence where $S = \{s_i: -1 \leq i \leq 4\}$.

**Proof.** Substituting the value for $p$ in $d = \frac{(s_2^2 - 1)p^2 + 1}{s_2^2}$ yields that

$$(-t^2s_2^2 + s_3^2 - s_3^2 s_1^2 + t^2s_2^2 s_3^2)^2 d$$

$$= (s_2^4 - 2s_2^4 s_1^2 + s_2^4 s_1^4) + (4s_2^2 - 8s_2^2 s_3^2 + 4s_2^2 s_3^2 - 4s_2^2 + 8s_2^2 s_3^2) t$$

$$+ (-4s_2^2 + 4s_2^4 - 4s_2^2 + 14s_2^2 s_3^2 - 10s_2^2 s_3^2 + 4s_3^2 - 10s_2^2 s_3^2 + 6s_2^2 s_3^2) t^2$$

$$+ (4s_2^2 - 4s_2^4 - 8s_2^4 s_3^2 + 8s_2^2 s_3^2 - 4s_2^2 s_3^2 - 4s_2^2 s_3^2) t^3 + (s_2^2 - 2s_2^2 s_3^2 + s_2^2 s_3^2) t^4.$$

Thus, for fixed values of $s_2$ and $s_3$, we have $d \in \mathbb{Q}(t)$.

Now we show the existence of infinitely many values of $t$ such that $s_4$ is the $x$-coordinate of a rational point on $E_d$. In fact, we will show that $t$ can be chosen to be the $x$-coordinate of a rational point on an elliptic curve with positive Mordell-Weil rank, hence the existence of infinitely many such
possible values for $t$. Forcing $(s_4, r)$ to be a point in $E_d(\mathbb{Q})$ for some rational $r$ yields that

$$r^2 = \frac{s_3^2 - 1}{s_4^2 - 1} = (A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4)/B(t)^2,$$

where $A_i \in \mathbb{Z}$ and $B(t) = -t^2 s_2^2 + t^2 s_2 s_3^2 + s_2^2 - s_3^2 s_4^2$. This implies that $A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4$ must be a rational square. This yields the elliptic curve $C$ defined by

$$z^2 = A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4,$$

with the following rational point

$$(t, z) = \left(0, s_3^2(s_2^2 - 1)\right).$$

The latter elliptic curve is isomorphic to the elliptic curve described by the Weierstrass equation $E_{I, J} : y^2 = x^3 - 27 I x - 27 J$ where

$$I = 12A_0 A_4 - 3A_1 A_3 + A_2^2$$

$$J = 72A_0 A_2 A_4 + 9A_1 A_2 A_3 - 27A_1^2 A_4 - 27A_0 A_3^2 - 2A_2^3,$$

see for example [16, §2]. The latter elliptic curve has the following rational point

$$P = \left(-12(-1 + s_2^2)(-1 + s_3^2)(-1 + s_3^2), -216(-1 + s_3^2)^2(-1 + s_3^2)^2\right).$$

One notices that the coordinates of $3P$ are rational functions. Indeed,

$$3P = \left(\frac{g_1(s_2, s_3)}{h(s_2, s_3)^2}, \frac{g_2(s_2, s_3)}{h(s_2, s_3)^3}\right),$$

where $g_1, g_2 \in \mathbb{Q}[s_2, s_3]$ and

$$h(s_2, s_3) = -3 + 4s_2^2 + s_2^4 + 2s_2^2(4 - 6s_3^2).$$

Hence, as long as $h(s_2, s_3) \neq 0$, and $g_1/h^2 \notin \mathbb{Z}$ or $g_2/h^3 \notin \mathbb{Z}$, one sees that $3P$ is a point of infinite order by virtue of Lutz-Nagell Theorem. Thus, $P$ itself is a point of infinite order. It follows that $E_{I, J}$ is of positive Mordell-Weil rank.

Since $C$ is isomorphic to $E_{I, J}$, it follows that $C$ is also of positive Mordell-Weil rank. Therefore, there are infinitely many rational points $(t, z) \in C(\mathbb{Q})$, each giving rise to a value for $d$, by substituting in (2.2), hence an Edwards curve $E_d$ possessing the aforementioned rational points. That infinitely many of these curves are pairwise non-isomorphic over $\mathbb{Q}$ follows, for instance, from [8, Proposition 6.1].

3. Twisted Edwards curves with $S$-sequences of length 4

A Twisted Edwards curve over $k$ is given by

$$E_{a, d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where $a$ and $d$ are nonzero elements in $k$. Note that the point $(x, y) = (0, \pm 1) \in E_{a, d}(k)$. Given a set $\{u_0 = 0, u_1, u_2, u_3\} \subset k$, $u_i \neq u_j$ if $i \neq j$, we prove that
there are infinitely many twisted Edwards curves \( E_{a,d} \) for which \( S \) is realized as the \( x \)-coordinates of rational points on \( E_{a,d} \).

We begin by assuming that \( u_1 \) is the \( x \)-coordinate of a point in \( E_{a,d}(k) \), then one must get
\[
y^2 = \frac{au_1^2 - 1}{u_1^2d - 1}, \quad \text{or} \quad u_1^2d - 1 = (au_1^2 - 1)i^2 \text{ for some } i \in k.
\]

Now, if \( u_2 \) is the \( x \)-coordinate of a point in \( E_{a,d}(k) \), then
\[
y^2 = \frac{au_2^2 - 1}{u_2^2d - 1} \quad \text{or} \quad u_2^2d - 1 = (au_2^2 - 1)i^2. \quad \text{So}
\]
\[
d = \frac{(au_1^2 - 1)i^2 + 1}{u_1^2} = \frac{(au_2^2 - 1)i^2 + 1}{u_2^2}. \]

Hence we obtain the following quadratic surface
\[
u_2^2 \left[ (au_1^2 - 1)i^2 + 1 \right] - u_1^2 \left[ (au_2^2 - 1)i^2 + 1 \right] = 0,
\]
on which we have the rational point \((i, j) = (1, 1)\). Solving the above quadratic surface gives the following
\[
i = \frac{-au_1^2u_2^2 + u_2^2 + 2au_1^2u_2^2 - 2u_1^2 - at^2u_1^2u_2^2 + u_1^2t^2}{au_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2},
\]
\[
j = \frac{-2atu_1^2u_2^2 + 2u_1^2 + at^2u_1^2u_2^2 - u_1^2t^2 + au_1^2u_2^2 - u_2^2}{au_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2}.
\]

Now we get the following result.

**Theorem 3.1.** Let \( u_0 = 0 \), \( u_1 \), \( u_2 \) and \( u_3 \), \( u_i \neq u_j \) if \( i \neq j \), be a sequence in \( \mathbb{Z} \) such
that \( h(u_1, u_2) \neq 0 \), and either \( g_1(s_2, s_3)/h(s_2, s_3)^2 \) or \( g_2(s_2, s_3)/h(s_2, s_3)^3 \) are not integers, where \( h, g_1, g_2 \) are defined
in (3.3). There are infinitely many twisted Edwards curves described by
\[
E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \quad d \in \mathbb{Q}, \ a \in \mathbb{Q}^\times \text{ is arbitrary}
\]
on which \( u_i \), \( 0 \leq i \leq 3 \), are the \( x \)-coordinates of rational points in \( E(\mathbb{Q}) \). In other words, there are infinitely many twisted Edwards curves that possess an S-sequence where \( S = \{ u_i : 0 \leq i \leq 3 \} \).

**Proof.** Substituting the expression for \( i \) in \( d = \frac{(au_1^2 - 1)i^2 + 1}{u_1^2} \) gives that
\[
(u_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2)^i d
\]
\[
= (u_1^4a^4u_2^4 - 2u_1^4a^4u_2^2 + u_1^4a^4u_2^2) t^4 + (-8au_1^2u_2^2 + 4u_1^2 + 4u_1^2a^2u_2^2 - 4u_1^2a
\]
\[
- 4u_1^4a^3u_2^4 + 8u_1^4a^3u_2^2) t^3 + (-4u_1^2 - 10u_1^2a^2u_2^2 + 14au_1^2u_2^2 + 6u_1^4a^3u_2^4
\]
\[
- 4u_2^2 - 10u_1^2a^2u_2^2 + 4a^4u_2^2 + 4u_1^2a + 4au_1^2) t^2 + (4u_2^2 + 8u_1^2a^2u_2^2 - 8au_1^2u_2^2
\]
\[
+ 4u_1^4a^3u_2^4 - 4au_1^4 - 4u_1^4a^3u_2^4) t + u_1^4a^3u_2^2 - 2u_1^2a^2u_2^2 + au_1^2.
\]
Then, assuming \((u_3, \ell) \in E(\mathbb{Q})\) yields
\[
\ell^2 = \frac{au_3^2 - 1}{du_3^2 - 1} = \frac{(C_0 + C_1 t + C_2 t^2 + C_3 t^3 + C_4 t^4)/D(t)^2},
\]
where \(C_i \in \mathbb{Q}\) and \(D(t) = au_3^2 u_2^2 - u_2^3 - at^2 u_2^2 + u_1^2 t^2\).

For the latter equation to be satisfied, one needs to find rational points on the elliptic curve \(C'\) defined by
\[
z^2 = C_0 + C_1 t + C_2 t^2 + C_3 t^3 + C_4 t^4
\]
that possesses the rational point
\[
(t, z) = (0, u_2^3(au_1^2 - 1)).
\]
The latter elliptic curve is isomorphic to the elliptic curve described by the Weierstrass equation \(E_{I', J}: y^2 = x^3 - 27Ix - 27J\) where
\[
I = 12C_0C_4 - 3C_1C_3 + C_2^2,
J = 72C_0C_2C_4 + 9C_1C_2C_3 - 27C_0^2C_4 - 27C_0C_3^2 - 2C_2^3,
\]
see for example [16, §2]. The latter elliptic curve has the following rational point
\[
Q = (-12(-1 + au_2^2)(-1 + au_1^2)(-3 + au_2^2 + u_1^2), -216(-1 + au_2^2)^2(-1 + au_1^2)^2).
\]
One notices that the coordinates of \(3Q\) are rational functions. In fact,
\[
3Q = \left(\frac{g_1(u_1, u_2)}{h(u_1, u_2)^2}, \frac{g_2(u_1, u_2)}{h(u_1, u_2)^2}\right), \quad \text{where } g_1, g_2 \in \mathbb{Q}[u_1, u_2]
\]
and
\[
h(u_1, u_2) = -27 - 72u_1^3 + 36u_1^4 + 18u_1^3u_2^2 - 12u_1^4u_2^2 - 18u_2^4 + 12u_1^2u_2^2
+ u_1^4u_2^2 - 2u_1^2u_2^6 + u_2^8 + a(36u_1^2 - 12u_1^4 - 24u_1^2(-3 + u_1^2))
+ 36u_2^4 + 72u_1^2u_2^2 - 24u_1^4u_2^2 - 12u_1^2u_2^4 + 4u_1^4u_2^4
- 4(-3 + u_1^2)u_2^6 + a^2(-144u_1^2u_2^2 + 36u_1^4u_2^2 + 18u_2^4)
- 36u_1^2u_2^6 + 4u_1^2u_2^6 + 2u_1^4u_2^6 - 2u_2^8 + a^3(36u_1^2u_2^4)
+ 4(-3 + u_1^2)u_2^6 + a^4u_2^8.
\]

Therefore, as long as \(h(u_1, u_2) \neq 0\) and \(g_1/h^2 \notin \mathbb{Z}\) or \(g_2/h^3 \notin \mathbb{Z}\), one sees that \(E_{I', J}\) is of positive Mordell-Weil rank where the point \(Q\) is of infinite order. Since \(C'\) is isomorphic to \(E_{I', J}\), it follows that \(C'\) is also of positive Mordell-Weil rank. Hence, there are infinitely many rational points \((t, z) \in C'(\mathbb{Q})\), each giving rise to a value for \(d\), by substituting in (3.2), therefore a twisted Edwards curve \(E_{a, d}\) possessing the aforementioned rational points. That infinitely many of these curves are pairwise non-isomorphic over \(\mathbb{Q}\) again follows from [8, Proposition 6.1].
Remark 3.2. Since $(0, -1), (0, 1)$ are rational points on any twisted Edwards curve, one can show that if $u_{-1} = -1, u_1 = 1, u_2, u_3$ and $u_4, u_i \neq u_j$ if $i \neq j$, is a sequence in $\mathbb{Z}$, there are infinitely many Edwards curves on which \(u_i, i \in \{-1, 1, 2, 3, 4\}\), are the $y$-coordinates of rational points in $E_{a,d}(\mathbb{Q})$.

4. Huff curves with $S$-sequences of length 5

A Huff curve over a number field $k$ is defined by
\[(4.1) \quad H_{a,b} : ax(y^2 - 1) = by(x^2 - 1),\]
with $a^2 \neq b^2$. Note that the points $(x, y) = (-1, \pm 1), (0, 0), (1, \pm 1)$ are in $H_{a,b}(k)$. We prove that given $s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3 \in k, s_i \neq s_j$ if $i \neq j$, there are infinitely many Huff curves on which these numbers are realized as the $x$-coordinates of rational points.

Assuming $(s_2, p)$ and $(s_3, q)$ are two points on $H_{a,b}$ yields
\[(4.2) \quad as_2(p^2 - 1) = bp(s_2^2 - 1),\]
and
\[(4.3) \quad as_3(q^2 - 1) = bq(s_3^2 - 1),\]
respectively. Using (4.2) and (4.3), one obtains
\[
\frac{s_2(p^2 - 1)}{s_3(q^2 - 1)} = \frac{p(s_2^2 - 1)}{q(s_3^2 - 1)},
\]
therefore, one needs to consider the curve
\[C' : Apq^2 - Ap - Bqp^2 + Bq = 0,\]
where $A = s_3s_2^2 - s_2$ and $B = s_2s_3^2 - s_2$. Dividing both sides of the above equality by $q^2$ gives
\[\frac{A}{q}p - \frac{A}{q}p\frac{1}{q^2} - B\frac{p}{q} + B\frac{1}{q^2} = 0.
\]
Substituting $x = \frac{p}{q}$ and $y = \frac{1}{q^2}$ in the above equation yields the following quadratic curve
\[Ax - Axy - Bx^2 + By = 0,
\]
on which we have the rational point $(x, y) = (1, 1)$. Parametrizing the rational points on the latter quadratic curve gives
\[(4.4) \quad x = \frac{Bt - B}{At + B},
\]
\[(4.5) \quad y = \frac{At(1 - t) + B(1 - t)^2}{At + B}.
\]
Now we have the following result.
Theorem 4.1. Let $s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3, s_m \neq s_n$ if $m \neq n$, be a sequence in $\mathbb{Z}$ such that
\[
h = -4 + A^2 - 3AB + B^2 \neq 0
\]
where $A$ and $B$ are defined as above, and either $g_1/h^2$ or $g_2/h^3$ are not integers, where $g_1, g_2$ are defined in (4.6). There are infinitely many Huff curves described by
\[
H_{a,b} : ax(y^2 - 1) = by(x^2 - 1), \quad a, b \in \mathbb{Q}, \quad a^2 \neq b^2
\]
on which $s_m, -1 \leq m \leq 3$, are the $x$-coordinates of rational points in $H_{a,b}(\mathbb{Q})$. In other words, there are infinitely many Huff curves that possess an $S$-sequence where $S = \{s_i : -1 \leq i \leq 3\}$.

Proof. Using the equalities (4.4) and (4.5), we obtain the following
\[
p^2 = \frac{x^2}{y} = \frac{B^2(-1 + t)}{(B(-1 + t) - At)(B + At)},
\]
\[
q^2 = \frac{1}{y} = \frac{(B + At)}{(-1 + t)(B(-1 + t) - At)}.
\]
In both cases we need $(B + At)(-1 + t)(B(-1 + t) - At)$ to be a square or in other words we need $t$ to be the $x$-coordinate of a rational point on the elliptic curve $C''$ defined by
\[
z^2 = (At + B)(t - 1)(t(B - A) - B),
\]
with the following $k$-rational point $(t, z) = (0, B)$. The latter curve can be described by the following equation
\[
Y^2 = X^3 + ((B - A)^2 - AB)X^2 - 2AB(B - A)^2X + A^2B^2(B - A)^2,
\]
where $A(B - A)t = X$ and $A(B - A)z = Y$. This curve has the rational point $R = (X, Y) = (0, AB(B - A))$.

Observing that
\[
(4.6) \quad 3R = \left( \frac{g_1(A, B)}{h(A, B)^2}, \frac{g_2(A, B)}{h(A, B)^3} \right)
\]
where $h(A, B) = -4 + A^2 - 3AB + B^2$, one concludes as in the proof of Theorem 2.1.

5. General Huff curves with $S$-sequences of length 4

A general Huff curve over a number field $k$ is defined by
\[
G_{a,b} : x(ay^2 - 1) = y(bx^2 - 1),
\]
where $a, b \in k$ and $ab(a - b) \neq 0$. It is clear that the point $(x, y) = (0, 0) \in G_{a,b}(k)$. We show that given $u_0 = 0, u_1, u_2, u_3$ in $k$, $u_i \neq u_j$ if $i \neq j$, there
are infinitely many general Huff curves over which these points are realized as the \( x \)-coordinates of rational points.

We start by assuming that if \( u_1 \) is the \( x \)-coordinates of a point in \( G_{a,b}(k) \), then one must have \( \frac{ay^2 - 1}{y} = \frac{bu_1^2 - 1}{u_1} \) or \( \frac{a - i^2}{i} = \frac{bu_1^2 - 1}{u_1} \) for some \( i \in k \).

Similarly, if \( u_2 \) is the \( x \)-coordinate of a point in \( G_{a,b} \), then one must have

\[
\frac{bu_2^2 - 1}{u_2} \quad \text{or} \quad \frac{a - j^2}{j} = \frac{bu_2^2 - 1}{u_2} \quad \text{for some} \ j \in k.
\]

Thus, one obtains

\[
a = \frac{(bu_1^2 - 1)i + u_1i^2}{u_1} = \frac{(bu_2^2 - 1)j + u_2j^2}{u_2},
\]

which gives the following quadratic curve

\[
S : Ai^2 + Bj^2 + Ciz + Dz = 0,
\]

where \( A = -u_1u_2, \ B = u_1u_2, \ C = -u_1^2u_2b + u_2, \ D = bu_1u_2^2 - u_1 \). Then consider the line

\[
mP + nQ = (np : nq : m + nr)
\]

connecting the rational points \( P = (i : j : z) = (0 : 0 : 1) \) and \( Q = (p : q : r) \) lying on \( S \subset \mathbb{P}^2 \). The intersection of \( S \) and \( mP + nQ \) yields the quadratic equation

\[
n^2(Ap^2 + Bq^2 + Cpr + Dqr) + mn(Cp + Dq) = 0.
\]

Using \( P \) and \( Q \) lying on \( S \), one solves this quadratic equation and obtains formulae for the solution \((i : j : z)\) with the following parametrization:

\[
i = np = Cp^2 + Dpq, \quad j = nq = Cpq + Dq^2, \quad z = m + nr = -Ap^2 - Bq^2.
\]

Now we obtain the following result.

**Theorem 5.1.** Let \( u_0 = 0, u_1, u_2 \) and \( u_3 \), \( u_i \neq u_j \) if \( i \neq j \), be a sequence in \( k \). There are infinitely many general Huff curves described by

\[
G_{a,b} : x(ay^2 - 1) = y(bx^2 - 1), \quad a, b \in k, \ ab(a - b) \neq 0.
\]

on which \( u_i, 0 \leq i \leq 3 \), are the \( x \)-coordinates of rational points in \( G_{a,b}(k) \).

In other words, there are infinitely many general Huff curves that possess an \( S \)-sequence where \( S = \{u_i : 0 \leq i \leq 3\} \).

**Proof.** Substituting the value for \( i \) in \( a = \frac{(bu_1^2 - 1)i + u_1i^2}{u_1} \) yields that

\[
a = u_2^2 \left( bu_1^2 - 1 \right)^2 p^4 - 2u_1u_2 \left( bu_2^2 - 1 \right) \left( bu_1^2 - 1 \right) p^2 q
\]

\[
+ u_1^2 \left( bu_2^2 - 1 \right)^2 p^2 q^2 - \frac{u_2 \left( bu_1^2 - 1 \right)^2}{u_1} p^2 + \left( bu_2^2 - 1 \right) \left( bu_1^2 - 1 \right) pq.
\]
Now we assume that \((u_3, \ell) \in G_{a,b}(k)\). This yields that
\[
pu_3 (b^2 u_1^3 u_2 - bpqu_1^2 u_2 - p^2 u_1 u_2 + pqu_1^2 - bu_1^2 + 1) \\
(bpu_1^2 u_2 - bpu_1 u_2 - pu_2 + qu_1) \ell^2 - u_1 (bu_3^2 - 1) \ell - u_1 u_3 = 0.
\]
This can be rewritten as
\[
Z^2(b^2 p^4 u_1^5 u_2^3 - 2bp^4 u_1^3 u_2^2 u_3 - b^2 p^2 u_1^2 u_2 u_3 + p^3 u_1 u_2^2 u_3 + 2bp^2 u_1^2 u_2 u_3 \\
-p^2 u_2 u_3 + qZ(-2bp^3 u_1^4 u_2^2 u_3 + 2bp^3 u_1^2 u_2 u_3 + 2bp^2 u_1^2 u_2 u_3 + b^2 pu_1^3 u_2^2 u_3 \\
- 2p^3 u_1^2 u_2 u_3 - bpqu_1^2 u_3 - bpqu_1 u_2^2 u_3 + pu_1 u_3) + q^2 p^2 u_1^3 u_3 (bu_2^2 - 1)^2 \\
- T Zu_1 (bu_3^2 - 1) - T^2 u_1 u_3 = 0,
\]
where \(T = 1/\ell\). One sees that the rational point \(P = (q : T : Z) = (1 : 0 : u_1(-1 + bu_2^2)/pu_2(-1 + bu_1^2))\) lies on the quadratic curve above, hence we may parametrize the rational points on the quadratic curve above. This is obtained by considering the intersection of the line \(dP + eQ\) where \(Q = (q_1 : q_2 : q_3)\) is a point on the quadratic curve. In fact, this yields that
\[
d = pu_2(bu_1^2 - 1)(q_3 b^2 p^4 u_1^5 u_2^2 u_3 - 2q_3 b^2 p^4 u_1^3 u_2^2 u_3 \\
- q_3^2 b^2 p^2 u_1^4 u_2 u_3 + q_3^2 p^4 u_1 u_2^2 u_3 + 2q_3^2 b^2 u_1^2 u_2 u_3 \\
- q_3 b^2 p^2 u_2 u_3 - u_1 q_3 b u_3^2 + u_1 q_3 u_3 + p^2 u_1^3 u_3^2 b^2 u_2^4 \\
- 2p^3 u_1^3 u_3 q_1^2 u_2^2 - p^2 u_1^3 u_3 q_1 - 2q_1 q_3^2 b^2 p^3 u_1^4 u_2^3 u_3 \\
+ 2q_1 q_3 b p^3 u_1^4 u_2 u_3 + 2q_1 q_3 b p^2 u_1^2 u_2^2 u_3 + q_1 q_3 b^2 p u_1^3 u_2^2 u_3 \\
- 2q_1 q_3^2 u_1^3 u_2 u_3 - q_1 q_3 b p u_1 u_2^2 u_3 + q_1 q_3 p u_1 u_3 \\
- u_1 u_3 q_2^2),
\]
\[
e = u_1(bu_2^2 - 1)(-pu_1^3 u_3 q_1 b^2 u_2^2 + p^2 u_3^2 u_3 b^2 u_1^4 + pu_1 u_3 q_1 bu_2^2 \\
- 2p^2 u_3 q_u u_2 u_1^2 + pu_1^3 u_3 q_1 b + u_1 q_2 bu_2 + p^2 u_3 q u_2 - u_1 q_2 - pu_1 u_3 q_1).
\]

**Acknowledgements.**

We would like to thank the referees for carefully reading our manuscript and for giving such constructive comments which substantially helped improving the presentation of the paper.

**References**


G. S. Çelik
Department of Mathematics
Bursa Uludağ University
16059 Bursa
Turkey
E-mail: gamzesavascelik@gmail.com

M. Sadek
Faculty of Engineering and Natural Sciences
Sabancı University
34956 Tuzla, Istanbul
Turkey
E-mail: mmsadek@sabanciuniv.edu

G. Soydan
Department of Mathematics
Bursa Uludağ University
16059 Bursa
Turkey
E-mail: gsoydan@uludag.edu.tr

Received: 22.9.2018.
Revised: 5.3.2019.