RATIONAL POINTS IN GEOMETRIC PROGRESSION ON THE UNIT CIRCLE

GAMZE SAVAŞ ÇELİK, MOHAMMAD SADEK AND GÖKHAN SOYDAN

Abstract. A sequence of rational points on an algebraic planar curve is said to form an r-geometric progression sequence if either the abscissae or the ordinates of these points form a geometric progression sequence with ratio r. In this work, we prove the existence of infinitely many rational numbers r such that for each r there exist infinitely many r-geometric progression sequences on the unit circle \( x^2 + y^2 = 1 \) of length at least 3.

1. Introduction

In the past 30 years, several mathematicians have been interested in whether the \( x \)-coordinates (or \( y \)-coordinates) of rational points on various families of algebraic plane curves over the rational field \( \mathbb{Q} \) form a sequence of rational numbers which is either an arithmetic or a geometric progression sequence. In 1992, Lee and Vélez, [18], proved that for infinitely many rational values \( a \) the curve \( y^2 = x^3 + a \) possesses a sequence of rational points whose \( x \)-coordinates form an arithmetic progression sequence of length at least 4. Seven years later, Bremner, [6], discussed arithmetic progression sequences on other families of elliptic curves over \( \mathbb{Q} \). He investigated the size of these sequences and produced elliptic curves with 7-term and 8-term arithmetic progression sequences. The problem of finding rational points in arithmetic progression on elliptic curves, hyperelliptic curves and different models of elliptic curves including Edwards and Huff curves has been explored extensively, [2, 7, 9, 10, 19–24].

In 2013, the first work on geometric progression sequences was introduced by Bremner and Ulas, [8]. For any non-trivial four term geometric progression \( x_i, i = 1, 2, 3, 4 \), they first proved that there exist infinitely many pairwise non-isomorphic hyperelliptic curves \( C : y^2 = ax^n + b \) such that \( x_i \) is the \( x \)-coordinate of a rational point on \( C \). Secondly, they showed that there exist infinitely many parabolas \( y^2 = ax + b \) which contain five points in geometric progression. Three years later, Alaa and Sadek, [1], found a family of hyperelliptic curves defined by the equation \( y^2 = ax^{2n} + bx^n + a, a, b \in \mathbb{Z} \), such that this family possesses a geometric progression sequence of rational points whose length is at least 8. In 2017, Ciss and Moody, [13], considered long geometric progressions on different models of elliptic curves, including Weierstrass curves, Edwards curves, Huff curves and quartic curves. They presented infinite families of (twisted) Edwards curves, and Huff curves containing five rational points in geometric progression, an infinite family of Weierstrass
curves containing eight points in progression, as well as an infinite family of quartic curves with 10-term progression sequences. Given an arbitrary sequence of rational points of length 4, 5, or 6, Çelik, Sadek and Soydan, [15], provided explicit examples of (twisted) Edwards curves and (general) Huff curves on which this sequence is realized as the \( x \)-coordinate of rational points.

Arithmetic and geometric progression sequences have also been studied on conics. In 2013, Alvarado and Goins, [3], gave a generalization of 3-term arithmetic progressions on an arbitrary conic section. Three years later, Choudhry and Juyal, [11], parameterized infinitely many arithmetic progressions of three rational points on the unit circle, such that the three points lie in the first quadrant. They also used these progressions to derive infinitely many arithmetic progressions on the ellipse \( x^2/a^2 + y^2/b^2 = 1 \). Recently, Ciss and Moody, [12], considered long arithmetic progressions on conics. They gave a slightly more general result on 3-term arithmetic progressions on the unit circle \( x^2 + y^2 = 1 \), and similarly on the unit hyperbola \( x^2 - y^2 = 1 \). They also provided infinitely many conics \( ax^2 + cy^2 = 1 \) that have 8-term arithmetic progression sequences.

In the present work, we investigate sequences of rational points in geometric progression on the unit circle. We prove the existence of infinitely many rational numbers \( r \) such that for each \( r \), there exist geometric progression sequences of rational points on the unit circle \( x^2 + y^2 = 1 \) with ratio \( r \) and length at least 3. This will be accomplished by analyzing the arithmetic of several rational elliptic surfaces. In addition, we prove that there are infinitely many rational points \( P \) on the unit circle such that \( P \) is a term in infinitely many geometric progression sequences of length at least 3.

2. GEOMETRIC PROGRESSION SEQUENCES OF LENGTH 2 ON THE UNIT CIRCLE

Let \( C \) be the unit circle \( x^2 + y^2 = 1 \). The set \( C(K) \) of \( K \)-rational points on \( C \) is defined by \( C(\mathbb{Q}) = \{(x, y) : x^2 + y^2 = 1, x, y \in \mathbb{Q} \} \).

A sequence of rational points \((x_1, y_1), \ldots, (x_n, y_n)\) in \( C(\mathbb{Q}) \) will be said to form an \( r \)-geometric progression sequence of length \( n \) if \( x_i/x_{i-1} = r \) for every \( i = 2, \ldots, n \).

**Lemma 2.1.** Let \( r = \frac{-4m}{m^2 + 2} \) where \( m \in \mathbb{Q} \). There exists infinitely many pairs of rational points \((x_1, y_1), (x_2, y_2) \in C(\mathbb{Q})\) such that \( x_2/x_1 = r \). In particular, there are infinitely many \( r \)-geometric progression sequences of length 2.

**Proof:** Let \((x_1, y_1)\) and \((rx_1, y_2)\) be such that \( x_1^2 + y_1^2 = 1 \) and \((rx_1)^2 + y_2^2 = 1 \). We consider the following intersection of two quadratic surfaces in \( \mathbb{P}^3 \):

\[
H_r : x_1^2 + y_1^2 = z^2, \quad r^2x_1^2 + y_2^2 = z^2.
\]

One may check using MAGMA [5] that the latter curve is an elliptic curve that may be described by the following Weierstrass equation

\[
E_r : y^2 = x(x-4)(x-4r^2).
\]

A full description of the birational isomorphism \( \phi_r : E_r \to H_r \) between the two curves can be found for example in [4, Theorem 3.1]. Choosing \( x = 2r^2 \) yields that \( y^2 = -8(r^2-2)r^4 \). If \((r_0, s_0)\) is a point on the conic \( Q : s^2 + 2r^2 = 4 \), then \( P_0 = (x(P_0), y(P_0)) = (2r_0^2, 2r_0^2s_0) \in E_{r_0}(\mathbb{Q}) \) is a point of infinite
order. Since the conic $Q$ possesses one rational point $(r, s) = (0, 2)$, it contains infinitely many rational points whose parametrization is given by $(r, s) = \left(-4m/(m^2 + 2), 2(m^2 - 2)/(m^2 + 2)\right)$. Setting $mP_0$ to be the $m$-th multiple of $P_0$, then $Q_m := \phi_r(mP_0) := (x_1, y_1, y_2, z) \in H_r(Q)$ where $x_1$ and $x_2 = rx_1$ are the $x$-coordinates of rational points forming an $r$-geometric sequence in $C(Q)$. This proves the statement.

In fact, the lemma above can be strengthened as follows:

**Proposition 2.2.** There are infinitely many rational numbers $r$ such that for each such $r$, there exists infinitely many pairs of rational points $(x_1, y_1), (x_2, y_2) \in C(Q)$ with $x_2/x_1 = r^2$.

**Proof:** To guarantee the existence of such rational number $r$, one has

$$x_1 = \frac{2s}{1 + s^2}, \quad x_2 = \frac{2t}{1 + t^2} = r^2 \frac{2s}{1 + s^2}.$$ 

In other words, the existence of such pair yields a rational point on the following planar curve

$$E_r : t(s^2 + 1) = r^2 s(t^2 + 1).$$

The curve $E_r$ is a twisted Huff curve, see [17]. In particular, the above equation describes an elliptic curve whose Weierstrass equation is

$$E'_r : y^2 = x(x - 1)(x - r^4).$$

The curves $E_r$ and $E'_r$ are birationally isomorphic via the following transformations

$$(x, y) = (-r^2(r^2t - s)/(-t + r^2s), -r^2(r^4 - 1)/(-t + r^2s)), \quad (s, t) = ((x - r^4)/y, r^2(x - 1)/y),$$

see [17] §3.3 for details. The above Weierstrass equation $E'_r$ is a Legendre equation, and the torsion group of the curve contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Fix $u \in \mathbb{Q} \setminus \{0, 1\}$. Setting $x = u^4$, we have $y^2 = u^4(u^4 - 1)(u^4 - r^4)$. Setting $w = y/u^2$, one obtains the quartic elliptic curve

$$H : w^2 = -(u^4 - 1)r^4 + (u^4 - 1)u^4.$$ 

The point $P = (r, w) = (1, u^4 - 1)$ is a point of infinite order on the curve $H$. In conclusion, there are infinitely many $r$ such that

$$(x, y) = (u^4, u^2(u^4 - 1)) \in E'_r(Q) \quad \text{is a point of infinite order.}$$

More precisely, if we choose $r$ to be the $r$-coordinate of $mP, m \neq \pm 1$, in $H(Q)$, then $E_r$ is a curve of positive rank. A point of infinite order may be found on the latter curve by using the transformation in [17] to find the image of $(u^4, u^2(u^4 - 1))$ in $E_r(Q)$.

**Example 1.** In this example we produce three pairs of rational points on the unit circle that form $r^2$-geometric progression sequences when $r = 5/4$. For $(s, t) = (8, 1/5)$, we find the points $(x_1, y_1) = (16/65, 63/65))$ and $(x_2, y_2) = (5/13, 12/13)$. For $(s, t) = (64/273, 21/52)$, we obtain the pair $(34944/78625, 70433/78625)$ and $(2184/3145, 2263/3145)$. When $(s, t) = (37523/119144, 67159/41605)$, we get the following pair of rational points $(9841280624/15603268265, 12787317207/15603268265)$, $(2794150195/3120653653, 1389677628/3120653653)$ on the unit circle.
We recall that the three points \((s, t)\) above are rational points on the curve \(E_{5/4}\) in the proof of Proposition 2.2. Moreover, the images of these three rational points in the elliptic curve described by the Weierstrass equation \(E'_{5/4}\) are \((125/128, 375/2048)\), \((4225/256, 61425/1024)\) and \((351125/114242, 876825375/436861408)\), respectively.

Remark 2.3. The rational values \(r\) are parametrized by rational points on a conic in Lemma 2.1, whereas the rational values \(r\) are parametrized by rational points on an elliptic curve of positive rank in Proposition 2.2.

3. Geometric progression sequences of length 3 on the unit circle

Assume that the points \((x_1, y_1) = (u/r, f), (x_2, y_2) = (u, g), (x_3, y_3) = (ur, h)\) are in \(C(\mathbb{Q})\) where \(C: x^2 + y^2 = 1\). Set

\[
(1) \quad (u/r, f) = \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right), \quad (u, g) = \left(\frac{2s}{1+s^2}, \frac{1-s^2}{1+s^2}\right),
\]

so that \(r = \frac{2s}{1+s^2} \cdot \frac{1+t^2}{2t}\). Now, the fact that \((x_3, y_3) \in C(\mathbb{Q})\) is equivalent to the following condition

\[
h^2 = 1 - \left(\frac{2s}{1+s^2}\right)^4 \cdot \left(\frac{1+t^2}{2t}\right)^2.
\]

Equivalently, one has

\[
(2) \quad t^2(s^2 + 1)^4 - 4s^4(t^2 + 1)^2 = H^2,
\]

where \(H = h(s^2 + 1)^2t\). The curve \(2\) is a quartic elliptic curve over \(\mathbb{Q}(s)\), with the \(\mathbb{Q}(s)\)-rational point \((t, H) = (s, s^5 - s)\). It can be described by the Weierstrass equation

\[
(3) \quad E_s : y^2 = x(x + 16s^4)(x + (1 + s^2)^4),
\]

and its torsion group is \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\), see for example \[16\] §2.

Now we give the main result:

Theorem 3.1. There are infinitely many rational numbers \(r\) such that for each \(r\) there is an \(r\)-geometric progression sequence of length at least 3 on the unit circle \(x^2 + y^2 = 1\).

Proof. The above discussion asserts that one only needs to find infinitely many rational values for \(s\) such that \(E_s\) has positive rank over \(\mathbb{Q}\).

If \(x = 8s^3(1 + s^2)\) is the \(x\)-coordinate of a rational point on \(E_s\), then \(s^4 - 2s^3 + 6s^2 - 2s + 1\) must be a rational square. In other words, one will get a rational point on the quartic elliptic curve

\[
w^2 = s^4 - 2s^3 + 6s^2 - 2s + 1
\]
which possesses the $\mathbb{Q}$-rational point $(s, w) = (0, \pm 1)$. Using the procedure in [14, chapter 3, pp. 89-91], we see that the latter quartic curve is birationally equivalent to the elliptic curve defined by the Weierstrass equation

$$G : v^2 = u^3 - 972u$$

and the point $(u, v) = (-27, 81) \in G(\mathbb{Q})$ is a point of infinite order. In fact, one can check using MAGMA [5] that $\text{rank}(G(\mathbb{Q})) = 1$. This completes the proof.

The following corollary follows from the proof above.

**Corollary 3.2.** There are infinitely many rational numbers $s$ such that the point $\left(\frac{2s}{1 + s^2}, \frac{1 - s^2}{1 + s^2}\right) \in C(\mathbb{Q})$ lies in infinitely many geometric progression sequences on $C$ of length at least 3.

In the following table we give examples of geometric progression sequences of length at least 3 in $C(\mathbb{Q})$.

| $(r, s, t)$                | $(x_1, x_2, x_3)$                      |
|---------------------------|----------------------------------------|
| $\left(\frac{39}{25}, 3, 5\right)$ | $\left(\frac{5}{13}, 3/5, 117/125\right)$ |
| $\left(\frac{6409}{3034}, 4, 328/37\right)$ | $\left(\frac{24272}{108953}, 8/17, 1508/1517\right)$ |
| $\left(\frac{5987825}{3616561}, 5, 1537/181\right)$ | $\left(\frac{278197}{1197565}, 5/13, 29939125/47015293\right)$ |
| $\left(\frac{55045}{24531}, 6, 234/17\right)$ | $\left(\frac{7956}{55045}, 12/37, 220180/302549\right)$ |
| $\left(\frac{7935762913}{2225017375}, 7, 125885/4949\right)$ | $\left(\frac{623004865}{7935762913}, 7/25, 7935762913/7946490625\right)$ |
| $\left(\frac{6548713889}{6051759025}, 8, 80392/9265\right)$ | $\left(\frac{1489663760}{6548713889}, 16/65, 104779422224/393364336625\right)$ |

**Table 1.**

One notices that if $ur^2$ is the $x$-coordinate of a rational point on the unit circle in Theorem 3.1 then this implies the existence of an $r$-geometric progression sequence of length at least 4. However, this will require studying rational solutions of the following system of Diophantine equations:

\[
t^2(s^2 + 1)^4 - 4s^4(t^2 + 1)^2 = H_1^2 \\
t^4(s^2 + 1)^6 - 4s^6(t^2 + 1)^4 = H_2^2.
\]

The authors intend to study the above system of equations. Moreover, they will tackle the question of the existence of geometric progression sequences on planar conics in future work.

4. **Acknowledgements**

We are grateful to the anonymous referee for many valuable suggestions and useful comments. We would also like to thank Professors Andrew Bremner, Andrej Dujella and Allan J. Macleod for their usefull ideas. The first and third authors were supported by the Research Fund of Bursa Uludağ University under Project No: F-2020/8.


References

[1] M. Alaa, M. Sadek, On geometric progressions on hyperelliptic curves, *J. Integer Seq.* 19 (2016), Article 16.6.3.

[2] A. Alvarado, An arithmetic progression on quintic curves, *ibid.* 12 (2009), Article 09.7.3.

[3] A. Alvarado, E. H. Goins, Arithmetic progressions on conic sections, *Int J Number Theory* 9 (2013), 1379–1393.

[4] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum, A.R. Perlis, Jacobians of genus one curves, *Journal of Number Theory* 90 (2001), no. 2, 304–315.

[5] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra System I. The user language, *J. Symbolic Comput.* 24 (1997), no. 3-4, 235–265.

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

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

[8] A. Bremner, M. Ulas, Rational points in geometric progressions on certain hyperelliptic curves, *Publ. Math. Deb.* 82 (2013), 669–683.

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

[10] A. Choudhry, Arithmetic progressions on Huff curves, *ibid.* 18 (2015), Article 15.5.2.

[11] A. Choudhry, A. Juval, Rational points in arithmetic progression on the unit circle, *ibid.* 19 (2016), Article 16.4.1.

[12] A. A. Ciss, D. Moody, Arithmetic progressions on conics, *ibid.* 20 (2017), Article 17.2.6.

[13] A. A. Ciss, D. Moody, Geometric progressions on elliptic curves, *Glasnik Math.* 52 (2017), 1–10.

[14] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press., 2nd ed., (1997).

[15] G. S. Çelik, M. Sadek and G. Soydan, Rational sequences on different models of elliptic curves, *Glasnik Math.* 54 (2019), 53–64.

[16] A. Dujella, J. C. Peral, High-rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples, *LMS J. Comput. Math.* 17 (1) (2014) 282–288.

[17] M. Joye, M. Tibouchi, D. Vergnaud, Huff’s Model for Elliptic Curves. *Algorithmic Number Theory-ANTS-IX*, Lecture Notes in Computer Science, 6197 (2010), Springer, 234–250.

[18] J. B. Lee, W. Y. Vélez, Integral solutions in arithmetic progression for $y^2 = x^3 + k$, *Per. Math. Hung.* 25 (1992), 31–49.

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

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

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

[22] I. Garcia-Selfa, J. Tornero, Searching for simultaneous arithmetic progressions on elliptic curves, *Bull. Austral. Math. Soc.* 71 (2005), 417–424.

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

[24] M. Ulas, On arithmetic progressions on genus two curves, *Rocky Mountain J. Math.* 39 (2009), 971–980.

Gamze Savaş Çelik. Department of Mathematics, Bursa Uludağ University, Görükle Campus, 16059 Bursa, Turkey

Email address: gamzesavascelik@gmail.com

Mohammad Sadek. Faculty of Engineering and Natural Sciences, Sabanci University, 34956 Tuzla, Istanbul, Turkey

Email address: mmsadek@sabanciuniv.edu
Gökhan Soydan, Department of Mathematics, Bursa Uludağ University, Görükle Campus, 16059 Bursa, Turkey

Email address: gsoydan@uludag.edu.tr