Journal of Integer Sequences, Vol. 19 (2016),
Article 16.4.1

Rational Points in Arithmetic Progression on the Unit Circle

Ajai Choudhry
13/4 A Clay Square
Lucknow - 226001
India
ajaic203@yahoo.com

Abhishek Juyal
Department of Mathematics
Motilal Nehru National Institute of Technology
Allahabad - 211004
India
abhinfo1402@gmail.com

Abstract

Several authors have considered the problem of finding rational points $(x_i, y_i), i = 1, 2, \ldots, n$ on various curves $f(x, y) = 0$, including conics, elliptic curves and hyperelliptic curves, such that the x-coordinates $x_i, i = 1, 2, \ldots, n$ are in arithmetic progression. In this paper we find infinitely many sets of three points, in parametric terms, on the unit circle $x^2 + y^2 = 1$ such that the x-coordinates of the three points are in arithmetic progression. It is an open problem whether there exist four rational points on the unit circle such that their x-coordinates are in arithmetic progression.

1 Introduction

A sequence of rational points $(x_i, y_i), i = 1, 2, \ldots, n$ lying on a curve $f(x, y) = 0$ is said to be in arithmetic progression if the x-coordinates $x_i, i = 1, 2, \ldots, n$ are in arithmetic progression.

The problem of finding rational points in arithmetic progression on conics, elliptic curves and hyperelliptic curves has been extensively studied by several mathematicians [1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15].

This paper is concerned with finding rational points in arithmetic progression on the unit circle defined by the equation,

$$x^2 + y^2 = 1. \tag{1}$$

This problem does not appear to have been discussed in the existing literature, and the general result concerning arithmetic progressions on conic sections contained in [3] seems to be of little help in solving the problem.

It is obvious that the three points, $(-1, 0), (0, 1)$, and $(1, 0)$, lying on the unit circle (1) are in arithmetic progression. In general, if (x_1, y_1) is any rational point on the unit circle, the three points, $(-x_1, y_1), (0, 1)$, and (x_1, y_1), lie on the unit circle and their x-coordinates are in arithmetic progression. However, in all these examples, only one of the three points lies in the first quadrant.

In this paper we will obtain, in parametric terms, infinitely many arithmetic progressions of three rational points on the unit circle such that all of the three points lie in the first quadrant. We use these arithmetic progressions to find infinitely many arithmetic progressions of three rational points on the ellipse,

$$X^2/a^2 + Y^2/b^2 = 1, \tag{2}$$

where a and b are positive rational numbers.

We also consider the problem of finding four rational points in arithmetic progression on the unit circle. We prove that for any rational point (x_1, y_1) lying on the unit circle, the arithmetic progression consisting of the three rational points, $(-x_1, y_1), (0, 1)$ and (x_1, y_1), cannot be extended to an arithmetic progression of four rational points. Further, we show that there is no arithmetic progression of four rational points of the type, $(-3x_1, y_2), (-x_1, y_1), (x_1, y_1)$ and $(3x_1, y_2)$, on the unit circle. The problem of finding four rational points in arithmetic progression on the unit circle, however, remains open.

2 Three rational points in arithmetic progression on the unit circle

We assume that there exist three rational points P_1, P_2 and P_3 in arithmetic progression on the unit circle (1) with their coordinates being given by $(u - v, y_1), (u, y_2)$ and $(u + v, y_3)$ respectively. As these points lie on the circle (1), we have,

$$(u - v)^2 + y_1^2 = 1, \tag{3}$$

$$u^2 + y_2^2 = 1, \tag{4}$$

$$(u + v)^2 + y_3^2 = 1. \tag{5}$$

It is easily seen that for the three points to be in the first quadrant and have distinct x-coordinates, we must have

$$uv(u^2 - v^2) \neq 0 \quad \text{and} \quad (y_1^2 - y_2^2)(y_2^2 - y_3^2)(y_3^2 - y_1^2) \neq 0. \tag{6}$$

Taking the difference of the Eqs. (3) and (4), we get, after suitable transpositions, the equation,

$$v(2u - v) = (y_1 - y_2)(y_1 + y_2), \tag{7}$$

while, taking the difference of the Eqs. (4) and (5), we get, after suitable transpositions, the equation,

$$v(2u + v) = (y_2 - y_3)(y_2 + y_3). \tag{8}$$

Under the conditions (6), Eqs. (7) and (8) are solvable if and only if there exist nonzero rational numbers m and n such that,

$$\begin{aligned} v &= m(y_1 - y_2), \qquad & m(2u - v) &= y_1 + y_2, \\ v &= n(y_2 - y_3), \qquad & n(2u + v) &= y_2 + y_3. \end{aligned} \tag{9}$$

Now (9) may be considered as four linear equations in five variables u, v, y_1, y_2 and y_3, and are therefore readily solved. We thus get the following solution of (9):

$$\begin{aligned} u &= r(m + n)(mn + 1), & v &= 2r(m - n)mn, \\ y_1 &= r(2m^2n^2 + m^2 + 2mn - n^2), & y_2 &= r(2m^2n^2 + m^2 + n^2), \\ y_3 &= r(2m^2n^2 - m^2 + 2mn + n^2), \end{aligned} \tag{10}$$

where r is an arbitrary parameter.

We now substitute the values of u and y_2 given by (10) in Eq. (4), and thus get,

$$(n^2 + 1)(m^2 + 1)(4m^2n^2 + m^2 + 2mn + n^2)r^2 = 1, \tag{11}$$

which, on writing,

$$n = 2t/(t^2 - 1), \tag{12}$$

$$r = (t^2 - 1)^2/(s(t^2 + 1)), \tag{13}$$

may be written as,

$$s^2 = (t^4 + 14t^2 + 1)m^4 + 4(t^3 - t)m^3 + (t^4 + 18t^2 + 1)m^2 + 4(t^3 - t)m + 4t^2. \tag{14}$$

The right-hand side of Eq. (14) may be considered as a quartic function of m, and it has to be made a perfect square. A method of making a quartic function a perfect square has been described by Fermat [10, p. 639] and, on applying this method, we get the following solution of equation (14):

$$m = 6t(t^2 - 1)/(t^4 - 11t^2 + 1), \tag{15}$$

$$s = 2t(t^4 + 7t^2 + 1)(4t^4 + t^2 + 4)/(t^4 - 11t^2 + 1)^2. \tag{16}$$

With the value of s given by (16), we get, on using (13),

$$r = (t^6 - 12t^4 + 12t^2 - 1)^2/2t(t^4 + 7t^2 + 1)(4t^4 + t^2 + 4)(t^2 + 1), \tag{17}$$

and a solution of Eqs. (3), (4) and (5) is given by (10) where the values of m, n and r are given, in terms of an arbitrary parameter t, by (12), (15) and (17).

We thus get the desired set of three rational points, P_1, P_2, and P_3, whose x-coordinates, in terms of the arbitrary parameter t, are given below explicitly:

$$\begin{aligned} &(4t^{10} - 65t^8 - 68t^6 + 68t^4 + 65t^2 - 4)/f(t), \\ &(4t^{10} - 17t^8 + 4t^6 - 4t^4 + 17t^2 - 4)/f(t), \\ &(4t^{10} + 31t^8 + 76t^6 - 76t^4 - 31t^2 - 4)/f(t), \end{aligned} \tag{18}$$

where $f(t) = (t^2 + 1)(t^4 + 7t^2 + 1)(4t^4 + t^2 + 4)$.

It is easily seen that when $t > 4.145$, the x-coordinates of all the three points are positive. As a numerical example, taking $t = 5$, we get the following three rational points which lie on the unit circle and whose x-coordinates are in arithmetic progression:

$$\begin{gathered} (78108/325117, 315595/325117), \quad (200508/325117, 255925/325117) \\ \text{and} \quad (322908/325117, 37835/325117). \end{gathered}$$

We have already found one value of m, given by (15), which makes the quartic function on the right-hand side of Eq. (14) a perfect square. Using this known value of m, we can repeatedly apply the aforementioned method of Fermat to find infinitely many values of m (in terms of the parameter t) that make the right-hand side of Eq. (14) a perfect square, and we can thus find infinitely many parametric solutions of the system of Eqs. (3), (4) and (5). We thus obtain infinitely many sets of three points, in terms of an arbitrary parameter, whose x-coordinates are in arithmetic progression, and such that the three points lie on the unit circle.

We also note that there is a one-to-one correspondence between rational points (x, y) on the unit circle (1) and the rational points on the ellipse (2) given by $\phi(x, y) = (ax, by)$. As we have already found infinitely many sets of three rational points, P_1, P_2 and P_3, in arithmetic progression on the unit circle (1) with all three points having positive x-coordinates, the images of these points, $\phi(P_1), \phi(P_2)$, and $\phi(P_3)$, on the ellipse (2) immediately yield infinitely many sets of three rational points in arithmetic progression on the ellipse (2) with all the three points $\phi(P_1), \phi(P_2)$, and $\phi(P_3)$ having positive x-coordinates.

3 Four rational points in arithmetic progression on the unit circle

We now explore the possibility of finding four rational points in arithmetic progression on the unit circle (1).

We have noted in the introduction that if (x_1, y_1) is any arbitrary rational point on the unit circle, the three points, $(-x_1, y_1), (0, 1)$ and (x_1, y_1), on the unit circle are in arithmetic progression. We now show that this sequence of rational points cannot be extended to a longer sequence of rational points whose x-coordinates are in arithmetic progression. Assuming this is possible, there must be a rational point on the unit circle whose x-coordinate is $2x_1$ or $-2x_1$. In either case, the following two diophantine equations must be satisfied:

$$x_1^2 + y_1^2 = 1, \tag{19}$$
$$4x_1^2 + y_2^2 = 1, \tag{20}$$

It is well-known that the complete solution of equation (19) is given by,

$$x_1 = 2t/(1 + t^2), \quad y_1 = (1 - t^2)/(1 + t^2), \tag{21}$$

where t is an arbitrary parameter. Substituting the value of x_1 given by (21) in Eq. (20), we get, after suitable transpositions, the equation,

$$y_2^2(t^2 + 1)^2 - t^4 + 14t^2 - 1 = 0. \tag{22}$$

The birational transformation given by,

$$t = (X - 2)/Y, \quad y_2 = (X^3 - 6X^2 + 16)/(X^2 + Y^2 - 4X + 4), \tag{23}$$

and

$$X = (t^2y_2 - 3t^2 + y_2 + 1)/(2t^2), \quad Y = (t^2y_2 - 7t^2 + y_2 + 1)/(2t^3), \tag{24}$$

transforms Eq. (22) to the cubic equation,

$$Y^2 = X^3 + X^2 - 4X - 4. \tag{25}$$

Now equation (25) represents an elliptic curve and a reference to Cremona's well-known tables of elliptic curves [9] shows that the rank of the elliptic curve (25) is 0. Further, the torsion points of the curve (25) yield only the trivial solutions of equations (19) and (20), namely $(x_1, y_1, y_2) = (0, \pm1, \pm1)$. As there are no nontorsion rational points on the curve (25), it follows that Eqs. (19) and (20) do not have any nontrivial solutions. Thus the sequence of three points $(-x_1, y_1), (0, 1), (x_1, y_1)$ on the unit circle (1) cannot be extended to a longer sequence of rational points whose x-coordinates are in arithmetic progression.

Next we consider whether there exists an arithmetic progression, on the unit circle (1), of four rational points of the type $(\pm x_1, y_1), (\pm 3x_1, y_2)$. For four such rational points to lie on the unit circle, we must have,

$$x_1^2 + y_1^2 = 1, \tag{26}$$
$$9x_1^2 + y_2^2 = 1. \tag{27}$$

Proceeding as in the case of Eqs. (19) and (20), we find that the diophantine Eqs. (26) and (27) lead to the elliptic curve,

$$Y^2 = X^3 - X^2 - 24X - 36, \tag{28}$$

which is also of rank 0, and we conclude, as before, that there is no arithmetic progression, on the unit circle (1), of four rational points of the type $(\pm x_1, y_1), (\pm 3x_1, y_2)$.

Limited trials, conducted to check whether the arithmetic progression of three rational points whose x-coordinates are given by (18) can be extended to an arithmetic progression of four rational points, did not yield any positive result.

It still remains an open problem whether there exists a sequence of four rational points in arithmetic progression on the unit circle.

4 Acknowledgments

The first author thanks the Harish-Chandra Research Institute, Allahabad for providing him with all necessary facilities that have helped him to pursue his research work in mathematics. The second author thanks his supervisors Prof. Shiv Datt Kumar and Prof. Kalyan Chakraborty for their support and also the Harish-Chandra Research Institute, where he is visiting, for its hospitality and support.

References

[1] A. Alvarado, An arithmetic progression on quintic curves, *J. Integer Sequences* **12** (2009), Article 09.7.3.

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

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

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

[5] A. Bremner, On square values of quadratics, *Acta Arith.* **108** (2003), 95–111.

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

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

[8] A. Choudhry, Arithmetic progressions on Huff curves, *J. Integer Sequences* **18** (2015), Article 15.5.2.

[9] J. E. Cremona, Elliptic curve data. Available at `http://johncremona.github.io/ecdata/`.

[10] L. E. Dickson, *History of the Theory of Numbers,* Vol. 2, Chelsea Publishing Company, 1992, reprint.

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

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

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

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

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

2010 *Mathematics Subject Classification*: 11D09.
Keywords: arithmetic progression, unit circle.

Received December 10 2015; revised version received March 14 2016. Published in *Journal of Integer Sequences*, April 7 2016.

Return to Journal of Integer Sequences home page.