Journal of Integer Sequences, Vol. 20 (2017),
Article 17.2.6

Arithmetic Progressions on Conics

Abdoul Aziz Ciss
Laboratoire de Traitement de l'Information et Systèmes Intelligents
École Polytechnique de Thiès
BP A10 Thiès
Sénégal
aaciss@ept.sn

Dustin Moody
Computer Security Division
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899-8930
USA
dustin.moody@nist.gov

Abstract

In this paper, we look at long arithmetic progressions on conics. By an arithmetic progression on a curve, we mean the existence of rational points on the curve whose x-coordinates are in arithmetic progression. We revisit arithmetic progressions on the unit circle, constructing 3-term progressions of points in the first quadrant containing an arbitrary rational point on the unit circle. We also provide infinite families of 3-term progressions on the unit hyperbola, as well as conics $ax^2 + cy^2 = 1$ containing arithmetic progressions as long as 8 terms.

1 Introduction

Recently, several researchers have explored arithmetic and geometric progressions on various families of plane curves. By a progression on a curve, we mean there is a sequence of rational points on the curve whose x-coordinates (or y-coordinates) form an arithmetic or geometric progression. The historical motivation for this problem on elliptic curves seems to be an apparent connection between long progressions and high ranks for the corresponding Mordell-Weil groups (see [12, 20] for a lengthier discussion). Perhaps for this reason, much of the work in this area has pertained to elliptic (or hyperelliptic) curves.

Bremner [5], Campbell [8], Garcia-Selfa and Tornero [12], have looked at arithmetic progressions on elliptic curves defined by Weierstrass equations, while Campbell [8], MacLeod [17] and Ulas [21] have investigated progressions on curves represented by quartic models. Alvarado [3] and Ulas [22] extended similar results to genus 2 curves. In addition, Moody [18, 19], Choudhry [9], Bremner [6], and Gonzalez-Jiménez [13] studied longer arithmetic progressions on Edwards and Huff curves.

The problem of finding long arithmetic progressions on conics has not been explored quite as extensively. Alvarado and Goins [4] gave a generalization of 3-term arithmetic progressions on an arbitrary conic section C. Allison [1, 2], Bremner [7], and González-Jiménez/Xarles [15] all looked at progressions on parabolas, with infinitely many with 8 term progressions found. More recently, Choudhry and Juyal [10] parameterized infinitely many arithmetic progressions of three rational points on the unit circle, such that the three points all lie in the first quadrant. They also used these progressions to derive infinitely many arithmetic progressions on the ellipse $x^2/a^2 + y^2/b^2 = 1$.

In this work, we look at finding arithmetic progressions on the unit circle, as well as on the unit hyperbola and conics of the form $ax^2 + cy^2 = 1$. We give 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 $x^2 - y^2 = 1$. We also provide infinitely many conics $C : ax^2 + cy^2 = 1$ having 8-term arithmetic progressions. This matches the highest known length of a progression on conics.

2 Arithmetic progressions on the unit circle

Consider the unit circle $x^2 + y^2 = 1$. Trivially, the points $(-1, 0)$, $(0, 1)$, and $(1, 0)$ are always on the circle yielding a progression of length 3. Similarly, given any rational point (x, y), there is the progression obtained from the points $(-x, y)$, $(0, 1)$, and (x, y). However, Choudhry and Juyal sought to find a progression of length 3 whose points were all in the first quadrant. That is, the x-coordinates x_i all satisfied $0 < x_i < 1$. We will work under the same restriction, and present a different approach to finding a 3-term progression.

We begin by parameterizing the rational points on the unit circle by setting

$$x(t) = \frac{2t}{t^2 + 1},$$

$$y(t) = \frac{t^2 - 1}{t^2 + 1}.$$

To find a progression of length 3 in the first quadrant, we need to find rational t_0, t_1, t_2 such that $0 < x(t_0), x(t_1), x(t_2) < 1$ and $x(t_2) - x(t_1) = x(t_1) - x(t_0)$. An easy calculation shows this will be possible if the following quadratic equation in t_2 has rational solutions:

$$(2t_0t_1^2 - 4t_0^2t_1 + 2t_0 - 4t_1)t_2^2 + 2(t_0^2 + 1)(t_1^2 + 1)t_2 + 2t_0t_1^2 - 4t_0^2t_1 + 2t_0 - 4t_1 = 0. \quad (1)$$

We obtain rational solutions to the quadratic if the resulting discriminant

$$D = 4(t_0^2 - 1)^2t_1^4 + 64t_0(t_0^2 + 1)t_1^3 - (56t_0^4 + 144t_0^2 + 56)t_1^2 + 64t_0(t_0^2 + 1)t_1 + 4(t_0^2 - 1)$$

is square. As the coefficient of t_1^4 is square, we can use a trick from Fermat in [11, p. 639] to make the entire quartic in t_1 be equal to a square by setting

$$t_1 = 8\frac{t_0(t_0 - 1)^2(t_0 + 1)^2(t_0^2 + 1)}{(3t_0^4 + 2t_0^2 + 3)(t_0^4 + 6t_0^2 + 1)}.$$

Substituting in this value of t_1, the quadratic (1) factors, resulting in the roots

$$t_2 = t_0\frac{3t_0^8 + 4t_0^6 - 30t_0^4 - 28t_0^2 - 13}{13t_0^8 + 28t_0^6 + 30t_0^4 - 4t_0^2 - 3},$$

and its inverse. A 3-term arithmetic progression on the unit circle is thus given by $x(t_0), x(t_1)$, and $x(t_2)$ with the above values of t_1 and t_2.

We next find conditions under which the corresponding points will be in the first quadrant. As $x(t) = \frac{2t}{t^2+1}$ is always an x-coordinate on the unit circle, then clearly $0 < x(t) < 1$ exactly when $t > 0$, $t \neq 1$. We therefore assume that $t_0 > 0$. We see that $t_1 > 0$ if and only if $(3t_0^4 + 2t_0^2 + 3)(t_0^4 + 6t_0^2 + 1) > 0$, which is always true. An easy analysis shows that if $t_0 > 1.8$ then the expression for $t_2 > 0$. Thus, when $t_0 > 1.8$, we see that the points with x-coordinates $x(t_0)$, $x(t_1)$, and $x(t_2)$ can all be taken to lie in the first quadrant. As an example, when $t = 2$ we obtain the progression $4/5, 3483360/6369961, 9353756/31849805$.

An interesting property of the progression above is that given any rational point $(x^*, y^*) \neq (0, \pm 1)$ on the unit circle, we can find a 3-term progression in the first quadrant containing it. Set $t_0 = (1 \pm y^*)/x^*$, and then an easy calculation verifies that $x(t_0) = x^*$. The 3-term progressions on the unit circle found by Choudhry and Juyal do not have this property. We note the property cannot be extended to two arbitrary rational points on the unit circle. For example, with the points $(7/25, 24/25)$ and $(3/5, 4/5)$ the progression would need to have third term $-1/25, 11/25$, or $23/25$. However none of these values are x-coordinates of rational points on the unit circle.

We remark that if we allow circles which are not the unit circle, it is possible to have progressions of length 4, although the points do not all lie in the first quadrant. A simple example is the circle $x^2 + y^2 = 5/2$ which has $x = -3/2, -1/2, 1/2, 3/2$. Any such symmetric progression of length 4 of the form $\{-3x_1, -x_1, x_1, 3x_1\}$ requires finding rational points satisfying

$$x_1^2 + y_1^2 = R,$$

$$9x_1^2 + y_2^2 = R,$$

where the circle has equation $x^2 + y^2 = R$. These simultaneous quadratic equations can be transformed into more common models for an elliptic curve. For example, when $R = 5/2$, we parameterize solutions to the first quadratic by setting $x(t) = (-3t^2 + 4t + 12)/(2t^2 + 8)$. Substituting this expression into the second quadratic yields the curve $C := z^2 = -71t^4 + 216t^3 + 584t^2 - 864t - 1136$. The points $(t, z) = (-1, 5)$ and $(2, 8)$ are on C. We then have $x(-1) = x(2) = 1/2$, leading to the progression $-3/2, -1/2, 1/2, 3/2$. It is not hard to find other values of R which lead to similar 4-term progressions.

3 Progressions on the unit hyperbola

It is simple to extend this approach to the unit hyperbola $x^2 - y^2 = 1$. We parameterize the rational points on the hyperbola by setting $x(t) = (t^2 + 1)/(2t)$. Following the exact same procedure as above, we find that for any rational t_2 we can set

$$t_0 = \frac{3t_2}{t_2^2 + 1},$$

$$t_1 = \frac{2(t_2^2 + 1)}{3t_2}.$$

The resulting 3-term progression is $x(t_0), x(t_1)$, and $x(t_2)$:

$$x(t_0) = \frac{t_2^4 + 11t_2^2 + 1}{6t_2(t_2^2 + 1)},$$

$$x(t_1) = \frac{(t_2^2 + 4)(4t_2^2 + 1)}{12t_2(t_2^2 + 1)},$$

$$x(t_2) = \frac{t_2^2 + 1}{2t_2}.$$

We attempted to extend these progressions to four terms for both the unit circle, as well as the unit hyperbola. If we let $d = x(t_2) - x(t_1)$ be the common difference of a progression, a fourth term would come from either $x(t_0) - d$ or $x(t_2) + d$ being a valid x-coordinate on the corresponding curve. Upon simplfying the resulting equations, they all lead to needing a rational point on certain quartic equations. Transforming these quartics into elliptic curves, we found that none of them have positive rank. Thus, we do not get 4-term progressions from this approach.

4 Arithmetic progressions on general conics

The general conic is of the form $ax^2 + bxy + cy^2 + dx + ey + f = 0$. We assume the conic is not degenerate, meaning it is not the product of two linear equations. If we were to consider degenerate conics, we would trivially obtain progressions of infinite length as every rational value is a valid x-coordinate for a linear equation.

Considering $ax^2 + bxy + cy^2 + dx + ey + f = 0$, then we can complete the square (in y) to transform the equation into the form

$$(cy + \frac{b}{2}x + \frac{e}{2})^2 = (\frac{b^2}{4} - ac)x^2 + (\frac{be}{2} - cd)x + \frac{e^2}{4} - cf.$$

Thus, any arithmetic progression on the general conic will become a progression on a conic of the form $y^2 = ax^2 + bx + c$. As mentioned in the introduction, arithmetic progressions on parabolas have been considered by a few authors [1, 2, 7, 15]. Allison found infinitely many parabolas with eight points in arithmetic progression, while González-Jiménez and Xarles were able to show that there does not exist integer arithmetic progressions with nine or more terms on parabolas with both integral coefficients and axis of symmetry. They note without the restrictions requiring integers, an upper bound on the length of progressions on parabolas is not known.

For the remainder of this section, we consider conic sections in standard form, i.e., those for which $b = 0$. We may complete the square, to write the conic equation as

$$a(x - d/(2a))^2 + c(y - e/(2c))^2 + f - d^2/(4a) - e^2/(4c) = 0.$$

An arithmetic progression shifted by $x-b/(2a)$ is still an arithmetic progression, and similarly shifting by $y - d/(2c)$ does not affect the progression. Thus we can rewrite the equation as

$$ax^2 + cy^2 = 1,$$

for some constants $a, c, \in \mathbb{Q}$. Note that by multiplying the entire equation by a suitable rational, we can scale so that the constant coefficient is 1. If we wish the progression to be of the form $\{-2x_1, -x_1, 0, x_1, 2x_1\}$, then we need that c is a square and the equation reduces to $ax^2 + y^2 = 1$.

Now given any rational m, let $a = -m^4 + 10m^2 - 9$ and $x^* = \frac{1}{4m}$. Then a straightforward calculation shows that the points $(\pm 2x^*, \frac{m^2-3}{2m})$, $(\pm x^*, -\frac{m^2+3}{4m})$, and $(0, 1)$ all lie on $ax^2+y^2 = 1$ and hence yield infinitely many 5-term progressions. If $1 < |m| < 3$, then $a > 0$ and the conic will be a circle, while otherwise $a < 0$ and the conic is a hyperbola. It is also possible to instead fix a value of a, which would then require $-1/a(m^4 - 10m^2 + 9)$ to be square. Such an equation defines an elliptic curve. If the curve has positive rank then the curve will yield an infinite number of progressions for that fixed a. For example, if $a = 15/64$ then the quartic is isomorphic to the curve $Y^2 = X^3 - 63897600X - 146800640000$, which is a rank 1 curve with generator $(-4864, 221184)$.

We can further improve the results for $ax^2 + cy^2 = 1$, and obtain progressions of length greater than five. Set

$$a = \frac{t(t+1)(t-2)}{(t-1)(2t-1)(t+4)(t+2)},$$

$$c = \frac{2}{(t-1)(2t-1)(t+4)(t+2)},$$

for any $t \neq 1/2, 1, 2, -1, -2, -4$. Then the rational points $(\pm 1, \pm(t^2+2t-t))$, $(\pm 3, \pm(t^2+2))$, and $(\pm 5, \pm(t^2-4t-2))$ all satisfy $ax^2 + y^2 = 1$. Thus, there are infinitely many conics of this form with 6 terms in progression. In order for there to be a point with x-coordinate ± 7, then there needs to be a rational solution to the equation

$$s^2 = t^4 - 20t^3 + 24t^2 + 40t + 4.$$

The curve defined is birationally equivalent to the elliptic curve $E : Y^2 = X^3 - 1008X + 10368$. The curve E is a rank 1 curve with generator $(-12, -144)$, and hence has infinitely many rational points. Given any such point (X, Y), we set $t = (40X - 480 + 4Y)/(X^2 - 16X + 48)$. For these values of t, then $x = \pm 7$ is a valid x-coordinate, showing we have an infinite number of conics with 8 points in progression. As a concrete example, the point $(28, 64)$ is on E, and leads to $t = 7/3$. When $t = 7/3$, the conic $(105/5434)x^2 + (81/5434)y^2 = 1$ has eight points in progression with x-coordinates $\{-7, -5, -3, -1, 1, 3, 5, 7\}$.

5 Conclusion and future work

In this work, we have studied long arithmetic progression on conics. We gave a more general result on finding progressions on the unit circle, and similarly provided infinitely many unit hyperbolas with 3-term arithmetic progressions. We also constructed infinitely many conics in standard form having 8-term arithmetic progressions. Future work would be to improve the length of these progressions. It might also be possible to use the techniques of [14] to prove upper bounds on the maximum length of (integer) progressions on the unit circle, hyperbola, or conics in standard form. It would be interesting to study long geometric progressions on conics as well.

6 Acknowledgments

The first author acknowledges support from the MACISA-LIRIMA project and the Simons Foundation through the Pole of Research in Mathematics and their Applications to Information Security in Subsaharan Africa (PRMAIS). We would also like to thank the anonymous reviewer for their valuable comments and suggestions, and in particular for pointing us to some of the previous results in the literature which we were not aware of.

References

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

[2] D. Allison, On square values of quadratics, *Math. Proc. Cambridge Philos. Soc.* **99** (1986), 381–383.

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

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

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

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

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

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

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

[10] A. Choudhry and A. Juyal, Rational points in arithmetic progression on the unit circle, *J. Integer Sequences* **19** (2016), Article 16.4.1.

[11] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea Publishing Co., 1920.

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

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

[14] E. González-Jiménez, Covering techniques and rational points on some genus 5 curves, *Contemp. Math.* **649** (2015), 89–105.

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

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

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

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

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

[20] D. Moody and A. S. Zargar, On the rank of elliptic curves with long arithmetic progressions, to appear in *Colloq. Math.*, 2016.

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

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

2010 *Mathematics Subject Classification*: Primary 11B25; Secondary 11D09.
Keywords: arithemetic progression, conic.

Received June 18 2016; revised versions received September 13 2016; November 15 2016. Published in *Journal of Integer Sequences*, December 27 2016.

Return to Journal of Integer Sequences home page.