Journal of Integer Sequences, Vol. 16 (2013),
Article 13.8.5

Arithmetic Progressions on Edwards Curves

Andrew Bremner
School of Mathematical and Statistical Sciences
Arizona State University
Tempe AZ 85287-1804
USA
bremner@asu.edu

Abstract

Several authors have investigated the problem of finding elliptic curves over $\mathbb{Q}$ that contain rational points whose x-coordinates are in arithmetic progression. Traditionally, the elliptic curve has been taken in the form of an elliptic cubic or elliptic quartic. Moody studied this question for elliptic curves in Edwards form, and showed that there are infinitely many such curves upon which there exist arithmetic progressions of length 9, namely, with $x = 0, \pm 1, \pm 2, \pm 3, \pm 4$. He asked whether any such curve will allow an extension to a progression of 11 points. This note shows that such curves do not exist. A certain amount of luck comes into play, in that we need only work over a quadratic extension field of $\mathbb{Q}$.

1 Introduction

A sequence of points on an elliptic curve is said to be an *arithmetic progression* on the curve if the x-coordinates of the points lie in arithmetic progression. The model chosen for the elliptic curve will clearly affect the consequent theory. Bremner [1], Campbell [2], and Garcia-Selfa and Tornero [3] have investigated arithmetic progressions on curves in Weierstrass cubic form; and Campbell [2], Macleod [5], and Ulas [8] have investigated progressions on quartic models. Recntly, Moody [7] investigates progressions on elliptic curves in the Edwards form

$$E_d: \ x^2 + y^2 = 1 + dx^2y^2, \qquad d \neq \pm 1,$$

which automatically contain the length three progression consisting of the points $(-1, 0)$, $(0, 0)$, $(1, 0)$. He shows that there exist infinitely many d such that this length 3 progression extends to a sequence of nine points whose x-coordinates lie in arithmetic progression. He asks whether such progressions of length 9 can ever be extended to progressions of length 11. By investigating a curve of genus 5 and using elliptic Chabauty techniques, we prove here that such an extension is not possible.

2 Progressions of length 11

The condition that there be rational points on E_d at $\pm x = 2, 3, 4, 5$ is precisely that there exist rationals p, q, r, s satisfying

$$\frac{24p^2+1}{25} = \frac{15q^2+1}{16} = \frac{8r^2+1}{9} = \frac{3s^2+1}{4} (= d).$$

Homogenizing by setting $(p, q, r, s) = (P/T, Q/T, R/T, S/T)$, we get

$$32P^2 = 25S^2 + 7T^2, \qquad 5Q^2 = 4S^2 + T^2, \qquad 32R^2 = 27S^2 + 5T^2. \tag{1}$$

As an intersection of three quadrics in projective four-dimensional space, these equations define a (non-singular) curve C of genus 5. The trick in the following analysis is finding an amenable way of writing down the equations for C. We choose the following formulation:

$$125Q^2 = 128P^2 - 3T^2, \quad 25R^2 = 27P^2 - 2T^2, \quad 25S^2 = 32P^2 - 7T^2.$$

From (1), if both P, T are divisible by 5, then S, R, Q are each divisible by 5; and so without loss of generality, P (and hence T) is not divisible by 5. We may certainly suppose that $P > 0$; and the sign of T may be chosen so that $P \equiv T \bmod 5$.
Let $K = \mathbb{Q}(\theta)$, $\theta^2 = 6$, a field with class number 1. A fundamental unit is $\epsilon = 5 - 2\theta > 0$. We have the prime ideal factorizations:

$$(2) = \mathfrak{p}_2^2 = (2+\theta)^2, \qquad (3) = \mathfrak{p}_3^2 = (3-\theta)^2, \qquad (5) = \mathfrak{p}_5\mathfrak{p}_5' = (1+\theta)(1-\theta).$$

Now $\mathrm{Norm}_{K/\mathbb{Q}}(16P - \theta T) = 10(5Q)^2$ and thus

$$16P - \theta T = \pm(2+\theta)(1-\theta)\epsilon^i G^2 = \pm(-4-\theta)\epsilon^i G^2 = (4+\theta)\epsilon^i G^2,$$

where G is an integer of K, $i = 0, 1$, and the sign is determined by the fact that the left hand side is positive. Similarly, $\mathrm{Norm}_{K/\mathbb{Q}}(9P - \theta T) = 3(5R)^2$, so that

$$9P - \theta T = \pm(3-\theta)\epsilon^j H^2 = (3-\theta)\epsilon^j H^2,$$

for an integer H of K, $j = 0, 1$, and the sign determined by positivity. We can now deduce

$$\begin{aligned}(16P - \theta T)(9P - \theta T) &= (4+\theta)(3-\theta)\epsilon^k\Box = (6-\theta)\epsilon^k\Box,\\ (16P + \theta T)(9P + \theta T)(32P^2 - 7T^2) &= (6+\theta)\epsilon^{-k}\Box,\end{aligned} \tag{2}$$

where $k = 0, 1$.

Case $k = 0$. The second equation at (2) on setting $x = P/T$ gives the equation of an elliptic quartic curve over K:

$$(16x + \theta)(9x + \theta)(32x^2 - 7) = (6 + \theta)y^2, \tag{3}$$

with cubic form

$$Y^2 = X(X^2 + 68(6 + \theta)X + 6250(7 + 2\theta)).$$

Computations with Magma [6] show that this curve has rank 1 over the field K of degree 2 over $\mathbb{Q}$, and since the rank is less than the degree of the field extension, elliptic Chabauty methods apply. Magma returns that the only K-points of (3) with $x \in \mathbb{Q}$ are $(x, \pm y) = (1, 25)$.

Case $k = 1$. The second curve at (2) becomes on setting $x = P/T$

$$(16x + \theta)(9x + \theta)(32x^2 - 7) = (42 + 17\theta)y^2, \tag{4}$$

with cubic model

$$Y^2 = X(X^2 + 68(18 - 7\theta)X + 6250(103 - 42\theta)).$$

This curve has rank 0, and the $\mathbb{Z}/2\mathbb{Z}$ torsion points correspond to the points $x = -\theta/9, -\theta/16$ on (4), with non-rational x.

Consequently, the only rational points on the curve C at (1) are given by $P^2 = Q^2 = R^2 = S^2 = T^2$, and it follows there are no length 11 arithmetic progressions of the desired type.

Remark 1. There are ten ways to write the intersection at (1), with the three formulations

$$5p^2 = 7r^2 - 2s^2, \qquad 25q^2 = 32r^2 - 7s^2, \qquad 5t^2 = 32r^2 - 27s^2$$

$$7p^2 = 10q^2 - 3r^2, \qquad 7s^2 = -25q^2 + 32r^2, \qquad 7t^2 = 135q^2 - 128r^2$$

$$3r^2 = -7p^2 + 10q^2, \qquad 3s^2 = -32p^2 + 35q^2, \qquad 3t^2 = 128p^2 - 125q^2$$

also affording a similar treatment to the above involving factorization over a quadratic field, namely $\mathbb{Q}(\sqrt{14})$, $\mathbb{Q}(\sqrt{30})$, and $\mathbb{Q}(\sqrt{70})$, respectively. An argument over $\mathbb{Q}(\sqrt{30})$ is successful, with both elliptic curves that arise having rank 1; but over $\mathbb{Q}(\sqrt{14})$ and $\mathbb{Q}(\sqrt{70})$ a corresponding elliptic curve has rank at least 2 over K, and elliptic Chabauty methods are inapplicable. In the remaining six formulations, it would be necessary to work over a quartic extension of $\mathbb{Q}$.

3 Concluding remarks

The result of this note shows that Moody's centrally symmetric 9-term progression of points on E_d cannot be extended to a centrally symmetric 11-term progression. The question as to whether E_d may possess arithmetic progressions that are not centrally symmetric has been addressed in González-Jiménez [4], where he expresses the belief that *no* arithmetic progression on E_d can have more than 9 elements.

An upper bound for the length of arithmetic progressions on elliptic curves under any presentation, remains elusive. In the cases of Weierstrass cubics or elliptic quartics, examples are known (Bremner [1], Macleod [5]) of progressions of length 8 and length 14, respectively (the latter examples being centrally symmetric). To show, for example, that there are no progressions of length 9 on a cubic model of an elliptic curve is equivalent to finding all the rational points on the (non-singular) intersection of five quadrics in $\mathbb{P}^8$, a variety of dimension 3, and which at present seems an intractable problem.

References

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

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

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

[4] E. González-Jiménez, On arithmetic progressions on Edwards curves, preprint, http://arxiv.org/pdf/1304.4361.pdf.

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

[6] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[7] D. Moody, Arithmetic Progressions on Edwards Curves, *J. Integer Seq.* **14** (2011), Article 11.1.7.

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

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11B25, 11G30.

Keywords: arithmetic progression, elliptic curve, Edwards curve, Chabauty.

Received August 6 2013; revised version received September 9 2013. Published in *Journal of Integer Sequences*, October 12 2013.

Return to Journal of Integer Sequences home page.