Journal of Integer Sequences, Vol. 14 (2011),
Article 11.1.7

Arithmetic Progressions on Edwards Curves

Dustin Moody
Computer Security Division
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD, 20899-8930
USA
dbmoody25@gmail.com

Abstract

We look at arithmetic progressions on elliptic curves known as Edwards curves. By an arithmetic progression on an elliptic curve, we mean that the x-coordinates of a sequence of rational points on the curve form an arithmetic progression. Previous work has found arithmetic progressions on Weierstrass curves, quartic curves, and genus 2 curves. We find an infinite number of Edwards curves with an arithmetic progression of length 9.

1 Introduction

Recently, several researchers have looked at arithmetic progressions on elliptic curves. Bremner [3], Campbell [4], Garcia-Selfa and Tornero [7] used elliptic curves given by a Weierstrass equation, while Campbell [4], MacLeod [10], and Ulas [11] have looked at quartic models. Alvarado [1], and Ulas [12] have extended similar results to genus 2 curves. The historical motivation for this problem is discussed in [7].

Weierstrass equations and quartic curves are only two of several possible models for elliptic curves. H. Edwards recently proposed a new parameterization for elliptic curves [6]. These Edwards curves are of the form

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

with $d \neq 1$. In this work, we look at *arithmetic progressions on Edwards curves*. By this we mean a sequence of rational points $(x_1, y_1), \ldots, (x_n, y_n)$ on E_d with the x_i forming an arithmetic progression.

2 Arithmetic Progressions

Unlike other models for elliptic curves, the Edwards curve E_d has only one parameter we can modify. Still, we are able to prove the following result:

Theorem 1. *There are infinitely many choices for d such that the Edwards curve*

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

has (at least) 9 points in an arithmetic progression.

Proof. The curve E_d clearly has the points $(-1, 0), (0, 1)$, and $(1, 0)$ for any choice of d. We seek to find d to extend this arithmetic progression. In order for the curve to have a point with x-coordinate $x = \pm 2$, then we must have $4 + y^2 = 1 + 4dy^2$, or equivalently

$$y^2 = \frac{3}{4d - 1}.$$

For y to be rational, we need $4d - 1 = 3j^2$, for some rational j. Solving this for d, this is

$$d = \frac{1 + 3j^2}{4}. \tag{1}$$

For the same reason, if we require that E_d has a point with x-coordinate ± 3, then we must have

$$y^2 = \frac{8}{9d - 1}.$$

For y to be rational, we need $9d - 1 = 2k^2$ for some rational k, or

$$d = \frac{1 + 2k^2}{9}. \tag{2}$$

Equating (1) and (2) yields the conic

$$C_d : 27j^2 - 8k^2 + 5 = 0.$$

By inspection, the point $(1, 2)$ lies on the conic. We can use this point to parameterize all rational points on the curve C_d:

$$(j, k) = \left(\frac{8m^2 - 32m + 27}{8m^2 - 27}, \frac{-2(8m^2 - 27m + 27)}{8m^2 - 27} \right),$$

where m is any rational number. By equation (1) (or (2)),

$$d = \frac{64m^4 - 384m^3 + 984m^2 - 1296m + 729}{(8m^2 - 27)^2}. \tag{3}$$

For any rational m, we have found an Edwards curve E_d which has rational points with x-coordinates $-3, -2, -1, 0, 1, 2$, and 3.

We now use this to obtain an infinite family of Edwards curves with arithmetic progressions of length (at least) 9. For a rational point to satisfy $x = \pm 4$, then we seek a rational y such that $y^2 = \frac{15}{16d-1}$. Substituting in the value of d from equation (3), this is

$$y^2 = \frac{5(8m^2-27)^2}{(320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645)}.$$

Then y will be rational provided that

$$\frac{1}{5}(320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645) = t^2, \tag{4}$$

for some rational t. As the discriminant of $320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645$ is non-zero, then (4) is the equation of an elliptic curve. Using MAGMA [2], this curve is found to be isomorphic to the elliptic curve with Weierstrass equation

$$E : y^2 = x^3 - x^2 - 19633x - 762863.$$

The curve E has rank 2, with generators $(-99, 448)$ and $(-93, 500)$. There are thus an infinite number of rational points on the curve (4). For each such rational point (m, t), if we substitute this value of m into (3), then we obtain a value of d for which the curve E_d has an arithmetic progression of length 9. Namely, the progression is -4, -3, -2, -1, 0, 1, 2, 3, and 4. $\square$

3 Future Work

It is possible that the family of curves given in the proof of Theorem 1 lead to longer arithmetic progressions. We performed a computer search to find a rational point (m, t) on the curve (4), leading to an E_d with points having x-coordinates ± 5. Our search has not found such a rational point, thus it is an open problem to find an Edwards curve with an arithmetic progression of length 10 or longer.

We remark that it would be interesting to examine other models for elliptic curves for arithmetic progressions. For example, this could include Jacobi intersections [5] , Hessian curves [9], or Huff curves [8].

References

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

[2] W. Bosma, J. Cannon, and C. Playoust, MAGMA 2.14-1, available at `http://magma.maths.usyd.edu.au/`.

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

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

[5] D. Chudnovsky and G. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Adv. App. Math.* **7** (1986), 385–434.

[6] H. Edwards, A normal form for elliptic curves, *Bull. Amer. Math. Soc.* **44** (2007), 393–422.

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

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

[9] M. Joye and J. Quisquater, Hessian elliptic curves and side-channel attacks, in Ç.K. Koç, D. Naccache, and C. Paar, eds., *Proceedings of Cryptographic Hardware and Embedded Systems b CHES 2001*, Springer-Verlag, 2001, pp. 402–410.

[10] A. MacLeod, 14-term arithmetic progressions on quartic elliptic curves, *J. Integer Seq.* **9** (2006), Paper 06.1.2.

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

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

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11B25.
Keywords: arithmetic progression, elliptic curve, Edwards curve.

Received December 13 2010; revised version received January 25 2011. Published in *Journal of Integer Sequences*, February 8 2011.

Return to Journal of Integer Sequences home page.