Annales Mathematicae et Informaticae
***38** (2011) pp. 111–116*
http://ami.ektf.hu

Arithmetic progressions on Huff curves

Dustin Moody

National Institute of Standards and Technology (NIST), Gaithersburg
e-mail: dmoody25@gmail.com

Submitted January 10, 2011 Accepted March 19, 2011

Abstract

We look at arithmetic progressions on elliptic curves known as Huff curves. By an arithmetic progression on an elliptic curve, we mean that either the x or y-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, Edwards curves, and genus 2 curves. We find an infinite number of Huff curves with an arithmetic progression of length 9.

Keywords: Diophantine equations, arithmetic progressions, elliptic curves

MSC: 11G05, 11B25

1. Introduction

Recently, several researchers have looked at arithmetic progressions on elliptic curves. Bremner [3], Campbell [4], Garcia-Selfa and Tornero [8] used elliptic curves given by a Weierstrass equation, while Campbell [4], MacLeod [12], and Ulas [15] have looked at quartic models. Moody [13] has studied the problem on Edwards curves. Alvarado [1] and Ulas [16] have extended similar results to genus 2 hyperelliptic curves. The historical motivation for this problem is discussed in [8].

Besides Weierstrass equations, quartic curves, and Edwards curves [6], there are other models for elliptic curves. These include Jacobi intersections [5], Hessian curves [10], and Huff curves [9], for example. Originally introduced in 1948, Huff curves have recently been shown to have applications in cryptography [11], [7]. An elliptic curve in Huff's model can be written as

$$H_{a,b} : x(ay^2 - 1) = y(bx^2 - 1).$$

In this work, we look at *arithmetic progressions on Huff curves*. By this we mean a sequence of rational points $(x_1, y_1), \ldots, (x_n, y_n)$ on $H_{a,b}$ with the x_i forming an

Source	Model	Longest progression	Longest progression for infinite family
[3],[4]	Weierstrass curves	8	8
This work	Huff curves	9	9
[13]	Edwards curves	9	9
[2],[12],[15]	quartic curves	14	12
[1],[16]	genus 2 quintics	12	12
[16]	genus 2 sextics	18	16

Table 1: Longest arithmetic progressions on curves

arithmetic progression. The main result of this paper is to show several infinite families of Huff curves with arithmetic progressions of length 9. In comparison, Table 1 gives the length of the longest arithmetic progression for the previously mentioned models. Note in general the length increases as we have more variables in the defining curve equation we can specify.

2. Arithmetic progressions

Huff curves are elliptic curves that can be written as $x(ay^2-1) = y(bx^2-1)$, when $ab(a-b) \neq 0$. Clearly we have symmetry in x and y if we switch a and b, so we only look for arithmetic progressions on the x-coordinates. Note trivially that the point $(0,0)$ is always on the curve. Notice also that an arithmetic progression of x-coordinates of the form $\{-kd, -(k-1)d, \ldots, -d, 0, d, 2d, \ldots, (k-1)d, kd\}$ can always be rescaled so that $d = 1$. This is seen as follows. If the point (jd, y) is on the curve $H_{a,b}$, then the point $(j, y/d)$ is on the curve H_{ad^2,bd^2}. As a consequence, we will focus on finding Huff curves which have x-coordinates in the set $\{\pm 1, \pm 2, \pm 3, \pm 4\}$.

We will repeatedly need the following calculation. If we require a rational point (x, y) on $H_{a,b}$ with $x = n$, then we must have that $any^2-(bn^2-1)y-n = 0$. In order for $y \in \mathbb{Q}$, the discriminant $(bn^2-1)^2+4an^2$ must be a rational square. Applying this to $x = 1$, we need $(b-1)^2+4a = j^2$ for some rational j. The same equation is true for $x = -1$. Similarly, if we require rational points with x-coordinate ± 2 and ± 3, then we must have $(4b-1)^2+16a = k^2$, and $(9b-1)^2+36a = l^2$ for some rational k and l. Solving for a in our first equation, we have

$$a = \frac{1}{4}\left(j^2 - (b-1)^2\right). \tag{2.1}$$

Eliminating a from the other two equations, we are left with the system

$$12b^2 + 4j^2 - k^2 = 3, \tag{2.2}$$

$$72b^2 + 9j^2 - l^2 = 8. \tag{2.3}$$

We now parameterize the solutions in terms of b and a parameter m. Some easy algebra verifies that $j = 3b^2 - 1$ and $k = 6b^2 - 1$ is a solution to (2.2). Let $j = 3b^2 - 1 + t$ and $k = 6b^2 - 1 + mt$. Substituting these values into (2.2) yields

$$t \ \ (m^2 - 4)t + 12mb^2 - 24b^2 - 2m + 8 \ \ = 0.$$

Solving for t, we see $t = -2\frac{(6b^2-1)m-4(3b^2-1)}{m^2-4}$, and thus

$$j = \frac{(3b^2-1)m^2 - 2(6b^2-1)m + 4(3b^2-1)}{m^2-4}, \tag{2.4}$$

$$k = \frac{-(6b^2-1)m^2 + 8(3b^2-1)m - 4(6b^2-1)}{m^2-4}.$$

We substitute this expression for j into (2.3) and seek a rational solution for l. Some more algebra shows that this is equivalent to

$$81(m-2)^4b^4+18(m-2)^2(m^2+22m+4)b^2+m^4-36m^3+172m^2-144m+16 \tag{2.5}$$

being a rational square. Considering this as a polynomial in b, we first check to see what values of m will lead to the constant term being square. The equation $E : v^2 = m^4 - 36m^3 + 172m^2 - 144m + 16$ clearly has the rational point $(0, 4)$, and so determines an elliptic curve. Using SAGE [14], the curve E is found to have rank 0, and torsion points $(0, \pm 4), (1, \pm 3), (2, \pm 12), (4, \pm 12)$, and $(-2, \pm 36)$. We exclude $m = \pm 2$, as this leads to division by 0 in the expressions for j and k. When $m = 1$ or $m = 4$, then (2.5) is not the square of a polynomial in b. When $m = 0$, then (2.5) is $16(9b^2 + 1)^2$.

So letting $m = 0$, we have $j = -(3b^2 - 1)$, and $a = \frac{1}{4}b(3b - 2)(3b - 1)(b + 1)$ by (2.1). With this expression for a, then the curve $H_{a,b}$ has an arithmetic progression of length 7, namely $x = -3, -2, -1, 0, 1, 2, 3$. In order for $x = \pm 4$ to be a rational point, we are led to the discriminant $144b^4 + 144b^2 + 1$ needing to be a square. As the curve

$$E_1 : v^2 = 144b^4 + 144b^2 + 1$$

clearly has rational point $(0, 1)$, then E_1 is an elliptic curve. By SAGE, this curve has rank 2 with generators $(\frac{1}{12}, \frac{17}{12})$, and $(\frac{1}{8}, \frac{29}{16})$. Each rational point on E_1 leads to a value for b so that the Huff curve $H_{a,b}$ has an arithmetic progression of length 9. We thus have our first infinite family of Huff curves with a progression of length 9.

3. More families

Returning to (2.5),we consider it as a polynomial in m,

$$\begin{aligned}(9b^2 + 1)^2m^4 - 36(18b^4 - 9b^2 + 1)m^3 + 4(486b^4 - 360b^2 + 43)m^2 \\ - 144(18b^4 - 9b^2 + 1)m + 16(9b^2 + 1)^2.\end{aligned} \tag{3.1}$$

If we compare this to

$$\left((9b^2+1)m^2 - \frac{18(18b^4-9b^2+1)}{9b^2+1}m + 4(9b^2+1)\right)^2,$$

the difference is

$$\frac{160m^2(324b^4-45b^2+1)}{(9b^2+1)^2}.$$

If the difference is equal to 0, then (3.1) is a square. The case $m = 0$ was already examined. The other zeroes are when $b = \pm\frac{1}{3}, \pm\frac{1}{6}$. Letting $b = -\frac{1}{3}$, then

$$a = -\frac{(3m-4)(m-3)(m+1)(m+4)}{9(m^2-4)^2}.$$

The condition that $x = \pm 4$ is the coordinate of a rational point is equivalent to the corresponding discriminant being a rational square; i.e. we seek a rational point on the curve

$$E_2 : v^2 = 169m^4 - 128m^3 - 264m^2 - 512m + 2704.$$

The choice of $b = \frac{1}{3}$ leads to the same curve. Similarly, when $b = \pm\frac{1}{6}$, we are led to the curve

$$E_3 : v^2 = 46m^4 - 440m^3 + 1968m^2 - 1760m + 736.$$

Both E_2 and E_3 are elliptic curves with rank 2 and 1 respectively. These ranks were computed by SAGE. Each rational point on one of the curves leads to a Huff curve with a rational point having x-coordinate ± 4, and thus a progression of length 9.

By experimentation, we found a few other infinite families. Using the same parameterization as above, let $b = \pm\frac{1}{4}$ or $\pm\frac{1}{8}$. Then it can be checked that $x = \pm 4$ is the x-coordinate of a rational point on the Huff curve $H_{a,b}$ with a determined by (2.1) and (2.4). However, we are no longer guaranteed that $x = \pm 3$ is on the Huff curve. Requiring $x = \pm 3$, we arrive at the following curves

$$E_4 : v^2 = 625m^4 - 4680m^3 + 22936m^2 - 18720m + 10000, \qquad (b = \pm 1/4)$$

$$E_5 : v^2 = 5329m^4 - 127368m^3 + 614296m^2 - 509472m + 85624. \qquad (b = \pm 1/8)$$

These elliptic curves have ranks 1 and 2, leading to two more infinite families of Huff curves with progressions of length 9.

Finally, letting $b = \pm\frac{1}{2}$ the parameterized Huff curve is $H_{a,\pm 1/2}$, with

$$a = -\frac{(3m-2)(m-6)}{64(m-2)^2}. \tag{3.2}$$

The condition that there is a rational point with $x = \pm 3$ leads to a quadratic, instead of a quartic as in previous cases:

$$v^2 = 169m^2 - 604m + 676. \tag{3.3}$$

A parametric solution to (3.3) is given by

$$m = -\frac{4(13s + 151)}{s^2 - 169},$$

$$v = -\frac{2(13s^2 + 302s + 2197)}{s^2 - 169}.$$

Substituting this expression for m into (3.2), and requiring $x = \pm 4$ we have the curve

$$E_6 : r^2 = 46s^4 + 2288s^3 + 42124s^2 + 335712s + 1017846,$$

which has rank 1. Each rational point of E_6 gives a rational s, which in turn determines a rational m and a. The curve $H_{a,\pm 1/2}$ will have rational points with x-coordinates ± 3 and ± 4.

4. Conclusion

In the previous section, we produced six infinite families of Huff curves having the property that each has rational points with x-coordinate $x = -4, -3, -2, -1, 0, 1, 2, 3, 4$. This produces an arithmetic progression of length 9. We have performed computer searches to see if we can find any rational points on these curves leading to $x = \pm 5$ being the x-coordinate of a rational point on $H_{a,b}$. So far these searches have failed to turn up such a point. It is therefore an open problem to find a Huff curve with an arithmetic progression of length 10 (or longer). It would also be interesting to investigate arithmetic progressions on the remaining models of elliptic curves.

Acknowledgments. We would like to thank the anonymous referee for noticing a few minor mistakes in our formulas.

References

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

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

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

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

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

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

[7] Feng, R. and Wu, H., Elliptic curves in Huff's model, available at `http://eprint.iacr.org/2010/390.pdf`, (2010).

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

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

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

[11] Joye, M., Tibouchi, M., and Vergnaurd, D., Huff's model for elliptic curves, in *Algorithmic Number Theory Symposium (ANTS-IX) proceedings*, LNCS 6197, Springer, (2010), 234–250.

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

[13] Moody, D., Arithmetic progressions on Edwards curves, *J. Integer Seq.*, Paper 11.1.7, (2011).

[14] Stein, W. et al., Sage Mathematics Software, The Sage Development Team, (2010), `http://www.sagemath.org`.

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

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