Journal of Integer Sequences, Vol. 18 (2015),
Article 15.5.2

Arithmetic Progressions on Huff Curves

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

Abstract

Several mathematicians have studied the problem of finding a set of n rational points on various models of elliptic curves such that the abscissae of these n points are in arithmetic progression. This paper is concerned with finding such arithmetic progressions on the Huff model of elliptic curves. Moody has found arithmetic progressions of length 9 on several infinite families of Huff curves with numerical coefficients. In this paper we find infinitely many parametrized families of Huff curves on which there are arithmetic progressions of length 9, as well as several Huff curves on which there are arithmetic progressions of length 11.

1 Introduction

An arithmetic progression of length n on a curve $f(x, y) = 0$ consists of a set of rational points $(x_i, y_i), i = 1, 2, \ldots, n$ lying on the curve such that the abscissae $x_i, i = 1, 2, \ldots, n$ are in arithmetic progression. The problem of finding arithmetic progressions on various models of elliptic curves (as well as on hyperelliptic curves) has been studied by several mathematicians [1, 2, 3, 4, 7, 8, 9, 10, 11]. This paper is concerned with finding arithmetic progressions on the Huff model of elliptic curves defined by an equation of the type,

$$x(ay^2 - 1) = y(bx^2 - 1), \tag{1}$$

where a, b are rational parameters such that $ab(a-b) \neq 0$. The Huff curve (1) will be written briefly as $H(a, b)$. Moody [8] has found several infinite families of Huff curves with rational numerical values of a, b such that there are arithmetic progressions of length 9 on these Huff curves. The numerical values of a, b defining these families of Huff curves are based on the coordinates of points of an elliptic curve of positive rank, and hence explicit formulae for these families of Huff curves cannot be written down. Moody has also posed the problem of finding Huff curves on which there are arithmetic progressions of length 10 or more.

In this paper we obtain infinitely many parametrized families of Huff curves such that there exist arithmetic progressions of length 9 on these curves. As these parametrized families are given explicitly, they are an improvement on the families of Huff curves found by Moody. We also obtain several Huff curves on which there are arithmetic progressions of length 11.

2 Parametrized families of Huff curves with arithmetic progressions of length 9

Eq. (1) may be written as $axy^2 - (bx^2 - 1)y - x = 0$, which may be considered as a quadratic equation in y. It follows that for any arbitrary rational value of the abscissa x, the corresponding value of the ordinate y will be rational if and only if the discriminant $d(a, b, x) = b^2x^4 + (4a-2b)x^2 + 1$ is a perfect square. We note that $d(a-b, -b, x) = d(a, b, x)$ and hence if there exists a rational point on the curve $H(a, b)$ with abscissa x, there is also a rational point on the Huff curve $H(a - b, -b)$ with the same abscissa. It follows that if there exists an arithmetic progression of length n on the curve $H(a, b)$, then there is also an arithmetic progression of length n on the curve $H(a-b, -b)$. We will refer to the Huff curve $H(a - b, -b)$ as a conjugate of the Huff curve $H(a, b)$. It is readily seen that the conjugate of the Huff curve $H(a-b, -b)$ is the Huff curve $H(a, b)$ and thus the two Huff curves $H(a, b)$ and $H(a - b, -b)$ are conjugates of each other.

Similarly we note that when $k \neq 0$, we have $d(k^{-2}a, k^{-2}b, kx) = d(a, b, x)$. It follows that if there is an arithmetic progression on the Huff curve $H(a, b)$ with abscissae $x_i, i = 1, 2, \ldots, n$, then there is also an arithmetic progression of the same length on the Huff curve $H(k^{-2}a, k^{-2}b)$ with abscissae $kx_i, i = 1, 2, \ldots, n$.

Finally we note that since $d(a, b, x) = d(a, b, -x)$, if there is a rational point on $H(a, b)$ with abscissa x, there is also a rational point on $H(a, b)$ having abscissa $-x$. The point $(0, 0)$ lies on the curve (1) for arbitrary a and b. We will now determine suitable rational values of a, b such that there exist rational points on (1) having abscissae $1, 2, 3$ and 4. The curve (1) would then also have rational points having abscissae $-1, -2, -3, -4$ and we would get an arithmetic progression of length 9 on this Huff curve since there would exist rational points on the curve with abscissae $0, \pm 1, \pm 2, \pm 3, \pm 4$.

Equating the discriminant $d(a, b, x)$ to a perfect square when x takes successively the values $1, 2, 3$ and 4, we get four conditions which may be written as $b^2j^4 + (4a - 2b)j^2 + 1 = t_j^2, j = 1, 2, 3, 4$, where each t_j is some rational number. We write these equations in homogenized form as follows:

$$\begin{aligned} b^2 + (4a - 2b)z + z^2 &= t_1^2, \\ 16b^2 + 4(4a - 2b)z + z^2 &= t_2^2, \\ 81b^2 + 9(4a - 2b)z + z^2 &= t_3^2, \\ 256b^2 + 16(4a - 2b)z + z^2 &= t_4^2. \end{aligned} \tag{2}$$

Solving the first of these equations for a, we get

$$a = -(b^2 - 2bz + z^2 - t_1^2)/(4z),$$

and on substituting this value of a in the last three equations of (2), we get the three equations,

$$12b^2 - 3z^2 + 4t_1^2 = t_2^2, \tag{3}$$

$$72b^2 - 8z^2 + 9t_1^2 = t_3^2, \tag{4}$$

$$240b^2 - 15z^2 + 16t_1^2 = t_4^2. \tag{5}$$

Eq. (3) may be written as $3(2b - z)(2b + z) = -(2t_1 - t_2)(2t_1 + t_2)$ and its complete solution, obtained by solving the equations,

$$3(2b - z) = 12mu, \quad 2b + z = 4nv, \quad -(2t_1 - t_2) = 12mv, \quad 2t_1 + t_2 = 4nu,$$

is given by

$$b = mu + nv, \quad t_1 = nu - 3mv, \quad t_2 = 2nu + 6mv, \quad z = -2mu + 2nv,$$

where m, n, u, v are arbitrary rational parameters. Substituting the values of b, z and t_1 in Eqs. (4) and (5), we get the following two equations:

$$(40m^2 + 9n^2)u^2 + 154mnuv + (81m^2 + 40n^2)v^2 = t_3^2, \tag{6}$$

$$(180m^2 + 16n^2)u^2 + 504mnuv + (144m^2 + 180n^2)v^2 = t_4^2. \tag{7}$$

We note that taking $u = \pm v$ or $u = \pm 3v$ yields a solution of both the Eqs. (6) and (7) but these solutions lead to $ab(a-b) = 0$ when the curve (1) reduces to a curve of genus 0 and such solutions must therefore be excluded. Eq. (6) may be considered as a quadratic equation in u, v and t_3, and its complete solution obtained by taking $u = 1, v = 1, t_3 = 11m + 7n$ as an initial known solution is readily obtained and is given by

$$\begin{aligned} u &= T^2 - (22m + 14n)TU + (40m^2 + 154mn + 9n^2)U^2, \\ v &= T^2 - (40m^2 + 9n^2)U^2, \\ t_3 &= -(11m + 7n)T^2 + 2(5m + 9n)(8m + n)TU \\ &\quad - (11m + 7n)(40m^2 + 9n^2)U^2, \end{aligned} \tag{8}$$

where T, U are arbitrary rational parameters. On substituting these values of u, v in (7), we get the condition,

$$\begin{aligned} & 4(9m+7n)^2T^4 - 16(15m+n)(11m+7n)(3m+4n)T^3U \\ & \quad + (90000m^4 + 166320m^3n + 108168m^2n^2 + 14784mn^3 + 184n^4)T^2U^2 \\ & \quad - 16(11m+7n)(1800m^4 + 4410m^3n + 565m^2n^2 + 49mn^3 + 36n^4)TU^3 \\ & \quad + (518400m^6 + 1411200m^5n + 1711120m^4n^2 + 333200m^3n^3 \\ & \quad - 151724m^2n^4 + 3528mn^5 + 15876n^6)U^4 = t_4^2. \end{aligned} \tag{9}$$

As the coefficient of T^4 in (9) is a perfect square, a solution of this equation is readily obtained by applying the method devised by Fermat [6, p. 639] and is given by

$$\begin{aligned} T = {} & U(1196370m^8 + 4657095m^7n + 7590681m^6n^2 + 6133293m^5n^3 \\ & + 1673847m^4n^4 - 1130479m^3n^5 - 1123969m^2n^6 - 371077mn^7 - 46305n^8) \\ & \times (280665m^7 + 1032183m^6n + 1361619m^5n^2 + 619821m^4n^3 \\ & - 206577m^3n^4 - 312767m^2n^5 - 108731mn^6 - 12005n^7)^{-1}. \end{aligned} \tag{10}$$

By repeatedly applying Fermat's method, we can obtain infinitely many solutions of (9), and working backwards, we can obtain infinitely many sets of rational values of a, b, expressed in terms of arbitrary parameters m, n such that there are arithmetic progressions of length 9 on the corresponding Huff curves (1).

We now describe a method of obtaining solutions of (9) that are much simpler than the solution (10). We first obtain solutions of (9) that lead to trivial solutions of our problem. As noted earlier, we get trivial solutions when $u = \pm v$ or $u = \pm 3v$, and substituting the values of u, v given by (8) in the condition of triviality $(u^2 - v^2)(u^2 - 9v^2) = 0$, we obtain seven values of T that yield solutions of (9). We will use four of these solutions to obtain simple solutions of (9). We first rewrite (9) by dividing it by $4(9m+7n)^2$ and taking $t_4/(2(9m+7n)) = Y$ when (9) may be written as

$$Y^2 = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4, \tag{11}$$

where

$$\begin{aligned} a_1 &= -4(15m+n)(11m+7n)(3m+4n)U/(9m+7n)^2, \\ a_2 &= 2(11250m^4 + 20790m^3n + 13521m^2n^2 + 1848mn^3 + 23n^4)U^2/(9m+7n)^2, \\ a_3 &= -4(11m+7n)(1800m^4 + 4410m^3n + 565m^2n^2 + 49mn^3 + 36n^4)U^3/(9m+7n)^2, \\ a_4 &= (129600m^6 + 352800m^5n + 427780m^4n^2 + 83300m^3n^3 - 37931m^2n^4 \\ & \quad + 882mn^5 + 3969n^6)U^4/(9m+7n)^2. \end{aligned}$$

Four solutions $(T_i, Y_i), i = 1, 2, 3, 4$, of the quartic equation (11), obtained as described above by using the condition of triviality, are as follows:

$$\begin{aligned}
&T_1 = -(16m+9n)U, && Y_1 = -216(7m+3n)(3m+n)(m+n)U^2/(9m+7n),\\
&T_2 = (5m+2n)U, && Y_2 = -15(m-n)(3m-n)(7m+3n)U^2/(9m+7n),\\
&T_3 = -(5m-9n)U/2, && Y_3 = -135(3m-n)(7m-3n)(m+n)U^2/(4(9m+7n),\\
&T_4 = (8m-n)U, && Y_4 = -24(m-n)(3m+n)(7m-3n)U^2/(9m+7n).
\end{aligned}$$

A method of combining two known solutions of the quartic equation (11) to generate a new solution has been given by Choudhry [5, Theorem 5]. Applying this method, we obtain two solutions of (11) by first combining the solutions (T_1, Y_1) and (T_2, Y_2) and then by combining the solutions (T_3, Y_3) and (T_4, Y_4). These two solutions of (11) are given by

$$T = (420m^2 + 67mn - 63n^2)U/(21m + 11n), \tag{12}$$

and

$$T = (5880m^2 - 533mn - 1197n^2)U/(41(21m - 11n)). \tag{13}$$

The values of T given by (12) and (13) also naturally yield solutions of (9). These solutions are clearly much simpler than the solution (10) obtained by Fermat's method. Using these two solutions and working backwards, we obtain two sets of values of a and b which are such that there exist rational points on the corresponding Huff curves (1) having abscissae $0, \pm1, \pm2, \pm3, \pm4$ and thus there are arithmetic progressions of length 9 on these Huff curves. The two sets of values of a and b are given by

$$\begin{aligned}
a &= (3m-n)(3m+n)(7m+3n)(21m+11n)(3m^2-n^2)\\
&\quad\times(21m^2-4mn-7n^2)(21m^2-6mn-7n^2)\\
&\quad\times(16(189m^4+54m^3n-66m^2n^2-19mn^3+2n^4)n)^{-2},\\
b &= (63m^4-3m^3n-27m^2n^2+3mn^3+4n^4)\\
&\quad\times(4(189m^4+54m^3n-66m^2n^2-19mn^3+2n^4))^{-1},
\end{aligned}\tag{14}$$

and by

$$\begin{aligned}
a &= -41(3m-n)(3m+n)(7m-3n)(21m-11n)(3m^2+n^2)\\
&\quad\times(147m^2-164mn+49n^2)(399m^2-492mn+133n^2)\\
&\quad\times(130977m^5-192969m^4n+229014m^3n^2\\
&\qquad-148326m^2n^3+34889mn^4-1105n^5)^{-2},\\
b &= -(130977m^5-220311m^4n+91254m^3n^2\\
&\qquad+10566m^2n^3-11031mn^4+1105n^5)\\
&\quad\times(261954m^5-385938m^4n+458028m^3n^2\\
&\qquad-296652m^2n^3+69778mn^4-2210n^5)^{-1},
\end{aligned}\tag{15}$$

where m, n are arbitrary rational parameters.

For the first set of values of a, b given by (14), we must choose m, n such that

$$(m-n)(m+n)(3m+n)(7m+3n)(3m-n)(21m+11n)n \neq 0,$$

and for the second set of values of a, b given by (15), we must choose m, n such that

$$(m-n)(m+n)(3m-n)(7m-3n)(3m+n)(21m-11n) \neq 0.$$

These conditions are necessary to ensure that a, b satisfy the condition $ab(a-b) \neq 0$.

As specific examples, taking $(m, n) = (1, -2)$ in (14) and $(m, n) = (0, 1)$ in (15), we get the following two Huff curves which have rational points having abscissae $0, \pm 1, \pm 2, \pm 3, \pm 4$:

$$x\left(\frac{25y^2}{1024} - 1\right) = y\left(\frac{x^2}{4} - 1\right),$$

and

$$x\left(\frac{8817501y^2}{1221025} - 1\right) = y\left(\frac{x^2}{2} - 1\right).$$

We note that in addition to the two parametrized families of Huff curves defined by the two sets of values of a, b given by (14) and (15), there are arithmetic progressions of length 9 also on the two families of Huff curves that are conjugates of the Huff curves already obtained. Further, as already mentioned, we can obtain infinitely many parametrized families of Huff curves with the desired property by using the infinitely many solutions of (9) and working backwards to find infinitely many sets of values of a, b such that there are arithmetic progressions of length 9 on the corresponding Huff curves. With these values of a, b, there are also arithmetic progressions with abscissae $0, \pm k, \pm 2k, \pm 3k, \pm 4k$ on the Huff curves $H(k^{-2}a, k^{-2}b)$ where k is a nonzero rational number.

3 Huff curves with arithmetic progressions of length 11

We will now obtain Huff curves on which there are arithmetic progressions of length 11. It is natural to perform trials to check if the parametrised Huff curves obtained in Section 2 have arithmetic progressions of length 11 for specific numerical values of m, n. However, trials performed on the range $|m| + |n| < 10000$ yielded no such result.

We therefore begin as in Section 2 and impose five conditions such that the Huff curve (1) has rational points with abscissae $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5$. As in Section 2, this leads to the conditions $b^2j^4 + (4a-2b)j^2 + 1 = t_j^2, j = 1, 2, 3, 4, 5$. The first four of these conditions, written in homogenized form, are given explicitly by (2) while the last condition, written similarly in homogenized form, is given by

$$625b^2 + 25(4a-2b)z + z^2 = t_5^2.$$

As in Section 2, we eliminate a from these equations to get the Eqs. (3), (4), (5) and the following additional equation,

$$600b^2 - 24z^2 + 25t_1^2 = t_5^2. \tag{16}$$

Since (3) may be written as $3(2b-z)(2b+z) = -(2t_1-t_2)(2t_1+t_2)$, it may be replaced by the following two linear equations in b, z, t_1, t_2,

$$3(2b-z) = -m_1(2t_1-t_2), \quad m_1(2b+z) = 2t_1+t_2, \tag{17}$$

where m_1 is an arbitrary rational parameter, and similarly, (4) may be replaced by the following two linear equations in b, z, t_1, t_3,

$$8(3b-z) = -m_2(3t_1-t_3), \quad m_2(3b+z) = 3t_1+t_3, \tag{18}$$

where m_2 is an arbitrary rational parameter. Solving the four linear equations given by (17) and (18), we obtain the following solution of equations (3) and (4):

$$\begin{aligned}
b &= -6m_1^2m_2 + 4m_1m_2^2 + 32m_1 - 18m_2,\\
z &= 12m_1^2m_2 - 12m_1m_2^2 + 96m_1 - 36m_2,\\
t_1 &= -m_1^2m_2^2 + 40m_1^2 - 15m_2^2 + 24,\\
t_2 &= -2m_1^2m_2^2 + 80m_1^2 - 72m_1m_2 + 30m_2^2 - 48,\\
t_3 &= -3m_1^2m_2^2 - 120m_1^2 + 192m_1m_2 - 45m_2^2 - 72,
\end{aligned}$$

where m_1 and m_2 are arbitrary rational parameters. Substituting these values in the Eqs. (5) and (16), we get the two equations,

$$\begin{aligned}
&(16m_2^4 + 5200m_2^2 + 25600)m_1^4 - (7200m_2^3 + 126720m_2)m_1^3\\
&\quad + (2160m_2^4 + 140832m_2^2 + 138240)m_1^2 - (47520m_2^3 + 172800m_2)m_1\\
&\quad + 3600m2^4 + 46800m_2^2 + 9216 = t_4^2,
\end{aligned} \tag{19}$$

and

$$\begin{aligned}
&(25m_2^4 + 16144m_2^2 + 40000)m_1^4 - (21888m_2^3 + 285696m_2)m_1^3\\
&\quad + (6894m_2^4 + 328032m_2^2 + 441216)m_1^2 - (107136m_2^3 + 525312m_2)m_1\\
&\quad + 5625m_2^4 + 145296m_2^2 + 14400 = t_5^2.
\end{aligned} \tag{20}$$

Solutions of the simultaneous equations (19) and (20) were obtained by trials. We took $m_1 = n_1/n_3$ and $m_2 = n_2/n_3$ where n_1, n_2, n_3 are integers and performed trials over the range $|n_1| + |n_2| + |n_3| \leq 2000$. This yielded several solutions, and working backwards we obtained seven distinct sets of values of a, b such that there are arithmetic progressions of length 11 on the corresponding Huff curves. We also worked out the conjugates of these Huff curves and thus obtained a total of 10 Huff curves on which there are arithmetic progressions of length 11. These results are listed in Table 1. The last three Huff curves in the table were found by taking conjugates of the curves found by trial. On each Huff curve listed in Table 1, there are rational points with abscissae $0, \pm1, \pm2, \pm3, \pm4, \pm5$.

Table 1: Huff Curves with Arithmetic Progressions of length 11

n_1	n_2	n_3	a	b
45	34	27	1247290/164019249	692/4269
96	115	40	29393/19784704	8/139
50	163	40	−1109295/19784704	−8/139
219	350	15	146965/60492	−97/1704
350	318	105	−49378329/518700625	−1009/9110
153	540	85	−25340042/164019249	−692/4269
175	681	30	−119821782951/583696000000	−5059/19100
			300817/120984	97/1704
			16143217/1037401250	1009/9110
			34781257049/583696000000	5059/19100

4 Acknowledgments

The author wishes to thank the anonymous referee for his comments.

References

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

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

[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] A. Choudhry, Quadratic diophantine equations with applications to quartic equations, *Rocky Mountain J. Math.*, to appear. Preprint available at http://arxiv.org/abs/1409.5527.

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

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

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

[9] D. Moody, Arithmetic progressions on Edwards curves, *J. Integer Seq.* **14** (2011), Paper 11.1.7.

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

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

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11D25.
Keywords: arithmetic progression, elliptic curve, Huff curve.

Received January 1 2015; revised version received March 23 2015. Published in *Journal of Integer Sequences*, May 19 2015.

Return to Journal of Integer Sequences home page.