COLLOQUIUM MATHEMATICUM

VOL. 148 2017 NO. 1

ON THE RANK OF ELLIPTIC CURVES WITH LONG ARITHMETIC PROGRESSIONS

BY

DUSTIN MOODY (Gaithersburg, MD) and ARMAN SHAMSI ZARGAR (Ardabil)

Abstract. We study the rank of elliptic curves associated to known curves of high arithmetic progressions. A set of rational points (x_i, y_i) on an elliptic curve E is said to be in arithmetic progression if the x-coordinates x_i form an arithmetic progression. One of the motivations for finding curves with long progressions is to construct elliptic curves with high rank. We examine several curve families with long progressions and find their generic rank over $\mathbb{Q}(t)$, in addition to computing the rank of the specific curves with the longest progressions. We show that one of the infinite curve families with an arithmetic progression of length 12 has rank at least 8 over $\mathbb{Q}(t)$, and give generators.

1. Introduction. Elliptic curves have interested mathematicians for well over a century. Over a field $\mathbb{K}$, an elliptic curve is a nonsingular curve of genus 1 with a distinguished point. In this work, we will primarily consider elliptic curves defined over the rationals. The famous Mordell–Weil theorem for elliptic curves over $\mathbb{Q}$ states that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$. The set $E(\mathbb{Q})_{\text{tors}}$ is a finite group of torsion points, and the nonnegative integer r is known as the *rank* over the curve.

There has been much work to determine the rank of elliptic curves. Despite this, there is no known algorithm guaranteed to compute the rank. It has been conjectured that the rank can be arbitrarily high, although the highest known rank is at least 28, found by Elkies (see [D] for a table of rank records). As a result, there has been much interest in finding elliptic curves with high rank. This appears to be one of the motivations for a line of research dealing with finding arithmetic progressions on elliptic curves.

A set of rational points (x_i, y_i) on an elliptic curve E is said to be in arithmetic progression if the x-coordinates x_i form an arithmetic progression. One of the early papers in this area, due to Bremner [B], states:

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11B25.
Key words and phrases: elliptic curve, arithmetic progression, rank.
Received 17 August 2016; revised 7 September 2016.
Published online 17 February 2017.

DOI: 10.4064/cm7036-9-2016

> It seems that points of an arithmetic progression tend to be linearly independent in the group of rational points. (...) Accordingly, progressions of length 9 or more, if they exist, should occur on curves of relatively high rank and correspondingly large coefficients.

Bremner was able to construct an infinite number of elliptic curves which had arithmetic progressions of length 8. The progressions were found on the traditional model for elliptic curves, the Weierstrass model given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^2 + a_6,$$

with the a_i in $\mathbb{Q}$. Since then, others have explored finding longer progressions on other models of elliptic curves. Campbell, Ulas, MacLeod, and Alvarado examined quartic models for elliptic curves and found an infinite number of such curves with progressions of length 10, and specific curves with 14-term progressions [A, Ca, Ma, U1]. Moody and Choudhry constructed long progressions on Huff curves [Ch, Moo2], and Moody also studied progressions on Edwards curves [Moo1].

In this work, we investigate Bremner's intuition that elliptic curves with long progressions should have relatively high rank. We use some theorems from Gusić and Tadić [GT1, GT2] to determine the generic ranks of the infinite families with long arithmetic progressions. We then construct subfamilies of these curves with long progressions which have even higher rank. We perform a computer search within these families to find specific curves with high rank. We also compute the ranks of the curves which hold the records for longest progression for each model of elliptic curve.

Our results can be seen as evidence that families of curves with long progressions do have high rank, particularly for Weierstrass curves. Indeed, although other models have longer arithmetic progressions, the Weierstrass families of curves with long progressions have the highest generic rank over $\mathbb{Q}(t)$, with a rank of 8. This is caused in part by the use of symmetry to construct long progressions. For example, on the quartic, Edwards, and Huff models, if (x, y) is a rational point on the curve, then so is $(-x, y)$. Thus k points on the curve can be used to create progressions of length $2k$ or $2k + 1$ on the curve. However, the points (x, y) and $(-x, y)$ are not linearly independent, and so the rank does not increase. For a summary of our results, see Tables 1 and 2.

2. Weierstrass curves. As is well known, every elliptic curve E over a field $\mathbb{K}$ may be represented by a Weierstrass equation, $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with the a_i in $\mathbb{K}$. If the characteristic of $\mathbb{K}$ is not 2 or 3, then by a suitable change of variables, E may be represented with a short Weierstrass equation $y^2 = x^3 + Ax + B$. It suffices to use the short Weierstrass form for constructing curves with long arithmetic progressions,

Table 1. Ranks of elliptic curves with long arithmetic progressions. The "$\geq$" sign indicates the rank could not be computed exactly, but a lower bound was found.

Curve family	Longest arithmetic progression	Highest rank of curves with longest progression
Weierstrass [B]	8	8
Weierstrass [Ca]	8	≥ 6
Quartic [Ca]	12	4
Quartic [U1]	12	6
Quartic [A]	14	8
Quartic [Ma]	14	7
Huff [Moo2]	9	≥ 4
Huff [Ch]	11	6
Edwards [Moo1]	9	5

Table 2. Ranks of infinite elliptic curve families with long arithmetic progressions. A *parameterized* elliptic curve family is one whose curve coefficients are defined over $\mathbb{Q}(t)$. A *conditional* infinite family is one which is parameterized by the points of a positive rank curve. The "$\geq$" sign indicates the rank could not be computed exactly, but a lower bound was found.

Curve family	Longest progressions in parameterized family	Longest progressions in (conditionally) infinite family	Generic rank of parameterized family	Highest rank of subfamily	Highest rank examples
Weierstrass [B]	7	8	5	6 (cond.)	8
Weierstrass [Ca]	7	8	5	6 (cond.)	≥ 6
Quartic [A]	8	8	3	4, 5 (cond.)	12
Quartic [Ma]	8	10	2	4	≥ 7
Quartic [Ca]	9	9	8	8	≥ 8
Quartic [U1]	10	10	4	5, 6 (cond.)	7
Huff [Moo2]	7	9	2	4	≥ 4
Huff [Ch]	9	9	4	4	9
Edwards [Moo1]	7	9	2	3	5

since the change of variables preserves arithmetic progressions. Some of the first papers worked on finding progressions on special cases like the curves

$y^2 = x^3 + k$, or $y^2 = x^3 - n^2x$ (see [B, BST, LV, Moh, U2]). The best results for these curves were obtained by Ulas [U2], who (over $\mathbb{Q}(t)$) found infinitely many curves $y^2 = x^3 + k(t)$ with four linearly independent points in progression. However, Bremner, who considered more general Weierstrass curves, was able to find longer progressions.

2.1. Bremner's curves. Concretely, Bremner (in [B]) constructed the elliptic curve $E_{u,v} : y^2 = x^3 + A_4x + A_6$, with

$$A_4 = -252u^2v^2(u-v)^2(u-2v)^2,$$
$$A_6 = 324u^2v^2(u-v)^2(u-2v)^2(u^2-2uv+2v^2)^2.$$

The curve $E_{u,v}$ has a progression of length 7, as it has rational points with x-coordinates $-3d, -2d, -d, 0, d, 2d, 3d$, where $d = 6uv(u-v)(u-2v)$.

Bremner further showed how to extend this family to an infinite number of elliptic curves with eight terms in progression. If we consider $x = 4d$, then there will be a rational point (x, y) whenever the following equation is satisfied (for some rational u, v, w):

$$u^4 + 20u^3v - 64u^2v^2 + 40uv^3 + 4v^4 = w^2. \tag{2.1}$$

This curve can be transformed into the Weierstrass equation $E : Y^2 = X^3 - X^2 - 36X + 36$. Given a point (X, Y), there is a corresponding point (u, v) which satisfies (2.1). The rank of E is 1 (as computed by SAGE [Sa]), meaning there are an infinite number of rational points on E, and hence an infinite number of curves with $x = 4d$, leading to an 8-term progression family. We call this infinite family *conditional*, by which we mean the curves in the family are parameterized by the points of an elliptic curve with positive rank. Thus Bremner constructed an infinite 7-term progression family, as well as a conditional infinite 8-term family.

THEOREM 2.1. *The rank of Bremner's curve family $E_{u,v}$ over $\mathbb{Q}(u, v)$ is at least 5, and the rank of the conditional 8-term family is at least 6.*

Proof. To determine the rank of $E_{u,v}$ over $\mathbb{Q}(u, v)$, we use the Silverman specialization theorem (see [Si, Therorem 11.4]). Specializing at $(u_0, v_0) = (1/2, 2)$, we have the curve $E_{1/2,2} : y^2 = x^3 - (27783/4)x + 22325625/64$. The five points $(-63/2, 5859/8)$, $(0, 4725/8)$, $(63/2, 3213/8)$, $(63, 3213/8)$, and $(189/2, 5859/8)$ are independent with infinite order. This is verified by computing the determinant of the Néron–Tate height pairing matrix of these five points, which is the nonzero value 20.4685795453747 as computed by SAGE. This guarantees the generic rank of the family of curves $E_{u,v}$ over $\mathbb{Q}(u, v)$ is at least 5.

Similarly, for the extended 8-term family, on the curve $E : Y^2 = X^3 - X^2 - 36X + 36$ we have the rational point $(21, -90)$. This corresponds to $(u, v) = (2/15, 1)$ under the birational transformation. The resulting curve $E_{2/15,1}$ has six linearly independent points with x-coordinates corresponding to $x = -3d, -2d, -d, 0, d, 4d$, where $d = 1456/1125$. We know the points are independent, since the determinant of their height pairing matrix is 808.310470655924. Thus, the conditional 8-term family has rank at least 6 over $\mathbb{Q}(u, v)$ by the specialization theorem. ∎

Besides the family of curves $E_{u,v}$, Bremner [B] also found (by a computer search) many other examples of elliptic curves in short Weierstrass form with 8-term arithmetic progressions. The curves found all have ranks between 4 and 8.

2.2. Campbell's curves. In [Ca], Campbell also constructed Weierstrass curves with long arithmetic progressions. His curve is given by the equation $E_m : y^2 = x^3 + A_2x^2 + A_4x + A_6$, with

$$\begin{aligned}
A_2 &= 236896m^4 - 9821952m^3 - 22598349824m^2 + 508953231360m \\
&\quad + 520252184657920, \\
A_4 &= 4515840(m^2 - 72256)(m^2 - 36m - 29920)(3995m^4 - 170772m^3 \\
&\quad - 374719456m^2 + 8157182208m + 8805680998400), \\
A_6 &= 3186376704(m^2 - 72256)^2(m^2 - 36m - 29920)^2(379m^2 - 8400m \\
&\quad - 17506624)^2.
\end{aligned}$$

If we set $d = -18816(m^2 - 72256)(m^2 - 36m - 29920)$, then E_m has an infinite number of 7-term progressions with x-coordinates $0, -d, -2d, -3d, -4d, -5d$, and $-6d$.

Enforcing a sixth point with x-coordinate $x_6 = -7d$ leads to the condition

$$\begin{aligned}
z^2 &= -264815m^4 - 19343520m^3 + 62846856064m^2 - 2906312951808m \\
&\quad - 495507443511296,
\end{aligned}$$

for some rational z. This quartic is equivalent to a rank 2 elliptic curve, which therefore has an infinite number of points (see [Ca] for full details).

THEOREM 2.2. *The rank of Campbell's curve family E_m over $\mathbb{Q}(m)$ is at least 5, and the rank of the extended 8-term family is at least 6.*

Proof. We again use Silverman's specialization theorem. Specialization at $m = 2$ shows that the five points with x-coordinates $0, -d, -2d, -3d, -4d$

on the specialized curve

$$Y^2 = X^3 + 521179622936064X^2 + 863035953782649251746834022 40X + 459255811354873178061517796179219175807 3856$$

are independent, since the determinant of their Néron–Tate height pairing matrix is the nonzero value 108786.137503878. Thus, the rank of the family E_m is at least 5.

For the extended family, we specialize at $m = -88$. The resulting Weierstrass curve is

$$Y^2 = X^3 + 321362607734784X^2 + 3068881550823685107486818304 0X + 916746096752559734758631272892734485037056.$$

The six points

$$\begin{aligned} P_1 &= (0, 957468587867278147584),\\ P_2 &= (-23073008910336, 606185903472909484032),\\ P_3 &= (-46146017820672, 294348096775366115328),\\ P_4 &= (-69219026731008, 24187896700883435520),\\ P_5 &= (-92292035641344, 188665594266890797056),\\ P_6 &= (-161511062372352, 360585721587016138752) \end{aligned}$$

are independent, as the corresponding determinant of the height paring matrix is 196.654126678448. Hence, there is a conditional family of curves with rank at least 6, having eight points in arithmetic progression. ∎

A computer search for specific curves of high rank was not successful, as the coefficients of the curves (even for small values of m) are quite large.

3. Quartic curves. Campbell was able to extend his method for constructing long progressions on (cubic) Weierstrass curves to similarly construct them on quartic curves, that is, elliptic curves given by $y^2 = h(x)$, where $h(x)$ is a degree 4 polynomial. The longest arithmetic progressions on elliptic curves have been found on curves given in the quartic model. Campbell's technique resulted in a 12-term progression, which was later beaten by a 14-term progression found by MacLeod [Ma]. In this section, we examine the ranks of the families of quartic curves which have long progressions.

3.1. Campbell's family of quartic curves. Campbell used an idea of Mestre [Me] to express the degree 10 polynomial $(x-a)\prod_{j=0}^{8}(x-j)$ in the form $u(x)^2 - v(x)$, where u has degree 5, and v degree 4 in $\mathbb{Q}(a)[x]$. By the construction, there are an infinite number of quartic curves $y^2 = v(x)$

with nine points in progression [Ca]. The polynomial $v(x) = \sum_{i=0}^{4} c_i x^4$ is given by

$$c_0 = \frac{1}{65536}(7a^4 - 180a^3 + 1776a^2 - 8640a + 26112)^2 a^2,$$

$$c_1 = \frac{1}{16384}(35a^8 - 1908a^7 + 47232a^6 - 739584a^5 + 7456512a^4 - 45093888a^3 + 149299200a^2 - 225607680a - 21233664)a,$$

$$c_2 = \frac{1}{16384}(81a^8 - 4896a^7 + 154272a^6 - 2301696a^5 + 16962816a^4 - 61378560a^3 + 92749824a^2 + 9437184a + 21233664),$$

$$c_3 = \frac{1}{256}(3a^7 - 252a^6 + 4980a^5 - 41040a^4 + 155520a^3 - 235008a^2 - 16384a - 147456),$$

$$c_4 = \frac{1}{512}(21a^6 - 504a^5 + 4440a^4 - 17280a^3 + 26112a^2 + 32768).$$

Transforming this curve into short Weierstrass form $y^2 = x^3 + A_4 x + A_6$, we have

$$\begin{aligned} A_4 = -\frac{9(a-4)^2}{268435456}(&3155a^{14} - 176680a^{13} + 4248400a^{12} - 56925440a^{11} \\ &+ 462966016a^{10} - 2370119680a^9 + 8237690880a^8 \\ &- 25989611520a^7 + 96131350528a^6 - 273950965760a^5 \\ &+ 307484426240a^4 + 309371863040a^3 - 687463202816a^2 \\ &+ 57982058496a + 1043677052928), \end{aligned}$$

$$\begin{aligned} A_6 = -\frac{3(a-4)^4}{2199023255552}(&107567a^{20} - 8605360a^{19} + 287962240a^{18} \\ &- 5037104640a^{17} + 41829713408a^{16} \\ &+ 76074090496a^{15} - 6059336581120a^{14} \\ &+ 74590968217600a^{13} - 516822339223552a^{12} \\ &+ 2281393760501760a^{11} - 6533203053510656a^{10} \\ &+ 12130096617881600a^9 - 15908582956466176a^8 \\ &+ 19337448152629248a^7 - 25037606341312512a^6 \\ &+ 71607893782167552a^5 - 184989464118951936a^4 \\ &- 88318271501107200a^3 + 417159109624725504a^2 \\ &- 153896443516551168a - 461689330549653504). \end{aligned}$$

From the progression, we obtain eight points $P_i = (x_i, y_i)$ on the curve, with

$$\begin{aligned}
x_1 &= \frac{(a-4)^2}{16284}(49a^8 - 2058a^7 + 36283a^6 - 347640a^5 + 1946032a^4 \\
&\quad - 6290688a^3 + 10592256a^2 - 6758400a + 442368), \\
x_2 &= \frac{(a-4)^2}{65536}(49a^8 - 1988a^7 + 33276a^6 - 292832a^5 + 1385152a^4 \\
&\quad - 2899968a^3 - 442368a^2 + 7372800a + 1769472), \\
x_3 &= \frac{1}{147456}(49a^{10} - 2310a^9 + 46563a^8 - 519696a^7 + 3438240a^6 \\
&\quad - 12976128a^5 + 20853504a^4 + 22892544a^3 - 117522432a^2 \\
&\quad + 84934656a + 63700992), \\
x_4 &= \frac{a-4}{262144}(49a^9 - 2044a^8 + 35152a^7 - 316096a^6 + 1538560a^5 \\
&\quad - 3450880a^4 - 786432a^3 + 14352384a^2 + 14942208a - 28311552), \\
x_5 &= \frac{(a-4)^2}{409600}(49a^8 - 1778a^7 + 25251a^6 - 170744a^5 + 556336a^4 - 837888a^3 \\
&\quad + 36864a^2 - 368640a + 11059200), \\
x_6 &= \frac{1}{589824}(49a^{10} - 2100a^9 + 37356a^8 - 352512a^7 + 1991040a^6 - 8008704a^5 \\
&\quad + 26790912a^4 - 58392576a^3 + 589824a^2 + 226492416a + 254803968), \\
x_7 &= \frac{1}{802816}(49a^{10} - 2030a^9 + 34619a^8 - 309968a^7 + 1790624a^6 - 9783296a^5 \\
&\quad + 51129088a^4 - 153513984a^3 + 88326144a^2 + 473432064a + 346816512), \\
x_8 &= \frac{(a-4)^2}{1048576}(49a^8 - 1568a^7 + 18720a^6 - 98048a^5 + 645376a^4 - 7360512a^3 \\
&\quad + 33472512a^2 - 30670848a + 28311552).
\end{aligned}$$

THEOREM 3.1. *The rank of Campbell's quartic curve family E_a over $\mathbb{Q}(a)$ is at least 8. The points $P_i(a)$, for $i = 1, \ldots, 8$, are linearly independent.*

Proof. Specializing at $a = -8/7$, the curve E_m is equivalent to the Weierstrass curve

$$y^2 = x^3 - \frac{29193944574263692032}{33232930569601}x + \frac{5370936563968738465484742656}{191581231380566414401}.$$

The eight points with x-coordinates

$$\frac{330138824112}{5764801}, \quad \frac{250629552}{5764801}, \quad \frac{-53142767312}{51883209}, \quad \frac{3975921072}{5764801},$$
$$\frac{5257004976}{5764801}, \quad \frac{13252418608}{51883209}, \quad \frac{91993718448}{282475249}, \quad \frac{17363117232}{5764801}$$

correspond to the points in progression with $x = 1, 2, 3, 4, 5, 6, 7, 8$. The

determinant of their height pairing matrix is $32394.875 \neq 0$. Thus the generic rank of Campbell's family is at least 8.

In fact, when $a = -8/7$, the generators of the resulting elliptic curve are

$$\begin{aligned}
G_1 &= \left(\tfrac{-4745502288}{5764801}, \tfrac{41743036108800}{1977326743}\right),\\
G_2 &= \left(\tfrac{-3312029520}{5764801}, \tfrac{984668285952}{40353607}\right),\\
G_3 &= \left(\tfrac{2193005232}{5764801}, \tfrac{909480960}{823543}\right),\\
G_4 &= \left(\tfrac{9616481712}{5764801}, \tfrac{16608120422400}{282475249}\right),\\
G_5 &= \left(\tfrac{14681278512}{5764801}, \tfrac{99374169600}{823543}\right),\\
G_6 &= \left(\tfrac{27169551792}{5764801}, \tfrac{261502525440}{823543}\right),\\
G_7 &= \left(\tfrac{46420577712}{5764801}, \tfrac{4138374758400}{5764801}\right),\\
G_8 &= \left(\tfrac{122590154160}{5764801}, \tfrac{125018237140992}{40353607}\right).
\end{aligned}$$

We see that the $P_i(-8/7)$ can be written in terms of the G_i via the transformation matrix

$$\begin{pmatrix}
-1 & -1 & 2 & 0 & -1 & 0 & 0 & -1\\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0\\
0 & 2 & -1 & 0 & 0 & -1 & -1 & 0\\
2 & 1 & -3 & 1 & 1 & 0 & -1 & 1\\
0 & 1 & 1 & -1 & 1 & 0 & 0 & 0\\
-1 & -1 & 1 & 0 & -1 & 1 & 0 & -1\\
0 & -1 & 0 & 1 & 0 & 1 & 1 & 0\\
0 & 1 & -1 & 0 & 0 & -1 & -1 & 1
\end{pmatrix},$$

which has determinant 1. The $P_i(-8/7)$ are thus generators. ∎

Attempts to find specific high rank curves within this family were not successful, as the coefficients are too large (even for small values of a). However, we were able to compute the rank of the curve with a progression of length 12, which was 4.

3.2. Ulas' family of quartic curves. Ulas later used the same technique as Campbell, but was able to create longer progressions [U1]. The quartic used to define the elliptic curve is $y^2 = \sum_{i=0}^{4} a_i x^i$, where

$$\begin{aligned}
a_0 &= 9(7744a^4 + 25216a^3 + 22544a^2 - 784a - 5831),\\
a_1 &= -66(a+1)(16a+21)(24a^2 - 52a - 119),\\
a_2 &= 3(a+1)(16a+21)(48a^2 - 709a - 1085),
\end{aligned}$$

$$a_3 = 66(a+1)(5a+7)(16a+21),$$
$$a_4 = -3(a+1)(5a+7)(16a+21).$$

For all but finitely many choices of a, the curve has a progression of length 10, with x-coordinates $1, \ldots, 10$. Ulas also showed the existence of infinitely many quartic elliptic curves containing twelve points in arithmetic progression, where each such curve comes from a point on an elliptic curve with positive rank. We attempted to compute the rank for several curves in these families with long progressions. The largest rank which we were able to compute was 6.

THEOREM 3.2. *The rank of Ulas' quartic curve family E_a is at least* 4 *over $\mathbb{Q}(a)$. There exist infinite subfamilies with ranks at least* 5 *and* 6.

Proof. Ulas used symmetry to construct his progression—if x' is an x-coordinate on the curve, then so is $11 - x'$, and these two points are actually inverses of each other. In other words, only five of the ten points in the progression could potentially be independent. We use Ulas' curve family in Weierstrass form. Using standard transformations, it is not hard to obtain a Weierstrass model $E_a : y^2 = x^3 + A_2x^2 + A_4x$, where

$$A_2 = -3(16a+21)(a+1)(96a^2+397a+371),$$
$$A_4 = 72(4a+7)(2a+7)(2a+3)(12a+17)$$
$$\times (4a+5)(6a+7)(16a+21)(a+1).$$

The ten points $P_i(a) = (x_i(a), \pm y_i(a))$ (which come from the progression) are then given by the x-coordinates

$$x_1 = (2a+3)(12a+17)(6a+7)(16a+21),$$
$$x_2 = 36(2a+3)(12a+17)(6a+7)(16a+21),$$
$$x_3 = (2a+7)(12a+17)(4a+5)(6a+7),$$
$$x_4 = 4(2a+7)(12a+17)(6a+7)(4a+5),$$
$$x_5 = 6(a+1)(4a+5)(6a+7)(16a+21).$$

It can be checked that $P_4(a) = P_1(a) + P_2(a) - P_3(a) - 2P_5(a)$. Specializing at $a = 2$, the determinant of the height pairing matrix associated to $P_1(a), P_2(a), P_3(a), P_5(a)$ is nonzero. The generic rank of Ulas' family is thus at least 4. We note that the rank is less than that of Campbell's family, even though both families were constructed using the same basic idea. This is because of the symmetry used in Ulas' construction.

We now show how to increase the rank, by focusing on a subfamily of the curves E_a. Observe that a value $\tilde{x}$ is a valid x-coordinate on the curve $\tilde{y}^2 = \tilde{x}^3 + A\tilde{x}^2 + B\tilde{x}$ if and only if $\tilde{x} + A + B/\tilde{x}$ is a rational square. Thus in seeking to find additional points on the curve, it is natural to try the

divisors of B. A search found that if we set

$$x_6 = 3(4a+7)(2a+3)(6a+7)(16a+21),$$

then we will get a rational point if $9a^2+132a+168$ is square. This is easily accomplished by parameterizing $a = (168-m^2)/(6(m-22))$. This leads to infinitely many rank 5 families. We remark there were many other alternate choices for x_6 among the divisors of B.

In fact, we can show these five points are generators of the free part of $E(\mathbb{Q}(m))$. We first use the isomorphism $(x,y) \to (k^2x, k^3y)$, where $k = 6(m-22)^2$, to map the coefficients to $\mathbb{Z}[m]$. It is then easily checked that $m = 1$ satisfies the conditions of [GT2, Theorem 1.3]. Note that when $m = 1$, then we deduce that the points $P_1(1) = (526240, 9802272480)$, $P_2(1) = (18944640, 60250270080)$, $P_3(1) = (9579040, 31294723680)$, $P_5(1) = (810160, 11994418800)$, $P_6(1) = (2448160, 19279260000)$ on the rank 5 curve, $E_2 : y^2 = x^3 - 18980663x^2 + 192298385044480x$, are independent, since the determinant of their height pairing matrix is the nonzero value 385.239159126777. The relations

$$\begin{aligned} P_1(1) &= G_2, & P_5(1) &= G_1 - G_3 - G_4, \\ P_2(1) &= -G_2 - 2G_4 + G_5, & P_6(1) &= G_3 \\ P_3(1) &= -2G_1 + 2G_3 + 3G_4 - G_5 + E_2(0,0), \end{aligned}$$

show the points $P_i(1)$, and hence the points $P_i(m)$, are free generators, where $G_1 = (12103, 1524666780)$, $G_2 = (526240, 9802272480)$, $G_3 = (2448160, 19279260000)$, $G_4 = (5018728, -24767422680)$, and $G_5 = (203689984, -2775371483136)$ are generators of E_2 (as computed by SAGE). Note the determinant of the change of basis matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -2 & 1 \\ -2 & 0 & 2 & 3 & -1 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

is -1.

To further increase the rank to 6, we impose the additional condition that

$$x_7 = 3\frac{(38+2m^2-17m)(-14+m^2-7m)(42+8m^2-63m)(-36+m^2-6m)}{(m-22)^2}$$

be an x-coordinate on the curve. A calculation shows this requires $-256m^4 + 3696m^3 - 8391m^2 - 44748m + 97092$ to be a square. The quartic equation

being square is equivalent to the elliptic curve $E : Y^2 = X^3 - 89436027X - 248815866026$, which is a rank 2 curve. For every point (X, Y) on E, we can recover a corresponding value for m. Thus, we have an infinite number of curves, each of which has rank at least 6 (specialize at $m = 3$), which arises from Ulas' progression family. ∎

3.3. MacLeod's family of quartic curves. MacLeod [Ma] gives an 8-length arithmetic progression for quartic elliptic curves of the form $y^2 = ax^4 + bx^2 + c$ with the points $(\pm 1, p)$, $(\pm 3, q)$, $(\pm 5, r)$, $(\pm 7, s)$. The first three points imply

$$a = \frac{2p^2 - 3q^2 + r^2}{384}, \quad b = -\frac{34p^2 - 39q^2 + 5r^2}{192}, \quad c = \frac{150p^2 - 25q^2 + 3r^2}{128},$$

which forces $s^2 = 5p^2 - 9q^2 + 5r^2$ representing a quadric surface. He uses the following parameterization in u and v:

$$\begin{aligned} p &= -5u^2 - 9v^2 + 18uv + 5w^2 - 10uw, \\ q &= 5u^2 - 10uv + 9v^2 - 10vw + 5w^2, \\ r &= 5u^2 - 10uw - 9v^2 + 18vw - 5w^2, \\ s &= 5u^2 - 9v^2 + 5w^2 \end{aligned}$$

so that

$$\begin{aligned} a &= -\frac{(-9v + 5u + 5w)(-3v^2u + 6v^2w + 3vu^2 - 6vw^2 - 5wu^2 + 5w^2u)}{96}, \\ b &= \frac{(-9v + 5u + 5w)(-111v^2u + 150v^2w + 111vu^2 - 150vw^2 - 145wu^2 + 145w^2u)}{48}, \\ c &= \frac{1}{32}(7105uvw^2 + 800w^4 + 5635v^2uw - 12740u^2vw + 1600u^2w^2 \\ &\quad + 14270u^2v^2 - 6125u^3v + 3675u^3w - 11025v^3u - 4252v^2w^2 \\ &\quad - 3675w^3u + 2592v^4 + 800u^4 + 490vw^3 + 882v^3w). \end{aligned}$$

MacLeod was also able to find four examples of these curves which had abscissae $\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13$, yielding progressions of length 14. These four curves had ranks 4, 5, 6 and 7.

THEOREM 3.3. *MacLeod's family of quartic curves with arithmetic progressions of length* 8 *has rank at least* 2 *over* $\mathbb{Q}(u, v, w)$.

Proof. By using the standard transforms [Mor], the curve is transformed into

$$E_{u,v,w} : W^2 = U^3 + A_2U^2 + A_4U \tag{3.1}$$

with

$$A_2 = -6(-111v^2u + 150v^2w + 111vu^2 - 150vw^2 - 145wu^2 + 145w^2u) \times (-9v + 5u + 5w),$$
$$A_4 = 144(-5w + 3v)(-2w + u)(5u - 6v)(-5w + 5u + 3v)(-3w + u + 3v) \times (w + 3u - 3v)(w + 2u - 3v)(-9v + 5u + 5w).$$

The curve (3.1) has points with abscissae

$$U_1 = 24(5u - 6v)(w + 3u - 3v)(w + 2u - 3v)(-9v + 5u + 5w),$$
$$U_2 = 18(-2w + u)(w + 2u - 3v)(-9v + 5u + 5w)(-5w + 5u + 3v),$$

coming from the points $x = 3, 5$. The point with $x = 1$ leads to the point at infinity, and the other points do not turn out to be independent.

Specialization at $(u, v, w) = (0, 1, -1)$ shows that the points $P_1(0, 1, -1) = (32256, 3483648)$ and $P_2(0, 1, -1) = (16128, 193536)$ on the rank 2 curve $W^2 = U^3 - 25200U^2 + 148635648U$ are independent with determinant of their Néron–Tate height pairing matrix being 0.332545562300242. ∎

Starting with MacLeod's family, we were able to construct a subfamily with generic rank 4. However we omit the details as the subfamily constructed in the previous section has higher rank.

3.4. Alvarado's family of quartic curves. In her paper [A], Alvarado followed the same approach of MacLeod, except parameterizing p, q, r, s in a different way. Her results also produced an infinite family of curves with progressions of length 8, and led to 15 specific examples with progressions of length 14 (eleven of which were new). These 15 curves had ranks between 3 and 8.

THEOREM 3.4. *The generic rank of Alvarado's quartic curve family is at least* 3 *over* $\mathbb{Q}(u, v, w)$.

Proof. Using the standard transforms (see [Mor]), her curve familiy is transformed into $W^2 = U^3 + A_2U^2 + A_4U$, with

$$A_2 = 6(u + v + w)(25v^2w + 170v^2u + 5w^2v + 34u^2v + 29u^2w - 29w^2u),$$
$$A_4 = -144(w + 2v)(w + 2u)(-v + u)(w + 3u + 5v)(u + v + w) \times (-w + u + 3v)(-2w + u - 5v)(-3w + u + 5v).$$

The points corresponding to the x-coordinates $x = 3, 5, 7$ become

$$U_1 = -24(w + 2v)(-2w + u - 5v)(-w + u + 3v)(-3w + u + 5v),$$
$$U_2 = -18(w + 2v)(-v + u)(w + 3u + 5v)(-3w + u + 5v),$$
$$U_3 = 16(-v + u)(u + v + w)(-2w + u - 5v)(-3w + u + 5v).$$

The point with $x = 1$ leads to the point at infinity.

Specialization at $(u, v, w) = (0, 1, 1)$ shows that the points $P_1(0, 1, 1) = (2016, 96768)$, $P_2(0, 1, 1) = (648, 18144)$, $P_3(0, 1, 1) = (448, 9856)$ on the rank 3 curve $W^2 = U^3 + 360U^2 - 145152U$ are independent with the Néron–Tate height pairing matrix determinant 8.93242155257441. Thus Alvarado's family has rank at least 3 by Silverman's specialization theorem. ∎

We were able to increase the rank, by considering subfamilies of Alvarado's family. We constructed a subfamily with generic rank 4, as well as a conditional subfamily with rank 5. We omit the details, as the rank is not as high as that of the subfamily given in Section 3.2.

4. Huff curves. An elliptic curve in the Huff model is given by

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

These curves were originally introduced in 1948 [H], but recently have been shown to have applications in cryptography [JTV]. The torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Huff curves are easily transformed into Weierstrass curves of the form $y^2 = x^3 + (a - 2b)x^2 + b(a - b)x$ (see [Ch]).

In [Moo2], Moody examined finding long progressions on Huff curves. He produced four different parameterized infinite families, each of which had 7-term progressions coming from the x-coordinates in the set $\{-3, -2, -1, 0, 1, 2, 3\}$. We analyzed each family, and they all led to the same values for the columns in Tables 1 and 2. Thus, we only include the details for one of these families.

4.1. Moody's Huff curve family. Moody set $a = \frac{1}{4}b(3b - 1)(3b - 2) \times (b + 1)$, which leads to the curve $E_b : y^2 = x^3 + A_2x^2 + A_4x$ with $A_2 = b(-6 + 9b^3 - 7b)$, and $A_4 = -4b^2(b - 1)(3b + 2)(3b + 1)$. The three points

$$P_1(b) = (2b(3b + 1), 2b^2(3b - 1)(3b + 1)),$$
$$P_2(b) = (b(3b + 2), b^2(3b - 2)(3b + 2)),$$
$$P_3(b) = (2(3b + 2)(3b + 1)/9, 2(3b + 2)(3b - 1)(3b + 1)(3b - 2)/27)$$

correspond, respectively, to points with x-coordinates $x_1 = \pm 1$, $x_2 = \pm 2$ and $x_3 = \pm 3$ on the Huff curve.

THEOREM 4.1. *The rank of Moody's Huff curve family over $\mathbb{Q}(b)$ is exactly 2, with $P_1(b)$ and $P_2(b)$ as generators.*

Proof. A calculation finds $P_3(b) = -P_1(b) - P_2(b)$, and specialization easily shows that $P_1(b)$ and $P_2(b)$ are independent. Thus the rank is at least 2. We can actually prove the rank (over $(\mathbb{Q}(b))$ of this family is 2, and that $P_1(b)$ and $P_2(b)$ are generators.

Let $T_1(b) = (0, 0)$, $T_2(b) = (4b, 0)$, and $T_3(b) = (b(-9b^3 + 7b + 2), 0)$ be the three 2-torsion points. By [GT1, Theorem 3.1], these three x-coordinates

are the e_i (in their notation), and a computation checks that the value $b = 5$ satisfies the conditions of the theorem. Thus, rank $E_b(\mathbb{Q}(b)) = 2$. Continuing, with $b = 5$, E_5 is a rank 2 curve with generators $G_1 = (-4096, 150528)$ and $G_2 = (160, 11200)$. A calculation shows that $P_1(5) = G_2$ and $P_2(5) = G_1 - 2G_2 + T_3(5)$. As the determinant of the height pairing matrix of $\{P_1(5), P_2(5)\}$ is 1.84534817367656, and the transformation matrix has determinant -1, we can conclude that the points $P_1(5)$, $P_2(5)$, and hence $P_1(b)$, $P_2(b)$, are free generators, by [GT1, Corollary 3.2]. For $|b| \leq 100$, we computed the ranks of the curves E_b, for which the largest rank found was 4. ∎

COROLLARY 4.2. *There exists an infinite subset of Moody's Huff curve family with generic rank exactly* 4.

Proof. We construct a subfamily with rank 4. Let $x_3 = -2b(3b+1)$ and $x_4 = b(3b+1)(b-1)$, which we desire to be the x-coordinates of new points on the curve. The condition for x_3 leads to the equation $3b(3b-4) = y^2$, while that for x_4 leads to $3b(3b-5)$ needing to be square. We parameterize solutions of the first quadratic by setting $b = 4t^2/(3(t^2-9))$. The expression for x_4 becomes $x_4 = (t-3)(t+3)(t^2+27)(5t^2-9)$, and the condition for x_4 to be a valid x-coordinate on the curve is now $45 - t^2 = v^2$. We parameterize the rational solutions by $t = 3(u^2-4u-1)/(u^2+1)$, with curve coefficients transformed into

$$\begin{aligned} A_2 &= u^{12} - 24u^{11} + 206u^{10} - 708u^9 + 1176u^8 - 1080u^7 - 164u^6 + 1080u^5 \\ &\quad + 1176u^4 + 708u^3 + 206u^2 + 24u + 1, \\ A_4 &= 12(u^4 - 10u^3 + 17u^2 + 10u + 1)(u^4 - 12u^3 + 20u^2 + 12u + 1) \\ &\quad \times (u^4 - 2u^3 + 5u^2 + 2u + 1)(2u+1)^3(u-2)^3u^3 \end{aligned}$$

on the curve $E_u : y^2 = x^3 + A_2x^2 + A_4x$. We have four points $Q_i(u)$ with x-coordinates

$$\begin{aligned} x_1 &= 3(2u+1)^2(u-2)^2u^2(u^4 - 12u^3 + 20u^2 + 12u + 1), \\ x_2 &= 6(2u+1)^2(u-2)^2u^2(u^4 - 10u^3 + 17u^2 + 10u + 1), \\ x_3 &= -6(2u+1)^2(u-2)^2u^2(u^4 - 10u^3 + 17u^2 + 10u + 1), \\ x_4 &= -(2u+1)(u-2)u(u^4 - 2u^3 + 5u^2 + 2u + 1) \\ &\quad \times (u^4 - 10u^3 + 17u^2 + 10u + 1). \end{aligned}$$

Specialization at $u = 3$ shows the determinant of the height pairing matrix of these points on the rank 4 curve $E : y^2 = x^3 + 121402x^2 + 1141325640x$ is 28.4957071003444. We see the rank is at least 4.

We now show that $\operatorname{rank} E_u(\mathbb{Q}(u)) = 4$, and the four points whose x-coordinates are given by the x_i's are generators of E_u. To do so, we use

[GT2, Theorem 1.1], and check that $u = 3$ satisfies the hypotheses of the theorem, which shows the rank is 4. With this same value of u, the curve E has as generators $S_1 = (-12996, -1864584)$, $S_2 = (1080/49, 54465480/343)$, $S_3 = (1422, 1367964)$, and $S_4 = (137592, 71135064)$ as computed by SAGE. The points $Q_i(u)$ become $Q_1(3) = (-34398, 7980336)$, $Q_2(3) = (-13230, 1958040)$, $Q_3(3) = (13230, 6218100)$, and $Q_4(3) = (8295, 4288515)$, which are checked to be independent. Labelling the 2-torsion points as $T_1 = (0, 0)$, $T_2 = (-111132, 0)$, $T_3 = (-10270, 0)$, we have the following relations: $Q_1(3) = -S_1 + S_4$, $Q_2(3) = S_1 - S_2 - 2S_4$, $Q_3(3) = S_1 - S_3 + T_3$, and $Q_4(3) = -P_4 + T_1$. Since the transformation matrix has determinant 1, the four points $P_i(u)$ are therefore free generators of E_u. ∎

4.2. Choudhry's Huff curves. Choudhry was able to improve Moody's results for arithemetic progressions on Huff curves [Ch]. He found two parameterized families of Huff curves with progressions of length 9, as well as several Huff curves on which there are arithmetic progressions of length 11. Each of these 11-length progression curves has rank 4, 5, or 6. Both parameterized families have the same generic rank, so we only include the details for the first one.

The progression of length 9 has as abscissae $0, \pm1, \pm2, \pm3, \pm4$. Choudhry used the Huff curve $H_{a,b}$ with

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

THEOREM 4.3. *Choudhry's Huff curve family has rank* 4 *over* $\mathbb{Q}(m, n)$. *The points in the progression corresponding to* $x = 1, 2, 3, 4$ *are free generators.*

Proof. The isomorphic Weierstrass curve is given by $E_{m,n} : y^2 = x^3 + A_2x^2 + A_4x$, where

$$\begin{aligned} A_2 &= 1750329m^{10} + 833490m^9n - 3774519m^8n^2 - 1663200m^7n^3 \\ &\quad + 2143926m^6n^4 + 933660m^5n^5 - 477018m^4n^6 - 211680m^3n^7 \\ &\quad + 36689m^2n^8 + 18130mn^9 + 593n^{10}, \\ A_4 &= -64n^2(189m^4+54m^3n-66m^2n^2-19mn^3+2n^4)(63m^2-13n^2) \\ &\quad \times (63m^4-3m^3n-27m^2n^2+3mn^3+4n^4)(m-n)(m+n) \\ &\quad \times (21m^2+12mn+n^2)(63m^2-6mn-17n^2)(21m^2-5n^2). \end{aligned}$$

The points corresponding to the arithmetic progression $x = \pm i$ are mapped to $P_i(m,n) = (x_i, y_i)$, $i = 1,2,3,4$:

$$\begin{aligned}
x_1 &= 16n(189m^4 + 54m^3n - 66m^2n^2 - 19mn^3 + 2n^4)(n+m)\\
&\quad \times (63m^2 - 6mn - 17n^2)(21m^2 + 12mn + n^2),\\
x_2 &= 8n(189m^4 + 54m^3n - 66m^2n^2 - 19mn^3 + 2n^4)(m+n)\\
&\quad \times (21m^2 - 5n^2)(63m^2 - 13n^2),\\
x_3 &= \frac{16}{9}n(189m^4 + 54m^3n - 66m^2n^2 - 19mn^3 + 2n^4)(m+n)\\
&\quad \times (63m^2 - 13n^2)(-17n^2 - 6mn + 63m^2),\\
x_4 &= 4n(189m^4 + 54m^3n - 66m^2n^2 - 19mn^3 + 2n^4)(m+n)\\
&\quad \times (63m^2 - 6mn - 17n^2)(21m^2 - 5n^2).
\end{aligned}$$

Without loss of generality, we assume $m = 1$. We now show the rank is 4 over $\mathbb{Q}(n)$. The curve factors as $y^2 = (x - e_1)(x - e_2)(x - e_3)$, where $e_1 = 0$ and

$$\begin{aligned}
e_2 &= -(n-1)(n+1)(13n^2 - 63)(n^2 + 12n + 21)(17n^2 + 6n - 63)(5n^2 - 21),\\
e_3 &= 64n^2(63 - 3n - 27n^2 + 3n^3 + 4n^4)(189 + 54n - 66n^2 - 19n^3 + 2n^4),
\end{aligned}$$

so that

$$(e_1 - e_2)(e_1 - e_3)(e_2 - e_3) = 2^6 n^2 \prod_{i=1}^{15} f_i(n),$$

where the $f_i(n)$ are irreducible factors. The specialization $n = 2$ shows that the points

$$\begin{aligned}
P_1(1,2) &= (6957216, 19445418720), \qquad & P_3(1,2) &= (173536, 186551200),\\
P_2(1,2) &= (-45936, 25678224), & P_4(1,2) &= (35496, 43837560)
\end{aligned}$$

on the rank 4 curve $E : V^2 = U^3 + 851553U^2 + 22652695296U$ are independent with the determinant of their Néron–Tate height pairing matrix equal to 26.7353396147015. Hence, by [GT1, Theorem 3.1, Corollary 3.2], the injectivity is proven. The points $P_i(m,n)$ are free generators, since $P_1(1,2) = G_1 + G_3 + G_4 + T_2$, $P_2(1,2) = -G_4 + T_2$, $P_3(1,2) = -G_1 - G_4 + T_2$, $P_4(1,2) = -G_1 + G_2 - 2G_4$ where

$$T_1 = (0,0), \qquad T_2 = (-27489, 0), \qquad T_3 = (-824064, 0)$$

and the points $G_1 = (-44064, -23868000)$, $G_2 = (-27869, -2903770)$, $G_3 = (77616, 85765680)$, $G_4 = (1159536, -1652338800)$ are generators of E (calculated by SAGE), and since the transformation matrix is nonsingular with determinant 1. ∎

5. Edwards curves. Edwards curves were first introduced in 2007 [E]. After a simple change of variables, they can be written in the form $E_d : x^2 + y^2 = 1 + dx^2y^2$, with $d \neq 0, 1$. Following Moody [Moo1], we consider the Edwards curve E_d with

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

With this value of d, there are infinitely many Edwards curves with arithmetic progressions of length 9. For (almost) any value of m, the progression always contains the x-coordinates $0, \pm 1, \pm 2, \pm 3$.

THEOREM 5.1. *Moody's Edwards curve family has rank* 2 *over* $\mathbb{Q}(m)$.

Proof. Transforming this curve family into Weierstrass form, we obtain $E_m : y^2 = x^3 + A_2x^2 + A_4x$, where

$$A_2 = 256m^4 - 768m^3 + 1104m^2 - 2592m + 2916,$$
$$A_4 = 576m^2(16m - 27)^2(m - 2)^2.$$

The points

$$P_1(m) = \big(-648(m-2)^2, 432(8m^2 - 27)(m-2)^2\big),$$
$$P_2(m) = \big(-3(16m-27)^2, 3(8m^2 - 27)(16m-27)^2\big),$$
$$P_3(m) = \big(24m(16m-27)(m-2), 48m(16m-27)(m-2)(8m^2-27)\big)$$

correspond to the points $x_1 = \pm 3$, $x_2 = \pm 2$ and $x_3 = \pm 1$. We note that $2P_3(m) = -2P_3(m) = (0, 0)$, and so $P_3(m)$ is of order 4.

Specialization at $m = 1$ shows that the points $P_1(1) = (-648, 8208)$ and $P_2(1) = (-363, 6897)$ on the rank 2 curve $y^2 = x^3 + 916x^2 + 69696x$ are independent with the determinant of the Néron–Tate height pairing matrix computed to be 2.44026401649641.

Using [GT2, Theorem 1.3] we show the rank is 2. The curve E_m factors as $y^2 = (x - e_1)(x - e)(x - \bar{e})$, where $e_1 = 0$ and

$$e = -128m^4 + 384m^3 - 552m^2 + 1296m - 1458 + 2(-27 + 8m^2)\sqrt{64m^4 - 384m^3 + 984m^2 - 1296m + 729},$$
$$\bar{e} = -128m^4 + 384m^3 - 552m^2 + 1296m - 1458 - 2(-27 + 8m^2)\sqrt{64m^4 - 384m^3 + 984m^2 - 1296m + 729}.$$

We have

$$e_1^2 - (e + \bar{e})e_1 + e\bar{e} = 576m^2(16m - 27)^2(m - 2)^2,$$
$$(e - \bar{e})^2 = 16(64m^4 - 384m^3 + 984m^2 - 1296m + 729)(-27 + 8m^2)^2.$$

It can easily be seen that both conditions in $(\mathcal{A})$ of [GT2, Theorem 1.3] hold for $m = 1$. The curve $E_1 : y^2 = x^3 + 916x^2 + 69696x$ is generated

by $G_1 = (-792, 4752)$, $G_2 = (-648, 8208)$. By the relations $P_1(1) = G_2$, $P_2(1) = -G_1 + 3T$, where $T = (264, 10032)$ is a 4-torsion point, the points $P_1(m)$ and $P_2(m)$ are thus free generators. Note the transformation matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ has determinant 1. ∎

COROLLARY 5.2. *There exists an infinite subfamily of Moody's Edwards curve family with rank at least* 3.

Proof. We show how to increase the rank by restricting to a subfamily. Imposing

$$x_4 = -12m(m-2)^2(16m-27),$$

we are led to solve

$$729 - 432m^2 + 81m^3 + 16m^4 = w^2,$$

which is isomorphic to the rank 4 curve

$$y^2 + 4374y = x^3 - 432x^2 - 46656x + 20155392.$$

Specialization at $m = -9$ shows that the points

$$(-19602, 4057614),\ (-87723/4, 54475983/8),\ (-558657, 60334956)$$

on the specialized rank 3 curve $y^2 = x^3 + 588789x^2 + 10317277476x$ have determinant of the corresponding Néron–Tate height pairing matrix equal to 16.3097088159316. Thus the rank of this subfamily is at least 3. ∎

6. Heuristics. We performed a computer search to look for individual curves from each of the curve families with long progressions described in this paper. Computing the rank of an elliptic curve is nontrivial, so we used Mestre–Nagao sums [Me, N] to perform an initial sieving process. These sums are of the form

$$S(N, E) = \sum_{p \le N,\, p \text{ prime}} \left(1 - \frac{p-1}{\#E(\mathbb{F}_p)}\right) \log p.$$

Elliptic curves with large rank tend to have high Mestre–Nagao sums $S(N, E)$. For our calculations, we searched for curves which satisfied $S(523, E) > 25.41$, $S(1979, E) > 40.52$, $S(3559, E) > 48.11$, and $S(7907, E) > 55.58$. After this initial sieving, we calculated the Selmer rank of the remaining curves with Cremona's `mwrank` program [Cr], and then computed the rank of those curves with high Selmer rank using SAGE. The results for each class of curve families are described in the following sections.

6.1. High rank Weierstrass curves. As mentioned in Section 2, we attempted to compute ranks for the families of Weierstrass curves with long arithmetic progressions. The coefficients of the resulting curves were too

large to enable computing many ranks. Thus, we do not include any results for these curves.

6.2. High rank quartic curves. We searched among the various quartic curve progression families in Section 3, and found the highest rank curves which we could compute in Alvarado's family. For some of the quartic curve families, the coefficients quickly grew too large to compute their ranks.

Without loss of generality, when considering Alvarado's quartic curves we assumed $w = 1$. We searched for high rank curves among this family, and found several curves with rank 11 and two curves with rank 12. We searched for (u, v) with $|u, v| < 2500$ as well as for u, v fractions whose numerator and denominator were bounded by 50. The rank 11 and 12 curves are listed in Table 3. We verified the curves listed are all nonisomorphic, by computing their j-invariants.

Table 3. High rank Alvarado's curves with $w = 1$

u	v	Rank	u	v	Rank
572	−1198	12			
979	−1690	12			
$-\frac{47}{5}$	$\frac{29}{38}$	11	−1265	−308	11
$-\frac{19}{9}$	$-\frac{2}{31}$	11	−490	−909	11
$-\frac{38}{27}$	$\frac{31}{41}$	11	−454	70	11
$-\frac{31}{3}$	$\frac{11}{43}$	11	289	686	11
$-\frac{31}{50}$	$\frac{1}{47}$	11	1084	73	11
$-\frac{19}{34}$	$\frac{14}{45}$	11	1985	823	11
−1949	484	11	2064	−200	11
−1667	547	11	2362	2013	11
−1579	1119	11			

6.3. High rank Huff curves. When searching for high rank Huff curves, we found the highest ranks in Choudhry's family. We were able to compute ranks for curves with $|m|, |n| \leq 25$, and found that when $(m, n) = (20, 7)$, the curve $E_{m,n}$ had rank 9. We also found another rank 9 curve from Choudhry's second family (whose details we did not include in this paper). The record for elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is 15, and there are only seven known curves with this torsion group having rank higher than 10 [D].

6.4. High rank Edwards curves. We computed some curves from the Edwards progression family in Section 5. The coefficients of the curves with large Mestre–Nagao sums were too large to compute the ranks exactly, but

we were able to obtain upper bounds. Only two curves had upper bound 7, while the rest had upper bounds at most 6. We did find several curves with rank 5:

$$m = \frac{11}{15}, -\frac{10}{13}, \frac{8}{23}, -\frac{22}{13}, \frac{19}{15}, -\frac{19}{7}, \frac{17}{20}, -\frac{17}{14}, \frac{21}{23}, -\frac{3}{19}, \frac{1}{23}.$$

We searched for rational values of m, whose numerator and denominator were bounded in absolute value by 25. The record for curves with torsion group $\mathbb{Z}/4\mathbb{Z}$ is 12 [D].

7. Conclusion. In this paper we investigated the relationship between elliptic curves with long arithmetic progressions and their rank. One of the initial motivations for constructing curves with long progressions was to find high rank curves. We found that especially for Weierstrass curves, the points in the progression do tend to be linearly independent, leading to high rank curves. This relationship was not as strong for the other curve families. Nonetheless, finding long progressions on the various models of elliptic curves is interesting from the perspective of Diophantine equations.

Similar to finding arithmetic progressions on elliptic curves, some researchers have looked at geometric progressions. We leave it as future work to examine the ranks of the families with long geometric progressions. In general, the lengths of the progressions are less, which potentially means the families do not have as high rank. For example, the longest progressions on quartic curves have seven terms, while for most other models of curves the progressions are of length 5.

REFERENCES

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

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

[BST] A. Bremner, J. H. Silverman and N. Tzanakis, *Integral points in arithmetic progression on* $y^2 = x(x^2 - n^2)$, J. Number Theory 80 (2000), 187–208.

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

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

[Cr] J. Cremona, `mwrank` *program*, http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/.

[D] A. Dujella, *High rank elliptic curves with prescribed torsion*, http://web.math.pmf.unizg.hr/~duje/tors/tors.html.

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

[GT1] I. Gusić and P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III 47 (2012), 265–275.

[GT2] I. Gusić and P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory 148 (2015), 137–152.

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

[JTV] M. Joye, M. Tibouchi, and D. Vergnaud, *Huff's model for elliptic curves*, in: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 6197, Springer, Berlin, 2010, 234–250.

[LV] J.-B. Lee and W. Y. Vélez, *Integral solutions in arithmetic progression for* $y^2 = x^3 + k$, Period. Math. Hungar. 25 (1992), 31–49.

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

[Me] J.-F. Mestre, *Construction d'une courbe elliptique de rang* ≥ 12, C. R. Acad. Sci. Paris Sér. I Math. 295 (1982), 643–644.

[Moh] S. P. Mohanty, *On consecutive integral solutions for* $y^2 = x^3 + k$, Proc. Amer. Math. Soc. 48 (1975), 261–265.

[Moo1] D. Moody, *Arithmetic progressions on Edwards curves*, J. Integer Sequences 14 (2011), paper 11.1.7.

[Moo2] D. Moody, *Arithmetic progressions on Huff curves*, Ann. Math. Inform. 38 (2011), 111–116.

[Mor] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1968.

[N] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Ser. A Math. Sci. 69 (1993), 291–293.

[Sa] *Sage software, version 4.5.3*, http://sagemath.org.

[Si] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[U1] M. Ulas, *A note on arithmetic progressions on quartic elliptic curves*, J. Integer Sequences 8 (2005), paper 05.3.1.

[U2] M. Ulas, *Rational points in arithmetic progressions on* $y^2 = x^n + k$, Canad. Math. Bull. 55 (2012), 193–207.

Dustin Moody
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-8930, U.S.A.
E-mail: dustin.moody@nist.gov

Arman Shamsi Zargar
Young Researchers and Elite Club
Ardabil Branch
Islamic Azad University
Ardabil, Iran
E-mail: shzargar.arman@gmail.com