ACTA ARITHMETICA
167.2 (2015)

# On arithmetic progressions on Edwards curves

by

Enrique González-Jiménez (Madrid)

**1. Introduction.** Let $F(x,y) \in \mathbb{Q}[x,y]$ be a polynomial in two variables whose locus defines a plane model of an elliptic curve $E$ over $\mathbb{Q}$. We say that a rational number $x$ belongs to $E(\mathbb{Q})$ if $x$ is the $x$-coordinate of a point $P \in E(\mathbb{Q})$. We also say that $P_1,\ldots,P_n \in E(\mathbb{Q})$ are in arithmetic progression if the corresponding $x$-coordinates $x_1,\ldots,x_n$ form an arithmetic progression. Several authors [1, 2, 6, 8, 11, 13, 14, 17–25] have studied arithmetic progressions on $E(\mathbb{Q})$ for different shapes of the polynomial $F(x,y)$, and some of these authors have worked with $y$-coordinates instead of $x$-coordinates. It is interesting to point out that the shape of the polynomial $F(x,y)$ makes a big difference in this context. For example, if $F(x,y)$ is symmetric in both variables then there is no difference between studying the points with respect to $x$-coordinates or to $y$-coordinates. This is the case of the so called Edwards curves, when $F(x,y) = x^2+y^2-1-dx^2y^2$ for some $d \in \mathbb{Q}$, $d \neq 0,1$. These elliptic curves will be denoted by $E_d$. They have been deeply studied in cryptography and it has been found that the resulting addition formulas are very efficient, simple and symmetric (for instance, without distinction of addition and doubling).

In this paper we focus on Edwards curves. The starting point is Moody's paper [20] where the case $0,\pm1,\pm2,\ldots$ is studied, and in particular it is proved that there are infinitely many choices of $d$ such that $0,\pm1,\ldots,\pm4$ form an arithmetic progression on $E_d(\mathbb{Q})$. At the end of his paper, Moody asked if this arithmetic progression could be longer and he tried, with no success, by computer search, to find a rational $d$ such that $\pm5$ also belongs to the arithmetic progression. We prove that a rational $d$ such that $0,\pm1,\pm2,\pm3,\pm4,\pm5$ form an arithmetic progression in $E_d(\mathbb{Q})$ does not exist. Moreover, Moody stated that it was an open problem whether there is an Edwards curve with an arithmetic progression of length 10 or longer. Although we have found no

2010 *Mathematics Subject Classification*: Primary 11G05, 11G30; Secondary 11B25, 11D45, 14G05.
*Key words and phrases*: arithmetic progression, elliptic curves, Edwards curves.

DOI: 10.4064/aa167-2-2  

answer to this question, we will try to convince the reader that the maximum possible length of an arithmetic progression on an Edwards curve is 9.

Let $m \in \mathbb{Z}_{>0}$ and $a, q \in \mathbb{Q}$ with $q > 0$, and denote

$$\mathcal{AP}_m(a,q) = \{d \in \mathbb{Q} \mid a, a+q, a+2q, \dots, a+(m-1)q \text{ in } E_d(\mathbb{Q})\}.$$

Note that $\mathcal{AP}_m(a,q) = \mathcal{AP}_m(a+(m-1)q, -q)$, so we can assume without loss of generality that $q > 0$.

Let us restrict for a moment to the case of *symmetric* progressions, i.e. such that if an element belongs to the sequence, then so does its opposite. There are two possibilities: either $a = 0$ (*central*) or $a = \pm q/2$ (*non-central*). Note that if $0, q, \dots, mq$ belong to $E_d(\mathbb{Q})$, then so do $-q, \dots, -mq$. Therefore we denote

$$\mathcal{S}_{\mathrm{c}}\mathcal{AP}_{2m+1}(q) = \mathcal{AP}_{2m+1}(-mq, q).$$

Similarly, if $q/2, 3q/2, \dots, (2m-1)/2q$ belong to $E_d(\mathbb{Q})$, then so do $-q/2$, $-3q/2, \dots, -(2m-1)/2q$, and we denote

$$\mathcal{S}_{nc}\mathcal{AP}_{2m}(q) = \mathcal{AP}_{2m}(-(2m-1)q/2, q).$$

Therefore if we denote by $\mathcal{SAP}_m$ the set of rationals $d$ such that a symmetric arithmetic progression of length $m$ belongs to $E_d(\mathbb{Q})$, we have

$$\mathcal{SAP}_m(q) = \begin{cases} \mathcal{S}_{\mathrm{c}}\mathcal{AP}_m(q) & \text{if } m \text{ is odd}, \\ \mathcal{S}_{nc}\mathcal{AP}_m(q) & \text{if } m \text{ is even}. \end{cases}$$

Theorem 1.1 (Non-symmetric case). *Let $m \in \mathbb{Z}_{>0}$ and $a, q \in \mathbb{Q}$ be such that $q > 0$ and $(a,q)$ does not correspond to a symmetric arithmetic progression. Then*

(i) *$\#\mathcal{AP}_m(a,q) = \infty$ if $m \le 3$, except for maybe a finite number of pairs $(a,q)$.*
(ii) *$\#\mathcal{AP}_4(a,q) = \infty$ if and only if $a + kq \in \{\pm 1\}$ for some $k \in \{0,1,2,3\}$.*
(iii) *If $m \ge 5$, then $\#\mathcal{AP}_m(a,q) < \infty$ for any pair $(a,q)$.*

Theorem 1.2 (Central symmetric case). *Let $m \in \mathbb{Z}_{>0}$ be odd and $q \in \mathbb{Q}_{>0}$. Then:*

(i) *$\#\mathcal{S}_{\mathrm{c}}\mathcal{AP}_m(q) = \infty$ if $m \le 7$.*
(ii) *$\#\mathcal{S}_{\mathrm{c}}\mathcal{AP}_9(q) = \infty$ if and only if $q \in \{1, 1/2, 1/3, 1/4\}$.*
(iii) *If $m \ge 11$ and $q \in \{1, 1/2, 1/3, 1/4\}$, then $\#\mathcal{S}_{\mathrm{c}}\mathcal{AP}_m(q) = 0$.*

Theorem 1.3 (Non-central symmetric case). *Let $m \in \mathbb{Z}_{>0}$ even and $q \in \mathbb{Q}_{>0}$. Then:*

(i) *$\#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_m(q) = \infty$ if $m \le 6$.*
(ii) *$\#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_8(q) = \infty$ if and only if $q \in \{2, 2/3, 2/5, 2/7\}$.*
(iii) *If $m \ge 10$ and $q \in \{2, 2/3, 2/5, 2/7\}$, then $\#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_m(q) = 0$.*

A computer search was undertaken (see Section 6) to find a $q$ such that the set $\mathcal{SAP}_m(q)$ is non-empty for $m \geq 10$, but it was not successful. So we leave the following question to the reader:

QUESTION. *Is* 9 *the maximum length of an arithmetic progression on an Edwards curve, or in other words, is* $\#\mathcal{AP}_m(a,q) = 0$ *for any pair* $a, q$ *and* $m \geq 10$*?*

**2. Arithmetic-algebraic-geometric translation.** Let $d \in \mathbb{Q}$ be such that $d \neq 0, 1$. Then the Edwards curve is the elliptic curve defined by

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

We have $(\pm 1, 0), (0, \pm 1) \in E_d(\mathbb{Q})$ (called *trivial points* later). Moreover, since the model defined above is symmetric, it follows that if $(x, y) \in E_d(\mathbb{Q})$, then $(\pm x, \pm y), (\pm y, \pm x) \in E_d(\mathbb{Q})$.

If $(x, y) \in E_d(\mathbb{Q})$ is a non-trivial point, then we can recover $d$ from $(x, y)$:

$$d(x, y) = \frac{x^2 + y^2 - 1}{x^2y^2}.$$

Assume that this point has the form $(x, y) = (a + nq, w/z_n)$, where $n \in \mathbb{Z}_{\geq 0}$ and $a, q \in \mathbb{Q}$ with $q \neq 0$. Then we define

$$d_n := d\left(a + nq, \frac{w}{z_n}\right) = \frac{w^2 + z_n^2((a + nq)^2 - 1)}{(a + nq)^2w^2}.$$

Notice that $a + nq \neq 0, \pm 1$ and $w \neq \pm z_n$ (resp. $n, q, w \neq 0$) since $d_n \neq 0, 1$ (resp. the point is non-trivial).

Now, denote $\mathcal{S} = \{n_0, \ldots, n_{m-1}\} \subset \mathbb{Z}_{\geq 0}$. Then the finite set of equations

$$\mathcal{C}_{\mathcal{S}}^{a,q} : \{d_i = d_j \mid i, j \in \mathcal{S},\, i < j\}$$

defines a curve in $\mathbb{P}^m$, where the points are $[w : z_0 : \cdots : z_{m-1}]$. Moreover, it is easy to check that a model for this curve may be obtained by fixing one element of $\mathcal{S}$, say $n_0$, and varying the others:

$$\begin{aligned}\mathcal{C}_{\mathcal{S}}^{a,q} : \{(n_0 - n_j)q(2a + q(n_0 + n_j))w^2 + (a + n_jq)^2(1 - (a + n_0q)^2)z_{n_0}^2 \\ = (a + n_0q)^2(1 - (a + n_jq)^2)z_{n_j}^2\}_{j=1,\ldots,m-1}.\end{aligned}$$

That is, $\mathcal{C}_{\mathcal{S}}^{a,q}$ is the intersection of $m - 1$ quadric hypersurfaces in $\mathbb{P}^m$ and therefore its genus is $(m - 3)2^{m-2} + 1$ (cf. [16, Prop. 4] or [3]). Moreover, the points $[1 : \pm 1 : \cdots : \pm 1] \in \mathcal{C}_{\mathcal{S}}^{a,q}$ correspond to the disallowed case $d = 1$. Therefore, if $d \neq 0, 1$, we obtain the following bijection:

$$\begin{aligned}\{(a + n_iq, w/z_{n_i}) \in E_d(\mathbb{Q}) \setminus \{(\pm 1, 0), (0, \pm 1)\} \mid n_i \in \mathcal{S}\} \\ \leftrightarrow \mathcal{C}_{\mathcal{S}}^{a,q}(\mathbb{Q}) \setminus \{[\pm 1 : \cdots : \pm 1]\}.\end{aligned}$$

Remark 2.1. Note that if $a$ and $q$ are not fixed, then $\mathcal{C}_{\mathcal{S}}^{a,q}$ is a variety of dimension 3 in $\mathbb{P}^{m+2}$. Therefore, Edwards curves with $m$ points in arithmetic progression are characterized by the rational points of a variety of dimension 3. However, the computation of the whole set of rational points of a variety of dimension greater than one is still an intractable problem nowadays.

We are going to rewrite the equations of $\mathcal{C}_{\mathcal{S}}^{a,q}$. For this purpose, and for any $i,j,k \in \mathbb{Z}_{>0}$, we denote

$$s_{ij} = \frac{q(i-j)(2a+(i+j)q)}{(a+iq)^2(1-(a+jq)^2)}, \qquad r_{ij} = s_{ij}^{-1}, \qquad t_{ijk} = \frac{s_{ik}}{s_{ij}}.$$

Then

$$\mathcal{C}_{\mathcal{S}}^{a,q} : \{X_{j+1}^2 = a_j X_0^2 + (1-a_j)X_1^2\}_{j=1,\dots,m-1}$$

where $a_j = s_{n_0 n_j}$, $X_0 = w$ and $X_{j+1} = z_{n_j}$ for any $n_j \in \mathcal{S}$.

Now we parametrize the first equation as

$$[X_0 : X_1 : X_2] = [t^2 - 2t + a_1 : -t^2 + a_1 : t^2 - 2a_1 t + a_1].$$

Using this parametrization we substitute $X_0, X_1$ and $X_2$ in the other equations to obtain a new system of equations of the curve, which depends on the parameter $t$:

$$\mathcal{C}_{\mathcal{S}}^{a,q} : \{X_{j+1}^2 = t^4 - 4a_j t^3 + 2(-a_1 + 2a_j + 2a_1 a_j)t^2 - 4a_1 a_j t + a_1^2\}_{j=2,\dots,m-1}.$$

Notice that each single equation defines an elliptic curve $\mathbb{Q}$-isomorphic to the elliptic curve with Weierstrass model

$$\mathcal{C}_{\{n_0,n_1,n_j\}}^{a,q} : y^2 = x(x + a_1 - a_j)(x + a_j(a_1 - 1)).$$

Here the isomorphism sends $[1:1:1:1]$ to $\mathcal{O} = [0:1:0]$, and if we denote $P_0 = (0,0), P_1 = (a_j - a_1, 0), Q = (a_j, a_1 a_j)$ then it sends the set $\{[\pm 1 : \pm 1, \pm 1 : \pm 1]\}$ to $\{\mathcal{O}, P_1, P_2, P_1+P_2, Q, Q+P_1, Q+P_2, Q+P_1+P_2\}$.

Moreover, each pair of equations define a genus five curve $\mathcal{C}_{\{n_0,n_1,n_i,n_j\}}^{a,q}$ whose Jacobian $\mathrm{Jac}(\mathcal{C}_{\{n_0,n_1,n_i,n_j\}}^{a,q})$ splits completely over $\mathbb{Q}$ as the product of five elliptic curves. To check this, let us write $\mathcal{C}_{\{n_0,n_1,n_i,n_j\}}^{a,q}$ as (see [5])

$$\mathcal{C}_{\{n_0,n_1,n_i,n_j\}}^{a,q} : \begin{cases} X_2^2 = b_2 X_0^2 + (1-b_2)X_1^2, \\ X_3^2 = b_3 X_0^2 + (1-b_3)X_1^2, \\ X_4^2 = b_4 X_0^2 + (1-b_4)X_1^2, \end{cases} \tag{2.1}$$

where $X_3 = X_i$, $X_4 = X_j$ and $b_2 = a_1$, $b_3 = a_i$, $b_4 = a_j$. Then we have five quotients of genus one, each being the intersection of two quadric surfaces in $\mathbb{P}^3$. These are elliptic curve $E_{(k)}$ whose equations are obtained by removing the variable $X_k$ from the previous system of equations. We display the Weierstrass model for those elliptic curves together with a (generally) non-torsion point on it:

$$
\begin{aligned}
&E_{(4)}: y^2 = x(x+b_2-b_3)(x+b_3(b_2-1)), && Q_4 = (b_3, b_2b_3),\\
&E_{(3)}: y^2 = x(x+b_2-b_4)(x+b_4(b_2-1)), && Q_3 = (b_4, b_2b_4),\\
&E_{(2)}: y^2 = x(x+b_3-b_4)(x+b_4(b_3-1)), && Q_2 = (b_4, b_3b_4),\\
&E_{(1)}: y^2 = x(x+b_2(b_3-b_4))(x+b_4(b_3-b_2)), && Q_1 = (b_2b_4, b_2b_3b_4),\\
&E_{(0)}: y^2 = x(x+(b_2-1)(b_3-b_4))(x+(b_4-1)(b_3-b_2)),\\
&\qquad Q_0 = ((b_4-1)(b_2-1), (b_2-1)(b_3-1)(b_4-1)).
\end{aligned}
$$

Thus we have obtained $\operatorname{Jac}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}) \overset{\mathbb{Q}}{\sim} E_{(0)} \times E_{(1)} \times \cdots \times E_{(4)}$ (cf. [5]). In general, $\operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}) \geq 5 = \operatorname{genus}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}})$, that is, the classical Chabauty method [12] does not work to obtain $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q})$. The curve $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ has the same shape as the curve treated in [16] (with $m_0 = b_2-1$, $m_1 = -b_3$ and $m_2 = -b_4$), where we developed a method based on covering collections and elliptic Chabauty techniques to obtain (under some hypotheses) the set of rational points of those curves (see also [15]).

We now apply this method to our curves, so let us write $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ in the form

$$\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}} : \{X_k^2 = t^4 - 4b_kt^3 + 2(-b_2+2b_k+2b_2b_k)t^2 - 4b_2b_kt + b_2^2\}_{k=3,4}.$$

For $k \in \{3,4\}$ denote:

| l | $d_{k,l}$ | $e_{k,l}$ | $p_{k,l,\pm}(t)$ |
|---|---|---|---|
| 1 | $b_k(b_k-1)$ | $b_k(1-b_2)$ | $t^2-2(b_k\pm\alpha_{k,1})t+b_2(-1+2(b_k\pm\alpha_{k,1}))$ |
| 2 | $(b_k-1)(b_k-b_2)$ | $b_k-b_2$ | $t^2-2(b_k\pm\alpha_{k,2})t+b_2$ |
| 3 | $b_k(b_k-b_2)$ | 0 | $t^2-2(b_k\pm\alpha_{k,3})t-b_2+2(b_k\pm\alpha_{k,3})$ |

where $\alpha_{k,l} = \sqrt{d_{k,l}}$. Next, choose $l_3, l_4 \in \{1,2,3\}$ and for any $k \in \{3,4\}$ denote:

- $\phi_k : E'_{(k)} \to E_{(k)}$ the 2-isogeny corresponding to the 2-torsion point $(e_{k,l_k}, 0) \in E_{(k)}(\mathbb{Q})$,
- $L = \mathbb{Q}(\alpha_{3,l_1}, \alpha_{4,l_2})$,
- $\mathcal{S}_L(\phi_k)$ a set of representatives in $\mathbb{Q}$ of the image of the $\phi_k$-Selmer group $\operatorname{Sel}(\phi_k)$ in $L^*/(L^*)^2$ via the natural map,
- $\widetilde{\mathcal{S}_L}(\phi_3)$ a set of representatives of $\operatorname{Sel}(\phi_3)$ modulo the subgroup generated by the image of $[1:\pm1:\pm1:\pm1:\pm1]$ in this Selmer group,
- $\mathfrak{S} = \{\delta_3\delta_4 : \delta_3 \in \widetilde{\mathcal{S}_L}(\phi_3), \delta_4 \in \mathcal{S}_L(\phi_4)\} \subset \mathbb{Q}^*$,
- $H_s^\delta : \delta z^2 = p_{3,l_3,s_3}(t)p_{4,l_4,s_4}(t)$, a genus one curve for any $\delta \in \mathfrak{S}$ and $s = (s_3, s_4) \in \{\pm\} \times \{\pm\}$.

So we obtain

$$\left\{ t \in \mathbb{P}^1(\mathbb{Q}) \;\middle|\; \begin{array}{l} \exists X_3, X_4 \in \mathbb{Q} \text{ such that} \\ (t, X_3, X_4) \in \mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q}) \end{array} \right\}$$
$$\subseteq \bigcup_{\delta \in \mathfrak{S}} \left\{ t \in \mathbb{P}^1(\mathbb{Q}) \;\middle|\; \begin{array}{l} \exists w \in L \text{ such that } (t,w) \in H^\delta_s(L) \\ \text{for some } s \in \{\pm\} \times \{\pm\} \end{array} \right\}.$$

Note that to compute $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q})$ we must find a pair $l_3, l_4 \in \{1,2,3\}$ such that for any $\delta \in \mathfrak{S}$ we can find $s \in \{\pm\}\times\{\pm\}$ for which we can carry out all these computations to obtain the rational $t$-coordinates of $H^\delta_s(L)$. Before undertaking this task, however, we must face several problems, which in practice are solved by implementations in `Magma` [4]:

• Is $H^\delta_s(L)$ empty? To answer this question we use the Bruin and Stoll's algorithm [10]. If the answer is yes, we have finished with $\delta$ and turn to another element of $\mathfrak{S}$. Otherwise, we must find (by brute force) a point on $H^\delta_s(L)$.

• Once we have found a point on $H^\delta_s(L)$, we use it to create an $L$-isomorphism with its Jacobian $\mathrm{Jac}(H^\delta_s)$ and compute an upper bound for the rank $r$ of the Mordell–Weil group of the elliptic curve $\mathrm{Jac}(H^\delta_s)(L)$.

• If the rank $r < [L:\mathbb{Q}]$ we use the elliptic Chabauty algorithm (see [9]) to compute the $t$-coordinates of $H^\delta_s(L)$. For this purpose, we must first determine a system of generators of the Mordell–Weil group of $\mathrm{Jac}(H^\delta_s)(L)$.

If $\mathcal{S} = \{i,j,k,l\}$, then the curve $\mathcal{C}^{a,q}_{\mathcal{S}}$ is defined by $\{d_i = d_j,\ d_i = d_k,\ d_i = d_l\}$. Note that we may describe it by $\{d_{n_1} = d_{n_2},\ d_{n_3} = d_{n_4},\ d_{n_5} = d_{n_6}\}$ with $\{n_1,\dots,n_6\} = \{i,j,k,l\}$. If the order of the equations is assumed to be irrelevant, there are 16 such descriptions; that is, we can consider 16 models of $\mathcal{C}^{a,q}_{\mathcal{S}}$ of the form (2.1). The possible values of $b_2, b_3, b_4$ (as a set) appear in Table 1. Thus, we parametrized the first conic and make the appropriate substitutions on the other two conics. Therefore, if we take care now of the order of the equations, we have 48 different models of $\mathcal{C}^{a,q}_{\mathcal{S}}$ of the form (2.1). This is an important fact, since all the computations that we must carry out may only work (if they do) in a particular model. Notice that we only consider the case when $L$ is an at most quadratic field, as some of the computations are not well implemented for number fields of higher degree.

**Table 1.** Models for $\mathcal{C}^{a,q}_{\{i,j,k,l\}}$

| $N$ | $\{b_2,b_3,b_4\}$ | $N$ | $\{b_2,b_3,b_4\}$ | $N$ | $\{b_2,b_3,b_4\}$ | $N$ | $\{b_2,b_3,b_4\}$ |
|---|---|---|---|---|---|---|---|
| 1 | $s_{ij}, s_{ik}, s_{il}$ | 2 | $s_{ji}, s_{jk}, s_{jl}$ | 3 | $s_{ki}, s_{kj}, s_{kl}$ | 4 | $s_{li}, s_{lj}, s_{lk}$ |
| 5 | $r_{ij}, t_{ijk}, t_{ijl}$ | 6 | $r_{ik}, t_{ikj}, t_{ikl}$ | 7 | $r_{il}, t_{ilj}, t_{ilk}$ | 8 | $r_{ji}, t_{jik}, t_{jil}$ |
| 9 | $r_{jk}, t_{jki}, t_{jkl}$ | 10 | $r_{jl}, t_{jli}, t_{jlk}$ | 11 | $r_{ki}, t_{kij}, t_{kil}$ | 12 | $r_{kj}, t_{kji}, t_{kjl}$ |
| 13 | $r_{kl}, t_{kli}, t_{klj}$ | 14 | $r_{li}, t_{lij}, t_{lik}$ | 15 | $r_{lj}, t_{lji}, t_{ljk}$ | 16 | $r_{lk}, t_{lki}, t_{lkj}$ |

We will use the following notation:

**Table 2.** Notation for $\mathcal{C}_{\mathcal{S}}^{a,q}$

| $\mathcal{S}$ | $\mathcal{C}_{\mathcal{S}}^{a,q}$ | genus$(\mathcal{C}_{\mathcal{S}}^{a,q})$ |
|---|---|---|
| $\{i,j\}$ | $\mathcal{C}_{ij}(a,q)$ | 0 |
| $\{i,j,k\}$ | $\mathcal{E}_{ijk}(a,q)$ | 1 |
| $\{i,j,k,l\}$ | $\mathcal{D}_{ijkl}(a,q)$ | 5 |

**3. Proof of Theorem 1.1. Non-symmetric case.** We analyze under which conditions a non-symmetric arithmetic progression $a, a+q, \dots, a+(m-1)q$ belongs to $E_d$. In particular $a \notin \{0, \pm q/2\}$. For this purpose, we are going to use the translation given in the previous section with $\mathcal{S} = \{0, 1, \dots, m-1\}$. First notice that if $a + kq = 0$ then this case corresponds to the central symmetric case. Now, if $a + kq \in \{\pm 1\}$ for some $k \in \mathcal{S}$, then we have $d_k = 1$ and therefore we cannot use it and we should use instead the curve $\mathcal{C}_{\mathcal{S}^*}^{a,q}$, where $\mathcal{S}^*$ is $\mathcal{S}$ with such values of $k$ removed. Finally, if there exist $i, j \in \mathbb{Z}_{\geq 0}$, $i \neq j$, satisfying $a + iq = -1$ and $a + jq = 1$, then the arithmetic progression must necessarily extend to a symmetric one. Therefore, we can assume that there is at most one value of $k \in \mathcal{S}$ satisfying $a + kq = 1$ or $a + kq = -1$.

Let us prove the theorem depending on the set $\mathcal{S}^*$:

- $\#\mathcal{S}^* \leq 1$: These cases are particularly simple. If $a = \pm 1$ then the set $\mathcal{AP}_m(a,q)$ is described by $d \neq 1$ when $m = 1$ and by $d_1$ when $m = 2$. Meanwhile, $d_0$ describes the case $m = 1$ with $a \neq \pm 1$, and $m = 2$ with $a + q = \pm 1$.

For the remaining cases (that is, when $\#\mathcal{S}^* > 1$), there is a bijection between the sets $\mathcal{C}_{\mathcal{S}^*}^{a,q}(\mathbb{Q})$ and $\mathcal{AP}_m(a,q)$ for $m = \#\mathcal{S}$. The next table shows $\mathcal{C}_{\mathcal{S}^*}^{a,q}$ for each case (see Table 2).

<table>
<tr><th></th><th>$m=1$</th><th>$m=2$</th><th>$m=3$</th><th>$m=4$</th><th>$m=5$</th></tr>
<tr><td>$a=\pm 1$</td><td>$d\neq 1$</td><td>$d_1$</td><td>$\mathcal{C}_{12}(a,q)$</td><td>$\mathcal{E}_{123}(a,q)$</td><td>$\mathcal{D}_{1234}(a,q)$</td></tr>
<tr><td>$a+q=\pm 1$</td><td rowspan="4">$d_0$</td><td>$d_0$</td><td>$\mathcal{C}_{02}(a,q)$</td><td>$\mathcal{E}_{023}(a,q)$</td><td>$\mathcal{D}_{0234}(a,q)$</td></tr>
<tr><td>$a+2q=\pm 1$</td><td rowspan="3">$\mathcal{C}_{01}(a,q)$</td><td>$\mathcal{C}_{01}(a,q)$</td><td>$\mathcal{E}_{013}(a,q)$</td><td>$\mathcal{D}_{0134}(a,q)$</td></tr>
<tr><td>$a+3q=\pm 1$</td><td rowspan="2">$\mathcal{E}_{012}(a,q)$</td><td>$\mathcal{E}_{012}(a,q)$</td><td>$\mathcal{D}_{0124}(a,q)$</td></tr>
<tr><td></td><td>$\mathcal{D}_{0123}(a,q)$</td><td></td></tr>
</table>

We split the proof depending on the cardinality of $\mathcal{S}^*$:

- $\mathcal{S}^* = \{i,j\}$: Then the curve is the conic $\mathcal{C}_{ij}(a,q)$ with equation

$$\mathcal{C}_{ij}(a,q) : z_j^2 = s_{ij} w^2 + (1 - s_{ij}) z_i^2.$$

This conic has been parametrized in the previous section by

$$[w : z_i : z_j] = [t^2 - 2t + s_{ij} : -t^2 + s_{ij} : t^2 - 2s_{ij}t + s_{ij}],$$

and therefore $\#\mathcal{AP}_m(a,q) = \infty$ when $m = \#\mathcal{S}$ and $\#\mathcal{S}^* = 2$. These cases correspond to $\mathcal{S} = \{0,1\}$ and $a + kq \notin \{\pm 1\}$ for $k \in \{0,1\}$, or $\mathcal{S} = \{0,1,2\}$ and $a + kq \in \{\pm 1\}$ for $k \in \{0,1,2\}$.

• $\mathcal{S}^* = \{i,j,k\}$: We have proved in the previous section that the corresponding curve is elliptic, i.e. it is $\mathbb{Q}$-isomorphic to the elliptic curve with Weierstrass model

$$\mathcal{E}_{ijk}(a,q) : y^2 = x(x + s_{ij} - s_{ik})(x + s_{ik}(s_{ij} - 1)),$$

and such that it has full 2-torsion defined over $\mathbb{Q}$ and the extra rational point $Q = (s_{ik}, s_{ij}s_{ik})$. Our first goal here is to prove that $Q$ is not a point of finite order for

$$(i,j,k,a) \in \{(1,2,3,\pm 1), (0,2,3,\pm 1 - q), (0,1,3,\pm 1 - 2q), (0,1,2,\pm 1 - 3q)\}.$$

By Mazur's theorem, $Q$ has infinite order if and only if $nQ$ is not a point of order 2 for $n = 1,2,3,4$, or equivalently, the $y$-coordinate $y_n$ of $nQ$ (which belongs to $\mathbb{Q}(q)$) is not 0. We have factorized the numerator and denominator of $y_n$ for $n = 1,2,3,4$ and found that the factors of degree one correspond to symmetric arithmetic progressions. Thus we have proved that $\mathcal{E}_{ijk}(a,q)$ has positive rank for any $(i,j,k,a)$ as above and any $q$ that do not correspond to a symmetric arithmetic progression. Same arguments may be applied to the case $(i,j,k) = (0,1,2)$ and any $a,q$. In this case, $y_n \in \mathbb{Q}(a,q)$ and therefore the factors of its numerator and denominator define plane affine curves. All the corresponding genus zero curves come from the locus of the polynomials $a, q, a+q, 2a+q, a+q \pm 1, a+2q \pm 1$. But these genus zero curves do not provide solutions since the possible rational points correspond to cases that have been excluded previously. The genus one curves define elliptic curves of rank zero and therefore only a finite number of points (in fact, the corresponding points are related to symmetric arithmetic progressions). The rest of the curves are of genus greater than one, and so they have only a finite number of rational points. In particular this concludes the proof of the first two statements of Theorem 1.1.

To finish the proof, notice that if $m = \#\mathcal{S} \geq 5$ then $\#\mathcal{S}^* \geq 4$ and in this case the corresponding curve is of genus greater than one. Then, by Faltings' Theorem, this curve has a finite number of rational points. This proves that $\#\mathcal{AP}_m(a,q) < \infty$ when $m \geq 5$.

**4. Proof of Theorem 1.2. Central symmetric case.** The same arguments as above will be adapted to the central symmetric case. In this instance $a = 0$, $\mathcal{S} = \{1,\dots,m\}$ and the condition $a + kq \in \{\pm 1\}$ becomes $kq = 1$. Let $\mathcal{S}^*$ be the set $\mathcal{S}$ with $k$ removed.

If $\#\mathcal{S}^* \leq 1$ the set $\mathcal{S}_c\mathcal{AP}_{2s+1}(q)$ is described by the function $d_1$ when $s = 1$ and $q \neq 1$; by $d \neq 1$ if $(s, q) = (1, 1)$; by $d_2$ when $(s, q) = (2, 1)$; and by $d_1$ when $(s, q) = (2, 1/2)$.

If $\#\mathcal{S}^* \geq 2$, we use the bijection between $\mathcal{C}^{0,q}_{\mathcal{S}^*}(\mathbb{Q})$ and $\mathcal{S}_c\mathcal{AP}_{2s+1}(q)$ for $s = \#\mathcal{S}$. Table 3 gives $\mathcal{C}^{0,q}_{\mathcal{S}^*}$ for each case (see Table 2).

**Table 3.** Moduli for $\mathcal{S}_c\mathcal{AP}_m(q)$

<table>
<tr><th>$q$</th><th>$m=3$</th><th>$m=5$</th><th>$m=7$</th><th>$m=9$</th><th>$m=11$</th></tr>
<tr><td>1</td><td>$d \neq 1$</td><td>$d_2$</td><td>$\mathcal{C}_{23}(0,1)$</td><td>$\mathcal{E}_{234}(0,1)$</td><td>$\mathcal{D}_{2345}(0,1)$</td></tr>
<tr><td>1/2</td><td rowspan="4">$d_1$</td><td>$d_1$</td><td>$\mathcal{C}_{13}(0,1/2)$</td><td>$\mathcal{E}_{134}(0,1/2)$</td><td>$\mathcal{D}_{1345}(0,1/2)$</td></tr>
<tr><td>1/3</td><td rowspan="3">$\mathcal{C}_{12}(0,q)$</td><td>$\mathcal{C}_{12}(0,1/3)$</td><td>$\mathcal{E}_{124}(0,1/3)$</td><td>$\mathcal{D}_{1245}(0,1/3)$</td></tr>
<tr><td>1/4</td><td rowspan="2">$\mathcal{E}_{123}(0,q)$</td><td>$\mathcal{E}_{123}(0,1/4)$</td><td>$\mathcal{D}_{1235}(0,1/4)$</td></tr>
<tr><td></td><td>$\mathcal{D}_{1234}(0,q)$</td><td></td></tr>
</table>

Now, if $\mathcal{S}^* = \{i, j\}$, the corresponding curve is the conic $\mathcal{C}_{ij}(0, q)$ that has infinitely many points. Therefore $\#\mathcal{S}_c\mathcal{AP}_{2s+1}(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 2$. These cases correspond to $\mathcal{S} = \{1, 2, 3\}$ and $q \in \{1, 1/2, 1/3\}$, or $\mathcal{S} = \{1, 2\}$ and $q \notin \{1, 1/2\}$.

The case $\mathcal{S}^* = \{i, j, k\}$ corresponds to the elliptic curve $\mathcal{E}_{ijk}(0, q)$ which has full 2-torsion defined over $\mathbb{Q}$ and the extra rational point $Q = (s_{ik}, s_{ij}s_{ik})$. Our objective is to prove that $Q$ is not a point of finite order for the cases $(i, j, k, q) \in \{(2, 3, 4, 1), (1, 3, 4, 1/2), (1, 2, 4, 1/3)\}$ and $(i, j, k) = (1, 2, 3)$ for any $q \in \mathbb{Q}_{>0}$, $q \notin \{1, 1/2, 1/3\}$. The first attempt is to use the Nagell–Lutz Theorem, so we compute an integral model of $\mathcal{E}_{ijk}(0, q)$ and we check if the coordinates of $Q'$ (the image of the point $Q$ in this integral model) are not rational integers. The following table shows, for every case, an integral model and the $x$-coordinate of $nQ'$ for the first $n$ such that $nQ'$ does not have integral coordinates.

| $(i,j,k,q)$ | Integral model | $n$ | $x(nQ')$ |
|---|---|---|---|
| $(2,3,4,1)$ | $y^2 = x^3 - 25444800x - 35897472000$ | 2 | $185721/16$ |
| $(1,3,4,1/2)$ | $y^2 = x^3 - 11697075x + 15251172750$ | 3 | $4532055/961$ |
| $(1,2,4,1/3)$ | $y^2 = x^3 - 308700x - 55566000$ | 1 | $-4095/16$ |

Therefore if $(i, j, k, q) \in \{(2, 3, 4, 1), (1, 3, 4, 1/2), (1, 2, 4, 1/3)\}$ we infer that the point $Q$ is not of finite order.

Note that this procedure does not work for $(i, j, k) = (1, 2, 3)$ with $q \in \mathbb{Q}_{>0}$, $q \notin \{1, 1/2, 1/3\}$. By Mazur's theorem, $Q$ has infinite order if and only if $nQ$ is not a point of order 2 for $n = 1, 2, 3, 4$. That is, the $y$-coordinate $y_n$ of $nQ$, which belongs to $\mathbb{Q}(q)$, is not 0. We have factorized the numerator and denominator of $y_n$ for $n = 1, 2, 3, 4$ and found that they have no root $q \in \mathbb{Q}_{>0}$

with $q \notin \{1, 1/2, 1/3\}$. Thus, $\mathcal{E}_{ijk}(0,q)$ has positive rank for any $(i,j,k,q)$ as above, and this proves that $\#\mathcal{S}_c\mathcal{AP}_{2s+1}(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 3$. These cases correspond to $\mathcal{S} = \{1,2,3,4\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$, or $\mathcal{S} = \{1,2,3\}$ and $q \notin \{1, 1/2, 1/3, 1/4\}$. In particular this concludes the proof of the statement that $\#\mathcal{S}_c\mathcal{AP}_7(q) = \infty$ for any $q \in \mathbb{Q}_{>0}$.

The last case is $\mathcal{S}^* = \{i,j,k,l\}$, which corresponds to the genus five curve $\mathcal{D}_{ijkl}(0,q)$. By Falting's Theorem we have $\#\mathcal{D}_{ijkl}(0,q)(\mathbb{Q}) < \infty$. This proves that the set $\mathcal{S}_c\mathcal{AP}_{2s+1}(q)$ is finite when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 4$. These cases correspond to $\mathcal{S} = \{1,2,3,4,5\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$, or $\mathcal{S} = \{1,2,3,4\}$ and $q \notin \{1, 1/2, 1/3, 1/4\}$. This concludes the proof of the fact that $\#\mathcal{S}_c\mathcal{AP}_9(q) = \infty$ if and only if $q \in \{1, 1/2, 1/3, 1/4\}$, and $\#\mathcal{S}_c\mathcal{AP}_m(q) < \infty$ for $m \geq 11$ and any $q \in \mathbb{Q}_{>0}$.

In the remainder of this section, we will check that $\#\mathcal{S}_c\mathcal{AP}_m(q) = 0$ if $q \in \{1, 1/2, 1/3, 1/4\}$ for $m \geq 11$. Note that it is enough to prove this for $m = 11$. That is, for $\mathcal{S} = \{1,2,3,4,5\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$ the corresponding curve has genus five and therefore only a finite number of rational points. In fact, we are going to prove that

$$\mathcal{C}^{0,q}_{\mathcal{S}^*}(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$$

for those values of $q$. For this purpose we apply the algorithm described in Section 2.

Let us start with the case $(a,q) = (0,1)$. Then the genus five curve is $\mathcal{D}_{2345}(0,1)$ and we choose the model $N = 11$ from Table 1 with $b_2 = -4$, $b_3 = 7/32$, $b_4 = -3/32$, and the pair $(l_3, l_4) = (1,2)$. In this case $L = \mathbb{Q}(\sqrt{-7})$, $\mathfrak{S} = \{\pm 1, \pm 10\}$ and we have the following polynomials:

$$\begin{aligned} p_{3,1,+}(t) &= t^2 + \frac{1}{16}(-5\sqrt{-7} - 7)t + \frac{1}{4}(-5\sqrt{-7} + 9), \\ p_{4,2,+}(t) &= t^2 + \frac{1}{16}(-25\sqrt{-7} + 3)t - 4. \end{aligned}$$

Now for any $\delta \in \mathfrak{S}$, we must compute all the points $(t,w) \in H^{\delta}_{\pm,\pm}(\mathbb{Q}(\sqrt{-7}))$ with $t \in \mathbb{P}^1(\mathbb{Q})$ for some choice of signs $s = (s_3, s_4) \in \{\pm\} \times \{\pm\}$ where

$$H^{\delta}_s : \delta w^2 = p_{3,1,s_3}(t)\, p_{4,2,s_4}(t).$$

We have $\operatorname{rank}_{\mathbb{Z}} H^{\pm 1}_{(+,+)}(\mathbb{Q}(\sqrt{-7})) = 1$, so we can apply elliptic Chabauty to obtain the possible values of $t$. For $\delta = 1$ (resp. $\delta = -1$) we obtain $t = \infty$ (resp. $t = -1$ ). For all those values we obtain the trivial points $[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1] \in \mathcal{D}_{2345}(0,1)(\mathbb{Q})$. For $\delta \in \{\pm 10\}$, we obtain $H^{\delta}_{(+,+)}(\mathbb{Q}(\sqrt{-7})) = \emptyset$ using Bruin and Stoll's algorithm [10].

The following table shows all the previous data. In the last column it is stated whether the corresponding points attached to $t$ in the curve are trivial or not.

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{-7})) = \emptyset$? | $\mathrm{rank}_{\mathbb{Z}}\, H_s^\delta(\mathbb{Q}(\sqrt{-7}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,+)$ | no | 1 | $\infty$ | yes |
| $-1$ | $(+,+)$ | no | 1 | 1 | yes |
| 10 | $(+,+)$ | yes | – | – | – |
| $-10$ | $(+,+)$ | yes | – | – | – |

$(i,j,k,l) = (2,3,4,5)$, $q = 1$, $N = 11$, $(b_2,b_3,b_4) = (-4, 7/32, -3/32)$, $(l_3,l_4) = (1,2)$

From the table we obtain $\mathcal{D}_{2345}(0,1)(\mathbb{Q}) = \{[1 : \pm1 : \pm1 : \pm1 : \pm1]\}$, and therefore $\#\mathcal{S}_{\mathrm{c}}\mathcal{AP}_m(1) = 0$ for any $m \geq 11$. In particular, this answers one of Moody's questions ([1]).

The following three tables include the data related to the computation of all rational points of the curves $\mathcal{D}_{ijkl}(0,q)(\mathbb{Q})$ with $(i,j,k,l,q) \in \{(1,3,4,5,1/2), (1,2,4,5,1/3), (1,2,3,5,1/4)\}$. In all these cases we have $\mathcal{D}_{ijkl}(0,q) = \{[1 : \pm1 : \pm1 : \pm1 : \pm1]\}$.

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{14})) = \emptyset$? | $\mathrm{rank}_{\mathbb{Z}}\, H_s^\delta(\mathbb{Q}(\sqrt{14}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,-)$ | no | 1 | $\infty$ | yes |
| 2 | $(+,+)$ | yes | – | – | – |
| $-5$ | $(+,+)$ | yes | – | – | – |
| $-10$ | $(+,+)$ | yes | – | – | – |

$(i,j,k,l) = (1,3,4,5)$, $q = 1/2$, $N = 3$, $(b_2,b_3,b_4) = (-3/25, 32/25, -64/125)$, $(l_3,l_4) = (1,3)$

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{21})) = \emptyset$? | $\mathrm{rank}_{\mathbb{Z}}\, H_s^\delta(\mathbb{Q}(\sqrt{21}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,+)$ | no | 1 | $\infty$, 27/25 | yes |
| $-1$ | $(+,+)$ | yes | – | – | – |
| 6 | $(+,+)$ | yes | – | – | – |
| $-6$ | $(+,+)$ | yes | – | – | – |

$(i,j,k,l) = (1,2,4,5)$, $q = 1/3$, $N = 3$, $(b_2,b_3,b_4) = (27/25, 189/125, -81/175)$, $(l_3,l_4) = (1,1)$

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{105})) = \emptyset$? | $\mathrm{rank}_{\mathbb{Z}}\, H_s^\delta(\mathbb{Q}(\sqrt{105}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,-)$ | no | 1 | $\infty$ | yes |
| 6 | $(+,+)$ | yes | – | – | – |

$(i,j,k,l) = (1,2,3,5)$, $q = 1/4$, $N = 1$, $(b_2,b_3,b_4) = (128/3, -4, -128/7)$, $(l_3,l_4) = (3,2)$

These computations conclude the proof of Theorem 1.2.

**5. Proof of Theorem 1.3. Non-central symmetric case.** We invoke the same arguments again. In this case we choose $a = -q/2$, $\mathcal{S} = \{1,\ldots,m\}$, and the condition $a + kq \in \{\pm1\}$ becomes $(2k-1)q = 2$. Let $\mathcal{S}^* = \mathcal{S} \setminus \{k\}$.

([1]) Moody [20] asked if there exists $d \in \mathbb{Q}$, $d \neq 0,1$, such that $0, \pm1, \pm2, \pm3, \pm4, \pm5$ form an arithmetic progression in $E_d(\mathbb{Q})$. Note that after this paper was online (arXiv: 1304.4361), Bremner [7] obtained a different proof of the non-existence of such a $d$.

If $\#\mathcal{S}^* \leq 1$ the set $\mathcal{S}_{\rm nc}\mathcal{AP}_m(q)$ is described by the function $d_1$ when $m = 2$ and $q \neq 2$; by $d \neq 1$ if $(m, q) = (2, 2)$; by $d_2$ when $(m, q) = (4, 2)$; and by $d_1$ when $(m, q) = (4, 2/3)$.

Table 4 identifies $\mathcal{C}_{\mathcal{S}^*}^{-q/2,q}$ when $\#\mathcal{S}^* > 1$ (see Table 2).

**Table 4.** Moduli for $\mathcal{S}_{\rm nc}\mathcal{AP}_m(q)$

<table>
<tr><th>$q$</th><th>$m=2$</th><th>$m=4$</th><th>$m=6$</th><th>$m=8$</th><th>$m=10$</th></tr>
<tr><td>$2$</td><td>$d \neq 1$</td><td>$d_2$</td><td>$\mathcal{C}_{23}(-1,2)$</td><td>$\mathcal{E}_{234}(-1,2)$</td><td>$\mathcal{D}_{2345}(-1,2)$</td></tr>
<tr><td>$2/3$</td><td rowspan="4">$d_1$</td><td>$d_1$</td><td>$\mathcal{C}_{13}(-1/3,2/3)$</td><td>$\mathcal{E}_{134}(-1/3,2/3)$</td><td>$\mathcal{D}_{1345}(-1/3,2/3)$</td></tr>
<tr><td>$2/5$</td><td rowspan="3">$\mathcal{C}_{12}(-q/2,q)$</td><td>$\mathcal{C}_{12}(-1/5,2/5)$</td><td>$\mathcal{E}_{124}(-1/5,2/5)$</td><td>$\mathcal{D}_{1245}(-1/5,2/5)$</td></tr>
<tr><td>$2/7$</td><td rowspan="2">$\mathcal{E}_{123}(-q/2,q)$</td><td>$\mathcal{E}_{123}(-1/7,2/7)$</td><td>$\mathcal{D}_{1235}(-1/7,2/7)$</td></tr>
<tr><td></td><td>$\mathcal{D}_{1234}(-q/2,q)$</td><td></td></tr>
</table>

If $\#\mathcal{S}^* = 2$, then $\mathcal{S}_{\rm nc}\mathcal{AP}_{2s}(q)$ is parametrized by a conic with infinitely many rational points. Therefore $\#\mathcal{S}_{\rm nc}\mathcal{AP}_{2s}(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 2$. These cases correspond to $\mathcal{S} = \{1, 2, 3\}$ and $q \in \{2, 2/3, 2/5\}$ or $\mathcal{S} = \{1, 2\}$ and $q \notin \{2, 2/3\}$.

Now, the elliptic curve $\mathcal{E}_{ijk}(-q/2, q)$ parametrizes the case when $\mathcal{S}^* = \{i, j, k\}$. This curve has all the 2-torsion points defined over $\mathbb{Q}$ and the extra rational point $Q = (s_{ik}, s_{ij}s_{ik})$. Using the Nagell–Lutz Theorem we can prove that $Q$ has infinite order for the cases

$$(i, j, k, q) \in \{(2, 3, 4, 2), (1, 3, 4, 2/3), (1, 2, 4, 2/5)\}.$$

First we compute a suitable integral model of $\mathcal{E}_{ijk}(-q/2, q)$. The next table shows for every case the corresponding integral model and the $x$-coordinate of $nQ'$ for the first $n$ such that $nQ'$ does not have integral coordinates (where $Q'$ is the image of $Q$ in this model):

| $\{i,j,k,q\}$ | Integral model | $n$ | $x(nQ')$ |
|---|---|---|---|
| $\{2,3,4,2\}$ | $y^2 = x^3 - 22427712x - 33269059584$ | 3 | 2550847992/151321 |
| $\{1,3,4,2/3\}$ | $y^2 = x^3 - 735300x + 242352000$ | 2 | 18649/36 |
| $\{1,2,4,2/5\}$ | $y^2 = x^3 - 4615488x - 3696371712$ | 2 | 109761/25 |

The proof that $Q$ has infinite order in the case $(i, j, k, a, q) = (1, 2, 3, -q/2, q)$ with $q \notin \{2, 2/3, 2/5\}$ is analogous to the case $(i, j, k, a, q) = (1, 2, 3, 0, q)$ with $q \notin \{1, 1/2, 1/3\}$ already discussed on the proof of Theorem 1.2. This proves that $\#\mathcal{S}_{\rm nc}\mathcal{AP}_{2s}(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 3$. These cases correspond to $\mathcal{S} = \{1, 2, 3, 4\}$ and $q \in \{2, 2/3, 2/5, 2/7\}$, or $\mathcal{S} = \{1, 2, 3\}$ and $q \notin \{2, 2/3, 2/5, 2/7\}$. Thus $\#\mathcal{S}_{\rm nc}\mathcal{AP}_6(q) = \infty$ for any $q \in \mathbb{Q}_{>0}$.

Finally, the genus five curve $\mathcal{D}_{ijkl}(-q/2, q)$ corresponds to the case $\mathcal{S}^* = \{i, j, k, l\}$. Now, since $\#\mathcal{D}_{ijkl}(-q/2, q)(\mathbb{Q}) < \infty$, the set $\mathcal{S}_{\rm nc}\mathcal{AP}_{2s}(q)$ is finite when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 4$. These cases correspond to $\mathcal{S} = \{1, 2, 3, 4, 5\}$

and $q \in \{2, 2/3, 2/5, 2/7\}$, or $\mathcal{S} = \{1, 2, 3, 4\}$ and $q \notin \{2, 2/3, 2/5, 2/7\}$. So we have proved that $\#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_8(q) = \infty$ if and only if $q \in \{2, 2/3, 2/5, 2/7\}$ and $\#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_m(q) < \infty$ for $m \geq 10$ and any $q \in \mathbb{Q}_{>0}$.

The following four tables include the data related to the computation of all rational points of the curves $\mathcal{D}_{ijkl}(-q/2, q)$ with

$$(i, j, k, l, q) \in \{(2, 3, 4, 5, 2), (1, 3, 4, 5, 2/3), (1, 2, 4, 5, 2/5), (1, 2, 3, 5, 2/7)\}.$$

In all these cases we have $\mathcal{D}_{ijkl}(-q/2, q)(\mathbb{Q}) = \{[1 : \pm1 : \pm1 : \pm1 : \pm1]\}$.

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{15})) = \emptyset$? | $\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{15}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,+)$ | no | 1 | $\infty$ | yes |
| $-1$ | $(+,+)$ | yes | – | – | – |
| 6 | $(+,+)$ | no | 1 | 1 | yes |
| $-6$ | $(+,+)$ | yes | – | – | – |

$(i, j, k, l) = (2, 3, 4, 5)$, $a = -1$, $q = 2$, $N = 9$, $(b_2, b_3, b_4) = (7/5, 50, -4)$, $(l_3, l_4) = (2, 3)$

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{10})) = \emptyset$? | $\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{10}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,-)$ | no | 1 | $\infty, 0$ | yes |
| $-6$ | $(+,+)$ | yes | – | – | – |

$(i, j, k, l) = (1, 3, 4, 5)$, $a = -1/3$, $q = 2/3$, $N = 2$, $(b_2, b_3, b_4) = (7/25, 27/25, 27/125)$, $(l_3, l_4) = (2, 2)$

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{21})) = \emptyset$? | $\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{21}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(+,+)$ | no | 1 | $\infty$ | yes |
| $-1$ | $(+,+)$ | yes | – | – | – |
| 6 | $(+,+)$ | yes | – | – | – |
| $-6$ | $(+,+)$ | yes | – | – | – |

$(i, j, k, l) = (1, 2, 4, 5)$, $a = -1/5$, $q = 2/5$, $N = 6$, $(b_2, b_3, b_4) = (5/7, 1/50, -1/4)$, $(l_3, l_4) = (2, 3)$

| $\delta$ | $s$ | $H_s^\delta(\mathbb{Q}(\sqrt{7})) = \emptyset$? | $\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{7}))$ | $t$ | trivial? |
|---|---|---|---|---|---|
| 1 | $(-,+)$ | no | 1 | $\infty, 0$ | yes |
| 2 | $(+,+)$ | yes | – | – | – |
| 5 | $(+,+)$ | yes | – | – | – |
| 10 | $(+,+)$ | yes | – | – | – |

$(i, j, k, l) = (1, 2, 3, 5)$, $a = -1/7$, $q = 2/7$, $N = 1$, $(b_2, b_3, b_4) = (245/2, -49/5, -49)$, $(l_3, l_4) = (2, 2)$

This concludes the proof of Theorem 1.3.

**6. Some computations.** We would like to find an arithmetic progression on an Edwards curve as long as possible. As in the symmetric cases fewer restrictions appear, we have undertaken a computer search on `Magma` to find a non-trivial rational point $P$ of height $H(P) \leq 10^6$ on the curve $\mathcal{D}_{1234}(0,q)$ or on the curve $\mathcal{D}_{1234}(-q/2,q)$ for positive rationals $q$ of height $H(q) \leq 100$ and $q \notin \{1,1/2,1/3,1/4\}$ or $q \notin \{2,2/3,2/5,2/7\}$ respectively. There are 6087 such $q$'s. We have used the following models for $\mathcal{D}_{1234}(0,q)$ and $\mathcal{D}_{1234}(-q/2,q)$:

$$\mathcal{D}_{1234}(0,q) : \begin{cases} 3X_0^2 + 4(q^2-1)X_1^2 + (1-4q^2)X_2^2 = 0, \\ 8X_0^2 + 9(q^2-1)X_1^2 + (1-9q^2)X_3^2 = 0, \\ 15X_0^2 + 16(q^2-1)X_1^2 + (1-16q^2)X_4^2 = 0, \end{cases}$$

$$\mathcal{D}_{1234}(-q/2,q) : \begin{cases} 32X_0^2 + 9(q^2-4)X_1^2 + (4-9q^2)X_2^2 = 0, \\ 96X_0^2 + 25(q^2-4)X_1^2 + (4-25q^2)X_3^2 = 0, \\ 192X_0^2 + 49(q^2-4)X_1^2 + (4-49q^2)X_4^2 = 0. \end{cases}$$

We have found no such rational point. On the other hand, using the techniques of the proof of the last item of Theorems 1.2 and 1.3, we are able to prove that $\#\mathcal{D}_{1234}(0,q) = 16$ for

$$q \in \left\{ \begin{array}{c} 19/11, 11/13, 49/46, 13/3, 3/2, 3/7, 2, 11/43, 1/11, \\ 7/11, 1/8, 1/7, 1/6, 8/17, 1/5, 11/38, 5/17, 2/3, 11/37, \\ 7/13, 59/61, 29/53, 3/4, 11/19, 3/8, 37/95, 11/28 \end{array} \right\},$$

and $\#\mathcal{D}_{1234}(-q/2,q) = 16$ for

$$q \in \left\{ \begin{array}{c} 2/9, 22/13, 14, 22/7, 14/11, 2/35, 6/7, 22/25, 34/19, \\ 2/17, 2/15, 22/73, 62/33, 2/13, 38/35, 10/7, 34/49, 22/31, \\ 26/21, 10/23, 34/77, 14/19, 26/11, 38/77, 22/43, 6/11 \end{array} \right\},$$

Thus for the corresponding list we have proved that

$$\#\mathcal{S}_{\mathrm{c}}\mathcal{AP}_9(q) = 0 \quad \text{and} \quad \#\mathcal{S}_{\mathrm{nc}}\mathcal{AP}_8(q) = 0$$

respectively.

**Acknowledgements.** We would like to thank to Nils Bruin, Luis Dieulefait and Xevi Guitart for some interesting and useful discussions, and José M. Tornero, who read the earlier versions of this paper carefully.

This research was partly supported by the grant MTM2012–35849.

## References

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

[2] A. Alvarado, *Arithmetic progressions in the y-coordinates on certain elliptic curves*, in: F. Luca and P. Stanica (eds.), Aportaciones Matemáticas, Investigación 20, Proceedings of the Fourteenth International Conference on Fibonacci Numbers, Sociedad Matemática Mexicana, 2011, 1–9.

[3] E. Bombieri, A. Granville, and J. Pintz, *Squares in arithmetic progressions*, Duke Math. J. 66 (1992), 369–385.

[4] W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions, Edition 2.19*, http://magma.maths.usyd.edu.au/magma, 2012.

[5] A. Bremner, *Some special curves of genus* 5, Acta Arith. 79 (1997), 41–51.

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

[7] A. Bremner, *Arithmetic progressions on Edwards curves*, J. Integer Sequences 16 (2013), no. 8, art. 13.8.5, 5 pp.

[8] 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.

[9] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. 562 (2003), 27–49.

[10] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. 78 (2009), 2347–2370.

[11] G. Campbell, *A note on arithmetic progressions on elliptic curves*, J. Integer Sequences 6 (2003), no. 1, art. 03.1.3, 5 pp.

[12] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris 212 (1941), 882–885.

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

[14] I. García-Selfa and J. M. Tornero, *On simultaneous arithmetic progressions on elliptic curves*, Experiment. Math. 15 (2006), 471–478.

[15] E. González-Jiménez, *Covering techniques and rational points on some genus 5 curves*, in: Contemp. Math., Amer. Math. Soc., to appear.

[16] E. González-Jiménez and X. Xarles, *On a conjecture of Rudin on squares in arithmetic progression*, LMS J. Comput. Math. 17 (2014), 58–76.

[17] 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.

[18] A. J. MacLeod, *14-term arithmetic progressions on quartic elliptic curves*, J. Integer Sequences 9 (2006), no. 1, art. 06.1.2, 4 pp.

[19] S. P. Mohanty, *On consecutive integer solutions for* $y^2 - k = x^3$, Proc. Amer. Math. Soc. 48 (1975), 281–285.

[20] D. Moody, *Arithmetic progressions on Edwards curves*, J. Integer Sequences 14 (2011), no. 1, art. 11.1.7, 4 pp.

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

[22] R. Schwartz, J. Solymosi, and F. de Zeeuw, *Simultaneous arithmetic progressions on algebraic curves*, Int. J. Number Theory 7 (2011), 921–931.

[23] B. K. Spearman, *Arithmetic progressions on congruent number elliptic curves*, Rocky Mountain J. Math. 41 (2011), 2033–2044.

[24] M. Ulas, *A note on arithmetic progressions on quartic elliptic curves*, J. Integer Sequences 8 (2005), no. 8, art. 05.3.1, 5 pp.

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

Enrique González-Jiménez
Departamento de Matemáticas
Universidad Autónoma de Madrid
and
Instituto de Ciencias Matemáticas (ICMat)
Madrid, Spain
E-mail: enrique.gonzalez.jimenez@uam.es
URL: http//www.uam.es/enrique.gonzalez.jimenez

*Received on 30.3.2014*
*and in revised form on 31.10.2014* (7759)