On Simultaneous Arithmetic Progressions on Elliptic Curves

Irene García-Selfa and José M. Tornero

CONTENTS

In this paper we study elliptic curves that have a number of points whose coordinates are in arithmetic progression. We first motivate this Diophantine problem; then we prove some results, provide a number of interesting examples, and finally point out open questions that focus on the most interesting aspects of the problem for us.

2000 AMS Subject Classification: Primary 11G05; Secondary 14H52, 11B25

Keywords: Elliptic curves, arithmetic progressions

1. INTRODUCTION

We will deal with elliptic curves defined over a field K by a Weierstrass equation:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in K.$$

We will denote, as usual, by $E(K)$ the locus of the above equation, together with the point at infinity, $O = (0 : 1 : 0)$.

The changes of variables preserving Weierstrass form are those given by [Silverman 86]

$$X' = u^2X + s, \quad Y' = u^3Y + rX + t,$$

and we consider two equations related by such a change of variables to represent the same curve (equivalently, we will deal with elliptic curves up to so-called Weierstrass changes of variables).

Consider $P_0, \dots, P_n \in E(K)$, with $P_i = (x_i, y_i)$ such that $x_0, \dots, x_n$ is an arithmetic progression. We say that $P_0, \dots, P_n$ are in x-arithmetic progression (x-a.p.) and also say that E has an x-arithmetic progression of length $n+1$. This does not depend on the Weierstrass equation considered.

The same definition goes for y-arithmetic progressions (y-a.p.). However, in this case, changes of variables (even those that preserve Weierstrass equations) can create and remove y-arithmetic progressions.

1058-6458/2006 $ 0.50 per page

Example 1.1. Let us consider the following equation over $\mathbb{Q}$:

$$E : Y^2 - \frac{5}{16}XY + \frac{1}{64}Y = X^3 - \frac{1}{64}X^2,$$

with

$$\left(\frac{1}{8}, \frac{-4}{128}\right), \left(\frac{-1}{32}, \frac{-3}{128}\right), \left(\frac{5}{64}, \frac{-2}{128}\right), \left(\frac{1}{32}, \frac{-1}{128}\right),$$

$$\left(\frac{1}{64}, 0\right), \left(\frac{3}{64}, \frac{1}{128}\right), \left(\frac{1}{16}, \frac{2}{128}\right) \in E(\mathbb{Q}).$$

The reader can easily check that after the change of variables $Y' = Y + X$, the corresponding points are not in y-a.p. Hence we can properly talk of x-a.p. in a curve, but if we speak of y-a.p. in a curve, we must keep in mind that we are considering a specific equation.

This paper studies elliptic curves that have a simultaneous arithmetic progression. First we need a proper definition of these progressions. Let us consider $P_0, \ldots, P_n$ as above. If we want both $x_0, \ldots, x_n$ and $y_0, \ldots, y_n$ to be arithmetic progressions, then the problem is far too easy, since $P_0, \ldots, P_n$ must be collinear and hence $n \leq 2$. Many examples can be found with this property; for instance, all curves in the family

$$E(b) : Y^2 + (2b - 1)XY + bY = X^3 - bX^2$$

have the arithmetic progression $(0, -b)$, $(b, 0)$, $(2b, b)$.

Definition 1.2. With the above notation, $P_0, \ldots, P_n$ define a simultaneous arithmetic progression (s.a.p.) for E, or E has a simultaneous arithmetic progression if the following conditions are satisfied:

(a) $x_0, \ldots, x_n$ are in arithmetic progression (called the support of the s.a.p.).

(b) There exists a permutation σ in the symmetric group of $n+1$ elements S_{n+1} such that $y_{\sigma(0)}, \ldots, y_{\sigma(n)}$ are in arithmetic progression.

The definition is clearly symmetric: it is equivalent (up to point ordering) to saying that $y_0, \ldots, y_n$ are in arithmetic progression and there exists $\mu \in S_{n+1}$ such that $x_{\mu(0)}, \ldots, x_{\mu(n)}$ are in arithmetic progression, but our version has proved more useful for computational purposes.

With this definition, at least three problems arise:

(a) The detection problem: Given an elliptic curve, does there exist an algorithm for deciding whether it contains an s.a.p. of length n (providing a change of variables if needed)?

(b) The subsequence problem: Given an s.a.p. of length $n+1$ in an elliptic curve, does it contain an s.a.p. of length n? (Note that this is not at all trivial from the definition.)

(c) The bound problem: Is there a bound for the possible lengths of s.a.p. in elliptic curves?

In trying to understand these three problems, we have developed some computational methods (actually, two partial answers to the detection problem) whose application may shed some light on the matter at hand. Nevertheless, the results achieved can be considered only as a first step toward a fully satisfactory understanding of these sequences. We have managed to prove the following results:

Theorem 1.3. *Given an elliptic curve with an x-a.p., there exists an algorithm that decides whether the curve also has an s.a.p. with the given x-a.p. as support.*

Theorem 1.4. *There are integers n, and examples of curves with s.a.p. of length n, that do not contain any s.a.p. of length $n - 1$.*

Theorem 1.5. *There are no elliptic curves defined over $\mathbb{Q}$ with s.a.p. of length* 7. *There are only finitely many nonisomorphic curves defined over $\mathbb{Q}$ with s.a.p. of length* 6.

We will finish this introduction with a word on motivation. At first, our interest was drawn to this subject by the articles of Bremner–Silverman–Tzanakis [Bremner et al. 00] and Bremner [Bremner 99b]. Apparently, these papers had their starting point in the relationship between x-a.p. and Latin square problems (see more on this in [Bremner 99a, Bremner 01]). However, highly interesting results were sketched in both papers around the interplay between the existence of arithmetic progressions on a certain elliptic curve and its rank. In this same direction, Campbell [Campbell 03] has pointed out far-reaching questions, probably too difficult for the current state of the art.

The history of the problem, though, can be traced back considerably further, since (for the specific case of

Mordell curves) it was treated previously by S. P. Mohanty [Mohanty 75], who studied x- and y-a.p. separately, and by Lee and Vélez [Lee and Vélez 92], who first treated s.a.p., if only in the naive form mentioned above, with no permutations involved. The motivation for these first works was, as has been the case many other times in number theory, purely Diophantine.

We became interested in this specific problem while trying to improve Bremner's record of longest x-a.p. by narrowing the search.[1] Our first attempts were shown in [García-Selfa and Tornero 05], using a specific kind of s.a.p. that allowed us to find examples of s.a.p. of length 5. These methods were not at all exhaustive, as was accurately pointed out by Bremner in his *MathSciNet* review. After this work, we feel that some of the posed problems are worth a closer look, and the setup remains challenging. As Bremner points out in [Bremner 99b], "Questions in number theory that interrelate two group structures are easily posed, but often lead to intractable problems."

2. THE DETECTION PROBLEM

Let us consider a set of points $P_0 = (x_0, y_0), \ldots, P_n = (x_n, y_n)$ on an elliptic curve, defined over K by the Weierstrass equation

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

with $a_i \in K$. Let us suppose the points $P_0, \ldots, P_n \in E(K)$ to be in x-a.p. We are interested in finding, if there exist any, a change of variables preserving the Weierstrass form of E that transforms $P_i = (x_i, y_i)$ into $P'_i = (x'_i, y'_i)$, so that $P'_0, \ldots, P'_n$ is an s.a.p. for the corresponding equation E'. This change of variables must be of the form

$$X' = u^2X + s, \quad Y' = u^3Y + rX + t.$$

If $x_i = a + i \cdot d$, and we want $y'_{\sigma(0)}, \ldots, y'_{\sigma(n)}$ to be an arithmetic progression for some $\sigma \in S_{n+1}$, then we must have

$$\begin{aligned} x'_i &= u^2(a + id) + s, \\ y'_i &= b + \sigma(i)d', \quad \text{for } i = 0, \ldots, n. \end{aligned}$$

We can take, with no loss of generality, $u = 1$, $s = 0$, $t = 0$. This involves simply choosing an appropriate reference system by translation and scaling (which would not affect s.a.p. in any case). Then we want

$$\begin{aligned} x'_i &= x_i = a + id, \\ y'_i &= y_i - r(a + id) = b + \sigma(i)d', \quad \text{for } i = 0, \ldots, n, \end{aligned}$$

for some $b, d' \in K$.

These latter identities can be written as a system of $n + 1$ linear equations in r, b, and d', with matrix

$$A^* = \left(\begin{array}{ccc|c} a + 0d & 1 & \sigma(0) & y_0 \\ a + 1d & 1 & \sigma(1) & y_1 \\ \vdots & \vdots & \vdots & \vdots \\ a + nd & 1 & \sigma(n) & y_n \end{array} \right).$$

Note that the y-sequence $y_0, \ldots, y_n$ is not an arithmetic progression if and only if the first, second, and fourth columns are independent, equivalently, if

$$\exists s \in \{2, \ldots, n\} \text{ such that} \begin{vmatrix} -0 & 1 & y_0 \\ -1 & 1 & y_1 \\ -s & 1 & y_s \end{vmatrix} \neq 0.$$

Our first detection algorithm uses that the existence of a solution to our system (that is, the existence of an s.a.p.) is equivalent to A^* having rank 3. The formal algorithm goes like this:

Algorithm 2.1.

Input Data: $E, x_0, \ldots, x_n$ (equivalently E, x_0, n, d).

Step 0. For all sets $\{y_0, \ldots, y_n\}$ such that $(x_i, y_i) \in E(K)$, do

Step 1. (Foolproof checking) Check whether $\{y_0, \ldots, y_n\}$ is an arithmetic progression. If so, we are done; if not, find s, $2 \leq s \leq n$, as above.

Step 2. For every $\sigma \in S_n$ and every $i \in \{2, \ldots, n\}$, $i \neq s$, compute the minor formed by the first, second, sth, and ith rows of A^*.

Step 3. If for some $\sigma \in S_n$ the $n - 2$ minors are null, solve the system to find r, b, and d'. If not, go to step 0.

The main inconvenience of this procedure is the necessity for $2^{n+1}(n + 1)!(n - 2)$ determinant computations, since there are $(n + 1)!$ possibilities for σ and 2 possibilities for each y_i. So we will try to find a more efficient procedure, although this setup will prove useful later on.

Consider the affine points $Q_0 = (0, y_0, \sigma(0)), \ldots, Q_n = (nd, y_n, \sigma(n)) \in \mathbf{A}^3(K)$. Note that $P_0, \ldots, P_n$ are an s.a.p. if and only if $Q_0, \ldots, Q_n$ lie in the same plane. This is the basis for our algorithm, whose input data and steps 0 and 1 are those of Algorithm 2.1.

[1] The longest x-a.p. found in an elliptic curve has 8 terms [Bremner 99b]; for y-a.p. the record is 7 so far [García-Selfa and Tornero 05].

y_0	y_1	y_2	y_3	σ	y_0'	y_1'	y_2'	y_3'
28	−20	4	4	(1023)	4	−20	28	52
−28	−20	−4	4	(0213)	−44/3	−20	−52/3	−68/3
				(1032)	−18	−20	−14	−16
				(1302)	−84/5	−20	−76/5	−92/5
28	20	4	−4	(0213)	44/3	20	52/3	68/3
				(1032)	18	20	14	16
				(1302)	84/5	20	76/5	92/5
−28	20	−4	−4	(1023)	−4	20	−28	−52

TABLE 1. Four of the 2^4 y-sequences lead to simultaneous arithmetic progressions.

Algorithm 2.2.

Step 2. For each $\{i, j, k\} \subset \{0, 1, \ldots, n\}$, we consider the plane

$$\pi_{ijk} = \langle (0, y_0, i), (d, y_1, j), (sd, y_s, k) \rangle.$$

Step 3. For $l = 2, \ldots, n$ and $l \neq s$, we intersect the plane π_{ijk} with the line $x = ld,\ y = y_l$.

Step 4a. If any of these intersections gives a point (ld, y_l, z_l) such that $z_l \notin \{0, 1, \ldots, n\}$ or z_l is equal to another $z_{l'}$, then $\{z_0, \ldots, z_n\}$ does not correspond to $\{\sigma(0), \ldots, \sigma(n)\}$ for any $\sigma \in S_{n+1}$. Go to step 2, change the plane, and repeat the process or go to step 0 if all planes have been exhausted.

Step 4b. If we find a set of points $Q_0 = (x_0, y_0, z_0), \ldots, Q_n = (x_n, y_n, z_n)$ with $z_i = \sigma(i)$ for $i = 0, \ldots, n$ and $\sigma \in S_{n+1}$, then σ yields a solution r, b, d' of our system.

As for the computational complexity, note that we have $(n+1)n(n-1)/6$ possibilities for π_{ijk}, and for each plane we have at most $n-2$ intersections. This, together with the 2^{n+1} possibilities for the sets $y_0, \ldots, y_n$, means a saving of around $(n-3)!$ computations.

The implementation of both algorithms shows that the time difference is not huge (n does not go very far), but it is already significant for $n \geq 5$.

From now on, we will denote $\sigma \in S_{n+1}$ by $\sigma = (a_0 \ldots a_n)$, meaning $\sigma(0) = a_0, \ldots, \sigma(n) = a_n$.

Example 2.3. The curve $Y^2 = X^3 - 112X + 400$, defined over $\mathbb{Q}$, has the following x-arithmetic progression of length 4:

$$x_k : -4, 0, 4, 8.$$

And four of the 2^4 y-sequences lead to simultaneous arithmetic progressions, as shown in Table 1.

This x-arithmetic progression can be extended to one of length 5,

$$x_k : -4, 0, 4, 8, 12,$$

and two of the 2^5 possible y-sequences lead to simultaneous arithmetic progressions, as shown in Table 2.

The equation for both cases is

$$Y^2 - \frac{20}{3}XY = X^3 - \frac{100}{9}X^2 - 112X + 400.$$

If we try to repeat the procedure for length 6 with

$$x_k : -4, 0, 4, 8, 12, 16,$$

we find that none of the 2^6 possible y-sequences leads to a simultaneous arithmetic progression.

Open Problem 2.4. Find a procedure for deciding whether an elliptic curve has an x-a.p. of given length.

The most interesting results in this direction are the parameterizations by Bremner [Bremner 99b], which will be used later in this paper. However, they are still far from being useful from a computational point of view.

3. THE SUBSEQUENCE PROBLEM

The algorithms described in the previous section (especially the second one) were of great help, both in testing the examples we created with the techniques shown in [García-Selfa and Tornero 05] and in creating new ones. The counterexamples announced in Theorem 1.4 appeared within the framework of these extensive calculations. Here we present the simplest one.

Counterexample 3.1. Consider the following elliptic curve over $\mathbb{Q}$, in Tate normal form:

$$E\left(\frac{25}{21}, \frac{-2}{7}\right) : Y^2 + \frac{25}{21}XY - \frac{2}{7}Y = X^3 + \frac{2}{7}X^2.$$

This curve has an x-arithmetic progression of length 5:

$$x_k : \frac{-6}{7},\ \frac{-4}{7},\ \frac{-2}{7},\ 0,\ \frac{2}{7}.$$

Using the above procedure we obtain a y-sequence that gives the simultaneous arithmetic progression

$$y_k : \frac{4}{7},\ \frac{16}{147},\ \frac{92}{147},\ 0,\ \frac{4}{21}.$$

There is only one permutation σ that passes Algorithm 2.2 and thus allows a change of variables, namely $\sigma = (20413)$. The y'-arithmetic progression is

$$y'_k : \frac{8}{49},\ \frac{-8}{49},\ \frac{24}{49},\ 0,\ \frac{16}{49},$$

y_0	y_1	y_2	y_3	y_4	σ	y_0'	y_1'	y_2'	y_3'	y_4'
-28	-20	-4	4	28	(13240)	$-44/3$	-20	$-52/3$	$-68/3$	-12
28	20	4	-4	-28	(13240)	$44/3$	20	$52/3$	$68/3$	12

TABLE 2. Two of the 2^5 possible y-sequences lead to simultaneous arithmetic progressions.

for the equation

$$Y^2 + \frac{5}{21}XY - \frac{2}{7}Y = X^3 + \frac{92}{147}X^2 - \frac{20}{147}X.$$

In this way we have found a simultaneous arithmetic progression of length 5 containing no simultaneous arithmetic progressions of length 4, because the permutation involved is not the extension of an S_4 permutation. In our many calculations these are atypical cases: first of all, the permutation found is seldom unique, and among the collected ones, we usually find an extension of some S_4 permutation. These counterexamples mean an additional difficulty for arguments involving induction.

Interestingly, in the above example there are other suitable s.a.p. of length 5 with the same support (that is, other choices for the y_i) that happen to have subsequences of length 4.

Open Problem 3.2. Given an elliptic curve with an s.a.p. of length n, prove or disprove that there is always an s.a.p. of length $n-1$ whose support is contained in the support of the given one.

We have found no counterexamples to this problem. If it is true, note that it could serve as a weak induction result.

4. THE BOUND PROBLEM

As was pointed out by Bremner [Bremner 99b], this kind of problem tends to become unmanageable quite quickly. From our many attempts, we will describe here the most successful, which relies on a parameterization of curves with x-a.p. due to Bremner [Bremner 99b] (here slightly changed for our purposes). In what follows we will assume $K = \mathbb{Q}$. Note that the previous arguments do not rely on the base field at all.

First of all, we will parameterize elliptic curves in short Weierstrass form

$$Y^2 = X^3 + AX + B$$

with four points in x-a.p.:

$$P_0 = (a, y_0),\ \ P_1 = (a+d, y_1),\ \ P_2 = (a+2d, y_2),$$
$$P_3 = (a+3d, y_3).$$

Consider the four polynomials $F_0, \ldots, F_3$ in $\mathbb{Q}[y_0, y_1, y_2, y_3, a, d, A, B]$ given by

$$F_i = y_i^2 - (a+id)^3 - A(a+id) - B,$$

and compute a Gröbner basis of the ideal $\langle F_0, \ldots, F_3 \rangle$. The `tdeg` ordering in Maple V gives a basis of ten elements that can be used for computing a, A, B taking $d, y_0, \ldots, y_3$ as parameters:

$$A = \frac{-1}{6^2 d^4}\Big(y_0^4 - 9y_0^2y_1^2 + 6y_2^2y_0^2 + y_3^2y_0^2 + 21y_1^4 - 39y_2^2y_1^2 + 6y_3^2y_1^2 + 21y_2^4 - 9y_3^2y_2^2 + y_3^4\Big) = -P/36d^4,$$

$$B = \frac{1}{6^3 d^6}\Big(y_3^4y_0^2 + 4y_3^4y_1^2 + y_3^4y_2^2 - 9y_3^2y_2^4 - 8y_3^2y_2^2y_0^2 + 24y_3^2y_1^4 - 8y_3^2y_0^2y_1^2 - 12y_3^2y_2^2y_1^2 + y_3^2y_0^4 + y_0^4y_1^2 - 9y_0^2y_1^4 + 20y_1^6 - 21y_1^4y_2^2 + 4y_0^4y_2^2 + 20y_2^6 - 21y_1^2y_2^4 + 24y_0^2y_2^4 - 12y_0^2y_2^2y_1^2\Big)$$
$$= Q/6^3d^6,$$

$$a = \frac{-1}{6d^2}\left(-2y_0^2 + 5y_1^2 - 4y_2^2 + y_3^2\right) = -R/6d^2.$$

In addition, the first member of the basis is

$$-y_3^2 + 6d^3 + y_0^2 - 3y_1^2 + 3y_2^2.$$

Setting $u = 6d$ we obtain the following parameterization:

$$\begin{aligned} \text{Curve:}\quad & Y^2 = X^3 - 6^2PX + 6^3Q, \\ \text{First term:}\quad & 36d^2a = -6R, \\ \text{Difference:}\quad & 36d^3 = 6y_3^2 - 6y_0^2 + 18y_1^2 - 18y_2^2. \end{aligned}$$

We will rename our parameters and use from now on A and B for -6^2P and 6^3Q, respectively, with a and d for the new first term and difference. It is interesting to note that the points in x-a.p. are now

$$P_i = (a + id,\ \pm 6y_id),\ \text{ for } i = 0, \ldots, 3.$$

We will try to produce curves with an s.a.p. of given length with a variant of Algorithm 2.1, which we will illustrate with the case of length 6. In fact, using this procedure we might compute all curves with such an s.a.p., in contrast to the lack of exhaustiveness of [García-Selfa and Tornero 05]. If we want points $P_4 = (a+4d,\ z_4)$ and

$P_5 = (a + 5d,\, z_5)$ to be on the curve, then the following must hold:

$$\begin{aligned} z_4 &= \pm 36\sqrt{4y_3^2 + 4y_1^2 - y_0^2 - 6y_2^2} \\ &\quad \times (-y_3^2 + y_0^2 - 3y_1^2 + 3y_2^2), \\ z_5 &= \pm 36\sqrt{-4y_0^2 - 20y_2^2 + 15y_1^2 + 10y_3^2} \\ &\quad \times (-y_3^2 + y_0^2 - 3y_1^2 + 3y_2^2). \end{aligned}$$

Hence, for the sake of consistency, we will set

$$\begin{aligned} y_4^2 &= 4y_3^2 + 4y_1^2 - y_0^2 - 6y_2^2, \\ y_5^2 &= -4y_0^2 - 20y_2^2 + 15y_1^2 + 10y_3^2, \end{aligned}$$

and our new points will then be $P_i = (a + id,\, \pm 6y_i d)$ for $i = 4, 5$.

Example 4.1. We will show how to proceed using $\sigma = (120345)$. By the above arguments, we may use the matrix

$$M = \left(\begin{array}{ccc|c} 0 & 1 & 1 & y_0 \\ 1 & 1 & 2 & y_1 \\ 2 & 1 & 0 & y_2 \\ 3 & 1 & 3 & y_3 \\ 4 & 1 & 4 & y_4 \\ 5 & 1 & 5 & y_5 \end{array}\right),$$

instead of the original matrix A^* from Algorithm 2.1, and require M to have rank 3, since we are assuming $d \neq 0$. Note that $\{y_0, \ldots, y_5\}$ are not the y-coordinates of $P_0, \ldots, P_5$. All the minors are linear polynomials on $y_0, \ldots, y_5$, and we also have two quadratic relations. It is not surprising that the complete solutions are two linear varieties, actually a plane and a line, given by the following parameterizations:

$$\left\{ y_0,\, \frac{y_4 + 3y_0}{4},\, \frac{y_4 + y_0}{2},\, \frac{3y_4 + y_0}{4},\, y_4,\, \frac{5y_4 - y_0}{4} \right\}$$

and

$$\left\{ y_0,\, \frac{7y_0}{19},\, \frac{y_0}{19},\, \frac{-15y_0}{19},\, \frac{-27y_0}{19},\, \frac{-39y_0}{19} \right\},$$

where the first one contains only points yielding $d = 0$ and therefore must be discarded. In fact, these trivial solutions appear in all cases, and this is clearly a byproduct of our previous assumptions.

Now we make the substitutions induced by the second parameterization, obtaining

$$\begin{aligned} A &= \frac{-7840512}{130321} y_0^4, & B &= \frac{8449090560}{47045881} y_0^6, \\ a &= \frac{1536}{361} y_0^2, & d &= \frac{48}{361} y_0^2, \end{aligned}$$

and the linear system given by A^* has solution

$$r = \frac{-60y_0}{19}, \quad b = \frac{98208y_0^3}{19^3}, \quad d' = \frac{-576y_0^3}{19^3}.$$

This gives, after the corresponding substitution, the equation

$$\begin{aligned} Y^2 - \frac{120y_0}{19} XY = X^3 - \frac{3600y_0^2}{361} X^2 - \frac{7840512y_0^4}{130321} X \\ + \frac{8449090560y_0^6}{47045881}, \end{aligned}$$

which has the following s.a.p.:

$$\begin{aligned} &\left(\frac{1536y_0^2}{19^2}, \frac{97632y_0^3}{19^3} \right), \left(\frac{1584y_0^2}{19^2}, \frac{97056y_0^3}{19^3} \right), \\ &\left(\frac{1632y_0^2}{19^2}, \frac{98208y_0^3}{19^3} \right), \left(\frac{1680y_0^2}{19^2}, \frac{96480y_0^3}{19^3} \right), \\ &\left(\frac{1728y_0^2}{19^2}, \frac{95904y_0^3}{19^3} \right), \left(\frac{1776y_0^2}{19^2}, \frac{95328y_0^3}{19^3} \right). \end{aligned}$$

All these curves are isomorphic to the one given by the case $y_0 = 19/2$,

$$Y^2 - 60YX = X^3 - 900X^2 - 490032X + 132017040,$$

having the sequence $\{(384, 12204),\ (396, 12132),\ (408, 12276),\ (420, 12060),\ (432, 11988),\ (444, 11916)\}$.

We have not computed all curves with s.a.p. of length 6, although we have bounded the number of curves by 19200, using the previous computations with all possible sign and permutation choices, counting only the number of possible solutions, that is, cases in which the line does not induce $d = 0$.

To be precise, only half of the sign choices have to be considered, since every arithmetic progression of difference d is also an arithmetic progression of difference $-d$, and hence every curve appears at least twice, for a pair of inverse choices of signs and permutations.

Even so, not all of these cases are nonisomorphic elliptic curves; there might be isomorphic curves among them as well as genus-0 curves. We have computed some explicit data for the first 100 curves found with this method, in which repeated curves already appear [García-Selfa and Tornero 06a, García-Selfa and Tornero 06b] (in fact, there are only 56 nonisomorphic curves).

As a side remark, we note that the distribution of possible curves is extremely regular. For every sign choice in $y_0, \ldots, y_5$, there are 600 permutations giving $d \neq 0$. In addition, for a fixed permutation, all possible sign choices usually lead to the same solution of the linear system.

This, together with the repeated cases shown in the supplement, gives a heuristic estimation of only around 350 nonisomorphic curves, but filling in the details of such a list is beyond our computational possibilities so far.

As for length 7, our procedure shows that there are no solutions, since all possible ones yield $d = 0$. This case exhausts the possibilities of computer checking, at least with these methods, since it took around 20 hours of CPU time (which implied four days in real time) and, more constraining, 2^{11} MB of stack memory. To extend this method of attack to length 8, these figures should be multiplied by at least 16 (there are 8 times as many permutations, and twice as many minors), and that is without considering the additional difficulty of adding a new quadratic polynomial to the system, the effect of which is not easy to measure.

Open Problem 4.2. Find a universal bound for the length of an s.a.p. on elliptic curves over $\mathbb{Q}$.

Note that an affirmative answer to Open Problem 3.2 would mean that 6 is the answer to Open Problem 4.2.

5. FINAL REMARKS

A supplement containing 100 curves with s.a.p. of length 6 as well as their rank computations can be found in [García-Selfa and Tornero 06a, García-Selfa and Tornero 06b].

We will finish with a comment on ranks. As Bremner noticed in [Bremner 99b], points in arithmetic progression seem to have a tendency to be independent. If we take into account only the ranks actually computed in [García-Selfa and Tornero 06a, García-Selfa and Tornero 06b], we get an average greater than 4, when in fact, the average for random curves is known to be much smaller [Young 06].

It should be noted that example 039 from [García-Selfa and Tornero 06a], given by the equation

$$Y^2 - 720YX + 129600X^2 - X^3 + 9969629720832X \\ - 13778174775900128256,$$

is a remarkable case. As far as we know, it is the first curve with an x-a.p. of length 6 and rank one. (See the final remark of [Bremner 99b], and [Bremner et al. 00] shows why this is so uncommon.) The relation, if any, between the rank and the length of s.a.p. (or x-a.p.) seems definitely a much harder problem to tackle.

ACKNOWLEDGMENTS

Both authors were supported by FQM-218 (Junta de Andalucía) and MTM2004-07203-C02-01 and FEDER (Ministerio de Educación y Ciencia).

REFERENCES

[Bremner 99a] A. Bremner. "On Squares of Squares." *Acta Arith.* 88 (1999), 289–297.

[Bremner 99b] A. Bremner. "On Arithmetic Progressions on Elliptic Curves." *Experiment. Math.* 8:4 (1999), 409–413.

[Bremner 01] A. Bremner. "On Squares of Squares II." *Acta Arith.* 99:3 (2001), 289–308.

[Bremner et al. 00] 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.

[Campbell 03] G. Campbell. "A Note on Arithmetic Progressions on Elliptic Curves." *J. Integer Seq.* 6 (2003), 03.1.3.

[García-Selfa and Tornero 05] I. García–Selfa and J. M. Tornero. "Searching for Simultaneous Arithmetic Progressions on Elliptic Curves." *Bull. Austral. Math. Soc.* 71 (2005), 417–424.

[García-Selfa and Tornero 06a] I. García–Selfa and J. M. Tornero. Supplement to this article. Available online (www.expmath.org/expmath/volumes/15/15.4/tornero/list6ap.pdf).

[García-Selfa and Tornero 06b] I. García–Selfa, and J. M. Tornero. Supplement to this article. Available online (www.expmath.org/expmath/volumes/15/15.4/tornero/list6ap.txt).

[Lee and Vélez 92] 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.

[Mohanty 75] S. P. Mohanty. "On Consecutive Integral Solutions for $y^2 = x^3 + k$." *Proc. Amer. Math. Soc.* 48 (1975), 281–285.

[Silverman 86] J. H. Silverman. *The Arithmetic of Elliptic Curves*. New York: Springer, 1986.

[Young 06] M. P. Young. "Low-Lying Zeros of Families of Elliptic Curves." *J. Amer. Math. Soc.* 19 (2006), 205–250.

Irene García-Selfa, Departamento de Álgebra, Facultad de Matemáticas, Universidad de Sevilla, Apdo. 1160. 41080 Sevilla, Spain (igselfa@us.es)

José M. Tornero, Departamento de Álgebra, Facultad de Matemáticas, Universidad de Sevilla, Apdo. 1160. 41080 Sevilla, Spain (tornero@us.es)

Received February 27, 2006; accepted in revised form May 8, 2006.