

On simultaneous arithmetic progressions on elliptic curves

Irene García–Selfa José M. Tornero

February, 2006

Abstract

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

MSC 2000: 11G05, 14H52 (primary); 11B25 (secondary).

Keywords: Elliptic curves, arithmetic progressions.

1 Introduction

During this paper, all standard results unless otherwise explicitly stated are taken from [9]. Extensive use has been made of Maple V + APECS (by Ian Connell, McGill University).

We will deal with elliptic curves defined over a field K by a Weierstrass equation, that is

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

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

Changes of variables preserving this form are those given by

$$X' = u^2X + r, \quad Y' = u^3Y + sX + t;$$

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

Consider then $P_0, \dots, P_n \in E(K)$, with $P_i = (x_i, y_i)$ such that x_0, \dots, x_n is an arithmetic progression. Then we say that P_0, \dots, P_n are in x -arithmetic progression (x -a.p.) and also E is said to have an x -arithmetic progression of length $n + 1$. From the previous remarks, 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 which preserve Weierstrass equations) can create and destroy y -arithmetic progressions.

Example.— Let us consider the equation over \mathbf{Q}

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

which verifies that

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

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

The reader can easily check that, after the change of variables

$$Y' = Y + X,$$

for instance, 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 bear in mind that we are considering a specific equation.

This paper studies with elliptic curves which have a simultaneous arithmetic progression. First we need a proper definition of these progressions. Let us consider P_0, \dots, P_n as above. If we ask for both x_0, \dots, x_n and y_0, \dots, y_n to be arithmetic progressions then the problem is far too easy, as P_0, \dots, P_n must be collinear and hence $n \leq 2$. Lots of 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.— With the above notation, P_0, \dots, P_n are a simultaneous arithmetic progression (s.a.p.) or the equation E is said to have a simultaneous arithmetic progression if:

- (a) x_0, \dots, 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 $y_{\sigma(0)}, \dots, y_{\sigma(n)}$ are in arithmetic progression.

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

With this definition, at least three straight problems arise:

- (a) The detection problem: Given an elliptic curve, does there exist an algorithm for deciding whether it contains or not a s.a.p. of length n (giving as well a change of variables if needed)?
- (b) The subsequence problem: If an elliptic curve has a s.a.p. of length $n + 1$, does it possess a s.a.p. of length n ? (Note 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?

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

Theorem 1.— Given an elliptic curve with an x -a.p., there exists an algorithm which decides whether or not the curve also has a s.a.p. with the given x -a.p. as support.

Theorem 2.— There are integers n such that there are examples of s.a.p. of length n which do not contain any s.a.p. of length $n - 1$.

Theorem 3.— There are no elliptic curves defined over \mathbf{Q} with s.a.p. of length 7. There are only finitely many non-isomorphic curves defined over \mathbf{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 ([4]) and Bremner ([3]). Apparently these papers had their starting point in the featuring of x -a.p. as by-product of a latin square problem (see more on this in [1, 2]). However, highly interesting results were sketched in both papers around the relationship between the existence of arithmetic progressions on a certain elliptic curve and its rank. In this same line a paper by Campbell appeared ([5]) pointing out far-reaching questions, probably too difficult for the state-of-the-art.

The history of the problem, though, can be traced back quite further, as (for the specific case of Mordell curves) it was treated previously by S.P. Mohanty ([8]) who studied x and y -a.p. separately and by Lee and Vélez ([7]) who first treated s.a.p., if only in the naive form mentioned above, without permutations involved. The motivation for these first works was, as many other times in the history of 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 search¹. Our first attempts were shown in [6], using a specific kind of s.a.p., which allowed us to find examples of s.a.p. of length 5. These methods were not at all exhaustive, as it accurately pointed out by Bremner in his MathSciNet review. After this work, we feel that some of the problems posed are worth a closer look and the setup remains challenging. As Bremner points out in [3]: “*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 $P_0 = (x_0, y_0), \dots, P_n = (x_n, y_n)$ in an elliptic curve, defined over K by a Weierstrass equation:

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

Let us suppose the points $P_0, \dots, P_n \in E(K)$ to be in x -a.p. We are interested then on finding, if there exists any, a change of variables, preserving the Weierstrass form of E , which transforms $P_i = (x_i, y_i)$

¹The longest x -a.p. found in an elliptic curve has 8 terms ([3]); for y -a.p. the record is 7 so far ([6]).

into $P'_i = (x'_i, y'_i)$ so that P'_0, \dots, P'_n is a s.a.p. on the corresponding equation E' . This change of variables must be of the form

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

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

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

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

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

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

These last 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, \dots, y_n is not an arithmetic progression if and only if first, second and fourth columns are independent; equivalently

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

Algorithm 1.– Our first detection algorithm is based on the fact that, the existence of a solution to our system (that is, the existence of a s.a.p.) is equivalent to A^* having rank 3. The formal algorithm goes like this:

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

Step 0: Choose a suitable set $\{y_0, \dots, y_n\}$ such that $(x_i, y_i) \in E(K)$.

Step 1: (Fool-proof checking) Check whether $\{y_0, \dots, y_n\}$ is an arithmetic progression. If so, we are finished; if not, find an s , $2 \leq s \leq n$ as above.

Step 2: For any $\sigma \in S_n$ and any $i \in \{2, \dots, n\}$, $i \neq s$, compute the minor formed by the first, second, s -th and i -th 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, back to step 0.

The main inconvenience of this procedure is its needing of $2^{n+1}(n+1)!(n-2)$ determinant computations, as 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 set-up will prove useful later on.

Algorithm 2.— Consider the affine points $Q_0 = (0, y_0, \sigma(0)), \dots, Q_n = (nd, y_n, \sigma(n)) \in \mathbf{A}^3(K)$. Note that, what we need from all them, in order to have a s.a.p., is to be in the same plane. This is the basis for our algorithm, whose input data and steps 0 and 1 are identical to the previous one:

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

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

Step 3: For $l = 2, \dots, n$ and $l \neq s$, we intersect the line

$$x = ld, \quad y = y_l$$

with the plane π_{ijk} .

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

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

As for computations is concerned, 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 each y_i , means a saving of around $(n-3)!$ computations.

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

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

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

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

and there are 4 of the 2^4 y -sequences that lead to simultaneous arithmetic progressions.

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

Now this x -arithmetic progression can be extended to one of length 5:

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

and there are 2 of the 2^5 possible y -sequences that lead to simultaneous arithmetic progressions.

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

The equation for both cases is

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

Now, 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 1: Find a procedure for deciding whether an elliptic curve has an x -a.p. of given length.

The most interesting results on this line are the parametrizations by Bremner in [3] which will be used afterwards in this paper. However they are still far from being useful from a computational point of view.

3 The subsequence problem

The programs developed in the previous section (specially the second one) were of great help with testing the examples we had created with the techniques shown on [6] and also with creating new ones. The counterexamples announced in Theorem 2 were product of these extensive calculations. Here we present the simplest one.

(Counter)Example.— Consider the following elliptic curve over \mathbf{Q} , in Tate normal form,

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

which has the 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 find a y -sequence that gives simultaneous arithmetic progression:

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

There is only one permutation σ which passes Algorithm 2 and, henceforth, allows the change of variables, $\sigma = (20413)$. The y' -arithmetic progression is

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

for the equation

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

This way, we have found a simultaneous arithmetic progression of length 5 not containing a simultaneous arithmetic progression of length 4, because the permutation involved is not the extension of an S_4 permutation. In our many calculations these are singular 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. But the fact is that these counterexamples happen, which, by the way, carry an additional difficulty for all arguments involving induction.

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

Open problem 2: Given an elliptic curve with a s.a.p. of length n , is there always a s.a.p. of length $n - 1$ whose support is contained in the support of the given one?

We have found no examples to support a negative answer to this question which, by the way, may serve as a weak induction result.

4 The bound problem

Our final look will be to the bound problem. As it was pointed out by Bremner in [3], this kind of problems tend to become unmanageable quite quickly. From our many attempts, we will describe here the most successful of them all; which relies on a parametrization of curves with x -a.p. due to Bremner ([3]) (here slightly changed for our purposes). In what follows we will assume $K = \mathbf{Q}$. Note that all the previous arguments do not rely on the base field at all.

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

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

with four points in x -a.p.;

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

Now, we consider the four polynomials F_0, \dots, F_3 given by

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

in $\mathbf{Q}[y_0, y_1, y_2, y_3, a, d, A, B]$, and compute a Gröbner basis of the ideal $\langle F_0, \dots, F_3 \rangle$. The `tdeg` ordering in Maple V gives a basis of ten elements which can be used for computing a, A, B taking d, y_0, \dots, y_3 as

parameters:

$$\begin{aligned}
A &= \frac{-1}{6^2 d^4} \left(y_0^4 - 9y_0^2 y_1^2 + 6y_2^2 y_0^2 + y_3^2 y_0^2 + 21y_1^4 - 39y_2^2 y_1^2 + 6y_3^2 y_1^2 + \right. \\
&\quad \left. 21y_2^4 - 9y_3^2 y_2^2 + y_3^4 \right) = -P/36d^4 \\
B &= \frac{1}{6^3 d^6} \left(y_3^4 y_0^2 + 4y_3^4 y_1^2 + y_3^4 y_2^2 - 9y_3^2 y_2^4 - 8y_3^2 y_2^2 y_0^2 + 24y_3^2 y_1^4 \right. \\
&\quad - 8y_3^2 y_0^2 y_1^2 - 12y_3^2 y_2^2 y_1^2 + y_3^2 y_0^4 + y_0^4 y_1^2 - 9y_0^2 y_1^4 + 20y_1^6 \\
&\quad - 21y_1^4 y_2^2 + 4y_0^4 y_2^2 + 20y_2^6 - 21y_1^2 y_2^4 + 24y_0^2 y_2^4 \\
&\quad \left. - 12y_0^2 y_2^2 y_1^2 \right) = Q/6^3 d^6 \\
a &= \frac{-1}{6d^2} \left(-2y_0^2 + 5y_1^2 - 4y_2^2 + y_3^2 \right) = -R/6d^2
\end{aligned}$$

and, in addition, the first member of the basis is

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

Now, making the scaling with $u = 6d$ we obtain the following parametrization:

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

We will use from now on A, B, a, d for these new polynomials. It is interesting noting that the points in x -a.p. are now

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

We will try to produce curves with a s.a.p. of given length with a variant of Algorithm 1 which we will illustrate with the case of length 6. In fact, using this procedure we might compute all curves with such a s.a.p. in contrast with the lack of exhaustiveness of [6]. If we want points $P_4 = (a + 4d, z_4)$ and $P_5 = (a + 5d, z_5)$ to be in the curve it must hold

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

Hence, for the sake of consistency, we will call

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

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

Example.— We will show how to proceed using the 3-cycle $\sigma = (210345)$. After the above remarks, we may use the matrix M , given by

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

instead of the original matrix A^* from Algorithm 1; and ask M to have rank 3, as we are assuming $d \neq 0$. Note that $\{y_0, \dots, y_5\}$ are *not* the y -coordinates of the points P_0, \dots, P_5 . As all the minors are linear polynomials on y_0, \dots, y_5 and we have also 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 parametrizations:

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

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

from which the first one only contains points inducing $d = 0$ and therefore must be discarded. In fact, these trivial solutions appear in all cases, which is clearly a by-product of our previous assumptions.

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

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

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

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

which has the following s.a.p.

$$\left(\frac{1536y_0^2}{19^2}, \frac{97632y_0^3}{19^3} \right), \left(\frac{1584y_0^2}{19^2}, \frac{97056y_0^3}{19^3} \right), \left(\frac{1632y_0^2}{19^2}, \frac{978208y_0^3}{19^3} \right),$$

$$\left(\frac{1680y_0^2}{19^2}, \frac{96480y_0^3}{19^3}\right), \left(\frac{1728y_0^2}{19^2}, \frac{95904y_0^3}{19^3}\right), \left(\frac{1776y_0^2}{19^2}, \frac{95328y_0^3}{19^3}\right);$$

All these curves are isomorphic to (an *easy*) 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 cases, using the previous computations with all possible sign and permutation choices, counting only the number of possible solutions, that is, cases where the line does not induce $d = 0$.

To be precise, only half of the sign choices have to be considered, as 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 choice of signs and permutations.

Even so, not all of these cases are non-isomorphic elliptic curves; there might be isomorphic curves among them as well as genus 0 curves. In the appendix we have given some explicit data for the first 100 curves actually computed with this method where repeated curves already appear (in fact, there are only 56 non-isomorphic curves).

As a side remark, the distribution of the possible is extremely regular: there are 600 allowed permutations (that is 600 lines not giving $d = 0$) for every sign choice and only sign changes were allowed most for the solutions for a fixed permutation. By the way, these differences usually disappeared when finding the solutions to the system given by A^* . This, together with the repeated cases shown in the appendix, gives a heuristic estimation of only around 350 non-isomorphic curves, but filling the details of such a list is beyond our computational possibilities so far.

As for length 7 is concerned our procedure shows there are no solutions, as all induce $d = 0$. This case exhausts the possibilities of computer checking, at least with these methods, as it took around 20 hours of CPU (which implied four days in real time) and, more constraining, 2^{11} Mb of stack memory. For considering this attack to length 8, these figures should be multiplied at least by 16 (8 for the number of permutations and there are twice as many minors now), let

alone the additional difficulty of adding a new quadratic polynomial to the system, which is not easy to measure.

Open problem 3: Find a universal bound for the length of a s.a.p. on elliptic curves over \mathbf{Q} .

Note that an affirmative answer to the open problem 2 would mean 6 is the answer to open problem 3.

Appendix: Examples of curves with s.a.p. of length 6

Please note that this stream was computer-generated taking as a unique choice the permutation. Due to this, some of the curves (for instance examples 009 and 010) appear more than once, as they have different s.a.p. Also one may find isomorphic curves (as 001 and 002). As we said above, only 56 non-isomorphic curves can be found in this table, but we have preferred to leave as it came, as we feel it illustrated better the phenomenon. The entries of the table after each equation are:

- 1) Permutation (σ): noted as above by $(\sigma(0)\sigma(1)\dots\sigma(5))$.
- 2) Numerical data (N.D.): The set $[a, d, b, d']$ which fits the equation.
- 3) Rank (r): The rank of the curve, computed with APECS (\leq means APECS failed to actually compute the rank, in which case the best upper bound given is shown). All curves have trivial torsion group.

001	$Y^2 - 180YX + 8100X^2 - X^3 + 4892251392X - 134063884477440$
	$\sigma = (321450)$, N.D. = $[66432, -20304, 13044672, -5725728]$, $r = 5$

002	$Y^2 + 180YX + 8100X^2 - X^3 + 4892251392X - 134063884477440$
	$\sigma = (054123)$, N.D. = $[-35088, 20304, -13044672, 5725728]$, $r = 5$

003	$Y^2 + 20YX + 100X^2 - X^3 + 36478512X - 82321246080$
	$\sigma = (423150)$, N.D. = $[5724, -1584, -367704, 139392]$, $r = 5$

004	$Y^2 - 60YX + 900X^2 - X^3 + 86832X - 8864640$
-----	--

$$\sigma = (534201), \text{ N.D.} = [-324, 144, 9288, -3456], r = 2$$

$$\begin{aligned} 005 \quad & Y^2 - 20YX + 100X^2 - X^3 + 466992X - 549797760 \\ & \sigma = (045312), \text{ N.D.} = [1308, -432, -33576, 3456], r = 3 \end{aligned}$$

$$\begin{aligned} 006 \quad & Y^2 - 2YX + X^2 - X^3 + 238707X - 41709006 \\ & \sigma = (150423), \text{ N.D.} = [-513, 180, 8487, -3600], r = 3 \end{aligned}$$

$$\begin{aligned} 007 \quad & Y^2 - 180YX + 8100X^2 - X^3 + 51432192X - 368371860480 \\ & \sigma = (034521), \text{ N.D.} = [-9312, 4752, -638496, 313632], r = 4 \end{aligned}$$

$$\begin{aligned} 008 \quad & Y^2 - 612YX + 93636X^2 - X^3 + 26962612992X - 1882111797863424 \\ & \sigma = (145032), \text{ N.D.} = [-164832, 66960, -19904832, 12454560], r = 5 \end{aligned}$$

$$\begin{aligned} 009 \quad & Y^2 + 396YX + 39204X^2 - X^3 + 388106595072X - 88686989876929536 \\ & \sigma = (250143), \text{ N.D.} = [-715488, 235440, 459510624, -153977760], r = 5 \end{aligned}$$

$$\begin{aligned} 010 \quad & Y^2 - 576YX + 82944X^2 - X^3 + 271059091200X - 49072046238950400 \\ & \sigma = (134502), \text{ N.D.} = [734160, -265680, -415035360, 130714560], r = 5 \end{aligned}$$

$$\begin{aligned} 011 \quad & Y^2 - 576YX + 82944X^2 - X^3 + 271059091200X - 49072046238950400 \\ & \sigma = (350124), \text{ N.D.} = [-594240, 265680, 238537440, -130714560], r = 5 \end{aligned}$$

$$\begin{aligned} 012 \quad & Y^2 + 396YX + 39204X^2 - X^3 + 388106595072X - 88686989876929536 \\ & \sigma = (305412), \text{ N.D.} = [-715488, 235440, -310378176, 153977760], r = 5 \end{aligned}$$

$$\begin{aligned} 013 \quad & Y^2 - 612YX + 93636X^2 - X^3 + 26962612992X - 1882111797863424 \\ & \sigma = (410523), \text{ N.D.} = [-164832, 66960, 42367968, -12454560], r = 5 \end{aligned}$$

$$\begin{aligned} 014 \quad & Y^2 - 180YX + 8100X^2 - X^3 + 51432192X - 368371860480 \\ & \sigma = (521034), \text{ N.D.} = [-9312, 4752, 929664, -313632], r = 4 \end{aligned}$$

$$\begin{aligned} 015 \quad & Y^2 - 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080 \\ & \sigma = (230145), \text{ N.D.} = [-30384, 11808, -6045408, 2904768], r = 6 \end{aligned}$$

$$\begin{aligned} 016 \quad & Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800 \\ & \sigma = (341250), \text{ N.D.} = [-7344, 3744, -714528, 292032], r = 5 \end{aligned}$$

$$\begin{aligned} 017 \quad & Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800 \\ & \sigma = (503412), \text{ N.D.} = [11376, -3744, 745632, -292032], r = 5 \end{aligned}$$

018	$Y^2 + 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080$ $\sigma = (014523)$, N.D. = [28656, -11808, -8478432, 2904768], $r = 6$
019	$Y^2 - 1800YX + 81000X^2 - X^3 + 7410269014272X - 8108956611489899520$ $\sigma = (302145)$, N.D. = [2763696, -577584, 3502719072, -1323822528], $r \leq 6$
020	$Y^2 + 2880YX + 2073600X^2 - X^3 + 403246536682752X - 3207719147336296058880$ $\sigma = (413250)$, N.D. = [-829968, 5312736, 62302243392, -30155089536], $r \leq 6$
021	$Y^2 + 4680YX + 5475600X^2 - X^3 + 3994541989632X - 6207305561351930880$ $\sigma = (524301)$, N.D. = [-2327712, 728784, -3390388704, 2107643328], $r \leq 7$
022	$Y^2 - 2880YX + 2073600X^2 - X^3 + 8792422324992X - 14409886139859502080$ $\sigma = (035412)$, N.D. = [7563792, -2228688, -8618074272, 1791865152], $r \leq 11$
023	$Y^2 + 7632YX + 14561856X^2 - X^3 + 1208964238739712X - 23944945010158503235584$ $\sigma = (140523)$, N.D. = [-42040752, 12290400, 265952884032, -83918851200], $r \leq 7$
024	$Y^2 - 6912YX + 11943936X^2 - X^3 + 214026269587200X - 1973672371225801958400$ $\sigma = (250134)$, N.D. = [-9752640, 7294320, 76016037600, -26872274880], $r \leq 8$
025	$Y^2 + 120YX + 3600X^2 - X^3 + 81948672X - 327577374720$ $\sigma = (532140)$, N.D. = [8064, -3168, 1169856, -418176], $r = 4$
026	$Y^2 + 960YX + 230400X^2 - X^3 + 92277352334592X - 342160070800370356224$ $\sigma = (043251)$, N.D. = [11544048, -3013920, -34095021120, 10813944960], $r = 4$
027	$Y^2 + 2616YX + 1710864X^2 - X^3 + 3327107104512X - 3360005144504534016$ $\sigma = (154302)$, N.D. = [-515808, 403920, -2454087456, 906396480], $r \leq 6$
028	$Y^2 - 3072YX + 2359296X^2 - X^3 + 2328753038487552X - 49786655684722942869504$ $\sigma = (205413)$, N.D. = [-55130112, 19313280, 240362650368, -111012733440], $r \leq 6$
029	$Y^2 - 4944YX + 6110784X^2 - X^3 + 14552162687232X - 21391150302252205056$ $\sigma = (310524)$, N.D. = [1164672, 340560, 5468006304, -44953920], $r \leq 7$
030	$Y^2 - 960YX + 230400X^2 - X^3 + 19321742592X - 1033886822584320$ $\sigma = (421035)$, N.D. = [60912, 6048, 38636352, -72576], $r = 5$

- 031 $Y^2 + 40YX + 400X^2 - X^3 + 8854272X - 8259978240$
 $\sigma = (153420)$, N.D. = $[-2448, 1584, 242208, -69696]$, $r = 4$
-
- 032 $Y^2 - 64YX + 1024X^2 - X^3 + 1389312X - 394896384$
 $\sigma = (204531)$, N.D. = $[-1152, 720, -44064, 14400]$, $r = 3$
-
- 033 $Y^2 - 64YX + 1024X^2 - X^3 + 1389312X - 394896384$
 $\sigma = (420153)$, N.D. = $[2448, -720, 27936, -14400]$, $r = 3$
-
- 034 $Y^2 - 40YX + 400X^2 - X^3 + 8854272X - 8259978240$
 $\sigma = (531204)$, N.D. = $[5472, -1584, 106272, -69696]$, $r = 4$
-
- 035 $Y^2 - 1080YX + 291600X^2 - X^3 + 4379037151491072X - 136063103467431710822400$
 $\sigma = (240315)$, N.D. = $[-77988192, 33054048, -438167226816, 226486336896]$, $r \leq 8$
-
- 036 $Y^2 - 720YX + 129600X^2 - X^3 + 9969629720832X - 13778174775900128256$
 $\sigma = (351420)$, N.D. = $[-3640128, 1648080, -6422790240, 2155688640]$, $r = 1$
-
- 037 $Y^2 + 5544YX + 7683984X^2 - X^3 + 422337203926272X - 3401406251614088487936$
 $\sigma = (402531)$, N.D. = $[-18956688, 10568880, 102961496736, -29550588480]$, $r \leq 7$
-
- 038 $Y^2 + 1080YX + 291600X^2 - X^3 + 4379037151491072X - 136063103467431710822400$
 $\sigma = (513042)$, N.D. = $[87282048, -33054048, 438167226816, -226486336896]$, $r \leq 8$
-
- 039 $Y^2 - 720YX + 129600X^2 - X^3 + 9969629720832X - 13778174775900128256$
 $\sigma = (024153)$, N.D. = $[4600272, -1648080, -6422790240, 2155688640]$, $r = 1$
-
- 040 $Y^2 - 5544YX + 7683984X^2 - X^3 + 422337203926272X - 3401406251614088487936$
 $\sigma = (135204)$, N.D. = $[33887712, -10568880, -102961496736, 29550588480]$, $r \leq 7$
-
- 041 $Y^2 + 20YX + 100X^2 - X^3 + 466992X - 549797760$
 $\sigma = (342015)$, N.D. = $[-852, 432, 16296, 3456]$, $r = 3$
-
- 042 $Y^2 - 60YX + 900X^2 - X^3 + 86832X - 8864640$
 $\sigma = (453120)$, N.D. = $[396, -144, -7992, 3456]$, $r = 2$
-
- 043 $Y^2 - 20YX + 100X^2 - X^3 + 36478512X - 82321246080$
 $\sigma = (504231)$, N.D. = $[-2196, 1584, -329256, 139392]$, $r = 5$
-
- 044 $Y^2 - 4YX + 4X^2 - X^3 + 3819312X - 2669376384$

$$\sigma = (231504), \text{ N.D.} = [1548, -720, -76104, 28800], r = 3$$

$$045 \quad Y^2 - 2880YX + 2073600X^2 - X^3 + 110993807215872X - 445121432212494274560$$
$$\sigma = (402315), \text{ N.D.} = [14071152, -3627936, 35652163392, -14061879936], r \leq 7$$

$$046 \quad Y^2 + 360YX + 32400X^2 - X^3 + 27909792000X - 1526822144640000$$
$$\sigma = (513420), \text{ N.D.} = [-99600, 75600, 73720800, -22680000], r \leq 5$$

$$047 \quad Y^2 - 7056YX + 12446784X^2 - X^3 + 129437671756032X - 543091962160151110656$$
$$\sigma = (135042), \text{ N.D.} = [17527152, -4944240, -5119105824, 6467065920], r \leq 5$$

$$048 \quad Y^2 - 7488YX + 14017536X^2 - X^3 + 841545692773632X - 15278101189303210758144$$
$$\sigma = (240153), \text{ N.D.} = [-34464912, 10864800, -202374030528, 65579932800], r \leq 8$$

$$049 \quad Y^2 - 6696YX + 11209104X^2 - X^3 + 1767944739520512X - 27067552170879621206016$$
$$\sigma = (351204), \text{ N.D.} = [-46912128, 22001760, 291906110016, -122241778560], r \leq 7$$

$$050 \quad Y^2 - 90YX + 2025X^2 - X^3 + 3434834187X - 77407635019590$$
$$\sigma = (053421), \text{ N.D.} = [39747, -2376, 3706047, -627264], r = 5$$

$$051 \quad Y^2 + 306YX + 23409X^2 - X^3 + 338359707X - 3186238861494$$
$$\sigma = (104532), \text{ N.D.} = [-21237, 11880, 3783861, -1425600], r = 4$$

$$052 \quad Y^2 - 612YX + 93636X^2 - X^3 + 5413755312X - 203919287135616$$
$$\sigma = (320154), \text{ N.D.} = [152652, -47520, 26753112, -11404800], r = 4$$

$$053 \quad Y^2 - 90YX + 2025X^2 - X^3 + 3434834187X - 77407635019590$$
$$\sigma = (431205), \text{ N.D.} = [27867, 2376, 569727, 627264], r = 5$$

$$054 \quad Y^2 + 396YX + 39204X^2 - X^3 + 388106595072X - 88686989876929536$$
$$\sigma = (214503), \text{ N.D.} = [461712, -235440, -310378176, 153977760], r = 5$$

$$055 \quad Y^2 - 612YX + 93636X^2 - X^3 + 26962612992X - 1882111797863424$$
$$\sigma = (325014), \text{ N.D.} = [169968, -66960, 42367968, -12454560], r = 5$$

$$056 \quad Y^2 - 180YX + 8100X^2 - X^3 + 51432192X - 368371860480$$
$$\sigma = (430125), \text{ N.D.} = [14448, -4752, 929664, -313632], r = 4$$

$$057 \quad Y^2 - 48YX + 576X^2 - X^3 + 9262512X - 8383430016$$
$$\sigma = (250341), \text{ N.D.} = [-3348, 1440, -123552, 43200], r = 2$$

058	$Y^2 - 24YX + 144X^2 - X^3 + 578907X - 130991094$ $\sigma = (412503)$, N.D. = $[963, -360, 11556, -5400]$, $r = 2$
-----	---

059	$Y^2 - 60YX + 900X^2 - X^3 + 767232X - 253808640$ $\sigma = (523014)$, N.D. = $[1008, -288, 16416, -1728]$, $r = 3$
-----	--

060	$Y^2 - 60YX + 900X^2 - X^3 + 767232X - 253808640$ $\sigma = (145230)$, N.D. = $[-432, 288, 7776, 1728]$, $r = 3$
-----	---

061	$Y^2 - 5184YX + 6718464X^2 - X^3 + 142783615579392X - 708085096419827994624$ $\sigma = (352041)$, N.D. = $[13189008, -5387040, -40963299264, 13898563200]$, $r = 4$
-----	--

062	$Y^2 - 2142YX + 1147041X^2 - X^3 + 15808640228307X - 39293749322977053294$ $\sigma = (403152)$, N.D. = $[5885823, -1961820, 10341141993, -4072738320]$, $r \leq 7$
-----	---

063	$Y^2 - 612YX + 93636X^2 - X^3 + 52888734000X - 42522157354464000$ $\sigma = (514203)$, N.D. = $[-243780, 110160, 98574840, -44945280]$, $r \leq 5$
-----	---

064	$Y^2 - 396YX + 39204X^2 - X^3 + 16655166000X - 690091901769600$ $\sigma = (025314)$, N.D. = $[250140, -71280, -60813720, 18817920]$, $r = 4$
-----	---

065	$Y^2 - 1710YX + 731025X^2 - X^3 + 1041760268307X - 785868626594613294$ $\sigma = (130425)$, N.D. = $[-1270977, 427140, -1427543055, 579201840]$, $r \leq 5$
-----	--

066	$Y^2 - 3240YX + 2624400X^2 - X^3 + 2359518446592X - 1392039372309073920$ $\sigma = (241530)$, N.D. = $[502176, 175392, 1361800512, 14732928]$, $r = 7$
-----	---

067	$Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800$ $\sigma = (503412)$, N.D. = $[11376, -3744, 745632, -292032]$, $r = 5$
-----	--

068	$Y^2 + 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080$ $\sigma = (014523)$, N.D. = $[28656, -11808, -8478432, 2904768]$, $r = 6$
-----	---

069	$Y^2 - 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080$ $\sigma = (230145)$, N.D. = $[-30384, 11808, -6045408, 2904768]$, $r = 6$
-----	---

070	$Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800$ $\sigma = (341250)$, N.D. = $[-7344, 3744, -714528, 292032]$, $r = 5$
-----	---

- 071 $Y^2 - 960YX + 230400X^2 - X^3 + 13201887036672X - 17372103328571019264$
 $\sigma = (502341)$, N.D. = [5909328, -1703520, 8039027520, -3454738560], $r = 6$
-
- 072 $Y^2 + 600YX + 90000X^2 - X^3 + 4185188352X - 119899753943040$
 $\sigma = (013452)$, N.D. = [52704, -12384, -22572864, 6390144], $r \leq 7$
-
- 073 $Y^2 + 768YX + 147456X^2 - X^3 + 28465015272192X - 52273748736104702976$
 $\sigma = (124503)$, N.D. = [4297392, -2075760, -8562479328, 3860913600], $r \leq 6$
-
- 074 $Y^2 - 4368YX + 4769856X^2 - X^3 + 102164509274112X - 521183246173070966784$
 $\sigma = (235014)$, N.D. = [7567488, -3850560, 20709101952, -8825483520], $r \leq 6$
-
- 075 $Y^2 - 192YX + 9216X^2 - X^3 + 1067634432X - 20407326188544$
 $\sigma = (340125)$, N.D. = [-32832, 12240, -6162912, 2496960], $r = 4$
-
- 076 $Y^2 + 120YX + 3600X^2 - X^3 + 210573084672X - 33546735732363264$
 $\sigma = (451230)$, N.D. = [-495072, 211680, -339888960, 124467840], $r = 6$
-
- 077 $Y^2 - 180YX + 8100X^2 - X^3 + 51432192X - 368371860480$
 $\sigma = (125430)$, N.D. = [14448, -4752, -638496, 313632], $r = 4$
-
- 078 $Y^2 - 612YX + 93636X^2 - X^3 + 26962612992X - 1882111797863424$
 $\sigma = (230541)$, N.D. = [169968, -66960, -19904832, 12454560], $r = 5$
-
- 079 $Y^2 + 396YX + 39204X^2 - X^3 + 388106595072X - 88686989876929536$
 $\sigma = (341052)$, N.D. = [461712, -235440, 459510624, -153977760], $r = 5$
-
- 080 $Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800$
 $\sigma = (214305)$, N.D. = [-7344, 3744, 745632, -292032], $r = 5$
-
- 081 $Y^2 - 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080$
 $\sigma = (325410)$, N.D. = [-30384, 11808, 8478432, -2904768], $r = 6$
-
- 082 $Y^2 + 300YX + 22500X^2 - X^3 + 894074112X - 19561912750080$
 $\sigma = (541032)$, N.D. = [28656, -11808, 6045408, -2904768], $r = 6$
-
- 083 $Y^2 - 60YX + 900X^2 - X^3 + 48045312X - 189087436800$
 $\sigma = (052143)$, N.D. = [11376, -3744, -714528, 292032], $r = 5$
-
- 084 $Y^2 - 3240YX + 2624400X^2 - X^3 + 2359518446592X - 1392039372309073920$

	$\sigma = (314025)$, N.D. = [502176, 175392, 1435465152, -14732928], $r = 7$
085	$Y^2 - 1710YX + 731025X^2 - X^3 + 1041760268307X - 785868626594613294$ $\sigma = (425130)$, N.D. = [-1270977, 427140, 1468466145, -579201840], $r \leq 5$
086	$Y^2 - 396YX + 39204X^2 - X^3 + 16655166000X - 690091901769600$ $\sigma = (530241)$, N.D. = [250140, -71280, 33275880, -18817920], $r = 4$
087	$Y^2 - 612YX + 93636X^2 - X^3 + 52888734000X - 4252215735446400$ $\sigma = (041352)$, N.D. = [-243780, 110160, -126151560, 44945280], $r \leq 5$
088	$Y^2 + 4284YX + 4588164X^2 - X^3 + 252938243652912X - 2514799956670531410816$ $\sigma = (152403)$, N.D. = [23543292, -7847280, 80180396856, -32581906560], $r \leq 7$
089	$Y^2 - 5184YX + 6718464X^2 - X^3 + 142783615579392X - 708085096419827994624$ $\sigma = (203514)$, N.D. = [13189008, -5387040, 28529516736, -13898563200], $r = 4$
090	$Y^2 - 60YX + 900X^2 - X^3 + 767232X - 253808640$ $\sigma = (410325)$, N.D. = [-432, 288, 16416, -1728], $r = 3$
091	$Y^2 - 60YX + 900X^2 - X^3 + 767232X - 253808640$ $\sigma = (032541)$, N.D. = [1008, -288, 7776, 1728], $r = 3$
092	$Y^2 - 24YX + 144X^2 - X^3 + 578907X - 130991094$ $\sigma = (143052)$, N.D. = [963, -360, -15444, 5400], $r = 2$
093	$Y^2 - 48YX + 576X^2 - X^3 + 9262512X - 8383430016$ $\sigma = (305214)$, N.D. = [-3348, 1440, 92448, -43200], $r = 2$
094	$Y^2 + 120YX + 3600X^2 - X^3 + 81948672X - 327577374720$ $\sigma = (514320)$, N.D. = [-7776, 3168, -921024, 418176], $r = 4$
095	$Y^2 - 960YX + 230400X^2 - X^3 + 19321742592X - 1033886822584320$ $\sigma = (025431)$, N.D. = [91152, -6048, 38273472, 72576], $r = 5$
096	$Y^2 - 4944YX + 6110784X^2 - X^3 + 14552162687232X - 21391150302252205056$ $\sigma = (130542)$, N.D. = [2867472, -340560, 5243236704, 44953920], $r \leq 7$
097	$Y^2 - 3072YX + 2359296X^2 - X^3 + 2328753038487552X - 49786655684722942869504$ $\sigma = (241053)$, N.D. = [41436288, -19313280, -314701016832, 111012733440], $r \leq 6$

098	$Y^2 - 2616YX + 1710864X^2 - X^3 + 3327107104512X - 3360005144504534016$ $\sigma = (352104)$, N.D. = [1503792, -403920, -2077894944, 906396480], $r \leq 6$
-----	---

099	$Y^2 - 960YX + 230400X^2 - X^3 + 92277352334592X - 342160070800370356224$ $\sigma = (403215)$, N.D. = [-3525552, 3013920, -19974703680, 10813944960], $r \leq 4$
-----	--

100	$Y^2 - 60YX + 900X^2 - X^3 + 767232X - 253808640$ $\sigma = (145230)$, N.D. = [-432, 288, 7776, 1728], $r = 3$
-----	--

As Bremner noticed in [3], points in arithmetic progression seem to have a tendency to be independent. If we only take into account the ranks actually computed, we get an average over 4, when the average for random curves is known to be much smaller ([10]).

It should be noticed that example 039 is a remarkable case: no x -a.p. of length 6 were known in groups of rank one (see the last remark of [3]), and [4] 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 a much harder problem to tackle.

References

- [1] A. Bremner: *On squares of squares*. Acta Arith. **LXXXVIII** (1999) 289–297.
- [2] A. Bremner: *On squares of squares II*. Acta Arith. **XCIX** (3) (2001) 289–308.
- [3] A. Bremner: *On arithmetic progressions on elliptic curves*. Experiment. Math. **8** (4) (1999) 409–413. -
- [4] A. Bremner, J.H. Silverman, N. Tzanakis: *Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$* . J. Number Theory **80** (2000) 187–208.
- [5] G. Campbell: *A note on arithmetic progressions on elliptic curves*. J. Integer Seq. **6** (2003) 03.1.3.
- [6] I. García-Selfa, J.M. Tornero: *Searching for simultaneous arithmetic progressions on elliptic curves*. Bull. Austral. Math. Soc. **71** (2005) 417–424.

- [7] J.B. Lee, W.Y. Vélez: *Integral solutions in arithmetic progression for $y^2 = x^3 + k$* . Period. Math. Hungar. **25** (1992) 31–49.
- [8] S.P. Mohanty: *On consecutive integral solutions for $y^2 = x^3 + k$* . Proc. Amer. Math. Soc. **48** (1975) 281–285.
- [9] J.H. Silverman: *The arithmetic of elliptic curves*. Springer (1986).
- [10] M.P. Young: *Low-lying zeros of families of elliptic curves*. J. Amer. Math. Soc. **19** (2006) 205–250.

Irene García-Selfa (Email: igselfa@us.es).

José M. Tornero (Corresponding author, email: tornero@us.es).

Departamento de Álgebra

Facultad de Matemáticas

Universidad de Sevilla

Apdo. 1160. 41080 Sevilla (Spain).