On Arithmetic Progressions on Elliptic Curves

Andrew Bremner

We study arithmetic progressions in the x-coordinates of rational points on elliptic curves. An infinite family of elliptic curves is found, each containing an arithmetic progression of length 8.

1. Questions in number theory that interrelate two group structures are easily posed, but often lead to intractable problems. For example, prime numbers are defined by multiplicative structure, and the Goldbach Conjecture that any even positive integer is the sum of two primes, remains unproved. Here, we ask a question about the rational points on an elliptic curve that relates the group structure of the elliptic curve to the addition of rational numbers. A set of points on a rational elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

with $a_1, \dots, a_6 \in \mathbb{Q}$, is said to be an arithmetic progression on the curve if the x-coordinates of the points form an arithmetic progression. For example, the curve $y^2 + y = x^3 - 7x + 6$ (which happens to be the curve of rational rank 3 with smallest conductor; see [Buhler et al. 1985]) contains an arithmetic progression of length 8: $(-3, 0)$, $(-2, 3)$, $(-1, 3)$, $(0, 2)$, $(1, 0)$, $(2, 0)$, $(3, 3)$, $(4, 6)$. Can there exist arbitrarily large arithmetic progressions on elliptic curves? In this note we show that there are infinitely many elliptic curves with length 8 arithmetic progressions. We have been unable to find a progression of length 9. It seems that points of an arithmetic progression have a tendency to be linearly independent in the group of rational points, and this was exploited in [Bremner et al. 1999], where careful height computations show that the curves $y^2 = x(x^2 - n^2)$ (with n squarefree) cannot contain any nontrivial arithmetic progressions if the rational rank is 1. Accordingly, progressions of length 9 or more, if they exist, should occur on curves of relatively high rank and

© A K Peters, Ltd.
1058-6458/1999 $0.50 per page
Experimental Mathematics **8**:4, page 409

correspondingly large coefficients. See also [Lee and Vélez 1992], where infinitely many curves of type $y^2 = x^3 + k$ are found containing arithmetic progressions of length 4.

All symbolic computations in this paper were performed with Maple V, and extensive use has been made of the APECS program [Connell n.d.].

2. It is in general straightforward to write down a cubic in x which takes on square values at the 8 values $x_1, \dots, x_8$, by writing $(x - x_1) \dots (x - x_8)$ identically equal to $q(x)^2 - c(x)$, where q is quartic and c is the required cubic. However, when the 8 values $x_1, \dots, x_8$ form an arithmetic progression, this idea fails in view of the identity

$$\begin{aligned} x(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)(x+7) \\ = (x^4+14x^3+63x^2+98x+28)^2 - 16(7+2x)^2. \end{aligned}$$

Another approach is needed. First, observe that an arithmetic progression on a curve E is independent of the Weierstrass equation chosen for E, since an x-coordinate x' is related to the original x-coordinate by a transformation of type $x' = u^2x + r$. Without loss of generality, therefore, we shall work with Weierstrass equations of the form

$$y^2 = x^3 + Ax + B. \tag{2}$$

First, consider the case of an arithmetic progression on the curve of length 5. Suppose that $a \pm 2d, a \pm d, a$ are x-coordinates of five points on (2). Then

$$\begin{aligned}
&a^3 + 6a^2d + 12ad^2 + 8d^3 + A\,(a+2d) + B = r^2 \\
&a^3 + 3a^2d + \ 3ad^2 + \ d^3 + A\,(a+d) \ + B = s^2 \\
&a^3 \qquad\qquad\qquad\qquad\quad + A\,a \qquad + B = t^2 \\
&a^3 - 3a^2d + \ 3ad^2 - \ d^3 + A\,(a-d) \ + B = u^2 \\
&a^3 - 6a^2d + 12ad^2 - 8d^3 + A\,(a-2d) + B = v^2.
\end{aligned}$$

Consequently, five points in arithmetic progression correspond to solutions of the system

$$s^2 - 2t^2 + u^2 = 6ad^2, \tag{3}$$

$$r^2 - 3s^2 + 3t^2 - u^2 = 6d^3, \tag{4}$$

$$r^2 - 4s^2 + 6t^2 - 4u^2 + v^2 = 0, \tag{5}$$

with

$$A = (1/d)(s^2-t^2) - (3a^2+3ad+d^2), \tag{6}$$

$$B = (1/d)((a+d)t^2-as^2) + a(a+d)(2a+d). \tag{7}$$

Given a solution r, s, t, u, v of (5), scaling by the factor $36(r^2 - 3s^2 + 3t^2 - u^2)$ results in a solution R, S, T, U, V of (3)–(5) with

$$a = 6(S^2 - 2T^2 + U^2), \tag{8}$$

$$d = 6(R^2 - 3S^2 + 3T^2 - U^2), \tag{9}$$

where

$$-R^2 + 4S^2 - 6T^2 + 4U^2 = \square \ \ (= V^2), \tag{10}$$

and, from (6), (7),

$$\begin{aligned} A = -36(&R^4 - 9R^2S^2 + 21S^4 + 6R^2T^2 - 39S^2T^2 \\ &+ 21T^4 + R^2U^2 + 6S^2U^2 - 9T^2U^2 + U^4) \end{aligned} \tag{11}$$

$$\begin{aligned} B = 216(&R^4S^2 - 9R^2S^4 + 20S^6 + 4R^4T^2 - 12R^2S^2T^2 \\ &- 21S^4T^2 + 24R^2T^4 - 21S^2T^4 + 20T^6 + R^4U^2 \\ &- 8R^2S^2U^2 + 24S^4U^2 - 8R^2T^2U^2 - 12S^2T^2U^2 \\ &- 9T^4U^2 + R^2U^4 + 4S^2U^4 + T^2U^4). \end{aligned} \tag{12}$$

It is further possible to parametrize the quadric (10) in the standard way, by putting

$$(R, S, T, U, V) = (v+w,\ v+x,\ v+y,\ v+z,\ v)$$

to give

$$\begin{aligned} R : S : T : U : V = \\ w^2 - 8wx + 12wy - 8wz + 4x^2 - 6y^2 + 4z^2 : \\ -w^2 + 2wx + 12xy - 4x^2 - 8xz - 6y^2 + 4z^2 : \\ -w^2 + 2wy + 4x^2 - 8xy + 6y^2 - 8yz + 4z^2 : \\ -w^2 + 2wz + 4x^2 - 8xz - 6y^2 + 12yz - 4z^2 : \\ -w^2 + 4x^2 - 6y^2 + 4z^2. \end{aligned} \tag{13}$$

3. For seven points in the arithmetic progression we demand that $a \pm 3d$ give x-coordinates of rational points on (2). This becomes

$$4R^2 - 6S^2 + 4T^2 - U^2 = \square, \tag{14}$$

$$-4R^2 + 15S^2 - 20T^2 + 10U^2 = \square, \tag{15}$$

which in virtue of (13) represents the intersection of two quartics in five-dimensional projective space.

A small computer search over the parameters w, x, y, z reveals that solutions of (14), (15) occur whenever $w = x$, $z = 0$. This corresponds to

$$\begin{aligned} R : S : T : U = -x^2 + 4xy - 2y^2 : \\ -x^2 + 4xy - 2y^2 : \\ x^2 - 2xy + 2y^2 : \\ x^2 - 2y^2, \end{aligned} \tag{16}$$

with (on removing 2^2 from a and d, and 2^4 from A, 2^6 from B)

$$(a, d) = (0,\ \ 6xy(x-y)(x-2y)) \tag{17}$$

and

$$\begin{aligned} A &= -252x^2y^2(x-y)^2(x-2y)^2, \\ B &= 324x^2y^2(x-y)^2(x-2y)^2(x^2-2xy+2y^2)^2. \end{aligned} \tag{18}$$

For 8 points in the arithmetic progression, one of the following equations must also be satisfied, corresponding to $x = a \pm 4d$ giving rational points on (2):

$$10R^2 - 20S^2 + 15T^2 - 4U^2 = \square, \tag{19}$$

$$-10R^2 + 36S^2 - 45T^2 + 20U^2 = \square. \tag{20}$$

For the parametrization (16) to satisfy (19) and (20) demands, respectively,

$$x^4 + 20x^3y - 64x^2y^2 + 40xy^3 + 4y^4 = \square, \tag{21}$$

$$x^4 - 28x^3y + 80x^2y^2 - 56xy^3 + 4y^4 = \square. \tag{22}$$

Individually, these equations are both models for the elliptic curve $y^2 = x^3 - x^2 - 36x + 36$ (not surprising, because arithmetic progressions with common difference d are also arithmetic progressions with common difference $-d$). APECS determines the rational rank of this curve to be 1. Thus (21) for example has a generator of infinite order at $(x, y) = (3, 1)$ with multiples giving the points with

$$\pm(x, y) = (3, 1),\ (13, 14),\ (-290, 11) \ldots$$

These in turn lead to infinitely many arithmetic progressions of length 8. The three points listed above correspond to the following progressions (where we have "minimized" the coefficients A, B at (2) in the sense of replacing A, B by $A/p^4, B/p^6$ in cases where this is possible).

1. $(-12, 4)$, $(-8, 28)$, $(-4, 28)$, $(0, 20)$, $(4, 4)$, $(8, 4)$, $(12, 28)$, $(16, 52)$ on $y^2 = x^3 - 112x + 400$ (note that in minimal model form this is precisely the example cited in the introduction, of rank 3).
2. $x = -5460, -3640, -1820, 0, 1820, 3640, 5460, 7280$ on

   $$y^2 = x^3 - 23186800x + 128550931600$$

   (a curve of rank 6).
3. $x = -49929880, -37447410, -24964940, -12482470, 0, 12482470, 24964940, 37447410$ on

   $$y^2 = x^3 - 1090684401106300x + 80150513839787062897225$$

   (the eight points of the progression generate a subgroup of rank 6 in the full group of rational points).

For nine points in the arithmetic progression, it is necessary to satisfy (21), (22) simultaneously, and this corresponds to determining rational points on a curve of genus 5. There are only finitely many such points, and it seems plausible that they are given by $\pm(x, y) = (1, 0)$, $(0, 1)$, $(1, 1)$, $(2, 1)$ (each leading to degenerate progressions) but we are unable to verify this.

4. In order to investigate instances of 7 points in arithmetic progression, other than those corresponding to $w = x, z = 0$, substitute into (14), (15) the parametrizations at (13). There result two quartics in w with coefficients in the ring $\mathbb{Z}[x, y, z]$, both of which must be made square. The discriminants of the two quartics have a common factor of $6x^2 - 24xy + 21y^2 + 16xz - 24yz + 6z^2$, which can be made zero by the parametrization

$$\begin{aligned} x : y : z = {} & 9m^2 + 6mn - n^2 : \\ & 2(3m^2 + 4mn - n^2) : \\ & 3(m^2 + 2mn - n^2). \end{aligned} \tag{23}$$

Then (14) and (15) become

$$w^2 - w(36m^2 - 40mn - 52n^2) + (324m^4 - 720m^3n - 536m^2n^2 - 240mn^3 + 36n^4) = \square \tag{24}$$

and

$$w^2 + w(36m^2 + 40mn - 52n^2) + (324m^4 + 720m^3n - 536m^2n^2 + 240mn^3 + 36n^4) = \square, \tag{25}$$

which, regarded as the intersection of two quadrics with coefficients in $\mathbb{Q}(m/n)$, is a curve of genus 1 over $\mathbb{Q}(m/n)$. The point $w = 1/0$ ensures that this curve is an elliptic curve, and a Weierstrass cubic form is given by

$$Y^2 = X^3 + (81m^4 - 234m^2n^2 + 89n^4)X - 1600n^6(4m^2 - n^2). \tag{26}$$

This latter possesses the point of infinite order

$$P(X,Y) = (40n^3(2m+n),\ 40n^3(2m+n)(9m^2-13n^2)), \tag{27}$$

and it seems likely that the $\mathbb{Q}(m/n)$-rank of the curve is equal to 1, though this has not been verified. There are in any event infinitely many points w on (24), (25), given as the ratio of homogeneous polynomials in m, n. These together with (23) and (13) then give rise via (8), (9), and (11), (12), to an infinite family of elliptic curves with coefficients in $\mathbb{Q}(m/n)$ each possessing an arithmetic progression of length 7. For each of these curves, the condition that the length 7 progression extend to a length 8 progression, is given by the condition on the parameters m, n resulting from the demand that either (19) or (20) be satisfied. For example, the point P at (27) determines a point on (24), (25) given by

$$w = \frac{-n(261m^4 - 334m^2n^2 + 169n^4)}{m(9m^2 - 13n^2)},$$

pulling back to

$$\begin{aligned} a &= 432m^2(9m^2-13n^2) \\ &\quad (9m^6-93m^4n^2+107m^2n^4-39n^6), \\ d &= -96mn(m^2-n^2)(9m^2-13n^2) \\ &\quad (162m^4+243m^2n^2-169n^4), \end{aligned}$$

with

$$\begin{aligned} A = &-2304m^2(9m^2-13n^2)^2 \\ &\times(19683m^{14}+774198m^{12}n^2+2142531m^{10}n^4 \\ &\quad -8769546m^8n^6+8513577m^6n^8 \\ &\quad -2315894m^4n^{10}-587951m^2n^{12}+285610n^{14}), \\ B = &\,331776m^2(9m^2-13n^2)^2 \\ &\times(3188646m^{24}+183524292m^{22}n^2 \\ &\quad +2098837656m^{20}n^4-6763196898m^{18}n^6 \\ &\quad +4628564613m^{16}n^8-11781396216m^{14}n^{10} \\ &\quad +68063427684m^{12}n^{12}-146498139396m^{10}n^{14} \\ &\quad +163046846764m^8n^{16}-105881078940m^6n^{18} \\ &\quad +40866792460m^4n^{20}-8775138762m^2n^{22} \\ &\quad +815730721n^{24}). \end{aligned}$$

The condition for a progression of length 8 is now

$$\begin{aligned} &46656m^{10} + 73872m^9n - 385479m^8n^2 \\ &\quad + 168480m^7n^3 + 812052m^6n^4 - 993216m^5n^5 \\ &\quad - 572738m^4n^6 + 1079520m^3n^7 + 108836m^2n^8 \\ &\quad - 316368mn^9 + 28561n^{10} = \square, \end{aligned}$$

representing a curve of genus 4, with accordingly only finitely many points. Inspection finds points with $(m,n) = (1,1)$, $(1,-1)$, $(2,3)$, $(13,12)$, of which the latter two have corresponding value of d nonzero. The case $(m,n) = (2,3)$ leads to the 8-term progression $x = -12108$, -6888, -1668, 3552, 8772, 13992, 19212, 24432 on the curve

$$y^2 = x^3 - 400817592x + 2877285882276,$$

of rank 7; and the case $(m,n) = (13,12)$ leads to $x = -545293$, -236893, 71507, 379907, 688307, 996707, 1305107, 1613507 on the curve

$$y^2 = x^3 - 2635091663547x + 2069796143216734486,$$

of rank 8.

The condition for progressions of length 8 rapidly becomes awesome (and awful): from the point $2P$ at (27), the condition is represented by a homogeneous irreducible polynomial of degree 30 being a square (geometrically a curve of genus 14); inspection in this case gives a solution at $(m,n) = (2,-3)$ leading to (a,d) and (A,B) with

$$\begin{aligned} a &= 4405644857065620, \\ d &= 358812799145892, \\ A &= -55951394751916151836779771093432, \\ B &= 16118599057578631894952983390 6\backslash \\ &\qquad 199556559553368740 \end{aligned}$$

(the eight points of the progression generate a subgroup of rank 6 in the full group of rational points).

Remark. After substituting (13) into (14), (15) we may instead regard the result as two quartics in x with coefficients in $\mathbb{Z}[w,y,z]$, or indeed as quartics in y and z with coefficients in $\mathbb{Z}[w,x,z]$ and $\mathbb{Z}[w,x,y]$ respectively. The common factor of the two discriminants now turns out to be $3w^2-12wy-12y^2+8wz+48yz-32z^2$, $7w^2-8wx-8x^2-8wz+32xz-8z^2$, and $3w^2+8wx-32x^2-12wy+48xy-12y^2$, respectively. The first two cases lead as above to an intersection of two quadrics that by a local argument possesses no global point; and the third case determines the same curve as at (26) returning the same arithmetic progressions as before (but with $-d$ for d).

5. As a final problem, one can ask what is the longest possible arithmetic progression on curves of a given rank. In the case of rank 1, [Bremner et al. 1999] displays the curve $y^2 = x(x^2 - 36)$ with the progression of length 5 given by $x = -6,\ 0,\ 6,\ 12,\ 18$. Another example, on a curve with only trivial torsion, is given by the rank 1 curve

$$y^2 = x^3 + x^2 - 1920x + 36864$$

with $x = -48,\ -24,\ 0,\ 24,\ 48$ corresponding respectively to the points $4P$, $7P$, P, $2P$, $5P$, where $P = (0, 192)$ is a generator of the group of rational points.

Appendix. The search over the parameters w, x, y, z discovered a number of length 8 arithmetic progressions other than those derived from the family at (17) and (18). They are listed in the table below, ordered by increasing d, the progression being given by $x = a - 4d,\ \ldots,\ a + 3d$. The table also lists the rank of the corresponding curve (2) as computed by APECS.

REFERENCES

[Bremner et al. 1999] A. Bremner, J. H. Silverman, and N. Tzanakis, “Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$”, *J. Number Theory* **79** (1999).

[Buhler et al. 1985] J. P. Buhler, B. H. Gross, and D. B. Zagier, “On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3”, *Math. Comp.* **44**:170 (1985), 473–481.

[Connell n.d.] I. Connell, “APECS: Arithmetic of Plane Elliptic Curves”, See ftp.math.mcgill.ca/pub/apecs/. Requires *Maple*.

[Lee and Vélez 1992] J.-B. Lee and W. Y. Vélez, “Integral solutions in arithmetic progression for $y^2 = x^3 + k$”, *Period. Math. Hungar.* **25**:1 (1992), 31–49.

A	B	a	d	rank
−291697	99920065	77	182	5
−321067	144130726	467	280	4
−1312807	550181770	185	308	6
−874492	365535700	650	308	6
−1213387	2779479430	315	448	5
−33333627	74473186646	3547	840	4
−13012272	18130381200	588	1188	4
−17985400	65358276100	1060	1540	6
−63259000	179145612100	840	2380	6
−400817592	2877285882276	8772	5220	7
−1431376075	19985013718150	18115	11480	6
−3752020272	113113256785936	39512	24420	7
−11861312112	493395820640784	69408	41580	5
−39353712307	2594895639848590	152295	94432	8
−279530795907	56783465251651710	327855	199584	6

Andrew Bremner, Department of Mathematics, Arizona State University, Tempe AZ 85287-1804 (bremner@asu.edu)

Received December 7, 1998; accepted in revised form January 6, 1999