Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.3

A NOTE ON ARITHMETIC PROGRESSIONS ON ELLIPTIC CURVES

Garikai Campbell
Department of Mathematics and Statistics
Swarthmore College
Swarthmore, PA 19081
USA

Abstract. Andrew Bremner (*Experiment. Math.* **8** (1999), 409–413) has described a technique for producing infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. This note describes another way to produce infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. We illustrate how the technique articulated here gives an easy way to produce an elliptic curve containing a length 12 progression and an infinite family of elliptic curves containing a length 9 progression, with the caveat that these curves are not in Weierstrass form.

1. Introduction.

There are two (affine) models of elliptic curve that are very common. They are $y^2 = f(x)$ where $f(x)$ is either a cubic or a quartic. We will say that *points on a particular model of an elliptic curve are in arithmetic progression* if their x-coordinates form an arithmetic progression. For example, Buhler, Gross and Zagier [3] found that the points $(-3, 0)$, $(-2, 3)$, $(-1, 3)$, $(0, 2)$, $(1, 0)$, $(2, 0)$, $(3, 3)$, and $(4, 6)$ form an arithmetic progression of length 8 on the curve $y^2 + y = (x - 1)(x - 2)(x + 3)$. Moreover, Bremner [2] proves:

Theorem 1.1. *Each point on the elliptic curve*

$$C : y^2 = x^3 - x^2 - 36x + 36$$

corresponds to an elliptic curve in Weierstrass form containing at least 8 points in arithmetic progression.

Before proving this theorem, Bremner considers the following strategy. First he remarks that any monic degree 8 polynomial, $P(x)$, can be written as $Q(x)^2 - R(x)$ where the degree of $R(x)$ is less than or equal to 3. If $R(x)$ has degree precisely 3 and no repeated zeros, then $y^2 = R(x)$ is an elliptic curve and for each zero, α, of $P(x)$, this elliptic curve contains a pair of points with x-coordinate α. So one possible strategy for producing an elliptic curve with an arithmetic progression of length 8 might be to let $P(x) = x(x + 1)(x + 2) \cdots (x + 7)$ and compute the corresponding $R(x)$ so that $P(x) = Q(x)^2 - R(x)$. Unfortunately, in this case, $R(x)$ is linear and so this strategy fails for *any* degree 8 polynomial whose zeros form an arithmetic progression. The goal of this note is to illustrate how to turn this strategy into a successful one.

2. Arithmetic Progressions of Length 8

The statement that a degree 8 polynomial can be written as $Q(x)^2 - P(x)$ is a special case of the following:

Proposition 2.1. *If $P(x)$ is a monic polynomial of degree $2n$ defined over a field k, then there are unique polynomials $Q(x)$ and $R(x)$ defined over k such that*

(1) *$P(x) = Q(x)^2 - R(x)$ and*
(2) *the degree of $R(x)$ is strictly less than n.*

Since $R(x)$ is a square at every zero of $P(x)$, if $R(x)$ is a cubic or a quartic with no repeated zeros, then we can produce elliptic curves $y^2 = R(x)$ with great control over many of the x-coordinates.

Remark 2.2. We note that Mestre [9] was first to observe that this relatively simple proposition could be used to produce elliptic curves of large rank. Since Mestre's first paper exploiting this idea, many others ([4], [6], [7], [8], [11]) have used the proposition in clever ways to produce elliptic curves and infinite families of elliptic curves with the largest known rank (often with some condition on the torsion subgroup).

Now consider the polynomial

$$p_t(x) = (x-t)^2 \prod_{j=0}^{5} (x-j) \ \in \mathbb{Q}(t)[x].$$

In this case, we can write

$$p_t(x) = q_t(x)^2 - f_t(x),$$

where $f_t(x)$ is a polynomial of degree 3 in $\mathbb{Q}(t)[x]$ such that

(1) the discriminant of $f_t(x)$ is an irreducible polynomial in $\mathbb{Q}[t]$
(2) the coefficient of x^3 is $c(2t-5)$, where $c \in \mathbb{Q}$.

Therefore, we have that

Theorem 2.3. *The curve E_t defined by $y^2 = f_t(x)$ is an elliptic curve defined over $\mathbb{Q}(t)$, containing at least six points in arithmetic progression and for each $t_0 \in \mathbb{Q}$, $t_0 \neq 5/2$, the specialization of E_t at $t = t_0$ gives an elliptic curve defined over $\mathbb{Q}$ containing at least six points in arithmetic progression.*

We next observe that $f_t(6)$ is a conic in $\mathbb{Q}[t]$ which is a rational square when $t = 6$. Therefore, we can parameterize all rational solutions to $y^2 = f_t(6)$ by letting

$$t \;=\; \frac{6m^2 - 126m - 285360}{m^2 - 72256}. \tag{2.1}$$

Since no rational value of m gives $t = 5/2$, we have:

Corrolary 2.4. *Let $g_m(x)$ be the polynomial $f_t(x)$ with t given by (2.1). The curve E_m defined by $y^2 = g_m(x)$ is an elliptic curve defined over $\mathbb{Q}(m)$ containing at least seven points in arithmetic progression and for each $m_0 \in \mathbb{Q}$, the specialization of E_m at $m = m_0$ gives an elliptic curve defined over $\mathbb{Q}$ containing at least seven points in arithmetic progression.*

If we continue in this vein and explore the conditions imposed by $y^2 = g_m(7)$, we find the following.

Theorem 2.5. *Let D be the elliptic curve defined by*

$$\begin{aligned} D : y^2 = -264815m^4 - 19343520m^3 + 62846856064m^2 \\ -2906312951808m - 495507443511296. \end{aligned}$$

Let

$$\begin{aligned} g_3 &= -18816m^4 + 677376m^3 + 1922543616m^2 \\ &\quad -48944480256m - 40678301368320, \\ g_2 &= 236896m^4 - 9821952m^3 - 22598349824m^2 \\ &\quad +508953231360m + 520252184657920, \\ g_1 &= -958800m^4 + 40985280m^3 + 89932669440m^2 \\ &\quad -1957723729920m - 2113363439616000, \quad \textit{and} \\ g_0 &= 1292769m^4 - 57304800m^3 - 118795148928m^2 \\ &\quad +2647001548800m + 2758336954896384. \end{aligned}$$

Then

$$E'_m : y^2 = g_3 \ x^3 + g_2 \ x^2 + g_1 \ x + g_0,$$

is an elliptic curve defined over $\mathbb{Q}(D)$ containing the 8 points in arithmetic progression with x-coordinates 0, 1, 2, ... , 7.

Proof. E'_m is isomorphic to E_m via the change of variables $y \mapsto y/(m^2 - 72256)$. Substituting $x = 7$ into E'_m, we get the curve D. □

Moreover, if we let $D(\mathbb{Q})$ be the group of rational points on D, then we have that $D(\mathbb{Q})$ is infinite. More specifically, we have:

Proposition 2.6. *D has rank 2 and torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.*

Proof. A short computer search reveals that $O = (-88, 15628032)$ is a point in $D(\mathbb{Q})$. Taking O taken to be the identity, $D(\mathbb{Q})$ is generated by

$$\begin{aligned} P_0 &= (10984/79, -80015523840/6241) \text{ and} \\ P_1 &= (-1363640/2531, 31969540657152/6405961), \end{aligned}$$

and contains the point of order two:

$$P_2 = (10984/79, 80015523840/6241).$$

□

(The calculations above were performed with the help of `mwrank` [5] and GP [1].)

An immediate consequence of the proposition above is the following:

Corrolary 2.7. *Each point on the elliptic curve D corresponds to an elliptic curve in Weierstrass form containing at least 8 points in arithmetic progression.*

Remark 2.8. This condition is very similar to the condition found in Bremner's construction–namely, that points on the curve C give rise to elliptic curves with 8 points in arithmetic progression. The differences are that C has rank 1 and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, while D has rank 2 and torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.

3. Longer Progressions

This construction can also be used to produce progressions of length greater than 8 on elliptic curves of the form $y^2 = f(x)$ where $f(x)$ is a quartic. More specifically, we have:

Theorem 3.1. *There exists an elliptic curve in the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 12 points in arithmetic progression.*

Proof. Let

$$g_0(x) = \prod_{j=0}^{11}(x - j).$$

Then $g_0(x) = u_0(x)^2 - (81/4) \cdot v_0(x)$, with

$$\begin{aligned} u_0(x) &= x^6 - 33x^5 + 418x^4 - 2541x^3 + (14993/2)x^2 \\ &\quad -(18513/2)x + (4851/2), \text{ and} \\ v_0(x) &= 429x^4 - 9438x^3 + 74295x^2 - 246246x + 290521. \end{aligned}$$

Since the discriminant of $v_0(x)$ is nonzero, the curve $E : y^2 = v_0(x)$ is an elliptic curve. This elliptic curve then contains a length 12 arithmetic progression. □

(Note that by using `mwrank`, we computed the rank of this curve to be 4 with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.)

The construction above produces a single curve and it is unclear how to produce an infinite family of curves containing a length 12 progression using this idea. The problem is that, in general, if the $P(x)$ of proposition 2.1 is taken to have degree 12, then the $R(x)$ is only guaranteed to have degree less than or equal to 5, not 4. Therefore, the curve $y^2 = R(x)$ need not be an elliptic curve. We can, however, prove the following.

Theorem 3.2. *There are infinitely many elliptic curves of the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 9 points in arithmetic progression.*

Proof. Let

$$g(x) = (x - a) \cdot \prod_{j=0}^{8}(x - j),$$

and write $g(x)$ as $u(x)^2 - v(x)$. $v(x)$ is a degree four polynomial in $\mathbb{Q}(a)[x]$ with discriminant zero only for $a \in \{0, 4, 8\}$. □

The work here (and that of Bremner) leaves open the following questions:

Open Question 3.3. *Is there an elliptic curve of the form $y^2 = f(x), f(x)$ a cubic, containing a length 9 arithmetic progression? Are there infinitely many?*

Open Question 3.4. *Is there an elliptic curve of the form $y^2 = f(x), f(x)$ a quartic, containing a length 13 arithmetic progression? Are there infinitely many curves in this form containing a length 10 progression?*

And finally,

Open Question 3.5. *What is the longest arithmetic progression one can find on an elliptic curve in the form $y^2 = f(x)$, where $f(x)$ is a cubic? a quartic?*

4. Acknowledgments

This work was completed with the support of the Lindback Foundation Minority Junior Faculty Grant.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. The Pari system. `ftp://megrez.math.u-bordeaux.fr/pub/pari/`, 2000.
[2] Andrew Bremner. On arithmetic progressions on elliptic curves. *Experiment. Math.*, **8** (1999), 409 – 413.
[3] 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** (1985), 473 – 481.
[4] Garikai Campbell. *Finding elliptic curves and infinite families of elliptic curves defined over Q of large rank.* PhD thesis, Rutgers University, June 1999. Available at `http://math.swarthmore.edu/kai/thesis.html`.
[5] John Cremona. Home page. `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/`.
[6] Stefane Férmigier. Un exemple de courbe elliptique définie sur Q de rang ≥ 19. *C. R. Acad. Sci. Paris Sér. I*, **315** (1992), 719 – 722.
[7] Shoichi Kihara. On an infinite family of elliptic curves with rank ≥ 14 over Q. *Proc. Japan Acad. Ser. A.*, **73** (1997) 32.
[8] L. Kulesz. *Arithmétique des courbes algébriques de genre au moins deux.* PhD thesis, Université Paris 7, 1998.
[9] Jean-François Mestre. Construction d'une courbe elliptique de rang ≥ 12. *C. R. Acad. Sci. Paris Sér. I*, **295** (1982), 643 – 644.
[10] Jean-François Mestre. Courbes elliptiques de rang ≥ 11 sur $Q(t)$. *C. R. Acad. Sci. Paris Sér. I*, **313** (1991), 139 – 142.
[11] Koh-Ichi Nagao. Examples of elliptic curves over Q with rank ≥ 17. *Proc. Japan Acad. Ser. A.*, **68** (1997), 287 – 289.

2000 *Mathematics Subject Classification*: 11G05, 11B25 .
Keywords: elliptic curves, arithmetic progression

Received February 5, 2003; revised version received February 7, 2003. Published in *Journal of Integer Sequences* February 25, 2003.

Return to Journal of Integer Sequences home page.