Annales Mathematicae et Informaticae
37 (2010) pp. 3–6
http://ami.ektf.hu

Arithmetic progressions on quartic elliptic curves

Alejandra Alvarado

University of Arizona

Submitted 19 October 2009; Accepted 20 March 2010

Abstract

Consider the curve $C : y^2 = ax^4 + bx^2 + c$. MacLeod previously found four curves of the given form, with an arithmetic progression in the x coordinates, of length 14. By similar methods, we also find the same four curves, and several more.

Keywords: Diophantine equations, arithmetic progressions.

1. Introduction

Let $F(x)$ be a quartic polynomial over the rationals, which is not the square of a quadratic. If a rational point exists on $y^2 = F(x)$, then this curve is birationally equivalent to an elliptic curve. We will call these curves *quartic elliptic curves* [4].

We will say that points on a curve are in *arithmetic progression* (AP) if their x coordinates form an arithmetic progression. Previously, Ulas found an infinite family of curves with an AP of length 12 [4]. The author first found a curve

$$C_a : y^2 = f_a(x),$$

where f_a is degree four and parameter a, with length ten AP. The AP in x is $\{1, 2, \ldots, 10\}$. Ulas then noted that $f_a(0) = f_a(11)$. The quartic curve $Y^2 = f_a(0)$ is birationally equivalent to an elliptic curve of rank three. Thus, points on this rank three elliptic curve map to points on $Y^2 = f_a(0)$ which give infinitely many values for a.

By the use of symmetry and methods similar to those found in Ulas, MacLeod [2] found an infinite family of curves with AP length ten. Numerical investigations lead to four examples with AP length 14. In this paper, we follow similar methods as Ulas and MacLeod. We find the same four curves, plus eleven more.

2. Arithmetic progressions

Macleod simplifies Ulas' approach when searching for points in AP. Because the general solution to length ten AP is difficult, Ulas instead considers a curve with symmetry. As noted in MacLeod, it is enough to consider the curve to be symmetric about the x-axis. In that case, we can write the curve as $y^2 = ax^4 + bx^2 + c$, i.e., $F(x) = ax^4 + bx^2 + c$ with rational coefficients. In this section, we construct curves with length 14 AP. From these, we will attempt to find examples of length 16.

Suppose

$$\begin{aligned} F(\pm 1) &= p^2 \\ F(\pm 3) &= q^2 \\ F(\pm 5) &= r^2 \\ F(\pm 7) &= s^2 \end{aligned}$$

This gives us an AP of length eight. The first three equations imply

$$\begin{aligned} a &= \frac{2p^2 - 3q^2 + r^2}{384} \\ b &= -\frac{34p^2 - 39q^2 + 5r^2}{192} \\ c &= \frac{150p^2 - 25q^2 + 3r^2}{128} \end{aligned}$$

which forces $s^2 = 5p^2 - 9q^2 + 5r^2$. This last equation, representing a quadric surface, has a parametrization in u and v:

$$\begin{aligned} (p : q : r : s) = (&-u^2 - 2uv - 5v^2 - 2uw + w^2 : \\ &u^2 - 5v^2 + w^2 : \\ &u^2 - 5v^2 - 2uw - 2vw - w^2 : \\ &u^2 + 10uv + 5v^2 + 10vw + w^2) \end{aligned}$$

Then $F(x) = ax^4 + bx^2 + c$ is a polynomial in x with coefficients in (u, v, w). Thus far, we have an infinite family of curves with an arithmetic progression of length eight in the x-coordinates. Up to this point, we have followed similar techniques as MacLeod, except that our parametrization has smaller coefficients. We now introduce a different approach to this problem. If we want an AP of length at least 14, then we must force

$$\begin{aligned} F(\pm 9) &= t_1^2 \\ F(\pm 11) &= t_2^2 \\ F(\pm 13) &= t_3^2 \end{aligned}$$

Consider the family of planes $w = Au + Bv$ in the (u, v, w) space. These last three homogeneous equations are now quartics in (u, v) with coefficients in (A, B). With respect to u, these curves are singular if and only if their discriminant is zero. With the help of Magma [1], we find that $(2A+1-B)^2(A+B+2)^2$ is a factor of the discriminant of all three. After substituting $B = 2A+1$, we find $(u+2v)^2$ is a factor of all three equations. If we substitute $B = -A-2$, then $(u-v)^2$ is a factor of the three equations.

Let us first consider the case $B = -A-2$. If $v = 1$, then

$$\begin{aligned}F(\pm 9) &= (u-1)^2(u^2 + A^4u^2 + 24Au^2 + 2A^2u^2 - 24A^3u^2 + 124Au + 38u - 2A^4u \\ &\quad + 180uA^2 + 76A^3u + 361 + 14A^2 + A^4 - 52A^3 + 412A) \\ F(\pm 11) &= (u-1)^2(841 - 2A^4u + 560uA^2 + 216A^3u + 384Au + 972A + 58u \\ &\quad + A^4u^2 + 14A^2 + A^4 - 132A^3 - 84A^3u^2 + u^2 + 84Au^2 + 2A^2u^2) \\ F(\pm 13) &= (u-1)^2(1681 - 2A^4u + 1280uA^2 + 472A^3u + 872Au + 1952A + 82u \\ &\quad + A^4u^2 + 14A^2 + A^4 - 272A^3 - 200A^3u^2 + u^2 + 200Au^2 + 2A^2u^2)\end{aligned}$$

Write the rational value $A = a_1/a_2$, and consider the degree six polynomial

$$f(u) = \frac{F(9)F(11)F(13)}{(u-1)^6}$$

with coefficients in (a_1, a_2). Then the equation $Y^2 = f(u)$ represents a hyperelliptic curve of degree six. The reason for considering the above curves with discriminant zero, is because it is much more practical to search for points on a hyperelliptic curve of degree six rather than twelve. With the aid of Magma, we found points on this curve by varying values of (a_1, a_2) up to $|a_1| + |a_2| = 200$. We then checked whether $F(\pm 9), F(\pm 11)$, and $F(\pm 13)$ are squares but F is not a perfect square. We found the same four curves listed in MacLeod:

1. $y^2 = -17x^4 + 3130x^2 + 8551$
2. $y^2 = 2002x^4 - 226820x^2 + 18168514$
3. $y^2 = 3026x^4 - 222836x^2 + 3709234$
4. $y^2 = 34255x^4 - 1436006x^2 + 447963175$

and seven new curves:

1. $y^2 = 2753x^4 - 728770x^2 + 59217921$
2. $y^2 = 627x^4 - 87870x^2 + 3312859$
3. $y^2 = 3689x^4 - 88994x^2 + 4312441$
4. $y^2 = -143644199x^4 + 26117509014x^2 - 24973534431$
5. $y^2 = -15015x^4 + 2758974x^2 + 25050025$

6. $y^2 = 506363x^4 - 1726486x^2 + 740805923$

7. $y^2 = -2219x^4 + 378494x^2 + 19089469$

If we now look at the case $B = 2A + 1$, we find at least four more distinct curves:

1. $y^2 = 1012726x^4 - 3452972x^2 + 1481611846$

2. $y^2 = -308503x^4 + 53324830x^2 + 72961849$

3. $y^2 = -31730x^4 + 4968916x^2 + 68267950$

4. $y^2 = -18750709x^4 + 5055585994x^2 + 16925811919$

We end this paper with some final comments. First, none of these curves contain a length 16 AP with x-coordinates $\{-13, -11, ..., 13\}$. Secondly, the reason we used Magma was because it effectively found rational points on hyperelliptic curves. Although, Michael Stoll's ratpoint package is now supported by Sage [3]. Ratpoints finds rational points of bounded height on hyperelliptic curves.

Acknowledgements. Thank you to Dr. Andrew Bremner for suggesting this problem, Dong-Quan Nguyen, and Robert Miller.

References

[1] Bosma, W., Cannon, J., Playoust, C., The Magma algebra system. I. The user language., *J. Symbolic Comput.*, 24 (1997) 235–265.

[2] MacLeod, A.J., 14-term arithmetic progressions on quartic elliptic curves, *J. Integer Seq.*, 9 (2006) 1, Article 06.1.2, 4 pp. (electronic).

[3] Stein, W.A. et al., *Sage Mathematics Software (Version 4.2.1)*, The Sage Development Team, 2009, `http://www.sagemath.org`.

[4] Ulas, M., A note on arithmetic progressions on quartic elliptic curves, *J. Integer Seq.*, 8 (2005) 3, Article 05.3.1, 5 pp. (electronic).

Alejandra Alvarado
617 N. Santa Rita Ave. Tucson, AZ 85721
e-mail: `alvarado@math.arizona.edu`