Journal of Integer Sequences, Vol. 12 (2009),
Article 09.7.3

An Arithmetic Progression on Quintic Curves

Alejandra Alvarado
Department of Mathematics
University of Arizona
617 N. Santa Rita Ave.
Tucson, AZ 85721
USA
alvarado@math.arizona.edu

Abstract

Consider a degree five curve of the form $y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$. Ulas previously showed the existence of an infinite family of curves C which contain an arithmetic progression (AP) of length 11. The author also found an example of said curve which contains 12 points in AP. In this paper, we construct an infinite family of curves with an AP of length 12.

1 Introduction

An *arithmetic progression* (AP) is a sequence of numbers such that the difference between any two consecutive numbers is constant. When we talk about an AP on a curve $y^2 = f(x)$, we mean an AP in the x-coordinates.

The study of solutions to diophantine equations has been around throughout history. But it was not until the twentieth century that remarkable theories and results flourished. The problem of finding consecutive integer solutions to a diophantine equation can be traced back to Mohanty [5]. On the curve $y^2 = x^3 + k$, Mohanty investigated integral AP's in the x and y-coordinates.

Let f be an irreducible degree five polynomial over the rationals. Consider the hyperelliptic curve $y^2 = f(x)$. Previously, Ulas [7] had found an infinite family of curves with length 11 AP. By computer search, he found one example with length 12. We will show the existence of an infinite family of curves which contain an AP of length 12. In order to construct an infinite family of curves, we make use of Mestre's Theorem [4]:

Theorem 1.1. *Let $P(x)$ be a monic polynomial of degree $2n$ defined over a field K. Then there exist unique polynomials $Q(x)$ and $R(x)$ defined over K such that*

1. $P(x) = Q(x)^2 - R(x)$

2. the degree of $R(x)$ *is strictly less than* n.

In this paper, we use the above theorem to construct an infinite family of curves.

2 Arithmetic Progressions of Length 12

In this section, we will prove the following theorem, whose proof uses similar techniques as Campbell [3].

Theorem 2.1. *There exists an infinite family of curves of the form* $y^2 = f(x)$ *which contain an arithmetic progression of length 12, where* f *is a degree five polynomial. The curves are defined over the rationals.*

Proof. Consider the following polynomial in $\mathbb{Q}(u)[x]$.

$$g(u,x) = (x-u)^2 \prod_{1 \leq i \leq 5} (x^2 - i^2)$$

We choose this form of polynomial to maximize the use of symmetry. Note that g vanishes identically at $x = \pm 1, \ldots, \pm 5$. By Mestre's theorem, there exist unique polynomials $h, f \in \mathbb{Q}(u)[x]$ of degree 6 and 5, respectively such that

$$f(u,x) = h(u,x)^2 - g(u,x).$$

We will write

$$h(u,x) = x^6 + h_5 x^5 + h_4 x^4 + h_3 x^3 + h_2 x^2 + h_1 x + h_0.$$

Since f is of degree 5, we easily find the coefficients h_i.

$$\begin{aligned}
f(u,x) &= h(u,x)^2 - g(u,x) \\
&= 2(h_5 + u)x^{11} + (h_5^2 + 2h_4 - u^2 + 55)x^{10} + 2(h_5 h_4 + h_3 - 55u)x^9 \\
&\quad + (2h_3 h_5 + h_4^2 + 2h_2 + 55u^2 - 1023)x^8 + 2(h_2 h_5 + h_3 h_4 + h_1 + 1023u)x^7 \\
&\quad + (h_3^2 + +2h_1 h_5 + 2h_2 h_4 + 2h_0 - 1023u^2 + 7645)x^6 + 2(h_0 h_5 + h_1 h_4 \\
&\quad + h_2 h_3 - 7645u)x^5 + (2h_0 h_4 + 2h_1 h_3 + h_2^2 + 7645u^2 - 21076)x^4 \\
&\quad + (h_0 h_3 + h_1 h_2 + 21076u)x^3 + (2h_0 h_2 + h_1^2 - 21076u^2 + 14400)x^2 \\
&\quad + 2(h_0 h_1 - 14400u)x + (h_0^2 + 14400u^2)
\end{aligned}$$

where

$$\begin{aligned}
h_5 &= -u & h_4 &= \frac{-55}{2} \\
h_3 &= \frac{55}{2}u & h_2 &= \frac{1067}{8} \\
h_1 &= \frac{-1067}{8}u & h_0 &= \frac{-2475}{16}
\end{aligned}$$

We can then write f as

$$f(u,x) = \frac{-2475}{8}ux^5 + \left(\frac{2475}{8}u^2 + \frac{334125}{64}\right)x^4 - \frac{61875}{32}ux^3 + \left(\frac{-210375}{64}u^2 - \frac{1719225}{64}\right)x^2 + \frac{797625}{64}ux + \left(14400u^2 + \frac{6125625}{256}\right)$$

By construction, $f(u,x) = h(u,x)^2$ for $x = \pm 1, \ldots, \pm 5$. We now add the constraint that f also be square at $x = 0$, so then we have an arithmetic progression of length at least 11 on the curve $C : p^2 = f(u,x)$. We want $f(u,0) = p^2$. In other words,

$$(120u)^2 + (\frac{2475}{16})^2 = p^2.$$

Without loss of generality, multiply through by $(\frac{16}{2475})^2$, then replace $\frac{16}{2475}p$ with p_1. Rewrite as

$$(\frac{128}{165}u)^2 + 1 = p_1^2.$$

We have a parametrization

$$\frac{128}{165}u = \frac{2t}{t^2-1} \qquad\qquad p_1 = \frac{t^2+1}{t^2-1}$$

Thus, $u = u(t) = \frac{165t}{64(t^2-1)}$. Substituting back for u in $f(u,x)$, and removing any squares, we obtain the curve

$$\begin{aligned} P^2 = {} & (-929280t^3 + 929280t)x^5 \\ & + (6082560t^4 - 9769320t^2 + 6082560)x^4 \\ & + (-5808000t^3 + 5808000t)x^3 \\ & + (-31297536t^4 + 37139697t^2 - 31297536)x^2 \\ & + (37435200t^3 - 37435200t)x \\ & + (27878400t^4 + 55756800t^2 + 27878400) \end{aligned}$$

where $P = \frac{2^{18}(t-1)^2(t+1)^2}{15^2}p$. The above curve has an arithmetic progression of length at least 11, for $t \in \mathbb{Q}$ except $t \neq \pm 1$. The arithmetic progression of the x coordinates is $\{-5, -4, \ldots, 4, 5\}$. To find an arithmetic progression of length at least 12 on C, we need to determine whether $x = 6$ or $x = -6$ gives us a point on the curve. At $x = -6$ we have

$$\left(\frac{P}{6}\right)^2 = 188449024t^4 + 229333280t^3 - 313007023t^2 - 229333280t + 188449024 \tag{2.1}$$

We find that $t = \frac{5}{6}$ gives $p = \frac{34001}{6}$. Note that because of symmetry, $t = -\frac{6}{5}$ also gives a point on the curve. Now we have at least one curve with an arithmetic progression of length at least 12. In particular, at $t = \frac{5}{6}$, the curve

$$y^2 = 70400x^5 + 663960x^4 + 440000x^3 - 6128751x^2 - 2836000x + 23814400$$

contains the x arithmetic progression $\{-6,-5,-4,\ldots,4,5\}$

Returning to the quartic curve (2.1), since a rational point exists, the curve is birationally equivalent to an elliptic curve. The quartic curve is commonly called a *quartic elliptic curve* [7]. With the aid of MAGMA [1], we found the minimal model of the quartic elliptic curve. The output is the elliptic curve, E,

$$\begin{aligned} Y^2+XY+Y=X^3&+X^2\\ &-14206480669846430X\\ &+651651670263534709965275. \end{aligned}$$

We thus have the maps to and from the quartic and cubic curve. If this curve has rank at least one, and if we can find at least one point on the curve of infinite order, then C will have an arithmetic progression of length at least 12, namely,

$$x=-6,-5,-4,\ldots,5.$$

The following commands were entered into SAGE [6], to determine the rank of this curve and find its generators.

```
E=mwrank_EllipticCurve([1,1,1,
                    -14206480669846430,651651670263534709965275])
E.rank() E.gens()
```

SAGE found the rank of F to be three, and its (possible) generators were found to be

$$[-118512027,-818950617977,1]$$

$$[578945454,404307680999,8]$$

$$[68136369,-1117555865,1]$$

So this constructs a three parameter family of degree five curves, containing an arithmetic progression of length 12. The equation of the family of curves is,

$$\begin{aligned} y^2=&-929280(t^3-t)x^5+3960(1536t^4-2467t^2+1536)x^4\\ &-5808000(t^3-t)x^3-9(3477504t^4-4126633t^2+3477504)x^2\\ &+37435200(t^3-t)x+27878400(t^4+2t^2+1) \end{aligned} \tag{2.2}$$

with x-AP,

$$\begin{gathered} \{(-6,6\sqrt{188449024t^4+229333280t^3-313007023t^2-229333280t+188449024}),\\ (-5,15(3680t^2+2079t-3680)),(-4,12(2744t^2+1485t-2744)),(-3,3(5152t^2+2915t-5152)),\\ (-2,6(16t^2+1155t-16)),(-1,3(544t^2-3135t-544)),(0,5280(t^2+1)),\\ (1,3(544t^2+3135t-544)),(2,6(16t^2-1155t-16)),(3,3(5152t^2-2915t-5152)),\\ (4,12(2744t^2-1485t-2744)),(5,(3680t^2-2079t-3680))\}. \end{gathered}$$

Since we have a map from C to E, we can express t in terms of the points on E,

$$t=\frac{27124113X+1405Y-1429181772291724}{2(18185324X+843Y-1413723166396761)}.$$

$\square$

3 An Arithmetic Progression of Length 13

It is natural to state the following question:

Open Question 3.1. *Can we find a quintic curve containing a length 13 arithmetic progression?*

By computer search, we attempted to find an example of length 13 AP on the curve (2.2). By modifying the polynomial $g(u,x)$, found at the beginning of section two, we attempted to construct an example of length 13. Thus far, by ranging the degree of g from 12 to 14, we have not found an example.

4 Acknowledgment

I would like to thank anonymous referee for his/her valuable comments, and A. Bremner for guiding me towards this problem.

References

[1] W. Bosma, J. Cannon, and C. Playoust, MAGMA `2.14-1`, available from http://magma.maths.usyd.edu.au/.

[2] A. Bremner, On arithmetic progressions on elliptic curves, *Experiment. Math.* **8** (1999), 409–413.

[3] G. Campbell, A note on arithmetic progressions on elliptic curves, *J. Integer Sequences* **6** (2003), Paper 03.1.3.

[4] J. Mestre, Construction d'une courbe elliptique de rang ≥ 12, *C. R. Acad. Sci. Paris Sér. I Math.* **295** (1982), 643–644.

[5] S. Mohanty, On consecutive integer solutions for $y^2 - k = x^3$, *Proc. Amer. Math. Soc.* **48** (1975), 281–285.

[6] W. Stein, SAGE: Software for Algebra and Geometry Experimentation. available from http://www.sagemath.org

[7] M. Ulas, On arithmetic progressions on genus two curves, *Rocky Mountain J. Math.* **39** (2009), 971–980.

2000 *Mathematics Subject Classification*: 11G05, 11B25, 14H45.
Keywords: arithmetic progression, elliptic curves, quartic curves.

Received August 16 2009; revised version received October 19 2009. Published in *Journal of Integer Sequences*, October 21 2009.

Return to Journal of Integer Sequences home page.