Journal of Integer Sequences, Vol. 8 (2005),
Article 05.3.1

A Note on Arithmetic Progressions on Quartic Elliptic Curves

Maciej Ulas
Jagiellonian University
Institute of Mathematics
Reymonta 4
30-059 Kraków
Poland
Maciej.Ulas@im.uj.edu.pl

Abstract

G. Campbell described a technique for producing infinite families of quartic elliptic curves containing a length-9 arithmetic progression. He also gave an example of a quartic elliptic curve containing a length-12 arithmetic progression. In this note we give a construction of an infinite family of quartics on which there is an arithmetic progression of length 10. Then we show that there exists an infinite family of quartics containing a sequence of length 12.

1 Introduction

Let us consider a curve $E: \ y^2 = f(x)$, where $f \in \mathbb{Q}[x]$ and f is not a square of a polynomial. We say that points $P_i = (x_i,\ y_i),\ i = 1, \ldots,\ k$ on the curve E form an *arithmetic progression of length* k if the sequence $x_1,\ x_2,\ \ldots,\ x_k$ form an arithmetic progression.

G. Campbell [2] proved the following theorems:

Theorem 1.1. *There are infinitely many elliptic curves of the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 9 points in arithmetic progression.*

Theorem 1.2. *There exists an elliptic curve in the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 12 points in arithmetic progression.*

In this paper we propose two different ways to obtain an infinite family of quartic elliptic curves with a sequence of length 10. Then we present a family of quartics (parametrized by the rational points on an elliptic curve with a non zero rank) with an arithmetic progression of length 12.

2 Arithmetic Progressions of Length 10

The proof of the first theorem is similar to the one given by G. Campbell [2].

Theorem 2.1. *There are infinitely many quartic elliptic curves $y^2 = f(x)$ containing 10 points in arithmetic progression.*

Proof. Let us consider the following polynomial

$$P_t(x) = (x^2 - 9x - 4t)\prod_{i=0}^{9}(x-i) \in \mathbb{Q}(t)[x]. \tag{2.1}$$

Then, we have

$$P_t(x) = Q_t(x)^2 - F_t(x),$$

where Q_t is the unique monic polynomial defined over $\mathbb{Q}(t)$ such that F_t has degree 4.

The discriminant of the polynomial $F_t(x)$ is non zero for $t \in \mathbb{Q} \setminus S$, where

$$S = \{\pm 1, \pm 2, \pm 4, -5, -6, -8, -11\}.$$

Hence, for such parameters t, the quartic elliptic curve

$$E_t : \; y^2 = F_t(x) \tag{2.2}$$

contain the points $P_i = (i, \; Q_t(i))$ for $i = 0, \ldots, \; 9$ which form an arithmetic progression of length 10 on the curve E_t. □

3 The sequence of length 12

There doesn't seem to be a way to construct an infinite family of quartics with an arithmetic progression of length 12 from family of curves (2.2). In this section we shall construct another family which will be better for our purposes. First let us consider the polynomial $f \in \mathbb{Q}[p, \; q, \; r, \; s, \; t][x]$

$$f(x) = \sum_{i=0}^{4} a_i x^i,$$

where

$$\begin{aligned}
a_0 &= 5p^2 - 10q^2 + 10r^2 - 5s^2 + t^2, \\
a_1 &= \frac{1}{12}(-77p^2 + 214q^2 - 234r^2 + 122s^2 - 25t^2), \\
a_2 &= \frac{1}{24}(71p^2 - 236q^2 + 294r^2 - 164s^2 + 35t^2), \\
a_3 &= \frac{1}{12}(-7p^2 + 26q^2 - 36r^2 + 22s^2 - 5t^2), \\
a_4 &= \frac{1}{24}(p^2 - 4q^2 + 6r^2 - 4s^2 + t^2).
\end{aligned}$$

We have

$$f(1) = p^2, \quad f(2) = q^2, \quad f(3) = r^2, \quad f(4) = s^2, \quad f(5) = t^2,$$

so we see that

$$E: \quad y^2 = f(x)$$

is a five parameter family of quartics containing an arithmetic progression of length 5. In order to obtain a family with a sequence of length 10 we have to consider the following system of equations

$$\begin{cases} f(6) = p^2 - 5q^2 + 10r^2 - 10s^2 + 5t^2 = P^2, \\ f(7) = 5p^2 - 24q^2 + 45r^2 - 40s^2 + 15t^2 = Q^2, \\ f(8) = 15p^2 - 70q^2 + 126r^2 - 105s^2 + 35t^2 = R^2, \\ f(9) = 35p^2 - 160q^2 + 280r^2 - 224s^2 + 70t^2 = S^2, \\ f(10) = 70p^2 - 315q^2 + 540r^2 - 420s^2 + 126t^2 = T^2, \end{cases} \tag{3.1}$$

in integers $p, q, r, s, t, P, Q, R, S, T$. Since the general solution is hard to obtain we will look for particular solutions with $P = t,\ Q = s,\ R = r,\ S = q,\ T = p$. Then, in this case it is easy to realize that (3.1) is equivalent to

$$\begin{cases} p^2 = 15r^2 - 35s^2 + 21t^2, \\ q^2 = 5r^2 - 9s^2 + 5t^2. \end{cases} \tag{3.2}$$

Making a substitution $(p,\ r,\ s,\ t) = (p,\ a+p,\ b+p,\ c+p)$ we get a parametrized solution of the first equation in (3.2)

$$\begin{cases} p = 15a^2 - 35b^2 + 21c^2, \\ r = -15a^2 + 70ab - 35b^2 - 42ac + 21c^2, \\ s = 15a^2 - 30ab + 35b^2 - 42bc + 21c^2, \\ t = 15a^2 - 35b^2 - 30ac + 70bc - 21c^2. \end{cases} \tag{3.3}$$

Now inserting $r,\ s,\ t$ from (3.3) to the second equation in (3.2), we obtain

$$\begin{aligned} q^2 = {} & 441c^4 - 168(15a - 7b)c^3 + 2(675a^2 + 2520ab - 2303b^2)c^2 \\ & + 40(45a^3 - 189a^2b + 63ab^2 + 49b^3)c \\ & + 25(9a^4 - 96a^3b + 278a^2b^2 - 224ab^3 + 49b^4). \end{aligned} \tag{3.4}$$

Moreover, if we take $b = 3(a+1),\ c = 2(a+1)$, we get that $q = 3(56a^2 + 142a + 91)$. Finally we have

$$\begin{cases} p = T = -3(72a^2 + 154a + 77), \\ q = S = 3(56a^2 + 142a + 91), \\ r = R = -3(40a^2 + 112a + 77), \\ s = Q = 3(24a^2 + 68a + 49), \\ t = P = -3(8a^2 + 6a - 7), \end{cases} \tag{3.5}$$

which is a solution of (3.1). Specializing the polynomial f as given by (3.5) we obtain

$$f_a(x) = \sum_{i=0}^{4} a_i x^i,$$

where

$$\begin{aligned}
a_0 &= 9(7744a^4 + 25216a^3 + 22544a^2 - 784a - 5831),\\
a_1 &= -66(a+1)(16a+21)(24a^2 - 52a - 119),\\
a_2 &= 3(a+1)(16a+21)(48a^2 - 709a - 1085),\\
a_3 &= 66(a+1)(5a+7)(16a+21),\\
a_4 &= -3(a+1)(5a+7)(16a+21),
\end{aligned}$$

and the discriminant R_a of the polynomial f_a is

$$\begin{aligned}
R_a = &-419904(a+1)^4(2a+3)^2(4a+5)^2(2a+7)^2(4a+7)^2(5a+7)^3\\
&\times (6a+7)^2(12a+17)^2(16a+21)^4(1008a^2 + 1831a + 623).
\end{aligned}$$

Then for $a \in \mathbb{Q} \setminus W$, where

$$W := \{-1, -3/2, -5/4, -7/2, -7/4, -7/5, -7/6, -17/12, -21/16\},$$

we get a nontrivial quartic elliptic curve

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

containing an arithmetic progression of length 10.

Now we are ready to prove the following:

Theorem 3.1. *There are infinitely many quartic elliptic curves $y^2 = f(x)$ containing 12 points in arithmetic progression.*

Proof. The curve C_a defined above contains the 10 points with $x = 1, \ldots, 10$. Observe that

$$f_a(0) = f_a(11) = 9(7744a^4 + 25216a^3 + 22544a^2 - 784a - 5831).$$

Now, consider the curve:

$$E : \ Y^2 = 9(7744a^4 + 25216a^3 + 22544a^2 - 784a - 5831).$$

A short computer search reveals that $P = (-1,\ 15)$ is a rational point on the quartic E. Using the program APECS [3] we found that E is birationally equivalent to the elliptic curve

$$E' : \ y^2 = x^3 - x^2 - 33433x + 2213737.$$

For the curve E' we have

$$\mathrm{Tors}\, E(\mathbb{Q}) = \{\mathcal{O},\ (127,\ 0)\},$$

and with the help of `mwrank` [4] we see that the free part of E' is generated by

$$G_1 = (77,\ -300),\ G_2 = (-193,\ -1200),\ G_3 = (-48,\ -1925).$$

Hence the curve E has an infinite number of rational points and it is clear that all but finitely many of them leads to the quartic C_a containing arithmetic progression of length 12. $\square$

It is natural to state the following question:

Open Question 3.2. *Is there an quartic elliptic curve E containing a length 13 arithmetic progression?*

4 Acknowledgment

I would like to thank anonymous referee for his/her valuable comments.

References

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

[2] G. Campbell, A note on arithmetic progressions on elliptic curves. *Journal of Integer Sequences*, Paper 03.1.3, 2003.

[3] I. Connel, APECS, available from `ftp.math.mcgill.ca/pub/apecs/`.

[4] J. Cremona, `mwrank` program, available from `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/`.

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

Received November 11 2004; revised version received May 21 2005. Published in *Journal of Integer Sequences*, May 24 2005.

Return to Journal of Integer Sequences home page.