ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 3, 2009

ON ARITHMETIC PROGRESSIONS ON GENUS TWO CURVES

MACIEJ ULAS

ABSTRACT. We study arithmetic progression in the x-coordinate of rational points on genus two curves. As we know, there are two models for curve C of genus two: $C : y^2 = f_5(x)$ or $C : y^2 = f_6(x)$, where $f_5,\ f_6 \in \mathbf{Q}[x]$, $\deg f_5 = 5$, $\deg f_6 = 6$ and the polynomials $f_5,\ f_6$ do not have multiple roots. First we prove that there exists an infinite family of curves of the form $y^2 = f(x)$, where $f \in \mathbf{Q}[x]$ and $\deg f = 5$, each containing 11 points in arithmetic progression. We also present an example of $F \in \mathbf{Q}[x]$ with $\deg F = 5$ such that, on the curve $y^2 = F(x)$, 12 points lie in arithmetic progression. Next, we show that there exist infinitely many curves of the form $y^2 = g(x)$ where $g \in \mathbf{Q}[x]$ and $\deg g = 6$, each containing 16 points in arithmetic progression. Moreover, we present two examples of curves in this form with 18 points in arithmetic progression.

1. Introduction. Let $f \in \mathbf{Q}[X]$ be a polynomial without multiple roots, and let us consider the curve $C : y^2 = f(x)$. We say that rational points $P_i = (x_i,\ y_i)$ for $i = 1, 2, \ldots, n$ are in *arithmetic progression* on the curve C, if rational numbers x_i are in arithmetic progression for $i = 1, 2, \ldots, n$. A positive integer n will be called the *length of arithmetic progression* on the curve C. A natural question arises here: How long can arithmetic progression be on the curve $y^2 = f(x)$ with a fixed degree of f? Throughout the whole paper, by a point we mean a rational one.

In the case of polynomials of degree one, this question is equivalent to the question about the number of squares which form an arithmetic progression.

It is not difficult to show that there exists an infinite family $\mathcal{A}_1$ of polynomials of degree one, with the property that, for each $f \in \mathcal{A}_1$,

2000 AMS *Mathematics subject classification.* Primary 11B25, 11D41.
Keywords and phrases. Rational points, genus two curves, arithmetic progression.
The author is a scholar of a project which is co-financed from the European Social Fund and Polish national budget within the Integrated Regional Operational Programme.
Received by the editors on June 29, 2006, and in revised form on October 2, 2006.
DOI:10.1216/RMJ-2009-39-3-971

there are three points in arithmetic progression on the curve $y^2 = f(x)$ (of genus 0). It turns out, however, which was already proved by Fermat, that it is impossible to construct arithmetic progression composed of four squares.

In paper [**1**], Allison has shown that there exists an infinite family $\mathcal{A}_2$ of polynomials of degree two such that, for each $f \in \mathcal{A}_2$ on the curve $y^2 = f(x)$ (of genus 0), eight points lie in arithmetic progression.

In the case of polynomials of degree three, Bremner in [**2**] has constructed an infinite family $\mathcal{A}_3$ with such a property that, for every $f \in \mathcal{A}_3$ on the curve $y^2 = f(x)$ (of genus 1), eight points lie in arithmetic progression. A similar result with the use of other methods was obtained by Campbell in [**3**].

In the case of polynomials of degree four, in [**8**] we have constructed an infinite family $\mathcal{A}_4$ with such a property that, for every $f \in \mathcal{A}_4$, there are 12 points in arithmetic progression on the curve $y^2 = f(x)$ (of genus 1).

It is worth noting that MacLeod in [**5**] has constructed polynomials F_i, $i = 1, 2, 3, 4$, of degree four such that on each curve $y^2 = F_i(x)$ there are 14 points in arithmetic progression.

In all of the above cases, each of the families $\mathcal{A}_2$, $\mathcal{A}_3$, $\mathcal{A}_4$ is parametrized by rational points on some elliptic curve of positive rank.

It is reasonable to define the following quantities

$$\begin{aligned} m(d) := \max\{k :\ & \text{there exists a polynomial } g \in Q[x] \\ & \text{of degree } \deg g = d \text{ such that on the curve } y^2 = g(x) \\ & \text{there are } k \text{ points in arithmetic progression}\}, \\ M(d) := \max\{k :\ & \text{there exists an infinite family } \mathcal{A}_d \\ & \text{of polynomials of degree } d, \text{ such that for every } g \in \mathcal{A}_d \\ & \text{there are } k \text{ points in arithmetic progression} \\ & \text{on the curve } y^2 = g(x)\}. \end{aligned}$$

We have an obvious inequality $m(d) \geq M(d)$. The above results can be grouped in the following manner:

TABLE 1.

d	1	2	3	4
$m(d)$	3	≥ 8	≥ 8	≥ 14
$M(d)$	3	≥ 8	≥ 8	≥ 12

In this paper we will concentrate on quantities $m(d)$ and $M(d)$ for $d = 5,\ 6$. Let us note that it corresponds to the construction of arithmetic progressions on hyperelliptic curves of genus 2. In the case of $d = 5$, we show that $m(5) \geq 12$ and $M(5) \geq 11$. When $d = 6$, we first show that there exists a polynomial $G(t, x) \in \mathbf{Q}(t)[x]$ such that there are 14 points in arithmetic progression on the curve $y^2 = G(t, x)$. Using another approach we prove that $m(6) \geq 18$ and $M(6) \geq 16$.

2. Case of $d = 5$. Using a method similar to that used by Campbell in [**3**] we will show the following

Theorem 2.1. *There exist polynomials $F_i(t, x) \in \mathbf{Q}(t)[x]$, $i = 1, 2$, of degree $\deg_x F_i = 5$ such that, on the curve $y^2 = F_i(t, x)$, 11 $\mathbf{Q}(t)$-rational points lie in arithmetic progression.*

Proof. Let u be a variable, and let us consider a polynomial

$$g(u, x) = (x - u)^2 \prod_{i=1}^{10} (x - i).$$

As we know, there is exactly one pair of polynomials $h,\ f \in \mathbf{Q}(u)[x]$ such that $\deg_x h = 6$, $\deg_x f = 5$ and

$$g(u, x) = h(u, x)^2 - \frac{25}{1048576} f(u, x).$$

In our case, polynomial f is in the form of

$$f(u, x) = a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0,$$

where

$$a_0 = 5695244944u^2 - 12894461800u + 263250625,$$

$$
\begin{aligned}
a_1 &= -8(533634200u^2 - 873304794u - 1611807725),\\
a_2 &= 32(37257330u^2 - 8034400u - 396302603),\\
a_3 &= -3520(41536u^2 + 145226u - 1285845),\\
a_4 &= 3520(1888u^2 + 31152u - 193477),\\
a_5 &= -(6645760u - 36551680).
\end{aligned}
$$

If u is rational and $u \neq 11/2$, then the polynomial $f(u,x)$ is without multiple roots. Thus, we see that, in this case, there are ten points in arithmetic progression on the curve $y^2 = f(u,x)$.

Let us now consider the curve Q_1 with the equation $p_1^2 = f(u_1, 11)$. This is a quadric with rational point $(11,\ 16225)$. Using the standard method we have a parametrization of the curve Q_1 given by:

$$
\begin{aligned}
p_1(t) &= \frac{16225(5695244944t^2 - 794728t + 1)}{5695244944t^2 - 1},\\
u_1(t) &= \frac{11(4523021144t^2 + 2950t - 1)}{5695244944t^2 - 1}.
\end{aligned}
$$

If we now define $F_1(t,x) = f(u_1(t), x)$, where $u_1(t)$ is as above, then on the curve

$$C_1 : y^2 = F_1(t,x)$$

there are 11 points in arithmetic progression.

We can similarly parametrize the quadric Q_2 given by the equation $p_2^2 = f(u_2, 0)$ with rational point $(0, 16225)$. In this case the parametrization takes the form

$$
\begin{aligned}
p_2(t) &= \frac{16225(5695244944t^2 + 794728t + 1)}{5695244944t^2 - 1},\\
u_2(t) &= \frac{32450t(397364t + 1)}{5695244944t^2 - 1}.
\end{aligned}
$$

If we now define $F_2(t,x) = f(u_2(t), x)$, where $u_2(t)$ is as above, then on the curve

$$C_2 : y^2 = F_2(t,x)$$

there are 11 points in arithmetic progression. □

Finding a rational t such that on the curve C_1 there are 12 points in arithmetic progression requires finding rational points on the curve

$$\begin{aligned} y^2 = &-5435428154579785379041230517 76t^4 \\ &- 58585325307889959181504 00t^3 \\ &+ 6115416111118567334 08t^2 - 633115875308400t \\ &- 30556659591, \end{aligned}$$

or on the curve

$$\begin{aligned} y^2 = &\ 1045272379721179724157530623 2064t^4 \\ &+ 160068248351041059216704 00t^3 \\ &- 4781502606421467214112t^2 \\ &- 3647410080111600t + 547548809049. \end{aligned}$$

Then, points with x-coordinates in $\{1,\ 2,\ \ldots,\ 12\}$ (respectively with x-coordinates in $\{0,\ 1,\ \ldots,\ 11\}$) will be in arithmetic progression on the curve C_1. In the case of the curve C_2, we obtain the same curves. It is easy to see that the above curves have $\mathbf{Q}_p$-rational points for every p, but unfortunately we did not manage to find a rational point on any of the above curves. It seems that finding a rational point on any of the curves (or showing that such points do not exist) may be a difficult task.

Remark 2.2. The statement of Theorem 2.1 can also be obtained using the following reasoning. Let us consider the polynomial

$$f(t,x) = (x-t)\prod_{i=1}^{11}(x-i).$$

Then there exist polynomials $p,\ F \in \mathbf{Q}(t)[x]$, such that $\deg_x p = 6$, $\deg_x F = 5$ and

$$f(t,x) = p(t,x)^2 - F(t,x)$$

Then the curve $C:\ y^2 = F(t,x)$ contains 11 points in arithmetic progression. Unfortunately, in this case the polynomials $F(t,0)$ and $F(t,12)$ are irreducible of degree 6, and each of the curves $y^2 = F(t,0)$, $y^2 = F(t,12)$ contain only finitely many rational points. Therefore, the

curve C cannot be used to construct an infinite family of curves with the required property.

The following example found with the use of computer shows that $m(5) \geq 12$. Consider the curve

$$C : y^2 = 12x^5 - 322x^4 + 3208x^3 - 14438x^2 + 27980x - 16079.$$

We have the following points in arithmetic progression on the curve C:

$$\{(1,19),\ (2,55),\ (3,37),\ (4,1),\ (5,11),\ (6,31),\ (7,35),\ (8,23),\ (9,29),\ (10,89),\ (11,181),\ (12,305)\}.$$

3. Case of $d = 6$. Let us begin with the following

Theorem 3.1. *There exists a polynomial $H(t,x) \in \mathbf{Q}(t)[x]$ of degree $\deg_x H = 6$, such that 14 $\mathbf{Q}(t)$-rational points lie in arithmetic progression on the curve $y^2 = H(t,x)$.*

Proof. Let t be a variable, and let us consider a polynomial

$$h(t,x) = (x^2 - 15x + 4t)\prod_{i=1}^{14}(x-i).$$

Then there is exactly one pair of polynomials $g,\ H \in \mathbf{Q}(t)[x]$ such that $\deg_x 8 = 6$, $\deg_x H = 6$ and

$$h(t,x) = g(t,x)^2 - H(t,x).$$

In our case the polynomial H is in the form

$$H(t,x) = a_3(x(15-x))^3 + a_2(x(15-x))^2 + a_1(x(15-x)) + a_0,$$

where

$$a_0 = 46228440064 - 37262033920t + 10620980224t^2 - 1420209280t^3 + 106891216t^4 - 4876960t^5 + 144760t^6 - 2800t^7 + 25t^8,$$

$$
\begin{aligned}
a_1 &= 4(-790888960 + 642389312t - 177526160t^2 + 21803240t^3 \\
&\quad - 1364540t^4 + 42826t^5 - 630t^6 + 5t^7), \\
a_2 &= 2(35503616 - 29056640t + 7910592t^2 - 929040u^3 + 52318t^4 \\
&\quad - 1260t^5 + 7t^6), \\
a_3 &= 2(-261120 + 215008t - 58040t^2 + 6636t^3 - 350t^4 + 7t^5).
\end{aligned}
$$

Therefore, we see that on the curve

$$C : y^2 = H(t, x)$$

14 points lie in arithmetic progression. These points are of the form $P_i = (i,\ g(t,i))$ for $i = 1, 2, \ldots, 14$. □

The first part of the proof of Theorem 3.1 suggests considering polynomials which are invariant with respect to the change of variables $x \to 15 - x$. Let us, therefore, consider the polynomial

$$f(x) = b_3(x(x-15))^3 + b_2(x(x-15))^2 + b_1 x(x-15) + b_0, \tag{3.1}$$

where

$$
\begin{aligned}
b_0 &= (6p^2 - 22q^2 + 27r^2 - 11s^2)/47520, \\
b_1 &= (159p^2 - 517q^2 + 567r^2 - 209s^2)/11880, \\
b_2 &= (5496p^2 - 14872q^2 + 14337r^2 - 4961s^2)/11880, \\
b_3 &= (156p^2 - 308q^2 + 273r^2 - 91s^2)/30.
\end{aligned}
$$

For f defined in this way we have

$$
\begin{aligned}
f(1) &= f(14) = p^2, \qquad & f(2) &= f(13) = q^2, \\
f(3) &= f(12) = r^2, \qquad & f(4) &= f(11) = s^2.
\end{aligned}
$$

Therefore, we see that, in order to obtain an arithmetic progression of length 14 on the curve $y^2 = f(x)$, it is necessary to investigate the system of equations

$$
\begin{cases}
f(5) = (-14p^2 + 77q^2 - 162r^2 + 154s^2)/55 = u^2 \\
f(6) = (-21p^2 + 110q^2 - 210r^2 + 154s^2)/33 = v^2 \\
f(7) = (-60p^2 + 308q^2 - 567r^2 + 385s^2)/66 = w^2.
\end{cases} \tag{3.2}
$$

Using a substitution $(p,\ q,\ r,\ s,\ u) = (a+u,\ b+u,\ c+u,\ d+u,\ u)$, we obtain a parametrization of solutions of the first equation of system (3.2)

$$\begin{aligned}(p,\ q,\ r,\ s,\ u)&\\ &= (14a^2 - 154ab + 77b^2 + 324ac - 162c^2 - 308ad + 154d^2,\\ &\quad 14a^2 - 28ab + 77b^2 - 324bc + 162c^2 + 308bd - 154d^2,\\ &\quad -14a^2 + 77b^2 + 28ac - 154bc + 162c^2 - 308cd + 154d^2,\\ &\quad 14a^2 - 77b^2 + 162c^2 - 28ad + 154bd - 324cd + 154d^2,\\ &\quad -14a^2 + 77b^2 - 162c^2 + 154d^2).\end{aligned}$$

Now, let us set

$$(a,\ b,\ c,\ d) = (946A,\ 946,\ 11(15A+71),\ 441A+505). \tag{3.3}$$

For $a,\ b,\ c,\ d$ defined in this way, we get a parametric solution of the system (3.2) given by

$$\begin{aligned}(p,\ q,\ r,\ s,\ u,\ v,\ w)&\\ &= (181144A^2 + 85170A - 42585, 59140A^2 - 118280A - 164589,\\ &\quad 17230A^2 - 112505A - 128454, 52874A^2 + 102845A + 68010,\\ &\quad 59140A^2 + 122004A + 42585, 43984A^2 + 104070A + 75675,\\ &\quad 15790A^2 + 107955A + 99984).\end{aligned}$$

For $p,\ q,\ r,\ s$ defined above, the coefficients of the polynomial $g_A(x) = 36f(x)$ are

$$\begin{aligned}b_0 &= 36(128941675300A^4 + 235814377620A^3 + 34730973441A^2\\ &\quad - 216866857320A - 132565503600),\\ b_1 &= 4(A-1)(254A+219)(354070194A^2+848446325A+620203644),\\ b_2 &= (A-1)(254A+219)(35708622A^2 + 96399845A + 73722213),\\ b_3 &= 4(A-1)(254A+219)(72474A^2 + 210275A + 164709).\end{aligned}$$

For $A \in \mathbf{Q} \setminus S$, where $S = \{-240/233, -219/254, 1, 475/2\}$, the polynomial g_A does not have multiple roots. From this, we can conclude that, for $A \in \mathbf{Q} \setminus S$ on the curve,

$$C_A : y^2 = g_A(x),$$

14 points lie in arithmetic progression. Now, it is an easy task to prove the following

Theorem 3.2. *There exist infinitely many $A \in \mathbf{Q}$ such that on the curve $C_A : y^2 = g_A(x)$ there are 16 points in arithmetic progression.*

Proof. Let us set $x = 0$ and consider the curve

$$C : y^2 = b_0(A).$$

It is easy to see that on C we have rational point $P = (1, 1342374)$. As we know, the curve of the form $y^2 = f_4(x)$, where $\deg f_4 = 4$, with rational point, is birationally equivalent to an elliptic curve with Weierstrass's equation [**6**]. Using the APECS program [**4**], we obtain that C is birational with the curve

$$E : y^2 + xy + y = x^3 - x^2 + 21015110653x + 1214962664541571.$$

For the curve E, we have

$$\operatorname{Tors} E(\mathbf{Q}) = \{\mathcal{O},\ (-51365, 25682)\},$$

and again using APECS we obtain that the free part of $E(\mathbf{Q})$ is generated by

$$\begin{aligned} G_1 &= (-45989,\ -12274606),\\ G_2 &= (751451,\ -664705966),\\ G_3 &= (-17669,\ -28941646),\\ G_4 &= (24913585/256,\ 264676595567/4096). \end{aligned}$$

As an immediate consequence, we get that there are infinitely many rational points on the curve C, and all but finitely many define the curve $C_A :\ y^2 = g_A(x)$ with 16 points in arithmetic progression. □

To show that $m(6) \geq 18$, we have taken the polynomial of the form

$$h(x) = c_3(x(x-19))^3 + c_2(x(x-19))^2 + c_1 x(x-19) + c_0. \tag{3.4}$$

With the help of the computer we found the following numbers $c_0,\ c_1,\ c_2,\ c_3$ such that the polynomial (3.4) has values which are squares of integers for $x = 1, 2, \ldots, 18$:

TABLE 2.

c_0	c_1	c_2	c_3
358043904	18892800	321792	1664
864002304	37085184	524544	2432

Acknowledgments. I would like to thank the anonymous referee for his valuable comments and Professor K. Rusek for remarks improving the presentation.

REFERENCES

1. D. Allison, *On certain simultaneous Diophantine equations*, Math. Colloq. Univ. Cape Town **11** (1977), 117–133.

2. Andrew 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), Article 03.1.3.

4. I. Connell, APECS: *Arithmetic of plane elliptic curves*, available from `ftp.math.mcgill.ca/pub/apecs/`.

5. A. MacLeod, *Fourteen-term arithmetic progressions on quartic elliptic curves*, J. Integer Sequences **9** (2006), Article 06.1.2.

6. L.J. Mordell, *Diophantine equations*, Academic Press, London, 1969.

7. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

8. M. Ulas, *A note on arithmetic progressions on quartic elliptic curves*, J. Integer Sequences **8** (2005), Article 05.3.1.

Jagiellonian University, Institute of Mathematics, Łojasiewicza 6, 30-348 Kraków, Poland
Email address: Maciej.Ulas@im.uj.edu.pl