GLASNIK MATEMATIČKI
Vol. 52(72)(2017), 45 – 52

ON SEQUENCES OF CONSECUTIVE SQUARES ON ELLIPTIC CURVES

Mohamed Kamel and Mohammad Sadek
Cairo University, Egypt and American University in Cairo, Egypt

Abstract. Let C be an elliptic curve defined over $\mathbb{Q}$ by the equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Q}$. A sequence of rational points $(x_i, y_i) \in C(\mathbb{Q})$, $i = 1, 2, \ldots$, is said to form a sequence of consecutive squares on C if the sequence of x-coordinates, $x_i, i = 1, 2, \ldots$, consists of consecutive squares. We produce an infinite family of elliptic curves C with a 5-term sequence of consecutive squares. Furthermore, this sequence consists of five independent rational points in $C(\mathbb{Q})$. In particular, the rank r of $C(\mathbb{Q})$ satisfies $r \geq 5$.

1. Introduction

In [3], Bremner initiated the discussion of certain arithmetic questions on rational points of elliptic curves attempting to relate the group structure on an elliptic curve E to the addition group operation on the rational line. He raised the question of the existence of a sequence of rational points in $E(\mathbb{Q})$ whose x-coordinates form an arithmetic progression in $\mathbb{Q}$. Such sequence is called an arithmetic progression sequence in $E(\mathbb{Q})$. A variety of questions may be posed. For instance, how long these sequences can be and how many elliptic curves would have such long sequences of rational points. The existence of infinitely many elliptic curves with length 8 arithmetic progressions was proved. Several authors introduced different approaches to find infinitely many elliptic curves with longer arithmetic progression sequences, see [1, 5, 7, 10].

In [4], the study of sequences of rational points on elliptic curves whose x-coordinates form a geometric progression in $\mathbb{Q}$ was initiated. An infinite family of elliptic curves having geometric progression sequences of length 4

2010 *Mathematics Subject Classification.* 14G05, 11B83.
Key words and phrases. Elliptic curves, rational points, sequences of consecutive squares.

was exhibited. It was remarked that infinitely many elliptic curves with 5-term geometric progression sequences can be constructed.

In this note, we discuss sequences of rational points on elliptic curves whose x-coordinates form a sequence of consecutive squares. We consider elliptic curves defined by the equation $y^2 = ax^3 + bx + c$ over $\mathbb{Q}$. We show that elliptic curves defined by the latter equation with 5-term sequences of rational points whose x-coordinates are elements in a sequence of consecutive squares in $\mathbb{Q}$ are parametrized by an elliptic surface whose rank is positive. Hence, one deduces the existence of infinitely many such elliptic curves. Moreover, we show that the five rational points forming the sequence are linearly independent in the group of rational points of the elliptic curve they lie on. In particular, we introduce an infinite family of elliptic curves of rank ≥ 5.

2. Sequences of Consecutive Squares

Definition 2.1. *Let C be an elliptic curve defined over a number field K by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in K$. The sequence $(x_i, y_i) \in C(K)$ is said to be a* sequence of consecutive squares *on C if there is a $u \in K$ such that $x_i = (u + i)^2$, $i = 1, 2, \ldots$.*

The following proposition ensures the finiteness of the sequence of consecutive squares on an elliptic curve.

Proposition 2.2. *Let C be an elliptic curve defined over a number field K by a Weierstrass equation of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K.$$

Let $(x_i, y_i) \in C(K)$ be a sequence of consecutive squares on C. Then the sequence (x_i, y_i) is finite.

Proof. We can assume without loss of generality that $x_i = (u + i)^2$, $i = 1, 2, \ldots$, $u \in K$. This sequence gives rise to a sequence of rational points on the genus 2 hyperelliptic curve

$$\mathcal{C} : y^2 + a_1x^2y + a_3y = x^6 + a_2x^4 + a_4x^2 + a_6.$$

Namely, the points $(u + i, y) \in \mathcal{C}(K)$. According to Faltings' Theorem, [6], one knows that $\mathcal{C}(K)$ is finite, hence the sequence is finite. □

Based on the above proposition, one may present the following definition.

Definition 2.3. *Let C be an elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation. Let $(x_i, y_i) \in C(\mathbb{Q})$, $i = 1, 2, \ldots, n$, be a sequence of consecutive squares on C. Then n is said to be the* length *of the sequence.*

3. Constructing elliptic curves with long sequences of consecutive squares

In this note, we focus our attention on the family of elliptic curves given by the affine equation $C : y^2 = ax^3 + bx + c$ over $\mathbb{Q}$. We will show that there are infinitely many elliptic curves defined by the latter equation containing 5-term sequences of consecutive squares.

One observes that if $(t^2, d), ((t+1)^2, e)$, and $((t+2)^2, f)$ lie in $C(\mathbb{Q})$, where $t \in \mathbb{Q}$, then these rational points form a 3-term sequence of consecutive squares. Indeed, one has

$$\begin{aligned} d^2 &= at^6 + bt^2 + c, \\ e^2 &= a(t+1)^6 + b(t+1)^2 + c, \\ f^2 &= a(t+2)^6 + b(t+2)^2 + c. \end{aligned}$$

It is a standard linear algebra exercise to show that

$$\begin{aligned} a &= \frac{(3+2t)d^2 - 4(1+t)e^2 + (1+2t)f^2}{4(15+73t+135t^2+125t^3+60t^4+12t^5)}, \\ b &= \frac{(3+2t)(3+3t+t^2)(7+9t+3t^2)d^2}{4(1+2t)(15+43t+49t^2+27t^3+6t^4)} \\ &\quad + \frac{(1+t)(-4(4+2t+t^2)(4+6t+3t^2)e^2)}{4(1+2t)(15+43t+49t^2+27t^3+6t^4)} \\ &\quad + \frac{(1+t)(4+2t+t^2)(4+6t+3t^2)f^2}{4(1+2t)(15+43t+49t^2+27t^3+6t^4)}, \\ c &= \frac{(2+t)^2(15+43t+46t^2+22t^3+4t^4)d^2}{4(1+2t)(15+28t+21t^2+6t^3)} \\ &\quad - \frac{8t^2(2+t)^2(2+2t+t^2)e^2 + t^2(1+5t+10t^2+10t^3+4t^4)f^2}{4(1+2t)(15+28t+21t^2+6t^3)}. \end{aligned} \tag{3.1}$$

In particular, one has the following result.

Remark 3.1. The above argument indicates that given $d, e, f \in \mathbb{Q}(t)$, there exist $a, b, c \in \mathbb{Q}(t)$ such that the ordered pairs $(t^2, d), ((t+1)^2, e)$ and $((t+2)^2, f)$ are three rational points on the elliptic surface $y^2 = ax^3 + bx + c$.

Now, if $((t+3)^2, g) \in C(\mathbb{Q})$, then one has a 4-term sequence of consecutive squares on C. In fact, using the above values for a, b, c, one then sees that

$$\begin{aligned} g^2 &= \frac{(5+2t)((2+t)(14+12t+3t^2)d^2 - 3(1+t)(13+10t+3t^2)e^2)}{(1+t)(1+2t)(5+6t+3t^2)} \\ &\quad + \frac{3(2+t)(1+2t)(10+8t+3t^2)f^2}{(1+t)(1+2t)(5+6t+3t^2)}. \end{aligned} \tag{3.2}$$

Therefore, in view of Remark 3.1, one needs to find the elements d, e, f and g in $\mathbb{Q}(t)$ satisfying the latter equation in order to construct an elliptic curve

C with a 4-term sequence of consecutive squares. In fact, since $(d, e, f, g) = (1, 1, 1, 1)$ is a solution for equation (3.2), the general solution (d, e, f, g) is given by the following parametrization:

(3.3)

$$\begin{aligned}
d = {} & (2+t)(5+2t)(14+12t+3t^2)p^2 + 3(1+t)(5+2t)(13+10t+3t^2)q^2 \\
& - 3(2+t)(1+2t)(10+8t+3t^2)w^2 + 6(20+66t+66t^2+31t^3+6t^4)pw \\
& - 6(65+141t+111t^2+41t^3+6t^4)pq, \\
e = {} & -(2+t)(5+2t)(14+12t+3t^2)p^2 - 3(1+t)(5+2t)(13+10t+3t^2)q^2 \\
& - 3(2+t)(1+2t)(10+8t+3t^2)w^2 + 6(20+66t+66t^2+31t^3+6t^4)qw \\
& + 2(140+246t+166t^2+51t^3+6t^4)pq, \\
f = {} & -(2+t)(5+2t)(14+12t+3t^2)p^2 + 3(1+t)(5+2t)(13+10t+3t^2)q^2 \\
& + 3(2+t)(1+2t)(10+8t+3t^2)w^2 - 6(1+t)(5+2t)(13+10t+3t^2)qw \\
& + 2(2+t)(5+2t)(14+12t+3t^2)pw, \\
g = {} & -p^2(140+246t+166t^2+51t^3+6t^4) \\
& + 3(q^2(65+141t+111t^2+41t^3+6t^4) \\
& - (20+66t+66t^2+31t^3+6t^4)w^2).
\end{aligned}$$

Consult [8, §7] for finding parametric rational solutions of a homogeneous polynomial of degree 2 in several variables.

REMARK 3.2. The points $(t^2, d), ((t+1)^2, e), ((t+2)^2, f), ((t+3)^2, g)$, where $d, e, f, g \in \mathbb{Q}(t, p, q, w)$ are given as above, are rational points on the elliptic surface $y^2 = ax^3 + bx + c$, where a, b, c are defined in (3.1).

Now, we assume that $((t+4)^2, h)$ is a rational point on the elliptic curve $y^2 = ax^3 + bx + c$. In particular, there exists a 5-term sequence of consecutive squares on the latter curve. Then one has

$$h^2 = Ap^4 + Bp^3 + Cp^2 + Dp + E \tag{3.4}$$

with

$$\begin{aligned}
A = {} & (140+246t+166t^2+51t^3+6t^4)^2, \\
B = {} & \frac{4(5+2t)^2(196+322t+202t^2+57t^3+6t^4)}{3+2t}((87+83t+27t^2+3t^3)q \\
& - 3(52+58t+22t^2+3t^3)w),
\end{aligned}$$

$$
\begin{aligned}
C = {} & \frac{2(5+2t)}{3+2t}(5(78330+250402t+346118t^2+271991t^3+132943t^4\\
& +41217t^5+7851t^6+828t^7+36t^8)q^2-12(41580+154358t+243358t^2\\
& +217563t^3+121708t^4+43727t^5+9852t^6+1272t^7+72t^8)qw\\
& +15(2+t)^2(-2828-2552t+784t^2+2364t^3\\
& +1395t^4+360t^5+36t^6)w^2),\\
D = {} & \frac{12(35+24t+4t^2)}{3+2t}((5655+17662t+23115t^2+16782t^3+7345t^4\\
& +1938t^5+285t^6+18t^7)q^3+(6660+18502t+22620t^2+15567t^3\\
& +6515t^4+1683t^5+255t^6+18t^7)q^2w-5(3708+11842t+16104t^2\\
& +12237t^3+5651t^4+1593t^5+255t^6+18t^7)qw^2\\
& +3(2+t)^2(260+888t+972t^2+544t^3+153t^4+18t^5)w^3),\\
E = {} & 9((65+141t+111t^2+41t^3+6t^4)^2q^4+8(22750+79965t+121251t^2\\
& +105282t^3+57708t^4+20529t^5+4643t^6+612t^7+36t^8)wq^3\\
& -2(120300+457050t+737244t^2+678163t^3+394077t^4+149001t^5\\
& +35957t^6+5088t^7+324t^8)w^2q^2+8(2+t)^2(1750+6380t+7959t^2\\
& +5294t^3+1987t^4+408t^5+36t^6)qw^3\\
& +(20+66t+66t^2+31t^3+6t^4)^2w^4).
\end{aligned}
$$

Observing that the above expressions are homogeneous in q and w, one may assume that $w=1$. The following result then holds.

THEOREM 3.3. *The curve*

$$\mathcal{C}: Y^2 = AX^4+BX^3+CX^2+DX+E$$

is birationally equivalent over $\mathbb{Q}(t,q)$ *to an elliptic curve* $\mathcal{E}$ *with*

$$\operatorname{rank}\mathcal{E}(\mathbb{Q}(t,q)) \geq 1.$$

PROOF. After homogenizing the equation describing $\mathcal{C}$, one obtains $Y^2 = AX^4+BX^3Z+CX^2Z^2+DXZ^3+EZ^4$ with a rational point $R=(X:Y:Z)=(1:140+246t+166t^2+51t^3+6t^4:0)$. The curve $\mathcal{C}$ is birationally equivalent to the cubic curve $\mathcal{E}$ defined by the equation $V^2=U^3-27IU-27J$, [9], where $I=12AE-3BD+C^2$ and $J=72ACE+9BCD-27AD^2-27B^2E-2C^3$. The discriminant $\Delta(\mathcal{E})$ of $\mathcal{E}$ is given by $(4I^3-J^2)/27$, and the specialization of $\mathcal{E}$ is singular only if $\Delta(\mathcal{E})=0$. Moreover, the point

$$P=\left(3\frac{3B^2-8AC}{4A}, 27\frac{B^3+8A^2D-4ABC}{8A^{3/2}}\right)$$

lies in $\mathcal{E}(\mathbb{Q}(t,q))$ since A is a square. One considers the specialization $t = 1, q = \dfrac{81}{40}$ to obtain the specialization

$$\widetilde{P} = \left(\frac{-4786935489}{100}, \frac{-56568093052527}{50}\right)$$

of the point P on the specialized elliptic curve

$$\widetilde{\mathcal{E}} : y^2 = x^3 - \frac{147183268996968521373}{10000}x + \frac{171278570868444028577352480093}{250000}.$$

Using MAGMA, [2], the point $\widetilde{P}$ is a point of infinite order on $\widetilde{\mathcal{E}}$. Therefore, according to Silverman's specialization Theorem, the point P is of infinite order on $\mathcal{E}$. □

Corollary 3.4. *For any nontrivial sequence of consecutive rational squares $t_0^2, (t_0+1)^2, (t_0+2)^2, (t_0+3)^2, (t_0+4)^2$, there exist infinitely many elliptic curves $E_m : y^2 = a_m x^3 + b_m x + c_m$, $m \in \mathbb{Z} \setminus \{0\}$, such that $(t_0+i)^2, i = 0,1,2,3,4$, is the x-coordinate of a rational point on E_m. Moreover, these five rational points are independent.*

Proof. We fix $t = t_0$, $q = q_0$, and $w = 1$ in $\mathbb{Q}$. Substituting these values into (3.4), one obtains the elliptic curve

$$\mathcal{C}_{t_0,q_0,1} : h^2 = Ap^4 + Bp^3 + Cp^2 + Dp + E,\ A, B, C, D \in \mathbb{Q},$$

with positive rank, see Theorem 3.3. Now, one fixes a point $P = (p, h)$ of infinite order in $\mathcal{C}_{t_0,q_0,1}(\mathbb{Q})$. For any nonzero integer m, we set $mP = (p_m, h_m)$ to be the m-th multiple of the point P in $\mathcal{C}_{t_0,q_0}(\mathbb{Q})$.

Now, one substitutes $t = t_0, q = q_0, w = 1$, and $p = p_m$ into the formulas for $d, e, f, g \in \mathbb{Q}(t, p, q, w)$ in (3.3) in order to obtain the rational numbers d_m, e_m, f_m, g_m, respectively. Then one substitutes d_m, e_m, f_m into the formulas for $a, b, c \in \mathbb{Q}(t, d, e, f)$ in (3.1) to get the rational numbers a_m, b_m, c_m, respectively.

To sum up, one constructed an infinite family of elliptic curves $E_m : y^2 = a_m x^3 + b_m x + c_m$, where m is a nonnegative integer. The latter infinite family E_m of elliptic curves satisfies the property that the points $(t_0^2, d_m), ((t_0+1)^2, e_m), ((t_0+2)^2, f_m), ((t_0+3)^2, g_m), ((t_0+4)^2, h_m) \in E_m(\mathbb{Q})$. Thus, one obtains an infinite family of elliptic curves with a 5-term sequence of rational points whose x-coordinates form a sequence of consecutive squares in $\mathbb{Q}$.

To show that the points $(t^2, d_m), ((t+1)^2, e_m), ((t+2)^2, f_m), ((t+3)^2, g_m), ((t+4)^2, h_m) \in E_m(\mathbb{Q})$ are independent, one specializes $t = 1, q = 81/40, w = 1$ which yields the existence of the infinite point

$$(p, h) = \left(\frac{2201}{2320}, \frac{-62736289}{18852320}\right) \in \mathcal{C}_{1,81/40,1}(\mathbb{Q}).$$

Therefore, the specialization $t = 1, q = 81/40, w = 1, p = 2201/2320$ gives us the specialized elliptic curve

$$E : y^2 = \frac{42674183}{52786496000}x^3 - \frac{612989889}{7540928000}x + \frac{1180698375893607}{2487869785676800}$$

with the following set of rational points in $E(\mathbb{Q})$:

$$\left(1, \frac{-2367005}{3770464}\right), \left(2^2, \frac{8455597}{18852320}\right), \left(3^2, \frac{-10868031}{18852320}\right),$$

$$\left(4^2, \frac{-29720351}{18852320}\right), \left(5^2, \frac{-62736289}{18852320}\right).$$

Using MAGMA, [2], these rational points are independent.

According to Silverman's Specialization Theorem, it follows that the points $(t^2, d_m), ((t+1)^2, e_m), ((t+2)^2, f_m), ((t+3)^2, g_m), ((t+4)^2, h_m)$ are independent in E_m over $\mathbb{Q}(t, q, p_m)$. □

Remark 3.5. Corollary 3.4 implies the existence of an infinite family of elliptic curves whose rank $r \geq 5$.

Remark 3.6. In order to construct a 6-term sequence of consecutive squares, we assume that the point $((t+5)^2, k)$ is a rational point on our elliptic curve $y^2 = ax^3 + bx + c$. Then the following relation is satisfied

$$k^2 = A'p^4 + B'p^3 + C'p^2 + D'p + E'$$

for some $A', B', C', D', E' \in \mathbb{Q}(t, q)$. Thus, the existence of a 6-term sequence of consecutive squares on the elliptic curve is equivalent to the existence of a rational point (p, h, k) on the algebraic curve defined by the following intersection

$$C : h^2 = Ap^4 + Bp^3 + Cp^2 + Dp + E,\ k^2 = A'p^4 + B'p^3 + C'p^2 + D'p + E'.$$

The curve C is a curve of genus 5. Therefore, Faltings' Theorem implies that given $t \in \mathbb{Q}$, there are only finitely many elliptic curves over $\mathbb{Q}$ defined by $y^2 = ax^3 + bx + c$ for which $(t+i)^2,\ i = 0, 1, \ldots, 5$, are the x-coordinates of a 6-term sequence of consecutive squares.

Acknowledgements.

We would like to thank Professor Nabil Youssef, Cairo University, for his support, thorough reading of the manuscript, and several useful suggestions. We would like also to thank an anonymous referee for his careful reading, remarks, and corrections.

References

[1] A. Alvarado, *An arithmetic progression on quintic curves,* J. Integer Seq. **12** (2009), Article 09.7.3, 6pp.
[2] W. Bosma and J. Cannon and C. Playoust, *The Magma algebra system. I. The user language,* J. Symbolic Comput. **24** (1997), 235–265.
[3] A. Bremner, *On arithmetic progressions on elliptic curves,* Exp. Math. **8** (1999), 409–413.
[4] A. Bremner and M. Ulas, *Rational points in geometric progressions on certain hyperelliptic curves,* Publ. Math. Debrecen **82** (2013), 669–683.
[5] G. Campbell, *A note on arithmetic progressions on elliptic curves,* J. Integer Seq. **6** (2003), Article 03.1.3, 5pp.
[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Invent. Math. **73** (1983), 349–366.
[7] A. J. MacLeod, *14-term arithmetic progressions on quartic elliptic curves,* J. Integer Seq. **9** (2006), Article 06.1.2, 4pp.
[8] L. J. Mordell, Diophantine Equations, Academic Press, New York, 1969.
[9] M. Stoll and J. E. Cremona, *Minimal models for 2-coverings of elliptic curve,* LMS J. Comput. Math. **5** (2002), 220–243.
[10] M. Ulas, *A note on arithmetic progressions on quartic elliptic curves,* J. Integer Seq. **8** (2005), Article 05.3.1, 5pp.

M. Kamel
Department of Mathematics
Faculty of Science
Cairo University
Giza
Egypt
E-mail: mohgamal@sci.cu.edu.eg

M. Sadek
Mathematics and Actuarial Science Department
American University in Cairo
AUC Avenue, New Cairo
Egypt
E-mail: mmsadek@aucegypt.edu

Received: 13.8.2016.
Revised: 21.8.2016.