Functiones et Approximatio
60.2 (2019), 245–252
doi: 10.7169/facm/1740

SEQUENCES OF CONSECUTIVE SQUARES ON QUARTIC ELLIPTIC CURVES

Mohamed Kamel, Mohammad Sadek

Abstract: Let $C : y^2 = ax^4 + bx^2 + c$, be an elliptic curve defined over $\mathbb{Q}$. A set of rational points $(x_i, y_i) \in C(\mathbb{Q})$, $i = 1, 2, \cdots$, is said to be a sequence of consecutive squares if $x_i = (u + i)^2$, $i = 1, 2, \cdots$, for some $u \in \mathbb{Q}$. Using ideas of Mestre, we construct infinitely many elliptic curves C with sequences of consecutive squares of length at least 6. It turns out that these 6 rational points are independent. We then strengthen this result by proving that for a fixed 6-term sequence of consecutive squares, there are infinitely many elliptic curves C with the latter sequence forming the x-coordinates of six rational points in $C(\mathbb{Q})$.

Keywords: elliptic curves, rational points, sequences of consecutive squares.

1. Introduction

In [3], Bremner started discussing the existence of long sequences on elliptic curves. He produced an infinite family of elliptic curves with arithmetic progression sequences of length 8. Several authors displayed infinite families of elliptic curves with long arithmetic progression sequences, see [5, 8, 11].

A geometric progression sequence is another type of sequence that has been studied on elliptic and hyperelliptic curves. Infinitely many (hyper)elliptic curves with 5-term and 8-term geometric progression sequences have been introduced in [4] and [1] respectively.

In [7], sequences of consecutive squares on elliptic curves were studied. Infinitely many elliptic curves defined by equations of the form $E : y^2 = ax^3 + bx + c$, $a, b, c \in \mathbb{Q}$, with 5-term sequences of consecutive squares were presented. This was achieved by identifying these curves as rational points on an elliptic surface whose rank is positive.

In this note, we discuss sequences of consecutive squares on elliptic curves defined by the equation $y^2 = ax^4 + bx^2 + c$, $a, b, c \in \mathbb{Q}$. We construct infinitely many such curves with 6-term sequences of consecutive squares. More precisely, given a 6-term sequence of consecutive squares, we prove the existence of an elliptic

2010 Mathematics Subject Classification: primary: 14G05; secondary: 11B83

curve on which the latter sequence forms the x-coordinates of six rational points. For the construction, we use an idea due to Mestre. This sequence corresponds to six linearly independent rational points on the elliptic curve. In particular, we give an infinite family of elliptic curves with 2-torsion points and rank $\geqslant 6$.

Finally, given a fixed 6-term sequence of consecutive squares $(t+i)^2$, $i = 0, \pm 1, \pm 2, 3$, we find infinitely many elliptic curves of the form $y^2 = ax^4 + bx^2 + c$ for which $(t+i)^2$ is an x-coordinate of a rational point. This is performed by realizing these elliptic curves as rational points on an elliptic surface of positive Mordell-Weil rank.

2. First construction

Let C be an elliptic curve defined over a number field K by $y^2 = P(x)$ where $P \in K[x]$ is a polynomial of degree either 3 or 4. 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 authors proved in [7] that this sequence must be finite.

Mestre, [9], constructed elliptic curves with Mordell-Weil rank $\geqslant 11$, using the following idea: For any monic polynomial $P \in \mathbb{Q}(x)$ of degree $2n$ there exists a monic polynomial $Q \in \mathbb{Q}(x)$ of degree n and $R \in \mathbb{Q}(x)$ of degree at most $n-1$ such that $P = Q^2 - R$. If $x \in \mathbb{Q}$ is a root of P, then there is a rational point $(x, Q(x))$ on the algebraic curve $y^2 = R(x)$.

Theorem 2.1. *For any nontrivial sequence of consecutive squares* $\left(t-\frac{5}{2}\right)^2$, $\left(t-\frac{3}{2}\right)^2$, $\left(t-\frac{1}{2}\right)^2$, $\left(t+\frac{1}{2}\right)^2$, $\left(t+\frac{3}{2}\right)^2$, $\left(t+\frac{5}{2}\right)^2$, *there is an elliptic curve described by*

$$E_t : y^2 = a(t)x^4 + b(t)x^2 + c(t), \qquad a, b, c \in \mathbb{Q}(t),$$

such that $(t+i)^2$, $i = \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}$, *is the* x*-coordinate of a rational point in* $E_t(\mathbb{Q}(t))$. *In particular, there are infinitely many elliptic curves described by* $y^2 = ax^4 + bx^2 + c$ *with* 6*-term sequences of consecutive squares.*

Proof. Consider the degree 12 polynomial

$$\begin{aligned} P(x) = &\left(x^2 - \left(t-\frac{5}{2}\right)^4\right)\left(x^2 - \left(t-\frac{3}{2}\right)^4\right)\left(x^2 - \left(t-\frac{1}{2}\right)^4\right) \\ &\times \left(x^2 - \left(t+\frac{1}{2}\right)^4\right)\left(x^2 - \left(t+\frac{3}{2}\right)^4\right)\left(x^2 - \left(t+\frac{5}{2}\right)^4\right). \end{aligned}$$

One may write $P(x) = Q(x)^2 - R(x)$, where

$$\begin{aligned}
Q(x) &= x^6 + \frac{1}{16}\Big(-48t^4 - 840t^2 - 707\Big)x^4 \\
&\quad + \frac{1}{256}\Big(768t^8 + 8960t^6 - 9184t^4 - 322000t^2 + 51331\Big)x^2 \\
&\quad + \frac{\begin{array}{r}-4096t^{12} + 71680t^{10} - 1994496t^8 - 50973440t^6 \\ - 251212528t^4 - 260162280t^2 - 50625\end{array}}{4096}, \\
R(x) &= 9t^2\Bigg\{\frac{1}{64}\Big(5376t^{10} + 779520t^8 + 11657184t^6 \\
&\quad + 57509200t^4 + 95561365t^2 + 36613360\Big)x^4 \\
&\quad - \frac{1}{512}\Big(86016t^{14} + 6113280t^{12} + 71158528t^{10} + 145053440t^8 \\
&\quad - 1767894864t^6 - 8757574840t^4 - 7679989163t^2 + 1441328880\Big)x^2 \\
&\quad + \frac{1}{16384}\Big(336t^6 + 11320t^4 + 54229t^2 + 56560\Big)\Big(4096t^{12} - 71680t^{10} \\
&\quad + 1220352t^8 + 24892160t^6 + 126268912t^4 + 129848040t^2 + 50625\Big)\Bigg\}.
\end{aligned}$$

We consider the elliptic curve $E_t : y^2 = R(x) := a(t)x^4 + b(t)x^2 + c(t)$. By definition of $P(x)$, the latter curve possesses the 6 rational points $\big((t+i)^2, Q((t+i)^2)\big)$, $i = \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}$. ∎

Using the rational transformation $x \mapsto x - (t - \frac{1}{2})^2$, the elliptic curve $E_t : y^2 = R(x) = a(t)x^4 + b(t)x^2 + c(t)$ may be described by an equation of the form $y^2 = A(t)\,x^4 + B(t)\,x^3 + C(t)\,x^2 + D(t)\,x + E(t)^2$. By virtue of [6, Proposition 1.2.1], the curve E_t is birationally equivalent, hence isomorphic, over $\mathbb{Q}(t)$ to the curve

$$E_t^* : T^2 = S(S^2 + \alpha(t)S + \beta(t))$$

which has a nontrivial 2-torsion point $(0, 0)$, where

$$\begin{aligned}
\alpha(t) &= \frac{9}{256}t^2\Big(86016t^{14} + 6113280t^{12} + 71158528t^{10} + 145053440t^8 \\
&\quad - 1767894864t^6 - 8757574840t^4 - 7679989163t^2 + 1441328880\Big), \\
\beta(t) &= -\frac{243t^4}{1024}\left(4t^2+17\right)\left(4t^2+33\right)\left(4t^2+97\right)\left(28t^2+151\right)\left(4t^3-48t^2+t-68\right) \\
&\quad \times \left(4t^3-24t^2+9t-26\right)\left(4t^3+24t^2+9t+26\right)\left(4t^3+48t^2+t+68\right) \\
&\quad \times \left(20t^3-24t^2+125t-10\right)\left(20t^3+24t^2+125t+10\right).
\end{aligned}$$

The rational points $(x_i, y_i) = ((t+i-\frac{5}{2})^2, Q((t+i-\frac{5}{2})^2))$, $i = 0,1,2,3,4,5$, on the curve E_t correspond to $q_i = (S_i, T_i)$ on the curve E_t^*, where

$$\begin{aligned}
S_i = &-\frac{1}{64\,(4t^2-4t+4x_i+1)^2}\Big\{-1024D(t)t^2+1024D(t)t-1024D(t)x\\
&-256D(t)-2048E^2(t)-2048E(t)y_i+3096576t^{19}-122978304t^{18}\\
&+6193152t^{17}x_i+687992832t^{17}-239763456t^{16}x_i-3489546240t^{16}\\
&+3096576t^{15}x_i^2+1134673920t^{15}x_i+12386571264t^{15}-116785152t^{14}x_i^2\\
&-5784477696t^{14}x_i-36507285504t^{14}+449777664t^{13}x_i^2+18704996352t^{13}x_i\\
&+84282105600t^{13}-2413264896t^{12}x_i^2-52863455232t^{12}x_i-186072109056t^{12}\\
&+6826788864t^{11}x_i^2+111024506880t^{11}x_i+294253225920t^{11}\\
&-19001622528t^{10}x_i^2-247903847424t^{10}x-482333956992t^{10}\\
&+34803933696t^9x_i^2+312846477696t^9x_i+595208516688t^9\\
&-84397584384t^8x_i^2-589845474432t^8x_i-578162334528t^8\\
&+63324671040t^7x_i^2+522359939520t^7x_i+478308410748t^7\\
&-210498670080t^6x_i^2-486503360928t^6x_i-249506322696t^6\\
&+34850131920t^5x_i^2+339523475688t^5x_i+37405300797t^5\\
&-155776881024t^4x_i^2-37863329472t^4x_i+25555102056t^4\\
&+5272323840t^3x_i^2-47933596800t^3x_i-12312919440t^3\\
&+25284879360t^2x_i^2+12642439680t^2x_i+1580304960t^2\Big\},\\
T_i = &\frac{1}{(4t^2-4t+4x_i+1)^3}\Big\{64B(t)E(t)t^6-192B(t)E(t)t^5+192B(t)E(t)t^4x_i\\
&+240B(t)E(t)t^4-384B(t)E(t)t^3x_i-160B(t)E(t)t^3+192B(t)E(t)t^2x_i^2\\
&+288B(t)E(t)t^2x_i+60B(t)E(t)t^2-192B(t)E(t)tx_i^2-96B(t)E(t)tx_i\\
&-12B(t)E(t)t+64B(t)E(t)x_i^3+48B(t)E(t)x_i^2+12B(t)E(t)x_i+B(t)E(t)\\
&+128C(t)E(t)t^4-256C(t)E(t)t^3+256C(t)E(t)t^2x_i+192C_i(t)E(t)t^2\\
&-256C(t)E(t)tx_i-64C(t)E(t)t+128C(t)E(t)x_i^2+64C(t)E(t)x_i\\
&+8C(t)E(t)+192D(t)E(t)t^2-192D(t)E(t)t+192D(t)E(t)x_i\\
&+48D(t)E(t)+64D(t)t^2y_i-64D(t)ty_i+64D(t)x_iy_i\\
&+16D(t)y_i+256E^3(t)+256E^2(t)y_i\Big\}.
\end{aligned}$$

Using MAGMA [2], the specialization $t = \frac{3}{4}$ shows that the rational points q_i, $i = 0,1,2,3,4,5$, on the elliptic curve E_t^* are independent. According to Silverman's Specialization Theorem, the curve E_t^* has rank $\geqslant 6$. Therefore, the above procedure yields an infinite family of elliptic curves with a 2-torsion point and rank at least 6.

3. Second construction

In this section, given a 6-term sequence of consecutive squares, we establish the existence of infinitely many elliptic curves C described by $y^2 = ax^4 + bx^2 + c$ over $\mathbb{Q}$ with this sequence making up the x-coordinates of rational points on C.

In fact, given $t \in \mathbb{Q}$ such that $((t-1)^2, d), (t^2, e)$, and $((t+1)^2, f)$ are rational points in $C(\mathbb{Q})$, where $C : y^2 = ax^4 + bx^2 + c$, one sees that

$$\begin{aligned} d^2 &= a(t-1)^8 + b(t-1)^4 + c \\ e^2 &= at^8 + bt^4 + c \\ f^2 &= a(t+1)^8 + b(t+1)^4 + c. \end{aligned}$$

The values of $a, b, c \in \mathbb{Q}[d, e, f](t)$ can be determined by solving the above system of linear equations.

Furthermore, if $((t-2)^2, g)$ is a fourth rational point in $C(\mathbb{Q})$, then the values of a, b, c yield that

$$\begin{aligned} g^2 = {} & \frac{3\left(8t^8 - 20t^7 + 36t^6 - 24t^5 + 2t^4 + 15t^3 + 9t^2 - 16t - 10\right) d^2}{t\left(8t^7 + 4t^6 + 8t^5 + 4t^4 + 2t^3 + t^2 + 2t + 1\right)} \\ & - \frac{3\left(4t^3 - 18t^2 + 28t - 15\right)\left(2t^4 - 2t^3 + 7t^2 - 2t + 5\right) e^2}{8t^7 + 4t^6 + 8t^5 + 4t^4 + 2t^3 + t^2 + 2t + 1} \\ & + \frac{\left(4t^3 - 18t^2 + 28t - 15\right)\left(2t^5 - 8t^4 + 15t^3 - 15t^2 + 8t - 2\right) f^2}{t\left(8t^7 + 4t^6 + 8t^5 + 4t^4 + 2t^3 + t^2 + 2t + 1\right)}. \end{aligned} \tag{1}$$

In the quadratic equation above, since $(d, e, f, g) = (1, 1, 1, 1)$ is a solution, one may find a parametric solution $(d, e, f, g) \in \mathbb{Q}[t][p, q, w]$.

Now in order for the elliptic curve $C : y^2 = ax^4 + bx^2 + c$ to possess a 5-term sequence of consecutive squares we assume the existence of the fifth rational point $((t+2)^2, h)$ in $C(\mathbb{Q})$. This will yield that

$$h^2 = Ap^4 + Bp^3 + Cp^2 + Dp + E, \qquad A, B, C, D, E \in \mathbb{Q}[t][q, w]. \tag{2}$$

The specialization

$$q = \frac{8\left(20t^6w - 54t^5w + 130t^4w - 219t^3w + 257t^2w - 132tw - 2w\right)}{3\left(48t^6 - 96t^5 + 420t^4 - 496t^3 + 756t^2 - 312t + 5\right)}$$

kills the discriminant of the the binary quartic (2). In other words, the algebraic curve defined by eq (2) is singular. More precisely, a parametric solution (p, h) can

be given by

$$\begin{aligned} h = & \frac{(t-1)(2t+1)\left(t^2-2t+2\right)\left(2t^2+2t+1\right)}{3(2t-1)^2\left(2t^2-2t+5\right)\left(12t^3-6t^2+60t-1\right)^2} \\ & \Big(9(2t-1)^2\left(2t^2-2t+5\right)^2\left(12t^3-6t^2+60t-1\right)^2p^2 \\ & -96t(2t-1)\left(t^2+4\right)\left(2t^2-2t+5\right)\left(4t^3-42t^2+4t-31\right) \\ & \times\left(12t^3-6t^2+60t-1\right)pw-(2t-3)\left(2t^2-6t+5\right) \\ & \times\Big(1088t^9+22944t^8+13680t^7+179048t^6+67104t^5+400204t^4 \\ & +110908t^3+211754t^2-2140t-15\Big)w^2\Big). \end{aligned}$$

We summarize our findings in the following proposition.

Proposition 3.1. *Given a nontrivial sequence of consecutive rational squares* $(t+i)^2$, $i=0,\pm1,\pm2$, *there exist infinitely many elliptic curves of the form* $C: y^2=a(t,p,w)x^4+b(t,p,w)x^2+c(t,p,w)$ *such that* $(t+i)^2$ *is the* x*-coordinate of a rational point on* C.

Now we are looking for elliptic curves containing 6-term sequences of consecutive squares. So we let $((t+3)^2,k)$ be a point in $C(\mathbb{Q})$ where C is given by $y^2=ax^4+bx^2+c$. Therefore, one has

$$k^2=\overline{A}p^4+\overline{B}p^3w+\overline{C}p^2w^2+\overline{D}pw^3+\overline{E}w^4 \tag{3}$$

where the description of $\overline{A},\overline{B},\overline{C},\overline{D},\overline{E}\in\mathbb{Q}(t)$ can be found, for instance, using MAGMA .

Theorem 3.2. *The curve* $\mathcal{C}: k^2=\overline{A}p^4+\overline{B}p^3+\overline{C}p^2+\overline{D}p+\overline{E}$ *defined over* $\mathbb{Q}(t)$ *is birationally equivalent over* $\mathbb{Q}(t)$ *to an elliptic curve* $\mathcal{E}$ *with Mordell–Weil rank* $\operatorname{rank}\mathcal{E}(\mathbb{Q}(t))\geqslant 1$.

Proof. The curve $\mathcal{C}$ is nonsingular as the discriminant is nonzero. Moreover, since $\overline{A}$ is a square in $\mathbb{Q}(t)$, one knows that $\mathcal{C}$ is an elliptic curve over $\mathbb{Q}(t)$. In fact, $\mathcal{C}$ is birationally equivalent to $\mathcal{E}$ defined by $y^2=x^3-27Ix-27J$ where $I=12\overline{A}\,\overline{E}-3\overline{B}\,\overline{D}+\overline{C}^2$ and $J=72\overline{A}\,\overline{C}\,\overline{E}+9\overline{B}\,\overline{C}\,\overline{D}-27\overline{A}\,\overline{D}^2-27\overline{B}^2\overline{E}-2\overline{C}^3$ with $P=\left(3\frac{3\overline{B}^2-8\overline{A}\,\overline{C}}{4\overline{A}},27\frac{\overline{B}^3+8\overline{A}^2\overline{D}-4\overline{A}\,\overline{B}\,\overline{C}}{8\overline{A}^{3/2}}\right)$ in $\mathcal{E}(\mathbb{Q}(t))$, see [10].

One considers the specialization $t=3$ in order to obtain the specialized point

$$\widetilde{P}=\left(\frac{19558022787408000000}{201601},\frac{864767547801187430400000000000}{90518849}\right)$$

of the point P on the specialized elliptic curve

$$\widetilde{\mathcal{E}} : y^2 = x^3 - \frac{15621778916298777453235200000000000}{40642963201}x + \frac{22789637573454810302335707893243904000000000000000000}{8193662024284801}.$$

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 $\mathcal{E}$. ■

Theorem 3.3. *For any 6-term nontrivial sequence of consecutive squares $(t+i)^2$, $i = 0, \pm 1, \pm 2, 3$, $t \in \mathbb{Q}$, there is an infinite family of elliptic curves described by $C : y^2 = ax^4+bx^2+c$, $a, b, c \in \mathbb{Q}$, such that $(t+i)^2$ is the x-coordinate of a rational point in $C(\mathbb{Q})$. In particular, there are infinitely many elliptic curves described by $y^2 = ax^4 + bx^2 + c$ with 6-term sequences of consecutive squares.*

Proof. Fix $t = t_0 \in \mathbb{Q}$. The values of a, b, c in $\mathbb{Q}[p, q, w]$ guarantees the existence of the points $((t-1)^2, d), (t^2, e), ((t+1)^2, f), ((t-2)^2, g)$ in $C(\mathbb{Q})$, where $d, e, f, g \in \mathbb{Q}[p, q, w]$. Choosing

$$q = \frac{8\left(20t^6w - 54t^5w + 130t^4w - 219t^3w + 257t^2w - 132tw - 2w\right)}{3\left(48t^6 - 96t^5 + 420t^4 - 496t^3 + 756t^2 - 312t + 5\right)}$$

yields the existence of a rational point $((t_0 + 2)^2, h)$ in $C(\mathbb{Q})$, see Proposition 3.1. Theorem 3.2 establishes the existence of infinitely many projective pairs $(p : w)$ for which $((t_0 + 3)^2, k)$ lies in $C(\mathbb{Q})$. ■

Acknowledgements. We would like to thank the referees for many comments, corrections, and suggestions that helped the authors improve the manuscript.

References

[1] M. Alaa and M. Sadek, *On geometric progressions on hyperelliptic curves*, J. Integer Seq. **19** (2016), Article 16.6.3.

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

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

[4] A. Bremner and M. Ulas, *Rational points in geometric progressions on certain hyperelliptic curves*, Publicationes Mathematica **82** (2013), 669–683.

[5] G. Campbell, *A note on arithmetic progressions on elliptic curves*, J. Integer Seq. **6** (2003), Article 03.1.3.

[6] I. Connell, *Elliptic curve handbook*, Montreal, McGill University, Preprint 1996.

[7] M. Kamel and M. Sadek, *On the sequence of consecutive squares on elliptic curves*, Glas. Mat. **52(72)** (2017), 45–52.

[8] A. J. MacLeod, *14-term arithmetic progressions on quartic elliptic curves*, J. Integer Seq. **9** (2006), Article 06.1.2.
[9] J.-F. Mestre, *Courbes elliptiques de rang* $\geqslant 11$ *sur* $\mathbb{Q}(t)$, C. R. Acad. Sci. Paris, Ser. A **313** (1991), 139–142.
[10] M. Stoll and J. E. Cremona, *Minimal models for 2-coverings of elliptic curve*, LMS J. Comput. Math. **5** (2002), 220–243.
[11] M. Ulas, *A note on arithmetic progressions on quartic elliptic curves*, J. Integer Seq. **8** (2005), Article 05.3.1.

Addresses: Mohamed Kamel: Department of Mathematics, Faculty of Science, Cairo University, Giza, Egypt;
Mohammad Sadek: American University in Cairo, Mathematics and Actuarial Science Department, AUC Avenue, New Cairo, Egypt.

E-mails: mohgamal@sci.cu.edu.eg, mmsadek@aucegypt.edu

Received: 19 February 2018