ELLIPTIC CURVES ARISING FROM THE TRIANGULAR NUMBERS

Abhishek Juyal
Harish-Chandra Research Institute, HBNI, Allahabad, India
abhinfo1402@gmail.com

Shiv Datt Kumar
Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, India
sdt@mnnit.ac.in

Dustin Moody
National Institute of Standards and Technology, Gaithersburg, Maryland
dustin.moody@nist.gov

Received: 8/27/18, Accepted: 1/1/19, Published: 2/1/19

Abstract

We study the Legendre family of elliptic curves $E_t : y^2 = x(x-1)(x-\Delta_t)$, parametrized by triangular numbers $\Delta_t = t(t+1)/2$. We prove that the rank of E_t over the function field $\overline{\mathbb{Q}}(t)$ is 1, while the rank is 0 over $\mathbb{Q}(t)$. We also produce some infinite subfamilies whose Mordell-Weil rank is positive, and find high rank curves from within these families.

1. Introduction and Main Result

The study of polygonal numbers is an ancient problem and has been widely studied. Among polygonal numbers, triangular numbers occupy a central place and they have drawn considerable attention from many researchers. For example, Legendre proved that a triangular number can never be a cube or a fourth power of an integer. As a second example, Gauss famously noted in his diary that every natural number can be expressed as a sum of at most three triangular numbers, and Euler proved that there are infinitely many squares among the triangular numbers and found all such numbers [1].

This brief paper is an attempt to establish some interesting connections between triangular numbers and elliptic curves. The specific curves belong to the Legendre family (see definition below), and are parameterized by triangular numbers. In this

context, we first begin with a brief review. Let Δ_t be the t^{th} triangular number, which is defined as the sum of the first t natural numbers:

$$\Delta_t = 1 + 2 + 3 + \cdots + t = \frac{t(t+1)}{2}.$$

For any field k with $\mathrm{char}(k) \neq 2$, an elliptic curve in Legendre form is one given by the equation

$$y^2 = x(x-1)(x-\lambda),$$

for some $\lambda \in k$, with $\lambda \neq 0, 1$. A Legendre curve always has three rational points of order two, namely the points $(0,0), (1,0)$, and $(\lambda, 0)$. Conversely, any elliptic curve E/k which has three rational points of order two can be given by an elliptic curve of the form $y^2 = x(x-\alpha)(x-\beta)$ with $\alpha, \beta \in k^*$. Investigating the possible transformations ([19, III, Sect. 1]) yields that E is isomorphic to a curve in Legendre form if and only if at least one of $\pm\alpha, \pm\beta, \pm(\alpha-\beta)$ is a square in k^*.

Over the years, several authors have given considerable effort to study the ranks of certain families of Legendre curves with connections to other interesting areas. In [8], the authors showed that there exist infinitely many Pythagorean triples (a, b, c) for which the rank of the family

$$E_{a,b} : y^2 = x(x-a^2)(x-b^2)$$

is positive. Naskręcki, Izadi, and Nabardi continued in this line and showed constructions of families with rank at least two [7, 12]. Other researchers have looked at congruent number curves [4, 14, 15], or families of Legendre curves associated to Heron and Brahmagupta quadrilaterals [5, 6]. It is conjectured that there exist elliptic curves with arbitrarily high rank, although the highest known rank is 28. On the other hand, it has also been conjectured that the rank is absolutely bounded, with only finitely many elliptic curves of rank greater than 21 [13]. Restricting to Legendre curves, the record is 15 for an individual curve and 8 for an infinite family (all these records are due to Elkies [2, 3]).

We will set $\lambda = \Delta_t$, and define the main object of study as the family of elliptic curves

$$E_t : y^2 = x(x-1)(x-t(t+1)/2),$$

parametrized by the triangular numbers. We extend the definition of Δ_t to allow for rational values of t. As far as we can tell, this is the first time triangular numbers have been used to define a family of elliptic curves. Other papers relating triangular numbers and elliptic curves have tended to prove properties about triangular numbers using elliptic curve techniques [1].

The main result of this paper is the following. Our approach is similar to [21].

Theorem 1. *Let E_t be an elliptic curve over $\mathbb{Q}(t)$ given by the equation*

$$E_t : y^2 = x(x-1)(x-t(t+1)/2).$$

Then

(i) The associated elliptic surface (denoted $\mathcal{E}$) is rational.

(ii) The rank of $E_t(\overline{\mathbb{Q}}(t))$ is 1, with $(x,y) = (-t/2, t(t+2)/(2\sqrt{-2}))$ being a generator of the free part of the group $E_t(\overline{\mathbb{Q}}(t))$.

(iii) The rank of $E_t(\mathbb{Q}(t)) = 0$.

(iv) The torsion subgroup of $E_t(\mathbb{Q}(t))$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

In Section 2, we will introduce the notion of elliptic surfaces and certain results necessary for the proof of Theorem 1. We then give the detailed proof of Theorem 1 in Section 3, and construct infinite families of the curves E_t with positive rank in Section 4. We conclude in Section 5 by giving some examples of specific curves E_t with high rank, and end with directions for further study.

2. Elliptic Surfaces

Definition. Let C be a smooth, irreducible projective curve over an algebraically closed field k. An elliptic surface over C is a pair (S, f), where S is a smooth, irreducible, projective surface over k, and $f : S \longrightarrow C$ is a relatively minimal elliptic fibration having a singular fiber and a zero section. We often write $f : S \longrightarrow C$ to denote the elliptic surface (S, f) over C.

Let $k(C)$ denote the function field of the curve C. Given an elliptic curve E over $k(C)$, one can associate an elliptic surface $f : \mathcal{E} \longrightarrow C$ with generic fiber E, the existence and uniqueness of which is guaranteed by the work of Kodaira and Néron. This elliptic surface is known as the Kodaira-Néron model of the elliptic curve E over $k(C)$.

Given that all the relevant results needed to prove our main theorem are well known, we just give their statements and omit their proofs.

Theorem 2 (Corollary 2.2, [17]). *Let (S, f) be an elliptic surface over C. The Néron-Severi group, denoted $NS(S)$, is finitely generated and torsion-free.*

Recall the classical Shioda-Tate formula.

Theorem 3 (Corollary 5.3, [17]). *Let (S, f) be an elliptic surface over C. For each point v of C having singular fiber, let m_v denote the number of components of the singular fiber above v. Let E denote the generic fiber of S. The rank of the Néron-Severi group of S, denoted $\rho(S)$, can be obtained from the equality*

$$\rho(S) = \text{rank E(k(C))} + 2 + \sum_{\text{v}} (\text{m}_\text{v} - 1),$$

where the summation ranges over the the points of C under singular fibers.

We also need the following lemma.

Lemma 1 (Theorem IV.8.2, [20] and Corollary 7.5, [18]). *Let E be an elliptic curve over $\overline{\mathbb{Q}}(t)$. Let $\Sigma \subset \mathbb{P}^1(\overline{\mathbb{Q}}(t))$ be the set of points of bad reduction of E. Let $G(F_v)$ denote the group generated by simple components of the fiber F_v at $v \in \Sigma$. There exists an injective homomorphism*

$$\phi : E(\overline{\mathbb{Q}}(t))_{tors} \longrightarrow \prod_{v \in \Sigma} G(F_v).$$

If F_v is of multiplicative type I_n in Kodaira notation, the corresponding group is $\mathbb{Z}/n\mathbb{Z}$. If F_v is of additive type I_{2n}^*, the group is $(\mathbb{Z}/2\mathbb{Z})^2$.

3. Proof of Main Theorem

In this section, we give the proof of Theorem 1.

Proof. The elliptic curve E_t over $\mathbb{Q}(t)$ can be written in short Weierstrass form as

$$y^2 = x^3 + A(t)x + B(t),$$

where

$$A(t) = -\frac{4}{3}(t^4 + 2t^3 - t^2 - 2t + 4),$$

$$B(t) = -\frac{16}{27}(t^6 + 3t^5 - 5t^3 - 9t^2 - 6t + 8).$$

The discriminant of E_t is given by

$$\Delta(t) = -256t^2(t-1)^2(t+1)^2(t+2)^2.$$

We now prove each of the parts of the theorem.

(i) Given an elliptic curve

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

over $\mathbb{Q}(t)$ in long Weierstrass form, we know from [17, Equation 10.14] that if $\deg(a_i(t)) \leq i$ for each i, then the associated elliptic surface $\mathcal{E}$ is rational. In our case, since $\deg(A(t)) = 4$ and $\deg(B(t)) = 6$, therefore the underlying elliptic surface is rational.

(ii) From the expression of the discriminant of E_t, we see that E_t has singular fibers at the values $t = 0, -2, \pm 1$, and ∞. We determine the numbers m_v, of irreducible components of the fiber over v, from Kodaira types of singular fibers [10, section 4]:

v	coefficients				
	$ord_{t=v}(A)$	$ord_{t=v}(B)$	$ord_{t=v}(\Delta)$	Kodaira type	$m_v - 1$
0	0	0	2	I_2	1
-2	0	0	2	I_2	1
-1	0	0	2	I_2	1
1	0	0	2	I_2	1
∞	0	0	4	I_4	3

Since $\mathcal{E}$ is a rational surface, we have $\rho(\mathcal{E}) = 10$. Thus by Theorem (3) we get,

$$10 = \text{rank } \mathrm{E_t}(\overline{\mathbb{Q}}(\mathrm{t})) + 2 + 1 + 1 + 1 + 1 + 3,$$

and hence rank $\mathrm{E_t}(\overline{\mathbb{Q}}(\mathrm{t})) = 1$.

The group $E_t(\overline{\mathbb{Q}}(t))$ is generated with the points of the form $(a_2T^2 + a_1T + a_0,\ b_3T^3 + b_2T^2 + b_1T + b_0),\ a_i, b_i \in \overline{\mathbb{Q}}$ (see [17, Equation 10.14]). A straightforward calculation shows that the point $P = (-t/2, t(t+2)/(2\sqrt{-2}))$ is a generator of $E_t(\overline{\mathbb{Q}}(t))$.

(iii) This part's proof follows the idea in Corollary 6.3 of [12]. Since rank $\mathrm{E_t}(\overline{\mathbb{Q}}(\mathrm{t})) = 1$, then necessarily rank $\mathrm{E_t}(\mathbb{Q}(\mathrm{t})) \leq 1$. We claim that rank $\mathrm{E_t}(\mathbb{Q}(\mathrm{t})) = 0$. On the contrary, assume that rank $\mathrm{E_t}(\mathbb{Q}(\mathrm{t})) = 1$. Then $H = E_t(\mathbb{Q}(t))$ is a finite indexed subgroup of $G = E_t(\overline{\mathbb{Q}}(t))$, and $G_{\mathbb{Q}} = H_{\mathbb{Q}}$, where $G_{\mathbb{Q}} = G \otimes_{\mathbb{Z}} \mathbb{Q}$ and $H_{\mathbb{Q}} = H \otimes_{\mathbb{Z}} \mathbb{Q}$ are one dimensional vector spaces over $\mathbb{Q}$.

We have a canonical Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{G}_{\mathbb{Q}}^{\times} = \mathrm{Aut}(\mathrm{G}_{\mathbb{Q}})$$

which is defined as follows. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $g \in G$, we define $\sigma(g\otimes 1) = \sigma(g)\otimes 1$, where $\sigma(g)$ is obtained by the action of σ on the coefficients of rational functions in the coordinates of g. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the element such that $\sigma(\sqrt{-1}) = -\sqrt{-1}$ and $\sigma(\sqrt{2}) = \sqrt{2}$. Then we get $\sigma(P \otimes 1) = -(P \otimes 1)$. Therefore ρ is a non-trivial character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Clearly ρ acts trivially on $H_{\mathbb{Q}}$ which is a contradiction as $G_{\mathbb{Q}} = H_{\mathbb{Q}}$.

(iv) By Lemma 1 and the table in the proof of (ii) above, we see that the torsion subgroup of $E_t(\overline{\mathbb{Q}}(t))$ is embedded in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$. From the well-known specialization theorem [20], the specialization homomorphism is injective on the torsion. Specializing at $t = 3$, the curve is $E_3 : y^2 = x^3 - 7x^2 + 6x$. The torsion group of E_3 is easily computed to be $\mathbb{Z}_2 \times \mathbb{Z}_2$. We have exactly three 2-torsion points, namely $(0, 0), (1, 0)$ and $(t(t + 1)/2, 0)$, on the elliptic curve E_t. Since these 2-torsion points are also the points of $E_t(\mathbb{Q}(t))$, it implies that $E_t(\mathbb{Q}(t))_{tors} = \mathbb{Z}_2 \times \mathbb{Z}_2$.

□

4. Infinite Families With Positive Rank

4.1. Rank 1 Families

In this section we construct infinite families of the curve E_t which have positive rank. We first construct a couple of subfamilies of rank (at least) 1, followed by a family with rank (at least) 2.

In order to construct a subfamily of rank one, we consider the right hand side of the curve $y^2 = x(x - 1)(x - t(t + 1)/2)$ as a polynomial in t. The coefficient of t^2 is $-x(x - 1)/2$. Putting

$$-x(x - 1)/2 = m^2,$$

we can rewrite the equation E_t as $(y - mt)(y + mt) = m^2t - 2m^2x$. Now writing $y-mt = p$, we get $p(y+mt) = m^2t-2m^2x$. These two equations may be considered as two linear equations in y and t, and solving we find

$$t = \frac{p^2 + 2m^2x}{m(m - 2pm)}, \quad y = \frac{-p^2 + 2m^2x + pm}{m - 2p}.$$

We divide both the numerator and denominators by m^2, and setting $p/m = g,\ x = 2/(h^2 + 2)$, and $m = h/(h^2 + 2)$, we obtain

$$t(g, h) = -\frac{(h^2g^2 + 2g^2 + 4)}{(h^2 + 2)(2g - 1)},$$

for which the point

$$(x,y)=\left(\frac{2}{h^2+2},\ \frac{h(h^2g^2-gh^2+2g^2-2g-4)}{(h^2+2)^2(2g-1)}\right)$$

always lies on the elliptic curve

$$y^2=x(x-1)(x-t(g,h))(x-(t(g,h)+1)/2).$$

Specialization at $(g,h)=(1,1)$ yields the curve $E_{t(1,1)}: y^2=x^3-\frac{23}{9}x^2+\frac{14}{9}x$, which has rank 1 over $\mathbb{Q}$, with the point $(2/3,-4/9)$ of infinite order. Since the specialization map [20, Theorem 11.4] is a homomorphism, this implies that the rank of the curve is at least 1 over $\mathbb{Q}(g,h)$.

It is not hard to find other families with rank at least one. For example, if we set $t=4/(m^2+2)$, then the point with x-coordinate $t+1$ is rational and has infinite order. Similarly, if we set $t=(m^2+1152)/(8m^2+1024)$, or $t=(6-3m^2)/(m^2+2)$ yields curves with a point of infinite order given by the x-coordinate $x=t-1/8$, $x=t+3$ respectively. For a more general construction, setting

$$t=\frac{(2c-1)m^2+2c}{m^2+2c^2}$$

then the point with x-coordinate $x=ct$ will be rational and have infinite order.

4.2. A Subfamily of Rank Two

To construct a family with rank (at least) two, we begin by forcing the point with x-coordinate $x=-2t-2$ to be rational. This requires that the expression $-(t+4)(2t+3)$ be square. We can parameterize

$$t=-\frac{4m^2+3}{m^2+2},$$

to ensure the expression is square. It can be checked that this point has infinite order via specialization. We then try to increase the rank by forcing the point with x-coordinate $x=(t+4)/5$ to be rational. Some simple algebra shows this condition is equivalent to requiring that $(12m^2-1)/2$ is square. We therefore set

$$m=-\frac{k^2+8k+24}{2k^2-48}.$$

Substituting back in, we find that

$$t=-16\frac{k^4+4k^3-8k^2+96k+576}{(9k^2+88k+216)(k^2-8k+24)},$$

with the two points having x-coordinates $x_1(t)=-2t-2$ and $x_2(t)=(t+4)/5$.

It is easy to show via specialization that these points are independent and have infinite order. Indeed, for $k = 4$ then $t = -336/89$, with points $P_1 = (494/89, 22230/7921)$ and $P_2 = (4/89, 3740/7921)$. As verified by SAGE [16], both P_1 and P_2 have infinite order (which is easy to see since the torsion group is $\mathbb{Z}_2 \times \mathbb{Z}_2$). The determinant of the height pairing matrix for P_1 and P_2 is $6.94053525377041 \neq 0$, which implies the points are independent. In fact, the curve E_t has rank 2, and P_1 and P_2 can be shown to be generators. We thus have constructed an infinite family with rank (at least) two.

It is possible to construct other families with rank (at least) 2 by using the above technique, with different x-coordinates. We note that we attempted to find a rank 3 subfamily, but were unsuccessful.

5. Examples of Elliptic Curves of High Rank

We searched for curves with high rank, and were able to find some elliptic curves of rank 6 in the family E_t. We use the sieving method based on Mestre-Nagao sums ([9], [11]). Let $E/\mathbb{Q}$ be an elliptic curve, and p be a prime. Set $a_p = a_p(E) = p + 1 - |E(\mathbf{F_p})|$. Given a fixed integer N, the Mestre-Nagao sum is defined by

$$S(N, E) = \sum_{\text{primes } p \leq N} \left(1 - \frac{p-1}{|E(\mathbf{F_p})|}\right) \log(p) = \sum_{\text{primes } p \leq N} \frac{-a_p + 2}{p + 1 - a_p} \log(p).$$

It has been conjectured that in general, larger values of $S(N, E)$ tend to correspond to curves with high rank. Provided N is not too large, $S(N, E)$ can be calculated using SAGE [16].

Searching through the curves E_t with $t = t_1/t_2$ with $-10000 \leq t_1 \leq 10000, 1 \leq t_2 \leq 10000$, we found that for the curves with $S(523, E) > 20$, the rank was frequently 3 or 4. In the above range, we found only one curve with rank 6, which occurred for $t = 2961/3116$. Concretely, the elliptic curve

$$y^2 = x^3 - 74825818x^2 + 1397695377085056x,$$

which has generators:

$P_1 = (39037824, 4879728000)$,

$P_2 = (86307147531/2209, 549837626486445/103823)$,

$P_3 = (139324262094/3481, 2843260991496900/205379)$,

$P_4 = (1023658496/25, 2586273190144/125)$,

$P_5 = (1364049981504/32041, 185551816648665600/5735339)$,

$P_6 = (45163475, 51198909265)$.

There were several values of $t = t_1/t_2$ which correspond to curves E_t which have rank 5. See Table 1 below.

rank	$t = t_1/t_2$
5	324/965, 1572/1390, 1602/935, 1696/801, 1984/619, 1142/2192, 1360/2043, 1558/1771, 1817/3029, 2135/2614, 2143/3034, 2408/3005, 2578/2761, 2631/2255, 2697/2910, 2817/2712, 3048/2345, 5057/5215, 5156/5522, 5232/5597, 5394/5820, 5634/5424, 5635/5289, 5178/6806, 5331/6499, 2512/1513, 5081/3497, 10177/6255.

Table 1: Rank 5 curves

We similarly searched the other families given in Section 4. For the rank 1 family, we did not find any additional rank 5 or 6 curves. For the family described in Section 4.2, we found curves of rank 5 for $k = -23/12, -15/7$ (corresponding to $t = -115438864/71696361$ and -1345744/838881), and rank 6 for $k = 20, 7/3$ (corresponding to $t = -47824/23001$ and $= -1084624/410601$ respectively).

6. Conclusion

One can easily prove that a similar result is true for any polygonal number. If s is the number of sides in a polygon, the formula for the n^{th} s-gonal number $P(s, n)$ is

$$P(s, n) = (s - 2)\frac{n(n-1)}{2} + n.$$

The case $s = 2$ corresponds to Legendre curves, while the case $s = 3$ are the triangular number curves treated in this paper. When $s = 4$, then $P(4, n) = n^2$, with the related curve family $y^2 = x(x - 1)(x - n^2)$ closely related to the works mentioned earlier involving Pythagorean triples [7], [8], [12]. It would be interesting to further examine the elliptic curves that arise from other polygonal numbers.

Acknowledgement. The authors would like to thank the referee for carefully reading the paper and for his/her helpful comments. The first author sincerely thanks Prof. Andrew Bremner and Pradeep Das for some fruitful discussion and Prof. Ajai Choudhry for his help in getting the parametrization used to construct the first subfamily of rank 1. The first author also thanks the Harish-Chandra Research Institute, Allahabad, for providing research facilities to pursue his research work

and is indebted to his co-supervisor Prof. Kalyan Chakraborty for his continuous support and encouragement.

References

[1] J. S. Chahal and J. Top, Triangular numbers and elliptic curves, *Rocky Mountain J. Math.*, **26** (3), (1996), 937–949.

[2] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/~duje/tors/tors.html` (accessed January 2018).

[3] A. Dujella, Infinite families of elliptic curves with high rank and prescribed torsion, `https://web.math.pmf.unizg.hr/~duje/tors/generic.html` (accessed January 2018).

[4] A. Dujella, A. S. Janfada, S. Salami, A search for high rank congruent number elliptic curves, *J. Integer Seq.*, **12** (2009), Article 09.5.8.

[5] F. Izadi, F. Khoshnam, D. Moody, Heron quadrilaterals via elliptic curves, *Rocky Mountain J. Math.*, **47** (4), (2017) 1227-1258.

[6] F. Izadi, F. Khoshnam, D. Moody, A. S. Zargar, Elliptic curves arising from Brahmagupta quadrilaterals, *Bull. Aust. Math. Soc.* **90** (01) (2014) 47-56.

[7] Farzali Izadi and Kamran Nabardi, Elliptic curves and Pythagorean triples, *Eur. J. Pure Appl. Math.*, **7** (2), (2014), 131-139.

[8] F. A. Izadi, K. Nabardi, F. Khoshnam, A new family of elliptic curves with positive rank arising from Pythagorean triples, *ArXiv e-prints (2010), arXiv:1012.5837v4.*

[9] J.F. Mestre, Construction de courbes elliptiques sur $\mathbb{Q}$ de rang ≥ 12, *C. R. Acad. Sci. Paris Ser. I*, **295** (1982), 643–644.

[10] R. Miranda, "*An overview of algebraic surfaces, in: Algebraic Geometry* (Ankara,1995)", Lecture Notes in Pure and Appl. Math. 193, Dekker, New York, 1997, 197–217.

[11] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20, *Proc. Japan Acad. Ser. A Math. Sci.* **69** (1993), 291–293.

[12] B. Naskręcki, Mordell-weil ranks of families of elliptic curves associated to Pythagorean triples, *Acta Arith.* **160**: (2013), 159–183.

[13] J. Park, B. Poonen, J. Voight, M. M. Wood, A heuristic for boundedness of ranks of elliptic curves, *ArXiv e-prints (2017), arXiv:1602.01431v2.*

[14] N. F. Rogers, Rank computations for the congruent number elliptic curves, *Exp. Math.*, **9** (2000), no. 4, 591-594.

[15] K. Rubin, and A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, *Exp. Math.* **10** (2001), no. 4, 559-569.

[16] SAGE software, Version 4.5.3 `http://www.SAGEmath.org`.

[17] T. Shioda, On the Mordell-Weil lattices, *Comment. Math. Univ. St. Pauli*, **39** (1990), 211–240.

[18] T. Shioda, M. Schütt, Elliptic surfaces. Algebraic geometry in East Asia-Seoul 2008, 51–160, *Adv. Stud. Pure Math.*, **60**, *Math. Soc. Japan, Tokyo*, 2010.

[19] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, (1986).

[20] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics*, **151** Springer-Verlag, New York (1994).

[21] P. Tadić, On the family of elliptic curves $Y^2 = X^3 - T^2X + 1$, *Glas. Mat. Ser. III* **47** (67) (2012), 81–93.