involve

a journal of mathematics

A family of elliptic curves of rank ≥ 4

Farzali Izadi and Kamran Nabardi

msp

2016 vol. 9, no. 5

INVOLVE 9:5 (2016)
dx.doi.org/10.2140/involve.2016.9.733

A family of elliptic curves of rank ≥ 4

Farzali Izadi and Kamran Nabardi

(Communicated by Ken Ono)

In this paper we consider a family of elliptic curves of the form $y^2 = x^3 - c^2 x + a^2$, where (a, b, c) is a primitive Pythagorean triple. First we show that the rank is positive. Then we construct a subfamily with rank ≥ 4.

1. Introduction

As is well known, an elliptic curve E over a field $\mathbb{K}$ can be explicitly expressed by the generalized Weierstrass equation of the form

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. In this paper we are interested in the case where $\mathbb{K} = \mathbb{Q}$. By the Mordell–Weil theorem [Washington 2008], every elliptic curve over $\mathbb{Q}$ has a commutative group $E(\mathbb{Q})$ which is finitely generated, i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$, where r is a nonnegative integer and $E(\mathbb{Q})_{\text{tors}}$ is the subgroup of elements of finite order in $E(\mathbb{Q})$. This subgroup is called the torsion subgroup of $E(\mathbb{Q})$ and the integer r is called the rank of E and is denoted by rank E.

By Mazur's theorem [Silverman and Tate 1992], the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. Besides, it is not known which values of rank r are possible. The folklore conjecture is that a rank can be arbitrarily large, but it seems to be very hard to find examples with large ranks. The current record is an example of an elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found by Elkies in May 2006 (see [Dujella 2012]). Having classified the torsion part, one is interested in seeing whether or not the rank is unbounded among all the elliptic curves. There is no known guaranteed algorithm to determine the rank and it is not known which integers can occur as ranks.

Specialization is a significant technique for finding a lower bound for the rank of a family of elliptic curves. One can consider an elliptic curve on the rational function field $\mathbb{Q}(T)$ and then obtain elliptic curves over $\mathbb{Q}$ by specializing the variable T to suitable values $t \in \mathbb{Q}$ (see [Silverman 1994, Chapter III, Theorem 11.4] for more

MSC2010: primary 11G05; secondary 14H52, 14G05.
Keywords: elliptic curves, rank, Pythagorean triple.

details). Using this technique, Nagao and Kouya [1994] found curves of rank ≥ 21, and Fermigier [1996] obtained a curve of rank ≥ 22.

In order to determine r, one should find the generators of the free part of the Mordell–Weil group. Determining the *associated height matrix* is a useful technique for finding a set of generators. In the following, we briefly describe it.

Let $m/n \in \mathbb{Q}$, where $\gcd(m, n) = 1$. Then the *height* of m/n is defined by

$$h\Big(\frac{m}{n}\Big) = \log\big(\max\{|m|, |n|\}\big).$$

Corresponding to $P = (x, y) \in E(\mathbb{Q})$, we define

$$H(P) = h(x) \quad \text{and} \quad \hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} \frac{H(2^N \cdot P)}{4^N},$$

where $H(P)$ is called the *canonical height* of $P \in E(\mathbb{Q})$. The Néron–Tate pairing to an elliptic curve is defined by

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}, \quad \langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

The *associated height matrix* to $\{P_i\}_{i=1}^r$ is

$$\mathcal{H} := \big(\langle P_i, P_j\rangle\big)_{1\leq i\leq r,\, 1\leq j\leq r}.$$

If $\det \mathcal{H} \neq 0$, then the points $\{P_i\}_{i=1}^r$ are linearly independent and $\operatorname{rank} E(\mathbb{Q}) \geq r$ (see[Silverman 1994, Chapter III] for more details and proofs).

In this work we deal with a family of elliptic curves which are related to the Pythagorean triples and, by using both the specialization and, the associated height matrix techniques, prove the following theorem.

Main Theorem 1.1. *Let (a, b, c) be a primitive Pythagorean triple. Then, there are infinitely many elliptic curves of the form*

$$E : y^2 = x^3 - c^2 x + a^2 \tag{1-1}$$

with rank ≥ 4.

If (a, b, c) is a primitive Pythagorean triple, then one can easily check that $a = i^2 - j^2$, $b = 2ij$, and $c = i^2 + j^2$, where $\gcd(i, j) = 1$, and i, j have opposite parity. So, we can consider (1-1) as

$$E_{i,j} : y^2 = x^3 - (i^2 + j^2)^2 x + (i^2 - j^2)^2. \tag{1-2}$$

It is clear that two points $P_{i,j} = (0,\ i^2 - j^2)$ and $Q_{i,j} = (i^2 + j^2,\ i^2 - j^2)$ are on (1-2) and so $\operatorname{rank} E_{i,j} > 0$. In the next section, we construct a subfamily with rank ≥ 3.

2. A subfamily with rank ≥ 3

First, we look at (1-2) as a one-parameter family by letting

$$a = t^2 - 1, \quad b = 2t, \quad c = t^2 + 1, \tag{2-1}$$

where $t \in \mathbb{Q}$. Then, instead of (1-2) one can take

$$E_t : y^2 = x^3 - (t^2+1)^2 x + (t^2-1)^2, \quad t \in \mathbb{Q}. \tag{2-2}$$

Lemma 2.1. *There are infinitely many elliptic curves of the form (2-2) with rank* ≥ 3.

Proof. Clearly we have two points

$$P_t = (0,\ t^2-1), \quad Q_t = (t^2+1,\ t^2-1). \tag{2-3}$$

We impose another point in (2-2) with x-coordinate 1. This implies $1-4t^2$ is a square, say v^2. Then $1-4t^2 = v^2$ defines a circle of the form $(2t)^2+v^2 = 1$. Hence

$$t = \frac{\alpha}{\alpha^2+1}, \quad v = \frac{\alpha^2-1}{\alpha^2+1}, \tag{2-4}$$

with $\alpha \in \mathbb{Q}$. Then, instead of (2-2), one can take

$$E_\alpha : y^2 = x^3 - \left(\left(\frac{\alpha}{\alpha^2+1}\right)^2+1\right)^2 x + \left(\left(\frac{\alpha}{\alpha^2+1}\right)^2-1\right)^2, \tag{2-5}$$

having three points

$$P_\alpha = \left(0,\ \left(\frac{\alpha}{\alpha^2+1}\right)^2-1\right), \quad Q_\alpha = \left(\left(\frac{\alpha}{\alpha^2+1}\right)^2+1,\ \left(\frac{\alpha}{\alpha^2+1}\right)^2-1\right), \quad R_\alpha = \left(1,\ \frac{\alpha^2-1}{\alpha^2+1}\right).$$

When we specialize to $\alpha = 2$, we obtain a set of points $S = \{P_2, Q_2, R_2\} = \left\{\left(0, \tfrac{-21}{25}\right), \left(\tfrac{29}{25}, \tfrac{-21}{25}\right), \left(1, \tfrac{3}{5}\right)\right\}$ on

$$E_2 : y^2 = x^3 - \tfrac{841}{25}x + \tfrac{44}{25}. \tag{2-6}$$

Using SAGE, one can easily check that the associated height matrix of S has nonzero determinant $\approx 22.879895 \neq 0$ showing that these three points are independent and so rank $E_2 \geq 3$. The specialization result of Silverman [1994] implies that for all but finitely many rational numbers, rank $E_\alpha \geq 3$. □

3. Proof of the main theorem

We impose another point with x-coordinate $-2\alpha/(\alpha^2+1)$ in (2-5). Hence we want $1+2\alpha/(\alpha^2+1)$ to be a square. It suffices that α^2+1 is a square, say β^2. Therefore,

$$\alpha = \frac{2m}{1-m^2}, \quad \beta = \frac{m^2+1}{1-m^2}, \tag{3-1}$$

where $m \in \mathbb{Q}$. From the above expressions, one can transform (2-5) to

$$E_m : y^2 = x^3 - \frac{(m^8+8m^6-2m^4+8m^2+1)^2}{(2m^2+m^4+1)^4}x + \frac{(m^8+14m^4+1)^2}{(2m^2+m^4+1)^4}. \tag{3-2}$$

So we get the four points

$$P_m=(0,\,\gamma),\qquad Q_m=\left(\frac{m^8+8m^6-2m^4+8m^2+1}{(m^2+1)^4},\,\gamma\right),$$

$$R_m=\left(1,\,\frac{(m^2-2m-1)(m^2+2m-1)}{(m^2+1)^2}\right),\qquad S_m=\left(\frac{4m(m^2-1)}{m^4+2m^2+1},\,\frac{(m^2-2m-1)}{m^2+1}\gamma\right),$$

where

$$\gamma=\frac{(m^4-2m^3+2m^2+2m+1)(m^4+2m^3+2m^2-2m+1)}{(m^2+1)^4}.$$

By specialization to $m=2$ in (3-2), we have

$$E_2 : y^2=x^3-\tfrac{591361}{390625}x+\tfrac{231361}{390625}, \tag{3-3}$$

and the set of points $S=\{P_2,Q_2,R_2,S_2\}=\bigl\{\bigl(0,\frac{481}{625}\bigr),\bigl(\frac{769}{625},\frac{481}{625}\bigr),\bigl(1,\frac{7}{5}\bigr),\bigl(\frac{24}{25},\frac{481}{3125}\bigr)\bigr\}$ on it. The associated height matrix of these four points has nonzero determinant $\approx 722.7181\neq 0$ showing that these points are independent and so rank $E_2\geq 4$. However, by using SAGE we see that rank $E_2=5$. Again, by specialization, we can conclude that for all but finitely many elliptic curves of the form (3-2), we have rank ≥ 4.

Acknowledgements

The authors express their hearty thanks to the anonymous referee for a careful reading of the paper and for many comments and remarks which improved its quality.

References

[Dujella 2012] A. Dujella, "High rank elliptic curves with prescribed torsion", 2012, available at https://web.math.pmf.unizg.hr/~duje/tors/tors.html.

[Fermigier 1996] S. Fermigier, "Construction of high-rank elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$ with non-trivial 2-torsion (extended abstract)", pp. 115–120 in *Algorithmic number theory* (Talence, 1996), edited by H. Cohen, Lecture Notes in Computer Science **1122**, Springer, Berlin, 1996. MR 1446503 Zbl 0890.11020

[Nagao and Kouya 1994] K.-I. Nagao and T. Kouya, "An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 21", *Proc. Japan Acad. Ser. A Math. Sci.* **70**:4 (1994), 104–105. MR 1276883 Zbl 0832.14022

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 1312368 Zbl 0911.14015

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, New York, NY, 1992. MR 1171452 Zbl 0752.14034

[Washington 2008] L. C. Washington, *Elliptic curves: number theory and cryptography*, 2nd ed., Chapman and Hall, Boca Raton, FL, 2008. MR 2404461 Zbl 1200.11043

Received: 2014-05-07 Revised: 2015-09-30 Accepted: 2015-10-01

f.izadi@urmia.ac.ir *Department of Mathematics, Urmia University, Urmia, Iran*

nabardi@azaruniv.edu *Department of Mathematics,*
Azarbaijan Shahid Madani University, Tabriz, Iran

mathematical sciences publishers msp

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 5