Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 25, 2019, No. 4, 24–29
DOI: 10.7546/nntdm.2019.25.4.24-29

A family of elliptic curves of rank ≥ 5 over $\mathbb{Q}(m)$

Arman Shamsi Zargar[1] **and Naser Zamani**[2]

[1] Department of Mathematics and Applications, Faculty of Science
University of Mohaghegh Ardabili, Ardabil 56199-11367, Iran
e-mail: zargar@uma.ac.ir

[2] Department of Mathematics and Applications, Faculty of Science
University of Mohaghegh Ardabili, Ardabil 56199-11367, Iran
e-mail: naserzaka@yahoo.com

Received: 16 February 2019 **Revised:** 28 October 2019 **Accepted:** 1 November 2019

Abstract: We construct a subfamily of elliptic curves $E(r,s) : (y-s)(y+s) = x(x-r)(x+r)$ with $r = 2(m^4 - 2m^3 + 2m^2 + 2m + 1)$, $s = 2(m^2 - 2m - 1)(m^2 + 1)^2$, and show that its rank is at least five over $\mathbb{Q}(m)$. This improves the previous results on the rank of the curves $E(r,s)$ over $\mathbb{Q}(m)$.
Keywords: Elliptic curves, Independence, Rank, Torsion subgroup.
2010 Mathematics Subject Classification: 11G05, 14H52.

1 Introduction

In the literature one can find numerous results on the construction of an infinite family of elliptic curves over the rational numbers whose rank is at least r. Recall that the highest record is $r = 28$, due to N. Elkies. It has been conjectured that there is no upper bound on r, but there is some evidence to suggest that probably there are only finitely many elliptic curves with rank exceeding 21, see [15, 16].

In this note, we consider the following family of elliptic curves

$$E(r,s) : (y-s)(y+s) = x(x-r)(x+r), \tag{1}$$

which can be viewed as a generalization of the Diophantine elliptic curves $y^2 = x^3 - x + s^2$ introduced in [3]. Notice that Mordell curves [11] and congruent number elliptic curves [12] are thus examples for (1), but here we take $rs \neq 0$.

It seems appropriate to review briefly the state of the art. In [3], knowing that $E(1,s)$ contains two generators $P=(0,s)$, $Q=(1,s)$, Brown and Myers gave a certain quadratic polynomial $s(m)$ with the property that $E(1,s(m))$ contains an additional rational point which is independent from the two original generators. The rank search of (1) started from this work of Brown and Myers, who gave an infinitude of curves of rank ≥ 3 over $\mathbb{Q}(m)$. See, for example, [7, 1, 19, 20, 10, 8, 9], given in the chronological order of discovery. Specifically, in [7], Eikenberg generalized the above result of Brown and Myers and showed there exist infinitely many values of $s\in\mathbb{Q}$ such that $E(1,s)(\mathbb{Q})$ has rank at least five. In [19], Tadić, among other things, obtained a family of curves $E(r,1)$ of rank ≥ 5 over a field of rational functions in two variables and a family of $E(r,1)$ of rank ≥ 6 over an elliptic curve of positive rank. Then, in [20], she found families of $E(1,s)$ of rank ≥ 3 and ≥ 4 over fields of rational functions in four variables and a family of $E(1,s)$ of rank ≥ 5 parameterized by an elliptic curve of positive rank. In [10], Izadi and Nabardi considered $E(r,s)$ with the caveat that r^2-s^2 is a square and showed the existence of a family with rank ≥ 4 over $\mathbb{Q}(m)$. Recently, in a similar work [9], Izadi and Baghalaghdam have shown that the curve

$$E(t): y^2=x^3-(t^2+1)^2x+4t^2$$

is of rank ≥ 3 for infinitely many rational t.

Notably, the curves (1) over $\mathbb{Q}(m)$ also appear in some of recent works dealing with geometric problems, see, for example, [5, 21, 22]. In 2017, Das *et al.* [5] showed that the rank of the elliptic curve

$$y^2=x^3-16t^2(1+t^2)^2x+64t^4(1+t^2)^2 \tag{2}$$

is greater than or equal to 3 for infinitely many values of t, and asked that it might be interesting to find whether there exist curves in this family with high rank. In [22], Zhang and Zargar introduced a family of curves (2) of rank ≥ 4, giving a positive answer to the above question, and also gave a family of curves $E(r,s)$ over $\mathbb{Q}(m)$ of rank ≥ 4 coming from integral isosceles triangle and integral cyclic quadrilateral pairs with a common area and a common perimeter.

In what follows, we construct a subfamily of elliptic curves (1) over $\mathbb{Q}(m)$ with rank at least five. We also find some specific curves with higher rank and conclude the paper with some directions for future study.

2 Main result

Herein, we prove the following theorem, which improves the aforesaid results on the rank of the elliptic curves $E(r,s)$ over $\mathbb{Q}(m)$.

Theorem 2.1. *There exists a subfamily of elliptic curves* $(y-s)(y+s)=x(x-r)(x+r)$ *over* $\mathbb{Q}(m)$ *of rank at least five.*

Proof. Consider the elliptic curve $E(t): y^2=x^3-(t^2+1)^2x+4t^2$ over $\mathbb{Q}(t)$, taken from [9]. A quick check finds the non-obvious points:

$$P_1(t)=(0,2t)\,,\ P_2(t)=\left(-t^2+1,2t^2\right),\ P_3(t)=\left(t^2+1,2t\right).$$

By the specialization theorem of Silverman [18], in order to prove that the family of elliptic curves $E(t)$ has rank at least three over $\mathbb{Q}(t)$, it suffices to find a specialization $t = t_0$ such that the points $P_i(t)$, $i = 1, 2, 3$, are linearly independent on a specialized curve over $\mathbb{Q}$. If we take $t = 2$, then the points:

$$P_1(2) = (0, 4)\,,\ P_2(2) = (-3, 8)\,,\ P_3(2) = (5, 4)$$

are linearly independent points of infinite order on the elliptic curve $E(2) : y^2 = x^3 - 25x + 16$. Indeed, the regulator, i.e., the determinant of the Néron-Tate height pairing matrix of these points is the non-zero value 2.94853892225094, according to SAGE [17]. We note rank $E(2)(\mathbb{Q}) = 3$, carried out by Cremona's mwrank program [4].

In order to increase the rank of $E(t)$, we demand that 1 is x-coordinate of a point $P_4(t)$ on $E(t)$. This implies to have a u such that $u^2 = 2 - t^2$. Setting

$$t = \frac{-m^2 + 2m + 1}{m^2 + 1},$$

then $2 - t^2 = (m^2 + 2m - 1)^2/(m^2 + 1)^2$. Thus with this value of t, we are led to a fourth point, whose x-coordinate is $x_4 = 1$. In new coordinates, after rescaling by $(x, y) \mapsto (k^2x, k^3y)$ with $k = (m^2 + 1)^2$, the curve $E(t)$ transforms into

$$E_m : y^2 = x^3 - 4(m^4 - 2m^3 + 2m^2 + 2m + 1)^2x + 4(m^2 - 2m - 1)^2(m^2 + 1)^4,$$

with the points with abscissas

$$Q_1(m) = 0,\ Q_2(m) = 4m(m^2-1),\ Q_3(m) = 2(m^4-2m^3+2m^2+2m+1),\ Q_4(m) = (m^2+1)^2.$$

But, by a computer search, one can see that E_m contains a fifth point with abscissa

$$Q_5(m) = -4m(m^2 - 1).$$

Now, specialization at $m = 2$ shows that these five points are independent. In fact for this value of m, the specialized curve $E_2 : y^2 = x^3 - 676x + 2500$ with the points with abscissas

$$Q_1(2) = 0,\ Q_2(2) = 24,\ Q_3(2) = 26,\ Q_4(2) = 25,\ Q_5(2) = -24$$

has non-zero regulator 122.673049912775, and we have $E_2(\mathbb{Q}) \simeq \mathbb{Z}^5$. The concept of the specialization theorem, thus, shows the existence of infinitely many elliptic curves of the form E_m of rank at least five over $\mathbb{Q}(m)$ and trivial torsion subgroup, i.e., $E_m(\mathbb{Q}(m)) \simeq E_2(\mathbb{Q}) \simeq \mathbb{Z}^5$. This completes the proof. □

Remark 2.2. *For the other cases in [9] one can increase the rank by the strategy taken in the above proof. As the highest known rank for the curves* (1) *over* $\mathbb{Q}(m)$ *is* ≥ 4*, we only presented one family of rank* ≥ 5*.*

3 High rank examples

For almost all values of m, the coefficients were too large to be able to compute the rank of the corresponding elliptic curves E_m; for a few values, we were able to use mwrank to compute it. In the following, we present the highest rank examples we found. For $m = 8$, the corresponding elliptic curve

$$E_8 : y^2 = x^3 - 41396356x + 157728122500$$

has rank 8, while for $m = 17$, the curve

$$E_{17} : y^2 = x^3 - 1380419716x + 28519338122500,$$

has rank ≥ 8. We show conjecturally that rank $E_{17}(\mathbb{Q}) = 9$. For this we use the parity conjecture [2] and Mestre's conditional upper bound [13]:

$$\text{rank } \leq \frac{\pi^2}{8\lambda}\left(\log N - 2\sum_{p^m \leq e^\lambda} b(p^m)F_\lambda(m\log p)\frac{\log p}{p^m} - M_\lambda\right) =: M,$$

where N is the conductor, $b(p^m) = a_p^m$ if $p|N$ and $b(p^m) = \alpha_p^m + \alpha_p'^m$ if $p \not| N$ where α_p, α_p' are the roots of $x^2 - a_p x + p$,

$$M_\lambda = 2\left(\log 2\pi + \int_0^\infty \left(\frac{F_\lambda(x)}{e^x - 1} - \frac{e^{-x}}{x}\right)dx\right),$$

$F_\lambda(x) = F(x/\lambda)$ and the function F can be taken as

$$F(x) = \begin{cases} (1 - |x|)\cos(\pi x) + \sin(\pi|x|)/\pi & \text{for } x \in [-1, 1], \\ 0 & \text{elsewhere.} \end{cases}$$

Now, using PARI [14] for E_{17} with $\lambda = 17.1$, we get $M \approx 9.326$. But, by the parity conjecture, the rank of this curve is odd. Hence, rank $E_{17}(\mathbb{Q}) = 9$ conditionally.

4 Directions for future work

In this work, we constructed a family of (1) of rank ≥ 5 over $\mathbb{Q}(m)$. We explored further to try and increase the rank of the family E_m, but our attempts were not successful. So, a natural direction for further work would be to find higher rank subfamilies for E_m. Another challenging problem would be to find generators [6] for the family E_m.

References

[1] Antoniewicz, A. (2005). On a family of elliptic curves, *Univ. Iagel. Acta Math.*, 43, 21–32.

[2] Birch, B. J., Stephens, N. M. (1996). The parity of the rank of the Mordell-Weil group, *Topology*, 5, 295–299.

[3] Brown, E. A., & Myers, B. T. (2002). Elliptic curves from Mordell to Diophantus and back, *Amer. Math. Monthly*, 109, 639–649.

[4] Cremona, J. mwrank program, Available online at: `http://homepages.warwick.ac.uk/staff/J.E.Cremona//ftp/progs/`.

[5] Das, P., Juyal, A., & Moody, D. (2017). Integral isosceles triangle-parallelogram and Heron triangle-rhombus pairs with a common area and common perimeter, *J. Number Theory*, 180, 208–218.

[6] Duquesne, S., Nara, T., & Shamsi Zargar, A. (2019). Generators and integral points on elliptic curves associated with simplest quartic fields, *Math. Slovaca*, Accepted.

[7] Eikenberg, E. V. (2004). *Rational Points on Some Families of Elliptic Curves*, PhD thesis, University of Maryland.

[8] Fujita, Y., & Nara, T. (2018). The Mordell–Weil base for the elliptic curve of the form $y^2 = x^3 - m^2x + n^2$, *Publ. Math. Debrecen*, 92 (1–2), 79–99.

[9] Izadi, F., & Baghalaghdam, M. (2018). Some new families of positive-rank elliptic curves arising from Pythagorean triples, *Notes on Number Theory and Discrete Mathematics*, 24 (3), 27–36.

[10] Izadi, F., & Nabardi, K. (2016). A family of elliptic curves of rank ≥ 4, *Involve*, 9 (5), 733–736.

[11] Izadi, F., & Shamsi Zargar, A. (2017). A note on twists of $y^2 = x^3 + 1$, *Iran. J. Math. Sci. Inform.*, 12 (1), 27–34.

[12] Johnstone, J. A., & Spearman, B. K. (2010). Congruent number elliptic curves with rank at least three, *Canad. Math. Bull.*, 53 (4), 661–666.

[13] Mestre, J.-F. (1986). Formules explicites et minorations de conducteurs de variétés algébriques, *Compos. Math.*, 58, 209–232.

[14] Pari/gp, version 2.3.4, Available online at: `http://pari.math.u-bordeaux.fr/`.

[15] Park, J., Poonen, B., Voight, J., & Wood, M. M. (2019). A heuristic for boundedness of ranks of elliptic curves, *J. Eur. Math. Soc.*, 21 (9), 2859–2903.

[16] Poonen, B. Heuristics for the arithmetic of ellipric curves. *Proceedings of the 2018 International Congress of Mathematicians*, Accepted.

[17] Sage software, Available online at: `http://www.sagemath.org`.

[18] Silverman, J. H. (1983). Heights and the specialization map for families of abelian varieties, *J. Reine Angew. Math.*, 342, 197–211.

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

[20] Tadić, P. (2012). The rank of certain subfamilies of elliptic curve $Y^2 = X^3 - X + T^2$, *Ann. Math. Inform.*, 40, 145–153.

[21] Zhang, Y., Peng, J. Y., & Wang, J. M. (2018). Integral triangles and trapezoids pairs with a common area and a common perimeter, *Forum Geom.*, 18, 371–380.

[22] Zhang, Y., & Shamsi Zargar, A. (2019). Integral triangles and cyclic quadrilateral pairs with a common area and a common perimeter, *Forum Geom.*, Accepted.