COLLOQUIUM MATHEMATICUM
VOL. 143 2016 NO. 2

RANK OF ELLIPTIC CURVES ASSOCIATED TO BRAHMAGUPTA QUADRILATERALS

BY

FARZALI IZADI (Urmia), FOAD KHOSHNAM (Tabriz)
and ARMAN SHAMSI ZARGAR (Tabriz)

Abstract. We construct a family of elliptic curves with six parameters, arising from a system of Diophantine equations, whose rank is at least five. To do so, we use the Brahmagupta formula for the area of cyclic quadrilaterals (p^3, q^3, r^3, s^3) not necessarily representing genuine geometric objects. It turns out that, as parameters of the curves, the integers p, q, r, s along with the extra integers u, v satisfy $u^6 + v^6 + p^6 + q^6 = 2(r^6 + s^6)$, $uv = pq$, which, by previous work, has infinitely many integer solutions.

1. Introduction. Let E be an elliptic curve over $\mathbb{Q}$. The well-known theorem of Mordell and Weil states that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, where r is a nonnegative integer called the rank of $E(\mathbb{Q})$ and $E(\mathbb{Q})_{\text{tors}}$ is the subgroup of elements of infinite order called the *torsion subgroup* of $E(\mathbb{Q})$. By a celebrated theorem of Mazur [S1], the only possible torsion subgroups over $\mathbb{Q}$ are $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, \ldots, 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \le n \le 4$. Even though there exists a folklore conjecture which says that the rank can be arbitrarily high, it appears difficult to find examples of curves with high rank. The current record is an example of an elliptic curve over $\mathbb{Q}$ with rank ≥ 28 found by N. Elkies in May 2006 (see [D]). Moreover, no algorithm for determining the rank is known, nor is it not known which integers can occur as ranks.

The notion of rank has attracted the interest of several authors in the last decades, and has led to some information on the structure of elliptic curves as $\mathbb{Z}$-modules. Specifically, there have been some investigations regarding ranks of certain elliptic curves via the Heron formula. Izadi and Nabardi [IN] make a connection between the Heron formula for the area of triangles and elliptic curves. Recall that the Heron formula for the area of a triangle

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 14H52.
Key words and phrases: Brahmagupta formula, Heron formula, quadrilaterals, Diophantine equation, elliptic curves, rank of elliptic curves.
Received 23 February 2015; revised 12 July 2015.
Published online 21 December 2015.

of sides (a, b, c), say, is

$$S = \sqrt{P(P-a)(P-b)(P-c)},$$

where P is the semi-perimeter. Specifically, they use the Heron formula for the area of the formal triangle (a^2, b^2, c^2) to generate infinitely many elliptic curves with high rank. More precisely, they show that the elliptic curve

$$y^2 = x^3 + \tfrac{1}{4}(a^8 + b^8 + c^8 - 2a^4b^4 - 2a^4c^4 - 2b^4c^4)x$$

over the surface $a^4 + d^4 = 2(b^4 + c^4)$ has rank at least five and explicitly give five independent points.

Throughout this paper, the curves we generate all have the trivial torsion subgroup $\mathcal{T}$. In this work, we use the Brahmagupta formula for the area of cyclic quadrilaterals to similarly find infinitely many elliptic curves with high rank. In effect, we consider the elliptic curve

$$y^2 = x^3 - 3(pqrs)^2x + 2(pqrs)^3 + \tfrac{1}{4}(p^6 + s^6 - q^6 - r^6)^2 - (p^3s^3 + q^3r^3)^2,$$

denoted by $E_{u,v,p,q,r,s}$, over

$$C: \quad \begin{aligned} u^6 + v^6 + p^6 + q^6 &= 2(r^6 + s^6) \quad (1.1)\\ uv &= pq \quad (1.2) \end{aligned}$$

and prove that the group of the rational maps $C \to E_{u,v,p,q,r,s}$ that commute with the projection $E_{u,v,p,q,r,s} \to C$ has rank at least five. We do this by exhibiting five explicit sections P_1, P_2, P_3, P_4, P_5, and showing that these are linearly independent. We use the fact that $C(\mathbb{Q})$, the set of rational solutions on C, is infinite in order to deduce that infinitely many specializations of $E_{u,v,p,q,r,s}$ have ranks at least five over the rationals. This is done by using

$$y^2 - 28xy - 560y = x^3 - 20x^2 - 400x + 8000,$$

an elliptic curve of positive rank lying on C found in [IZ]. In fact, we show the following theorem.

Main Theorem 1.1. *There are infinitely many elliptic curves $E_{u,v,p,q,r,s}$ over C of rank at least five, parameterized by an elliptic curve of rank at least three over $\mathbb{Q}(p, q, r, s)$.*

2. The construction of $E_{u,v,p,q,r,s}$. As is mentioned above, in this work we deal with elliptic curves related to (positive) integer solutions on C. The Brahmagupta formula for the area of a cyclic quadrilateral in terms of its side lengths states that for a quadrilateral with sides a, b, c, d, the area of the quadrilateral is given by

$$S = \sqrt{(P-a)(P-b)(P-c)(P-d)}, \quad (2.1)$$

where $P = (a+b+c+d)/2$ is the semi-perimeter. Equivalently,

$$16S^2 = (b+c+d-a)(a+c+d-b)(a+b+d-c)(a+b+c-d), \tag{2.2}$$

which can be written in the form

$$\tfrac{1}{4}(b^2+c^2-a^2-d^2)^2 = (ad+bc)^2 - 4S^2. \tag{2.3}$$

Now, take $(a,b,c,d) = (p^3, q^3, r^3, s^3)$. By substitution, (2.3) turns into

$$\tfrac{1}{4}(q^6+r^6-p^6-s^6)^2 = (p^3s^3+q^3r^3)^2 - 4S^2. \tag{2.4}$$

Expanding and rearranging the right hand side of (2.4), we get

$$\tfrac{1}{4}(q^6+r^6-p^6-s^6)^2 = (p^2s^2)^3 + (q^2r^2)^3 + 2(pqrs)^3 - 4S^2,$$

or

$$\left(\frac{q^6+r^6-p^6-s^6}{2}\right)^2 = (p^2s^2+q^2r^2)^3 - 3p^2q^2r^2s^2(p^2s^2+q^2r^2) + 2(pqrs)^3 - 4S^2.$$

Setting $x = p^2s^2+q^2r^2$, $y = (q^6+r^6-p^6-s^6)/2$, and using (2.4), we can define the following elliptic curve:

$$y^2 = x^3 - 3(pqrs)^2x + 2(pqrs)^3 + \tfrac{1}{4}(p^6+s^6-q^6-r^6)^2 - (p^3s^3+q^3r^3)^2, \tag{2.5}$$

denoted by $E_{p,q,r,s}$, over $\mathbb{Q}(p,q,r,s)$.

By symmetry of p,q,r,s in our formulas, the elliptic curve has the following nonobvious points:

$$P_1(p,q,r,s) = \left(p^2q^2+r^2s^2, \frac{p^6+q^6-r^6-s^6}{2}\right),$$
$$P_2(p,q,r,s) = \left(p^2r^2+q^2s^2, \frac{p^6-q^6+r^6-s^6}{2}\right),$$
$$P_3(p,q,r,s) = \left(p^2s^2+q^2r^2, \frac{p^6-q^6-r^6+s^6}{2}\right).$$

By the specialization theorem ([S2] or [S1, Theorem 11.4, p. 271]), in order to prove that the family of elliptic curves defined in (2.5) has rank at least three over $\mathbb{Q}(p,q,r,s)$, it suffices to find a specialization $p = p_0$, $q = q_0$, $r = r_0$, $s = s_0$ such that the points $P_i(p,q,r,s)$, $i = 1,2,3$, are linearly independent on the specialized curve over $\mathbb{Q}$. If we take $p = 1$, $q = 1/2$, $r = 2$, $s = 0$, then the points $P_1(1,1/2,2,0) = (1/4, 4031/128)$, $P_2(1,1/2,2,0) = (4, 4159/128)$, $P_3(1,1/2,2,0) = (1, 4033/128)$ are linearly independent points of infinite order on the elliptic curve

$$E_{1,1/2,2,0} : y^2 = x^3 + 16248705/16384.$$

Indeed, the determinant of the Néron–Tate height pairing matrix of these points is the nonzero value 170.021501512688, according to SAGE [S]. We note that rank $E_{1,1/2,2,0}(\mathbb{Q}) = 4$, as computed by Cremona's `mwrank` program [C].

3. Infinitude of curves $E_{u,v,p,q,r,s}$ with rank at least five. In order to increase the rank of (2.5), we demand that u and v satisfy (1.1)–(1.2), i.e.,

$$u^6+v^6+p^6+q^6=2(r^6+s^6), \qquad uv=pq.$$

Note that since the quadrilateral (p,q,r,s) comes from (1.1)–(1.2), there is no guarantee that (p,q,r,s) and (p^3,q^3,r^3,s^3) represent genuine geometric objects.

In [IZ], the authors show the existence of infinitely many integer solutions to (1.1). The method is based on the points of the elliptic curve

$$E: y^2-28xy-560y=x^3-20x^2-400x+8000,$$

being generated by $(-50,400)$, as follows.

Suppose $G=(U/W,V/W)$ is a rational point on E. Then

$$\begin{aligned}
u &= 10(U-20W)(U^3-20U^2W+24UVW-400UW^2+640VW^2\\
&\quad +8000W^3),\\
v &= (U+20W)(18U^3+U^2V+40U^2W+464UVW-23200UW^2\\
&\quad +21680VW^2+304000W^3),\\
p &= 10(U^4+72U^3W+32U^2VW-2240U^2W^2+2976UVW^2\\
&\quad -28800UW^3+53120VW^3+736000W^4),\\
q &= (U-20W)(U+20W)(10U^2+UV-400UW+260VW\\
&\quad +4000W^2),\\
r &= (U+60W)(14U^3+U^2V-280U^2W+352UVW-5600UW^2\\
&\quad +8240VW^2+112000W^3),\\
s &= 6(U-20W)(U+20W)(U^2-40UW+28VW+400W^2),
\end{aligned}$$

is an integral solution to (1.1).

One can readily observe that

$$\begin{aligned}
uv-pq = 80(U+20W)(U-20W)^4(U^3-20U^2W-400UW^2+8000W^3\\
-V^2W+28UVW+560VW^2).
\end{aligned}$$

But the point $(U/W,V/W)$ lies on E, i.e.,

$$U^3-20U^2W-400UW^2+8000W^3-V^2W+28UVW+560VW^2=0.$$

Hence, $uv=pq$.

From now on, the curve (2.5) is denoted by $E_{u,v,p,q,r,s}$. We first show that the points

$$\begin{aligned}
P_4(u,v,p,q,r,s) &= \left(u^2r^2+v^2s^2, \frac{u^6-v^6+r^6-s^6}{2}\right),\\
P_5(u,v,p,q,r,s) &= \left(u^2s^2+v^2r^2, \frac{u^6-v^6-r^6+s^6}{2}\right)
\end{aligned}$$

lie on $E_{u,v,p,q,r,s}$: The point $P_4(u,v,p,q,r,s)$ satisfies $E_{u,v,p,q,r,s}$ if and only if

$$\begin{aligned}&(u^{12}+v^{12}-p^{12}-q^{12})\\&\quad-2(v^6s^6-p^6s^6-p^6q^6-p^6r^6+u^6r^6-s^6q^6+u^6v^6+u^6s^6-q^6r^6+r^6v^6)\\&\quad-12(u^4r^4v^2s^2+u^2r^2v^4s^4-p^2q^2r^4s^2u^2-p^2q^2r^2s^4v^2)=0,\end{aligned}$$

or equivalently, by (1.2),

$$\begin{aligned}(q^2-u^2)(q^2+qu+u^2)(q^2-qu+u^2)(p^2-u^2)(p^2+pu+u^2)(p^2-pu+u^2)\\\times(p^6q^6+p^6u^6-2u^6r^6-2s^6u^6+q^6u^6+u^{12})=0.\end{aligned}$$

The first six factors lead to trivial cases, so we are left with

$$p^6q^6+p^6u^6-2u^6r^6-2s^6u^6+q^6u^6+u^{12}=0,$$

or equivalently

$$u^{12}+(p^6-2r^6-2s^6+q^6)u^6+p^6q^6=0,$$

which by using (1.1) is the same as

$$u^{12}-(u^6+v^6)u^6+p^6q^6=0,$$

or equivalently $u^6v^6-p^6q^6=0$, which holds by (1.2). Similarly, one can see that $P_5(u,v,p,q,r,s)$ lies on $E_{u,v,p,q,r,s}$.

Now, specialization at $(u,v,p,q,r,s)=(748,6825,6188,825,6545,468)$ shows these five points are independent. In fact, for this value of (u,v,p,q,r,s), the specialized curve $E_{748,6825,6188,825,6545,468}$, i.e.,

$$\begin{aligned}y^2=x^3&-73356866160554547370800000x\\&+126120106752478587342832201925322189643214400\end{aligned}$$

with the points

$$\begin{aligned}&P_1(748,6825,6188,825,6545,468)\\&\qquad=(35444382573600,11231145747112000830120),\\&P_2(748,6825,6188,825,6545,468)\\&\qquad=(1640436333421600,67374938649066874419880),\\&P_3(748,6825,6188,825,6545,468)\\&\qquad=(37542673468881,11231450539996549524921),\\&P_4(748,6825,6188,825,6545,468)\\&\qquad=(34169761645600,11230981104248186419880),\\&P_5(748,6825,6188,825,6545,468)\\&\qquad=(1995497942444721,89837370293311610364681)\end{aligned}$$

has nonzero regulator $1.29010146713893\times10^7$, and we have

$$E_{748,6825,6188,825,6545,468}\simeq\mathbb{Z}^5.$$

The specialization theorem thus shows the existence of infinitely many elliptic curves of the form $E_{u,v,p,q,r,s}$ of rank at least five over $u^6+v^6+p^6+q^6 = 2(r^6+s^6)$ and $uv = pq$, and with trivial torsion subgroup $\mathcal{T}$.

Acknowledgments. The authors would like to thank the referee for carefully reading of the paper and offering insightful comments which improved the presentation.

References

[C] J. Cremona, http://maths.nottingham.ac.uk/personal/jec/ftp/progs.

[D] A. Dujella, http://web.math.pmf.unizg.hr/~duje/tors.html.

[IN] F. Izadi and K. Nabardi, *A family of elliptic curves with rank* ≥ 5, Period. Math. Hungar. 71 (2015), 243–249.

[IZ] F. Izadi, F. Khoshnam, and A. S. Zargar, *A note on the Diophantine equations* $x_1^k + x_2^k + x_3^k + x_4^k = 2(y_1^k + y_2^k)$, $k = 3, 6$, Notes Number Theory Discrete Math. 20 (2014), no. 5, 1–10.

[S] Sage software, version 4.5.3, http://www.sagemath.org.

[S1] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[S2] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. 342 (1983), 197–211.

Farzali Izadi
Department of Mathematics
Faculty of Science
Urmia University
Urmia 165-57153, Iran
E-mail: f.izadi@urmia.ac.ir

Foad Khoshnam, Arman Shamsi Zargar
Department of Pure Mathematics
Faculty of Basic Science
Azarbaijan Shahid Madani University
Tabriz 53751-71379, Iran
E-mail: khoshnam@azaruniv.edu
shzargar.arman@azaruniv.edu