Submitted to the Bulletin of the Australian Mathematical Society
doi:10.1017/S ...

ELLIPTIC CURVES ARISING FROM BRAHMAGUPTA QUADRILATERALS

FARZALI IZADI, FOAD KHOSHNAM, DUSTIN MOODY ✉ and ARMAN SHAMSI ZARGAR

Abstract

A Brahmagupta quadrilateral is a cyclic quadrilateral whose sides, diagonals, and area are all integer values. In this article, we characterize the notions of Brahmagupta, introduced by K. R. S. Sastry, by means of elliptic curves. Motivated by these characterizations, we use Brahmagupta quadrilaterals to construct infinite families of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ having ranks (at least) 4, 5, and 6. Furthermore, by specializing we give examples from these families of specific curves with rank 9.

2010 *Mathematics subject classification:* primary 14H52.

Keywords and phrases: Brahmagupta quadrilateral, elliptic curve, Heron triangle, rank.

1. Introduction

In [11], Dujella and Peral illustrate a connection between Heron triangles, and elliptic curves. Recall a Heron triangle is a triangle whose side lengths and area are all integers. Specifically, they used Heron triangles to generate certain families of elliptic curves with high rank. More generally, a polygon with integer sides, diagonals, and area is known as a Heron polygon. In this work, we use Heron quadrilaterals to similarly find families of elliptic curves with high rank.

Let E be an elliptic curve over $\mathbb{Q}$. The well known theorem of Mordell-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. By a theorem of Mazur [20], the only possible torsion groups over $\mathbb{Q}$, $E(\mathbb{Q})_{\text{tors}}$, 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 $1 \leq n \leq 4$.

Let T be an admissible torsion group for an elliptic curve E over $\mathbb{Q}$. Define

$$B(T) = \sup\{\text{rank } E(\mathbb{Q}) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\},$$

$$G(T) = \sup\{\text{rank } E(\mathbb{Q}(t)) : \text{torsion group of } E \text{ over } \mathbb{Q}(t) \text{ is } T\},$$

$$C(T) = \limsup\{\text{rank } E(\mathbb{Q}) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\}.$$

There exists a conjecture in this setting that says $B(T)$ is unbounded for all T. Even though $B(T)$ is conjectured to be arbitrarily high, it appears difficult to find examples

of curves with high rank. See [9, 10] for tables with the best known lower bounds for $B(T), G(T)$, and $C(T)$, including references to the papers where each bound is found.

Throughout this paper, the elliptic curves we generate all have the torsion group $\mathcal{T} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. There have been a variety of techniques used to find high rank elliptic curves with torsion group $\mathcal{T}$. The best result $B(\mathcal{T}) \geq 15$ is due to Elkies [9]. Elkies also established the best known lower bounds for $G(\mathcal{T})$ and $C(\mathcal{T})$, which are 7 and 8 respectively [10, 12]. Elkies' technique involves using $K3$ surfaces of high rank and their moduli. In another direction, Dujella et al. used irregular Diophantine m-tuples to prove $B(\mathcal{T}) \geq 8$, $C(\mathcal{T}) \geq 4$. These results were subsequently improved to $B(\mathcal{T}) \geq 11$, $C(\mathcal{T}) \geq 5$, again using the theory of rational Diophantine m-tuples [1, 7, 8].

Dujella and Peral [11] used Heron triangles to find families of elliptic curves over $\mathbb{Q}(t)$ with ranks (at least) 3, 4, and 5, and torsion subgroup $\mathcal{T}$, showing $C(\mathcal{T}) \geq 5$. They also gave examples (from these families) of curves with rank 9 and 10, thus $B(\mathcal{T}) \geq 10$. This improved upon earlier work by Izadi, et. al. [15] which had used Heron triangles to find a family of curves with rank 3, and examples of curves with rank 7.

In a similar fashion, we use Heron quadrilaterals to find families of high rank elliptic curves with torsion group $\mathcal{T}$. We first construct a family with rank at least 4, and then by specializing find subfamilies with ranks (at least) 5 and 6. In particular, the rank 6 family provides the best lower bound for $C(\mathcal{T})$ other than Elkies' bound mentioned above. We also performed a computer search within our first rank 4 family, and were able to find examples of curves with rank 9.

2. Brahmagupta quadrilaterals

A cyclic polygon is one with vertices upon which a circle can be circumscribed. Mathematicians have long been interested in Brahmagupta's work on Heron triangles and cyclic quadrilaterals. For example, consider Kummer's complex construction to generate Heron quadrilaterals outlined in [6]. The existence and parametrization of quadrilaterals with rational side lengths (and additional conditions) has a long history [2, 5, 6, 13, 14]. Buchholz and Macdougall [3] have shown that there exist no nontrivial cyclic quadrilaterals with rational area and having the property that the rational side lengths form an arithmetic or geometric progression.

We will refer to a cyclic Heron quadrilateral as a Brahmagupta quadrilateral [19]. Sastry [19] used Pythagorean triangles to construct general Heron triangles and cyclic quadrilaterals whose side lengths, diagonals, and area are integers, i.e., Brahmagupta quadrilaterals. He introduced a rational parametrization of the four sides of these quadrilaterals:

$$\begin{cases} a = (t(u+v)+1-uv)(u+v-t(1-uv)), \\ b = (1+u^2)(v-t)(1+tv), \\ c = t(1+u^2)(1+v^2), \\ d = (1+v^2)(u-t)(1+tu), \end{cases} \tag{2.1}$$

where $t, u, v \in \mathbb{Q}$ such that $abcd \neq 0$. Brahmagupta's formula gives the area S of a cyclic quadrilateral, in terms of the side lengths a, b, c, and d:

$$S = \sqrt{(s-a)(s-b)(s-c)(s-d)}, \tag{2.2}$$

where $s = (a+b+c+d)/2$. Letting $d = 0$, this reduces to the well known Heron's formula for the area of a triangle in terms of its side lengths. Brahmagupta also determined formulas for the lengths of the diagonals:

$$D_1 = \sqrt{\frac{(ac+bd)(ad+bc)}{ab+cd}}, \text{ and } D_2 = \sqrt{\frac{(ac+bd)(ab+cd)}{ad+bc}}. \tag{2.3}$$

Using the parameterization in (2.1) above, it is easily checked the area S and diagonal lengths D_1, D_2 are rational.

3. Elliptic curves and Brahmagupta quadrilaterals

A priori, there is no reason to associate Brahmagupta quadrilaterals with elliptic curves. However, by the area formula (2.2) we see the point $(\alpha, \beta) = (s, S)$ lies on the quartic

$$\beta^2 = (\alpha - a)(\alpha - b)(\alpha - c)(\alpha - d). \tag{3.1}$$

This quartic is birationally equivalent to an elliptic curve in the following manner. Taking $\zeta = -1/\alpha$, the equation (3.1) turns into

$$\beta^2 = \left(a + \frac{1}{\zeta}\right)\left(b + \frac{1}{\zeta}\right)\left(c + \frac{1}{\zeta}\right)\left(d + \frac{1}{\zeta}\right),$$

or equivalently

$$(\zeta^2\beta)^2 = (1 + \zeta a)(1 + \zeta b)(1 + \zeta c)(1 + \zeta d).$$

By the substitution

$$x = \frac{(1 + a\zeta)(d - b)(d - c)}{1 + d\zeta}, \quad y = \frac{\zeta^2\beta(d - a)(d - b)(d - c)}{(1 + d\zeta)^2},$$

the curve (3.1) thus turns into

$$E: \quad y^2 = x(x + (b - a)(d - c))(x + (c - a)(d - b)), \tag{3.2}$$

or

$$E: \quad y^2 = x^3 + Ax^2 + Bx, \tag{3.3}$$

where $A = (b-a)(d-c) + (c-a)(d-b)$ and $B = (b-a)(d-c)(c-a)(d-b)$. Equation (3.2) (or (3.3)) defines an elliptic curve so long as $a \neq b \neq c \neq d$. We note that by setting $d = 0$, this elliptic curve becomes the same elliptic curve studied in [11], which arose from Heron triangles.

Assuming $a \neq b \neq c \neq d$, the curve E has three 2-torsion points:

$$T_1 = (0, 0), \ T_2 = ((a - b)(d - c), 0), \ T_3 = ((a - c)(d - b), 0),$$

which shows the torsion group $\mathcal{T}$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It can be easily checked that $\mathcal{T} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by using the specialization monomorphism [20, III.11.4]. In addition, a simple calculation verifies the following three points also lie on E:

$$P_1 = \frac{(b+c+d-a)(d-b)(d-c)}{a+b+c-d}, \frac{4S(d-b)(d-c)(a-d)}{(a+b+c-d)^2},$$
$$P_2 = ((b-d)(c-d), (a-d)(b-d)(c-d)),$$
$$P_3 = (ad+bc, (ab+cd)D_1) = (ad+bc, (ad+bc)D_2),$$

where a, b, c, d, and S are as in Section 2. The points P_1 and P_2 both come from rational points on (3.1). Specifically, P_1 is the image of (s, S), while P_2 is the image of the point at infinity. The point P_3 is easily found, and is rational since D_1 (or D_2) is.

By the specialization theorem [20], in order to prove that the family of elliptic curves defined in (3.3) has rank ≥ 3 over $\mathbb{Q}(t, u, v)$, it suffices to find a specialization $t = t_0, u = u_0, v = v_0$ such that the points P_1, P_2, P_3 are linearly independent points on the specialized curve over $\mathbb{Q}$. If we take $(t, u, v) = (2, 4, 3)$, then the points

$$P_1 = (-14720, 456320),$$
$$P_2 = (-9760, 907680),$$
$$P_3 = (56120, 14310600),$$

are linearly independent points of infinite order on the elliptic curve

$$y^2 = x^3 + 10313x^2 - 79016960x.$$

Indeed, the determinant of the Néron-Tate height pairing matrix of these three points is the nonzero value 6.62644785139830 according to `SAGE` [18].

3.1. Families with rank at least 4 We specialize in order to find families of elliptic curves with higher rank. Note that $x^3 + Ax^2 + Bx = x^2(x + A + B/x)$. Thus, if we can find a value x_0 such that $x_0 + A + B/x_0 = y_0^2$ is a square, then (x_0, y_0) is a point on the curve $y^2 = x^3 + Ax^2 + Bx$. So a natural approach to find additional rational points on E is to examine the factors f of B, and check if $f + A + B/f$ is a square polynomial. The irreducible factors of B are

$$u,$$
$$u - v,$$
$$1 + v^2,$$
$$1 - uv,$$
$$2t - u + t^2u,$$
$$2t - u - v + t^2u - 2tuv + t^2v,$$
$$1 + 2tu + 2tv - uv - t^2 + t^2uv,$$
$$1 + 2tu + 4tv - 2uv - t^2 - v^2 - 2tuv^2 + 2t^2uv + t^2v^2.$$

Searching through all factors of B failed to lead to a fourth linearly independent point on E. However, we widened the search by modifying these factors slightly. For

example, one factor of B is

$$-u(u-v)(1+v^2)(2t-u+t^2u)(2t-u-v+t^2u-2tuv+t^2v).$$

If we change $u-v$ to $u+v$ and let

$$x_4 = -u(u+v)(1+v^2)(2t-u+t^2u)(2t-u-v+t^2u-2tuv+t^2v),$$

then $x_4 + A + B/x_4$ will be a square provided that

$$h = (u+v)(1-t^2+2tv)(t^2u+2t^2v^2u-t^2v+2tv^2+2tuv-u-2uv^2+v)$$

is square. Note that h is a quadratic polynomial in u, for which we can easily parameterize all rational solutions to $h = j^2$. Indeed, letting

$$u = \frac{-v(m+1-t^2+2tv)(m-1+t^2-2tv)}{2t^4v^2+4tv^3-8t^2v^2-4t^3v^3+1-2t^2+2v^2+t^4+m^2}, \tag{3.4}$$

then h is a square for arbitrary m. We denote the elliptic curve which depends on t, v, and m (with u as in (3.4)) as $E_{t,v,m}$. By specialization we verify x_4 is the x-coordinate of a fourth linearly independent point P_4. We take $(t,v,m) = (2,3,1)$, which makes $u = -12/31$. Then the points

$$\begin{aligned}
P_1 &= (566596800/923521, 1313937979200/887503681),\\
P_2 &= (256646880/923521, 3686732431200/887503681),\\
P_3 &= (125014617000/28629151, 16575/961),\\
P_4 &= (437088960/923521, 482983300800/887503681),
\end{aligned}$$

are independent points of infinite order on the elliptic curve

$$y^2 = x^3 - \frac{984279015}{923521}x^2 + \frac{7732400922892800}{27512614111}x,$$

since the corresponding height pairing matrix has nonzero determinant 105.651433982602 [18]. This shows the family of elliptic curves $E_{t,v,m}$ has rank ≥ 4 over $\mathbb{Q}(t,v,m)$ with independent points P_1, P_2, P_3, P_4.

We can similarly find other families with rank at least 4. For example, if we change $1-uv$ to $1+uv$, then

$$\begin{aligned}
x_4' = &-(1+uv)(t^2uv+2ut-uv+1-t^2+2tv)\\
&\times(-2uv-2utv^2+2ut+2t^2uv+4tv-t^2+t^2v^2+1-v^2),
\end{aligned}$$

similarly leads to a quadratic polynomial in u which we need to be square in order for x_4' to be the x-coordinate of a rational point P_4' on E. Setting

$$u = \frac{8t^3v^3+2t^2v^2-v^2t^4-16t^2v^4-8tv^3-v^2-m^2-4t^3v^52t^4v^4+4tv^5+2v^4}{v(m-v+t^2v-2tv^2)(m+v-t^2v+2tv^2)} \tag{3.5}$$

leads to a second family where we obtain a fourth linearly independent point. The independence can be easily verified, and we omit the details.

3.2. Families with ranks 5 and 6 Using the rank 4 family $E_{t,v,m}$ from the previous subsection, we set $t = 3, v = 2$. It was observed experimentally that the resulting family of curves had high ranks. These curves are defined by $E_{3,2,m} : y^2 = x^3+Ax^2+Bx$, where

$$A = 2^4 \cdot 5^3 \cdot \frac{13m^8 - 6848m^6 + 923136m^4 + 17973248m^2 - 1419444224}{(m^2 - 336)^4},$$

$$B = 2^{10} \cdot 5^6 \cdot \frac{(m-4)(m+4)(m^2+16)(m-28)(m+28)(m^2-80)}{(m^2-336)^7} \times (m^2 - 176)(m^2 + 176)(m^2 - 784)(3m^2 + 752)(m^4 - 256).$$

A calculation checks that if we let

$$x_5 = -5^2 \cdot \frac{(m-4)(m+4)(m^2+16)(m^2-176)(m^2+176)(3m^2-752)}{(m^2-336)^4},$$

$$x_6 = 5^3 \cdot \frac{(m-4)(m+4)(m^2+16)(m^2-176)(3m^2-752)}{(m^2-336)^3},$$

then these will be x-coordinates of rational points on the curve $E_{3,2,m}$ if $-(3m^2 - 832)$ and $5(3m^2 - 752)$ are respectively squares. Setting

$$m = 4\frac{3w^2 - 10w - 9}{w^2 + 3}, \tag{3.6}$$

then $-(3m^2 - 832) = 16(5w^2 + 18w - 15)^2/(w^2 + 3)^2$. Thus with this value of m, we are led to a fifth point P_5, whose x-coordinate is x_5. If we take $w = 4$ (with $t = 3$ and $v = 2$), then $m = -4/19$ and $u = -36/379$. Then the points

$$P_1 = \frac{2407523415840}{20632736881}, \frac{74527294860743040}{2963706958323721},$$

$$P_2 = \frac{5708320080}{54439939}, \frac{353413512792960}{7819807277899},$$

$$P_3 = \frac{1105374240}{54439939}, \frac{3204192524457600}{7819807277899},$$

$$P_4 = \frac{2189208949920}{20632736881}, \frac{66799447910432640}{2963706958323721},$$

$$P_5 = \frac{87152347653408}{7448418014041}, \frac{6922116696889413422208}{20328066027142402339},$$

are independent on the rank 7 specialized curve

$$y^2 = x^3 - \frac{4595501059952}{20632736881}x^2 + \frac{13904787542147195950080}{1123244937204690259}x.$$

Indeed, the determinant of the height pairing matrix of these five points has nonzero value 18322.9878246105. Hence, in light of the specialization theorem, the family

which we denote by $E_{t,v,m}$ with m defined in (3.6) has generic rank equal to (at least) 5 over $\mathbb{Q}(t, v, m)$.

To increase the rank to 6, we need $5(3m^2 - 752)$ to be a square. Using (3.6), this is equivalent to

$$E_6 : z^2 = 5(5w^4 - 180w^3 + 6w^2 + 540w + 45).$$

Note the rational point $(0, 15)$ is on E_6, and hence E_6 is an elliptic curve. Using standard transformations, E_6 is isomorphic to

$$E_6 : y^2 + 180xy - 27000y = x^3 - 8070x^2 - 22500x + 181575000.$$

Specifically, given a point (x_0, y_0) on E_6, let $w = (30x_0 - 242100)/y_0$ and $m = 4(3w^2 - 10w - 9)/(w^2 + 3)$. Then x_6 leads to a rational point on our elliptic curve arising from a Brahmagupta quadrilateral. Specializing shows these six points are independent. For example, if we take the point $(x_0, y_0) = (181806, 61174224)$ on E_6, then $w = 635/7453$, which makes $m = -42003212/3212401$ and $u = 49973671730004/26610765059003$. The specialized curve $E_{t,v,m}$ is

$$y^2 = x^3 + \frac{7464814131653897571967263151619135103328958047281380650000}{501452086548406443006704876667043173755384278600372081}x^2 + \frac{3060263006557775008751062983866670716202422694636141978026580228620357104744696463097717561\cdot 10^{10}}{5983981349^7\cdot 4447^7}x,$$

which has the six points $P_1, \ldots, P_6$ with x-coordinates

$$x_1 = -\frac{17504292551134080110304062606007877191310954011907 4100000}{501452086548406443006704876667043173755384278600372081},$$

$$x_2 = -\frac{25966402076418488423958917945532973943106442401607945593815 0400}{113406518841790937138762854790250768607561653549792 01},$$

$$x_3 = -\frac{116166630956048059520459277603831108062100000}{188439560244343409780592724763309855930 27},$$

$$x_4 = -\frac{55616926208784782851067011805488037941673937570867705000 00}{501452086548406443006704876667043173755384278600372081},$$

$$x_5 = -\frac{21107793402368374118801521401733973585785819692587340606165364101000 00}{51747449288468583029686101829451532853784087238708817669484809408 81},$$

$$x_6 = -\frac{18864638337826674135327950924853216190501678605546210000 0}{19446058455565258768139287059127874534539645561698262 7}.$$

These points are linearly independent, as the canonical height pairing matrix has nonzero determinant 2491225492.50894. We note that the rank of E_6 is 2, being generated by $(-1130, 156800)$ and $(-930, 140400)$. As there are thus an infinite number of points on E_6, we obtain an infinite number of Brahmagupta curves with rank at least 6.

We note that the equations for the rank 5 and rank 6 families above can be simplified somewhat by clearing denominators. In addition, we observed that other families with high rank can be obtained by setting t, v, and/or m to different values for the curve $E_{t,v,m}$. For example, if instead we let $t = 2$, and $v = 3$, and set

$$m = 3\frac{7\ell^2 - 2\ell + 28}{(\ell - 2)(\ell + 2)},$$

then

$$x_5 = \frac{(b - a)(c - a)(m^2 - 351)}{270}$$

TABLE 1. Curves $E_{t,v,m}$ with high rank

t	v	m	rank
2/5	3/4	3/2	9
5/8	−3	9/8	9
2	1/8	7/6	9
2	14	26	9
14/5	10/11	13/5	9
4	−3	32	9
4	2	87	9
8	18	20	$7 \leq \text{rank} \leq 9$
10	1/4	7/4	$8 \leq \text{rank} \leq 10$
13	−3	41	9

is the x-coordinate of a fifth point P_5, leading to a family with 5 linearly independent points. We omit further details.

4. Search for higher rank

We did a computer search to look for individual curves $E_{t,v,m}$ with high rank. Because computing the rank of an elliptic curve can be time consuming, we used Mestre-Nagao sums ([16, 17]) to perform an initial sieving process. These sums are of the form

$$S(N,E) = \sum_{p \leq N,\ p \text{ prime}} 1 - \frac{p-1}{\#E(\mathbb{F}_p)} \log p.$$

Elliptic curves with large rank tend to have high values for $S(N,E)$.

We used the bounds $-60 \leq t \leq 60$ and $-100 \leq v, m \leq 100$ looking for those curves E with $S(523,E) > 24$ and $S(1979,E) > 33$. We also searched by letting t, v, and m be fractions whose numerators and denominators were bounded by 15 in absolute value. After this initial sieving, we calculated the Selmer rank of the remaining curves with Cremona's `mwrank` program [4], and then computed the rank of those curves with high Selmer rank. We also searched the rank 5 and rank 6 families, but the coefficients quickly grew too large to be able to compute ranks. We found many examples of curves with rank 8 and 9. The results of the curves with rank 9 are displayed in Table 1, along with the curves with high rank for which we were not able to determine the rank precisely.

5. Conclusion

We believe our approach can be used to find many other families of curves with high rank and torsion group $\mathcal{T} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, using as a starting point the family $E_{t,v,m}$ of Section 3.1. We obtained our rank 5 families by specializing t and v, however it is

certainly possible that such families might be found be specializing only one variable. This would open the door to finding families with even higher rank. We leave this as an open problem.

References

[1] J. Aguirre, A. Dujella, and J. C. Peral. *On the rank of elliptic curves coming from rational Diophantine triples*, Rocky Mountain J. Math., **42** (2012), 1759–1776.

[2] C. Alsina, and R. B. Nelsen, *On the diagonals of a cyclic quadrilateral*, Forum Geom., **7** (2007), 147–149.

[3] R.H. Buchholz, and J.A. Macdougall, *Heron quadrilaterals with sides in sides in arithmetic or geometric progression*, Bull. Austral. Math. Soc., **59** (1999), 263–269.

[4] J. Cremona, *mwrank program,* available at `http://maths.nottingham.ac.uk/personal/jec/ftp/progs/`.

[5] L. Daia, *On a conjecture (Romanian)*, Gaz. Mat., **89** (1984), 276–279.

[6] L. E. Dickson, *History of the theory of numbers II*, Chelsea publishing company, New York, 1971.

[7] A. Dujella, *Diophantine triples and construction of high-rank elliptic curves over $\mathbb{Q}$ with three non-trivial 2-torsion points*, Rocky Mountain J. Math., **30** (2000), 157–164.

[8] A. Dujella, *Irregular Diophantine m-tuples and elliptic curves of high rank*, Proc. Japan Acad. Ser. A Math. Sci., **76** (2000), 66–67.

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

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

[11] A. Dujella, and J. C. Peral, *Elliptic curves coming from Heron triangles*, Rocky Mountain J. Math., to appear (2013).

[12] N. D. Elkies, Three lectures on elliptic surfaces and curves of high rank, (2007), preprint. arXiv:0709.2908.

[13] R. C. Gupta, *Parameśvara's rule for the circumradius of a cyclic quadrilateral*, Historia Math., **4** (1977), 67–74.

[14] D. Ismailescu, and A. Vojdany, *Class preserving dissections of convex quadrilatrals*, Forum Geom., **9** (2009), 195–211.

[15] F. Izadi, F. Khoshnam, and K. Nabardi, *A new family of elliptic curves with positive ranks arising from the Heron triangles*, (2010), preprint, arXiv:1012.5835.

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

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

[18] SAGE software, *Version 4.3.5*, `http://sagemath.org`.

[19] K.R.S. Sastry, *Brahmagupta quadrilaterals,* Forum Geom., **2** (2002), 167–173.

[20] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

Farzali Izadi, Department of Mathematics, Azarbaijan Shahid Madani University, Tabriz 53751-71379, Iran
e-mail: izadi@azaruniv.edu

Foad Khoshnam, Department of Mathematics, Azarbaijan Shahid Madani University, Tabriz 53751-71379, Iran
e-mail: khoshnam@azaruniv.edu

Dustin Moody, Computer Security Division, National Institute of Standards & Technology, 100 Bureau Drive, Gaithersburg, MD 20899-8930
e-mail: dustin.moody@nist.gov

Arman Shamsi Zargar, Department of Mathematics, Azarbaijan Shahid Madani University, Tabriz 53751-71379, Iran
e-mail: shzargar.arman@azaruniv.edu