MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 42 No. 2 (2019) pp. 11-20

A family of elliptic curves with rank at least 2 derived from Brahmagupta's formula

Raiza Corpuz
Institute of Mathematics
University of the Philippines, Diliman
Quezon City 1101, Philippines
rcorpuz@math.upd.edu.ph

Jerome Dimabayao
Institute of Mathematics
University of the Philippines, Diliman
Quezon City 1101, Philippines
jdimabayao@gmail.com

Abstract

Motivated by recent works of Izadi, Khoshnam, Moody, and Zargar, we construct an infinite family of elliptic curves with rank at least 2. We do this by applying Brahmagupta's formula for the area of cyclic quadrilaterals on quadruples of squares, which need not be the four sides of a real cyclic quadrilateral. We apply a parametrization due to Euler to obtain a family of elliptic curves, and identify three points lying on these curves in the process. Then we show that two of the points we identified have infinite order and are linearly independent, proving that our family of elliptic curves have rank at least 2. Finally, we extract elliptic curves of rank 3, 4, and 5 from this family.

Keywords: elliptic curve, Mordell-Weil rank, specialization theorem, Brahmagupta's formula, Euler parametrization

2010 MSC: 11G05

1 Introduction

The congruent number problem is a millennium-old problem that seeks to determine whether a positive integer n is the area of some right triangle with rational side lengths. It is well-known that rational right triangles with area n correspond to points of infinite order on the elliptic curve $E_n/\mathbb{Q} : y^2 = x(x-n)(x+n)$. An immediate consequence from this result is that when E_n has positive rank over $\mathbb{Q}$, then there exists a rational right triangle whose area is n. Because of its useful application to the congruent number problem, the family of elliptic curves E_n is often referred to as (the family of) *congruent number elliptic curves.* While these curves are helpful in shining a light on the congruent number problem, it has its limitations. For one, this family does not generate the set of all congruent numbers. Moreover, there is no general way to compute the rank of an elliptic curve. What we can do is find an expression that generates infinitely many congruent numbers by constructing a family of congruent number elliptic curves which can be proven to have positive rank.

More than a decade ago, Goins and Maddox [3] have successfully made a link between elliptic curves and (not necessarily right) rational triangles, otherwise known as Heron triangles. They did so by considering a more general family of congruent number elliptic curves

$$E_{\tau}^{(n)} : y^2 = x\,(x - n\tau)\left(x + n\tau^{-1}\right), \tag{1}$$

where τ is a nonzero rational number. Izadi, Khoshnam, and Nabardi [6] also obtained a family of elliptic curves related to Heron triangles in an attempt to construct families of elliptic curves with positive rank. They derived this family from Heron's formula for the area of a triangle

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

Here, a, b, and c are the sides of the triangle and s is the semiperimeter. The authors showed that the family of elliptic curves induced by Heron triangles has rank at least 2, and went on to exhibit a subfamily with rank at least 3. In 2014, Dujella and Peral [1] improved these results by producing subfamilies with ranks at least 3, 4, and 5. Similarly, in 2015, Izadi and Nabardi [8] revisited Heron's formula and set $(a, b, c) = (A^2, B^2, C^2)$, where A^2, B^2, and C^2 are sides of a rational triangle. From this specialization, they obtained a family of elliptic curves with rank at least 3. They found a subfamily of rank at least 5 by imposing a degree 4 equation on A, B, C, and an additional parameter D.

Izadi, Khoshnam, Moody, and Zargar [5] extended the work of Goins and Maddox [3] by showing a correspondence between cyclic Heron quadrilaterals with area n and elliptic curves of the form

$$E_{\alpha,n} : y^2 = x\left(x^2 + \alpha x - n^2\right).$$

They formed the connection by manipulating Brahmagupta's formula for the area of a cylic quadrilateral

$$S = \sqrt{(s-A)\,(s-B)\,(s-C)\,(s-D)}. \tag{2}$$

Here, A, B, C, and D are the sides of the quadrilateral and s is the semiperimeter. Izadi, Khoshnam, and Moody[4] demonstrated that the case $\alpha = 0$ is consistent with the elliptic curve $E_{\tau}^{(n)}$. They also showed that if for any particular $n \in \mathbb{Q}$, the elliptic curve $E_{\alpha,n}$ corresponds to a cyclic quadrilateral, then the torsion subgroup can only be isomorphic to one of the following: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Furthermore, they extracted subfamilies of $E_{\alpha,n}$ with ranks 3, 4, 5, and 6. They even found some specific curves of rank 9 [5, 7].

This paper aims to follow the strides of the above works. We contribute to the emerging list of families of elliptic curves with positive rank by deriving a family with rank at least 2 from Brahmagupta's formula. Afterwards, we list some elliptic curves from our family whose rank exceeds 2. We state the main result of this paper.

Theorem. *For all but finitely many values of* $t = \frac{p}{q} \in \mathbb{Q}$ *with* $(p, q) = 1$, *the elliptic curve*

$$\mathcal{E} : y^2 = x\left(x^2 - 4S^2\right),$$

where

$$4S^2 = -16\left(3t^4 + 2t^2 + 27\right)\left(t^2 + 3\right)^2\left(t^4 - 2t^3 + 10t^2 + 6t + 9\right)\left(t^4 + 2t^3 + 10t^2 - 6t + 9\right),$$

has rank at least 2, and its torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

2 A Family of Elliptic Curves

The idea is to consider Brahmagupta's formula (2) for a quadruple of squares which need not be the four sides of a real cyclic quadrilateral. So we begin by taking algebraic numbers a, b, c, and d so that a^2, b^2, c^2, and d^2 are positive integers. If we put $(A, B, C, D) = (a^2, b^2, c^2, d^2)$ in formula (2), we have

$$S^2 = \left(s - a^2\right)\left(s - b^2\right)\left(s - c^2\right)\left(s - d^2\right), \tag{3}$$

where $s = \frac{1}{2}(a^2 + b^2 + c^2 + d^2)$.

Notice that we can expand equation (3) as

$$\begin{aligned} S^2 &= \left(\frac{b^2 + c^2 + d^2 - a^2}{2}\right)\left(\frac{a^2 + c^2 + d^2 - b^2}{2}\right)\left(\frac{a^2 + b^2 + d^2 - c^2}{2}\right)\left(\frac{a^2 + b^2 + c^2 - d^2}{2}\right) \\ &= \frac{-a^8 + 2a^4b^4 + 2a^4c^4 + 2a^4d^4 - b^8 + 2b^4c^4 + 2b^4d^4 - c^8 + 2c^4d^4 - d^8 + 8a^2b^2c^2d^2}{16}. \end{aligned}$$

Multiplying both sides by 16, we obtain

$$\begin{aligned} 16S^2 &= -a^8 + 2a^4b^4 + 2a^4c^4 + 2a^4d^4 - b^8 + 2b^4c^4 + 2b^4d^4 - c^8 + 2c^4d^4 - d^8 + 8a^2b^2c^2d^2 \\ &= -\left(a^8 + 2a^4b^4 - 2a^4c^4 - 2a^4d^4 + b^8 - 2b^4c^4 - 2b^4d^4 + c^8 + 2c^4d^4 + d^8\right) + 4a^4b^4 \\ &\quad + 4c^4d^4 + 8a^2b^2c^2d^2 \\ &= -\left(a^4 + b^4 - c^4 - d^4\right)^2 + 4\left(a^2b^2 + c^2d^2\right)^2. \end{aligned}$$

Dividing both sides by 4, we get

$$4S^2 + \left(\frac{a^4 + b^4 - c^4 - d^4}{2}\right)^2 = \left(a^2b^2 + c^2d^2\right)^2. \tag{4}$$

Here, the 4-tuple (a^2, b^2, c^2, d^2) represents the same object regardless of order, so following a similar method of manipulating equation (3), we obtain two more equations:

$$4S^2 + \left(\frac{a^4 + c^4 - b^4 - d^4}{2}\right)^2 = \left(a^2c^2 + b^2d^2\right)^2 \tag{5}$$

$$4S^2 + \left(\frac{a^4 + d^4 - b^4 - c^4}{2}\right)^2 = \left(a^2d^2 + b^2c^2\right)^2. \tag{6}$$

2.1 A Parametrization Due to Euler

We now impose a condition on the right hand side of equations (4), (5), and (6). In particular, let us introduce the framework defined by the following system of Diophantine equations:

$$\begin{cases} a^2b^2 + c^2d^2 = u^2 \\ a^2c^2 + b^2d^2 = v^2 \\ a^2d^2 + b^2c^2 = w^2, \end{cases}$$

with $u, v, w \in \mathbb{Z}$. The following proposition due to Euler parametrizes the integer solutions to the above system of equations (cf. [2], pp. 27-28).

Proposition 2.1. *The solutions* (a, b, c, d, u, v, w) *of the system of Diophantine equations*

$$\begin{cases} a^2b^2 + c^2d^2 = u^2 \\ a^2c^2 + b^2d^2 = v^2 \\ a^2d^2 + b^2c^2 = w^2 \end{cases} \tag{7}$$

can be parametrized by relatively prime integers p *and* q *as follows:*

$$\begin{cases} a = 4pq \\ b = 2\left(p^2 + 3q^2\right) \\ c = (p-q)(p+3q) \\ d = (p+q)(p-3q) \end{cases} \qquad \begin{cases} u = p^4 + 22p^2q^2 + 9q^4 \\ v = 2\left(p^4 - 2p^3q + 2p^2q^2 + 6pq^3 + 9q^4\right) \\ w = 2\left(p^4 + 2p^3q + 2p^2q^2 - 6pq^3 + 9q^4\right). \end{cases}$$

Introducing the system (7) to equations (4), (5), and (6), we have

$$4S^2 + \left(\frac{a^4 + b^4 - c^4 - d^4}{2}\right)^2 = u^4 \tag{8}$$

$$4S^2 + \left(\frac{a^4 + c^4 - b^4 - d^4}{2}\right)^2 = v^4 \tag{9}$$

$$4S^2 + \left(\frac{a^4 + d^4 - b^4 - c^4}{2}\right)^2 = w^4. \tag{10}$$

Finally, we multiply u^2, v^2, and w^2 to equations (8), (9), and (10), respectively to get

$$4S^2u^2 + \left(\frac{a^4 + b^4 - c^4 - d^4}{2}\right)^2 u^2 = u^6 \tag{11}$$

$$4S^2v^2 + \left(\frac{a^4 + c^4 - b^4 - d^4}{2}\right)^2 v^2 = v^6 \tag{12}$$

$$4S^2w^2 + \left(\frac{a^4 + d^4 - b^4 - c^4}{2}\right)^2 w^2 = w^6. \tag{13}$$

Now if we consider the elliptic curve

$$E : y^2 = x\left(x^2 - 4S^2\right),$$

the form of equations (11), (12), and (13) suggests that the points

$$P = \left(u^2, \frac{u\left(a^4 + b^4 - c^4 - d^4\right)}{2}\right),$$

$$Q = \left(v^2, \frac{v\left(a^4 + c^4 - b^4 - d^4\right)}{2}\right), \text{ and}$$

$$R = \left(w^2, \frac{w\left(a^4 + d^4 - b^4 - c^4\right)}{2}\right)$$

belong to $E(\mathbb{Q}(p, q))$.

2.2 A Family of Elliptic Curves over $\mathbb{Q}(t)$

Let us briefly summarize what we have done so far. First, we derived three equations from Brahmagupta's formula for the area of cyclic quadrilaterals over the parameters (a, b, c, d). Then we introduced the system of Diophantine equations (7) to obtain a surface with parameters (a, b, c, d, u, v, w). We applied the parametrization in Proposition 2.1 to get the elliptic curve E defined over $\mathbb{Q}(p, q)$.

To move the setting to $\mathbb{Q}(t)$, we rewrite the parametrization from Proposition 2.1 as follows:

$$\begin{cases} a = 4pq\left(\frac{q}{q}\right)^2 \\ b = 2\left(p^2+3q^2\right)\left(\frac{q}{q}\right)^2 \\ c = (p-q)(p+3q)\left(\frac{q}{q}\right)^2 \\ d = (p+q)(p-3q)\left(\frac{q}{q}\right)^2 \end{cases} \qquad \begin{cases} u = \left(p^4+22p^2q^2+9q^4\right)\left(\frac{q}{q}\right)^4 \\ v = 2\left(p^4-2p^3q+2p^2q^2+6pq^3+9q^4\right)\left(\frac{q}{q}\right)^4 \\ w = 2\left(p^4+2p^3q+2p^2q^2-6pq^3+9q^4\right)\left(\frac{q}{q}\right)^4. \end{cases}$$

Letting $t = \frac{p}{q}$, and dropping the excess powers of q, we have the resulting parametrization

$$\begin{cases} a(t) = 4t \\ b(t) = 2\left(t^2+3\right) \\ c(t) = (t-1)(t+3) \\ d(t) = (t+1)(t-3) \end{cases} \qquad \begin{cases} u(t) = t^4+22t^2+9 \\ v(t) = 2\left(t^4-2t^3+2t^2+6t+9\right) \\ w(t) = 2\left(t^4+2t^3+2t^2-6t+9\right), \end{cases}$$

which still satisfies the system of Diophantine equations (7).

Applying this new parametrization to E, we obtain the elliptic curve

$$\mathcal{E} : y^2 = x\left(x^2-4S^2\right),$$

where

$$4S^2 = -16\left(3t^4+2t^2+27\right)\left(t^2+3\right)^2\left(t^4-2t^3+10t^2+6t+9\right)\left(t^4+2t^3+10t^2-6t+9\right).$$

Moreover, $\mathcal{E}(\mathbb{Q}(t))$ contains the points $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $R = (x_3, y_3)$ with

$$\begin{aligned} x_1 &= (t^4+22t^2+9)^2 \\ y_1 &= (7t^8+84t^6+634t^4+756t^2+567)(t^4+22t^2+9) \\ x_2 &= 4(t^4-2t^3+2t^2+6t+9)^2 \\ y_2 &= -16(t^8-t^7+12t^6+5t^5+38t^4-15t^3+108t^2+27t+81)(t^4-2t^3+2t^2+6t+9) \\ x_3 &= 4(t^4+2t^3+2t^2-6t+9)^2 \\ y_3 &= -16(t^8+t^7+12t^6-5t^5+38t^4+15t^3+108t^2-27t+81)(t^4+2t^3+2t^2-6t+9). \end{aligned}$$

We restate the main result of this study.

Theorem. *For all but finitely many values of* $t = \frac{p}{q} \in \mathbb{Q}$ *with* $(p, q) = 1$, *the elliptic curve*

$$\mathcal{E} : y^2 = x\left(x^2-4S^2\right),$$

where

$$4S^2 = -16\left(3t^4+2t^2+27\right)\left(t^2+3\right)^2\left(t^4-2t^3+10t^2+6t+9\right)\left(t^4+2t^3+10t^2-6t+9\right),$$

has rank at least 2, and its torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Remark 1. *We observe that the points P, Q and R are generally not linearly independent due to the symmetry of the functions defining Q and R. This is the reason why the rank is at least 2 instead of 3.*

3 The Torsion Subgroup of the Family $\mathcal{E}$

To determine the torsion subgroup of $\mathcal{E}$, we refer to the following result (cf. [11], pp. 346-347).

Proposition 3.1. *Let $D \in \mathbb{Z}$ be a fourth-power-free integer, and let E_D be the elliptic curve given by*

$$E_D : y^2 = x^3 + Dx.$$

Then

$$E_D(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z}, & \text{if } D = 4, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & \text{if } -D \text{ is a perfect square}, \\ \mathbb{Z}/2\mathbb{Z}, & \text{otherwise.} \end{cases}$$

We will also need the following lemma.

Lemma 3.1. *For all $t \in \mathbb{Q}$, $4S^2$ is not a rational square.*

Proof: Write

$$4S^2 = -16 \cdot \left(t^2 + 3\right)^2 \left(3t^4 + 2t^2 + 27\right) \cdot m(t) \cdot n(t),$$

where

$$\begin{aligned} m(t) &:= t^4 - 2t^3 + 10t^2 + 6t + 9 \\ n(t) &:= t^4 + 2t^3 + 10t^2 - 6t + 9. \end{aligned}$$

Notice that $n(t) = m(-t)$. Now we write $m(t)$ as

$$m(t) = t^2 \left(t - 1\right)^2 + 8t^2 + \left(t + 3\right)^2.$$

From this we see that $m(t)$ and $n(t)$ are positive rational functions of t. As a consequence, $4S^2 < 0$ and hence it cannot be a rational square.

Remark 2. *Let S be as in the theorem. Lemma 3.1 tells us that:*

(i) S^2 is negative. That is, the area that we get by applying the parametrization in Proposition 2.1 to Brahmagupta's formula is an imaginary number. So we do not expect a correspondence between our constructed family of elliptic curves and real quadrilaterals.

(ii) As a function of t, $-4S^2$ is even. So without losing generality, we may focus on positive rational values t.

Lemma 3.2. *For all $t \in \mathbb{Q}$, the torsion subgroup of $\mathcal{E}$ is $\mathbb{Z}/2\mathbb{Z}$.*

Proof: Without loss of generality, we can assume that $-4S^2$ is a fourth power-free rational number. If $-4S^2$ takes the form $\alpha^4 d$ for some $\alpha \in \mathbb{Q}$, we can simply perform the change of variables $(x, y) \longmapsto \left(\frac{x_1}{\alpha^2}, \frac{y_1}{\alpha^3}\right)$ to get a fourth power-free coefficient of x. This lets us utilize Proposition 3.1 with $D = -4S^2$. Since

$$4 + 4S^2 = -4\left(12t^{16} + 272t^{14} + 3248t^{12} + 18032t^{10} + 62472t^8 + 162288t^6 + 263088t^4 + 198288t^2 + 78731\right)$$

is a strictly negative function of t, no such t satisfies $-4S^2 = 4$. From this and from Lemma 3.1, we see that the torsion subgroup of $\mathcal{E}$ is indeed $\mathbb{Z}/2\mathbb{Z}$ for all $t \in \mathbb{Q}$.

4 Proof of the Theorem

We have already shown that the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ in Lemma 3.2. It remains to show that rank $(\mathcal{E}) \geq 2$. Suppose P and Q are independent points in $\mathcal{E}(\mathbb{Q}(t))$, both of infinite order. By Silverman's Specialization Theorem (cf. [11], Theorem 20.3, C.20) it is enough to demonstrate for a single specific $t \in \mathbb{Q}$ that P and Q are independent points in $\mathcal{E}(\mathbb{Q})$ which are both of infinite order, to justify its truth for all but finitely many $t \in \mathbb{Q}$. We can make this assumption about P and Q over $\mathbb{Q}(t)$ because otherwise, there will exist no specialization of t for which the points P and Q are linearly independent points of infinite order over $\mathbb{Q}$ to begin with.

Notice that if we specialize at $t = 5$, we obtain the elliptic curve

$$\mathcal{E}_{t=5} : y^2 = x\left(x^2 + 17949527113728\right),$$

which possesses the points:

$$P = (1401856, 5283708928), \text{ and}$$
$$Q = (861184, -4012048384).$$

It can be easily verified that the y-coordinates of P and Q are nonzero, and they do not divide the discriminant $\Delta_E = -484637232070656$ of E. Thus, by the Nagell-Lutz Theorem (see [10], page 56), the points $P, Q \in \mathcal{E}_{t=5}(\mathbb{Q})$ have infinite order. Now, if we compute the determinant of the height-pairing matrix of $\{P, Q\}$ using SAGE, we would get a nonzero value ≈ 56.49326. This indicates the linear independence of the points P and Q. Finally, we remark that the Specialization Theorem to extends this result for all but finitely many values $t \in \mathbb{Q}$. This proves the theorem.

Remark 3. *In the specialization above, the point* $R = (3268864, -9674911744)$ *is dependent on* P *and* Q*, because of the relation*

$$P - Q - R = \mathcal{O},$$

where $\mathcal{O}$ *is the identity element of* $\mathcal{E}(\mathbb{Q})$*. This was also computed using SAGE.*

5 Numerical Results

Using SAGE, we obtain the following data which demonstrates the capacity of $\mathcal{E}$ to reach ranks above the lower bound.

t	$-4S^2$	$[P, Q]$	rank $(\mathcal{E})$
4	811135480368	$(380689, 603292111)$ $(148996, -352368592)$	3
6	253766941981488	$(4397409, 34654734711)$ $(3849444, -32154370416)$	3
7	2534807241228288	$(12166144, 180664336384)$ $(13897984, -194713022464)$	3
10	602538928555150128	$(149059681, 9650190982903)$ $(273505444, -13610926281904)$	4
$\frac{8}{9}$	$\frac{13162663740596772929536}{617673396283947}$	$\left(\frac{31397359249}{43046721}, \frac{12236917596563599}{282429536481}\right)$ $\left(\frac{39433222084}{43046721}, \frac{-14509033705571344}{282429536481}\right)$	4
$\frac{13}{9}$	$\frac{10147893437442727979753216}{617673396283947}$	$\left(\frac{151140557824}{43046721}, \frac{97060865182203904}{282429536481}\right)$ $\left(\frac{70017393664}{43046721}, \frac{-55750354050678784}{282429536481}\right)$	4
$\frac{3}{10}$	$\frac{247078619390646249363}{625000000000000}$	$\left(\frac{12073834161}{100000000}, \frac{7034989226536287}{1000000000000}\right)$ $\left(\frac{11955454281}{25000000}, \frac{-1079671794400431}{62500000000}\right)$	4
$\frac{7}{11}$	$\frac{39487991221790318788608}{45949729863572161}$	$\left(\frac{70017393664}{214358881}, \frac{55750354050678784}{3138428376721}\right)$ $\left(\frac{151140557824}{214358881}, \frac{-97060865182203904}{3138428376721}\right)$	4
$\frac{11}{2}$	$\frac{290333560107499923}{4096}$	$\left(\frac{646837489}{256}, \frac{57231233469439}{4096}\right)$ $\left(\frac{120055849}{64}, \frac{-3024345212263}{256}\right)$	5
$\frac{18}{5}$	$\frac{30761297790711443808048}{152587890625}$	$\left(\frac{83406017601}{390625}, \frac{56088293122330407}{244140625}\right)$ $\left(\frac{26883537444}{390625}, \frac{-29092987031906736}{244140625}\right)$	5
$\frac{5}{6}$	$\frac{97677239847557041}{58773123072}$	$\left(\frac{1029703921}{1679616}, \frac{76938673693183}{2176782336}\right)$ $\left(\frac{363626761}{419904}, \frac{-6217606313839}{136048896}\right)$	5
$\frac{6}{11}$	$\frac{30478055805844911916848}{45949729863572161}$	$\left(\frac{52393836609}{214358881}, \frac{41721569199221031}{3138428376721}\right)$ $\left(\frac{136812693924}{214358881}, \frac{-82040268709436976}{3138428376721}\right)$	5
$\frac{13}{11}$	$\frac{307266028351175915470848}{45949729863572161}$	$\left(\frac{372353803264}{214358881}, \frac{407477047383752704}{3138428376721}\right)$ $\left(\frac{263604203776}{214358881}, \frac{-315140807447277568}{3138428376721}\right)$	5
$\frac{5}{13}$	$\frac{304436803123281839259648}{665416609183179841}$	$\left(\frac{122937189376}{815730721}, \frac{198203487830867968}{23298085122481}\right)$ $\left(\frac{432395674624}{815730721}, \frac{-460956022817357824}{372353803264}\right)$	5

Numerical Computation of rank $(\mathcal{E})$ using SAGE

6 References

[1] E. Dujella and J. C. Peral, *Elliptic curves coming from Heron triangles*, Rocky Mountain Journal of Mathematics, 44 (2014), pp. 1145–1160.

[2] L. Euler, *Solutio problematis difficillimi, quo hae duae formulae: aaxx+bbyy & aayy+bbxx quadrata reddi debent,*, Mémoires de l'académie des sciences de St. Petersbourg, 11 (1830), pp. 12–30.

[3] E. H. Goins and D. Maddox, *Heron triangles via elliptic curves*, Rocky Mountain Journal of Mathematics, 36 (2006), pp. 1511–1526.

[4] F. A. Izadi, F. Khoshnam, and D. Moody, *Heron quadrilaterals via elliptic curves*, Rocky Mountain Journal of Mathematics, 47 (2017), pp. 1227–1258.

[5] F. A. Izadi, F. Khoshnam, D. Moody, and A. S. Zargar, *Elliptic curves arising from Brahmagupta quadrilaterals*, Bulletin of the Australian Mathematical Society, 90 (2014), pp. 47–56.

[6] F. A. Izadi, F. Khoshnam, and K. Nabardi, *A new family of elliptic curves with positive ranks arising from the Heron triangles*, preprint, arXiv:1012.5835v1.

[7] F. A. Izadi, F. Khoshnam, and A. S. Zargar, *Rank of elliptic curves associated to the Brahmagupta quadrilaterals*, Colloquium Mathematicum, 143 (2016), pp. 187–192.

[8] F. A. Izadi and K. Nabardi, *A family of elliptic curves with rank $\geq$ 5*, Periodica Mathematica Hungarica, 71 (2015), pp. 243–249.

[9] SageMath, the Sage Mathematics Software System Version(`8.1`), The Sage Developers, 2017, *http://www.sagemath.org.*

[10] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer Science+Business Media, New York, 1992.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Science+Business Media, New York, 2009.

This page is intentionally left blank