EUCLIDEAN GEOMETRY AND ELLIPTIC CURVES

FARZALI IZADI

ABSTRACT. In this paper, we demonstrate the intimate relationships among some geometric figures and the families of elliptic curves with positive ranks. These geometric figures include Heron triangles, Brahmagupta quadrilaterals and Bicentric quadrilaterals. Firstly, we investigate the important properties of these figures and then utilizing these properties, we show that how to construct various families of elliptic curves with different positive ranks having different torsion subgroups.

1. INTRODUCTION

In geometry, Heron’s formula (sometimes called Hero’s formula), named after hero of Alexandria, gives the area of a triangle by requiring no arbitrary choice of side as base or vertex as origin, contrary to other formulas for the area of a triangle, such as half the base times the height or half of the norm of a cross product of two sides. Precisely, Heron’s formula states that the area of a triangle whose sides have lengths $a$, $b$, and $c$ is

$$A = \sqrt{p(p-a)(p-b)(p-c)},$$

where $p$ is the semiperimeter of the triangle; that is,

$$p = \frac{a + b + c}{2}.$$

The Indian mathematician Brahmagupta, 598-668 A.D., showed that for a triangle with integral sides $a$, $b$, $c$ and integral area $A$ there are positive integers $k, m, n$, with $k^2 < mn$, such that

$$\begin{align*}
  a &= n(k^2 + m^2), \\
  b &= m(k^2 + n^2), \\
  c &= (m + n)(mnk^2), \\
  A &= kmn(m + n)(mnk^2).
\end{align*}$$

We observe that the value of $A$ is a consequence of the Heron formula. A classical reference for Heron triangles is the second volume of the History of the
Heron's formula is a special case of Brahmagupta formula for the area of a cyclic quadrilateral (i.e., a simple quadrilateral that is inscribed in a circle) whose sides, diagonals and area are with sides of length a, b, c, and d as

\[ A = \sqrt{(p-a)(p-b)(p-c)(p-d)}, \]

where \( p \) is the semiperimeter

\[ s = \frac{a + b + c + d}{2}. \]

Similarly, a bicentric quadrilateral is a convex quadrilateral that has both a circumcircle passing through the four vertices and incircle having the four sides as tangents. In what follows, we consider a bicentric quadrilateral with rational sides, and discuss the problem of finding such quadrilateral where the ratio of the radii of the circumcircle and incircle is rational. The radii of these circles are denoted by \( R \) and \( r \) respectively. Examples of bicentric quadrilateral are squares, right kits, and isosceles tangential trapezoids. By Pitot's theorem we have \( s = a + c = b + d \) where \( s \) is the semiperimeter. In addition we have

\[ R = \frac{1}{4} \sqrt{\frac{(ab+cd)(ac+bd)(ad+bc)}{abcd}}, \]

and \( r = \frac{K}{s} \) where \( K = \sqrt{abcd} \) is the area of the quadrilateral.

In this review paper, we show that many authors utilize these formulas form all three figures to construct different elliptic curves with positive ranks. The main goal of the paper is that how the Euclidean geometry intimately related to the theory of elliptic curves.

The use of Heron's formula in number theory was not new. However the author together with some other people provided with a series of papers utilizing Heron's formula, Brahmagupta quadrilaterals as well as Bicentric quadrilaterals in an attempt to construct new families of elliptic curves with positive ranks. In this paper, we try to demonstrate the main results of these series of papers and leave the details for the corresponding original papers. To make it more accessible for the readers we devote separate sections to separate papers. Each section comes with the title of the corresponding original paper.

2. A Family of Elliptic Curves With Rank \( \geq 5 \)

In this paper, [19] the authors construct a family of elliptic curves with rank \( \geq 5 \). To do this, they use the Heron formula for a triple \((A^2, B^2, C^2)\) which are not necessarily the three sides of a triangle. It turns out that as parameters of a family of elliptic curves, these three positive integers \( A, B, \) and \( C, \) along with the extra parameter \( D \) satisfy the quartic Diophantine equation \( A^4 + D^4 = 2(B^4 + D^4) \). For the solutions of this diophantine equation see [17].

Take \((A^2, B^2, C^2)\), where \((A, B, C)\) are as in diophantine equation mentioned above. Since the triple \((A, B, C)\) is arising from the Diophantine equation, there is no guarantee to have a real triangle. Now by taking
EUCLIDEAN GEOMETRY AND CURVES

\[ a = A^2, \ b = B^2, \text{ and } c = C^2, \] one finds that
\[ (2.1) \]
\[ S = \sqrt{(A^2 + B^2 + C^2)(A^2 + B^2 - C^2)(A^2 + C^2 - B^2)(B^2 + C^2 - A^2) / 16}. \]

Expanding (2.1), one gets
\[ S^2 = -\left(\frac{A^8 + B^8 + C^8 - 2A^4B^4 - 2A^4C^4 - 2B^4C^4}{16}\right), \]
equivalently,
\[ 16S^2 = 2A^4B^4 + 2A^4C^4 + 2B^4C^4 - A^8 - B^8 - C^8, \]
or
\[ \left(\frac{A^4 + B^4 - C^4}{2}\right)^2 + 4S^2 = A^4B^4. \]

Multiplying both sides by \( A^2B^2 \) yields
\[ A^2B^2 \left(\frac{A^4 + B^4 - C^4}{2}\right)^2 + 4A^2B^2S^2 = A^6B^6. \]

Taking \( y = AB \left(\frac{A^4 + B^4 - C^4}{2}\right) \) and \( x = A^2B^2 \), the following family of elliptic curves is obtained:
\[ (2.2) \]
\[ E : y^2 = x^3 - 4S^2x. \]

Since the roles of \( A, \ B, \text{ and } C \) are symmetric in the Heron formula, the following points lie on the family (2.2) also.
\[ P_1 = \left(A^2B^2, \frac{AB(A^4 + B^4 - C^4)}{2}\right), \]
\[ P_2 = \left(A^2C^2, \frac{AC(A^4 + C^4 - B^4)}{2}\right), \]
\[ P_3 = \left(B^2C^2, \frac{BC(B^4 + C^4 - A^4)}{2}\right). \]

Next it is easy to impose two more points on the curve (2.2) with \( x \)-coordinates as \( B^2D^2 \) and \( C^2D^2 \). Substituting \( x = B^2D^2 \) in (2.2) yields
\[ y^2 = B^2D^2 \left(\frac{4B^4D^4 + A^8 + B^8 + C^8 - 2A^4B^4 - 2A^4C^4 - 2B^4C^4}{4}\right), \]
or
\[ (2.3) \]
\[ y^2 = B^2D^2 \left(\frac{A^4(A^4 - 2B^4 - 2C^4) + B^8 + C^8 - 2B^4C^4 + 4B^4D^4}{4}\right). \]

Let
\[ (2.4) \]
\[ A^4 - 2B^4 - 2C^4 = -D^4, \]
then by substituting \( A^4 = 2B^4 + 2C^4 - D^4 \) in (2.3), we get
\[ y^2 = B^2D^2 \left(\frac{B^2 + D^2 - C^2}{2}\right)^2. \]
Thus, the point $P_4 = \left( B^2D^2, \frac{BD(B^4+D^4-C^4)}{2} \right)$ is a new point on (2.2). Similarly, one can easily check that the point $P_5 = \left( C^2D^2, \frac{CD(C^4+D^4-B^4)}{2} \right)$ lies on (2.2) as well.

It is clear that the existence of these extra points on the family depends exactly on the existence of the solutions of the Diophantine equation $A^4 + D^4 = 2(B^4 + C^4)$.

In the final stage, the authors proved that the torsion subgroup of the (2.2) is $\mathbb{Z}/2\mathbb{Z}$.

3. Rank of elliptic curves associated to Brahmagupta quadrilaterals

In this paper, [22] the authors 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, they 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 the system of diophantine equations

$u^6 + v^6 + p^6 + q^6 = 2(r^6 + s^6)$, $uv = pq$ (see [23]), and they then utilize a subset of solutions of the system by the solutions of a specific positive rank elliptic curve.

In this work, the authors use the Brahmagupta formula for the area of cyclic quadrilaterals to find infinitely many elliptic curves with high rank. In effect, the elliptic curve is

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

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

$$C : \quad u^6 + v^6 + p^6 + q^6 = 2(r^6 + s^6)$$

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. This is done by exhibiting five explicit sections $P_1, P_2, P_3, P_4, P_5$, and showing that these are linearly independent. They 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 rationales. This last assertion 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 [23]. In fact, the following theorem is proved.
Theorem 3.1. 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 $\mathbb{Q}(p, q, r, s)$.

3.1. The construction of $E_{u,v,p,q,r,s}$. As is mentioned above, in this work, the authors deal with the 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

\begin{equation}
S = \sqrt{(P-a)(P-b)(P-c)(P-d)},
\end{equation}

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

\begin{equation}
16S^2 = (b + c + d - a)(a + c + d - b)(a + b + d - c)(a + b + c - d),
\end{equation}

which can be written in the form

\begin{equation}
\frac{1}{4}(b^2 + c^2 - a^2 - d^2)^2 = (ad + bc)^2 - 4S^2.
\end{equation}

Now, take $(a, b, c, d) = (p^3, q^3, r^3, s^3)$. By substitution, (3.5) turns into

\begin{equation}
\frac{1}{4}(q^6 + r^6 - p^6 - s^6)^2 = (p^2 s^2 - q^2 r^2)^3 + 2(pqrs)^3 - 4S^2,
\end{equation}

Expanding and sorting the right hand side of (3.6), leads to

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

or

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

Setting $x = p^2 s^2 + q^2 r^2$, $y = (q^6 + r^6 - p^6 - s^6)/2$, and using (3.6), one can define the following elliptic curve

\begin{equation}
y^2 = x^3 - 3(pqrs)^2 x + 2(pqrs)^3 + \frac{1}{4}(p^6 + s^6 - q^6 - r^6)^2 - (p^3 s^3 + q^3 r^3)^2,
\end{equation}

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

By symmetric roles of $p, q, r, s$ in the formulas, the elliptic curve has the following non-obvious points:

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

By the specialization theorem [29], they proved that the family has rank at least 3. Finally utilizing the system of equations

\[ u^6 + v^6 + p^6 + q^6 = 2(r^6 + s^6), \quad uv = pq. \]
discussed in [23] the authors showed that the following points also lie on the above family of elliptic curves.

\[ P_4(u, v, p, q, r, s) = \left( u^2r^2 + v^2s^2, \frac{u^6 - v^6 + r^6 - s^6}{2} \right), \]

\[ P_5(u, v, p, q, r, s) = \left( u^2s^2 + v^2r^2, \frac{u^6 - v^6 - r^6 + s^6}{2} \right), \]

4. On Elliptic Curves Via Heron Triangles and Diophantine Triples

In this paper F. Izadi et al. [17], constructed families of elliptic curves arising from Heron triangles and Diophantine triples with the Mordell-Weil torsion subgroup of \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). These families have ranks at least 2 and 3, respectively, and contain particular examples with rank equal to 7.

The following are the main results:

Consider the elliptic curve \( E_k : y^2 = (x + a(k)b(k))(x + b(k)c(k))(x + a(k)c(k)) \) associated to the triples:

\[
\begin{align*}
\{ a(k) &= 10k^2 - 8k + 8, \\
b(k) &= k(k^2 - 4k + 20), \\
c(k) &= (k + 2)(k^2 - 4),
\}
\]

**Theorem 4.1.** Let \( a(k), b(k) \) and \( c(k) \) be defined as (4.1) functions, where \( k \) is an arbitrary rational number different from 0, -2 and 2. Then the elliptic curve

\[ E : y^2 = (x + a(k)b(k))(x + b(k)c(k))(x + a(k)c(k)) \]

defined over \( \mathbb{Q}(k) \) has torsion subgroup \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

**Theorem 4.2.** With the terminology in theorem (4.1), rank \( E(\mathbb{Q}(k)) \geq 2 \).

**Proposition 4.3.** For each \( 2 \leq r \leq 7 \), there exists some \( k \) such that the elliptic curve \( E_k \) defined in the theorem (4.1) has torsion subgroup \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and rank \( r \).

**Theorem 4.4.** There exists a subfamily of \( E_k \) of rank \( \geq 3 \) over \( \mathbb{Q}(m) \).

The last result related to the diophantine triples. Let the diophantine triple \((a, b, c)\) has the property \( D(n) \) ([1]) if for any non zero integer \( n \), there exist rationales \( r, s \) and \( t \) such that

\[ ab + n = r^2, \quad ac + n = s^2, \quad bc + n = t^2. \]

**Theorem 4.5.** Consider \((a, b, c) = (k - 1, k + 1, 4k)\) with property \( D(1) \). Then there exists a subfamily of \( C : Y^2 = (aX + 1)(bX + 1)(cX + 1) \) over \( \mathbb{Q} \) with rank \( \geq 2 \).

5. Elliptic Curves Coming From Heron Triangles

The paper by Dujella and peral [9] adopted the method from [17] to construct families of elliptic curves with ranks at least 2, 3, 4, and 5. For the subfamily with rank \( \geq 5 \), they show that its generic rank is exactly equal to 5 and found free generators of the corresponding group. By specialization,
examples of elliptic curves over $Q$ with rank equal to 9 and 10 are also obtained.

6. Heron Triangles Via Elliptic Curves

Goin and Maddox [13] generalized some of Koblit’s notions [25, Ch. 1, §2, ex. 3] by exploring the correspondence between positive integers $n$ associated with arbitrary triangles (with rational side lengths) which have area $n$ and the family of elliptic curves

$$E^{(n)}_n : y^2 = x(x-n\tau)(x+n\tau^{-1}).$$

(6.1)

for nonzero rational $\tau$. Congruent number elliptic curves are obtained by taking $\tau = 1$. In fact, they broadened the study from rational right triangles to simply arbitrary rational triangles known as the Heron triangles.

The main result of the Goin-Maddox paper is the following.

Theorem 6.1. A positive integer $n$ can be expressed as the area of a triangle with rational sides if and only if for some nonzero rational number $\tau$ the elliptic curve

$$E^{(n)}_\tau : y^2 = x(x-n\tau)(x+n\tau^{-1})$$

(6.2)

has a rational point which is not of order 2. Moreover, $n$ is a congruent number if and only if we can choose $\tau = 1$.

The more general elliptic curve $E^{(n)}_\tau$ constructed above has all of its 2-torsion rational. Explicitly, when $\tau = 4n/(a+b)^2 - c^2$, then

$$E^{(n)}_\tau[2] = \{(0,0), \left(\frac{c^2-(a+b)^2}{4},0\right), \left(\frac{c^2-(a-b)^2}{4},0\right), \mathcal{O}\}.$$  

(6.3)

They showed that the torsion subgroup of $E^{(n)}_\tau$ is either

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

(6.4)

with the latter case corresponding to isosceles triangles.

7. Heron Quadrilaterals Via Elliptic Curves

In other direction, Izadi, Khoshnam and Moody, [20] established a correspondence between cyclic quadrilaterals with rational side lengths and area $n$, i.e., the correspondence between the Heron quadrilaterals and the family of elliptic curves of the form

$$y^2 = x^3 + \alpha x^2 - n^2 x$$

(7.1)

This correspondence generalizes the notions of Goins-Maddox [13] who established a similar connection between Heron triangles and elliptic curves. The authors further study this family of elliptic curves, looking at their torsion groups and ranks. They also explore their connection with congruent numbers, which are the $\alpha = 0$ case. Congruent numbers are positive integers which are the area of a right triangle with rational side lengths. We give explicit formulas which show how to construct the elliptic curve and some non-trivial
points on the curve given the side lengths and area of the quadrilateral. If we set one of the side lengths to zero, then the formulas collapse to exactly those of Maddox-Goins. They also show the other direction of the correspondence, that is, how to find a cyclic quadrilateral which corresponds to a given elliptic curve in our family. The pair \((\alpha, n)\) is called a \textit{generalized congruent number pair} if the elliptic curve \(y^2 = x^3 + \alpha x^2 - n^2 x\) has a point of infinite order. Similarly one can call the curve a generalized congruent number elliptic curve. The generalized congruent number curves with \(\alpha = 0\) are precisely the congruent number curves. Stated in this way, the results relate generalized congruent number pairs with cyclic quadrilaterals with area \(n\). Some important results are as follows:

**Theorem 7.1.** For every cyclic quadrilateral with rational side lengths and area \(n\), there is an elliptic curve

\[ E_{\alpha, -n^2} : y^2 = x^3 + \alpha x^2 - n^2 x \]

with 2 rational points, neither of which has order 2. Conversely, given an elliptic curve \(E_{\alpha, -n^2}\) with positive rank, then there is a cyclic quadrilateral with area \(n\) whose side lengths are rational (under the correspondence given above).

**Theorem 7.2.** If the curve \(E_{\alpha, -n^2}\) arising from a cyclic quadrilateral has rank 0 then the associated quadrilateral is either a square, or an isosceles trapezoid with three sides equal \((a = b = d)\) such that \((a + c)(3a - c)\) is a square. The torsion group is \(\mathbb{Z}/6\mathbb{Z}\) for this rank 0 case.

**Theorem 7.3.** If the quadrilateral is a square, then the rank is 0, with torsion group \(\mathbb{Z}/6\mathbb{Z}\).

The rank need not be 0 for isosceles trapezoids with three sides equal. Take, for example the quadrilateral with side lengths \((13, 13, 23, 13)\), which yields the curve \(E_{-11, -216^2}\). This curve has rank 1, with generating point \((-196, 1092)\) and has torsion group \(\mathbb{Z}/6\mathbb{Z}\). One can have rank 0 curves \(E_{\alpha, -n^2}\) with torsion group \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\). Take for example \(\alpha = 7, n = 12\). The previous results prove that such curves do not correspond with a cyclic quadrilateral. By allowing the quadrilaterals with \(d = 0\), then it can be shown that these curves come from quadrilaterals with \(d = 0\), i.e. triangles with rational area.

**Theorem 7.4.** If the quadrilateral is a three-sides-equal trapezoid \((a, a, c, a)\), then the torsion group is \(\mathbb{Z}/6\mathbb{Z}\).

By scaling the sides of a rational cyclic quadrilateral, one can always assume that area is an integer \(N\) (since only the quadrilaterals with rational area are considered). Using the definition of the generalized congruent number elliptic curve and taking into account Theorems 7.3, 7.4, and 7.5, one can restate Theorem 7.1 in the following way.

**Theorem 7.5.** Every non-square and non-three-sides equal trapezoidal rational cyclic quadrilateral with area \(N \in \mathbb{N}\) gives rise to a generalized congruent number elliptic curve \(E_{\alpha, -N^2}\) with positive rank. Conversely, for any integer \(N\) and generalized congruent curve \(E_{\alpha, -N^2}\) with positive rank, there are infinitely many non-rectangular cyclic quadrilaterals.
Next the structure of torsion points are discussed.

**Proposition 7.6.** There is no point $P$ on the curve $E_{\alpha,-n^2}$ such that $2P = (0,0)$. Consequently, the torsion group $T \neq \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, \text{ or } \mathbb{Z}/12\mathbb{Z}$.

**Proposition 7.7.** There are no points of order 5 on the curve $E_{\alpha,-n^2}$.

By an old result, an elliptic curve with a rational point of order 5 will have its $j$-invariant of the form $(s^2 + 10s + 5)/s$ for some $s \in \mathbb{Q}$ [12]. Calculating the $j$-invariant of $E_{\alpha,-n^2}$, one must have

$$256\frac{(\alpha^2 + 3n^2)^3}{n^4(\alpha^2 + 4n^2)} = \frac{(s^2 + 10s + 5)^3}{s}.$$ 

**Proposition 7.8.** The torsion group $T$ is not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

**Proposition 7.9.** The torsion group $T$ is not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Combining the above series of results, the following corollary is immediate.

**Corollary 7.10.** Given a cyclic quadrilateral with corresponding elliptic curve $E_{\alpha,-n^2}$, the torsion group must be $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Note that all four torsion groups are possible. As it was previously showed, any square will have torsion group $\mathbb{Z}/6\mathbb{Z}$. For any $m > 2$, and letting $a = m^2 - 4$ and $b = 2m$, then the rectangle with side lengths $a$ and $b$ will have torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

It turns out that if the cyclic quadrilateral is a non-square rectangle, two of the possible torsion groups can be ruled out.

**Proposition 7.11.** The elliptic curve arising from a rectangle has a point of order 3 if and only if the rectangle is actually a square.

**Corollary 7.12.** Given a non-square rectangle with sides $a$ and $b$, then $T = \mathbb{Z}/2\mathbb{Z}$ or $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. one gets the latter group if and only if $4a^2 + b^2$ is a square.

This characterization of congruent numbers can be added to the list of the many other known characterizations of congruent numbers. Several of these are given in Koblitz’s book [25]. Given an integer $n$, it is a well-known open problem to determine whether or not $n$ is congruent. A partial answer is given by Tunnell’s theorem, which gives an easily testable criterion for determining if a number is congruent. However, this result relies on the unproven Birch and Swinnerton-Dyer Conjecture for curves of the form $y^2 = x^3 - n^2x$. The criterion involves counting the number of integral solutions $(x, y, z)$ to a few Diophantine equations of the form $ax^2 + by^2 + cz^2 = n$.

In the remainder of the paper, the authors give two different new infinite families of congruent number elliptic curves with (at least) rank three. Searching for families of congruent curves with high rank has been done before [11],[10],[26],[27]. Currently, the best known results are a few infinite families with rank at least 3 [24],[27], and several individual curves with rank 7.

The authors conclude the paper by constructing an infinite family with rank at least 4 as well as an infinite family of rank 5. By computer search examples of the curves with rank 10 are also obtained.
8. On Parametric Spaces of Bicentric Quadrilaterals

In Euclidean geometry, a bicentric quadrilateral is a convex quadrilateral that has both a circumcircle passing through the four vertices and an incircle having the four sides as tangents. In this work, the authors consider a bicentric quadrilateral with rational sides, and discuss the problem of finding such quadrilaterals where the ratio of the radii of the circumcircle and incircle is rational. The radii of these circles are denoted by \( R \) and \( r \) respectively. Examples of bicentric quadrilaterals are squares, right kites, and isosceles tangential trapezoids.

First, we briefly recall some basic facts concerning these objects. Let \( ABCD \) be a convex quadrilateral with sides of rational length \( a, b, c, d \) in anti-clockwise direction. It is bicentric if and only if the opposite sides satisfy Pitot’s theorem and the opposite angles are supplementary, that is, \( s = a + c = b + d, \angle A + \angle C = \angle B + \angle D = \pi \), where \( s \) is the semi-perimeter.

In addition, we have

\[
R = \frac{1}{4} \sqrt{\frac{(ab + cd)(ac + bd)(ad + bc)}{abcd}}
\]

and \( r = K/s \), where \( K = \sqrt{abcd} \) is the area of the quadrilateral, see [14, Page 67].

Consider a bicentric quadrilateral with rational sides. We discuss the problem of finding such quadrilaterals where the ratio of the radii of the circumcircle and incircle is rational. The authors show that this problem can be formulated in terms of a family of elliptic curves given by \( E_a : y^2 = x^3 + (a^4 - 4a^3 - 2a^2 - 4a + 1)x^2 + 16a^4x \) which have, in general, \( \mathbb{Z}/8\mathbb{Z} \), and in rare cases \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) as torsion subgroups. It can be show that the existence of infinitely many elliptic curves \( E_a \) of rank at least two with torsion subgroup \( \mathbb{Z}/8\mathbb{Z} \), parameterized by the points of an elliptic curve of rank at least one, and give five particular examples of rank 5. It can be also show the existence of a subfamily of \( E_a \) whose torsion subgroup is \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \).

The authors show that a given bicentric quadrilateral, with \( N \) rational, leads to a member of a family of elliptic curves, denoted by \( E_a \), dependent on a single side. They also discuss the torsion subgroup of \( E_a(\mathbb{Q}) \), which is either \( \mathbb{Z}/8\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \).

The main results are the followings:

**Theorem 8.1.** All rational bicentric quadrilaterals with rational \( N \) correspond to rational points on \( E_a \) for some \( a > 0 \), where \( E_a(\mathbb{Q}) \) will have strictly positive rank.

**Theorem 8.2.** The torsion subgroup of \( E_a(\mathbb{Q}) \) equals \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) if and only if

\[
a = \frac{r + 1}{r(r - 1)} \text{ for some } r \in \mathbb{Q} \setminus \{0, \pm1\}.
\]

From this, refer to [13, 7] to see what is known concerning the ranks of curves with prescribed torsion subgroup \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \).
They close this section by listing, in Table 1, 26 out of 27 known rank-three curves which come from the family $E_a$, with $a$ defined as in Theorem 8.2, (see also [8]).

| $r$       | Authors                  | Date |
|----------|--------------------------|------|
| 12/17    | Connell-Dujella          | 2000 |
| 47/18    | Dujella                  | 2001 |
| 133/86   | Rathbun                  | 2003 |
| 201/239  | Campbell-Goins          | 2003 |
| 299/589, 247/160, 281/138, 281/133 | Dujella      | 2006 |
| 439/17, 569/159 | Rathbun           | 2006 |
| 923/230  | Dujella-Rathbun         | 2006 |
| 247/419, 200/99, 337/65 | Flores-Jones-Rollick-Weigandt-Rathbun | 2007 |
| 1017/352 | Dujella                  | 2008 |
| 999/76, 412/697, 349/230, 217/425, 440/217, 309/470, 496/319, 585/391, 219/313, 336/191 | Fisher      | 2009 |
| 257/287  | Rathbun                  | 2013 |

Table 1. Curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ having rank 3

9. **Elliptic Curves Arising from Brahmagupta Quadrilaterals**

A Brahmagupta quadrilateral is a cyclic quadrilateral whose sides, diagonals, and area are all integer values. In this article, the authors [7] characterize the notions of Brahmagupta, introduced by K. R. S. Sastry [28], by means of elliptic curves. Motivated by these characterizations, The authors 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 they give examples from these families of specific curves with rank 9.

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, 14, 15]. 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.
Let us refer to a cyclic Heron quadrilateral as a Brahmagupta quadrilateral \cite{28}. Sastry \cite{28} 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{equation}
    \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}
\end{equation}

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 \( d \):

\begin{equation}
    S = \sqrt{(s - a)(s - b)(s - c)(s - d)},
\end{equation}

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:

\begin{equation}
    D_1 = \sqrt{\frac{(ac + bd)(ad + bc)}{ab + cd}}, \quad \text{and} \quad D_2 = \sqrt{\frac{(ac + bd)(ab + cd)}{ad + bc}}.
\end{equation}

Using the parameterizations in (9.1) above, it is easily checked the area \( S \) and diagonal lengths \( D_1, D_2 \) are rational.

A priori, there is no reason to associate Brahmagupta quadrilaterals with elliptic curves. However, by the area formula (9.2) one see the point \((\alpha, \beta) = (s, S)\) lies on the quartic

\begin{equation}
    \beta^2 = (\alpha - a)(\alpha - b)(\alpha - c)(\alpha - d).
\end{equation}

This quartic is birationally equivalent to an elliptic curve in the following manner. Taking \( \zeta = -1/\alpha \), the equation (9.4) turns into

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

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 (9.4) thus turns into

\begin{equation}
    E : \quad y^2 = x(x + (b - a)(d - c))(x + (c - a)(d - b)),
\end{equation}

or

\begin{equation}
    E : \quad y^2 = x^3 + Ax^2 + Bx,
\end{equation}

where \( A = (b - a)(d - c) + (c - a)(d - b) \) and \( B = (b - a)(d - c)(c - a)(d - b) \). Equation (9.5) (or (9.6)) defines an elliptic curve so long as \( a \neq b \neq c \neq d \).

Note that by setting \( d = 0 \), this elliptic curve becomes the same elliptic curve
Table 2. 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    |

studied in [9], which arose from Heron triangles. Since the coefficients of the elliptic curve defined in terms of $a, b, c, d$ and these in turn depend on the variables $t, u, v$ by Sastry representation, it follows that the main family of elliptic curves defined over $\mathbb{Q}(t, u, v)$.

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

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

which shows the torsion group $T$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It can be easily checked that $T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by using the specialization monomorphism [29, III.11.4]. Next, the authors construct an infinite family of rank at least 3, and families of rank at least 4. From families of rank at least 4 they finally found a subfamily of rank at least 5 as well as a family of rank at least 6. A computer search also shows the following special examples for the ranks.

References

[1] J. Aguirre, A. Dujella and J. C. Peral, On the rank of elliptic curves coming from rational Diophantine triples, Rocky Mountain J. of 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. Aust. Math. Soc., 59 (1999), 263–269.
[4] G. Campbell and E. H. Goins, Heron triangles, Diophantine problems and elliptic curves, 2003 (preprint).
[5] L. Daia, On a conjecture, Gaz. Math., 89 (1984), 276-279.
[6] L. E. Dickson, History of the theory of numbers II, Chelsea publishing company, New York, 1971.
[7] A. Dujella, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, Glas. Mat. Ser. III 42 (2007), 3–18.
[8] A. Dujella, High rank elliptic curves with prescribed torsion, https://web.math.pmf.unizg.hr/~duje/tors/tors.html.
[9] A. Dujella and J. C. Peral, Elliptic curves coming from Heron triangles, Rocky Mountain J. Math. Vol. 44, No. 4 (2014), 1145-1160.
[10] A. Dujella, A. S. Janfada, J. C. Peral, S. Salami, On the high rank $\pi/3$ and $2\pi/3$ - congruent number elliptic curves, Rocky Mountain J. Math. Vol. 44, No. 6, (2014), 1867-1880.
[11] A. Dujella, A. S. Janfada and S. Salami, A search for high rank congruent number elliptic curves, J. Integer Seq., 12 (2009), Article 09.5.8.
[12] R. Fricke, Die elliptischen Funktionen und ihre Anwendungen, Bd. 2. B. G. Teubner, Leipzig, (1922).
[13] E. H. Goin and D. Maddox, Heron triangles Via elliptic curves, Rocky Mountain J. of Math., 4 (1977), no. 1, 67-74.
[14] D. Ismailescu and A. Vojdany, Class preserving dissections of convex quadrilaterals, Forum Geom., 9 (2009), 195–211.
[15] R. C. Gupta, Paramesvara’s rule for the circumradius of a cyclic quadrilateral, Historia Math., 4 (1977), no. 1, 67-74.
[16] F. Izadi, F. Khoshnam, A. J. MacLeod, A. S. Zargar, On parametric spaces of bicentric quadrilaterals, Math. Slovaca 67 (2017), 611-622.
[17] F. Izadi and F. Khoshnam, On elliptic curves Via Heron triangles and diophantine triples, J. of Mathematical Extension, Vol. 8, No. 3, (2014), 17-26.
[18] F. Izadi and K. Nabardi, Diophantine equation $X^4 + Y^4 = 2(U^4 + V^4)$, Math. Slovaca 66 (2016), No.3 557-560.
[19] F. Izadi and K. Nabardi, A family of elliptic curves with rank $\geq 5$, Vol. 71, issue 2, 245-249.
[20] F. Izadi, F. Khoshnam and D. Moody, Heron quadrilaterals Via elliptic curves, Rocky Mountain J. Math. Vol. 47, No. 4 (2017), 1227-1258.
[21] F. Izadi, F. Khoshnam, D. Moody and A. S. Zargar, Elliptic curves arising from Brahmagupta quadrilaterals, Bull. Aust. Math. Soc, Vol. 92, (2015), 187-194.
[22] F. Izadi, F. Khoshnam and A. S. Zargar, Rank of elliptic curves associated to Brahmagupta quadrilaterals, Colloquium Mathematicum, Vol. 143, No. 2, 2016, 187-192.
[23] F. Izadi and A. S. Zargar, A note on the Diophantine equations $x_1^k + x_2^k + x_3^k + x_4^k = 2y_1^k + 2y_2^k$, $k = 3, 6$, Vol. 20, 2014, No. 5, Pages 110.
[24] J. A. Johnstone and B. K. Spearman, Congruent number elliptic curves with rank at least three, Canad. Math. Bull., 53 (2010), no. 4, 661-666.
[25] N. Koblitz, Introduction to elliptic curves and modular forms, Springer-Verlag, New York, 1984.
[26] N. F. Rogers, Rank computations for the congruent number elliptic curves. Exp. Math. 9, (2000), no. 4, 591-594.
[27] K. Rubin, and A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, Exp. Math. 10 (2001), no. 4, 559-569.
[28] K.R.S. Sastry, Brahmagupta quadrilaterals, Forum Geom., 2 (2002), 167–173.
[29] J. H. Silverman, Heights and the specialization map for families of abelian varieties, J. Reine Angew. Math. 342 (1983), 197-211.

Department of Mathematics, University Of Toronto, Toronto ON Canada
E-mail address: f.izadi@utoronto.ca