Journal of Mathematical Extension
Vol. 8, No. 3, (2014), 17-26

On Elliptic Curves Via Heron Triangles and Diophantine Triples

F. Izadi*
Azarbaijan Shahid Madani University

F. Khoshnam
Azarbaijan Shahid Madani University

Abstract. In this article, we construct families of elliptic curves arising from the 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.

AMS Subject Classification: 14H52; 11G05; 14G05
Keywords and Phrases: Diophantine triple, elliptic curve, family of elliptic curves, the Heron triangle, specialization, rank, torsion group

1. Introduction

Triangles with integral sides and area have been considered by Indian mathematician Brahmagupta (598-668 A.D.). In general, the sides and area are related by a formula first proved by Greek mathematician Heron of Alexandria (c. 10 A.D-c. 75 A.D.) as

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

where $P = (a+b+c)/2$ is the semi perimeter.
Triangles with rational sides and area are known as the Heron triangles (for more information and fundamental results on Heron triangles, see [7, 8, 11]).

Received: February 2014; Accepted: July 2014
*Corresponding author

Goins and Maddox have studied Heron triangles by considering the elliptic curve

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

as a generalization of the congruent number problem (see [8]). In the same paper, they also have found 4 curves of rank 3 with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Campbell and Goins ([2]) by analyzing the elliptic curve

$$E_t : y^2 = x^3 + (t^2 + 2)x^2 + x$$

defined over the rational function field $\mathbb{Q}(t)$ described connections between the problem of finding Heron triangles with a given area possessing at least one side of a particular length and rational Diophantine quadruples and quintuples. They also have studied the relation between these problems and elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and found a new elliptic curve with this torsion having rank 3 and an infinite family of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank at least 1. Having constructed a family of Diophantine triples such that the correspondent elliptic curve over $\mathbb{Q}$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 5, Aguirre et al. [1] have obtained two examples of elliptic curves over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank equal to 11. Dujella and Peral in a joint work [6] have created subfamilies of elliptic curves coming from the Heron triangles of ranks at least 3,4, and 5. They also have given examples of elliptic curves over $\mathbb{Q}$ with rank equal to 9 and 10.

This paper is organized as follows. In Section 2, a family of elliptic curves arising from Heron triangles introduced by Fine [7] is considered and shown that the family has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and rank at least 2, and a subfamily of rank $\geqslant 3$. In Theorem 2.6, a subfamily of $Y^2 = (aX + 1)(bX + 1)(cX + 1)$ of rank $\geqslant 2$ is given. This is a generalization of Dujella's work done in [4]. Therein, Dujella extended the Diophantine triple $(a, b, c) = (k - 1, k + 1, 4k)$ to a quadruple by studying $Y^2 = (aX + 1)(bX + 1)(cX + 1)$, and proved that this elliptic curve has generic rank 1 over $\mathbb{Q}$. In Section 3, some examples of elliptic curves with rank 7 are given.

2. Main Results

Let S be area of the triangle (a, b, c), i.e., $S = \sqrt{P(P-a)(P-b)(P-c)}$, where $P = (a+b+c)/2$. This formula, due to Heron, ensures us to have an elliptic curve $v^2 = u(u-a)(u-b)(u-c)$ with non torsion point $(u, v) = (P, S)$. The curve therefore is birationally equivalent to $y^2 = (x+ab)(x+bc)(x+ac)$, with corresponding (non torsion) point $(x, y) = \left(-abcP^{-1}, abcSP^{-2}\right)$, and is equivalent to $Y^2 = (aX+1)(bX+1)(cX+1)$, with corresponding point $(X, Y) = \left(-P^{-1}, SP^{-2}\right)$. In the sequel, we are going to treat with special families coming from these two kinds of elliptic curves.

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 Fine triple:

$$\begin{cases} a(k) = 10k^2 - 8k + 8, \\ b(k) = k(k^2 - 4k + 20), \\ c(k) = (k+2)(k^2 - 4), \end{cases} \tag{1}$$

arising from a Heron triangle which has rational area $4k(k^2-4)^2$ (see [7]). (Note that multiplication of sides in (1) by $(2(k^2-4))^{-1}$ implies that the resulting triangle to have area k.) One can easily check that E_k has three rational points of order two:

$$\begin{cases} T_1 = (-k(10k^2 - 8k + 8)(k^2 - 4k + 20), 0), \\ T_2 = (-k(k+2)(k^2 - 4k + 20)(k^2 - 4), 0), \\ T_3 = (-(k+2)(10k^2 - 8k + 8)(k^2 - 4), 0). \end{cases}$$

As the change of coordinates $(x, y) \to (x - a(k)b(k), y)$ does not affect the group structure of $E_k(\mathbb{Q})$, we may consider E_k in the form $y^2 = x^3 + Ax^2 + Bx$, in which

$$\begin{aligned} A &= k^6 - 12k^5 + 116k^4 - 480k^3 + 304k^2 - 448k - 64, \\ B &= 4k(5k^2 - 4k + 4)(k^2 - 4k + 20)(3k^2 - 12k - 4) \\ &\quad \times (k^3 - 8k^2 + 4k - 16). \end{aligned} \tag{2}$$

Theorem 2.1. *Let $a(k)$, $b(k)$ and $c(k)$ be defined as (1), 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 $Q(k)$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. The points $\mathcal{O}$ (the point at infinity), $T_1 = (-a(k)b(k), 0), T_2 = (-b(k)c(k), 0)$, and $T_3 = (-a(k)c(k), 0)$ form a subgroup of the torsion group $E(\mathbb{Q}(k))_{tors}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By Mazur's theorem and a theorem of Silverman (see [13], Theorem 11.4, p.271), it suffices to check that there exists no point $E(\mathbb{Q}(k))$ of order four, six or eight. If there exists a point T on $E(\mathbb{Q}(k))$ such that $2T \in \{T_1, T_2, T_3\}$, then 2-descent Proposition (see [9], 4.1, p.37), implies that all of the expressions

$$\begin{aligned}
&-a(k)b(k) + a(k)b(k) = 0,\\
&-a(k)b(k) + b(k)c(k) = k(k^2 - 4k + 20)(k^3 - 8k^2 + 4k - 16),\\
&-a(k)b(k) + a(k)c(k) = 4(5k^2 - 4k + 4)(3k^2 - 12k - 4),
\end{aligned}$$

must be perfect squares. But, it is easily seen that for $k = 1$ none of the above expressions are perfect squares. Similarly, if $2T = T_2$ and $2T = T_3$, then all of the expressions

$$\begin{aligned}
&-b(k)c(k) + a(k)b(k) = -k(k^2 - 4k + 20)(k^3 - 8k^2 + 4k - 16),\\
&-b(k)c(k) + b(k)c(k) = 0,\\
&-b(k)c(k) + a(k)c(k) = -(k^2 - 12k + 4)(k - 2)^2(k + 2)^2,
\end{aligned}$$

as well as

$$\begin{aligned}
&-a(k)c(k) + a(k)b(k) = -4(5k^2 - 4k + 4)(3k^2 - 12k - 4),\\
&-a(k)c(k) + b(k)c(k) = (k^2 - 12k + 4)(k - 2)^2(k + 2)^2,\\
&-a(k)c(k) + a(k)c(k) = 0,
\end{aligned}$$

must be perfect squares. But, it is easily seen that for $k = 1$ none of the above expressions are perfect squares. This contradiction shows that $T \notin \{T_1, T_2, T_3\}$. Thus, by [10] it is to prove that there exists no point T

such that $3T \in \{T_1, T_2, T_3\}$. If there exists a point $T = (x, y)$ on $E(\mathbb{Q}(k))$ such that $3T = T_1, T \neq T_1$, then from $2T = -T + T_1$, the equation

$$x^4 - 6h_1(k)x^2 - 4h_1(k)h_2(k)x - 3h_2(k)^2 = 0, \tag{3}$$

is obtained in which

$$\begin{aligned} h_1(k) &= -12k^5 - 480k^3 + 116k^4 + 304k^2 - 448k - 64 + k^6, \\ h_2(k) &= 4k(5k^2 - 4k + 4)(k^2 - 4k + 20)(3k^2 - 12k - 4) \\ &\quad \times (k^3 - 8k^2 + 4k - 16). \end{aligned}$$

It can be easily seen that for $k = 1$, the equation (3), namely

$$x^4 + 3498x^2 + 195841360x - 21157921200 = 0$$

has no rational solution. Similarly it can be checked that there does not exist any point T on $E(\mathbb{Q}(k))$ such that $3T = T_2$, $T \neq T_2$, and $3T = T_3$, $T \neq T_3$. Therefore, $E(\mathbb{Q}(k))_{tors} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\square$

Theorem 2.2. *With the terminology in Theorem 2.1, rank* $E(\mathbb{Q}(k)) \geqslant 2$.

Proof. Evidently the non torsion points

$$\begin{aligned} \mathcal{P}_1 &= (-a(k)b(k)c(k)P^{-1}(k), a(k)b(k)c(k)S(k)P(k)^{-2}), \\ \mathcal{P}_2 &= (0, a(k)b(k)c(k)), \end{aligned}$$

lie on $E(\mathbb{Q}(k))$, where $P(k)$ and $S(k)$ are respectively the associated semi perimeter and area to $(a(k), b(k), c(k))$.
For $k = 1$, the elliptic curve $E(\mathbb{Q}(k))$ turns into

$$E_1 : y^2 = x^3 - \frac{73}{36}x^2 - \frac{85}{4}x + \frac{7225}{144},$$

with

$$\mathcal{P}_1 = \left(\frac{85}{18}, \frac{85}{27}\right), \quad \mathcal{P}_2 = \left(0, \frac{85}{12}\right).$$

The Néron-Tate height matrix [14, p. 230] associated to these points is of non vanishing determinant ≈ 2.30842249514247 (carried out with `SAGE` [12]) showing that the points are linearly independent.Therefore the rank of E over $\mathbb{Q}(k)$ is $\geqslant 2$, and hence, by the specialization theorem of Silverman [13], the rank $E_k(\mathbb{Q}) \geqslant 2$, for all but finitely many rational numbers k. $\square$

Proposition 2.3. *For each $2 \leqslant r \leqslant 7$, there exists some k such that E_k defined in Theorem 2.1 has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank r.*

Proof. The first part is readily obtained from Theorem 2.1. For the second part, it suffices to note that for the values of k = 4,7,19,11, 98/625, and 88/31, the corresponding ranks with using of Mwrank [3], are 2,3,4,5,6, and 7, respectively. $\square$

Now, we are ready to show our main result:

Theorem 2.4. *There exists a subfamily of E_k of rank $\geqslant 3$ over $\mathbb{Q}(m)$.*

Proof. Obviously the non torsion points

$$\begin{aligned}\mathcal{P}_1 &= (4(5k^2-4k+4)(k^2-4k+20),\\ &\qquad 8(5k^2-4k+4)(k^2-4k+20)(k-2)^3),\\ \mathcal{P}_2 &= (2(5k^2-4k+4)k(k^2-4k+20),\\ &\qquad 2k(k-2)(5k^2-4k+4)(k^2-4k+20)(k+2)^2),\end{aligned}$$

lie on the curve $E_k: y^2 = x^3 + Ax^2 + Bx$. In order to find a subfamily of rank $\geqslant 3$, we proceed as following. Let $B_1 = 2k(3k^2-12k-4)(k^2-4k+20)$, and for some rational numbers M, N, e, $\mathcal{P}_3 = (B_1M^2/e^2, B_1MN/e^3)$ be on E_k. This implies the quartic equation $B_1M^4 + AM^2e^2 + B_2e^4 = N^2$. Taking $M = e = 1$, we get $(k-6)(k+2)^5 = N^2$, hence, $(k-6)(k+2) = z^2$, where $z = N/(k+2)^2$. Using the rational solution $(k, z) = (6, 0)$, the parametric solution is then $(k, z) = (2(3m^2+1)/(m^2-1), 8m/(m^2-1))$, where $m \in \mathbb{Q} \setminus \{\pm 1\}$. Therefore, $N = 2^9m^5/(m^2-1)^3$ and $\mathcal{P}_3$ turns into

$$\begin{aligned}\mathcal{P}_3 &= (B_1, B_1N)\\ &= \Bigg(\frac{2^{12}(3m^2+1)(m^4+4m^2+1)(m^4+1)}{(m^2-1)^5},\\ &\qquad \frac{2^{21}(3m^2+1)(m^4+4m^2+1)(m^4+1)m^5}{(m^2-1)^8}\Bigg).\end{aligned}$$

Thus E_k turns into $E_m : y^2 = x^3 + Ax^2 + Bx$ with

$$A = \frac{2^{13}(m^{12} + 14m^{10} - 5m^8 + 4m^6 + 11m^4 + 6m^2 + 1)}{(m^2-1)^6},$$
$$B = -\frac{2^{24}(m^6 - 5m^4 - 3m^2 - 1)M_1M_3}{(-1+m^2)^{10}},$$

and three non torsion points

$$\mathcal{P}_1 = \left(\frac{2^{12}M_1}{(m^2-1)^4}, \frac{2^{19}M_1(1+m^2)^3}{(m^2-1)^7}\right),$$
$$\mathcal{P}_2 = \left(\frac{2^{12}(m^4+1)M_2}{(-1+m^2)^5}, \frac{2^{20}(m^4+1)m^4(m^2+1)M_2}{(m^2-1)^8}\right),$$
$$\mathcal{P}_3 = \left(\frac{2^{12}(m^4+1)M_3}{(m^2-1)^5}, \frac{2^{21}(m^4+1)m^5M_3}{(m^2-1)^8}\right),$$

where

$$M_1 = (m^4+1)(5m^4+4m^2+1),$$
$$M_2 = (3m^2+1)(5m^4+4m^2+1),$$
$$M_3 = (3m^2+1)(m^4+4m^2+1).$$

Regarding the specialization theorem, since for $m = 1/2$, the Néron-Tate height matrix associated to these points has non vanishing determinant ≈ 11.9727247292862, then E_m as a subfamily of E_k is of rank $\geqslant 3$ over $\mathbb{Q}(m)$. $\square$

We say that ([5]) the Diophantine triple (a, b, c) has the property $D(n)$, for any non zero integer n, whenever there exist rational r, s, and t such that

$$ab + n = r^2, \qquad ac + n = s^2, \qquad bc + n = t^2.$$

Theorem 2.5. *Let $(a, b, c) = (k-1, k+1, 4k)$ with property $D(1)$. Then there exists a subfamily of $C : Y^2 = (aX+1)(bX+1)(cX+1)$ over $\mathbb{Q}$ with rank $\geqslant 2$.*

Proof. Consider the triple $(a, b, c) = (k-1, k+1, 4k)$ with property $D(1)$. The curve $C_k : Y^2 = ((k-1)X+1)((k+1)X+1)(4kX+1)$, $k \in \mathbb{Q}$, has non torsion point $\mathcal{P}_1 = (0, 1)$. [The triple $(k-1, k+1, 4k)$ has the property $D(1)$, but does not form any triangle (note $a(k)+b(k) < c(k)$).] In order to find a subfamily of C_k of rank $\geqslant 2$, let $\mathcal{P}_2 = (-P^{-1}, P^{-2}S)$, be on the curve, where $P = 3k$ and $S = k\sqrt{-3(4k^2-1)}$. This implies to have some rational u such that $-3(4k^2-1) = u^2$. Using the rational solution $(k, u) = (1/2, 0)$, the parametric solution for k is then $k = \frac{m^2-12}{2(m^2+12)}$, where $m \in \mathbb{Q}$. Henceforth, C_k turns into

$$C_m : Y^2 = \left(\frac{-m^2-36}{2(m^2+12)}X+1\right)\left(\frac{3(m^2+4)}{2(m^2+12)}X+1\right)\left(\frac{2(m^2-12)}{m^2+12}X+1\right),$$

with two non torsion points

$$\mathcal{P}_1 = (0, 1),$$
$$\mathcal{P}_2 = \left(\frac{-2(m^2+12)}{3(m^2-12)}, \frac{8m}{3(m^2-12)}\right).$$

The associated height matrix to these points at $m = 1$ has non vanishing determinant ≈ 2.87442404831027 showing that these points are linearly independent, hence rank $C_m(\mathbb{Q}) \geqslant 2$ for all but finitely many m's. The elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ with the point (x, y) is isomorphic to $y^2 = x^3 + (ab+ac+bc)x^2 + abc(a+b+c)x + a^2b^2c^2$, with the corresponding point $(abcx, abcy)$. $\square$

Remark 2.5. *We should mention that in [4], two subfamilies of C_k from Theorem 2.5 with rank $\geqslant 2$ and one subfamily with rank $\geqslant 3$ were constructed. However they considered the problem for the integer values of k between 1 and 1000, while in our case the values of $k = \frac{m^2-12}{2(m^2+12)}$, are rational numbers less than 1.*

3. Specialization of High Rank

In this stage we want to find curves having large ranks possible. The main idea here is that a curve is more likely to have large rank if $|E(\mathbb{F}_p)|$ is relatively large for many primes p. We will use the following realization of this idea. For a prime p we put $a_p = a_p(E) = p + 1 - |E(\mathbb{F}_p)|$ and

$$SN(E,N) = \sum_{p \leqslant N, p\ prime} (1 - \frac{p-1}{|E(\mathbb{F}_p)|}) \log(p) = \sum_{p \leqslant N, p\ prime} (\frac{-a_p + 2}{p + 1 - a_p}) \log(p).$$

This summation is defined as Mestre-Nagao sum. In order to give examples of high rank for $E_k : y^2 = x^3 + Ax^2 + Bx$ with A and B in the equation (2.2), we observe $k = p/q$, with $\gcd(p,q) = 1$, $|p|, |q| < 1000$, and Mestre-Nagao sums $SN(1000, E_k) > 20$, $SN(10000, E_k) > 30$, and $SN(100000, E_k) > 40$. Among these sieved k's, it is considered the ones with high Selmer-rank. Then, rank computations are carried out with `MWrank`. This process shows that for $k = \frac{30}{259}, \frac{67}{93}, \frac{88}{31}, \frac{98}{337}, \frac{263}{666}, \frac{280}{919}, \frac{593}{150}, \frac{596}{19}, \frac{609}{76}, \frac{845}{33}$, rank $E_k(\mathbb{Q}) = 7$.

References

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

[2] G. Campbell and E. H. Goins, Heron triangles, Diophantine problems and elliptic curves, *preprint.*

[3] J. Cannon, Mwrank, MAGMA, http://magma.maths.usyd.edu.au, 2003.

[4] A. Dujella, A parametric family of elliptic curves, *Acta Arith.,* 94 (2000), 87-101.

[5] A. Dujella, Diophantine m-tuples and elliptic curves, *J. Theor. Nombres Bordeaux,* 13 (2001), 111-124.

[6] A. Dujella and J. C. Peral, Elliptic curves coming from Heron triangles, *Rocky Mt. J. Math.,* to appear.

[7] N. J. Fine, On rational triangles, *Amer. Math. Monthly.,* 7 (83) (1976), 517-521.

[8] E. H. Goins and D. Maddox, Heron triangles via elliptic curves, *Rocky Mt. J. Math.,* 5 (36) (2006), 1511-1526.

[9] D. Husemoller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

[10] B. Mazur, Rational isogenies of prime degree, (with appendix by D. Goldfeld), *Invent. Math.,* 44 (1978), 129-162.

[11] D. J. Rusin, Rational triangles with equal area, *New York J. Math.,* 4 (1998), 1-15.

[12] W. A. Stein, et al. Sage mathematics software (version 4.7.2). The Sage Development Team, 2011. Online at http://www.sagemath.org/.

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

[14] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Second edition, Taylor & Francis Group, LLC, 2008.

Farzali Izadi
Department of Mathematics
Professor of Mathematics
Azarbaijan Shahid Madani University
Tabriz, Iran
E-mail: farzali.izadi@azaruniv.edu

Foad Khoshnam
Department of Mathematics
Assistant Professor of Mathematics
Azarbaijan Shahid Madani University
Tabriz, Iran
E-mail: khoshnam@azaruniv.edu