ELLIPTIC CURVES AND TRIANGLES WITH THREE RATIONAL MEDIANS

ANDREJ DUJELLA AND JUAN CARLOS PERAL

ABSTRACT. In his paper *Triangles with three rational medians*, Buchholz proves that each such triangle corresponds to a point on a one-parameter family of elliptic curves whose rank is at least 2.

We prove that in fact the exact rank of the family in Buchholz paper is 3. We also exhibit a subfamily whose rank is at least 4 and we prove the existence of infinitely many curves of rank 5 over $\mathbb{Q}$ parametrized by an elliptic curve of positive rank. Finally, we show particular examples of curves within those families having rank 9 and 10 over $\mathbb{Q}$.

1. INTRODUCTION

The existence and parametrization of rational-sided triangles with additional conditions has a long history, see the second volume of the History of the Theory of Numbers by L. E. Dickson [7] for older results. There exists also a more recent and extensive mathematical literature on these topics. See for example [2], [8] and [9] and the references given there. The existence of infinitely many rational-sided triangles with two rational medians is proved in [4]. Often these problems are deeply connected with a family of elliptic curves. This is the case for the problem of the parametrization of all the rational-sided triangles having also their three medians rational. This problem studied by Buchholz in [3], is the object of this note.

Let us briefly sketch the argument of Buchholz. The medians, m_a, m_b, m_c and the sides a, b, c of a triangle satisfy the following relationships:

$$\begin{cases} 4m_a^2 = 2b^2 + 2c^2 - a^2, \\ 4m_b^2 = 2c^2 + 2a^2 - b^2, \\ 4m_c^2 = 2a^2 + 2b^2 - c^2. \end{cases}$$

From here, and factorizing the first two equations over the field $\mathbb{Q}(\sqrt{2})$, Buchholz shows that the sides of all rational-sided triangles with two rational medians are given by

$$\begin{cases} a = -(-1 + r^2 - s - 2rs + r^2 s + 2rs^2)t, \\ b = (1 - r + 2rs + 2r^2 s - s^2 + rs^2)t, \\ c = -(r - r^2 - s - 2rs + r^2 s - s^2 - rs^2)t, \end{cases}$$

where r, s and t are rationals such that $t > 0$, $0 < r, s < 1$ and $r + 2s > 1$. These conditions are a consequence of the triangle inequality applied to the sides. The parameter t is just a scaling factor so it can assume any fixed positive value. The expressions $2b^2 + 2c^2 - a^2$ and $2c^2 + 2a^2 - b^2$ are rational squares and so the corresponding medians m_a and m_b are rational. For the other median m_c to be

2010 *Mathematics Subject Classification.* 11G05.

A. D. was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821. J. C. P. was supported by the UPV/EHU grant EHU 10/05.

rational it must be true that $2a^2 + 2b^2 - c^2$ is a rational square. So

$$\begin{aligned}\frac{4m_c^2}{t^2} =& r^4(1+3s)^2 + 2r^3(1-11s+9s^2+9s^3) + 3r^2(-1-2s+2s^2-6s^3+3s^4)\\ &-2r(1+s)(2-11s+8s^2+3s^3) + (-2+s)^2(1+s)^2. \end{aligned} \tag{1}$$

As said before the parameter t is a scaling factor so it can assume any fixed positive value. From now on we will take $t = 1$.

Remark. Now we include a couple of observations. First, let us mention that a simpler way to get the formulas for a, b and c is the following. Given rationals a, b, c, m_a and m_b satisfying the equations $4m_a^2 = 2b^2+2c^2-a^2$ and $4m_b^2 = 2c^2+2a^2-b^2$, define the rational numbers r and s as

$$r = \big(a\,b - 2\,b\,c + 2\,(a-c)\,m_a\big)/\big(a^2 + a\,b - 2\,c^2 - 2\,c\,m_a\big),$$

$$s = \big(b\,c - 2\,a\,c + 2\,(b-a)\,m_b\big)/\big(b^2 + b\,c - 2\,a^2 - 2\,a\,m_b\big).$$

Then the above formulas for a, b and c follow without having to appeal to factorizations over $\mathbb{Q}(\sqrt{2})$. Second, observe that the following relation holds

$$4(m_a^2 + m_b^2 + m_c^2) = 3(a^2 + b^2 + c^2),$$

which may give an alternative way to get the quartic (1).

Now the quartic (1) is interpreted as a family of quartics in one of the variables (say r) and depending on the other (i.e. s) as the parameter of the family.

Since the point $(0, (-2+s)(1+s))$ is on the quartic (1), it is birationally equivalent to an elliptic curve. Standard transformations carry the quartic to the form

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

where

$$\begin{aligned} A =& 9(1+m^2)^2,\\ B =& -576(-1+m)^2m^2(1+m)^2. \end{aligned}$$

The relationships with r and s are the following:

$$r = \frac{(1+3m)y - (1-11m+9m^2+9m^3)x + 48(1-m)m(1+m)^2(1-3m)}{2((1+3m)^2x + 24(1-m)m(1+m)(1-3m)^2)} \tag{3}$$

and $s = m$.

In [3, Theorem 1], Buchholz states that the rank of this family over $\mathbb{Q}(m)$ is ≥ 2. He also exhibits examples of curves with rank 7 over $\mathbb{Q}$.

The purpose of this note is to prove that in fact the rank of this family of curves over $\mathbb{Q}(m)$ is exactly 3. We also exhibit a subfamily whose rank is ≥ 4 and we show the existence of infinitely many curves of rank 5, parametrized by an elliptic curve of positive rank. Finally, we show curves within these two families having rank 9 and 10 over $\mathbb{Q}$.

2. Rank over $\mathbb{Q}(m)$ is 3

2.1. **Rank over $\mathbb{Q}(m)$ is ≥ 3.** By a direct search into the cubic we find the following three points of infinite order:

$$\begin{aligned} P_1(m) =& (12(-1+m)m(1+m), 36(-1+m)m(1+m)(-1-2m+m^2)),\\ P_2(m) =& (-8(-1+m)^2, 8(-1+m)^2(1+8m+9m^2)),\\ P_3(m) =& (72(1+m)^2, 72(1+m)^2(9+8m+m^2)). \end{aligned}$$

For the value $m = 5$ the curve has rank 3 and the three points become

$$P_1(5) = (1440, 60480)$$
$$P_2(5) = (-128, 34048)$$
$$P_3(5) = (2592, 191808).$$

A calculation with `mwrank` [5] shows that these three points are independent and since the specialization map is a homomorphism, we get that the rank over $\mathbb{Q}(m)$ is ≥ 3.

2.2. **Rank over $\mathbb{Q}(m)$ is equal to 3.** We will now show that the rank of E over $\mathbb{Q}(m)$ is equal to 3. We start by getting the information on the rank of E over $\mathbb{C}(m)$. We will obtain an upper bound for $\operatorname{rank}(E(\mathbb{C}(m)))$ using Shioda's formula [16, Corollary 5.3]:

$$\operatorname{rank}(E(\mathbb{C}(m))) = \operatorname{rank} NS(E, \mathbb{C}) - 2 - \sum_j (n_j - 1).$$

Here $NS(E, \mathbb{C})$ is the Néron-Severi group of E over $\mathbb{C}$, and the sum ranges over all singular fibres of E, with n_j being the number of irreducible components of the fibre. By transforming E into short Weierstrass form $y^2 = x^3 + Cx + D$, we find that $\deg C = 8$ and $\deg D = 12$, which implies that E is a K3 surface (see [11]). Hence, by [1, p. 311], we have that $\operatorname{rank} NS(E, \mathbb{C}) \leq 20$. The numbers n_j can be easily determined from Kodaira types of singular fibres (see [11, Section 4]), which are given in the following table (with the notation: $\alpha = \operatorname{ord}_{m=\mu} C$, $\beta = \operatorname{ord}_{m=\mu} D$, $\delta = \operatorname{ord}_{m=\mu} \Delta$, where $C = -9\,(3 + 76\,m^2 - 110\,m^4 + 76\,m^6 + 3\,m^8)$, $D = 54\,(1+m^2)^2\,(1 + 36\,m^2 - 58\,m^4 + 36\,m^6 + m^8)$ are the coefficients in the short Weierstrass form, while

$$\Delta = 2^{16} \cdot 3^6 \cdot (1-m)^4\, m^4\, (1+m)^4\, (9\,m^4 - 14\,m^2 + 9)\, (m^4 + 34\,m^2 + 1)$$

is the discriminant, and μ_i, $i = 1, 2, \ldots, 8$, are the roots of $(9m^4 - 14m^2 + 9)(m^4 + 34m^2 + 1) = 0$:

	coefficients				
μ	α	β	δ	Kodaira type	$n_j - 1$
0	0	0	4	I_4	3
1	0	0	4	I_4	3
-1	0	0	4	I_4	3
μ_i	0	0	1	I_1	0
∞	0	0	4	I_4	3

Therefore, we have

$$\operatorname{rank}(E(\mathbb{C}(m))) \leq 20 - 2 - 3 - 3 - 3 - 3 = 6.$$

Thus we now know that $3 \leq \operatorname{rank}(E(\mathbb{Q}(m))) \leq 6$. Let us consider now the curve E over $\mathbb{K}(m)$, where $\mathbb{K} = \mathbb{Q}(\sqrt{3}, \sqrt{-3})$. We know that $\operatorname{rank}(E(\mathbb{K}(m))) \leq \operatorname{rank}(E(\mathbb{C}(m))) \leq 6$. On the other hand,

$$\begin{aligned} \operatorname{rank}(E(\mathbb{K}(m))) &= \operatorname{rank}(E(\mathbb{Q}(m))) + \operatorname{rank}(E^{(3)}(\mathbb{Q}(m))) \\ &\quad + \operatorname{rank}(E^{(-3)}(\mathbb{Q}(m))) + \operatorname{rank}(E^{(-1)}(\mathbb{Q}(m))) \\ &\geq \operatorname{rank}(E(\mathbb{Q}(m))) + \operatorname{rank}(E^{(3)}(\mathbb{Q}(m))) + \operatorname{rank}(E^{(-3)}(\mathbb{Q}(m))), \qquad (4) \end{aligned}$$

where $E^{(d)}$ denotes the quadratic d-twist of E (see [14, Lemma 2.1], [15, Lemma 2.1]). We already have from the previous section that $\operatorname{rank}(E(\mathbb{Q}(m))) \geq 3$. So we need lower bounds for the other two summands on the right hand side of (4). We find two independent points

$$P_4(m) = (9(m^2+1)^2, 54(1+m^2)(m^2-2m-1)(m^2+2m-1)),$$
$$P_5(m) = (-18(m^2-2m-1)^2, 54(1+m^2)(m^2-2m-1)(m^2+2m-1),$$

on $E^{(3)}(\mathbb{Q}(m))$ (the independence can be checked by an appropriate specialization, e.g. $m=2$ gives independent points $P_4(2)=(225,-1890)$, $P_5(2)=(-18,-1890)$ on the specialized curve) and one point of infinite order

$$P_6(m) = (36(m^2+1)^2, 108(1+m^2)(m^2-2m-1)(m^2+2m-1))$$

on $E^{(-3)}(\mathbb{Q}(m))$. Since for $m=2$ the point $P_6(2)=(900,-3780)$ on $E^{(-3)}$ is of infinite order, we conclude that $\mathrm{rank}(E^{(-3)}(\mathbb{Q}(m))) \geq 1$. Therefore, we get that

$$\mathrm{rank}(E^{(3)}(\mathbb{Q}(m))) \geq 2 \quad \text{and} \quad \mathrm{rank}(E^{(-3)}(\mathbb{Q}(m))) \geq 1.$$

Comparing these lower bounds for the ranks on the right hand side of (4) with the upper bound for the left hand side $\mathrm{rank}(E(\mathbb{K}(m))) \leq 6$, we conclude that all these bounds are indeed equalities. In particular,

$$\mathrm{rank}(E(\mathbb{Q}(m))) = 3.$$

3. Subfamilies whose rank over $\mathbb{Q}(m)$ is ≥ 4

A new point, with x-coordinate

$$9m(-1+m)^2, \tag{5}$$

is on the cubic (2) if the expression $9-73m+9m^2$ is a rational square. This turns out to be equivalent to choosing

$$m = \frac{(-3+u)(3+u)}{-73+6u}.$$

The coefficients of the subfamily, written as $y^2 = x^3 + A_4x^2 + B_4x$, are

$$A_4 = 9(5410-876u+18u^2+u^4)^2,$$
$$B_4 = -576(-3+u)^2(3+u)^2(-73+6u)^2(64-6u+u^2)^2(-82+6u+u^2)^2.$$

Observe that we get an elliptic curve for rational $u \neq \pm 3, 73/6$. The x-coordinates of four independent points are:

$$Q_1(u) = 12(-3+u)(3+u)(-73+6u)(64-6u+u^2)(-82+6u+u^2),$$
$$Q_2(u) = -8(-73+6u)^2(-82+6u+u^2)^2,$$
$$Q_3(u) = 72(-73+6u)^2(-82+6u+u^2)^2,$$
$$Q_4(u) = 9(-3+u)(3+u)(-73+6u)(64-6u+u^2)^2.$$

In order to prove that this subfamily has rank at least 4 over $\mathbb{Q}(u)$ we use again the specialization. Take $u=2$, then the curve has rank exactly 4 and the four points, with their y-coordinates included, are

$$R_1 = (-13527360, 174746436480)$$
$$R_2 = (-129669408, 195282128448)$$
$$R_3 = (1167024672, 41959205057088)$$
$$R_4 = (8608320, 60791955840).$$

The Cremona program `mwrank` [5] gives the independence of these four points, and the fact that the specialization map is a homomorphism implies that the rank of the subfamily over $\mathbb{Q}(u)$ is at least 4.

Another way of obtaining a subfamily with rank ≥ 4 is by imposing

$$x = \frac{16(-1+m)^2(1+m)^2(9+4m^2)}{(-3+m^2)^2} \tag{6}$$

as x-coordinate on the curve (2). This leads to the condition that $4m^2+9$ is a rational square, and thus

$$m = -\frac{(-3+u)(3+u)}{4u}.$$

We get the subfamily $y^2 = x^3 + A_4' x^2 + B_4' x$, where

$$\begin{aligned} A_4' &= 9(81 - 2u^2 + u^4)^2, \\ B_4' &= -9216(-9+4u+u^2)^2(-3+u)^2(3+u)^2u^2(-9-4u+u^2)^2, \end{aligned}$$

which gives an elliptic curve for rational $u \neq 0, \pm 3$. The x-coordinates of four independent points are:

$$\begin{aligned} Q_1'(u) &= -48u(-3+u)(3+u)(-9+4u+u^2)(-9-4u+u^2), \\ Q_2'(u) &= -128u^2(-9+4u+u^2)^2, \\ Q_3'(u) &= 1152u^2(-9+4u+u^2)^2, \\ Q_4'(u) &= -96u(3+u)^2(-9-4u+u^2)(-9+4u+u^2), \end{aligned}$$

where by doubling the last point we get the point with x-coordinate (6). As before, the specialization $u=2$ shows that these four points are independent, which implies that the rank of this subfamily over $\mathbb{Q}(u)$ is ≥ 4.

3.1. **Families of rank 5.** The condition for

$$64(-73+6u)^2(64-6u+u^2)(-82+6u+u^2)$$

to be the x-coordinate of a new point on the curve $y^2 = x^3 + A_4x^2 + B_4x$, gives the quartic equation

$$v^2 = -285724 + 48180u - 3618u^2 + 91u^4.$$

Observe that $(14, 1782)$ is a rational point on the curve, so the quartic curve is birationally equivalent to the elliptic curve

$$w^2 = z^3 + 99640228z - 43125200064 \tag{7}$$

whose rank is 1. Now, a rational point (z, w) gives rise to the coordinate

$$u = \frac{2(567w + 6109z + 176619992)}{81w + 21493z - 5210906}.$$

In particular, the generator $(z, w) = (9686197/6561, 173996677855/531441)$ maps to $u = 14$.

Now, with this choice of u, there is a point (x, y) having x-coordinate

$$Q_5(u) = 64(-73+6u)^2(64-6u+u^2)(-82+6u+u^2).$$

Choosing $(u, v) = (14, 1782)$ we find $m = 17$, and so we have the point $(x, y) = (269862912, 5289852801024)$ and this point is independent of the four points with x-coordinates $Q_i(14)$, $i = 1, 2, 3, 4$. So the points on the elliptic curve (7) give a parametrization for an infinite family of curves with rank at least 5.

Furthermore, for

$$64(-3+u)(3+u)(-73+6u)(64-6u+u^2)^2,$$

the condition to be the x-coordinate of a new point on the curve $y^2 = x^3 + A_4x^2 + B_4x$ gives the quartic equation

$$v^2 = 96651 - 11826u - 5167u^2 + 438u^3 + 9u^4.$$

In this case $(u, v) = (15, 831)$ is a rational point on the curve, so the quartic curve is birationally equivalent to the elliptic curve

$$w^2 = z^3 - z^2 - 17558520z + 12652261632, \tag{8}$$

whose rank is 2. In fact, a rational point (z, w) gives rise to the coordinate

$$u = \frac{3(w + 201z - 1032844)}{w + 91 - 67704}.$$

In particular, the generator $(z, w) = (-17099/4, 782925/8)$ maps to $u = 15$. Now there is a point (x, y) having x-coordinate

$$Q_6(u) = 64(-3 + u)(3 + u)(-73 + 6u)(64 - 6u + u^2)^2.$$

Choosing $(u, v) = (15, 831)$ we find $m = 216/17$, and so we have the point $(x, y) = (9306551808, 1539015165937152)$ and this point is independent of the four points with x-coordinates $Q_i(15)$, $i = 1, 2, 3, 4$. So the points on the elliptic curve (8) also give a parametrization for an infinite family of curves with rank at least 5.

Finally, we construct a new infinite family of curves with rank ≥ 5 by finding the intersection of the two subfamilies with rank ≥ 4 given in Section 3. We have

$$m = \frac{(-3 + u')(3 + u')}{-73 + 6u'} = \frac{-(-3 + u)(3 + u)}{4u},$$

and by solving this equation for u', we get the condition that $729 - 2628u - 18u^2 + 292u^3 + 9u^4$ is a rational square, say v^2. This quartic has a rational point $(u, v) = (0, 27)$, so it is equivalent to the elliptic curve

$$w^2 = z^3 - 49608z + 1875393 \tag{9}$$

whose rank is 4. A point of infinite order $(w, z) = (121/4, -5075/8)$ gives $u = 1/4$, $v = 243/4$, $u' = 27/4$, $m = 143/16$, and we check that the five points with x-coordinates $P_1(m)$, $P_2(m)$, $P_3(m)$, (5) and (6) for $m = 143/16$ are independent. Thus the points on elliptic curve (9) give another parametrization for an infinite family of curves with rank ≥ 5.

4. Examples of curves with higher rank

In [3], several curves with rank 7 over $\mathbb{Q}$ in the family (2) were found, e.g. for $m = 17/70$. We searched for curves with higher rank, and we are able to find several examples with rank 9 and one example with rank 10. We use the sieving method based on Mestre-Nagao sums

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

(see [10, 12, 6]). For curves with large values of $S(N, E)$, we compute the Selmer rank, as an upper bound for the rank which is easier to compute than the rank itself. We combine these information with the conjectural parity for the rank. Finally, we try to compute the rank and find generators for the best candidates for large rank. We have implemented this procedure in PARI [13], using [5] for the computation of the Selmer rank and the rank. Since the family with rank ≥ 4 from Section 3 has relatively large coefficients, we were able to find only one curve with rank 9 within this family, and this was for $u = 211/77$. In the family (2) with generic rank 3, we find curves with rank 9 for the following values of the parameter m: 3516/2009, 3559/1868, 4633/208, 5159/136, 5421/614, 5525/1507. Finally, in the same family, for $m = 6148/5537$ we get the curve with rank equal to 10. The equation in minimal Weierstrass form is

$$\begin{aligned} y^2 + xy &= x^3 - 483774480338253198982501853180x \\ &\quad + 1293670641838891456792203018408268009105167 52. \end{aligned}$$

The ten independent points found by and further reduced by the LLL algorithm are:

$$\begin{aligned}
P_1 &= (228494903185104, 5545877808125415910508), \\
P_2 &= (66468030282664, 9874471247265386096148), \\
P_3 &= (309508339636324, 3047015930384441473908), \\
P_4 &= (46835094015384, 10334997553404168378148), \\
P_5 &= (-91659466587276, -13150646396773223885032), \\
P_6 &= (315440066829324, 2855216955196324201268), \\
P_7 &= (412578403366594, 405546636182828 19728), \\
P_8 &= (192035485460164, 6599015749717042248648), \\
P_9 &= (389692778108644, 1502263526632576 21928), \\
P_{10} &= (1599952885983644, 58745116981933330426928).
\end{aligned}$$

Remark. By using formula (3), we find that the rational point $P_1 = (228494903185104, 5545877808125415910508)$ corresponds to the following rational triangle with rational medians:

$$\begin{aligned}
a &= 4643288021024608029 50, & m_a &= 3694779628352258806 53, \\
b &= 381149866245702170 08, & m_b &= 5450920364610501608 94, \\
c &= 6159348959649055730 02, & m_c &= 1169745498680115643 41.
\end{aligned}$$

Acknowledgement. The authors would like to thank Ivica Gusić and Filip Najman for useful comments on the previous version of this paper.

The authors would like to thank also to the anonymous referee for a careful reading and his detailed remarks and suggestions which significantly improved our paper.

References

[1] W. P. Barth, K. Hulek, C. A. M. Peters, A. Van de Ven, Compact Complex Surfaces, Springer-Verlag, 2004.

[2] A. Bremner, On Heron triangles, Ann. Math. Inform. 33 (2006), 15–21.

[3] R. H. Buchholz, Triangles with three rational medians, J. Number Theory, 97 (2002), 113–131.

[4] R. H. Buchholz, R. L. Rathbun, An infinite set of Heron triangles with two rational medians, Amer. Math Montly 104 (1997), 107–115.

[5] J. Cremona, Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge, 1997.

[6] A. Dujella, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, Glas. Mat. Ser. III 42 (2007), 3–18.

[7] L. E. Dickson, History of the Theory of Numbers, Carnegie Institution, Washington, 1919

[8] E. H. Goins, D. Maddox, Heron triangles via elliptic curves, Rocky Mountain J. Math. 36 (2006), 1511–1526

[9] R. van Luijk, An elliptic $K3$ surface associated to Heron triangles, J. Number Theory 123 (2007), 92–119.

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

[11] R. Miranda, An overview of algebraic surfaces, in Algebraic Geometry (Ankara, 1995),Lecture Notes in Pure and Appl. Math. 193, Dekker, New York, 1997, pp. 157–217.

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

[13] PARI/GP, version 2.4.0, Bordeaux, 2008, http://pari.math.u-bordeaux.fr.

[14] K. Rubin, A. Silverberg, Twists of elliptic curves of rank at least four, in: Ranks of eliiptic curves and Random Matrix Theory, Cambridge University Press, 2007, pp. 177–188.

[15] K. Rubin, A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, Exper. Math. 10 (2001), 559–569.

[16] T. Shioda, On the Mordell - Weil lattices, Comment. Math.Univ. St. Pauli 39 (1990), 211–240.

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

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address, A. Dujella: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, UPV/EHU, Aptdo. 644, 48080 Bilbao, Spain

E-mail address, J. C. Peral: juancarlos.peral@ehu.es