ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 48, Number 1, 2018

ON RATIONAL TRIANGLES VIA ALGEBRAIC CURVES

MOHAMMAD SADEK AND FARIDA SHAHATA

ABSTRACT. A rational triangle is a triangle with rational side lengths. We consider three different families of rational triangles having a fixed side and whose vertices are rational points in the plane. We display a one-to-one correspondence between each family and the set of rational points of an algebraic curve. These algebraic curves are: a curve of genus 0, an elliptic curve and a genus 3 curve. We study the set of rational points on each of these curves and explicitly describe some of its rational points.

1. Introduction. Several arithmetic questions on the geometry of the Euclidean plane have been a subject of interest in mathematical literature. One of the techniques for tackling such a question is to construct a system of diophantine equations whose set of rational solutions provides an answer. Therefore, answering these questions reveals the interplay between analytical geometry and arithmetical geometry.

A rational subset of the plane is said to be *rational* if all pairwise distances among its points are rational. In 1945, Ulam wondered which rational subsets S of the plane are infinite. It is well known that a line and a circle have dense rational subsets. Erdős conjectured that S must be of a very special type. In [**10**], it was proven that the circle and the line are the only algebraic curves containing an infinite rational set. In order to prove the result, given an algebraic curve C, they constructed a new curve C' of genus $g \geq 2$ whose number of rational points is larger than the size of any rational subset of the algebraic curve C. According to Faltings' theorem, the number of rational points on C' is finite, hence, the result.

2010 AMS *Mathematics subject classification.* Primary 11G05, 11G30.
Keywords and phrases. Rational triangles, rational points, algebraic curves.
Received by the editors on June 17, 2016, and in revised form on December 1, 2016.
DOI:10.1216/RMJ-2018-48-1-325 Copyright ©2018 Rocky Mountain Mathematics Consortium

One more condition may be imposed on rational sets; their points may be required to be rational, i.e., the x- and y- coordinates of the points are rational numbers. In [**7**], it was proven that there exist infinitely many rational points on the x-axis lying at rational distances from four fixed points on the y-axis. The proof involves constructing an elliptic curve with positive rank. In [**5**], it was shown that, if the number of points on the y-axis is greater than four, then there are only finitely many rational points on the x-axis lying at rational distances from the points on the y-axis. This holds since the number of such points is the number of rational points on an algebraic curve whose genus is $g > 1$.

A *rational triangle* is a triangle whose side lengths are rational numbers. It is easily seen that the vertices of a rational triangle make up a rational set whose size is three. An arithmetical question on rational triangles which has occupied a prominent position since ancient times is which rational numbers appear as the area of a right-angled rational triangle. These rational numbers are called *congruent numbers*. A rational number n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ is of positive rank.

A *Heron triangle* is a rational triangle whose area is rational. In [**1, 3, 4, 8, 11**], rational and Heron triangles with certain properties were investigated via the study of algebraic curves and surfaces. Moreover, rational triangles were used to explore the size of the sets of rational points of some algebraic curves.

In this note, we are interested in rational triangles whose vertices are rational points in the plane. We consider three families of rational triangles with rational vertices. The first family of such triangles consists of isosceles triangles. It is well known that, given a line segment ℓ of rational length and with rational endpoints, there exist infinitely many isosceles triangles whose base is ℓ, namely, those whose vertices are points on the perpendicular bisector of ℓ. This yields that, out of the latter triangles, there are infinitely many whose sides are rational, and the third vertex is a rational point in the plane, in other words, there are infinitely many rational points on the perpendicular bisector of ℓ which lie at a rational distance from the endpoints of ℓ. This is proved by showing that these rational points on the perpendicular bisector are in one-to-one correspondence with the rational points on a genus 0 curve. In addition, we explicitly describe these points.

The second family of rational triangles consists of the triangles for which two of the vertices are the origin and a fixed rational point on the x-axis, whereas the third vertex is a rational point on a fixed line in the plane. These triangles possess rational areas; therefore, they are Heron triangles. We attach an elliptic curve of positive rank to this family, which implies the existence of infinitely many such triangles. We further study this elliptic curve by shedding some light on its torsion subgroup and detecting conditions that force the rank to be at least 2.

The third family consists of the triangles for which two of the vertices are the origin and a fixed rational point Q on the x-axis, and the third vertex is a rational point on the parabola $x = y^2$. It follows that such a triangle is a Heron triangle. Unlike the first and second families of triangles in this note, the third family turns out to consist of finitely many triangles. The reason is that the existence of a triangle in this family is equivalent to the existence of a rational point on a genus 3 curve. We display infinitely many rational points Q for which the corresponding family of rational triangles is nonempty. The latter is achieved by exhibiting an explicit rational point on the corresponding genus 3 curve.

2. Rational isosceles triangles and genus 0 curves. We recall that a rational triangle is a triangle with rational side lengths. A point in the xy-plane is rational if its x- and y-coordinates are rational.

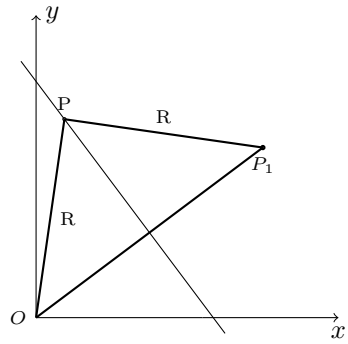

FIGURE 1.

Suppose that we fix a rational point $P_1 = (X_1, Y_1)$ in the xy-plane at a rational distance from the origin O where P_1 and O are distinct points. In this section, we consider the problem of finding rational points $P = (X, Y)$ which lie at the same rational distance, say R, from the origin O and the point P_1. In other words, we are seeking the rational isosceles triangles $\triangle OPP_1$ with the fixed base OP_1 and the vertex P itself being rational. We note that the point P lies on the perpendicular bisector of the line segment joining O and P_1, and that

$$R > \frac{\sqrt{X_1^2 + Y_1^2}}{2}.$$

The rational point $P = (X, Y)$, together with the rational distance R, form a solution

$$(x : y : z : w) = (X : Y : R : 1)$$

of the following system of Diophantine equations

$$\begin{aligned} x^2 + y^2 &= z^2 \\ (x - X_1 w)^2 + (y - Y_1 w)^2 &= z^2. \end{aligned} \tag{2.1}$$

Equation (2.1) describes the intersection curve of two quadratic surfaces in $\mathbb{P}^3$. We will call this curve $E_{(X_1,Y_1)}$. The curve $E_{(X_1,Y_1)}$ is birationally equivalent, hence isomorphic, to the singular cubic curve $C_{(X_1,Y_1)}$, defined by

$$y^2 = -16(X_1^2 + Y_1^2)x(x + 1)^2,$$

see for example [**2,** Theorem 2.8]. The curve $C_{(X_1,Y_1)}$ has a node at the point $S = (x, y) = (-1, 0)$. There is an isomorphism of abelian groups between the nonsingular part $C_{(X_1,Y_1)}(\mathbb{Q}) \setminus \{S\}$ of $C_{(X_1,Y_1)}$ and the multiplicative group $\mathbb{Q}^\times$ of $\mathbb{Q}$, see [**9,** Chapter 3, Exercise 3.5], in other words, a rational parametrization may be found for $C_{(X_1,Y_1)} \setminus \{S\}$.

Now, we let $\mathcal{R}$ denote the set of all rational isosceles triangles $\triangle OPP_1$ with base OP_1 where $|OP| = |PP_1| = R$ and the vertices P and P_1 are rational. We note that a triangle in $\mathcal{R}$ is determined completely by the vertex P.

Proposition 2.1. *A triangle $\triangle OP_1P$ with base OP_1 lies in $\mathcal{R}$ if and only if there exists a $t \in \mathbb{Q}$ such that*

$$X = \frac{X_1}{2} \pm \frac{t^2X_1(X_1^2+Y_1^2) - 4t(X_1^2+Y_1^2) + 4X_1}{2(t^2(X_1^2+Y_1^2)-4)},$$
$$Y = \frac{Y_1}{2} \pm \frac{X_1(4t(X_1^2+Y_1^2) - t^2X_1(X_1^2+Y_1^2) - 4X_1)}{2Y_1(t^2(X_1^2+Y_1^2)-4)},$$
$$R = \frac{(t(X_1^2+Y_1^2)-2X_1)^2+4Y_1^2}{2t^2Y_1(X_1^2+Y_1^2)-8Y_1}.$$

Proof. The perpendicular bisector L of the line segment joining O and $P_1 = (X_1, Y_1)$ is described by

$$L : y = -\frac{X_1}{Y_1}x + \frac{X_1^2+Y_1^2}{2Y_1}.$$

Since $P = (X, Y)$ lies on L and the distance between P and O is R, i.e., $X^2 + Y^2 = R^2$, by substitution and solving a quadratic equation, we obtain

$$X = \frac{X_1}{2} \pm \frac{Y_1}{2}\sqrt{\frac{4R^2}{X_1^2+Y_1^2} - 1}.$$

Thus, for X to be rational, we need to solve the following diophantine equation:

$$\frac{4R^2}{X_1^2+Y_1^2} - 1 = \delta^2. \tag{2.2}$$

Since $X_1^2 + Y_1^2 \neq 0$, we may assume without loss of generality that $Y_1 \neq 0$. Now the point

$$(R, \delta) = \left(\frac{X_1^2+Y_1^2}{2Y_1}, \frac{X_1}{Y_1}\right)$$

is a rational solution for the latter diophantine equation. It may be concluded that (2.2) has infinitely many rational solutions that can be parameterized as:

$$(R,\delta) = \left(\frac{(t(X_1^2+Y_1^2)-2X_1)^2+4Y_1^2}{2t^2Y_1(X_1^2+Y_1^2)-8Y_1}, \frac{t^2X_1(X_1^2+Y_1^2)-4t(X_1^2+Y_1^2)+4X_1}{Y_1(4-t^2(X_1^2+Y_1^2))}\right),$$

$t \in \mathbb{Q}$. Thus,

$$X = \frac{X_1}{2} \pm \frac{t^2 X_1(X_1^2 + Y_1^2) - 4t(X_1^2 + Y_1^2) + 4X_1}{2(t^2(X_1^2 + Y_1^2) - 4)}. \qquad \square$$

It is worth mentioning that, for each $t \in \mathbb{Q}$, we obtain a distance R and two values for X, which correspond to the points lying on the perpendicular bisector at a distance R from the origin O. Thus, the triangles that correspond to these two X-values are similar.

Remark 2.2. Proposition 2.1 yielded a parametric solution $(x : y : z : 1) = (X : Y : R : 1)$ to the curve of intersection of the two quadratic surfaces in (2.1).

Corollary 2.3. *Given a rational point P_1 in the xy-plane lying at a rational distance from the origin O, there exist infinitely many rational points P such that $\triangle OPP_1$ is a rational isosceles triangle for which $|OP| = |PP_1|$.*

Proof. This is a direct consequence of Proposition 2.1. $\square$

Remark 2.4. In Corollary 2.3, the origin O may be replaced with any rational point O' using a rational change of coordinates.

Example 2.5. Taking $P_1 = (3, 4)$ and $t = 0.5$, we obtain the point

$$P = \left(-\frac{25}{9}, \frac{125}{24} \right),$$

which lies at a distance

$$R = \frac{425}{72}$$

from both the origin and P_1. The triangle $\triangle OPP_1$ is rational.

3. Elliptic curves and rational triangles. In this section, we investigate a family of rational triangles with a fixed side and link the number of these triangles with the size of the rational subgroup of an elliptic curve. We recall that a set $\mathcal{S}$ of points in the xy-plane is said to be a rational distance set if the distance between any two points in $\mathcal{S}$ is rational.

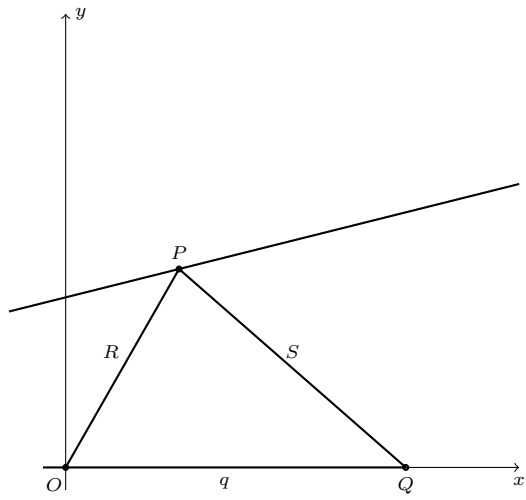

FIGURE 2.

3.1. Description of the problem. Let b, q and m be rational numbers. We consider the point $Q = (q, 0)$ on the x-axis and the line $L : y = mx + b$. We are looking for the rational points $P = (X, Y)$ lying on L at a rational distance, say R, from the origin O and at a rational distance, say S, from Q. This construction yields a rational distance set $\{O, P, Q\}$ of rational points. In other words, we are trying to find all of the rational triangles $\triangle OQP$ with the fixed base OQ and where the vertex P lies on the line $L : y = mx + b$. We set $A_{m,b,q}$ as the set of all such triangles. We remark that any triangle in $A_{m,b,q}$ is a Heron triangle. In fact, the area of a triangle $\triangle OQP$ is $|q(mX + b)|/2$.

The point $P = (X, Y)$ is a vertex of a triangle in $A_{m,b,q}$ if and only if $(x_1 : x_2 : x_3 : x_4) = (X : R : S : 1)$ is a solution of the following system of diophantine equations

$$\begin{aligned} (1 + m^2)x_1^2 + 2mbx_1x_4 + b^2x_4^2 &= x_2^2 \\ (1 + m^2)x_1^2 + 2(mb - q)x_1x_4 + (b^2 + q^2)x_4^2 &= x_3^2. \end{aligned} \tag{3.1}$$

System (3.1) represents an intersection curve $C_{m,b,q}$ of two quadratic surfaces in $\mathbb{P}^3$. We note that, with a simple change of variables, $C_{0,b,q}$ was extensively studied in relation to Heron triangles in [**1**].

If $m \neq 0$, the point

$$\left(-\frac{b}{m} : \pm\frac{b}{m} : \pm\left(\frac{b}{m} + q\right) : 1 \right)$$

is a rational point on the curve. By computing the discriminant of $C_{m,b,q}$, see **[2]**, we conclude that, for rational numbers b, m and q with $b \neq 0$, $q \neq 0$ and $q \neq -b/m$, the curve $C_{m,b,q}$ is an elliptic curve.

Let $C_{m,b,q}(\mathbb{Q})$ be the set of rational points on $C_{m,b,q}$. We define the following relation on $C_{m,b,q}(\mathbb{Q}) \setminus \{x_4 = 0\}$: the points

$$\left(\frac{x_1}{x_4} : \frac{x_2}{x_4} : \frac{x_3}{x_4} : 1\right) \sim \left(\frac{x_1'}{x_4'} : \frac{x_2'}{x_4'} : \frac{x_3'}{x_4'} : 1\right)$$

if

$$\frac{x_1}{x_4} = \frac{x_1'}{x_4'}, \quad \frac{x_2^2}{x_4^2} = \frac{x_2'^2}{x_4'^2} \quad \text{and} \quad \frac{x_3^2}{x_4^2} = \frac{x_3'^2}{x_4'^2}.$$

This is clearly an equivalence relation; therefore, we let $\mathcal{C}$ denote the set of equivalence classes.

Lemma 3.1. *There exists a one-to-one correspondence between the set of triangles $A_{m,b,q}$ and the set of equivalence classes $\mathcal{C}$.*

Proof. We define the one-to-one correspondence as follows. A triangle $\triangle OQP \in A_{m,b,q}$ will be sent to the equivalence class containing $(X : R : S : 1)$, where $P = (X, Y)$, R is the rational distance $|OP|$ and S is the rational distance $|PQ|$. An equivalence class in $\mathcal{C}$, say represented by the rational point $(x_1 : x_2 : x_3 : x_4) \in C_{m,b,q}(\mathbb{Q})$, $x_4 \neq 0$, will be sent to the triangle OQP, where

$$P = \left(\frac{x_1}{x_4}, m\frac{x_1}{x_4} + b\right).$$

This point lies at rational distance

$$\left|\frac{x_2}{x_4}\right|$$

from O and at rational distance

$$\left|\frac{x_3}{x_4}\right|$$

from Q. □

Remark 3.2. The rational side lengths q, R and S of a triangle in $A_{m,b,q}$ force

$$X = \frac{q^2 + R^2 - S^2}{2q}$$

itself to be rational. Thus, $A_{m,b,q}$ is precisely the set of Heron triangles with a fixed side of length q and a vertex on the line $y = mx + b$.

We now know that $C_{m,b,q}$ is an elliptic curve, except for finitely many possibilities for the values of b, m and q, described as the intersection of two quadratic surfaces in $\mathbb{P}^3$. We may wish to obtain a Weierstrass equation describing $C_{m,b,q}$. Indeed, when $b \neq 0$, $q \neq 0$ and $q \neq -b/m$, the curve $C_{m,b,q}$ is isomorphic to the elliptic curve $E_{m,b,q}$ described by the Weierstrass equation

$$y^2 = x^3 - 27I_{m,b,q}x - 27J_{m,b,q},$$

see [**2**], where

$$\begin{aligned} I_{m,b,q} &= 256(b^4+2b^3mq+(5m^2+4)b^2q^2+4mb(m^2+1)q^3+(m^2+1)^2q^4), \\ J_{m,b,q} &= 4096(2b^2+2bmq+(m^2+1)q^2) \\ &\quad \cdot (b^4+2b^3mq-b^2(7m^2+8)q^2-8bm(m^2+1)q^3-2(m^2+1)^2q^4). \end{aligned}$$

We recall that two elliptic curves defined over $\mathbb{Q}$ by the short Weierstrass equations $E_i : y^2 = x^3 + A_ix + B_i$ are isomorphic if and only if $\lambda^4 A_1 = A_2$ and $\lambda^6 B_1 = B_2$, for some nonzero λ in $\mathbb{Q}$.

In addition, we note that $I_{m,b,q} = b^4 I_{m,1,q/b}$ and $J_{m,b,q} = b^6 J_{m,1,q/b}$. Thus, given that $b \neq 0$, we obtain the next result.

Proposition 3.3. *The elliptic curves $E_{m,b,q}$ and $E_{m,1,q/b}$ are isomorphic.*

In view of Proposition 3.3 we will assume from now on that $b = 1$. Given q and m in $\mathbb{Q}^*$ such that $q \neq -1/m$, we will write $C_{m,q}$ and $E_{m,q}$ instead of $C_{m,1,q}$ and $E_{m,1,q}$, respectively. The curve $C_{m,q}$ is given by the intersection of the following two quadratic surfaces, see (3.1),

$$\begin{aligned} (1+m^2)x_1^2 + 2mx_1x_4 + x_4^2 &= x_2^2 \\ (1+m^2)x_1^2 + 2(m-q)x_1x_4 + (1+q^2)x_4^2 &= x_3^2; \end{aligned} \tag{3.2}$$

moreover, the elliptic curve $E_{m,q}$ is described by the following Weierstrass equation:

(3.3)
$$\begin{aligned} y^2 = x^3 &- \frac{1}{3}[(m^2+1)^2q^4 + 4m(m^2+1)q^3 + (5m^2+4)q^2 + 2mq + 1]x \\ &+ \frac{1}{27}[2(m^2+1)^2q^4 + 8m(m^2+1)q^3 + (7m^2+8)q^2 - 2mq - 1] \\ &\cdot [(m^2+1)q^2 + 2mq + 2]. \end{aligned}$$

The explicit formulae for the isomorphism between the elliptic curves $C_{m,q}$ and $E_{m,q}$ are given in Appendix A.

3.2. Torsion subgroup of $E_{m,q}(\mathbb{Q})$. We show that $E_{m,q}(\mathbb{Q})$ contains the subgroup $\mathbb{Z}_2$. Moreover, we characterize those values for m and q such that $E_{m,q}(\mathbb{Q})$ contains $\mathbb{Z}_2 \times \mathbb{Z}_2$.

In order to find the points of order 2 on $E_{m,q}$, we need to find the zeros of the polynomial $f_{m,q}(x)$ in the Weierstrass equation $y^2 = f_{m,q}(x)$, (3.3), describing the curve. Factoring the polynomial $f_{m,q}(x)$ yields that $x_1 = ((m^2+1)q^2 + 2mq + 2)/3$ is a zero of $f_{m,q}(x)$. In fact, this point $(x_1, 0)$ of order 2 corresponds to the rational point

$$\left(-\frac{1}{m} : -\frac{1}{m} : -q - \frac{1}{m} : 1 \right)$$

in $C_{m,q}(\mathbb{Q})$. The existence of the point $(x_1, 0)$ ensures that $E_{m,q}(\mathbb{Q})$ contains $\mathbb{Z}_2$.

In fact, the other two zeros x_2, x_3 of $f_{m,q}(x)$ are given by

$$-((m^2+1)q^2 + 2mq + 2)/6 \pm q\sqrt{(1+m^2)((1+m^2)q^2 + 4mq + 4)}/2.$$

Therefore, that the torsion subgroup of $E_{m,q}(\mathbb{Q})$ contains $\mathbb{Z}_2 \times \mathbb{Z}_2$ is equivalent to $(1+m^2)((1+m^2)q^2+4mq+4)$ being a complete $\mathbb{Q}$-square.

For a fixed value of $m \in \mathbb{Q}$, the conic may be parameterized as $t^2 = (1+m^2)((1+m^2)q^2 + 4mq + 4)$ and the following value obtained for q which forces the torsion subgroup of $E_{m,q}(\mathbb{Q})$ to contain $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$q := q(n) = \frac{1 - m^2(2+3m^2) + 2(1+m^2)n + n^2}{m(1 + m^2(2+m^2) - n^2)}, \quad n \in \mathbb{Q}.$$

Proposition 3.4. *The torsion subgroup of the elliptic curve $E_{m,q}(\mathbb{Q})$ contains the cyclic group $\mathbb{Z}_2$. Furthermore, for a fixed value of m, there exist infinitely many values for q such that the torsion subgroup of $E_{m,q}(\mathbb{Q})$ contains $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Now, we will introduce infinitely many values for q such that the torsion subgroup of $E_{m,q}$ contains a point of order 4.

Proposition 3.5. *For some nonzero rational m, if*

$$q = \frac{4(2t - m)}{1 + m^2 - 4t^2}$$

for some $t \in \mathbb{Q}$, such that

$$t \neq m \pm \frac{\sqrt{1 + m^2}}{2},$$

then the point $P = (x, y)$ given by

$$x = \frac{m^4 - 24m^3t + (104t^2 + 6)m^2 - mt(160t^2 + 24) + 80t^4 + 24t^2 + 5}{3(m^2 - 4t^2 + 1)^2}$$

$$y = -\frac{2(3m^2 - 8mt + 4t^2 - 1)(m^2 - 4mt + 4t^2 + 1)}{m^2 - 4t^2 + 1^2}$$

is a point of order 4 in $E_{m,q}(\mathbb{Q})$.

Proof. We first note that, if

$$t = m \pm \frac{\sqrt{1 + m^2}}{2},$$

then $q = -1/m$, and hence, $E_{m,q}$ is a singular curve. The order of P can be easily checked using the duplication formula on $E_{m,q}$, see, for example, [**9,** page 59]. In fact,

$$x(2P) = \frac{2(4t^4 - 8t^3 + 16t^2 - 12t + 3)}{3(2t^2 - 1)^2}$$

and $y(2P) = 0$. □

Remark 3.6. Point P in Proposition 3.5 is in correspondence with the following rational point in $C_{m,q}(\mathbb{Q})$, see (3.2),

$$\left(\frac{q}{2} : \sqrt{\frac{1+m^2}{4}q^2+mq+1} : \sqrt{\frac{1+m^2}{4}q^2+mq+1} : 1\right)$$
$$= \left(2\frac{2t-m}{1+m^2-4t^2} : \frac{m^2-4mt+4t^2+1}{m^2-4t^2+1} : \frac{m^2-4mt+4t^2+1}{m^2-4t^2+1} : 1\right).$$

The latter point corresponds to the isosceles triangle in the set $A_{m,q}$, whose base is $|q|$, and the two other sides are of length

$$\frac{m^2-4mt+4t^2+1}{m^2-4t^2+1}.$$

Note that the area of this triangle is

$$\left|\frac{q(qm+2)}{4}\right| \in \mathbb{Q}.$$

3.3. Rank of $E_{m,q}$. Now, we shall investigate the rank of $E_{m,q}(\mathbb{Q})$ and see the impact of the positivity of the rank on the size of the set $A_{m,q}$.

Theorem 3.7. $\operatorname{Rank} E_{m,q}(\mathbb{Q}(m,q)) \geq 1$.

Proof. Point

$$P_{m,q} = \left(-\frac{(2m^2-1)q^2+4mq+1}{3},\ q(mq+1)^2\right)$$

is a point in $E_{m,q}(\mathbb{Q}(m,q))$. By specializing with the values $m=1$ and $q=1$, the elliptic curve $E_{1,1}(\mathbb{Q})$ is defined by $y^2=x^3-8x+8$, where $P_{1,1}=(-2,4)\in E_{1,1}(\mathbb{Q})$ is of infinite order. Therefore, by Silverman's specialization theorem, [**9,** Appendix C, Section 20], $\operatorname{rank} E_{m,q}(\mathbb{Q}(m,q)) \geq 1$. □

Corollary 3.8. *For all but finitely many pairs $(m,q)\in\mathbb{Q}\times\mathbb{Q}$, the set $A_{m,q}$ contains infinitely many rational triangles with base $|q|$ whose vertices lie on the line $y=mx+1$.*

In what follows, we choose m and q so that we can construct elliptic curves $E_{m,q}$ with higher rank.

Theorem 3.9. *Set* $q := q(h) = (1-h^2)/2h$. *This yields*

$$\operatorname{rank} E_{m,q}(\mathbb{Q}(m,h)) \geq 2.$$

Proof. The point $Q_{m,q} = (x_{m,h}, y_{m,h})$, given by

$$x_{m,h} = \frac{h^4(1+m^2) - 4h^3m - 2h^2(m^2+3m-3) + 4h(m+3) + m^2 + 6m + 1}{12h^2}$$
$$y_{m,h} = \frac{(mh^2 - 2h - m)(h+1)(hm - m - h - 1)}{4h^3},$$

lies in $E_{m,q}(\mathbb{Q}(m,h))$. Moreover, the point $P_{m,q}$, see Theorem 3.7, is a point in $E_{m,q}(\mathbb{Q}(m,h))$. Taking $m = 1$ and $h = 1/2$, we obtain $P_{1,3/4} = (-73/48, 147/64)$ and $Q_{1,3/4} = (121/24, 21/2)$. Further, using `SAGE`, it is obtained that these points are linearly independent in $E_{1,3/4}$. The result now follows using Silverman's specialization theorem. □

Remark 3.10. The point $Q_{m,q(h)} \in E_{m,q(h)}$ in Theorem 3.9 corresponds to the point

$$\left(0 : 1 : \frac{1+h^2}{2h} : 1\right) \in C_{m,q(h)}.$$

The triangle in $A_{m,q(h)}$ that corresponds to $Q_{m,q(h)}$ is a right Heron triangle with area:

$$A(h) = \left|\frac{1-h^2}{4h}\right|.$$

Thus, the numbers $A(h)$ are congruent numbers.

Theorem 3.11. *Let*

$$q := q(u,m) = \frac{2(u-m)}{1+m^2-u^2}.$$

Then, $\operatorname{rank} E_{m,q}(\mathbb{Q}(m,u)) \geq 2$.

Proof. The point $H_{m,q} = (x_{m,u}, y_{m,u})$, given by

$$x_{m,u} = \frac{5m^4 + (6-10u)m^3 + (4u^2 - 6u + 10)m^2}{3(m^2 - u^2 + 1)^2} + \frac{2(u^3 - 3u^2 - 5u + 3)m - u^4 + 6u^3 - 6u + 5}{3(m^2 - u^2 + 1)^2}$$

$$y_{m,u} = \frac{2(m - u + 1)^2(m^2 - um + 1)}{(m^2 - u^2 + 1)^2},$$

together with the point $P_{m,q}$ are two linearly independent points. This can be proven by specializing $m = 1$, $u = 3$, and hence, $q = -4/7$. □

Remark 3.12. The point $H_{m,q}$ in Theorem 3.11 in $E_{m,q}(\mathbb{Q}(m,u))$ is in correspondence with the point

$$\left(\frac{2(u-m)}{1+m^2-u^2} : \frac{m^2 - 2mu + u^2 + 1}{m^2 - u^2 + 1} : -\frac{(m-1-u)(m+1-u)}{m^2 - u^2 + 1} : 1\right)$$

on $C_{m,q}(\mathbb{Q}(u,m))$. The latter point gives rise to a right rational triangle whose base is $|q|$ and area is

$$\left|\frac{(m-u)(m-u-1)(m-u+1)}{(m^2 - u^2 + 1)^2}\right|,$$

in particular, this area is a congruent number.

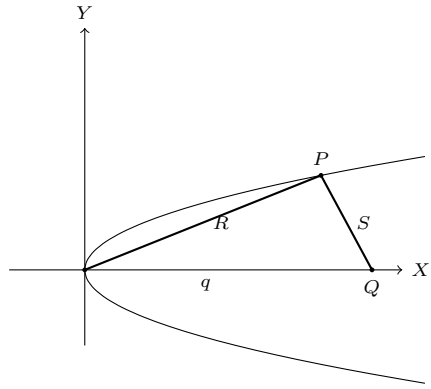

FIGURE 3.

4. Rational triangles via curves of genus 3. The problem we discuss in this section is similar to that in Section 3. Let q be a rational number. Consider the point $Q = (q, 0)$ on the x-axis and the parabola $x = y^2$. We are searching the plane for the rational points $P = (X, Y)$ lying on the parabola at a rational distance, say R, from the origin O and, at a rational distance, say S, from Q. Again this construction yields a rational distance set $\{O, P, Q\}$ of rational points.

The set S_q is the set of rational triangles whose base is OQ and whose third vertex P lies on the parabola $x = y^2$. Note that $\triangle OQP$ is a Heron triangle. Furthermore, a point $P = (X, Y)$ is a vertex of some triangle in S_q if and only if $(x_1 : x_2 : x_3 : x_4 : x_5) = (X : Y : R : S : 1)$ is a rational solution for the following intersection C_q of quadratic surfaces in $\mathbb{P}^4$:

$$\begin{aligned} x_1^2 + x_2^2 &= x_3^2 \\ (x_1 - qx_5)^2 + x_2^2 &= x_4^2 \\ x_2^2 &= x_1 x_5, \end{aligned}$$

where R is the distance between P and O, and S is the distance between P and Q. The point $(0 : 0 : 0 : \pm q : 1)$ lies in $C_q(\mathbb{Q})$. Yet, this point corresponds to a degenerate triangle in S_q.

It is known that the genus of a smooth complete intersection of three quadratic surfaces in $\mathbb{P}^4$ is 5. However, using the Jacobian criterion of smoothness, the intersection curve C_q has two ordinary double points, namely, $(0 : 0 : 0 : \pm q : 1)$. It follows that the curve C_q is of genus 3. Faltings' celebrated theorem implies that the set of rational points $C_q(\mathbb{Q})$ is finite as the genus of C_q is greater than 1. This yields the following result.

Corollary 4.1. *The set S_q is finite.*

It may be asked whether the set S_q can be nonempty.

Theorem 4.2. *If*

$$q = \frac{(u^2 + 1)^2}{8u^2}$$

for some $u \in \mathbb{Q} \setminus \{0, \pm 1\}$, then S_q contains an isosceles Heron triangle.

Similarly, if

$$q = \frac{(u^2-1)^2}{4u^2}$$

for some $u \in \mathbb{Q} \setminus \{0, \pm 1\}$*, then* S_q *contains a right Heron triangle.*

Proof. When $q = (u^2+1)^2/8u^2$, it is easily seen that

$$(x_1 : x_2 : x_3 : x_4 : x_5) = \left(\frac{(u^2-1)^2}{4u^2} : \frac{u^2-1}{2u} : \frac{u^4-1}{4u^2} : \frac{(u^2+1)^2}{8u^2} : 1 \right)$$

is a rational point in $C_q(\mathbb{Q})$. This produces an isosceles rational triangle in S_q as $q = S$.

If $q = (u^2-1)^2/4u^2$, then

$$\left(\frac{(u^2-1)^2}{4u^2} : \frac{u^2-1}{2u} : \frac{u^4-1}{4u^2} : \frac{u^2-1}{2u} : 1 \right)$$

is a rational point in $C_q(\mathbb{Q})$. Therefore, a right Heron triangle in S_q as $q^2 + S^2 = R^2$ has been obtained. □

Remark 4.3. Theorem 4.2 yielded the congruent numbers

$$\frac{(u^2-1)^3}{16u^3},$$

the area qS of the right Heron triangle.

APPENDIX

A. The isomorphism between $E_{m,q}$ and $C_{m,q}$. Recall that the curve $C_{m,q}$ is defined by

$$(1+m^2)x_1^2 + 2mx_1x_4 + x_4^2 = x_2^2,$$
$$(1+m^2)x_1^2 + 2(m-q)x_1x_4 + (1+q^2)x_4^2 = x_3^2.$$

The curve $C_{m,q}$ is isomorphic to the curve $C'_{m,q}$, defined by

$$y^2 = \frac{(1+mq)^2}{4}x^4 + q(1+mq)x^3z + \left(\left(1 - \frac{m^2}{2}\right)q^2 - mq + \frac{1}{2} \right)x^2z^2 - q(1+mq)xz^3 + \frac{(1+mq)^2}{4}z^4,$$

via the following isomorphism

$$\psi : C_{m,q} \longrightarrow C'_{m,q}; (x_1 : x_2 : x_3 : x_4) \longmapsto (x : y : z),$$

defined by

$$\psi(x_1 : x_2 : x_3 : x_4)$$
$$= \begin{cases} (mx_1 + x_4 : x_3(x_1 + x_2) : x_1 + x_2) & \text{if } (x_1 : x_2 : x_3 : x_4) \\ & \quad \neq (-\frac{1}{m} : \frac{1}{m} : q + \frac{1}{m} : 1) \\ (1 : \frac{mq+1}{2} : 0) & \text{if } (x_1 : x_2 : x_3 : x_4) \\ & \quad = (-\frac{1}{m} : \frac{1}{m} : q + \frac{1}{m} : 1), \end{cases}$$

whereas the inverse is given by

$$\psi^{-1}(x : y : z) =$$
$$\begin{cases} (\frac{z^2-x^2}{2z} : \frac{x^2+z^2}{2z} : \frac{y}{z} : \frac{m(x^2-z^2)+2xz}{2z}) & \text{if } (x:y:z) \neq (1 : \pm\frac{mq+1}{2} : 0) \\ (-\frac{1}{m} : \frac{1}{m} : q + \frac{1}{m} : 1) & \text{if } (x:y:z) = (1 : \frac{mq+1}{2} : 0) \\ (-\frac{1}{m} : \frac{1}{m} : -q - \frac{1}{m} : 1) & \text{if } (x:y:z) = (1 : -\frac{mq-1}{2} : 0). \end{cases}$$

Now the curve $C'_{m,q}$ is isomorphic to the elliptic curve $E_{m,q}$, defined by the following Weierstrass equation

$$Y^2 = X^3 - \frac{1}{3}[(m^2+1)^2q^4+4m(m^2+1)q^3+(5m^2+4)q^2+2mq+1]X$$
$$+ \frac{1}{27}[2(m^2+1)^2q^4+8m(m^2+1)q^3+(7m^2+8)q^2-2mq-1]$$
$$\cdot [(m^2+1)q^2+2mq+2].$$

Let

$$G_{m,q} = \left\{ \left(\frac{m^2q^2 + 2mq + q^2 - 1}{3}, \ \pm q \right) \right\} \subset E_{m,q}(\mathbb{Q}),$$

and

$$G'_{m,q} = \left\{ \left(1 : \pm\frac{mq+1}{2} : 0 \right) \right\} \subset C'_{m,q}(\mathbb{Q}).$$

The isomorphism

$$\phi : C'_{m,q} \longrightarrow E_{m,q}$$

is defined as follows: $\phi(G'_{m,q}) = G_{m,q}$; otherwise, $\phi(x : y : 1) = (X, Y)$, where

$$\begin{aligned} X &= y(1+mq) + \frac{1}{2}(m^2q^2 + mq + 1)x^2 + q(mq+1)x \\ &\quad + \frac{1-2mq+2q^2-m^2q^2}{6} \\ Y &= \frac{mq+1}{2}(2qy+2(1+mq)xy + (mq+1)^2x^3 \\ &\quad + 3q(1+mq)x^2 + x(1-m^2q^2+2q^2-2mq) - q(mq+1)), \end{aligned}$$

whereas the inverse is defined by $\phi^{-1}(G_{m,q}) = G'_{m,q}$, else $\phi^{-1}(X, Y) = (x : y : 1)$, where

$$\begin{aligned} x &= -\frac{3Y + (2-3X)q + 2mq^2 + (1+m^2)q^3}{(mq+1)(b(m,q) - 3X)} \\ y &= \frac{54X^3 - 27b(m,q)X^2 - 27Y^2 - 54qY + a(m,q)}{6(mq+1)(b(m,q) - 3X)^2} \end{aligned}$$

and

$$\begin{aligned} a(m,q) = q^6(m^2+1)^3 + 6mq^5(m^2+1)^2 + 3q^4(3m^2-1)(m^2+1) \\ -4mq^3(m^2+3) - 3q^2(3m^2+8) + 6mq - 1, \\ b(m,q) = m^2q^2 + 2mq + q^2 - 1. \end{aligned}$$

REFERENCES

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

2. J.E. Cremona, T.A. Fisher and M. Stoll, *Minimisation and reduction of* 2-, 3- *and* 4-*coverings of elliptic curves*, Alg. Num. Th. **4** (2010), 763–820.

3. A. Dujella and J. Peral, *Elliptic curves coming from Heron triangles*, Rocky Mountain J. Math. **44** (2014), 1145–1160.

4. N.J. Fine, *On rational triangles*, Amer. Math. Month. **83** (1976), 517–521.

5. D. Lorenzini, *Towers of curves and rational distance sets*, preprint.

6. L.J. Mordell, *Diophantine equations*, Academic Press, London, 1969.

7. W. Peeples, *Elliptic curves and rational distance sets*, Proc. Amer. Math. Soc. **5** (1954), 29–33.

8. D. Rusin, *Rational triangles with equal area*, New York J. Math. **4** (1998), 1–15.

9. J.H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. **106**, Springer-Verlag, New York, 1986.

10. J. Solymosi and F. de Zeeuw, *On a question of Erdős and Ulam*, Discr. Comp. Geom. **43** (2010), 393–401.

11. R. van Luijk, *An elliptic $K3$ surface associated to Heron triangles*, J. Num. Th. **123** (2007), 92–119.

American University in Cairo, Mathematics and Actuarial Science Department, AUC Avenue, New Cairo, Egypt
Email address: **mmsadek@aucegypt.edu**

American University in Cairo, Mathematics and Actuarial Science Department, AUC Avenue, New Cairo, Egypt
Email address: **farida.mahmoud@aucegypt.edu**