ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 5, 2006

HERON TRIANGLES VIA ELLIPTIC CURVES

EDRAY HERBER GOINS AND DAVIN MADDOX

ABSTRACT. Given a positive integer n, one may ask if there is a right triangle with rational sides having area n. Such integers are called congruent numbers, and are closely related to elliptic curves of the form $y^2 = x^3 - n^2\,x$. In this paper, we generalize this idea and show that there is a correspondence between positive integers n associated with arbitrary triangles with rational sides having area n and the family of elliptic curves $y^2 = x(x - n\,\tau)(x + n\,\tau^{-1})$ for nonzero rational τ.

1. Introduction. The Indian mathematician Brahmagupta, 598–668 A.D., considered triangles with integral sides and integral area. He showed that if such a triangle has sides of length a, b and c and has area n, then there are positive integers p, q and r such that

$$\begin{aligned} a &= q(p^2 + r^2) \\ b &= p(q^2 + r^2) \\ c &= (p + q)(p\,q - r^2) \end{aligned} \tag{1.1}$$

and

$$n = p\,q\,r(p + q)(p\,q - r^2);$$

as long as $p\,q > r^2$. (A modern proof can be found in [**4**].) 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.):

$$n = \sqrt{s(s-a)(s-b)(s-c)} \quad \text{where} \quad s = \frac{a+b+c}{2}. \tag{1.2}$$

2000 AMS *Mathematics Subject Classification.* Primary 14H52, Secondary 51M04, 11G05.
Key words and phrases. Congruent numbers, Heron triangles, rational triangles, elliptic curves.
The first author was supported by a fellowship from the Irvine Foundation. The second author was supported as a Richter Scholar by the Caltech Summer Undergraduate Research Fellowship (SURF) via an endowment from Charles Slamar.
Received by the editors on Oct. 16, 2003, and in revised form on April 20, 2004.

Triangles with *rational* sides and area are known as Heron triangles. We are motivated by the following question: given a positive rational number n, does there always exist a rational triangle $[a, b, c]$ with area n? This is a generalization of the congruent number problem, where the rational triangle is assumed to be a right triangle. For example, $n = 1$ is not a congruent number, but it is the area of a rational triangle:

$$a = \frac{3}{2}, \quad b = \frac{5}{3}, \quad \text{and} \quad c = \frac{17}{6} \implies n = 1. \tag{1.3}$$

We may restrict our attention to *integers* n because n_1/n_2 is the area of a rational triangle $[a, b, c]$ if and only if $n_1\, n_2$ is the area of a rational triangle $[a\, n_2,\, b\, n_2,\, c\, n_2]$.

In this paper we study Heron triangles by considering the family of elliptic curves

$$E_\tau^{(n)}: \quad y^2 = x\,(x - n\,\tau)\left(x + n\,\tau^{-1}\right) \tag{1.4}$$

as a generalization to the congruent number problem, i.e., when $\tau = 1$. In fact, our main result is

Theorem 1.1. *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 τ the elliptic curve*

$$E_\tau^{(n)}: \quad y^2 = x\,(x - n\,\tau)\left(x + n\,\tau^{-1}\right) \tag{1.5}$$

has a rational point which is not of order 2.

For example, the rational triangle $[a, b, c]$ is related to the curve with $\tau = 4\,n/(a + b)^2 - c^2$. (For more explicit formulas, see (2.11).) This is closely related to the notion of the θ-congruent number problem as first outlined in [**6**]. However, our results are different since we work with Heron triangles, i.e., we always assume the area of the rational triangle is rational.

As a consequence of this main result, we have

Proposition 1.2. *Fix a positive integer n.*

(1) *There are infinitely many rational triangles with area n.*

(2) *n is the area of a rational right triangle if and only if the curve $y^2 = x^3 - n^2\,x$ has a nontrivial rational point, i.e., a point (x, y) with $y \neq 0$.*

(3) *n is the area of a rational isosceles triangle if and only if the curve $v^2 = u^4 + n^2$ has a nontrivial rational point, i.e., a point (u, v) with $u \neq 0$.*

(4) *Say that n is the area of a rational triangle with an angle θ. If such a triangle is not isosceles, there are infinitely many rational triangles with area n possessing this fixed angle.*

Such statements were already shown in [**5**] and [**9**]. We present simplified proofs by exploiting properties of $E_\tau^{(n)}$.

We also present a detailed description of isosceles triangles by studying the torsion points on $E_\tau^{(n)}$, as explained in

Proposition 1.3. *Fix a positive integer n. The following are equivalent*:

(1) *n is the area of an isosceles triangle.*

(2) *$2\,n$ is a congruent number.*

(3) *$v^2 = u^4 + n^2$ has a nontrivial rational point.*

(4) *$E_\tau^{(n)}$ has a rational point of order 4 for some nonzero rational τ.*

(See Propositions 3.1 with Corollary 3.2.) In the congruent number problem, if the associated elliptic curve $E_1^{(n)}$ has a rational point of order different from 2, then the Mordell-Weil group is infinite. However, there are integers n associated to elliptic curves $E_\tau^{(n)}$ for $\tau \neq 1$ having rational points of order different from 2 yet having finite Mordell-Weil group. For example,

$$E_{4/3}^{(3)}(\mathbf{Q}) = \left\{ [m_1]\,(0,\,0) \bigoplus [m_2]\left(9,\,\frac{45}{2}\right) \;\middle|\; m_1,\,m_2 \in \mathbf{Z} \right\} \simeq \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/4\,\mathbf{Z} \tag{1.6}$$

arising from the isosceles triangle $[5/2, 5/2, 4]$ with area $n = 3$. These results do not appear to be in the literature.

Moreover, we list a table of data for Heron triangles $[a, b, c]$ with given area n for $1 \leq n \leq 50$, along with information about the Mordell-Weil Groups of the associated elliptic curves $E_\tau^{(n)}$. We find that the elliptic curves of interest often have rank at least 2, a phenomenon that was also discovered in [**3**]. As an example, consider $n = 30$; this is a congruent number since it is the area of the $[5, 12, 13]$ right triangle. The elliptic curve $E_1^{(30)} : \; y^2 = x^3 - 900\,x$ has rank 1 with generator (150, 1800), but a different orientation of the right triangle gives an elliptic curve $E_{1/5}^{(30)} : \; y^2 = x^3 + 144\,x^2 - 900\,x$ of rank 2 with generators (45, 585) and (240, 6480).

2. Elliptic curves. We begin our exposition by relating the geometry of Heron triangles to the algebra of elliptic curves.

Theorem 2.1. *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 τ the elliptic curve*

$$E_\tau^{(n)} : \quad y^2 = x(x - n\,\tau)(x + n\,\tau^{-1}) \tag{2.1}$$

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

A positive integer n is called congruent if it is the area of a right rational triangle. It is well known that such numbers correspond to the elliptic curve $y^2 = x^3 - n^2\,x$. More properties can be found in [**7**, Chapter 1]. The proof which follows mimics that construction. We are motivated by the formula in Exercise 3(b) on page 9 of that text. The reader may also notice similarities with the formulas in [**6**] for the so-called θ-congruent number problem.

Proof. Say that we have a triangle $\triangle\, A\,B\,C$ with area n. We explain how to construct the elliptic curve above. Let a denote the length of side A; and similarly with b and B; c and C. Denote θ as the measure of angle $\angle C$ between sides A and B so that the area of the triangle is $n = (1/2)\,a\,b\,\sin\theta$.

We give a parametrization of the lengths of the sides. First, we claim that both $\cos\theta$ and $\sin\theta$ are rational. Indeed, by considering the Law

of Cosines and the area, we have the relations

$$\cos\theta = \frac{a^2+b^2-c^2}{2\,a\,b} \quad \text{and} \quad \sin\theta = \frac{2\,n}{a\,b}. \tag{2.2}$$

Denote τ as the rational number

$$\tau = \tan\frac{\theta}{2} = \frac{\sin\theta}{1+\cos\theta} = \frac{4\,n}{(a+b)^2-c^2}; \tag{2.3}$$

in particular, if $\triangle A\,B\,C$ is a right triangle then we may orient the triangle such that $\tau = 1$. Now consider the rational numbers $u = (a - b\cos\theta)/c$ and $v = (b\sin\theta)/c$. The Law of Cosines states that $u^2 + v^2 = 1$, so that

$$u = \frac{t^2-1}{t^2+1} \quad \text{and} \quad v = \frac{2\,t}{t^2+1} \tag{2.4}$$

in terms of

$$t = \frac{u+1}{v} = \frac{(a+c)^2-b^2}{4\,n}.$$

Hence, there is a rational number r such that

$$a = r(t^2 + 2\,t\,\cot\theta - 1), \quad b = 2\,r\,t\,\csc\theta, \quad \text{and} \quad c = r(t^2+1). \tag{2.5}$$

Make the substitutions

$$\begin{aligned} x &= n\,t = n\,\frac{a-2\,b\,\cos\theta+c}{b\,\sin\theta} = \frac{(a+c)^2-b^2}{4}, \\ y &= \frac{n^2}{r} = 2\,n^2\,\frac{a-2\,b\,\cos\theta+c}{b^2\,\sin^2\theta} = a\,\frac{(a+c)^2-b^2}{4}. \end{aligned} \tag{2.6}$$

They are related by the equation $y^2 = x^3 + \alpha\,x^2 + \beta\,x$, where

$$\alpha = \frac{2\,n}{\tan\theta} = \frac{a^2+b^2-c^2}{2} = n(\tau^{-1}-\tau) \quad \text{and} \quad \beta = -n^2. \tag{2.7}$$

Denote by $E_\tau^{(n)}$ the (projective) curve defined by this cubic equation. We claim it is an elliptic curve, where the rational point $P = (x, y)$ does not have order 2. The discriminant of the curve is

$$\Delta[E_\tau^{(n)}] = 16\,(\alpha^2 - 4\,\beta)\,\beta^2 = 16\,a^2\,b^2\,n^4 = 16\,n^6\,(\tau+\tau^{-1})^2 \tag{2.8}$$

and is nonzero; hence, the cubic does indeed define a nonsingular curve. The point P has order 2 if and only if $y = 0$; but this cannot happen since $y = n^2/r \neq 0$.

Conversely, we explain how to construct a rational triangle with area n from points on the elliptic curve. Let (x, y) be a rational (affine) point on $E_\tau^{(n)}$ which is not of order 2. Of the four points

(2.9)
$$[\pm 1](x,\, y) = (x,\, \pm y) \quad \text{and} \quad (0,\, 0) \oplus [\pm 1](x,\, y) = \left(-\frac{n^2}{x},\, \pm \frac{n^2\, y}{x^2} \right)$$

we can choose one with positive x- and y-coordinates. Without loss of generality, say $(x,\, y)$ is such a rational point with $x > 0$ and $y > 0$. A rational triangle with sides of length

$$a = \frac{y}{x}, \quad b = \frac{\sqrt{\Delta[E_\tau^{(n)}]}}{4\, n^2}\, \frac{x}{y}, \quad \text{and} \quad c = \frac{x^2 + n^2}{y} \tag{2.10}$$

has area n, as can be verified by Heron's formula (1.2). □

We list for reference the transformation from the rational triangle to the elliptic curve:

(2.11)

Triangle to Curve	Curve to Triangle
$n = \sqrt{s(s-a)(s-b)(s-c)}$	$E_\tau^{(n)} : y^2 = x(x - n\,\tau)(x + n\,\tau^{-1})$
$\tau = \dfrac{4\, n}{(a+b)^2 - c^2}$	$a = \dfrac{y}{x}$
$x = \dfrac{(a+c)^2 - b^2}{4}$	$b = n(\tau + \tau^{-1})\dfrac{x}{y}$
$y = a\, \dfrac{(a+c)^2 - b^2}{4}$	$c = \dfrac{(x^2 + n^2)}{y}$

where $s = (a + b + c)/2$ in Heron's formula and $x > 0$, $y > 0$ for the elliptic curve. As an example, when $n = 1$, the rational triangle $[3/2, 5/3, (17)/6]$ mentioned in the introduction corresponds to the rational point $(4,\, 6)$ on the elliptic curve $E_2^{(1)}$. In fact,

$$\begin{aligned} E_2^{(1)}(\mathbf{Q}) &= \left\{ [m_1](0,\, 0) \oplus [m_2](2,\, 0) \oplus [m_3](4,\, 6) \,\middle|\, m_i \in \mathbf{Z} \right\} \\ &\simeq \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}. \end{aligned} \tag{2.12}$$

3. Torsion subgroups. As explained in the previous section, if the elliptic curve $E_1^{(n)}: y^2 = x^3 - n^2 x$ has a rational point which is not 2-torsion, then n is congruent. The more general elliptic curve $E_\tau^{(n)}$ constructed above has all of its 2-torsion rational. Explicitly, when $\tau = 4n/((a+b)^2 - c^2)$, then

$$E_\tau^{(n)}[2] = \left\{(0,0),\ \left(\frac{c^2-(a+b)^2}{4}, 0\right),\ \left(\frac{c^2-(a-b)^2}{4}, 0\right),\ \mathcal{O}\right\}. \tag{3.1}$$

Proposition 2.1 explains why we wish to avoid such points of order 2. In the congruent number problem, it is well known that the only torsion points on the elliptic curve $E_1^{(n)}$ are the points of order 2, but in general there may be points of other orders on $E_\tau^{(n)}$. Our goal in this section is to completely characterize the torsion points. We will show that the torsion subgroup of $E_\tau^{(n)}$ is either

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \quad \text{or} \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, \tag{3.2}$$

with the latter case corresponding to isosceles triangles.

Proposition 3.1. *Fix a positive integer n. Denote the (hyper)elliptic curves*

$$C^{(n)}: v^2 = (u^4 + n^2)(9u^4 + n^2) \quad \text{and} \quad D^{(n)}: v^2 = u^4 + n^2. \tag{3.3}$$

(1) *$E_\tau^{(n)}$ has a rational point of order 3 for some τ if and only if there exists a nontrivial rational point on $C^{(n)}$, i.e., a point (u, v) with $u \neq 0$.*

(2) *$E_\tau^{(n)}$ has a rational point of order 4 for some τ if and only if there exists a nontrivial rational point on $D^{(n)}$, i.e., a point (u, v) with $u \neq 0$.*

We will see below that $C^{(n)}$ has no nontrivial rational points. However, $D^{(n)}$ does have nontrivial rational points for certain n. For example, when $n = 3$ then $(u, v) = (2, 5)$ is such a point.

Proof. Say that (x, y) is a point of order 3 on $E_\tau^{(n)}$. Then x is a root of the 3-division polynomial

$$\psi_3(x) = 3x^4 - 4n(\tau - \tau^{-1})x^3 - 6n^2x^2 - n^4. \tag{3.4}$$

(See [**10**, p. 105] for the definition of a division polynomial.) Since $x \neq 0$ is rational, we express τ in terms of x:

$$\tau = \frac{3\,x^4 - 6\,n^2\,x^2 - n^4 \pm (x^2+n^2)\sqrt{(x^2+n^2)(9\,x^2+n^2)}}{8\,n\,x^3}. \tag{3.5}$$

Then $(x^2+n^2)(9\,x^2+n^2) = v^2$ for some rational number v. Moreover, since y is rational we have

$$y^2 = x(x - n\,\tau)(x + n\,\tau^{-1}) = \frac{(x^2+n^2)^2}{4\,x}; \tag{3.6}$$

so that $x = u^2$ for some rational number $u \neq 0$. Hence (u, v) is a nontrivial point on $C^{(n)}$. The converse is clear.

Now say that (x, y) is a point of order 4 on $E_\tau^{(n)}$. Then x is a root of the 4-division polynomial

$$\psi_4(x) = 2(x^2+n^2)(x^2 - 2\,n\,\tau\,x - n^2)(x^2 + 2\,n\,\tau^{-1}\,x - n^2). \tag{3.7}$$

Since x is rational, we only have four possibilities for x:

$$x = n\,\tau \pm n\sqrt{1+\tau^2} \quad \text{or} \quad x = -\,n\,\tau^{-1} \pm n\,\tau^{-1}\sqrt{1+\tau^2}. \tag{3.8}$$

In either case, this implies $n^2 + (n\,\tau)^2 = v^2$ for some rational number v. Again, considering the y-coordinate we have

$$y^2 = n\,\tau^{-1}\left(\frac{x^2+n^2}{2\,n}\right)^2 \quad \text{or} \quad -\,n\,\tau\left(\frac{x^2+n^2}{2\,n}\right)^2. \tag{3.9}$$

In either case this implies $(n\,\tau)^2 = u^4$ for some rational number u. Hence (u, v) is a nontrivial point on $D^{(n)}$. Again, the converse is clear. □

Corollary 3.2. *Fix a positive integer n. The following are equivalent*:

(1) *$D^{(n)}$ has a nontrivial rational point.*

(2) *n is the area of an isosceles triangle.*

(3) *$2\,n$ is a congruent number.*

Proof. $1 \Leftrightarrow 2$. Say that (u, v) is a point on $D^{(n)}$ with $u \neq 0$. Without loss of generality, assume u and v are positive. Inverting the formulas in (3.8) and (3.9) we set

(3.10)
$$\tau = \frac{u^2}{n}, \quad x = u^2 + v, \quad \text{and} \quad y = \frac{u^2 v + v^2}{u} \implies (x, y) \in E_\tau^{(n)}[4].$$

Then the positive numbers

(3.11)
$$a = \frac{y}{x} = \frac{v}{u}, \quad b = n(\tau + \tau^{-1})\,\frac{x}{y} = \frac{v}{u}, \quad \text{and} \quad c = \frac{x^2 + n^2}{y} = 2\,u$$

define a rational isosceles triangle with area n. The converse is clear.

$2 \Leftrightarrow 3$. Say that $[a, a, c]$ is an isosceles triangle with area n. Scale the triangle by a factor of 2 to find an isosceles triangle $[2\,a,\ 2\,a,\ 2\,c]$ with area $4\,n$. Choosing the side with length $2\,c$ as the base, the height of the triangle is $4\,n/c$, a rational number. We fold the isosceles triangle in half and find a right triangle with base c, height $4\,n/c$, hypotenuse $2\,a$, and area $2\,n$. Hence, $2\,n$ is a congruent number. Again, the converse is clear. □

We list for reference the transformation from the rational isosceles triangle to the curve $D^{(n)}$:

(3.12)

Isosceles Triangle to Curve	Curve to Isosceles Triangle
$n = \sqrt{s(s-a)(s-b)(s-c)}$	$D^{(n)} : v^2 = u^4 + n^2$
$u = \dfrac{c}{2}$	$a = b = \dfrac{v}{u}$
$v = \dfrac{a\,c}{2} = \dfrac{b\,c}{2}$	$c = 2\,u$

where $s = (2\,a + c)/2 = (2\,b + c)/2$ in Heron's formula and $u > 0$, $v > 0$ for the curve. As an example, when $n = 3$, the rational triangle $[5/2, 5/2, 4]$ corresponds to the rational point $(2, 5)$ on the curve $D^{(3)}$. As predicted by the corollary, $2\,n = 6$ is a congruent number because it is the area of the right triangle $[3, 4, 5]$.

Proposition 3.3. *Fix a positive integer n.*

(1) *$E_\tau^{(n)}$ does not have a point of order 6 or 8 for any nonzero rational τ.*

(2) *The torsion subgroup of $E_\tau^{(n)}$ is either $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.*

(3) *If any of the statements in Corollary 3.2 fail, then the torsion subgroup of $E_\tau^{(n)}$ is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.*

The proof of the first part of the proposition is similar to that of [**9**, Theorem 3; note the remarks on page 10 of that article]. The proof of the complete proposition uses the full power of a result of Mazur [**8**] classifying the torsion subgroups of rational elliptic curves, although a more creative proof using class field theory has been pointed out to the authors by Archimescu and Ramakrishnan; it will appear in the doctoral thesis [**1**] of the former.

Proof. Assume that $E_\tau^{(n)}$ has a rational point of order 6. Then it also has a point of order 3, so $C^{(n)}$ has a nontrivial rational point, say (u, v), by Proposition 3.1. Denote $(U, V) = (u^2/n, v/n)$ as a nontrivial rational point on the elliptic curve

$$V^2 = (U^2 + 1)(9\,U^2 + 1). \tag{3.13}$$

However, using a symbolic computer package, we see that the only (affine) rational points on this curve are $(U, V) = (0, \pm 1)$. (For example, one may do this using MAGMA: the commands `Points()` with `PointsKnown()` find four projective points, where two are at "infinity.") This is a contradiction, so $E_\tau^{(n)}$ does not have any rational points of order 6.

Similarly, say (x, y) is a rational point on $E_\tau^{(n)}$ of order 8. Consider the point

$$(X, Y) = [2](x, y) = \left(\left(\frac{x^2 + n^2}{2\,y} \right)^2, \frac{\psi_4(x)}{16\,y^3} \right) \tag{3.14}$$

in terms of the 4-division polynomial introduced in (3.7). This is a point of order 4, so say $X^2 - 2\,n\,\tau\,X - n^2 = 0$. (The other roots come from the reflection $\tau \mapsto -\tau^{-1}$.) As stated in the proof of

Corollary 3.2, $n\,\tau = u^2$ and $X = u^2 + v$ for some rational u and v on the curve $v^2 = u^4 + n^2$. Choose a rational number z such that $x = (1+z)\,v + u^2$; then the relation $X = ((x^2+n^2)/(2\,y))^2$ implies that $4(1+z)^2(u^2+v)^2 = u^2\,v\,z^4$, so that $v = w^2$ for some rational number w. Then $(U, V) = (w/u, n/u^2)$ is a nontrivial rational point on the elliptic curve

$$V^2 = U^4 - 1. \tag{3.15}$$

Again, using a symbolic computer package we see that the only (affine) rational points on this curve are $(U, V) = (\pm 1, 0)$. (Again, the MAGMA command `Points()` finds four projective points where two are at "infinity.") This is a contradiction, so $E_\tau^{(n)}$ does not have any rational points of order 8.

We now focus on the last two statements. The torsion subgroup of $E_\tau^{(n)}$ contains $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z}$ because the three points $(0, 0)$, $(n\,\tau, 0)$ and $(-n\,\tau^{-1}, 0)$ have order 2. Hence by the main result of [**8**] the torsion subgroup is $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,m\,\mathbf{Z}$ for m either 1, 2, 3 or 4. But m cannot be 3 or 4 by the discussion above. Further, m cannot be even when $D^{(n)}$ has no nontrivial rational points or else $E_\tau^{(n)}$ would have a point of order 4 by Proposition 3.2. □

There are elliptic curves $E_\tau^{(n)}$ with a finite group of rational points where not all such points are 2-torsion. This is not the case with $E_1^{(n)}$ because if a rational point is not 2-torsion then it must be of infinite order. Indeed, when $n = 3$ the isosceles triangle $[5/2, 5/2, 4]$ maps to a point $(9, 45/2)$ of order 4 on $E_\tau^{(3)}(\mathbf{Q})$ for $\tau = 4/3$. However,

$$E_{4/3}^{(3)}(\mathbf{Q}) = \left\{ [m_1](0,\,0) \oplus [m_2]\left(9,\,\frac{45}{2}\right) \,\middle|\, m_1,\,m_2 \in \mathbf{Z} \right\} \simeq \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/4\,\mathbf{Z}, \tag{3.16}$$

i.e., there are no points of infinite order! Of course, we may rotate the triangle to find a new elliptic curve, namely we may choose $[4, 5/2, 5/2]$, which maps to the point $(9, 36) \in E_\tau^{(3)}(\mathbf{Q})$ for $\tau = 1/3$. This curve does indeed have positive rank:

$$\begin{aligned} E_{1/3}^{(3)}(\mathbf{Q}) &= \left\{ [m_1]\,(0,\,0) \oplus [m_2](1,\,0) \oplus [m_3](9,\,36) \,\middle|\, m_i \in \mathbf{Z} \right\} \\ &\simeq \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}. \end{aligned} \tag{3.17}$$

4. More results. With the ideas introduced and results proved in the previous section, we present new proofs of well-known results about Heron triangles.

Proposition 4.1. *Fix a positive integer n.*

(1) *There are infinitely many rational triangles with area n.*

(2) *n is the area of a rational right triangle if and only if the curve $y^2 = x^3 - n^2\,x$ has a nontrivial rational point, i.e., a point (x, y) with $y \neq 0$.*

(3) *n is the area of a rational isosceles triangle if and only if the curve $v^2 = u^4 + n^2$ has a nontrivial rational point, i.e., a point (u, v) with $u \neq 0$.*

(4) *Say that n is the area of a rational triangle with an angle θ. If such a triangle is not isosceles, there are infinitely many rational triangles with area n possessing this fixed angle.*

The first part of this proposition was answered in [**5**, Theorem 2] and [**9**, Theorem 1]. We present a simplified proof using the formula due to Chowla in [**5**, equations 25 and 26]. The last part of the proposition is the fundamental result of [**6**] for the so-called θ-congruent numbers and was also discussed at the end of [**9**, see page 15 of that article].

Proof. First, we show that there exists at least one triangle having area n. Following Proposition 2.1, it suffices to find some $E_\tau^{(n)}$ with a rational point not of order 2. We choose

$$(4.1) \qquad (x,\, y) = \left(\frac{2\,n+1}{4},\, \frac{4\,n^2-1}{8}\right) \in E_\tau^{(n)}(\mathbf{Q}) \quad \text{for} \quad \tau = \frac{2}{2\,n+1}.$$

By the formulas in (2.11), we have the rational triangle with sides

$$(4.2) \qquad a = \frac{2\,n-1}{2}, \quad b = \frac{n(4\,n^2+4\,n+5)}{4\,n^2-1}, \quad \text{and} \quad c = \frac{20\,n^2+4\,n+1}{2(4\,n^2-1)}$$

which indeed has area n. The point (x, y) does not have order 2 because $y \neq 0$ when n is a positive integer.

It is easy to verify that $a \neq b$ so by Proposition 3.1, along with Corollary 3.2, the point (x, y) does not have order 4. Proposition 3.3 implies this point is not torsion, and hence must be a point of infinite order. Proposition 2.1 constructs a rational triangle out of $[m]\,P$ having area n for each nonzero integer m so we have infinitely many triangles.

The second statement was shown in Proposition 2.1 (and is well known) while the third statement is just Corollary 3.2.

To show the last statement, say that we have a triangle $\triangle\, A\, B\, C$ with area n, where θ is the measure of angle $\angle C$ between sides A and B. Then, by the proof of Proposition 2.1, we have a rational point on the elliptic curve $E_\tau^{(n)}$ where $\tau = \tan(\theta/2)$. Since $\triangle\, A\, B\, C$ is not isosceles, it corresponds to a point of infinite order on $E_\tau^{(n)}$ by the preceding discussion. But each point corresponds to a rational triangle of area n having fixed angle θ, so we have infinitely many such triangles. □

5. Examples and data. In this section we present examples of triangles and elliptic curves. We list rational triangles $[a, b, c]$ having small denominators associated to positive integers n not greater than 50. All of these entries may be verified by Heron's formula:

$$n = \sqrt{s(s-a)(s-b)(s-c)} \quad \text{in terms of} \quad s = \frac{a+b+c}{2}. \tag{5.1}$$

The Tables also contain information about the elliptic curves

$$E_\tau^{(n)} :\ y^2 = x(x - n\,\tau)(x + n\,\tau^{-1}) \quad \text{in terms of} \quad \tau = \frac{4\,n}{(a+b)^2 - c^2} \tag{5.2}$$

where we list the highest rank of the various orientations of the triangles; in many cases there was more than one such choice of orientation. We list only the generators of the free part of the Mordell-Weil group, where at least one of the generators maps to the triangle listed. The finite part of the Mordell-Weil group is chosen to be $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z}$.

In many cases, the rank is greater than 1. This phenomenon was also discovered in [**3**], where the authors considered Heron triangles with rational medians. It may be possible that the examples of rational triangles below have such properties, although we have not examined this in detail.

TABLE

n	Triangle	τ	Rank	Generators
1	$[3/2, 5/3, (17)/6]$	2	1	(4, 6)
2	$[5/6, (29)/6, 5]$	1/(12)	2	(8/3, (40)/3), ((392)/3, 1624)
3	$[5/2, 5/2, 4]$	1/3	1	(9, 36)
4	$[3, (10)/3, (17)/3]$	2	1	(16, 48)
5	$[3/2, (20)/3, (41)/6]$	1	1	(45, 300)
6	$[3, 4, 5]$	1	1	(18, 72)
7	$[3/2, (65)/6, (35)/3]$	1/2	1	(4, 6)
8	$[5/3, (29)/3, 10]$	1/(12)	2	((32)/3, (320)/3, ((1568)/3, 12992)
9	$[9/2, 5, (17)/2]$	2	1	(36, 162)
10	$[3, (41)/6, (41)/6]$	4/5	2	((25)/2, (75)/2), (72, 624)
11	$[(11)/6, 15, (97)/6]$	4/9	3	((11)/2, (121)/12), ((33)/4, (121)/4),(66, 605)
12	$[5, 5, 6]$	1/3	1	(36, 288)
13	$[(25)/6, (13)/2, (20)/3]$	1/3	2	((52)/3, (338)/3), ((1573)/3, (37180)/3)
14	$[8/3, (21)/2, (65)/6]$	7/9	2	(14, (112)/3), (42, 280)
15	$[4, (15)/2, (17)/2]$	1	1	(60, 450)
16	$[6, (20)/3, (34)/3]$	2	1	(64, 384)
17	$[(17)/6, (145)/12, (145)/12]$	8/9	1	(144, 1740)
18	$[5/2, (29)/2, 15]$	1/(12)	2	(24, 360), (1176, 43848)
19	$[(19)/6, (51)/2, (85)/3]$	4	2	(722, 18411), (6498, 520923)
20	$[3, (40)/3, (41)/3]$	1	1	(180, 2400)
21	$[5, (17)/2, (21)/2]$	1/2	2	(84, 882), ((63)/2, (441)/2)
22	$[(15)/2, (50)/3, (143)/6]$	1/8	1	(4, 30)
23	$[(221)/30, (89)/5, (149)/6]$	138/25	3	(180, 1326), (960, 27768), (690, 16422)
24	$[6, 8, 10]$	1	1	(72, 576)
25	$[(15)/2, (25)/3, (85)/6]$	2	1	(100, 750)
26	$[5, (41)/3, (52)/3]$	13/6	2	(78, 390), (726, 18942)

TABLE CONT'D.

n	Triangle	τ	Rank	Generators
27	$[(15)/2, (15)/2, 12]$	$1/3$	1	(81, 972)
28	$[3, (65)/3, (70)/3]$	$1/2$	1	(16, 48)
29	$[8/3, (145)/4, (461)/12]$	$1/(48)$	2	((29)/3, (4205)/12), ((999698)/75, (1212920009)/750)
30	$[5, 12, 13]$	$1/5$	2	(45, 585), (240, 6480)
31	$[(31)/6, (97)/6, 20]$	$9/4$	2	(93, (961)/2), (2883, (306559)/2)
32	$[(10)/3, (58)/3, 20]$	$1/12$	2	((128)/3, (2560)/3), ((6272)/3, 103936)
33	$[(11)/2, (25)/2, 15]$	$4/3$	1	(66, 363)
34	$[(17)/6, 24, (145)/6]$	1	2	(578, 13872), ((289)/4, (4335)/8)
35	$[(37)/6, 12, (91)/6]$	$9/(20)$	2	(25, (925)/6), (175, (15925)/6)
36	$[9, 10, 17]$	2	1	(144, 1296)
37	$[(20)/3, (37)/2, (145)/6]$	$1/12$	2	((37)/3, (1369)/6), ((9472)/75, (372368)/125)
38	$[10/3, (305)/6, (323)/6]$	$2/9$	2	(9, 30), ((2809)/81, (315350)/729)
39	$[13/2, 20, (51)/2]$	3	2	(156, 1014), (624, 14196)
40	$[6, (41)/3, (41)/3]$	$4/5$	2	(50, 300), (288, 4992)
41	$[(41)/12, (337)/12, 30]$	$2/41$	3	(82, 2460), (772, 28500), (164, 5166)
42	$[7, 15, 20]$	2	1	(126, 882)
43	$[(29)/2, (65)/3, (215)/6]$	$1/12$	2	(774, 27735), ((356083)/300, (18340231)/375)
44	$[(11)/3, 30, (97)/3]$	$4/9$	3	(22, (242)/3), (33, 242), (264, 4840)
45	$[9/2, 20, (41)/2]$	1	1	(405, 8100)
46	$[(13)/2, (85)/6, (46)/3]$	$23/24$	2	(69, (897)/2), ((196)/3, (1190)/3)
47	$[(17)/2, (235)/21, (545)/42]$	$47/84$	2	((329)/6, (5593)/12), ((278663)/3042, (243200419)/237276)
48	$[10, 10, 12]$	$1/3$	1	(144, 2304)
49	$[21/2, 35/3, (119)/6]$	2	1	(196, 2058)
50	$[25/6, 25/6, 25]$	$1/12$	2	((200)/3, (5000)/3), ((9800)/3, 203000)

The Heron triangles were computed on a dual processor PowerMac G4 using algorithms written in C and Mathematica®. The ranks of the elliptic curves were computed using MAGMA [**2**] on William Stein's "Mathematics Extreme Computation Cluster At Harvard" (MECCAH).

Acknowledgments. The authors would like to thank Garikai Campbell for helpful conversations, William Stein for use of his machine to do the computations, Lloyd Kilford for a careful reading of the first drafts of this manuscript, the referee for many useful suggestions and the Caltech Summer Undergraduate Research Fellowship (SURF) Program for the opportunity to conduct the research. The formulas and data found in this exposition were verified using either Mathematica® or MAGMA [**2**].

REFERENCES

1. Sever Achimescu, *Hilbert modular forms of weight* 1/2, Ph.D. Thesis, California Institute of Technology, 2004.

2. Wieb Bosma, John Cannon and Catherine Playoust, *The Magma algebra system* I, *The user language*, J. Symbolic Comput. **24** (1997), 235–265.

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

4. Robert D. Carmichael, *The theory of numbers and Diophantine analysis*, Dover Publ. Inc., New York, 1959.

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

6. Masahiko Fujiwara, *θ-congruent numbers*, in *Number theory* (Eger, 1996), de Gruyter, Berlin, 1998, pp. 235–241.

7. Neal Koblitz, *Introduction to elliptic curves and modular forms*, 2nd ed., Springer-Verlag, New York, 1993.

8. B. Mazur, *Rational isogenies of prime degree*, (with Appendix by D. Goldfeld), Invent. Math. **44** (1978), 129–162.

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

10. Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

Purdue University, Department of Mathematics, Mathematical Sciences Bldg., 150 N. University St., West Lafayette, IN 47907-2067
E-mail address: egoins@math.purdue.edu

California Institute of Technology, Mail Code 648, Pasadena, CA 91126
E-mail address: davin@caltech.edu