New York Journal of Mathematics

New York J. Math. **4** (1998) 1–15.

Rational Triangles with Equal Area

David J. Rusin

Abstract. We consider the set of triangles in the plane with rational sides and a given area A. We show there are infinitely many such triangles for each possible area A. We also show that infinitely many such triangles may be constructed from a given one, all sharing a side of the original triangle, unless the original is equilateral. There are three families of triangles (including the isosceles ones) for which this theorem holds only in a restricted sense; we investigate these families in detail. Our explicit construction of triangles with a given area may be viewed as a dynamical system in the plane; we consider its features as such. The proofs combine simple calculation with Mazur's characterization of torsion in rational elliptic curves. We discuss the isomorphism classes of the elliptic curves involved.

In this paper a *rational triangle* means a triangle in the plane whose sides are of rational length. We consider the set of such triangles with a given area A (necessarily the square root of a positive rational number). We show there are infinitely many rational triangles for each such area A (Theorem 1). This was previously known for rational A; the known proofs are, like ours, algebraic. So we ask whether there is a simple geometric manipulation of a rational triangle which yields infinitely many others with the same area. The answer is affirmative: these triangles may be selected to have a side in common with the original triangle, unless that triangle is equilateral (Theorems 2 and 4). The proof of this stronger statement combines simple calculation with Mazur's characterization of torsion in rational elliptic curves. We describe the construction of new rational triangles from old as a dynamical system. Three families of triangles (including the isosceles ones) play a special role; they are treated in depth (Theorem 3). Finally we discuss the isomorphism classes of the elliptic curves involved (Theorem 5).

Fermat (cf. [3]) showed that it is possible for infinitely many rational triangles to have the same area; all the triangles in his example are right triangles. When the triangles are all assumed to be right triangles, this subject is the "congruent number problem" (see, e.g., [5]): there are indeed infinitely many triangles with a given area if there are any at all; they may all be constructed in a simple way from just a few; and (assuming some unproven conjectures in algebraic geometry) there is a characterization by Tunnell [9] of which numbers do indeed arise as areas of rational right triangles. We seek results parallel to these in the general case.

Received November 21, 1996.

Mathematics Subject Classification. 11G05.

Key words and phrases. rational triangles, Heron surfaces, elliptic curves.

ISSN 1076-9803/98

In that special case of right triangles, rational triangles naturally have rational area. In the more general setting this is not always true, but by Heron's formula, if p, q, and r are the lengths of the sides of a triangle, the rational number[1]

$$C = -(p+q+r)(p+q-r)(p-q+r)(-p+q+r) \tag{1}$$

is $-(4A)^2$ where A is the area of the triangle. We investigate solutions (p, q, r) to equation (1) with a fixed rational negative C. The set of solutions forms a nonsingular algebraic surface. We refer to the surfaces defined by (1) as *Heron surfaces*.

Fine [4] showed that when $A = \sqrt{-C/16}$ is rational, then there are infinitely many points on the Heron surface. This equation has also been considered in other contexts. The special case $A = 1$ is discussed in [7] and [8], from which it follows that if (x_1, x_2, x_3) is a point satisfying

$$x_1^4 + x_2^4 + x_3^4 = (-C)$$

(cf. [2]) then $(\,(x_1^4+x_2^4)/(2x_1x_2x_3), (x_2^4+x_3^4)/(2x_1x_2x_3), (x_3^4+x_1^4)/(2x_1x_2x_3)\,)$ is a point on the Heron surface. (Elkies' surfaces are proper coverings of Heron surfaces, however — that is, one expects fewer rational points on them than on Heron surfaces.) Each of these methods finds points on the Heron surface which happen to lie on subvarieties selected more or less *ad hoc*, although one of Buddenhagen's methods sketched in [8] centers on the angles of the triangles and thus has the geometric flavor we seek. Our intent is to study some curves embedded in the Heron surface which correspond to geometrically interesting families of triangles.

Each rational triangle with the appropriate area yields a point on the Heron surface, but the converse is not true in general: p, q, and r must be positive, and the triangle inequalities must be met. However, one can easily see that these conditions do not affect the analysis. Indeed, under the affine change of coordinates $x = p + q$, $y = p - q$, we may write (1) in the form

$$C = (x^2 - r^2)(y^2 - r^2). \tag{2}$$

Expressed in these new variables, the geometric restrictions on p, q, and r become simply $|y| < r < x$. But if *any* solution (x, y, r) to (2) is given, we may change signs to obtain a solution with x, y, and r all non-negative. Since $C < 0$, it follows that r must be strictly between x and y in magnitude. Exchanging x and y as necessary gives a solution (x, y, r) which then corresponds to a triangle.

This argument uses some of the symmetry of the Heron surface. The full symmetry group includes the group $(\mathbb{Z}_2) \wr (S_3)$ of all sign changes and permutations of the variables. We will need several of these automorphisms in the sequel.

Now we look for rational points on the Heron surfaces for each (negative) rational number C.

Theorem 1. *For any rational C there exist rational points on the Heron surface* (1)*. Moreover, one may find an* (*infinite*) *parameterized family of such solutions.*

Proof. Since the theorem itself is proved simply by verifying an algebraic identity, it is necessary only to provide a sketch of its derivation.

[1] The equations in this paper were verified with Maple; source code for this verification is available as: http://nyjm.albany.edu:8000/j/1998/rusin/maple.input

We use a simple modification of Fine's idea in [4]: to abut two right triangles along legs of known equal length, and then scale as appropriate if their combined area differs from the desired value by a perfect square. Modifying the choice of variables a bit, we let the common leg have length $4(-C)u$ and let the hypotenuses have lengths $(s - C/s)u$ and $(t - C/t)u$. With these substitutions we find we are looking for points on another surface. (Interestingly, this surface is actually a 2-fold cover of the Heron surface, making it perhaps more surprising that it contain rational points.)

Thus we look for rational s and t making a certain rational function a square. Taking our cue from [4] we look for such points along the parabola $s^2 = Ct$, that is, we set $s = Cx$, $t = Cx^2$, and $u = x/(2y)$, and seek points on the curve $y^2 = (x+1)(Cx^3+1)$. This curve becomes an elliptic curve once we select a point to be the neutral element; $(0,1)$ serves since for no value of s is $x = 0$. Now, this elliptic curve clearly has another point $(-1,0)$, but we cannot solve for u when $y = 0$. However, we can compute the inverse of this element in the elliptic curve, which turns out to be $(x,y) = (3/(1-4C), 2(1+8C)(1-C)/(1-4C)^2)$; this point provides a rational s, t, u as sought above. (Fine, in essence, used instead the double of $(-1,0)$, leading to formulae more complex than those which follow.) Substituting back gives p, q, and r as rational functions of C.

This proves that for all C there is at least one point on the Heron surface (except perhaps for those C those making the denominators of $p(C)$, $q(C)$, or $r(C)$ vanish). As we mentioned in the previous paragraph, one can actually demonstrate that the elliptic curve we used has positive rank[2] for most C, so that the surface contains infinitely many points. However, it is easier to note that for any v, the point $(\,v\,p(C/v^4),\ v\,q(C/v^4),\ v\,r(C/v^4)\,)$ is also on the surface, allowing us a rational parameterization of infinitely many points. With a slight change of variables, this parameterization may be given as

$$p = \frac{v(C-v^4)}{(C+2v^4)},\ q = \frac{(C+2v^4)(C-16v^4)}{12v^3(C-4v^4)},\ r = \frac{(C^3+96Cv^8-16v^{12})}{12v^3(C-4v^4)(C+2v^4)}. \tag{3}$$

Thus for any $C < 0$ we see that each $v \neq 0, (-C/2)^{1/4}$ provides a point (p,q,r) which is easily verified to satisfy equation (1). $\square$

Thus we have found infinitely many points on the Heron surface by noting that it contains an elliptic curve of positive rank, as well as a curve of genus zero. These subvarieties may be computed to be the intersections of the Heron surface with the surfaces defined by

$$(p+q-r)(-p+q+r)^2 + (p-q+r)$$

and

$$13p^3 + 3p^3 - 5r^3 + 7pq^2 + 9p^2q + 5q^2r - 3qr^2 + 3r^2p + 21rp^2 + 6pqr$$

respectively — surfaces with no apparent geometric interpretation. The congruent number problem, on the other hand, studies the intersection of the Heron surface with the surface $p^2 + q^2 = r^2$ describing right triangles. We likewise describe geometrically interesting curves on the Heron surface: we show that given any point

[2] Claims made in the paper about rank and torsion of specific elliptic curves were verified with the Maple package `APECS`.

on the surface there are in general infinitely many others sharing a coordinate with it; that is, given a rational triangle there are typically infinitely many others having the same area and sharing a common side with the original triangle. We discuss a strict interpretation of this goal in Theorem 2; a more liberal reading of it leads to Theorem 4.

Theorem 2. *If p, q, and r are the lengths of the sides of a rational triangle T, then there are infinitely many rational triangles having the same area as T and having a side of length r, unless $p = q$, $r(p^2+q^2) = |p-q|(p+q)^2$, or $r^2(p^2+q^2) = (p^2-q^2)^2$.*

Proof. We are seeking rational solutions to (2), where now both $C < 0$ and $r > 0$ are treated as constants, and where one solution (x, y) is assumed. Among the original automorphisms of the Heron surface, eight preserve r and so give automorphisms of the curve E_1 determined by equation (2). In particular, if (x, y) is a point on the curve, so are its conjugates under this subgroup of symmetries, namely the four points $(\pm x, \pm y)$ and four more $(\pm y, \pm x)$. It is possible that this list includes fewer than eight distinct points, although equation (2) prohibits $x = \pm y$ since $C < 0$. For points (x, y) arising from a triangle, we have $x = p + q \neq 0$ and $y = p - q$ is also assumed nonzero. Thus for such points, all eight conjugates are indeed distinct.

The curve E_1 is an elliptic curve. In order to enumerate the points on it, we find it convenient to reduce equation (2) to Weierstrass form. A routine transformation of the biquadratic equation (2) to a cubic may be followed by the transformation to Weierstrass form which carries to infinity one of the two points at infinity present in the initial equation (2). (More explicit transformations are given below.) The resulting normal form is

$$Y^2 = (X^2 + 4r^4[C - r^4])(X + [C - 2r^4]). \tag{4}$$

This equation determines another curve, E_2.

This curve E_2 has a few rational points which are easily found: those with $X = 2r^4 - C$ or $X = 2r^4$. Besides the point O at infinity, we see E_2 contains the element $P_0 = (2r^4 - C,\, 0)$, necessarily of order 2, and two points $P_1 = (2r^4,\, 2r^2C)$ and $P_2 = (2r^4,\, -2r^2C)$, which are inverses of each other in the group E_2. With some standard computation (see below) we find that the doubles of these points both equal P_0, and hence P_1 and P_2 are of order 4 in the group.

In Theorem 5 we will investigate the curves E_2 in more detail. For now, we must clarify the connection with the original curve E_1.

The composite of the coordinate changes used to transform equation (2) into (4) may be viewed as a rational map $g : E_1 - - \to E_2$. A straightforward substitution of the given formulae yields X and Y as a rather complicated pair of functions of x and y, but if we apply this pair only to the points in E_1 we may use the relation (2) to simplify the component functions of g. (That is, we may use the fact that the function field on E_1 is a simple quadratic extension of $\mathbb{Q}(x)$.) With a bit of computation, this composite can be shown to simplify to $g(x, y) = (X, Y)$, where

$$\begin{aligned} X &= 2r(x^2r + yr^2 - yx^2) \\ Y &= 2rx(x - r)(x + r)(y - r)^2. \end{aligned} \tag{5}$$

In particular these functions are defined on the whole affine curve E_1.

Likewise, the inverse substitutions may be composed and simplified by use of (4) to describe a rational map $f : E_2 - - \to E_1$ given by $f(X, Y) = (x, y)$, where

$$x = \frac{Y}{2r(X + C - 2r^4)} \tag{6}$$

$$y = \frac{-r(X + 2(C - r^4))}{X - 2r^4}.$$

Using (2) and (4) one can compute that $g \circ f$ is indeed the identity map on that part of E_2 where it is defined; since $r \neq 0$, this set is precisely $E_2 \backslash \{P_0, P_1, P_2\}$. Likewise one may verify $f \circ g = 1$ on all of E_1 — it is easily checked that none of these three special points are in the image of g.

We conclude that f and g are isomorphisms between the affine portions of E_1 and $E_2 \backslash \{P_0, P_1, P_2\}$. In particular, for each rational point on E_1 we obtain a distinct rational point on E_2 not equal to P_0, P_1, or P_2. For each point on E_1 arising from a rational triangle, we have noted that its eight conjugates are distinct; now we know that their images under g are distinct as well.

Thus, the projective curve E_2 must have at least twelve points: the images under g of the eight conjugates of (x, y), the three missed points P_i, and the identity O. We already know the order of the last four; let us see if the first eight might also have low order.

First we use the standard formulae for addition on an elliptic curve given in canonical form (4). (See for example [1] for the formulae.) If $P = (X, Y)$ is any point on the (affine) curve, we write its coordinates as $X = X(P)$ and $Y = Y(P)$. If $Y(P) = 0$, then $2P$ is the identity element O in the group E_2 (the point at infinity); if instead $Y(P) \neq 0$, then $X(2P)$ and $Y(2P)$ may be computed as explicit rational functions in X, Y, C, and r. These functions are not particularly memorable but if we apply these formulae to points $P = g(x, y)$ in the image of g, then (using (2) again to eliminate C) we obtain the simpler expressions

$$\begin{aligned} X(2P) &= r^2(x^4 + r^2x^2 + r^2y^2 - x^2y^2)/x^2 \\ Y(2P) &= r^2y(x^2 - r^2)^2(x^2 + y^2)/x^3. \end{aligned} \tag{7}$$

Now we can check for points of low order in the curve E_2.

First we look for points of order 2 in the image of g. (Recall that E_2 also contains a point P_0 of order 2 which is not in the image of g.) Since (X, Y) has order 2 if and only if $Y = 0$, it is clear from (6) that $g(x, y)$ has order 2 if and only if $x = 0$. Thus when applying the doubling formula in the sequel we assume x is not zero. (For some values of C, equation (2) allows no rational solution for y when $x = 0$.)

A point P is of order 3 if and only if $2P = -P$; since $X(-P) = X(P)$, this would require $X(2P) = X(P)$. Since the points not in the image of g do not have order 3, we may write $P = g(x, y)$ and compare (7) to (5); the condition simplifies to

$$r(x^2 - r^2)(rx^2 + ry^2 - 2yx^2) = 0.$$

Since we are assuming $r \neq 0$ and assuming (2) holds with $C \neq 0$, the only way this can be satisfied by an (x, y) on E_1 is if the last factor is zero.

Points of order 4 are those whose double has order 2, i.e., $Y(2P) = 0$. We already know of two points of order 4 on E_2 — the two points P_1, P_2 not in the image of g; their X coordinate is $2r^4$. For rational (or even real) points in the image of g, we see from (7) that most of the conditions allowing $Y(2P)=0$ are inconsistent with (2). Hence for rational points (x,y) on E_1, the point $g(x,y)$ is of order 4 in E_2 if and only if $y=0$. Substituting $y=0$ into (5) and (2), we conclude that the X coordinate of any such point must be $2r^4-2C$.

Finally, points of order 8 are those whose double is a point of order 4. Comparing (7) to the two X-coordinates in the previous paragraph, we compute that $g(x,y)$ has order 8 if and only if either

$$(x^2-r^2)(x^2r^2+y^2r^2-2x^2y^2)=0$$

or

$$r^2(x^2-r^2)(x^2-y^2)=0.$$

As usual, (2) forbids most of the possible pairs (x,y), and so only those with $x^2r^2+y^2r^2-2x^2y^2=0$ actually have order 8. (In particular, P_1 and P_2 are never the doubles of any points on the elliptic curve.)

To summarize, an element $g(x,y)$ has order 2, 3, 4, or 8 if and only if

$$x, \qquad rx^2+ry^2-2yx^2, \qquad y, \qquad \text{or} \qquad x^2r^2+y^2r^2-2x^2y^2$$

vanishes, respectively. Applying these tests to the conjugates P of (x,y), we see that *none* of the eight points $g(P)$ has order 2, 3, or 4 unless

$$x=0, \qquad y=0, \tag{8}$$
$$r^2x^2+r^2y^2-2x^2y^2=0,$$
$$rx^2+ry^2-2|y|x^2=0,$$

or

$$rx^2+ry^2-2|x|y^2=0.$$

Now assume the point (x,y) on E_1 corresponds to a proper rational triangle satisfying the hypotheses of the theorem. Then I claim that none of the equations in the previous paragraph can hold. Certainly $x=p+q>0$. That $y=p-q$ is nonzero, and that the next two equations of (8) fail to hold, is the content of the three assumptions in the statement of the theorem. Finally, the last equation cannot hold for points (x,y) arising from a triangle. Indeed, $x=p+q$ is larger in magnitude than $y=p-q$, so from (2) we necessarily have $|y|<r<x$; since $2x|y|<(x^2+y^2)$, if the last equation did hold we would have $r=2x|y|^2/(x^2+y^2)<|y|$, a contradiction.

So, beginning with a rational triangle meeting the conditions of the theorem, we have an elliptic curve E_2 containing the identity element O, a point P_0 of order 2, two points P_1 and P_2 of order 4, and eight points not of order 2, 3, 4, or 8.

I claim E_2 is then infinite. If not, then as Mazur [6] has shown, E_2 would have to be one of several groups of order 16 or less. The only ones of order at least 12 are $\mathbb{Z}_2\times\mathbb{Z}_6$, $\mathbb{Z}_2\times\mathbb{Z}_8$, and $\mathbb{Z}_{12}$. The group E_2 cannot be the first of these three, as E_2 contains elements of order 4. It cannot be the second, as none of the eight points has order 2, 4, or 8, and it cannot be the third, since at least one of the eight points would have to have order 3.

Thus E_2 has infinitely many rational points. Since the image of $g: E_1 \longrightarrow E_2$ is cofinite, it follows that E_1 also has infinitely many rational points, and hence there are infinitely many solutions to (2). As noted in the introduction, each provides a rational triangle with the same area and base r as the original triangle T. $\square$

The triangles with $p = q$ are the isosceles triangles with their odd leg r as the base; these lead to points of order 2 in E_2. Triangles meeting the other conditions of Theorem 2 give points of order 3 (if $p > q$) and order 8 respectively. We wish to describe these geometrically as well. In addition, the proof of Theorem 2 shows that except for these three classes of triangles, we may construct infinitely many triangles with the given area and base by repeated doubling in the elliptic curve E_2; this process too we wish to view geometrically. That is, we wish to see what the "double" of a triangle looks like.

Using the doubling formulae (7), the inversion f in (6), and the definition (2) of C, one may compute that $2g(x, y) = g(x', y')$, where

$$x' = r(x^2 + y^2)/(2xy), \quad y' = (x^2r^2 + y^2r^2 - 2x^2y^2)/(r(y^2 - x^2)).$$

Thus it is fairly easy to "double" the solutions (x, y) to (2) — one need not even begin with a *rational* triangle. The corresponding formulae for "doubling" points on the Heron surface (1) are more complicated since as noted in the introduction we must apply one of the eight symmetries to (x', y') in order to satisfy the triangle inequalities. However, we can give a pictorial description of this operation.

By scaling and drawing axes appropriately, we may assume the original triangle has vertices at the points (1,0), $(-1, 0)$, and (a, b) in the Cartesian plane, with (a, b) in the first quadrant. Other triangles sharing the base edge and having the same area have the third vertex at some point (a', b) horizontally away from the original vertex. We can use the doubling equations above to compute a' from a. To avoid the extraction of square roots, we set $A = a^2$ and $A' = {a'}^2$, and eliminate the other variables to discover

$$A' = \frac{(A^2 - B^2)^2}{4A((A + B)^2 - 4A)},$$

where $B = b^2 + 1 = (-C/16) + 1$. Thus given a triangle with a fixed area and base, we may readily draw its double in its elliptic curve.

With repeated doublings, the top vertices (a, b) move around the fixed half-line $[0, \infty) \times \{b\}$; the iterations may be viewed as a dynamical system on this ray or, taking all the rays together, on the first quadrant. Some aspects of this system are easy to visualize. When the triangle is very obtuse (i.e., when a is large), its double is less so; in fact $a' \sim a/2$ so these a become quickly smaller and the top vertex moves towards the vertical axis. When on the other hand a triangle is nearly isosceles, its double is extremely obtuse. There is a single equilibrium point on each ray; its first coordinate is $a_0 = (x(b^2 + 1))^{1/2}$, where x is the positive root of $3x^4 + (8 - 16/(b^2 + 1))x^3 + 6x^2 - 1$ (which decreases from $x = 1$ at $b = 0$ to $x = 1/3$ as $b \to \infty$). This equilibrium point is repelling; indeed, $(a' - a_0) \sim (-2)(a - a_0)$. Points to the left of a_0 have their doubles to the right of a_0; points to the right of a_0 which are fairly close to it (specifically, if $a < (b^2 + 1)/a_0$) have doubles to the left of a_0.

If we compute the lengths of the sides of the triangles having one of the equilibrium points as the top vertex, we verify that the second relation in the hypotheses of Theorem 2 holds. That is, the equilibrium points are precisely the "triangles of order 3". Figure 1 makes it clear that most of these triangles are obtuse.

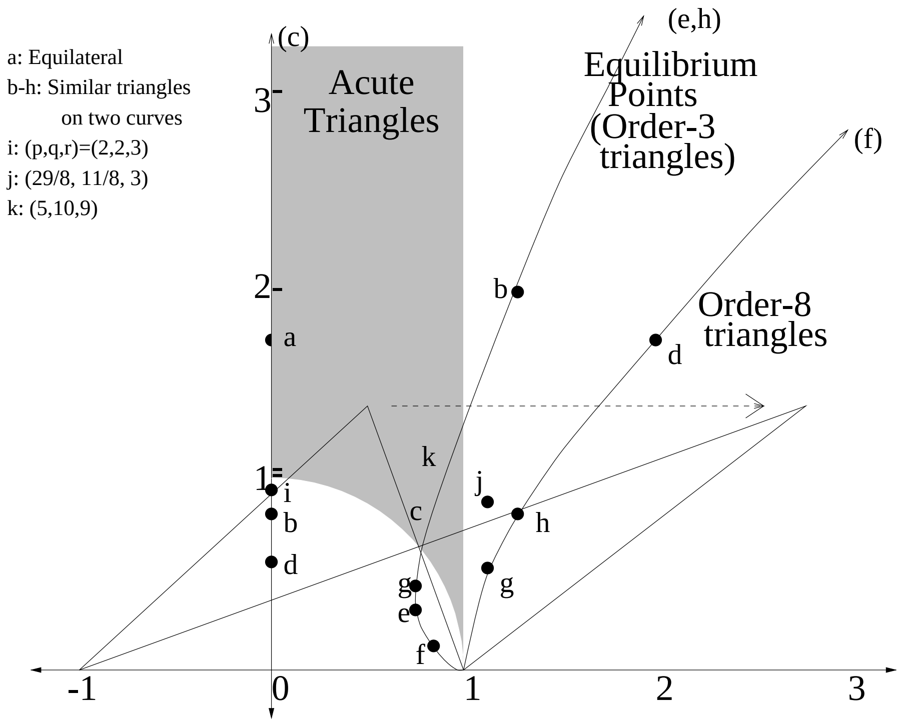

FIGURE 1. A triangle and its double

The remaining condition $r^2(p^2+q^2) = (p^2-q^2)^2$ of Theorem 2 may be expressed in the current variables as simply $A = B$. That is, these triangles of order 8 are those which are carried under the doubling map to isosceles triangles (the top vertex is moved to the vertical axis). Stated alternatively, these triangles are those whose top vertex lies on the hyperbola $a^2 = b^2 + 1$; in particular, these are never acute.

The dynamical system has cycles of all finite lengths, corresponding to points of finite order on the real locus of the elliptic curves E_2, but by Mazur's theorem, as investigated in Theorem 2, none of them are rational triangles.

It would be interesting to describe a simple construction with compass and straightedge which doubles a triangle.

By scaling suitably one may obtain arbitrarily large finite collections of integer triangles with common base and altitude, one of the many questions mentioned in Dickson's History [3].

The geometric picture suggests more algebraic questions about the families of triangles: just as the congruent number problem studies the intersection of the Heron surface with the locus of right triangles, we ask for the intersection of a Heron surface with the locus of isosceles triangles, and with the loci of the other two families of triangles from Theorem 2. For example, we ask if a surface can contain both order-3 and order-8 triangles (it cannot). We may also ask for rational points on the curves of interest in the geometric setting above; the coordinate a is rational for all rational triangles ($4a = p^2 - q^2$) while the height b is also the area and hence rational if and only if $-C$ is a rational square.

Theorem 3. (a) *The isosceles triangles in the Heron surface* (1) *are in one-to-one correspondence with points on the elliptic curve* $Y^2 = X^3 + 4CX$*; in particular, if there are any at all, there are infinitely many.* (*For some* C *there are no such triangles on the surface.*)

(b) *The order-*3 *triangles in the Heron surface* (1) *are in one-to-one correspondence with points on the affine curve*

$$Y^2 = (CX^4 - 1)(CX^4 - 9)$$
$$2Z^2 = Y + CX^4 - 3$$

in $\mathbb{Q}^3$*. In particular, there are at most finitely many on the surface. Thus for almost every* r*, the curve* E_2 *has no points of order* 3*. There are no order-*3 *points on the Heron surface if* $-C$ *is a square* (*that is, none of these triangles has rational area.*)

(c) *There are no order-*8 *points on the Heron surface if* $-C$ *is not a square* (*that is, all these triangles have rational area.*) *If* $-C = c^2$*, then the order-*8 *triangles in the Heron surface* (1) *are in one-to-one correspondence with points on the curve* $Y^2 = 2c(X^5 - X)$*. In particular, there are at most finitely many on the surface. Thus, for almost every* r*, the curve* E_2 *has no points of order* 8*.*

(d) *The set of equilibrium points forms an elliptic curve in the* (a, b) *plane. It has no rational points* (*that is, there are no equilibrium triangles whose vertices are rational — irrespective of the rationality of the sides*)*.*

(e) *The set of points carried to the vertical axis under doubling is a curve of genus zero. The set of rational triangles with such points as vertices is also of genus zero; indeed the rational order-*8 *triangles whose area is also rational are parameterized by*

$$a = (m^2 + 1)^2/(4(m^4 - 6m^2 + 1))$$
$$b = m(m^2 - 1)/(m^4 - 6m^2 + 1).$$

Proof. (a) We calculate that if (p, q, r) are the sides of an isosceles triangle satisfying (1), then $(X, Y) = (2r(p + q + r),\, 4r^2(p + q + r))$ is a point on the curve $Y^2 = X^3 + 4CX$ with $X \neq 0$. Since the rational torsion subgroup of this curve is known to consist only of elements of order 2 when $C < 0$, and since $p + q + r > 0$, isosceles triangles always determine elements of infinite order. Conversely, the sides of the triangle may be recovered from any nontorsion point on the curve by $p = q = (X^2 - 4C)/(4Y)$, $r = Y/(2X)$.

Note that when $-C$ is a square $-(4A)^2$, there are isosceles triangles on the Heron surface if and only if $A/2$ is the area of a rational right triangle. This then is the congruent number problem, and the answer is provided (conjecturally) by Tunnell's theorem [9] (and is certainly negative for some C).

This result provides a complement to Theorem 2 for isosceles triangles T: there are not infinitely many triangles of the same area as T which share the length of the base with T, but there are infinitely many which share the property of being isosceles.

(b) The order-3 triangles in the Heron surface (1) are those in the intersection with the rational surfaces determined by $\pm r(p^2 + q^2) = (p - q)(p + q)^2$. We can thus use (1) to determine C in terms of p and q.

Set $X = (p^2+q^2)/(2pq(p+q))$ and $Y = (p^2+q^2)(p^2+4pq+q^2)/((pq)^2(p+q)^2)$. Then this (X, Y) satisfies the first of the stated equations. Note that from X and Y we may only compute the symmetric polynomials $p+q$ and pq. So set $Z = (p-q)/(p+q)$; then (X, Y, Z) can be checked to satisfy the other stated equation as well. Moreover, we may now compute $(p, q) = 4X(Z \pm 1)/(Y - 4X^2)$ and then compute r as well from these p and q.

The projection of this curve to the (X, Y)-plane is a nonsingular hyperelliptic curve of genus 3 and hence finite; since the projection is at worst a two-to-one map, our curve also has at most finitely many rational points; thus there are only finitely many order-3 triangles on the surface. Moreover, if $C = -c^2$ were a square, then if we set $W = cX^2$ we would obtain a rational point on the curve $Y^2 = (W^2+1)(W^2+9)$. However, this elliptic curve may be checked to have rank zero; its only rational affine points are $(0, \pm 3)$, which do not correspond to nondegenerate triangles.

(c) The order-8 triangles in the Heron surface (1) are those in the intersection with the rational surface determined by $r^2(p^2+q^2) = (p^2-q^2)^2$. Eliminating r shows $C = -(2pq(p^2-q^2)/(p^2+q^2))^2$, that is, $-C$ is a perfect square if there are any such triangles on the Heron surface. Moreover, if $C = -c^2$, we have a point $(X, Y) = (q/p,\, c(p^2+q^2)/p^3)$ on the hyperelliptic curve $Y^2 = 2c(X^5 - X)$. Since the genus is two, there can be at most finitely many such points for any given c.

We may parameterize the c for which there are solutions. The rational surface containing all order-8 triangles is parameterized by

$$(p, q, r) = (\,2m(m^2+1)d, (m^4-1)d, (m^4-6m^2+1)d\,)$$

for rational m and d. Then $c = 4(m^7 - 7m^5 + 7m^3 - m)d^2$.

(d) Note that in (d) and (e) we study the rational surfaces of (b) and (c) through their intersections with the hyperplane $r = 2$ rather than with any single Heron surface.

We have already noted that the top vertices of the order-3 triangles trace out the curve of equilibrium points under the dynamical system. For those with rational coordinates (a, b), the ratio $x = A/B = a^2/(b^2+1)$ is also rational and we have a parameterization of A and B in terms of x. Then the condition that (a, b) also be rational is the statement that the pair of equations $a^2 = 16x^4/((3x-1)(x+1)^3)$ and $b^2 = (3x+1)(x-1)^3/((3x-1)(x+1)^3)$ have a rational solution x. Such an x makes $(3x-1)(x+1)$ and $(3x+1)(x-1)$ squares simultaneously, that is, we can parameterize these top vertices by an intersection of two quadric surfaces, which is an elliptic curve. Parameterizing the solutions to $y_1^2 = (3x-1)(x+1)$ with $x = (m^2+1)/(m^2+4m+1)$ shows that m must satisfy $y_2^2 = m^3+m^2+m$. But this curve has no rational points except where $m = 0, m = \pm 1$; these do not correspond to (finite) points (a, b).

(e) Since rational order-8 triangles only occur with rational area, the parameterization given in the proof of (c) (choosing d to make $r = 2$) gives in turn a parameterization of the rational triangles' top vertex, since $a = (p^2-q^2)/4$ and $b = c/4$. $\square$

Following the proof of Theorem 2, we see that the curves E_2 have torsion consisting only of the cyclic group $\{O, P_0, P_1, P_2\}$ of order 4, unless the curve contains triangles of one of the three special types. From Theorem 3, it is clear that most of these curves do not.

Given a triangle T whose sides satisfy one of the three disallowed equations of Theorem 2, the approach used in the proof of the theorem certainly fails: the subgroup of E_2 generated by the known points may be shown to be finite, and so there is no guarantee that there are more triangles sharing an edge of length r.

Among triangles violating one of the three hypotheses of Theorem 2, there are some for which E_2 has positive rank, although the twelve known points lie in a finite subgroup; in these cases there seems to be no natural way to construct the other triangles from T. For example, in addition to the isosceles triangle with $(p, q, r) = (2, 2, 3)$ there *are* infinitely many triangles with base 3 and $C = -63$, even though the one given point has finite order in the group. (An element of infinite order in this group is provided by the triangle $(29/8, 11/8, 3)$.) There also exist examples in which E_2 has rank zero, so that in fact there do *not* exist infinitely many triangles with the same area as T and a common side r. This is true of the minimal integral examples of triangles of order 3 and of order 8 (the triangles $(5, 10, 9)$ and $(15, 20, 7)$ respectively).

On the other hand, one may use the ideas of Theorem 2 with any of the three sides of the triangle as the fixed base r. Thus we are indeed able to use the theorem to find more triangles of the same area if there is some permutation of p, q, and r in which none of the three preceding relations holds.

Theorem 4. *Given any non-equilateral rational triangle T there exist infinitely many other rational triangles with the same area as T and sharing a side with T.*

Proof. We need only consider triangles whose sides violate the assumptions of Theorem 2: those with $p = q$, $r(p^2+q^2) = |p-q|(p+q)^2$, or $r^2(p^2+q^2) = (p^2-q^2)^2$.

For any such triangle, we consider whether Theorem 2 may be applied to its reflection (p, r, q). That theorem now applies unless either $p = r$, $q(p^2 + r^2) = |p - r|(p + r)^2$, or $q^2(p^2 + r^2) = (p^2 - r^2)^2$.

Since we are assuming the triangle is not equilateral, there must be some pair of equations from these two lists which is satisfied, other than the first pair ($p = q$ and $p = r$). We have seen (Theorem 3(b,c)) that it cannot be true that the same triangle is an order-3 triangle when using r as the base, and an order-8 triangle when q is the base. It is also clear from Figure 1 that (up to scaling) there is a unique isosceles order-8 triangle, and just two isosceles order-3 triangles; their side lengths however are not rational. (It is even possible to rule out geometrically the possibility that a triangle is order-8 when viewed with two different sides as the base, since these triangles are uniquely parameterized (up to scaling) by their nonacute angle.) However, in keeping with the pattern of this paper we resolve all these pairs of equations algebraically.

Setting aside the isosceles-isosceles pair, the eight remaining pairs are most easily handled on a computer algebra system by treating the second equation in each list as one of two possibilities, one with $|p-q| = p-q$ and the other with $|p-q| = q-p$; then there are 15 pairs of equations to examine. Whenever the first equation of the pair is $p = q$, we merely substitute p for q in the second equation; otherwise, we use the first equation to solve for r and substitute this into the second equation.

For example, if the sides of a triangle satisfy both $r(p^2+q^2)=(p-q)(p+q)^2$ and $q(p^2+r^2)=(p-r)(p+r)^2$, then by eliminating r we conclude

$$4p^2q(p-q)(3p^2+2pq+q^2)(p^3-pq^2-2q^3)=0.$$

Since these factors are homogeneous and irreducible, the factors of degree greater than one cannot be zero for any positive rational p and q. Since p and q are side lengths in a triangle, these factors are also nonzero. Finally, if $p-q=0$, then the first of the pair of equations shows $r=0$. In any case, we achieve a contradiction: no rational triangle is an order-3 triangle relative to two bases.

With similar simple but unenlightening calculations, one may show that each of the 15 pairs of the equations implies in this way an equation in two rational variables which is always the product of irreducible homogeneous factors, the only linear factors among them being either individual variables or sums or differences of two of them. In all non-equilateral cases we would conclude that one of the variables is zero, which is impossible in a proper triangle.

Therefore, the only rational triangles in which both (p,q,r) and (p,r,q) are disallowed by Theorem 2 are the equilateral triangles, and so Theorem 4 is proved.

(The similarity classes of real triangles which lie in the three special families with respect to more than one choice of "r" are shown on Figure 1.) □

When a triangle is equilateral, of course, all permutations of the edges yield the same elliptic curve (4), which may be shown to have rank zero. Therefore, there do not exist infinitely many triangles having a common side with and the same area as a given equilateral triangle. We proved in Theorem 1 that there are infinitely many triangles with this area;[3] but in fact, we can find infinitely many all sharing a common side. Indeed, by scaling, we may assume the equilateral triangle has side length 1; then $C=-3$. In order to find infinitely many other triangles with the same area, we need to find some value of r so that the elliptic curve (4) has positive rank. Taking $r=1/3$ suffices; a generator is provided by the triangle $(p,q,r)=(67/15,\ 21/5,\ 1/3)$. Applying Theorem 2 to this triple we conclude there are indeed infinitely many triangles with the same area as an equilateral one, all with a side of the same length.

The proof of Theorem 2 focuses attention on the curves E_2. We have discussed their torsion subgroups and described the actions of the eight symmetries. The principal question, naturally, is to know for which pairs (C,r) the curve E_2 has positive rank. This problem seems to be at least as hard as the corresponding question in the congruent number problem — in that setting the elliptic curves corresponding to the sets of triangles with various areas are twists of each other. (All have the same j-invariant, $j=1728$.) Our curves, however, show considerable variation, as the next result shows.

For each rational $\lambda<0$, let $E(\lambda)$ be the elliptic curve defined by equation (4) with $C=\lambda$ and $r=1$. These curves include, up to rational isomorphism, all the curves E_2 considered in this paper, since the scaling $(X,Y)\longrightarrow(X/r^4,Y/r^6)$ is a bijection $E_2\longrightarrow E(C/r^4)$. On the other hand, these curves are in general not isomorphic to each other, even over $\overline{\mathbb{Q}}$:

[3] Paul Desruisseaux has earned extra credit from me in his Linear Algebra class by discovering, by elementary means, the isosceles triangle $(7/4,\ 7/4,\ 1/2)$ whose area equals that of the equilateral triangle with side length 1.

Theorem 5. *Suppose λ and λ' are distinct negative rational numbers for which the curves $E(\lambda)$ and $E(\lambda')$ are isomorphic over $\overline{\mathbb{Q}}$. Then*

(a) *There exist rational numbers $s > 1$ and $t > 1$ such that $\lambda = 1 - s^4$ and $\lambda' = 1 - t^4$; in addition, we have $st = s + t + 1$. Thus for each λ there exists at most one such λ'. Conversely, for any such pair s, t, the curves $E(1 - s^4)$ and $E(1 - t^4)$ are $\overline{\mathbb{Q}}$-isomorphic.*

(b) *$E(\lambda)$ and $E(\lambda')$ are (-1)-twists of each other, that is, curves that are isomorphic over $\overline{\mathbb{Q}}$, are isomorphic over $\mathbb{Q}(i)$, and are not isomorphic over $\mathbb{Q}$.*

(c) *$-\lambda$ is not a square; in particular, the curves E_2 parameterizing triangles with a fixed rational area and base 1 are not isomorphic to any of the other curves E_2.*

(d) *The torsion subgroup of the elliptic curve $E(\lambda)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$; in particular, these curves contain no order-3 or order-8 triangles.*

(e) *There is no rational triangle for which $\lambda = C/r^4$ and $\lambda' = C/q^4$ unless $q = r$; that is, no two of the three curves E_2 associated to a rational triangle are ever isomorphic* (*unless of course the triangle is isosceles*)*.*

Proof. (a) We investigate the conditions under which $E(\lambda)$ and $E(\lambda')$ have the same j-invariant. A straightforward computation (see e.g. [1]) shows that the j-invariant of the curve $E(\lambda)$ is

$$j(\lambda) = -16(\lambda^2 - 16\lambda + 16)^3/(\lambda^4(\lambda - 1)). \tag{9}$$

It is an elementary graphing exercise to determine that $j(\lambda) > 1728$ for negative real λ, and that for each negative λ there is only one other negative real λ' for which $j(\lambda) = j(\lambda')$. We wish to determine the relationship between λ and λ'. The condition that λ and λ' have the same j-invariant may be expressed as the vanishing of a high-degree polynomial in λ and λ'. Perhaps surprisingly, this curve has genus zero, and so we may explicitly parameterize the set of such pairs (λ, λ').

For any $x \neq 1$ let $x^\sigma = x/(x - 1)$. Then we verify directly from (9) that $j(x) = j(x^\sigma)$ for all $x \neq 0, 1$. This implies the function j lies in the fixed subfield $\mathbb{Q}(x)^{\langle\sigma\rangle}$, which is $\mathbb{Q}(x \cdot x^\sigma)$; indeed we can eliminate λ and obtain

$$j(\lambda) = 16^2(1 - u)^3/u^2 \qquad \text{where} \qquad u = \lambda^2/(16(\lambda - 1)) = \lambda\lambda^\sigma/16. \tag{10}$$

Likewise, $j(\lambda')$ can be expressed in terms of $u' = (\lambda')^2/(16(\lambda' - 1))$.

Thus $j(\lambda) = j(\lambda')$ if and only if $(1-u)^3(u')^2 = (1-u')^3u^2$, which requires either $u = u'$ or $(u + u') = 3(uu') - (uu')^2$. Now since both λ and λ' are negative, we cannot have $\lambda' = \lambda^\sigma$; and we are assuming $\lambda' \neq \lambda$ as well. Thus u cannot equal u', and it is the other condition which must hold. In this case, the sum s and product p of u and u' satisfy $s = 3p - p^2$, so that u and u' can be recovered by the quadratic formula. This requires that $p(p - 4)$ be a square; this in turn is true if and only if $p = (t+1)^2/t$ for some t. Then we solve for $u, u' = -t(t+1), -(t+1)/t^2$. (Replacing t by $1/t$ if necessary we may take these to be u and u' in this order.)

We then solve for λ and λ' using (10). Solving first for λ' we discover that $(t + 1)$ must be square; then when solving for λ we find t is also a square. Both are true if and only if $t = ((1 - s^2)/(2s))^2$ for some rational s. In that case we compute $\lambda = 1 - s^4$ or $1 - s^{-4}$ and $\lambda' = -8s(1+s^2)/(1-s)^4$ or $8s(1+s^2)/(1+s)^4$. Replacing s by $1/s$, $-s$, or $-1/s$ as necessary, we may assume it is the first of these possibilities, in each case, which holds. Then $\lambda, \lambda' < 0$ forces $s > 1$.

Finally, we observe that this λ' equals $1-t^4$, where $t=(s+1)/(s-1)$. This completes the proof of (a) (the converse statement being a straightforward calculation that the j-invariants are equal).

(b) The Weierstrass normal form (4) of the curve $E(1-s^4)$ is

$$Y^2=(X-2s^2)(X+2s^2)(X-1-s^4). \tag{11}$$

Substituting $Y=i(s-1)^6Y'/8$, $X=-(s-1)^4X'/4+(s^2+1)^2/2$ gives the curve which simplifies to $Y^2=(X-2t^2)(X+2t^2)(X-1-t^4)$ where $t=(s+1)/(s-1)$, proving the curves are isomorphic over $\mathbb{Q}(i)$.

We can then show the curves are never $\mathbb{Q}$-isomorphic: writing the curves in the form $Y^2=X^3+A(s)X+B(s)$, substitutions roughly like those above show that $E(1-t^4)$ is $\mathbb{Q}$-isomorphic to the curve given by $Y^2=X^3+A(s)X-B(s)$; this is only isomorphic to $E(1-s^4)$ if $B(s)=0$. But $B(s)=(-2/27)(s^{12}-33s^8-33s^4+1)$, which has no rational roots, and so the isomorphisms cannot be realized over $\mathbb{Q}$.

For (c), we need only recall that the Fermat equation $-c^2=1-s^4$ has no solutions in $\mathbb{Q}$. Thus among the curves describing rational triangles with rational area, $E_2\cong E_2'$ would imply $E(C/r^4)\cong E(C'/(r')^4)$; since $-C$ is a square, so is $-C/r^4$; since this cannot be of the form $1-s^4$ for any rational s, we must have $C/r^4=C'/(r')^4$, so that E_2' simply parameterizes those triangles which are obtained from the triangles of E_2 by scaling.

(d) We see from (11) that the curve $E(\lambda)$ contains three elements of order two. In addition, we have seen in the proof of Theorem 2 that the curve contains elements P_1 and P_2 of order four. By Mazur's theorem, the torsion subgroup can only be $\mathbb{Z}_2\times\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_8$. But by Theorem 3(c), the latter can only hold if $-\lambda$ is a square, and by Theorem 5(c), this does not occur.

(e) We note first that we cannot have $\lambda=u^2\lambda'$ unless $u=\pm1$. Given two rational numbers $s>1$ and $t=(s+1)/(s-1)$ with $1-s^4=u^2(1-t^4)$, then setting $Y=us^2/(s-1)^2$ and $X=s/2$ gives a rational point on the curve $Y^2=X^3-4X$. But all the points on this curve have $Y=0$, forcing $u=0$, a contradiction. Now, since the curves associated to a rational triangle using r and q as base have $\lambda=C/r^4$ and $\lambda'=C/q^4$ respectively, the preceding argument shows (taking $u=(q/r)^2$) that if these curves are isomorphic over $\overline{\mathbb{Q}}$, then $q=r$.

Thus we see that the doubling operations, applied to the three sides of a scalene triangle, are fundamentally different procedures for producing more triangles of a given area. □

The twists have a nontrivial effect on the present arithmetic problems. For example, when $s=4$, the curve $E(1-s^4)$ has rank 1; the solution $x=33$, $y=7/8$ gives a generator of the infinite family of solutions to (2) with $C=-255$. On the other hand, the curve $E(1-t^4)$ (as in Theorem 5(a), $t=5/3$) has rank zero; the only solutions of (1) correspond to the eight torsion points on the curve.

We mention in passing that there are other curves of geometric interest in the Heron surface (1). For example, the points corresponding to triangles of a fixed perimeter P also form an elliptic curve; it may be reduced to

$$Y^2=X^3+(X+e)^2,$$

where $e=-4C/P^4$, using the transformation $p=(P/2)(X+e)/X$ and $q=-(P/2)(X^2+4e)/(1-2e+2X+2Y)$. Naturally, these curves are arithmetically distinct for different values of e, although they all have elements $(X, Y) = (0, \pm e)$ of order 3 (which do not correspond to triangles). One may identify five families of exceptional triangles corresponding to the possible torsion subgroups consistent with this observation and with Mazur's theorem; as in Theorem 2, all triangles not in one of these families lies on an elliptic curve of infinite order.

Likewise one may look for triangles of a given area and possessing a fixed angle, as done by Buddenhagen [8]. In this case, fixing the angle opposite the side of length r fixes $s(s-r)$ (where $s = (p+q+r)/2$); then (1) fixes $(s-p)(s-q)$ as well, so that the possible values of the variables are determined by the intersection of two quadric surfaces, which is again an elliptic curve. Once again we may exclude some families of triangles and deduce that all remaining triangles with a given area and interior angle lie in infinite families of such.

We have shown several ways to generate points on the Heron surface. It is interesting to speculate as to whether these techniques may be iterated to generate all points on the surface. That is, beginning with any one point (p, q, r) on the surface (e.g. using Theorem 1) we may find others sharing one of its coordinates (using Theorem 2). For each of these, we may in turn find more points sharing a coordinate with it, and so on. Does this procedure eventually exhaust the rational points on the surface? We know the answer is "no" when the initial triangle is equilateral, but I have no information about the general case.

I would like to thank Jim Buddenhagen for several suggestive conversations and pointers to the literature, and the anonymous referee for some stylistic improvements.

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society, London, 1991.

[2] Noam D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp. **51** (1988), 825–835.

[3] Cited in Leonard Eugene Dickson, *History of the Theory of Numbers*, vol.II Carnegie Institution of Washington, 1919, p.172. (Further citations of relevant material on rational right triangles are on pp. 172–174; other rational triangles with rational area on pp. 191–202; and other rational triangles on p. 215.)

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

[5] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Second edition. Graduate Texts in Mathematics, no. 97. Springer-Verlag, New York, 1993.

[6] Barry Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129-162.

[7] Paul T. Bateman et al, eds., *Advanced problem 6628*, American Mathematical Monthly **97** (1990), 350.

[8] Paul T. Bateman et al, eds., *Triangles with integer sides whose area is the square of an integer*, American Mathematical Monthly **98** (1991), 772-774.

[9] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

Department of Mathematical Sciences, Northern Illinois Univ., DeKalb IL, 60115, USA

rusin@math.niu.edu http://www.math.niu.edu/~rusin

This paper is available via http://nyjm.albany.edu:8000/j/1998/4-1.html.