

Heron triangles, Diophantine problems and elliptic curves

Garikai Campbell and Edray Herber Goins

ABSTRACT. For all nonzero rational t , $E_t : v^2 = u^3 + (t^2 + 2)u^2 + u$ is an elliptic curve defined over \mathbb{Q} . By analyzing this family of curves, we are able to describe connections between the problem of finding Heron triangles with a given area possessing at least one side of a particular length, finding points in the plane at rational distance and finding rational Diophantine quadruples and quintuples. We are then, quite naturally, led to study the relationship between these problems and elliptic curves defined over \mathbb{Q} with rational torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Consequently, we find a new elliptic curve with this torsion having rank 3 (tying the record for the largest known rank of an elliptic curve of this kind). We also find an infinite family of elliptic curves defined over \mathbb{Q} with rational torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank at least 1 (again tying the record).

CONTENTS

1. Introduction.	1
2. Summary of Results.	2
3. Heron Triangles and E_t .	4
4. Points at Rational Distance.	8
5. Heron Triangles and Diophantine Triples.	11
6. Heron Triangles and Elliptic Curves of Large Rank.	12
Acknowledgements	15
References	15

1. Introduction.

It is certainly no secret that elliptic curves play a central role in solving a number of Diophantine problems. In fact, there are instances when solving distinct Diophantine problems requires studying the same elliptic curve or family of elliptic

Mathematics Subject Classification. 14G05, 11G05, 11D25.

Key words and phrases. Heron triangles, rational distance sets, elliptic curves, rank, torsion, Diophantine triples.

The first author was supported by the Woodrow Wilson Career Enhancement Fellowship.

The second author was supported by a fellowship from the Irvine Foundation.

curves. One of the goals of this paper is to describe how several Diophantine problems are conjoined in just such a way. In particular, the family of curves defined by

$$E_t: v^2 = u^3 + (t^2 + 2)u^2 + u$$

weds the problem of finding Heron triangles possessing various properties to the problems of finding points in the plane at rational distance and finding rational Diophantine quadruples.

We show that E_t is an elliptic curve defined over \mathbb{Q} for all nonzero rational values of t and that for all such t , $E_t(\mathbb{Q})$ contains at least one rational point of order 4. Moreover, for certain rational values of t , $E_t(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. As a result, we are led to consider the relationship between elliptic curves defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the Diophantine problems discussed here. This in turn leads to the discovery of a new elliptic curve and an infinite family of elliptic curves with “large” rank whose group of rational points has torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Our work begins with a study of *Heron triangles*—triangles with rational area whose sides have rational length. In particular, we first describe how to find Heron triangles of a given area with the length of one of the sides being fixed. N. J. Fine [13] proved that every positive integer is the area of some Heron triangle and though Fine never explicitly mentions elliptic curves, a central step in achieving his result is the doubling of a point on a particular elliptic curve. Perhaps more well known, Jerrold Tunnell [21] essentially solved the *congruent number problem*—the problem that asks which positive integers are the area of some *right* Heron triangle—by proving some deeper facts about a family of elliptic curves. More recently, David Rusin [19] generalized Fine’s results by carrying out an extensive analysis of a family of elliptic curves. We perform an analysis similar to Rusin’s on the family of elliptic curves E_t . This analysis leads to the results outlined below.

2. Summary of Results.

Letting \mathbb{Q}^* denote the nonzero rationals, we prove the following statements about E_t :

Theorem 2.1. *For all $t \in \mathbb{Q}^*$, E_t is an elliptic curve defined over \mathbb{Q} and the torsion subgroup of $E_t(\mathbb{Q})$ must equal $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. In particular, $(-1, t)$ is a point of order 4 which is never in $2E_t(\mathbb{Q})$ and $E_t(\mathbb{Q})$ can never contain a point of order 3.*

We let G_t equal the group of order 4 generated by $(-1, t)$.

Theorem 2.2. *For all $t \in \mathbb{Q}^*$, each point $P_t \in E_t(\mathbb{Q}) - G_t$ corresponds to a Heron triangle and this correspondence is surjective.*

Theorem 2.3. *$E_t(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if and only if $t = (s^2 - 1)/s$ for some $s \in \mathbb{Q}^*$, $s \neq \pm 1$.*

Theorem 2.4. *If the torsion subgroup of $E_t(\mathbb{Q})$ equals $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then the 4 additional points of finite order (i.e. those not in G_t) correspond to an isosceles Heron triangle.*

Theorem 2.5. *The torsion subgroup of $E_t(\mathbb{Q})$ equals $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if and only if $t = (s^2 - 1)/s$ with $s = (r^2 - 1)/(2r)$ for some $r \in \mathbb{Q}^*, r \neq \pm 1$,*

We will denote the curve E_t where $t = (s^2 - 1)/s$ as $E_{t(s)}$ and similarly denote the curve $E_{t(s)}$ with $s = (r^2 - 1)/(2r)$ as $E_{t(s(r))}$.

We first apply our results on E_t to find a new infinite set of points in the plane at rational distance. A set of points in the plane is said to be *at rational distance* if the distance between each pair of points in the set is rational. The following theorem is an immediate consequence of Theorems 2.2 and 2.3:

Theorem 2.6. *If $h = 2s/(s^2 - 1)$, then for all $s \in \mathbb{Q}^*, s \neq \pm 1$, the set*

$$\left\{ \left(\frac{(u-1)vh}{2u(u+1)}, h \right) \mid (u, v) \in E_{t(s)}(\mathbb{Q}) - G_t \right\} \cup \{(-1, 0), (1, 0), (-1, 2h), (1, 2h)\}$$

is a set of (rational) points at rational distance. Furthermore, this set is infinite for infinitely many s .

When trying to find sets of points at rational distance, one often excludes the possibility that more than two points lie on a line or that more than three points lie on a circle. We call a set of points in the plane *concylic* if the points lie on a circle and we consider the following question recently posed by Nathaniel Dean [7]:

Question 2.7. *Are there four non-concylic points at rational distance on the parabola $y = x^2$?*

This question was answered affirmatively by one of the authors [3], with the family of curves E_t being central to the solution. As a result, we have:

Theorem 2.8. *Each triple of non-isosceles Heron triangles of equal area possessing precisely one side in common corresponds to a quadruple of non-concylic points at rational distance on the parabola $y = x^2$.*

We now shift focus and define a set of nonzero rationals $\{a_1, a_2, \dots, a_m\}$ to be a *rational Diophantine m -tuple* if for each $1 \leq i < j \leq m$, $a_i a_j + 1$ is a square. We show:

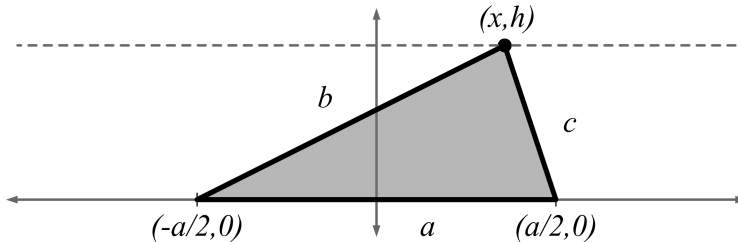
Theorem 2.9. *For all $s \in \mathbb{Q}^*, s \neq \pm 1$, the rational Diophantine triple $\{-1/s, s, (s^2 - 1)/s\}$ can be extended to a rational Diophantine quadruple if and only if $E_{t(s)}$ has positive rank.*

Equivalently, specific Heron triangles correspond to rational Diophantine quadruples containing $\{-1/s, s, (s^2 - 1)/s\}$.

Remark 2.10. We note that a theorem of Dujella's [8] implies that without loss of generality we may replace the word "quadruple" with the word "quintuple" in the statement of the theorem above.

Finally, we turn our attention to the relationship between elliptic curves defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and Heron triangles. More specifically, we show

Theorem 2.11. *Each elliptic curve defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ corresponds to a family of Heron triangles of equal area possessing at least one side in common.*

FIGURE 1. The triangle $\langle a, b, c \rangle$.

Consequently, we find the following record-tying examples of curves with torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and “large” rank:

Theorem 2.12. *The elliptic curve $E_{t(s(r))}$ with $r = 15/76$ has rank 3.*

Theorem 2.13. *If H is the curve defined by $H : n^2 = m^4 + 2m^2 + 4m + 2$, then for each rational point (m, n) in $H(\mathbb{Q})$, $n > 0, m \neq \pm 1, -1/2, -2$, the elliptic curve $E_{t(s(r))}$ with*

$$r = \frac{n - 2m - 1}{m^2 - 1}$$

has rank at least 1. Furthermore, $H(\mathbb{Q})$ is infinite.

3. Heron Triangles and E_t .

It will be convenient to refer to particular embeddings of a triangle in the plane and hence we let the ordered 3-tuple $\langle a, b, c \rangle$ denote the triangle with vertices $(-a/2, 0)$, $(a/2, 0)$ and (x, h) , where $h > 0$, b is the distance from (x, h) to $(-a/2, 0)$, and c is the distance from (x, h) to $(a/2, 0)$. (See Figure 1.) We will call a the *first side* and h the *primary altitude*.

Now suppose we fix a and h and consider the points, $[X, B, C, D]$, in projective 3-space defined by the intersection of the two quadrics

$$(3.1) \quad \left(X + \frac{a}{2}D\right)^2 + h^2D^2 = B^2$$

$$(3.2) \quad \left(X - \frac{a}{2}D\right)^2 + h^2D^2 = C^2.$$

We denote this curve by $C_{a,h}$ and make a few observations. First, $aX = B^2 - C^2$ so that X is rational whenever a, B and C are rational. Hence, the triangle $\langle a, b, c \rangle$ is a Heron triangle if and only if we can find a rational point of the form $[x, b, c, 1]$ on $C_{a,h}$. We will call the points on $C_{a,h}$ with $D \neq 0$, the affine points and denote them by (x, b, c) . We will call the points on $C_{a,h}$ with $D = 0$, the *points at infinity*. Observe that there are precisely four points on $C_{a,h}$ at infinity and they are all rational. We let $G'_{a,h} = \{[1, \pm 1, \pm 1, 0]\} \subset C_{a,h}(\mathbb{Q})$. With this, we have:

Theorem 3.1. *For all $t \in \mathbb{Q}^*$*

1. $E_t : v^2 = u^3 + (t^2 + 2)u^2 + u$ is an elliptic curve defined over \mathbb{Q} .
2. $G_t = \{(-1, t), (0, 0), (-1, -t), \mathcal{O}\}$, where \mathcal{O} is the point at infinity on E_t , is a subgroup of $E_t(\mathbb{Q})$ of order 4 generated by $(-1, t)$.

3. For all $a, h \in \mathbb{Q}^*$ satisfying $t = a/h$:
- a) E_t is isomorphic over \mathbb{Q} to $C_{a,h}$ and in particular, the map $\varphi_t : E_t \longrightarrow C_{a,h}$ given by

$$\varphi_t(u, v) = \left(\frac{a(u-1)v}{2tu(u+1)}, \frac{tau^2 - tau - auv - av}{2tu(u+1)}, \frac{tau^2 - tau + auv + av}{2tu(u+1)} \right)$$

is an isomorphism.

- b) $\varphi_t(G_t) = G'_{a,h}$.

Proof. The first two claims are easily verified by computing the discriminant of E_t and repeatedly doubling the point $(-1, t)$.

Now, suppose $a, t, h \in \mathbb{Q}^*$ are fixed such that $t = a/h$, then to verify that φ_t is an isomorphism, we give the inverse of the map:

$$\varphi_t^{-1}(x, b, c) = \left(\frac{a+b+c}{a-b-c}, \frac{t(-b+c)(a+b+c)}{a(a-b-c)} \right)$$

and argue that φ_t and its inverse are indeed morphisms and not simply birational maps. Working with the projective models of the curves, we can replace rational functions by ones equivalent over the function fields of the curves to show that the map is regular at all points. (See II.2 in [20] for a more complete discussion.) For example, φ_t appears not to be well-defined at $(0, 0)$, but we may express the map as $[\varphi_{t,1}, \varphi_{t,2}, \varphi_{t,3}, 1]$, clear denominators, divide through by v and replace u/v by $v/(u^2 + (t^2 + 2)u + 1)$ to see that $\varphi_t(0, 0) = [1, 1, -1, 0]$. Similar calculations demonstrate that $\varphi_t(G_t) = G'_{a,h}$. \square

Remark 3.2. Note that because we mean for the values a and h to represent lengths, despite the fact that $C_{a,h}$ is an elliptic curve for all $a, h \in \mathbb{Q}^*$, we need only consider the positive values of $a, h \in \mathbb{Q}$. From equations 3.1 and 3.2, we see that $C_{a,h} \cong C_{-a,h} \cong C_{a,-h}$ so that we do not lose any curves in restricting our attention to $C_{a,h}$ with $a, h > 0$. As a consequence, the equations defining E_t are even in t so that we need only consider $t \in \mathbb{Q}$ with $t > 0$. Given these remarks, we let \mathbb{Q}^+ denote the positive rationals and unless stated otherwise, only consider $a, h, t \in \mathbb{Q}^+$ for the remainder of the paper.

Similarly, $C_{a,h}$ and $C_{\alpha a, \alpha h}$ are isomorphic over \mathbb{Q} for all $\alpha \in \mathbb{Q}^*$ and $C_{a,h}$ admits the automorphism $[X, B, C, D] \mapsto [X, C, B, D]$. These statements are clear from the equations defining $C_{a,h}$, but we may also see this geometrically. In particular, scaling the Heron triangle $\langle a, b, c \rangle$ by a rational factor or reflecting the triangle across the y -axis keeps the ratio of first side to primary altitude fixed.

Therefore, if we let

$$[\langle a, b, c \rangle] = \{ \langle \alpha a, \alpha b, \alpha c \rangle \mid \alpha \in \mathbb{Q}^+ \} \cup \{ \langle \alpha a, \alpha c, \alpha b \rangle \mid \alpha \in \mathbb{Q}^+ \}$$

and let \mathcal{H}_t denote the set of these equivalence classes in which the ratio of first side to primary altitude of any representative triangle is t , then the discussion above and Theorem 3.1 imply:

Theorem 3.3. *For all $t \in \mathbb{Q}^+$, \mathcal{H}_t represents all Heron triangles with area congruent to $2t$ modulo $(\mathbb{Q}^+)^2$ and the map $\Phi_t : E_t(\mathbb{Q}) - G_t \longrightarrow \mathcal{H}_t$ defined by*

$\Phi_t(u, v) = [\langle a, |b|, |c| \rangle]$, where

$$\begin{aligned} b &= \frac{\tau u^2 - \tau u - a u v - a v}{2t u(u+1)} \quad \text{and} \\ c &= \frac{\tau u^2 - \tau u + a u v + a v}{2t u(u+1)} \end{aligned}$$

is surjective.

Remark 3.4. Observe that if $P = (u, v) \in E_t(\mathbb{Q}) - G_t$, for some $t \in \mathbb{Q}^+$ and $\varphi_t(P) = (x, b, c)$, then

$$(3.3) \quad \{\varphi_t(\pm P + Q) \mid Q \in G_t\} = \{(\pm x, \pm b, \pm c)\}.$$

This follows immediately from the fact that $(u, v) + (-1, t) = (u', v')$ where

$$u' = -\frac{(v + ut)^2}{u(u+1)^2} \quad \text{and} \quad v' = \frac{t(u-1)(v+ut)^2}{u(u+1)^3},$$

which gives us $\varphi_t(P + (-1, t)) = (-x, c, -b)$, and the fact that $-P = (u, -v)$, which gives us $\varphi_t(-P) = (-x, c, b)$. Hence, if we define $[P]$ to be the set $\{\pm P + Q \mid Q \in G_t\}$ and let $\mathcal{P}_t = \{[P] \mid P \in E_t(\mathbb{Q}) - G_t\}$, then equation 3.3 proves that the induced map $\overline{\Phi}_t : \mathcal{P}_t \rightarrow \mathcal{H}_t$ defined by $\overline{\Phi}_t([P]) = \Phi_t(P)$ is well-defined. Moreover, the map $\overline{\Phi}_t$ is not only surjective, but injective as well.

In order to complete our understanding of the relationship between E_t and Heron triangles, it is necessary for us to determine exactly what torsion subgroups are possible and when they occur. We begin by proving:

Proposition 3.5. *For all $t \in \mathbb{Q}^*$, $E_t(\mathbb{Q})$ does not contain a point of order 3.*

Proof. Suppose $(u, v) \in E_t(\mathbb{Q})$ for some $t \in \mathbb{Q}^*$. If we let ψ_3 be the three division polynomial for E_t , then

$$\psi_3(u, t) = 3u^4 + 4(t^2 + 2)u^3 + 6u^2 - 1.$$

Recall that $(u, v) \in E_t(\mathbb{Q})$ is a point of order three if and only if $\psi_3(u, t) = 0$. Making the substitution $t = \tau(\sigma + 1)/(2\sigma)$, $u = 1/\sigma$ gives

$$\psi_3\left(\frac{1}{\sigma}, \tau \frac{\sigma + 1}{2\sigma}\right) = (\sigma + 1)^2 \frac{\tau^2 - \sigma(\sigma + 1)(\sigma - 3)}{\sigma^5}.$$

Since the only rational points on the curve $\tau^2 = \sigma(\sigma + 1)(\sigma - 3)$ are the three points of order 2, $\psi_3(u, t)$ vanishes for rational u and t only when $t = 0$. Hence, we have the statement of the proposition. \square

We also have that:

Proposition 3.6. *For all $t \in \mathbb{Q}^*$, $(-1, t) \notin 2E_t(\mathbb{Q})$. In particular, the torsion subgroup of $E_t(\mathbb{Q})$ can never be equal to $\mathbb{Z}/8\mathbb{Z}$.*

Proof. If $P \in E_t(\mathbb{Q})$, then the x -coordinate of $2P$ is $[(x^2 - 1)/(2y)]^2$. Therefore, the x -coordinate of $2P$ can never be negative. \square

And finally, we prove:

Theorem 3.7. *For all $t \in \mathbb{Q}^*$, the only possible torsion subgroups of $E_t(\mathbb{Q})$ are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and they each occur. In particular, if we let \mathbb{T} be the torsion subgroup of $E_t(\mathbb{Q})$, then we have:*

1. $\mathbb{T} = G_t = \mathbb{Z}/4\mathbb{Z}$ if and only if $t^2 + 4$ is not a square.
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{T}$ if and only if $t^2 + 4$ is a square or equivalently

$$t = \frac{s^2 - 1}{s}, \text{ for some } s \in \mathbb{Q}^*, s \neq \pm 1.$$

If \mathbb{T} does contain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then

- a) the two additional points of order 2 are $(-s^2, 0)$ and $(-1/s^2, 0)$;
- b) the two additional points of order 4 are $(1, \pm(s^2 + 1)/s)$; and
- c) for each of the points of finite order, P , listed above,

$$\Phi_t(P) = [(2, b, b)], \text{ where } b = \left| \frac{s^2 + 1}{s^2 - 1} \right|.$$

3. $\mathbb{T} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if and only if $t = (s^2 - 1)/s$, where $s = (r^2 - 1)/(2r)$, or equivalently

$$t = \frac{r^4 - 6r^2 + 1}{2(r^3 - r)}, \text{ for some } r \in \mathbb{Q}^*, r \neq \pm 1.$$

If \mathbb{T} does equal $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then the points of order 8 are

$$\left\{ \pm P_8(\pm r), \pm P_8\left(\pm \frac{1}{r}\right) \right\} \text{ where } P_8(r) = \left(-\frac{r+1}{r(r-1)}, \frac{(r^2+1)(r^2-2r-1)}{2r^2(r-1)^2} \right).$$

Proof. The discriminant of $u^2 + (t^2 + 2)u + 1$ is $t^2(t^2 + 4)$ and hence $u^2 + (t^2 + 2)u + 1$ factors if and only if $t^2 + 4$ is a square. The rational solutions to $t^2 + 4$ equal a square can be parameterized by $t = (s^2 - 1)/s$, $s \in \mathbb{Q}^*$. Computing $\varphi_t(P)$ for each of the new points of finite order in $E_t(\mathbb{Q})$ when $t = (s^2 - 1)/s$ completes the proof of the first and second parts of the theorem.

Since $(-1, t) \notin 2E_t(\mathbb{Q})$ for any $t \in \mathbb{Q}^*$, if $E_t(\mathbb{Q})$ is going to contain a point of order 8, it must be the case that $(1, (s^2 + 1)/s) \in 2E_t(\mathbb{Q})$. Computing $2(u, v)$ and setting this equal to $(1, (s^2 + 1)/s)$ give us the remainder of the theorem. \square

Remark 3.8. As stated in the previous section, we denote the curves E_t with $t = (s^2 - 1)/s$ as $E_{t(s)}$ and the curves E_t with $s = (r^2 - 1)/(2r)$ as $E_{t(s(r))}$.

Remark 3.9. Observe that if n is a positive integer and $\langle a, b, b \rangle$ is an isosceles Heron triangle with area $2n$, then the right triangle with base $a/2$ and hypotenuse b is a right Heron triangle with area n . By part 2 of Theorem 3.7, we then have:

Corollary 3.10. A positive integer n is a congruent number if and only if there exists a positive $h \in \mathbb{Q}$ such that for $t = n/h^2$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq E_t(\mathbb{Q})$.

Note that this does not provide a more convenient way to determine if n is a congruent number, but rather is a reformulation of the standard theorem stating that n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ has rational rank at least 1.

Since there is no loss of generality in assuming that $a = 2$, we do so for the remainder of this paper. This fixes the two vertices at the base of the Heron triangle pictured in Figure 1 to be $(-1, 0)$ and $(1, 0)$. Both the primary altitude and area of this triangle are then $2/t$.

Remark 3.11. We conclude this section by pointing out that the results regarding the torsion subgroup of $E_t(\mathbb{Q})$ can be deduced from the (independent) work of Rusin [19]. Rusin studied the curve $R_{A,a} : y^2 = (x + A^2 + 2a^4)(x^2 - 4a^4(A^2 + a^4))$. The curve $R_{A,a}$ is derived from *Heron's formula*,

$$16A^2 = (a + b + c)(-a + b + c)(a - b + c)(a + b - c),$$

which relates the area, A , of a triangle to the length of its sides a, b, c . Fixing A and a in Heron's formula gives a curve isomorphic to $R_{A,a}$ which in turn is a (-1) -twist of (and 4-isogenous to) the curve $E_{t'}$, where $t' = 2a^2/A$. What is completely new is how this curve is related to other interesting Diophantine problems (beyond simply Heron triangles) and how this curve can be used to create elliptic curves of large rank with non-trivial torsion subgroups.

4. Points at Rational Distance.

It is clear that there are dense sets of points at rational distance on a line and Euler proved that there exist dense sets of points at rational distance on a circle. It is, however, a long standing open problem [14] whether or not there are more than six points in the plane with no three collinear and no four concyclic. All infinite sets of points at rational distance contain all but finitely many on a line or on a circle. By using the method described above for producing isosceles Heron triangles, we are able to produce another example of such an infinite set of points at rational distance. The example we produce consists of an infinite set of points on a line together with four points off that line. This example distinguishes itself from previously known examples in that the four "off-line" points contain no three which are collinear.

By Theorem 3.7, if $t = (s^2 - 1)/s$, then $E_t = E_{t(s)}$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and hence $\langle 2, b, b \rangle$, with $b = (s^2 + 1)/(s^2 - 1)$ is an isosceles Heron triangle with primary altitude $2s/(s^2 - 1)$. Therefore, we have:

Theorem 4.1. *If we let $h = 2s/(s^2 - 1)$ and $x_{u,v} = \frac{(u-1)vh}{2u(u+1)}$, then the set:*

$$\{(x_{u,v}, h) \mid (u, v) \in E_{t(s)}(\mathbb{Q}) - G_t\} \cup \{(\pm 1, 0), (\pm 1, 2h)\}$$

is a set of points at rational distance. This set is infinite if and only if $E_{t(s)}(\mathbb{Q})$ has positive rank.

Proof. All the points in the set lie on the three parallel lines $y = 0$, $y = h$, $y = 2h$. By the rationality of the coordinates of all the points and by symmetry, we need only verify that points on the line $y = h$ are at rational distance to the points $(\pm 1, 0)$ and that the distance between $(1, 0)$ and $(-1, 2h)$ is rational. The latter is easily verified by computing the distance or observing that by part 2 of Theorem 3.7, the triangle with vertices $(-1, 0)$, $(1, 0)$ and $(0, h)$ is necessarily a Heron triangle. The distances from point $(x_{u,v}, h)$ to $(-1, 0)$ and to $(1, 0)$ are rational since the points $(-1, 0)$, $(1, 0)$, $(x_{u,v}, h)$ determine a Heron triangle by Theorem 3.1. \square

To produce specific examples of *infinite* sets of this form, we need only find an s such that $E_{t(s)}(\mathbb{Q})$ contains at least one point of infinite order. For example, we have that $E_{t(s)}$ where $s = 9$ has rank 1 with $P = (169, 24050/9)$ being a point of infinite order.

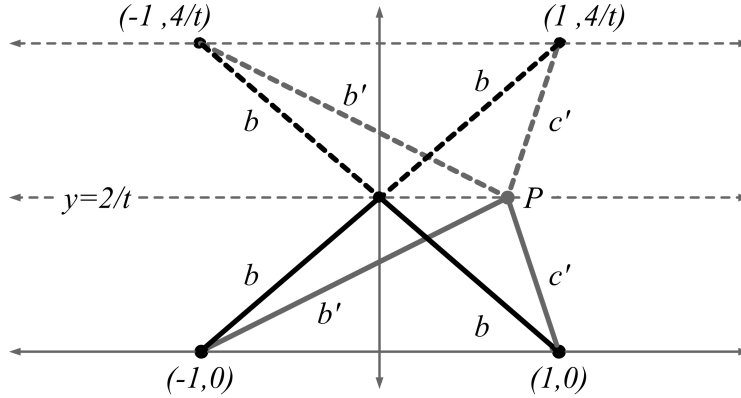


FIGURE 2. In the figure above, $t = (s^2 - 1)/s$ and so $b = (s^2 + 1)/(s^2 - 1)$. Also P comes from a point on $E_{t(s)}$ so that $\langle 2, b', c' \rangle$ is a Heron triangle. Therefore, all the distances between points are rational.

We can even produce infinitely many examples related to this one. The equation defining the curve $E_{t(s)}$ is

$$(4.1) \quad v^2 = u^3 + \left(\frac{s^4 + 1}{s^2} \right) u^2 + u.$$

If we set $u = k^2$ in this equation, we get the relation

$$v^2 = \frac{k^2(k^2 + s^2)(1 + k^2 s^2)}{s^2}.$$

Now suppose we let F_k be the curve defined by $F_k : \omega^2 = (k^2 + \mu^2)(1 + k^2 \mu^2)$. For each $k \in \mathbb{Q}^*, k \neq \pm 1$, F_k is an elliptic curve (if we consider this the affine piece of the intersection of two quadrics in \mathbb{P}^3). Hence, for each $k \in \mathbb{Q}^*, k \neq \pm 1$ for which $F_k(\mathbb{Q})$ has positive rank, there are infinitely many s such that $E_{t(s)}$ has a rational point with $u = k^2$. Therefore, for each such k , there are infinitely many isosceles Heron triangles and infinitely many sets of points at rational distance of the form given by Theorem 4.1. This is the case for $k = 13$, for example.

Less complicated than the construction above, we have the following proposition which also yields an infinity of examples:

Proposition 4.2. *If $s = -(2m + 1)/(m^2 - 1)$, then for any $m \in \mathbb{Q}^*, m \neq \pm 1, -1/2, -2$, $E_{t(s)}(\mathbb{Q})$ contains the point of infinite order:*

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

In particular, there are infinitely many s such that $E_{t(s)}(\mathbb{Q})$ has positive rank.

Proof. If we set $u = s$ in the equation 4.1 defining $E_{t(s)}$, then we have

$$v^2 = (s + 1)^2(s^2 - s + 1).$$

The rational points satisfying $\omega^2 = s^2 - s + 1$ are parameterized by $s = -(2m + 1)/(m^2 - 1)$, $m \in \mathbb{Q}$, $m \neq \pm 1$. Observing that $s \in \{0, \pm 1\}$ if and only if $m \in \{-1/2, -2\}$, we get the result. \square

Remark 4.3. This example forms the basis for producing an infinite family of elliptic curves of rank 1 with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and so we will revisit this curve in the last section of the paper.

We now turn our attention to the problem of finding four rational points on the parabola $y = x^2$ at rational distance. This problem seemingly has nothing at all to do with Heron triangles, but we will show that in fact the two Diophantine problems are intimately related. The first indications that there should be a connection are the following:

Proposition 4.4. *The triangle whose vertices $P_i = (x_i, x_i^2)$ are on the parabola $y = x^2$ has rational area if and only if $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ is rational.*

Proof. Using Heron's formula, we see that the area of such a triangle is $2(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. \square

This immediately gives us:

Corollary 4.5. *If $\{P_i \mid i = 1, 2, 3\}$ is a set of rational points on $y = x^2$ at rational distance, then the triangle with these points as vertices is a Heron triangle.*

Now consider the rational points $P_i = (x_i, x_i^2)$, $1 \leq i \leq 4$ on $y = x^2$. The distance between each pair is given by $(x_i - x_j)\sqrt{1 + (x_i + x_j)^2}$. If we parameterize the rational solutions to $1 + (x_i + x_j)^2$ equal a square for each $1 \leq i < j \leq 4$, then we see that we must have

$$x_i + x_j = g(m_{ij}) = \frac{m_{ij}^2 - 1}{2m_{ij}}, m_{ij} \in \mathbb{Q}^*.$$

This gives a linear system of six equations in the four unknowns x_i . The system is consistent if and only if one can find values of $m_{ij} \in \mathbb{Q}^*$ such that

$$(4.2) \quad g(m_{12}) + g(m_{34}) = g(m_{13}) + g(m_{24}) = g(m_{14}) + g(m_{23}).$$

Therefore, we consider the curve E'_t defined by $g(x) + g(y) = t$ and observe that this curve is an elliptic curve for all $t \in \mathbb{Q}^*$. The statement above is then equivalent to the following proposition.

Proposition 4.6. *Each triple of points $(m_{12}, m_{34}), (m_{13}, m_{24}), (m_{14}, m_{23})$ in $E'_t(\mathbb{Q})$ satisfying $m_{ij} \neq 0$ for all $1 \leq i < j \leq 4$ corresponds to a set of four points on the parabola $y = x^2$ at rational distance.*

The critical fact which connects this problem with Heron triangles to an even greater extent is the following:

Proposition 4.7. *For all $t \in \mathbb{Q}^*$, E'_t is isomorphic over \mathbb{Q} to E_t .*

Therefore, we have that four points at rational distance on $y = x^2$ correspond to a triple of points in $E_t(\mathbb{Q})$. Note that without some extra conditions on the triple of points, the four points on the parabola are not guaranteed to be distinct or non-concyclic. In order to guarantee this, a technical condition on the triple of points in $E_t(\mathbb{Q})$ must be met. This condition, presented and proved in [3], is equivalent to:

Theorem 4.8. *Let $t \in \mathbb{Q}^+$ be fixed and suppose $P_1, P_2, P_3 \in E_t(\mathbb{Q})$. (P_1, P_2, P_3) corresponds to a set of four distinct, non-concyclic points at rational points at rational distance on $y = x^2$ if and only if*

1. *For all $i = 1, 2, 3$, $P_i \notin G_t$.*
2. *For all $1 \leq i < j \leq 3$, $P_i \notin \{\pm P_j + Q \mid Q \in G_t\}$.*

By Remark 3.4 and the work in previous sections, this immediately gives us:

Theorem 4.9. *Every triple of Heron triangles of equal area possessing one side in common corresponds to a quadruple of non-concyclic rational points at rational distance on the parabola $y = x^2$.*

5. Heron Triangles and Diophantine Triples.

Recall that a *rational Diophantine m -tuple* is a set of nonzero rational numbers, $\{a_1, a_2, \dots, a_m\}$, such that $a_i a_j + 1$ is a square for all $1 \leq i < j \leq m$. Suppose $\{\alpha, \beta, \gamma\}$ is a rational Diophantine triple and observe that if $\{\alpha, \beta, \gamma, X_0\}$ is a rational Diophantine quadruple, then there must be some Y_0 such that (X_0, Y_0) is a rational point on the curve

$$D_{\alpha, \beta, \gamma} : Y^2 = (\alpha X + 1)(\beta X + 1)(\gamma X + 1).$$

This condition is necessary, but not sufficient to guarantee that $\{\alpha, \beta, \gamma, X_0\}$ is a Diophantine quadruple. Before we can write down a sufficient condition, we collect a few observations (see [8] for example).

First, since α, β and γ are distinct and nonzero, $D_{\alpha, \beta, \gamma}$ is an elliptic curve. For any $T \in D_{\alpha, \beta, \gamma}(\mathbb{Q})$, let $\chi(T)$ be the X -coordinate of T . Then, in addition to the three rational points of order 2, this curve contains the rational points $\pm P$ with $\chi(\pm P) = 0$, the rational points $\pm S$ with $\chi(\pm S) = 1/(\alpha\beta\gamma)$ and the rational points $\pm R$ such that $S = 2R$. Finally, we have the following two theorems of Dujella [9]:

Theorem 5.1. *If $T \in D_{\alpha, \beta, \gamma}(\mathbb{Q})$, then $\{\alpha, \beta, \gamma, \chi(T)\}$ is a rational Diophantine quadruple if and only if $T \in P + 2D_{\alpha, \beta, \gamma}(\mathbb{Q})$ and $\chi(T) \notin \{0, \alpha, \beta, \gamma\}$.*

Theorem 5.2. *If $T \in D_{\alpha, \beta, \gamma}(\mathbb{Q})$ and $\{\alpha, \beta, \gamma, \chi(T)\}$ is a rational Diophantine quadruple, then $\{\alpha, \beta, \gamma, \chi(T), \chi(T + S)\}$ and $\{\alpha, \beta, \gamma, \chi(T), \chi(T - S)\}$ are rational Diophantine quintuples, provided $\chi(T \pm S) \notin \{0, \alpha, \beta, \gamma, \chi(T)\}$.*

Remark 5.3. If we let $\delta_- = \chi(P - S)$ and $\delta_+ = \chi(P + S)$, then since $S = 2R$, Theorem 5.1 gives us that $\{\alpha, \beta, \gamma, \delta_+\}$ and $\{\alpha, \beta, \gamma, \delta_-\}$ are Diophantine quadruples whenever δ_+ and δ_- are not in $\{0, \alpha, \beta, \gamma\}$.

Now, consider the elliptic curve E_t . We claim that for specific rational values of t, α, β and γ , E_t will be isomorphic to $D_{\alpha, \beta, \gamma}$. Since $D_{\alpha, \beta, \gamma}(\mathbb{Q})$ always contains the subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E_t(\mathbb{Q})$ always contains the subgroup $\mathbb{Z}/4\mathbb{Z}$, if $E_t \cong D_{\alpha, \beta, \gamma}$, it must be the case that $D_{\alpha, \beta, \gamma}(\mathbb{Q})$ contains the subgroup $\mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z}$ and that $t = (s^2 - 1)/s$ for some $s \in \mathbb{Q}^* s \neq \pm 1$ so that $E_t(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as well.

If we plug the value $X = (x - \alpha\beta)/(\alpha\beta\gamma)$ into the equation for $D_{\alpha, \beta, \gamma}$, then we see that $D_{\alpha, \beta, \gamma}$ is isomorphic to the curve $y^2 = x(x - (\alpha\beta - \alpha\gamma))(x - (\alpha\beta - \beta\gamma))$. If this curve is to be isomorphic to $E_{t(s)} : v^2 = u(u + 1/s^2)(u + s^2)$, then we must have $(\alpha\beta - \alpha\gamma) = -1/s^2$ and $(\alpha\beta - \beta\gamma) = -s^2$ for some $s \in \mathbb{Q}^*, s \neq \pm 1$. Solving

this system for β and γ , we see that these two equations are satisfied if and only if $(2\alpha s^3)^2 + (1 - \alpha^2 s^2)^2$ is a square. This is clearly true if $\alpha = \pm 1/s$. Consequently, we have:

Theorem 5.4. *If we let $\alpha = -1/s, \beta = s$ and $\gamma = (s^2 - 1)/s$, then*

1. $\{\alpha, \beta, \gamma\}$ is a rational Diophantine triple.
2. $E_{t(s)} = E_\gamma \cong D_{\alpha, \beta, \gamma}$.
3. $\delta_- = \delta_+ = 0$
4. $\{\alpha, \beta, \gamma\}$ can be extended to a rational Diophantine quadruple if and only if $E_\gamma(\mathbb{Q})$ has positive rank.
5. $\{\alpha, \beta, \gamma\}$ can be extended to a rational Diophantine quintuple if and only if $E_\gamma(\mathbb{Q})$ has positive rank.
6. Specific Heron triangles correspond to rational Diophantine quadruples and quintuples containing $\{\alpha, \beta, \gamma\}$.

Proof. Computations verify that:

$$\begin{aligned} \alpha\beta + 1 &= 0, & \alpha\gamma + 1 &= \frac{1}{s^2}, & \beta\gamma + 1 &= s^2, \\ (\alpha\beta - \alpha\gamma) &= -s^2 & \text{and} & & (\alpha\beta - \beta\gamma) &= -1/s^2. \end{aligned}$$

so that $\{\alpha, \beta, \gamma\}$ is indeed a rational Diophantine triple and $E_\gamma \cong D_{\alpha, \beta, \gamma}$.

From the equations defining the curve, we see that $\{\pm P\} = \{(0, \pm 1)\}$ and $S = (-1/\gamma, 0) = (s/(1 - s^2), 0)$. We observe that S is a point of order 2 and compute that $2P$ must equal S . Therefore, $\{P - S, P + S\} = \{\pm P\}$ so that $\chi(P - S) = \chi(P + S) = 0$. This proves that δ_- and δ_+ are each 0.

If $E_\gamma(\mathbb{Q})$ has rank 0, then either $E_\gamma(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ in which case $S \notin 4E_\gamma(\mathbb{Q})$ or $E_\gamma(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ in which case $S \in 4E_\gamma(\mathbb{Q})$. Now observe that in the former case, $2D_{\alpha, \beta, \gamma}(\mathbb{Q}) = \{S\}$ and in the latter, $2D_{\alpha, \beta, \gamma}(\mathbb{Q}) = \{S, \pm P, S \pm P\}$. A quick calculation shows that in both cases $\chi(P + 2D_{\alpha, \beta, \gamma}(\mathbb{Q})) \subseteq \{0, \alpha, \beta\}$. Therefore, we are not able to extend $\{\alpha, \beta, \gamma\}$ to a rational Diophantine quadruple if the rank of $E_\gamma(\mathbb{Q})$ is 0.

Conversely, if $E_\gamma(\mathbb{Q})$ has positive rank, then there are infinitely many $T \in P + 2D_{\alpha, \beta, \gamma}(\mathbb{Q})$ such that $\chi(T) \notin \{0, \alpha, \beta, \gamma\}$ and $\chi(T \pm S) \notin \{0, \alpha, \beta, \gamma, \chi(T)\}$. Hence, we get infinitely many ways to extend $\{-1/s, s, (s^2 - 1)/s\}$ to a rational Diophantine quadruple and then to a rational Diophantine quintuple.

Since we have $D_{\alpha, \beta, \gamma} \cong E_\gamma = E_{t(s)}$, by the work in previous sections, we clearly then have that specific Heron triangles correspond to rational Diophantine quadruples and quintuples containing $\{-1/s, s, (s^2 - 1)/s\}$. \square

6. Heron Triangles and Elliptic Curves of Large Rank.

One of the fundamental open questions regarding elliptic curves is whether or not the rank can be arbitrarily large, particularly if one fixes the torsion subgroup. While there are examples of elliptic curves with positive rank for each of the 15 possible subgroups, in many cases, the highest known rank for a given torsion subgroup remains quite low. One such torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. We define

$$B(\mathbb{T}) = \sup\{\text{rank}(E(\mathbb{Q})) \mid \text{the torsion subgroup of } E(\mathbb{Q}) = \mathbb{T}\}$$

and

$$G(\mathbb{T}) = \limsup\{\text{rank}(E(\mathbb{Q})) \mid \text{the torsion subgroup of } E(\mathbb{Q}) = \mathbb{T}\}.$$

It is known that $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}) \geq 3$ and $G(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}) \geq 1$. In particular, Dujella and Connell [5] found a curve with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank 3 and Dujella [12] alone found another rank 3 example. Atkin and Morain [1] found a family of rank 1 elliptic curves with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ parameterized by the rational points on the curve $A : \omega^2 = \mu^3 - 8\mu - 32$ and Kulesz [17] found a family of rank 1 elliptic curves with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ parameterized by the rational points on the curve $K : \omega^2 = \mu^3 + 4\mu^2 + 4\mu + 16$. Below, we describe curves which tie these records and suggest a few more which might in fact have higher rank.

Before we demonstrate this, we let $t(s) = (s^2 - 1)/s$, $s(r) = (r^2 - 1)/(2r)$ and observe that

$$(6.1) \quad t(s) = t\left(-\frac{1}{s}\right), \quad s(r) = s\left(-\frac{1}{r}\right), \quad s\left(\frac{r-1}{r+1}\right) = -\frac{1}{s(r)},$$

$$(6.2) \quad t(-s) = t\left(\frac{1}{s}\right) = -t(s) \quad \text{and} \quad s(-r) = s\left(\frac{1}{r}\right) = -s(r).$$

For any $r \in \mathbb{Q}^*$, $r \neq \pm 1$, we define $\mathcal{S}(r)$ to be the set

$$\mathcal{S}(r) = \left\{ \pm r, \pm \frac{1}{r}, \pm \frac{r-1}{r+1}, \pm \frac{r+1}{r-1} \right\}.$$

Equations 6.1 and 6.2 then give us:

Proposition 6.1. $E_{t(s(r))} \cong E_{t(s(r'))}$ for all $r' \in \mathcal{S}(r)$.

Furthermore, it has been shown that

Theorem 6.2. *Every elliptic curve defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is of the form $E_{t(s(r))}$.*

Remark 6.3. One of the easiest ways to prove this fact is to start with the curve $y^2 = x(x-a)(x-b)$ and to write out the condition for $(0,0)$ be the double of a rational point and then write out the condition for that point to be the double of a rational point. In so doing, one is quickly led to a curve isomorphic to $E_{t(s(r))}$. (We note that D. S. Kubert [15] appears to be the first to have parameterized elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.)

We also point out that while all curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ appear in the family $E_{t(s(r))}$, not all curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (or $\mathbb{Z}/4\mathbb{Z}$) appear in the family $E_{t(s)}$ (respectively, E_t).

Given the work in the previous sections, theorem 6.2 immediately implies:

Theorem 6.4. *Each elliptic curve defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ corresponds to a family of Heron triangles with fixed area and side.*

Now observe that $r = \sqrt{2} - 1$ is the unique positive fixed point of the map $r \mapsto -\frac{r-1}{r+1}$ so that combining proposition 6.1 and theorem 6.2 gives us:

Theorem 6.5. *All elliptic curves defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ are of the form $E_{t(s(r))}$ with $0 < r < \sqrt{2} - 1$ and no two such curves are isomorphic over \mathbb{Q} .*

Therefore, every elliptic curve defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is completely defined by a value of r in the range 0 to $\sqrt{2} - 1$. For

example, if $r = 5/29$ we get the curve of rank 3 found by Dujella and Connell, if $r = 18/47$ we get the the curve of rank 3 found by Dujella and

Theorem 6.6. *If $r = 15/76$, then $E_{t(s(r))}$ has rank 3.*

Proof. A set of generators for $E_{t(s(15/76))}(\mathbb{Q})$ is given by the points whose u -coordinates are:

$$\begin{aligned} u_1 &= 586170317475288 \\ u_2 &= 323450989778280 \\ u_3 &= -\frac{174847681183843106579796800202465935023440}{2155454372702562136437503569}. \end{aligned}$$

□

Using Cremona's *mwrank* [6], we conducted a search for elliptic curves, $E_{t(s(r))}$, whose group of rational points have rank larger than 3. We found no such curves for values of r satisfying $0 < r < \sqrt{2} - 1$ and denominator less than or equal to 100. In many cases, *mwrank* was not able to definitively determine the rank. In these cases bounds based on the rank of the Selmer group and the number of independent points found on the curve combined with a computation of the sign of the functional equation allowed us to determine that no curves with values of r in this range have rank larger than 4, but there are some which (assuming the Parity Conjecture) have rank 2 or 4.

We now return to the infinite family of curves described in proposition 4.2. This family is given by $E_{t(s)}$ where $s = -(2m+1)/(m^2-1)$, $m \in \mathbb{Q}^*$, $m \neq \pm 1, -1/2, -2$ and contains a point of infinite order given by $u = s$. If we want this curve to have torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then we must have $s = (r^2-1)/(2r)$ for some $r \in \mathbb{Q}^*$, $r \neq \pm 1$. Setting

$$(6.3) \quad -\frac{2m+1}{m^2-1} = \frac{r^2-1}{2r}$$

we see that r must be a root of a quadratic polynomial with discriminant $m^4 + 2m^2 + 4m + 2$. Hence, we let H be the curve defined by $H : n^2 = m^4 + 2m^2 + 4m + 2$ (or more accurately, the smooth curve in projective 3-space for which this is an affine model) and prove:

Proposition 6.7. *H is an elliptic curve defined over \mathbb{Q} and $H(\mathbb{Q})$ has positive rank.*

Proof. A brief search finds more than 16 rational points. □

Remark 6.8. Though not particularly germane to the discussion, we note that while the rational torsion subgroups of A and K are $\mathbb{Z}/2\mathbb{Z}$, the rational torsion subgroup of H is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now, for each point in $H(\mathbb{Q})$, we can solve equation 6.3 for r . Since, we want to avoid values of r in $\{0, \pm 1\}$, we get the following theorem:

Theorem 6.9. *For each point (m, n) in $H(\mathbb{Q})$, $n > 0$, $m \neq \pm 1, -1/2$, the elliptic curve $E_{t(s(r))}$ with*

$$r = \frac{n - 2m - 1}{m^2 - 1}$$

contains the point of infinite order with u -coordinate $-(2m + 1)/(m^2 - 1)$.

This gives an infinite family of elliptic curves defined over \mathbb{Q} with rational torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and positive rank parameterized by the rational points on $H : n^2 = m^4 + 2m^2 + 4m + 2$.

Remark 6.10. We were recently informed of two infinite families of curves found by Odile Lecacheux also containing rational torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Upon corresponding with Lecacheux, we have verified that the two families found by her and the family described above, each found independently (using different techniques) over the last year, are in fact the same family.

Acknowledgements

Calculations were performed using a variety of packages: *GP/Pari* [2], *MAGMA* [4], *Mathematica* [22] and *mwrank* [6].

We would like to thank John Cremona for his great help with *mwrank* and his several suggestions for how to resolve certain computational issues in computing ranks of elliptic curves with very large coefficients. We would also like to thank Andrej Dujella for his thoughtful comments on a draft of this paper and for his facilitating conversations between us and Lecacheux.

References

1. A. O. L. Atkin and F. Morain. *Finding Suitable Curves for the Elliptic Curve Method of Factorization*, Math. Comp. **60** (1993), no. 201 399–405, MR1140645 , Zbl 0815.11063.
2. C. Batut and K. Belabas and D. Benardi and H. Cohen and M. Olivier. *User's Guide to PARI-GP*, <ftp://megrez.math.u-bordeaux.fr/pub/pari>, 1998. (See also <http://pari.home.ml.org>.)
3. Garikai Campbell. *Points on $y = x^2$ at rational distance*, Math. Comp. to appear, 2004.
4. Computational Algebra Group. *MAGMA*, University of Sydney <http://magma.maths.usyd.edu.au/magma/>, 2002.
5. Ian Connell and Andrej Dujella. <http://www.math.hr/duje/tors/z2z8.html>, 2000.
6. John Cremona. *mwrank*, <http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/>, 2002.
7. Nathaniel Dean. *Personal communication*. Rice University, 2001.
8. Andrej Dujella. *Diophantine m -tuples and elliptic curves*, *J. Theor. Nombres Bordeaux*. **13** (2001) 111–124, MR1838074.
9. Andrej Dujella. *On Diophantine quintuples*, *Acta Arith.* **81** (1997) 69–79, MR1454157, Zbl 0871.11019 .
10. Andrej Dujella. *High rank elliptic curves with prescribed torsion*, <http://www.math.hr/duje/tors/tors.html>, 2002.
11. Andrej Dujella. *Infinite families of elliptic curves with high rank and prescribed torsion*, <http://www.math.hr/duje/tors/generic.html>, 2002.
12. Andrej Dujella. <http://www.math.hr/duje/tors/z2z8.html>, 2001.
13. N. J. Fine. *On rational triangles*, *American Mathematical Monthly*. **83**, no. 7 (1976) 517–521, MR0414484, Zbl 0341.10016.
14. Richard K. Guy. *Unsolved Problems in Number Theory, Second Edition*, Springer-Verlag, 1994, MR1299330 ,Zbl 0805.11001.
15. D. S. Kubert. *Universal bounds on the torsion of elliptic curves*, *Proc. London Math. Soc.* **33** (1976) 193–237, MR0434947, Zbl 0331.14010 .
16. Leopoldo Kulesz. *Families of elliptic curves of high rank with nontrivial torsion group over \mathbb{Q}* , *Acta Arith.* **108** (2003) 339–356, MR1979903, Zbl pre01927511.
17. Leopoldo Kulesz. *Arithmetique des courbes algebriques de genre au moins deux*, These de doctorat, Universite Paris 7, 1998.
18. Odile Lecacheux. *Personal communication*, Universite Pierre et Marie Curie, July, 2003.

19. David Rusin. *Rational triangles with equal area*, New York Journal of Mathematics. **4** (1998) 1–15, MR1489407, Zbl 0893.11009.
20. Joseph Silverman. *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986, MR0817210, Zbl 0585.14026.
21. J. B. Tunnell. *A classical Diophantine problem and modular forms of weight*, Inventiones Math. **72** (1983) 323–334, MR0700775, Zbl 0515.10013 .
22. Wolfram Research, Inc. *Mathematica*, Version 4.2. Wolfram Research, Inc. Champaign, IL. 1999.

DEPARTMENT OF MATHEMATICS AND STATISTICS, SWARTHMORE COLLEGE, SWARTHMORE, PA
19081
kai@swarthmore.edu

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, MAIL CODE: 253-
37, PASADENA, CA 91125
goins@caltech.edu