

POINTS ON $y = x^2$ AT RATIONAL DISTANCE

GARIKAI CAMPBELL

ABSTRACT. Nathaniel Dean asks the following: Is it possible to find four non-concyclic points on the parabola $y = x^2$ such that each of the six distances between pairs of points is rational? We demonstrate that there is a correspondence between all *rational* points satisfying this condition and orbits under a particular group action of rational points on a fiber product of (three copies of) an elliptic surface. In doing so, we provide a detailed description of the correspondence, the group action and the group structure of the elliptic curves making up the (good) fibers of the surface. We find for example that each elliptic curve must contain a point of order 4. The main result is that there are infinitely many rational distance sets of four nonconcyclic (rational) points on $y = x^2$. We begin by giving a brief history of the problem and by placing the problem in the context of a more general, long-standing open problem. We conclude by giving several examples of solutions to the problem and by offering some suggestions for further work.

1. A BRIEF HISTORY OF THE PROBLEM

We say that a collection of points in $S \subset \mathbb{R}^n$ is *at rational distance* if the distance between each pair of points is rational. We will call such a collection of points a *rational distance set*. For example, the rationals themselves form a rational distance subset of the reals. Therefore, if S is any line in \mathbb{R}^n , S contains a dense set of points at rational distance.

Furthermore, it was known to Euler that

Proposition 1.1. *Every circle contains a dense set of points at rational distance.*

Remark 1.2. Several proofs of this exist (see [1] for example). We follow the ideas articulated in [7].

Proof. To make the writing of the argument a bit cleaner, we identify \mathbb{R}^2 with the complex plane in the usual manner. Now observe that if two points in the complex plane, z and w , are at rational distance *and have rational length*, then since

$$\left\| \frac{1}{z} - \frac{1}{w} \right\| = \frac{\|z - w\|}{\|z\| \cdot \|w\|},$$

$1/z$ and $1/w$ are at rational distance as well. Now, consider a vertical line L . One can easily parameterize all points on L whose lengths and imaginary parts

Received by the editor January 7, 2003 and, in revised form, February 4, 2003.

2000 *Mathematics Subject Classification.* Primary 14G05, 11G05, 11D25.

Key words and phrases. Rational distance sets, elliptic curves, elliptic surfaces.

This work was supported by the Swarthmore College Lang Grant and the Woodrow Wilson Career Enhancement Fellowship.

are rational (see Lemma 2.1 below). This set of points is dense in L and as long as L is not the imaginary axis, this set of points is mapped by the complex map $f(z) = 1/z$ to a dense, rational distance subset of a circle. As L moves through all vertical lines, we get circles of all radii. \square

So what can be said about rational distance subsets of sets other than circles and lines? This is the nature of the question posed by Nathaniel Dean [6]. We will say that points in a plane are *concylic* if they lie on a circle. Given Proposition 1.1 and the observation prior, it seems plausible that if we allow concyclic or collinear points, the problem of finding rational distance subsets is made a bit easier. This motivates adding to such questions the requirement that no three points be collinear and no four points be concyclic. Therefore Dean asks

Question 1.3. *What is the largest possible rational distance subset of points on $y = x^2$ with no four of the points concyclic?*

Note that since the (non)collinearity condition is always met in this case, we simply omit it. We also point out that this question is a new twist to an older, more general question:

Question 1.4. *What is the largest possible rational distance subset of points in the plane with no three of the points collinear and no four of the points concyclic?*

Not only is this more general question an open problem, but the best known result to date is (see [10])

Theorem 1.5. *There exist infinitely many rational distance sets of six points in the plane with no three collinear and no four concyclic.*

For a detailed summary of this problem, we encourage the reader to see [7]. The current state of Question 1.4 suggests that it might be quite difficult to produce even small sized rational distance sets on the parabola. With this in mind, we begin by proving

Proposition 1.6. *There are infinitely many rational distance sets of three points on the parabola $y = x^2$.*

Dean himself gives an excellent proof of this fact. We follow his idea below.

Proof. Let S be the set of points on the parabola $y = x^2$ and let d_1 and d_2 be two fixed rational values. For any point, $P_0(r) = (r, r^2) \in S$, let $C_1(r)$ be the circle of radius d_1 centered at $P_0(r)$ and let $C_2(r)$ be the circle of radius d_2 centered at $P_0(r)$. Each of these circles must intersect S in at least one point. Let $P_1(r)$ be any point in $C_1(r) \cap S$ and likewise, let $P_2(r)$ be any point in $C_2(r) \cap S$. Now let $\text{dist}(r)$ equal the distance between $P_1(r)$ and $P_2(r)$. The function $\text{dist}(r)$ is a continuous function of r and hence there are infinitely many values of r such that $P_0(r)$, $P_1(r)$ and $P_2(r)$ are at rational distance. \square

Remark 1.7. Observe that Dean's proof actually shows that the collection of three tuples of points on $y = x^2$ at rational distance is dense in S . By this we mean that there is a rational distance set of three points on $y = x^2$ arbitrarily close to any three points on this parabola. Moreover, this argument can easily be generalized to any conic.

The main goal of this paper is to extend Dean's result by proving

Theorem 1.8. *There are infinitely many nonconcylic rational distance sets of four points on $y = x^2$.*

In earlier work, we recognized that points on an elliptic curve give rise to four rational points with all but one of the distances rational. Allan MacLeod [9] improved on this by considering a different elliptic curve. He too found four rational points with all but one of the distances rational and then did a search to find which of these sets had all points at rational distance. To our knowledge he was among the first to produce numerical examples of such 4-tuples. The elliptic curve considered by MacLeod is at the core of the work presented here.

We also hope to convince the reader that even if we remove the nonconcylic condition from Question 1.3, it remains an interesting (and nontrivial) question.

2. GENERAL SETUP

If we let P_i denote the point on the parabola $y = x^2$ with x -coordinate x_i and let d_{ij} denote the distance between P_i and P_j , then we have

$$(2.1) \quad d_{ij} = (x_i - x_j)^2 \cdot (1 + (x_i + x_j)^2).$$

If we assume that each P_i is a rational point, then the d_{ij} are rational precisely when there are rational solutions to

$$(2.2) \quad \delta_{ij} = 1 + (x_i + x_j)^2.$$

Now, consider the following lemma, which follows immediately from the standard parameterization of rational points on the unit circle:

Lemma 2.1. *The (affine) rational solutions to*

$$(2.3) \quad \alpha^2 = 1 + \beta^2$$

can be parameterized by $\alpha = \frac{m^2 + 1}{2m}$, $\beta = \frac{m^2 - 1}{2m}$, $m \in \mathbb{Q}$, $m \neq 0$.

Proof. Rational points on $(\alpha')^2 + (\beta')^2 = 1$ are parameterized by lines of rational slope, m , through the point and $(0, 1)$. Taking $\alpha = 1/\alpha'$ and $\beta = \beta'/\alpha'$, we get the parameterization of the proposition. \square

Letting $g(m) = \frac{m^2 - 1}{2m}$, Lemma 2.1 immediately implies

Proposition 2.2. *Suppose P_1, P_2, P_3 and P_4 are rational points on $y = x^2$. The set $\{P_1, P_2, P_3, P_4\}$ is a rational distance set if and only if for each $1 \leq i < j \leq 4$, we can find a nonzero rational value m_{ij} such that*

$$(2.4) \quad x_i + x_j = g(m_{ij}).$$

In subsequent sections, it will be convenient to speak of m_{ij} even when $i > j$. Therefore, we set m_{ij} equal to m_{ji} whenever $i > j$.

We point out that $g(m)$ has the following properties:

$$\begin{aligned} g(m) &= g(-1/m), \\ g(-m) &= -g(m), \\ g\left(\frac{m-1}{m+1}\right) &= -1/g(m) \quad \text{which implies} \\ g\left(g\left(\frac{m-1}{m+1}\right)\right) &= g(-1/g(m)) = g(g(m)). \end{aligned}$$

These properties will prove to be relevant later in the discussion.

A reduced echelon form of a matrix representing the system (2.4) is

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & \frac{1}{2}(g(m_{12}) + g(m_{13}) - g(m_{23})) \\ 0 & 1 & 0 & 0 & \frac{1}{2}(g(m_{12}) - g(m_{13}) + g(m_{23})) \\ 0 & 0 & 1 & 0 & \frac{1}{2}(-g(m_{12}) + g(m_{13}) + g(m_{23})) \\ 0 & 0 & 0 & 1 & \frac{1}{2}(-g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{14})) \\ 0 & 0 & 0 & 0 & g(m_{13}) + g(m_{24}) - g(m_{23}) - g(m_{14}) \\ 0 & 0 & 0 & 0 & g(m_{12}) + g(m_{34}) - g(m_{23}) - g(m_{14}) \end{bmatrix}.$$

Now we have

Theorem 2.3. *Suppose P_1, P_2, P_3 and P_4 are rational points on $y = x^2$. The set $\{P_1, P_2, P_3, P_4\}$ is a rational distance set if and only if there are rational values m_{ij} , $1 \leq i < j \leq 4$, such that*

$$(2.5) \quad \begin{aligned} x_1 &= \frac{g(m_{12}) + g(m_{13}) - g(m_{23})}{2}, \\ x_2 &= \frac{g(m_{12}) - g(m_{13}) + g(m_{23})}{2}, \\ x_3 &= \frac{-g(m_{12}) + g(m_{13}) + g(m_{23})}{2}, \\ x_4 &= \frac{-g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{14})}{2}, \end{aligned}$$

and

$$(2.6) \quad g(m_{13}) + g(m_{24}) = g(m_{23}) + g(m_{14}) = g(m_{12}) + g(m_{34}).$$

We are now ready to divide the problem into two cases. First, we consider the case in which the four points are concyclic.

3. CONCYCLIC SUBSETS OF FOUR POINTS

The proposition below describes precisely when four points on the parabola are concyclic:

Proposition 3.1. *The four rational points $P_i = (x_i, x_i^2)$, $i = 1, 2, 3, 4$, are concyclic if and only if $x_1 + x_2 + x_3 + x_4 = 0$.*

Proof. Let $C_{\alpha, \beta, \rho}$ be the circle $(x - \alpha)^2 + (y - \beta)^2 = \rho^2$, where $\alpha, \beta, \rho \in \mathbb{R}$. This circle intersects $y = x^2$ at the points whose x -coordinates are the roots of $(x - \alpha)^2 + (x^2 - \beta)^2 - \rho^2$ or equivalently $x^4 - (2\beta - 1)x^2 - 2\alpha x - (\rho^2 - \alpha^2 - \beta^2)$. Since the coefficient of x^3 in this polynomial is 0, the roots must sum to 0.

Conversely, given four values, x_i , $i = 1, 2, 3, 4$, such that $x_1 + x_2 + x_3 + x_4 = 0$, one can solve

$$\prod_{i=1}^4 (x - x_i) = x^4 - (2\beta - 1)x^2 - 2\alpha x - (\rho^2 - \alpha^2 - \beta^2)$$

for α, β , and ρ . □

Theorem 3.2. *Suppose P_1, P_2, P_3 and P_4 are rational and concyclic. These points are at rational distance if and only if there are nonzero rational values m_{12}, m_{13} and m_{23} such that the first three equations of (2.5) hold. When this is the case, x_4 must equal $\frac{-g(m_{12}) - g(m_{13}) - g(m_{23})}{2}$. Furthermore, the points are distinct if and only if the $g(m_{ij})$ are distinct.*

Proof. By Proposition 3.1, $x_4 = -x_1 - x_2 - x_3$. Therefore, for each $i = 1, 2, 3$, $x_i + x_4 = g(m_{i4})$ can be rewritten as $x_j + x_k = -g(m_{i4})$, where i, j, k and 4 are distinct. Since $g(m)$ is an odd function, this is equivalent to requiring $m_{i4} = -m_{jk}$. Plugging this into the equations of Theorem 2.3 gives us the first part of the theorem.

If $x_i = x_j$ for some $i \neq j$, then we are equating two of the equations in (2.5). Solving the resulting equation proves the last statement of this theorem. \square

Remark 3.3. Observe that if precisely one of the values $g(m_{ij})$ is 0, then the points are symmetric across the y -axis. In this case, we need not assume the points are rational. It is easy to show that when the points are symmetric about the y -axis, four points on $y = x^2$ at rational distance must be rational points.

Remark 3.4. We also point out that Theorem 3.2 implies that given *any* three rational points on the parabola $y = x^2$ at rational distance, the point whose x -coordinate is the negative of the sum of the x -coordinates of the other three points is necessarily at rational distance to those three. This implies that one strategy for attempting to get five points at rational distance is to first find four nonconcyclic points at rational distance and take the fifth point to be concyclic with some three of them. This would immediately give five points with all but one of the ten distances rational.

One example of five points on $y = x^2$ at rational distance was found while producing nonconcyclic sets of four points—the set of points with x -coordinates $\{0, \pm 91/60, \pm 209/120\}$. It may be possible to extend this to an infinite family of examples, but we have not yet been able to do so.

Our inability to completely describe the situation for five points (even if we allow some four of them to be concyclic) suggests that removing the concyclic condition from Question 1.3 does not render it trivial.

We now turn our attention to finding four nonconcyclic points on $y = x^2$ at rational distance.

4. NONCONCYCLIC SUBSETS OF FOUR POINTS

Recall that Theorem 2.3 and equations (2.6) in particular describe a necessary and sufficient condition for points to be at rational distance. The equations (2.6) determine a variety. In order to better understand this condition, we “projectivize” the variety and characterize the set of points in the projective variety that correspond to points at rational distance.

We begin by letting \mathcal{E} be the subvariety of $\mathbb{P}^2 \times \mathbb{P}^1$ defined by

$$\mathcal{E} : T_1 (Y(X^2 - Z^2) + X(Y^2 - Z^2)) = 2T_0XYZ.$$

Observe that \mathcal{E} is simply the “projective version” of $g(x) + g(y) = t$. Let π be the projection map

$$\pi : \mathcal{E} \longrightarrow \mathbb{P}^1 \text{ defined by } \pi([X, Y, Z], [T_0, T_1]) = [T_0, T_1].$$

This projection is a morphism of varieties such that $\pi^{-1}(T)$ is a curve. If $\pi^{-1}(T)$ is a nonsingular, smooth curve of genus 1, then we call the curve a *good fiber*. Otherwise, we call the curve a *bad fiber*. With these definitions, we have

Proposition 4.1. *The only bad fibers of \mathcal{E} are $\pi^{-1}([1, 0])$ and $\pi^{-1}([0, 1])$ and all good fibers are elliptic curves.*

Proof. We define \mathcal{E}' to be the variety

$$\mathcal{E}' : Y^2Z = X \cdot (X^2 + (T_0^4 + 2T_0^2T_1^2) XZ + T_0^4T_1^4 Z^2).$$

The map $\phi : \mathcal{E} \rightarrow \mathcal{E}'$ which sends

$$\begin{bmatrix} X \\ Y \\ Z \\ T_0 \\ T_1 \end{bmatrix} \mapsto \begin{bmatrix} -T_0^2 T_1^3 & -T_0^2 T_1^3 & 0 & 0 & 0 \\ T_0^4 T_1^3 & -T_0^4 T_1^3 & 0 & 0 & 0 \\ T_1 & T_1 & -2T_0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \\ Z \\ T_0 \\ T_1 \end{bmatrix}$$

is an isomorphism with inverse

$$\begin{bmatrix} X \\ Y \\ Z \\ T_0 \\ T_1 \end{bmatrix} \mapsto \begin{bmatrix} -T_0^2 & 1 & 0 & 0 & 0 \\ -T_0^2 & -1 & 0 & 0 & 0 \\ -T_0 T_1 & 0 & -T_0^3 T_1^3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \\ Z \\ T_0 \\ T_1 \end{bmatrix}.$$

If we similarly define $\pi' : \mathcal{E}' \rightarrow \mathbb{P}^1$ to be the projection onto its second factor, then the fibers $(\pi')^{-1}([T_0, T_1])$ are clearly elliptic curves except when the discriminant $\Delta = T_0^{14} \cdot T_1^8 \cdot (T_0^2 + 4T_1^2)$ is zero. Since the curves $\pi^{-1}([T_0, T_1])$ and $(\pi')^{-1}([T_0, T_1])$ are isomorphic, this proves the theorem. \square

Remark 4.2. We will refer to the curve $\pi^{-1}([t, 1])$ as E_t and to the curve $\pi^{-1}([1, 0])$ as E_∞ . Likewise, we let E'_t denote the curve $(\pi')^{-1}([t, 1])$ and E'_∞ denote the curve $(\pi')^{-1}([1, 0])$. With this notation, we have

- (1) E_∞ is defined by the equation $XYZ = 0$.
- (2) E_0 is defined by the equation $(XY - Z^2)(X + Y) = 0$.
- (3) For all $t \in \mathbb{Q}^*$, E'_t is an elliptic curve defined over \mathbb{Q} in Weierstrass form isomorphic to E_t and ϕ maps E_t to E'_t .
- (4) The point $[1, -1, 0]$ is on E_t for every t and $\phi([1, -1, 0]) = [0, 1, 0]$.

Given the remark above, we take $\mathcal{O} = [1, -1, 0]$ to be the identity of the group of (rational) points on E_t . We note that the statements in the remark can be summarized by saying that \mathcal{E} , together with π and the *zero section* $\sigma_0 : \mathbb{P}^1 \rightarrow \mathcal{E}$ defined by $\sigma_0(T) = ([-1, 1, 0], T)$, is an *elliptic surface*. (See [12] for precise definitions.)

Now, we define \mathcal{H} to be

$$\mathcal{E} \times_{\mathbb{P}^1} \mathcal{E} \times_{\mathbb{P}^1} \mathcal{E} = \{(U, V, W) \in \mathcal{E} \times \mathcal{E} \times \mathcal{E} \mid \pi(U) = \pi(V) = \pi(W)\}.$$

(We say that \mathcal{H} is a *fiber product* over \mathbb{P}^1 . We again refer the reader to [12] for precise definitions.) Just as we can think of \mathcal{E} as the projective version of $g(x) + g(y) = t$, \mathcal{H} is the “projective version” of (2.6).

We let $\mathcal{H}(\mathbb{Q})$ be the set of rational points in \mathcal{H} and we let \mathcal{R} be the set of 4-tuples of rational points on $y = x^2$ at rational distance. Theorem 2.3 then gives a correspondence between elements of \mathcal{R} and sets of points in $\mathcal{H}(\mathbb{Q})$. The correspondence

is between \mathcal{R} and sets of points in $\mathcal{H}(\mathbb{Q})$ because there are many 6-tuples of rational values $\{m_{ij}\}$, $1 \leq i < j \leq 4$, that give rise to the same element of \mathcal{R} . If we let \mathcal{H}_0 be the set of points in $\mathcal{H}(\mathbb{Q})$ that correspond to some element of \mathcal{R} , then we can define a relation on \mathcal{H}_0 as follows: for $A, B \in \mathcal{H}_0$, we will say $A \sim B$ if they each correspond to the same four tuple of points on $y = x^2$ at rational distance. This is clearly an equivalence relation and we can let \mathcal{H}_0/\sim denote the set of equivalence classes. Much of Theorem 2.3 can then be restated as

Theorem 4.3. *There is a well-defined, one-to-one map $\psi : \mathcal{R} \longrightarrow \mathcal{H}_0/\sim$.*

Proof. Suppose $\{P_1, P_2, P_3, P_4\} \in \mathcal{R}$. By Theorem 2.3, there are rational values m_{ij} , $1 \leq i < j \leq 4$, such that

$$(4.1) \quad A = (([m_{13}, m_{24}, 1], [t, 1]), ([m_{23}, m_{14}, 1], [t, 1]), ([m_{12}, m_{34}, 1], [t, 1])),$$

$A \in \mathcal{H}_0$, where $t = g(m_{13}) + g(m_{24})$ and $m_{ij} \neq 0$. We define the map ψ by taking $\{P_1, P_2, P_3, P_4\}$ to the equivalence class of the point A . ψ is clearly well-defined and one-to-one. \square

Remark 4.4. When A is a point in \mathcal{H}_0 , we will often write

$$A = ((m_{13}, m_{24}), (m_{23}, m_{14}), (m_{12}, m_{34}))$$

to mean (4.1) with the understanding that $t = g(m_{13}) + g(m_{24})$. Moreover, we use the convention of letting $(X/Z, Y/Z)$ denote the point in projective space $[X, Y, Z]$ whenever $Z \neq 0$.

This theorem says that if we can describe the elements of \mathcal{H}_0/\sim (and in particular those equivalence classes coming from distinct, nonconcyclic points on $y = x^2$), then we can characterize all four tuples of rational points on $y = x^2$ at rational distance. The remainder of this section is dedicated to laying out this description. We begin by recharacterizing the equivalence relation \sim as the equivalence relation induced by a particular group action.

Let S_n denote the group of permutations on n letters. For any

$$A = ((m_{13}, m_{24}), (m_{23}, m_{14}), (m_{12}, m_{34})) \in \mathcal{H}_0$$

and any $\sigma \in S_4$, define $\sigma \circ A$ as follows:

$$\sigma \circ A = ((m_{\sigma(1)\sigma(3)}, m_{\sigma(2)\sigma(4)}), (m_{\sigma(2)\sigma(3)}, m_{\sigma(1)\sigma(4)}), (m_{\sigma(1)\sigma(2)}, m_{\sigma(3)\sigma(4)})).$$

We now have

Theorem 4.5. *S_4 acts on \mathcal{H}_0 by \circ . Furthermore, suppose*

$$A = ((m_{13}, m_{24}), (m_{23}, m_{14}), (m_{12}, m_{34})) \in \mathcal{H}_0.$$

Let $\langle P_1, P_2, P_3, P_4 \rangle$ be the ordered set of four points at rational distance given by Theorem 2.3 (determined by the m_{ij}). Then $\sigma \circ A$ corresponds to the ordered set $\langle P_{\sigma(1)}, P_{\sigma(2)}, P_{\sigma(3)}, P_{\sigma(4)} \rangle$.

Proof. First we note that if i, j, k and l are distinct in $\{1, 2, 3, 4\}$, then for any $\sigma \in S_4$, $\sigma(i), \sigma(j), \sigma(k)$ and $\sigma(l)$ are distinct as well. This implies that $\sigma \circ A \in \mathcal{H}_0$ whenever $A \in \mathcal{H}_0$. Since it is clear that $(\tau\sigma) \circ A = \tau \circ (\sigma \circ A)$, we have that \circ defines a group action.

It remains to show that $\sigma \circ A$ corresponds to permuting the points according to σ . Since the transpositions $(1\ 2), (1\ 3), (1\ 4)$, and $(2\ 3)$ generate S_4 , this correspondence follows from the information given in Table 1. The table illustrates the association

TABLE 1. Correspondence between changes to A and changes to P .

The change in coordinates:	Corresponds to interchanging:
$(U, V, W) \mapsto (V, U, W)$ or equivalently	
$(m_{13}, m_{24}) \mapsto (m_{23}, m_{14})$	P_1 and P_2 .
$(m_{23}, m_{14}) \mapsto (m_{13}, m_{24})$	
$(m_{12}, m_{34}) \mapsto (m_{12}, m_{34})$	
$(U, V, W) \mapsto (U, W, V)$ or equivalently	
$(m_{13}, m_{24}) \mapsto (m_{13}, m_{24})$	P_1 and P_3 .
$(m_{23}, m_{14}) \mapsto (m_{12}, m_{34})$	
$(m_{12}, m_{34}) \mapsto (m_{23}, m_{14})$	
$(U, V, W) \mapsto (-W, V, -U)$ or equivalently	
$(m_{13}, m_{24}) \mapsto (m_{34}, m_{12})$	P_1 and P_4 .
$(m_{23}, m_{14}) \mapsto (m_{23}, m_{14})$	
$(m_{12}, m_{34}) \mapsto (m_{24}, m_{13})$	
$(U, V, W) \mapsto (W, V, U)$ or equivalently	
$(m_{13}, m_{24}) \mapsto (m_{12}, m_{34})$	P_2 and P_3 .
$(m_{23}, m_{14}) \mapsto (m_{23}, m_{14})$	
$(m_{12}, m_{34}) \mapsto (m_{13}, m_{24})$	

between changes in the coordinates of A and changes in the P_i as determined by Theorem 2.3. A is written as (U, V, W) with $U = (m_{13}, m_{24})$, $V = (m_{23}, m_{14})$ and $W = (m_{12}, m_{34})$ to make things clearer. \square

Corollary 4.6. *If $A \in \mathcal{H}_0$ and $\sigma \in S_4$, then $A \sim \sigma \circ A$.*

Furthermore, suppose we let $n = (n_{13}, n_{24}, n_{23}, n_{14}, n_{12}, n_{34}) \in (\mathbb{Z}/2\mathbb{Z})^6$ and again let

$$A = ((m_{13}, m_{24}), (m_{23}, m_{14}), (m_{12}, m_{34})) \in \mathcal{H}_0.$$

Let A_n be A with m_{ij} replaced by $-1/m_{ij}$ whenever $n_{ij} = 1$ (and m_{ij} unchanged otherwise). Then since $g(m) = g(-1/m)$, $(\mathbb{Z}/2\mathbb{Z})^6$ acts on \mathcal{H}_0 by $n \cdot A = A_n$. To be concise, below we use (n_{ij}) to denote n .

We now combine the two individual group actions of S_4 and $(\mathbb{Z}/2\mathbb{Z})^6$ together into one action. In the theorem below, let θ be the homomorphism $\theta : S_4 \rightarrow \text{Aut}((\mathbb{Z}/2\mathbb{Z})^6)$ defined by $\theta(\sigma)(n_{ij}) = (n_{\sigma(i)\sigma(j)})$ and let

$$\Gamma = (\mathbb{Z}/2\mathbb{Z})^6 \rtimes S_4, \text{ the semidirect product relative to } \theta.$$

(As in the case of m_{ij} , we set n_{ij} to n_{ji} whenever $i > j$.)

Theorem 4.7. Γ acts on \mathcal{H}_0 by $(n, \sigma) \star A = n \cdot (\sigma \circ A)$ and the equivalence relation induced by this group action is \sim . Equivalently, two points, A and B , in \mathcal{H}_0 correspond to the same set of four rational points on $y = x^2$ at rational distance if and only if there is a $\gamma \in \Gamma$ such that $\gamma \star A = B$.

Proof. Let (m, τ) and (n, σ) be elements of Γ . We need to verify that

$$(4.2) \quad (m, \tau) \star ((n, \sigma) \star A) = (m\theta(\tau)(n), \tau\sigma) \star A.$$

Since $(\mathbb{Z}/2\mathbb{Z})^6$ and S_4 act on \mathcal{H}_0 individually, verifying (4.2) is equivalent to showing

$$\tau \circ (n \cdot B) = \theta(\tau)(n) \cdot (\tau \circ B),$$

where $B = \sigma \circ A$. But the homomorphism θ is constructed precisely so that this works.

The action of $(\mathbb{Z}/2\mathbb{Z})^6$ corresponds to choosing positive or negative values for δ_{ij} in equations (2.1). (To see this, observe how the value of α in Lemma 2.1 changes when m is replaced by $-1/m$.) This and Theorem 4.5 verify that for any $A, B \in \mathcal{H}_0$, if there exists a $\gamma \in \Gamma$ such that $A = \gamma \star B$, then $A \sim B$. The converse is clear from (2.4). \square

Let $[A]$ denote the orbit of a point $A \in \mathcal{H}_0$ under this group action and $\mathcal{H}_\Gamma = \mathcal{H}_0/\Gamma$ denote the set of orbits. The theorem above says that $\mathcal{H}_\Gamma = \mathcal{H}_0/\sim$. Let us also define $[A] \in \mathcal{H}_\Gamma$ to be a *free orbit* if the stabilizer subgroup Γ_A is trivial or equivalently $|[A]| = |\Gamma| = 4! \cdot 2^6$.

Proposition 4.8. *Let $A = ((u_1, u_2), (u_3, u_4), (u_5, u_6)) \in \mathcal{H}_0$. $[A]$ is a free orbit if and only if*

- (1) $g(u_i) \neq g(u_j)$ for all $i \neq j$, or
- (2) $g(u_{2k-1}) = g(u_{2k})$ for exactly one value of $k \in \{1, 2, 3\}$ and $g(u_i) \neq g(u_j)$ for all other $i \neq j$.

Proof. Let $U_i = (u_{2i-1}, u_{2i})$ so that we may write $A = (U_1, U_2, U_3)$. The points in the orbit of A resulting from the action of $S_4 \subset \Gamma$ consists of all points in \mathcal{H}_0 of the form

$$(4.3) \quad (\varepsilon_1 U_{\sigma(1)}, \varepsilon_2 U_{\sigma(2)}, \varepsilon_3 U_{\sigma(3)}), \quad \sigma \in S_3, \varepsilon_i \in \{\pm 1\} \quad \text{and} \quad \varepsilon_1 \varepsilon_2 \varepsilon_3 = 1.$$

No two of these are equal if and only if $u_i \neq u_j$ for all $i \neq j$ or U_i is of the form (m, m) for precisely one i . Since $-1/x \neq x$ for any rational value x , when we consider the action of the entire group Γ , we get the conditions of the theorem. \square

Remark 4.9. There are two group actions on \mathcal{H}_0 not covered by Γ . First, there is the action of $\mathbb{Z}/2\mathbb{Z}$ on \mathcal{H}_0 corresponding to reflecting four points on the parabola across the y -axis. Since $g(m)$ is an odd function, this action is defined by

$$\begin{aligned} 1 \bullet ((m_{13}, m_{24}), (m_{23}, m_{14}), (m_{12}, m_{34})) \\ = ((-m_{13}, -m_{24}), (-m_{23}, -m_{14}), (-m_{12}, -m_{34})). \end{aligned}$$

We will for the most part ignore this action since it is present in both \mathcal{R} and \mathcal{H}_0 .

More interesting is the action of $\mathbb{Z}/2\mathbb{Z}$ on \mathcal{H}_0 defined by

$$(4.4) \quad 1 \diamond (U, V, W) = (-U, V, W).$$

The existence of this last action means that one element of \mathcal{H}_0 may correspond to two distinct elements of \mathcal{R} . Before we can be more precise, we first observe that Proposition 4.8 (and the description (4.3) in particular) implies the following propositions.

Proposition 4.10. *Suppose $A \in \mathcal{H}_0$ such that $[A]$ is a free orbit. The $\mathbb{Z}/2\mathbb{Z}$ action described by (4.4) is trivial on $[A]$ (i.e. $[1 \diamond A] = [A]$) if and only if $[A]$ is of the second form in Proposition 4.8.*

Proposition 4.11. *If $A \in \mathcal{H}_0$ such that $[A]$ is not a free orbit, then the $\mathbb{Z}/2\mathbb{Z}$ action described by (4.4) is trivial on $[A]$.*

The former of the propositions above justifies defining a free orbit $[A]$ to be *doubly free* if A is of the first form in Proposition 4.8 and to be *singularly free* if A is of the second form in the proposition. We are now ready to prove

Proposition 4.12. *$\psi^{-1}([(U, V, W)]) \neq \psi^{-1}([(-U, V, W)])$ if and only if $[(U, V, W)]$ is a doubly free orbit.*

Proof. ψ is one-to-one and so $\psi^{-1}([(U, V, W)]) = \psi^{-1}([(-U, V, W)])$ if and only if $[(U, V, W)] = [(-U, V, W)]$. But then this occurs if and only if $[(U, V, W)]$ is not a doubly free orbit. \square

The propositions and theorems below give the necessary and sufficient conditions for an element of \mathcal{H}_Γ to correspond to a distinct and nonconcyclic set of points at rational distance.

Theorem 4.13. *Let $P = \{P_1, P_2, P_3, P_4\} \in \mathcal{R}$. P is a set of distinct points if and only if $\psi(P)$ is a free orbit.*

Proof. Suppose $\psi(P) = [((m_{13}, m_{24}), (m_{14}, m_{23}), (m_{12}, m_{34}))]$. The equations for the sum of the x -coordinates of two points given in Proposition 2.4 imply that points are *not* distinct if and only if $x_i + x_j = x_i + x_k$ for some set of distinct indices $i, j, k \in \{1, 2, 3, 4\}$. Since $x_i + x_j = g(m_{ij})$, this implies that the points are distinct if and only if the $g(m_{ij})$ are distinct with possible exceptions for $g(m_{ij}) = g(m_{kl})$, where i, j, k , and l are distinct.

By Proposition 4.8, the $g(m_{ij})$ are distinct if and only if $[\psi(P)]$ is a doubly free orbit. Now, suppose the $g(m_{ij})$ are not distinct. Then $g(m_{ij}) = g(m_{kl})$ for some distinct i, j, k and l . If $[\psi(P)]$ is a singularly free orbit, then there will only be one such equality and the points in P will be distinct.

Now suppose $[\psi(P)]$ is not a free orbit and we have

$$(4.5) \quad g(m_{ij}) = g(m_{kl}) \quad \text{and} \quad g(m_{ik}) = g(m_{jl})$$

for i, j, k and l distinct. By definition of \mathcal{H} , $g(m_{ij}) + g(m_{kl}) = g(m_{ik}) + g(m_{jl})$. Therefore (4.5) holds if and only if $g(m_{ij}) = g(m_{ik})$. But then the points of P are not distinct. \square

Theorem 4.14. *Let $P = \{P_1, P_2, P_3, P_4\} \in \mathcal{R}$ and $\psi(P) = [(U, V, W)] \in \mathcal{H}_\Gamma$. P is a set of nonconcyclic points if and only if $\pi(U) \neq [0, 1]$.*

Proof. First, note that π is well defined in this context. More precisely, if $(U, V, W) \sim (U', V', W')$, then $\pi(U) = \pi(U')$.

Suppose the x -coordinate of P_i is x_i . Theorem 4.3 and Proposition 2.4 say that $\psi(P) = [(U, V, W)]$, where U can be taken to be $([m_{13}, m_{24}, 1], [g(m_{13}) + g(m_{24}), 1])$ with $g(m_{13}) = x_1 + x_3$ and $g(m_{24}) = x_2 + x_4$. Therefore, $\pi(U) = [g(m_{13}) + g(m_{24}), 1] = [x_1 + x_2 + x_3 + x_4, 1]$. Hence, by Proposition 3.1, the points are concyclic if and only if $\pi(U) = [0, 1]$. \square

We may now turn our attention to the last piece of the puzzle of understanding the set \mathcal{H}_Γ —namely, that of describing all the points of $\mathcal{H}(\mathbb{Q})$ as completely as possible. Since \mathcal{H} is the fiber product of three copies of \mathcal{E} , this problem is equivalent to describing the rational points of the elliptic surface \mathcal{E} . The following theorems

outline the most general facts about \mathcal{E} . Recall that one way to characterize the group law of an elliptic curve is to say $R_1 + R_2 + R_3 = \mathcal{O}$ if and only if the R_i are collinear. Throughout the following, we let $Q = [1, 0, 0]$ and $\mathcal{O} = [1, -1, 0]$, the identity of the group.

Theorem 4.15. *For any $t \in \mathbb{Q}^*$, the group of rational points on E_t contains a subgroup of order 4. More specifically, $Q = [1, 0, 0]$ is a generator of this subgroup with*

$$2Q = (0, 0) \quad \text{and} \quad 3Q = [0, 1, 0].$$

Proof. The tangent line at Q intersects E_t at $(0, 0)$; the tangent line at $(0, 0)$ intersects E_t at $[1, -1, 0]$; and the three points $[1, 0, 0]$, $[0, 1, 0]$ and $[1, -1, 0]$ are collinear. \square

Theorem 4.16. *For all $t \in \mathbb{Q}^*$, if $P = (x, y) \in E_t(\mathbb{Q})$ with $xy \neq 0$, then we have the following group law formulas:*

$$(4.6) \quad -P = (y, x),$$

$$(4.7) \quad P + Q = (y, -1/x),$$

$$(4.8) \quad 2P = \left(\frac{y(x^2 + 1)(xy + 1)}{x(y^2 + 1)(x - y)}, -\frac{x(y^2 + 1)(xy + 1)}{y(x^2 + 1)(x - y)} \right).$$

Proof. The points P, \mathcal{O} and (y, x) are collinear and likewise for the points P, Q and $(-1/x, y)$. The final formula is attained by calculating the third point of intersection of the tangent line at P . \square

Corollary 4.17. *For all $t \in \mathbb{Q}^*$, if $P = (x, y) \in E_t(\mathbb{Q})$ with $xy \neq 0$, then*

- (1) P is a point of order 2 if and only if $x = y$. If this is the case, the torsion subgroup of $E_t(\mathbb{Q})$ is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
- (2) P is a point of order 4 if and only if $x = -1/y$. If this is the case, we again have that the torsion subgroup of $E_t(\mathbb{Q})$ is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
- (3) P is a point of order 8 if and only if $y = -(x + 1)/(x - 1)$ or $y = (x - 1)/(x + 1)$, $x \neq \pm 1$. If this is the case, the torsion subgroup of $E_t(\mathbb{Q})$ must be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Furthermore, the subgroups above are the only possibilities for the torsion subgroups.

Proof. If P is a point of order 2, then $P = -P$. By formula (4.6), this means that $(x, y) = (y, x)$.

If P is a point of order 4, then $2P = (x', y')$ is a point of order 2. Therefore, $x' = y'$ and so by formulas (4.8) and (4.6), $xy + 1 = 0$.

If P is a point of order 8, then $2P = [x', y', z']$ is a point of order 4. Therefore, either $x' = z' = 0$, $y' = z' = 0$ or $z' = 1$ and $x' = -1/y'$. By formula (4.8), the first two cases cannot occur. This rules out the possibility that the torsion subgroup is equal to $\mathbb{Z}/8\mathbb{Z}$. The last case occurs when $(x + \frac{y+1}{y-1}) \cdot (x - \frac{y-1}{y+1}) = 0$. In this case, the torsion subgroup of $E_t(\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Since $E_t(\mathbb{Q})$ must contain a subgroup of order 4, Mazur's theorem tells us that the only other torsion subgroup possible is $\mathbb{Z}/12\mathbb{Z}$. This subgroup contains a point of order 3 and so we need only check the condition that $2P = -P$. By formulas (4.6) and (4.8), we see that this cannot occur. \square

Using the formulas for the group law, we then have

Corollary 4.18. *If a rational point of a particular finite order exists on E_t , then it must be of the form given by*

Order of Points:	Points
8	$(x, -\frac{x+1}{x-1}), (x, \frac{x-1}{x+1}), (-\frac{x+1}{x-1}, x), (\frac{x-1}{x+1}, x),$ $(-\frac{1}{x}, -\frac{x+1}{x-1}), (-\frac{1}{x}, \frac{x-1}{x+1}), (-\frac{x+1}{x-1}, -\frac{1}{x}), (\frac{x-1}{x+1}, -\frac{1}{x})$
4	$(x', -\frac{1}{x'}), (-\frac{1}{x'}, x'), [1, 0, 0], [0, 1, 0]$
2	$(x', x'), (-\frac{1}{x'}, -\frac{1}{x'}), (0, 0)$
0	$[1, -1, 0]$

where $x' = g(x)$ if the points of order 8 are on the curve.

Corollary 4.19. *Let x and y be two rational values such that $xy \neq 0$ and $y \notin \{\pm x, \pm 1/x, \frac{x-1}{x+1}, -\frac{x+1}{x-1}\}$. If $t = g(x) + g(y)$, then E_t is an elliptic curve defined over \mathbb{Q} and (x, y) is a point of infinite order in $E_t(\mathbb{Q})$.*

Remark 4.20. Note that Corollary 4.19 does not imply that if $t = g(x) + g(y)$ where $y \in \{\pm x, \pm 1/x, \frac{x-1}{x+1}, -\frac{x+1}{x-1}\}$, then there are no points of infinite order in $E_t(\mathbb{Q})$. It only says that the point $(x, y) \in E_t(\mathbb{Q})$ is not one of them. Indeed it was discovered that there are curves of rank greater than 0 for each of the possible torsion subgroups. For example, if $t = 4$, then $E_t(\mathbb{Q})$ is an elliptic curve of rank 1 with torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. (The minimal Weierstrass form of this curve is $y + xy = x^3 - 49423080x + 130545230400$ and a generator for the group of rational points is (4760, 53720). The rank and generator were found using John Cremona’s **mwrnk** program [5].)

Corollary 4.21. *Let $A = (U_1, U_2, U_3)$ be a point in \mathcal{H}_0 such that $\psi(P) = [A]$ for some $P \in \mathcal{R}$ and let $t = \pi(U_1)$. If P is a set of distinct, nonconcyclic points, then*

- (1) U_i cannot equal $\mathcal{O}, Q, 2Q$ or $3Q$ for any i .
- (2) U_i cannot equal $m \cdot U_j + n \cdot Q$ where $m \in \{-1, 0, 1\}, n \in \mathbb{Z}$ and $i \neq j$.

In particular, $E_t(\mathbb{Q})$ must contain a point of infinite order.

Proof. U_i must be of the form $([u, v, 1], [t, 1])$ with $u, v \neq 0$ and $t \neq 0$. This immediately gives us the first condition. The second condition must be satisfied in order for $[A]$ to be a free or almost free orbit. □

Remark 4.22. Observe that **the corollary above completely characterizes all points in \mathcal{H}_0 that correspond to distinct, nonconcyclic sets of points at rational distance in \mathcal{R} .** A direct consequence of the two preceding corollaries is the following:

Corollary 4.23. *There are infinitely many sets of four distinct, nonconcyclic, rational points at rational distance on $y = x^2$.*

5. EXAMPLES

Let \mathcal{R}_0 be the subset of \mathcal{R} consisting of 4-tuples of *distinct, nonconcyclic* points. The points in \mathcal{R}_0 in Table 2 were found by choosing a pair of positive rational values

TABLE 2. Examples of nonconyclic points on $y = x^2$ at rational distance

t	\mathcal{H}_Γ	\mathcal{R}_0
13/6	$[(\frac{3}{10}, \frac{15}{2}), (\frac{1}{2}, 6), (\frac{4}{3}, 4)]$	$(-\frac{307}{240}, -\frac{19}{80}, \frac{127}{240}, \frac{757}{240})$
	$[(\frac{3}{10}, \frac{15}{2}), (\frac{1}{2}, 6), (4, \frac{4}{3})]$	$(-\frac{497}{240}, \frac{133}{240}, \frac{317}{240}, \frac{189}{80})$
16/15	$[(\frac{1}{3}, 5), (\frac{6}{7}, \frac{14}{5}), (\frac{5}{3}, \frac{5}{3})]$	$(-\frac{283}{280}, -\frac{271}{840}, \frac{719}{840}, \frac{1297}{840})$
19/12	$[(\frac{1}{3}, 6), (\frac{3}{4}, 4), (\frac{5}{3}, \frac{5}{2})]$	$(-\frac{259}{240}, -\frac{61}{240}, \frac{63}{80}, \frac{511}{240})$
	$[(\frac{1}{3}, 6), (\frac{3}{4}, 4), (\frac{5}{2}, \frac{5}{3})]$	$(-\frac{107}{80}, \frac{1}{240}, \frac{251}{240}, \frac{449}{240})$
21/8	$[(\frac{3}{4}, 6), (\frac{5}{4}, 5), (2, 4)]$	$(-\frac{49}{120}, \frac{7}{60}, \frac{19}{30}, \frac{137}{60})$
	$[(\frac{3}{4}, 6), (\frac{5}{4}, 5), (4, 2)]$	$(-\frac{233}{240}, \frac{163}{240}, \frac{287}{240}, \frac{413}{240})$
25/24	$[(\frac{1}{4}, 6), (\frac{7}{12}, \frac{7}{2}), (2, \frac{4}{3})]$	$(-\frac{67}{42}, -\frac{47}{168}, \frac{173}{168}, \frac{317}{168})$
	$[(\frac{1}{4}, 6), (\frac{7}{12}, \frac{7}{2}), (3, \frac{3}{4})]$	$(-\frac{317}{168}, \frac{1}{84}, \frac{37}{28}, \frac{67}{42})$
	$[(\frac{7}{12}, \frac{7}{2}), (\frac{3}{4}, 3), (2, \frac{4}{3})]$	$(-\frac{45}{56}, \frac{5}{21}, \frac{43}{84}, \frac{23}{21})$
	$[(\frac{7}{12}, \frac{7}{2}), (\frac{3}{4}, 3), (\frac{4}{3}, 2)]$	$(-\frac{193}{336}, \frac{1}{112}, \frac{95}{336}, \frac{445}{336})$
33/56	$[(\frac{3}{28}, \frac{21}{2}), (1, \frac{7}{4}), (\frac{5}{4}, \frac{10}{7})]$	$(-\frac{254}{105}, -\frac{1843}{840}, \frac{254}{105}, \frac{167}{60})$
	$[(\frac{1}{5}, 6), (\frac{11}{30}, \frac{11}{3}), (\frac{5}{2}, \frac{3}{5})]$	$(-\frac{382}{165}, -\frac{14}{165}, \frac{749}{660}, \frac{98}{55})$
	$[(\frac{1}{5}, 6), (\frac{9}{10}, \frac{9}{5}), (\frac{5}{4}, \frac{4}{3})]$	$(-\frac{983}{720}, -\frac{149}{144}, \frac{907}{720}, \frac{1193}{720})$
31/60	$[(\frac{3}{5}, \frac{5}{2}), (\frac{9}{10}, \frac{9}{5}), (\frac{5}{4}, \frac{4}{3})]$	$(-\frac{311}{720}, -\frac{73}{720}, \frac{47}{144}, \frac{521}{720})$
	$[(\frac{3}{5}, \frac{5}{2}), (\frac{9}{10}, \frac{9}{5}), (\frac{4}{3}, \frac{5}{4})]$	$(-\frac{67}{144}, -\frac{49}{720}, \frac{259}{720}, \frac{497}{720})$
	$[(\frac{1}{5}, 6), (\frac{9}{10}, \frac{9}{5}), (\frac{4}{3}, \frac{5}{4})]$	$(-\frac{1007}{720}, -\frac{721}{720}, \frac{931}{720}, \frac{1169}{720})$
	$[(\frac{4}{15}, \frac{20}{3}), (\frac{5}{9}, \frac{9}{2}), (3, \frac{6}{5})]$	$(-\frac{1331}{720}, \frac{77}{720}, \frac{883}{720}, \frac{1463}{720})$
91/60	$[(\frac{5}{9}, \frac{9}{2}), (\frac{4}{5}, \frac{15}{4}), (\frac{10}{3}, 1)]$	$(-\frac{851}{720}, \frac{403}{720}, \frac{689}{720}, \frac{851}{720})$
	$[(\frac{5}{9}, \frac{9}{2}), (\frac{4}{5}, \frac{15}{4}), (3, \frac{6}{5})]$	$(-\frac{157}{144}, \frac{337}{720}, \frac{623}{720}, \frac{917}{720})$
	$[(\frac{4}{15}, \frac{20}{3}), (\frac{5}{9}, \frac{9}{2}), (\frac{6}{5}, 3)]$	$(-\frac{917}{720}, -\frac{337}{720}, \frac{469}{720}, \frac{1877}{720})$
	$[(\frac{4}{15}, \frac{20}{3}), (\frac{5}{9}, \frac{9}{2}), (1, \frac{10}{3})]$	$(-\frac{851}{720}, -\frac{403}{720}, \frac{403}{720}, \frac{1943}{720})$
	$[(2, \frac{15}{2}), (\frac{9}{4}, \frac{36}{5}), (6, \frac{10}{3})]$	$(-\frac{91}{144}, \frac{199}{144}, \frac{221}{144}, \frac{1547}{720})$
133/30	$[(2, \frac{15}{2}), (\frac{9}{4}, \frac{36}{5}), (\frac{10}{3}, 6)]$	$(\frac{49}{720}, \frac{491}{720}, \frac{601}{720}, \frac{2051}{720})$
	$\dagger [(\frac{3}{10}, \frac{20}{3}), (1, \frac{15}{4}), (\frac{10}{3}, \frac{5}{4})]$	$\dagger (-\frac{91}{60}, 0, \frac{91}{60}, \frac{209}{120})$
	$[(\frac{3}{10}, \frac{20}{3}), (\frac{5}{4}, \frac{10}{3}), (\frac{12}{5}, 2)]$	$(-\frac{137}{120}, -\frac{3}{8}, \frac{41}{30}, \frac{227}{120})$
209/120	$[(\frac{3}{10}, \frac{20}{3}), (1, \frac{15}{4}), (\frac{12}{5}, 2)]$	$(-\frac{301}{240}, -\frac{21}{80}, \frac{301}{240}, \frac{481}{240})$
	$[(\frac{2}{5}, 8), (\frac{8}{5}, 5), (\frac{15}{4}, \frac{8}{3})]$	$(-\frac{553}{480}, \frac{49}{480}, \frac{787}{480}, \frac{1103}{480})$
231/80	$[(\frac{2}{5}, 8), (\frac{8}{3}, \frac{15}{4}), (\frac{16}{5}, \frac{16}{5})]$	$(-\frac{647}{960}, -\frac{361}{960}, \frac{1747}{960}, \frac{2033}{960})$
	$[(\frac{8}{5}, 5), (\frac{8}{3}, \frac{15}{4}), (\frac{16}{5}, \frac{16}{5})]$	$(\frac{91}{960}, \frac{377}{960}, \frac{1009}{960}, \frac{259}{192})$

x, y such that $y \notin \{x, 1/x, \frac{x-1}{x+1}, -\frac{x+1}{x-1}\}$, setting $t = g(x) + g(y)$ and searching for points in $E_t(\mathbb{Q})$. If we let \mathbb{T}_t be the subgroup of points of finite order in $E_t(\mathbb{Q})$, then the theorems in the previous section give very explicit formulas to determine when $U \in \mathbb{T}_t$ and when $U + \mathbb{T}_t = \pm V + \mathbb{T}_t$ for any $U, V \in E_t(\mathbb{Q})$. Therefore, producing elements of \mathcal{H}_Γ that correspond to elements of \mathcal{R}_0 from points in $E_t(\mathbb{Q})$ is an easy (and efficient) matter.

The points shown in the table represent a small fraction of the total list compiled. Those entries in the table written in bold have all x -coordinates positive and those that are italicized have one of the x -coordinates equal to the negative of the other. The entry marked by \dagger gives rise to the example of five points at rational distance with four of the points concyclic mentioned in Section 3.

We note that we could have set $U = (x, y) \in E_t(\mathbb{Q})$ and generated points in \mathcal{H} of the form $A = (n_1U, n_2U, n_3U)$. If $n_i \in \mathbb{Z}, n_i \neq 0$ and $n_i \neq \pm n_j$ for $i \neq j$, then A is a point in \mathcal{H}_0 such that $\psi^{-1}([A]) \in \mathcal{R}_0$. Unfortunately, since the height of $nU \in E_t$ is quadratic in n , this strategy generally produces points with very large numerators and denominators. Ideally we would like to find t such that E_t has both large rank and small regulator. This would give a number of points in \mathcal{H}_0 that correspond to elements of \mathcal{R}_0 with relatively small height.

6. FURTHER WORK

We see three natural progressions of this work. First, we might try to use the techniques presented here to characterize all 5-tuples (or more) of points on $y = x^2$ at rational distance. Given some preliminary work on this, it seems plausible that descriptions similar to those of Corollary 4.21 are possible. What is not yet clear is if such a description will tell us if there are infinitely many 5-tuples of rational points on $y = x^2$ at rational distance, a positive, finite number of them, or no such sets of points on $y = x^2$.

Second, we might extend the question to other conics (or other smooth, plane curves). Again, some preliminary work suggests that the techniques presented here might be able to answer the question

Question 6.1. *For which smooth conics are there four points at rational distance with no four concyclic?*

Note that the collinearity condition is unnecessary here as well since no line can intersect any conic in more than two points. Clearly the conic cannot be a circle, but what can we say beyond this trivial exclusion? As an immediate consequence of the work above, we have the following

Theorem 6.2. *Let C be a parabola and let d be the distance from the focus of C to its directrix. If d is rational, then there are infinitely many 4-tuples of nonconcyclic points on C at rational distance.*

Proof. If C and d are defined as in the statement of the theorem, then C is a translation and rotation of the parabola $C' : y = \frac{1}{2d}x^2$. Now suppose $\{P_1, P_2, P_3, P_4\}$ is a set of points at rational distance on $y = x^2$ and let x_i denote the x -coordinate of P_i . If $x'_i = 2d \cdot x_i$ and $P'_i = (x'_i, \frac{1}{2d}(x'_i)^2)$, then $\{P'_1, P'_2, P'_3, P'_4\}$ is a set of rational distance points on C' . Furthermore, $\{P_1, P_2, P_3, P_4\}$ is a concyclic set if and only if $\{P'_1, P'_2, P'_3, P'_4\}$ is a concyclic set. Therefore, Corollary 4.23 gives us the theorem. \square

Furthermore, we believe that we can take $d = \sqrt{c}$, $c \in \mathbb{Q}$, and get the same conclusion. The details of this have not been completely worked out, but the idea would be to parallel the work done here. We include the example of points on $y = \sqrt{5}x^2$ with x -coordinates

$$\left\{ \frac{840837}{2306524}, -\frac{941477}{2306524}, \frac{2618949}{2306524}, \frac{1675371}{2306524} \right\}$$

to give some hint as to how one might proceed. We found this example by first parameterizing solutions to $\delta^2 = 1 + 5 \cdot \beta^2$ using the chord and tangent method described in Section 2. The parameterization can be defined by $\beta = g_5(m) = (2m)/(m^2 - 5)$. To produce the example above, we “randomly” set $t = g_5(3) + g_5(7)$ and searched for other points on the elliptic curve $g_5(x) + g_5(y) = t$. We found that $(3, 7)$, $(4, -3/2)$, and $(37/340, 1234/435)$ were points on this curve. Now, by assuming that the theorems of the previous sections all hold with g_5 in place of g , we arrive at the example above. We believe more generally that all the theorems hold with $g_\alpha(m) = (2m)/(m^2 - \alpha)$ in place of g . Since $g_\alpha(m)$ parameterizes solutions to $\delta^2 = 1 + \alpha \cdot \beta^2$, this would give us the result.

Finally, observe that the focus of the parabola C' is $F = (0, d/2)$ and that rational points on C' are necessarily at rational distance to F . Therefore, we have immediately that the set F together with any four rational points on C' forms a rational distance set in the plane. This in turn may lead to new configurations of six points in the plane at rational distance with no three collinear and no four concyclic. More generally, this leads very naturally back to the unsolved problem mentioned in the opening section—namely

Question 6.3. *Can you find more than 6 points in the plane at rational distance with no four concyclic and no three collinear?*

ACKNOWLEDGMENTS

Unless stated otherwise, calculations were performed using GP/Pari [2].

We would like to thank Allan MacLeod for sharing a preprint [9] of his which bettered some earlier results of mine on this problem. As mentioned earlier, he found a number of examples of four nonconcyclic, rational points on $y = x^2$ at rational distance, and that in turn inspired much of the work here. We also thank Tom Hunter for his many thoughtful comments throughout the writing of this paper. Finally, we owe particular gratitude to Edray Goins for his meticulous reading of a draft of this paper and his significant suggestions.

REFERENCES

1. William Anderson, William Simons, J. G. Mauldon and James C. Smith. Elementary Problems and Solutions: A Dense Subset of the Unit Circle (E 2697). *American Mathematical Monthly*, 86(3):225, Mar. 1979.
2. C. Batut, K. Belabas, D. Benardi, 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. Andrew Bremner and Richard K. Guy. A Dozen Difficult Diophantine Dilemmas. *American Mathematical Monthly*, 95(1):31-36, Jan. 1998.
4. Andrew Bremner, *Arizona State University*. Rational Points on $y = x^2$. *Personal communication*. Dec. 2001.
5. John Cremona. **mwrnk**. <http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/>, 2002.
6. Nathaniel Dean, *Rice University*. *Personal communication*. Oct. 2000.

7. Richard K. Guy, *Unsolved Problems in Number Theory, Second Edition*. Springer-Verlag, 1994. MR **96e**:11002
8. J. Lagrange and J. Leech. Two Triads of Squares. *Mathematics of Computation*. 46(174):751-758, Apr. 1986. MR **87d**:11018
9. Allan J. MacLeod, *University of Paisley*. Rational Distance Sets on $y = x^2$. *Personal communication*. Jun. 2002.
10. Landon Curt Noll and David I. Bell. n -clusters for $1 < n < 7$. *Mathematics of Computation*. 53(187):439-444, Jul. 1989. MR **89j**:52008
11. Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986. MR **87g**:11070
12. Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994. MR **96b**:11074
13. W. D. Peebles, Jr., Elliptic Curves and Rational Distance Sets. *Proceedings of the American Mathematical Society*. 5(1):29-33, Feb. 1954. MR **15**:645f

DEPARTMENT OF MATHEMATICS AND STATISTICS, SWARTHMORE COLLEGE, SWARTHMORE, PENNSYLVANIA 19081

E-mail address: `kai@swarthmore.edu`