Rational configuration problems and a family of curves

Love, J.R.

Journal of Number Theory 269 (2025) 370–396

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Rational configuration problems and a family of curves ☆

Jonathan Love

McGill University, Canada

ARTICLE INFO

Article history:
Received 16 April 2024
Received in revised form 26 September 2024
Accepted 27 September 2024
Available online 22 November 2024
Communicated by S.J. Miller

Keywords:
Rational distance
Rational points
Elliptic curve

ABSTRACT

Given $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, we consider the number of rational points on the genus one curve

$$H_\eta : y^2 = (a(1-x^2)+b(2x))^2 + (c(1-x^2)+d(2x))^2.$$

We prove that the set of η for which $H_\eta(\mathbb{Q}) \neq \emptyset$ has density zero, and that if a rational point $(x_0, y_0) \in H_\eta(\mathbb{Q})$ exists, then $H_\eta(\mathbb{Q})$ is infinite unless a certain explicit polynomial in a, b, c, d, x_0, y_0 vanishes.

Curves of the form H_η naturally occur in the study of configurations of points in $\mathbb{R}^n$ with rational distances between them. As one example demonstrating this framework, we prove that if a line through the origin in $\mathbb{R}^2$ passes through a rational point on the unit circle, then it contains a dense set of points P such that the distances from P to each of the three points $(0,0)$, $(0,1)$, and $(1,1)$ are all rational. We also prove some results regarding whether a rational number can be expressed as a sum or product of slopes of rational right triangles.

☆ Supported by CRM-ISM postdoctoral fellowship.
E-mail address: jon.love@mcgill.ca.

https://doi.org/10.1016/j.jnt.2024.09.008
0022-314X/

1. Introduction

1.1. A family of curves

Fix $\eta := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, and let H_η be the curve defined by

$$H_\eta : y^2 = (a(z^2 - x^2) + b(2xz))^2 + (c(z^2 - x^2) + d(2xz))^2 \tag{1}$$

in the weighted projective plane where x, y, z have degree $1, 2, 1$, respectively. Rational points on this curve correspond to vectors $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) \in \mathbb{Q}^2 \setminus \{0\}$ such that both $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ and $\eta\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ have rational length, and as a result, curves of this form can be used to describe solutions to a collection of rational configuration problems; see Section 1.2 for more details. In this paper we study the loci of points η for which H_η has zero, finitely many, or infinitely many rational points.

First, we show that for most values of η, the curve H_η has no rational points.

Theorem 1.1. *Let $\mathcal{L}(X)$ be the set of $\eta \in \mathrm{GL}_2(\mathbb{Q})$ with $a, b, c, d \in \mathbb{Z} \cap [-X, X]$ such that $H_\eta(\mathbb{Q}_v)$ is nonempty for all $v \in \{\infty, 2, 3, 5, 7, \ldots\}$. Then for some constant $C > 0$,*

$$\frac{|\mathcal{L}(X)|}{(2X)^4} < C(\log X)^{-1/4}.$$

The proof is given in Section 4. Note that $H_\eta \simeq H_{m\eta}$ for any positive integer m, so by clearing denominators, every H_η is isomorphic to one of the curves counted in Theorem 1.1. For the sake of comparison, consider the following result by Bhargava, Cremona, and Fisher.

Theorem 1.2 *([4, Theorem 3]). Let $\mathcal{L}'(X)$ denote the set of $(a, b, c, d, e) \in (\mathbb{Z} \cap [-X, X])^5$ such that*

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

has a $\mathbb{Q}_v$ point for all $v \in \{\infty, 2, 3, 5, 7, \ldots\}$. Then

$$\lim_{X \to \infty} \frac{|\mathcal{L}'(X)|}{(2X)^5} \approx 0.7596.$$

We see that the subfamily H_η differs from the larger family, in that far fewer specializations are everywhere locally soluble.

Now suppose we restrict our attention to the collection of points η for which H_η does contain a rational point. In this case we have a stronger classification. Let η^t denote the transpose of η.

Proposition 1.3. *Suppose H_η (Eq. (1)) has a rational point. If $\eta\eta^t$ is a scalar matrix, then* $\det \eta = \lambda^2$ *for some $\lambda \in \mathbb{Q}^\times$ and H_η is a union of two rational conics,*

$$y = \pm\lambda(x^2 + 1).$$

Otherwise H_η is isomorphic to

$$E_{r,s} : y^2 = x^3 + (1 + r^2 + s^2)x^2 + s^2x$$

for some $r, s \in \mathbb{Q}$ with $s \neq 0$ and $(r, s) \neq (0, \pm 1)$.

A proof is given in Section 3.4 using the fact that the isomorphism type of H_η is invariant under acting on the left and right of η by elements of the orthogonal group $\mathrm{O}_2(\mathbb{Q})$. An explicit change of variables expressing r, s in terms of a, b, c, d and the rational point $(x_0 : y_0 : z_0) \in H_\eta(\mathbb{Q})$ is given by Lemma 3.2.

Theorem 1.4. *Let $r, s \in \mathbb{Q}$ with $s \neq 0$ and $(r, s) \neq (0, \pm 1)$. The point $(-1, r) \in E_{r,s}(\mathbb{Q})$ is non-torsion if and only if $r \neq 0$, $s \neq \pm 1$, and $4r^2s \neq \pm(1 - s^2)^2$.*

In particular, for most of the values η such that $H_\eta(\mathbb{Q})$ is nonempty, $H_\eta(\mathbb{Q})$ is actually infinite. The proof of this result is given in Section 3.5. We discuss several applications of this result to rational distance problems in Section 1.2, but mention one here as a representative example.

Corollary 1.5. *On any line of the form $x = 0$ or $y = \frac{2t}{1-t^2}x$ for $t \in \mathbb{Q} \setminus \{-1, 0, 1\}$, there exists a dense set of points with rational distance from each of $(0, 0)$, $(0, 1)$, and $(1, 1)$.*

In fact we prove a stronger result: there is an infinite collection of curves C_n in the plane such that the intersection points of the curves C_n with any fixed line $y = \frac{2t}{1-t^2}x$ (for $t \in \mathbb{Q} \setminus \{-1, 0, 1\}$) gives a dense set of solutions to the three-distance problem within the given line (Corollary 5.4).

Even in the cases where $(-1, r) \in E_{r,s}(\mathbb{Q})$ is torsion, there are still several cases in which we can prove $E_{r,s}(\mathbb{Q})$ has positive rank. We discuss these in more depth in Section 5.4, but note one special case here. Let

$$\mathcal{S}' = \{\alpha \in \mathbb{Q} : \sqrt{\alpha^2 + 1} \in \mathbb{Q}\}$$

denote the set of slopes of rational right triangles (including negatives and zero).

Proposition 1.6. *For all $t \in \mathbb{Q}$, the equations $x_1 + x_2 + x_3 = t$ and $x_1x_2x_3 = t$ each have an infinite set of solutions with $x_1, x_2, x_3 \in \mathcal{S}'$.*

See Section 5.4 for a proof.

1.2. Rational configuration problems

Given a finite simple graph $G = (V, E)$, an embedding $\phi : V \hookrightarrow \mathbb{R}^n$ is a *rational configuration* if the distance $d(\phi(v), \phi(w))$ is rational for all $(v, w) \in E$. We may add some additional constraints to the set of allowable embeddings (for instance, we may require some pairs of edges to be the same length, or to meet at right angles), and in doing so we obtain a corresponding *rational configuration problem*: to determine whether there exists a rational configuration satisfying the desired constraints, and if so, to classify or count the number of rational configurations. We describe a list of sample rational configurations below; the corresponding graphs can be found in Table 1.

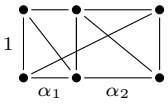
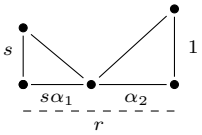
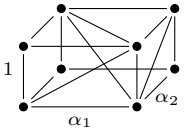
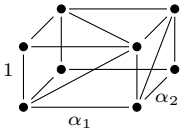
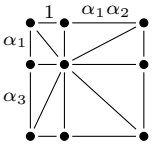
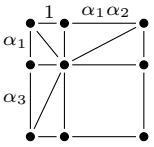
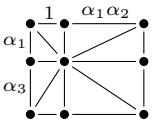
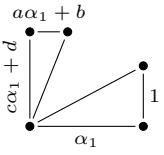
- "Adjacent rectangles:" Find two rectangles sharing an edge such that the distance between any two vertices is rational.
- "Detour:" Fix parameters $r, s, t \in \mathbb{Q}^\times$. Find a point x such that $(x, 0)$ has rational distance to $(0, 0)$, $(r, 0)$, $(0, s)$, and (r, t). (A traveller is going from $(0, s)$ to (r, t), but has to take a detour to stop at the x-axis along the way; can they do so using only two straight paths of rational length?)
- "Perfect cuboid:" Find a rectangular prism such that the distance between any two vertices is rational.
- "Body cuboid:" Find a rectangular prism such that the distance between any two vertices that share a face is rational.
- "Square four-distance:" Find a point $(x, y) \in \mathbb{R}^2$ such that the distance to each of $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$ is rational.
- "Square three-distance:" Find a point $(x, y) \in \mathbb{R}^2$ such that the distance to each of $(0, 0)$, $(0, 1)$, and $(1, 1)$ is rational.
- "Rectangle four-distance:" Find $r \in \mathbb{Q}^\times$ and a point $(x, y) \in \mathbb{R}^2$ such that the distance to each of $(0, 0)$, $(0, 1)$, $(r, 0)$, and $(r, 1)$ is rational.
- "Rational distances under Möbius transformation:" Fix $a, b, c, d \in \mathbb{Q}$ with $ad - bc \neq 0$. Find $z \in \mathbb{C}$ such that z and $\frac{az+b}{cz+d}$ both have rational distance from 0.

The perfect cuboid problem and square four-distance problem are classic unsolved problems (see Section 2); this paper does not present a solution to either of them. However, we can put all the remaining problems in this list into a common framework. Define

$$\mathcal{S} = \{(u : v) \in \mathbb{P}^1(\mathbb{Q}) \mid \sqrt{u^2 + v^2} \in \mathbb{Q}\},$$

so that whenever u, v, not both zero, are the legs of a (possibly degenerate) rational right triangle, the slope of the triangle is in $\mathcal{S}$. Then for distinct $P_1, P_2 \in \mathbb{Q}^2$, the distance between P_1 and P_2 is rational if and only if the line between P_1 and P_2 has slope in $\mathcal{S}$. Using this observation, we can parametrize solutions to many rational configuration problems by finding elements of $\mathcal{S}$ satisfying simple polynomial relations. We let $\mathcal{S}' = \mathcal{S} \cap \mathbb{Q}$ (that is, the set of $(u : v) \in \mathcal{S}$ with $v \neq 0$; note that this agrees with the previous definition of $\mathcal{S}'$), and $\mathcal{S}^\times = \mathcal{S} \cap \mathbb{Q}^\times$ (the set of $(u : v) \in \mathcal{S}$ with $uv \neq 0$).

Table 1
Diagrams of rational distance problems. Rational configurations are given by solutions to the given equation with $\alpha_i \in \mathcal{S}'$ for all i. By Proposition 1.9, some of these configurations are parametrized by rational points on a curve H_η. If a distinguished rational point on H_η is known, then the isomorphic elliptic curve $E_{r,s}$ is given (Proposition 1.3), and labeled with ∞ in the cases that $E_{r,s}(\mathbb{Q})$ is known to be infinite.

Configuration	Graph	Equation	Solutions given by
Adjacent rectangles		$\alpha_1 + \alpha_2 = \alpha_3$	$E_{\alpha_3,1}(\mathbb{Q})$ (∞ for all $\alpha_3 \in \mathcal{S}'$: Proposition 5.5)
Detour ($r, s \in \mathbb{Q}^\times$)		$s\alpha_1 + \alpha_2 = r$	$E_{r,s}(\mathbb{Q})$ (∞ if $\lvert s\rvert \neq 1$ and $4r^2s \neq \pm(1-s^2)^2$: Theorem 1.4)
Perfect cuboid		$\alpha_1^2 + \alpha_2^2 = \alpha_3^2$	Unknown
Body cuboid		$\alpha_1\alpha_3 = \alpha_2$	$E_{0,\alpha_3}(\mathbb{Q})$
(Square) Four-distance		$\alpha_1\alpha_2 = \alpha_3\alpha_4 = \alpha_1 + \alpha_3 - 1$	Unknown
(Square) three-distance		$\alpha_1\alpha_2 = \alpha_1 + \alpha_3 - 1$	$E_{-1,1-\alpha_3}(\mathbb{Q})$ (∞ for all $\alpha_3 \in \mathcal{S}'$: Corollary 1.5)
(Rectangle) four-distance		$\alpha_1\alpha_2 = \alpha_3\alpha_4$	$E_{0,\alpha_3\alpha_4}(\mathbb{Q})$
Rational distances under Möbius transformation, $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$		$(a\alpha_1 + b)\alpha_2 = (c\alpha_1 + d)$	$H_\eta(\mathbb{Q})$

Example 1.7. Given a hypothetical solution to the perfect cuboid problem, we can scale the solution so that one edge length has length 1; this implies there exist $\alpha_1, \alpha_2 \in \mathbb{Q} \setminus \{0\}$ such that

$$1+\alpha_1^2, \quad 1+\alpha_2^2, \quad \alpha_1^2+\alpha_2^2, \quad \text{and} \quad 1+\alpha_1^2+\alpha_2^2$$

are all perfect squares. If we set $\alpha_3 = \sqrt{\alpha_1^2+\alpha_2^2}$, then the polynomial constraints above are equivalent to requiring

$$\alpha_1^2+\alpha_2^2=\alpha_3^2 \qquad \text{for some } \alpha_1,\alpha_2,\alpha_3 \in \mathcal{S}'.$$

Allowing any $\alpha_i = 0$ gives a degenerate solution, so we really require $\alpha_1,\alpha_2,\alpha_3 \in \mathcal{S}^\times$.

Example 1.8. Given a hypothetical solution x to the "detour" problem, we can scale the solution so that $t = 1$. If we set $\alpha_1 := \frac{x}{s}$ and $\alpha_2 = r - s\alpha_1$, then each pair $(s, s\alpha_1)$ and $(\alpha_2, 1)$ forms the legs of a rational right triangle, so $\alpha_1,\alpha_2 \in \mathcal{S}^\times$ satisfy $s\alpha_1+\alpha_2 = r$. Conversely, given $\alpha_1,\alpha_2 \in \mathcal{S}^\times$ with $s\alpha_1+\alpha_2 = r$, we obtain a detour solution with $x = s\alpha_1$.

Similar polynomial constraints for each of the problems above are listed in Table 1. For every problem in Table 1 besides the perfect cuboid problem and the square four-distance problem, rational configurations correspond to solutions in $\mathcal{S}$ to a single polynomial in multiple variables that is linear in each variable.

Proposition 1.9. *Let* $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$*, and let* F_η *be the curve in* $\mathbb{P}^1 \times \mathbb{P}^1$ *defined by*

$$F_\eta : ax_1x_2 + bx_1z_2 + cz_1x_2 + dz_1z_2 = 0.$$

There is a degree 4 *morphism* $\Phi : H_\eta \to F_\eta$ *inducing a surjection*

$$H_\eta(\mathbb{Q}) \to F_\eta(\mathbb{Q}) \cap (\mathcal{S} \times \mathcal{S}).$$

This follows from Proposition 5.1. Proposition 1.9 shows that for a wide collection of problems, rational configurations can be classified using rational points on curves of the form H_η. We can use this observation to show that some rational configuration problems have infinitely many rational configurations. In some cases, such as the detour problem and the square three-distance problem, the infinitude of solutions will be a consequence of Theorem 1.4. For others, including the adjacent rectangles, body cuboid, and rectangle four-distance problems, the corresponding curve $E_{r,s}$ lands in one of the exceptional cases of Theorem 1.4, and so we cannot immediately conclude that there are infinitely many solutions.

1.3. Outline

We begin with a discussion of some related problems and their histories in Section 2. In Section 3 we analyze the algebraic structure of the family H_η, in particular showing

that the isomorphism type of H_η is invariant under a left- and right-action of the orthogonal group (Section 3.3). We then analyze the singular fibers (Section 3.4), followed by the non-singular fibers that contain a rational point (Section 3.5), proving that most fibers of this type have infinitely many rational points (Theorem 1.4). Completing our study of rational points on the fibers, Section 4 contains a proof the set of fibers containing a rational point has low density (Theorem 1.1). Note that Section 4 only requires Section 3.1 and Section 3.2 from Section 3.

We conclude with some applications of these results in Section 5, focusing primarily on the square three-distance problem.

2. Prior work on related problems

There are a number of open problems regarding rational configurations; in this section we will focus on two of them, namely the perfect cuboid problem in Section 2.1 and the square four-distance problem in Section 2.2 (both of these are discussed at greater length in [9]). In each case, we show that the problem is equivalent to the existence of a Pythagorean solution of a certain polynomial or system of polynomials. Finally, in Section 2.3, we compare to the congruent number problem.

2.1. Perfect cuboid problem

While the perfect cuboid problem is open, significant progress has been made towards studying the "body cuboid" problem, which is to give a cuboid in which all edges and all face diagonals (but not necessarily the body diagonal) have rational lengths. If $1, \alpha_1, \alpha_2$ are the edge lengths of a body cuboid, then $\alpha_1^2 + 1$, $\alpha_2^2 + 1$, and $\alpha_1^2 + \alpha_2^2$ are all perfect squares; the first two conditions say that $\alpha_1, \alpha_2 \in \mathcal{S}^\times$ and the third is equivalent to requiring $\frac{\alpha_2}{\alpha_1} \in \mathcal{S}^\times$.

For each fixed $\alpha_3 \in \mathcal{S}^\times$, the values $\alpha_1, \alpha_2 \in \mathcal{S}^\times$ satisfying $\alpha_1\alpha_3 = \alpha_2$ are parametrized by an elliptic curve (Proposition 1.9 and Proposition 1.3). This association between body cuboids and a family of elliptic curves is well-studied; van Luijk has an in-depth survey [14] that mentions this association as well as many other known results about perfect cuboids. Halbeisen and Hungerbühler [10] investigate this problem as well. Given a fixed $\alpha_3 = \frac{b}{a}$, they associate solutions $\alpha_1, \alpha_2 \in \mathcal{S}'$ satisfying $\alpha_1\alpha_3 = \alpha_2$ to rational points on the elliptic curve

$$E : y^2 = x^3 + (a^2 + b^2)x^2 + a^2b^2x. \tag{2}$$

Proposition 1.9 and Proposition 1.3 recovers this classification. They show that there is a subgroup of $E(\mathbb{Q})$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ which give degenerate solutions to the corresponding rational distance problem. Ruling out other possible torsion points, they conclude [10, Theorem 8] that nondegenerate solutions exist if and only if $E(\mathbb{Q})$ has positive rank. In this case they call (a, b) a *double-pythapotent pair*.

2.2. Four-distance problem

As with the perfect cuboid problem, the four-distance problem is currently out of reach, but a slightly weaker variant has many known solutions. The three-distance problem is to find points $P = (x, y) \in \mathbb{R}^2$ with rational distance to $(0, 0)$, $(0, 1)$, and $(1, 1)$. The coordinates x, y are not a priori assumed to be rational, but since $x^2 + y^2$, $x^2 + (1 - y)^2$, and $(1 - x)^2 + (1 - y)^2$ must all be rational, the differences $2y - 1$ and $2x - 1$ must also be rational, so in fact $P \in \mathbb{Q}^2$. We can then scale by an element of $\mathbb{Q}^\times$ so that $x = 1$, and a solution to the square three-distance problem is equivalent to the existence of $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{S}^\times$ satisfying $1 + \alpha_1\alpha_2 = \alpha_1 + \alpha_3$.

For many years it was believed that there were no solutions to the three-distance problem aside from points on the coordinate axes. The first one-parameter family of nontrivial solutions was found in 1967 by J.H. Hunter, and then many more infinite families were found in rapid succession; a historical overview is given by Berry, who also presents an "extraordinary abundance" of solutions lying in infinitely many one-parameter families [3]. We observe that the families of solutions obtained in Corollary 1.5 are distinct from those that appear in [3, Table 4], though it is unclear whether any (or all) of the one-parameter families we consider are eventually accounted for by Berry's construction.

2.3. Congruent number problem

A rational number $n \in \mathbb{Q}$ is a *congruent number* if it is the area of a right triangle with rational edge lengths; that is, if there is a solution to

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}ab = n, \qquad a, b, c \in \mathbb{Q}^\times. \tag{3}$$

The "congruent number problem" is to determine whether a given $n \in \mathbb{Q}$ is a congruent number. This problem is not a rational configuration problem, but the underlying methods used to study these two problems are similar enough that a comparison is worthwhile.

There is a well-known approach to studying the congruent number problem; see for example the expositions [6] and [5]. For fixed n, any solution to Eq. (3) corresponds to a rational point on an elliptic curve over $\mathbb{Q}$ defined by

$$E^{(n)} : y^2 = x^3 - n^2x. \tag{4}$$

There are "degenerate points" in $E^{(n)}(\mathbb{Q})$ that do not correspond to solutions; it can be shown that the set of degenerate points equals the torsion subgroup of $E^{(n)}(\mathbb{Q})$. Thus n is a congruent number if and only if $E^{(n)}(\mathbb{Q})$ has positive rank. A formula due to Tunnell can be used to determine whether the analytic rank of $E^{(n)}$ is zero or positive [17], so by assuming the Birch and Swinnerton-Dyer conjecture, this gives a criterion that determines whether a given number is congruent.

Many aspects of this paper are modeled off of the approach described for studying the congruent number problem. To put the two problems on a common footing, note that n is a congruent number if and only if $x_1 = a^2$ and $x_2 = \frac{b}{a}$ give a solution to

$$x_1 x_2 - 2n = 0, \qquad x_1 \in (\mathbb{Q}^\times)^2,\ x_2 \in \mathcal{S}^\times. \tag{5}$$

Both $\mathcal{S}'$ and $(\mathbb{Q}^\times)^2$ can be represented as the image of $\mathbb{A}^1(\mathbb{Q})$ under the image of a degree 2 rational map $\mathbb{A}^1 \to \mathbb{A}^1$. The curve $E^{(n)}$ comes equipped with a degree 4 rational map to the variety defined by $x_1 x_2 - 2n = 0$, and non-degenerate points in $E^{(n)}(\mathbb{Q})$ map to solutions to Eq. (5). This is directly analogous to the relation between $H_\eta(\mathbb{Q})$ and solutions to rational distance problems (Proposition 1.9).

However, it is worth highlighting a few key differences between the congruent number problem and the family of rational distance problems we consider.

- **Size of parameter space.** The isomorphism class of $E^{(n)}$ is determined by the class of n in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, while the isomorphism class of H_η is determined by the class of a corresponding matrix in a double quotient of $\mathrm{GL}_2(\mathbb{Q})$.
- **Existence of rational points.** Every n determines an elliptic curve $E^{(n)}$, which has a rational point. By contrast, the genus one curves H_η typically have no rational points (Theorem 1.1).
- **Closure under addition of degenerate points.** In both problems, the corresponding genus one curve has a set of "degenerate" rational points, which do not yield valid solutions to the original problem. For the congruent number problem, the set of degenerate points equals the torsion subgroup of $E^{(n)}(\mathbb{Q})$. For rational configuration problems, however, even if H_η is isomorphic to an elliptic curve (Proposition 1.3), the degenerate points in $H_\eta(\mathbb{Q})$ may not form a subgroup. This is to our advantage: we can often add together degenerate points to produce non-degenerate points, something that is not possible in the congruent number problem. This is the key idea behind Theorem 1.4.
- **Geometric variation in the family.** The curves $E^{(n)}$ are quadratic twists of the curve $y^2 = x^3 - x$, and are therefore all isomorphic over $\overline{\mathbb{Q}}$. This fact is used in a key way in the proof of Tunnell's theorem, as he applies a result due to Waldspurger [18] relating the central value of the L-function of an elliptic curve with that of each of its quadratic twists. By contrast, the curves H_η do not have constant j-invariant. This means that Tunnell's approach to computing the analytic rank does not apply to this family.

3. The structure of the family

3.1. Assumptions and notation

Let K be a field of characteristic not equal to 2, in which -1 is not a square; later we will restrict to $K = \mathbb{Q}$, but many of our results hold in more generality. Throughout

this paper, all schemes will be defined over K unless otherwise indicated, and if X and Y are schemes then $X \times Y := X \times_K Y$.

Throughout, $\mathbb{P}^1$ will denote the projective line over K, while $\mathbb{P}^2$ will denote a *weighted* projective space over K, where the variables x, y, z have weights $1, 2, 1$, respectively. We use the notation $(x : z)$ and $(x : y : z)$ to denote elements of $\mathbb{P}^1(K)$ and $\mathbb{P}^2(K)$, respectively. That is, for $(x, z) \in K^2 \setminus \{(0, 0)\}$ we have

$$(x : z) = \{(\lambda x : \lambda z) \mid \lambda \in K^\times\},$$

and for $(x, y, z) \in K^3 \setminus \{(0, 0, 0)\}$ we have

$$(x : y : z) = \{(\lambda x, \lambda^2 y : \lambda z) \mid \lambda \in K^\times\}.$$

Let $\mathrm{GL}_2 = \operatorname{Spec} K[a, b, c, d, (ad - bc)^{-1}]$ denote the algebraic group of 2×2 invertible matrices, with identity element I. Given a matrix $\eta \in \mathrm{GL}_2(K)$, its transpose will be denoted η^t. Let O_2 denote the orthogonal group of 2×2 matrices, that is, the algebraic subgroup of GL_2 defined by the condition that $M \in \mathrm{GL}_2(\overline{K})$ is in $\mathrm{O}_2(\overline{K})$ if and only if $MM^t = M^t M = I$.

3.2. Definition of $\mathcal{H}$ and basic properties

We first define a variety $\mathcal{H}_0$ in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathrm{GL}_2$. Using the coordinates $\left((x_1 : z_1), (x_2 : z_2), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)$, this variety is given by

$$\mathcal{H}_0 : \begin{pmatrix} z_1^2 - x_1^2 & 2x_1 z_1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_2^2 - x_2^2 \\ 2x_2 z_2 \end{pmatrix} = 0. \tag{6}$$

This variety comes equipped with a morphism $\pi_0 : \mathcal{H}_0 \to \mathrm{GL}_2$, which equips $\mathcal{H}_0$ with the structure of a flat family of curves. As a biquadratic form in $\mathbb{P}^1 \times \mathbb{P}^1$ over GL_2, the projection onto either component gives $\mathcal{H}_0$ the structure of a hyperelliptic curve. For now we consider the projection onto the second component, and provide an isomorphic model written in the standard form for a hyperelliptic curve as a double cover of $\mathbb{P}^1$. This can be given as a variety in $\mathbb{P}^2 \times \mathrm{GL}_2$. Using the coordinates $\left((x : y : z), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)$, and letting $N : K^2 \to K$ be defined by $N(u, v) = u^2 + v^2$, set

$$\begin{aligned} \mathcal{H} : y^2 &= N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix}\right) \\ &= (a(z^2 - x^2) + b(2xz))^2 + (c(z^2 - x^2) + d(2xz))^2. \end{aligned} \tag{7}$$

The variety $\mathcal{H}$ also comes equipped with a natural map $\pi : \mathcal{H} \to \mathrm{GL}_2$. Observe that given $\eta \in \mathrm{GL}_2(K)$, H_η as defined in Eq. (1) is the fiber of π over η. The fact that $\mathcal{H}_0 \simeq \mathcal{H}$ is a consequence of the fact that both equations express the property that the components of

the vector $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z^2-x^2 \\ 2xz \end{smallmatrix}\right)$ are the sides of a (possibly degenerate) rational right triangle. An explicit isomorphism $\mathcal{H} \to \mathcal{H}_0$ as varieties over GL_2 is given by

$$(x : y : z) \mapsto \big((a(z^2 - x^2) + b(2xz) : y - c(z^2 - x^2) - d(2xz)), (x : z))\big).$$

The generic fiber of $\pi : \mathcal{H} \to \mathrm{GL}_2$ is a genus one hyperelliptic curve over the function field $K(a, b, c, d)$, with discriminant

$$\Delta(\mathcal{H}) = 2^{16}(ad - bc)^4((a + d)^2 + (b - c)^2)((a - d)^2 + (b + c)^2). \tag{8}$$

The Jacobian variety of this curve is an elliptic curve over $K(a, b, c, d)$, which by classical invariant theory (see for example [19,2]) has a model

$$E : y^2 = x^3 + (a^2 + b^2 + c^2 + d^2)x^2 + (ad - bc)^2 x. \tag{9}$$

The two commuting involutions on $\mathcal{H}_0$ as a scheme over GL_2 induce commuting involutions on $\mathcal{H}$, given by

$$\sigma_1 : (x : y : z) \mapsto (x : -y : z) \qquad \text{and} \qquad \sigma_2 : (x : y : z) \mapsto (-z : y : x). \tag{10}$$

These generate a Klein four-group

$$\Gamma := \langle \sigma_1, \sigma_2 \rangle \tag{11}$$

acting on $\mathcal{H}$.

3.3. Double cosets and reduction

We show that the isomorphism class of H_η for $\eta \in \mathrm{GL}_2(K)$ is invariant on double cosets in

$$\mathrm{O}_2(K) \backslash \mathrm{GL}_2(K) / (K^\times \cdot \mathrm{O}_2(K)),$$

and use this to show that H_η has a K-point if and only if η is in the same double coset as $\left(\begin{smallmatrix} 1 & r \\ 0 & s \end{smallmatrix}\right)$ for some $r, s \in K$.

Invariance under $K^\times$ is clear. The fact that the isomorphism class is preserved under left multiplication by elements of $\mathrm{O}_2(K)$ is evident from Eq. (7), and the corresponding fact for right multiplication follows from the fact that we have an isomorphism with the model

$$y^2 = N\left(\begin{pmatrix} z^2 - x^2 & 2xz \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$$

We summarize these observations in the following lemma, though we also include an explicit formula for the isomorphism in the proof.

Lemma 3.1. *Let $\eta, \eta' \in \mathrm{GL}_2(K)$. If $\eta' \in K^\times \mathrm{O}_2(K)\eta\,\mathrm{O}_2(K)$, then there is an isomorphism $\tau : H_\eta \to H_{\eta'}$ over K that commutes with the action of Γ.*

Proof. Let $\eta' = \lambda r_1 \eta r_2^{-1}$, where $\lambda \in K^\times$ and $r_1, r_2 \in \mathrm{O}_2(K)$. Write $r_2 = \left(\begin{smallmatrix} u & -v \\ \epsilon v & \epsilon u \end{smallmatrix}\right)$, where $u, v \in K$, $\epsilon = \pm 1$, and $u^2 + v^2 = 1$. There exists $s, t \in K$ so that $u = \frac{t^2 - s^2}{t^2 + s^2}$ and $v = \frac{2st}{t^2+s^2}$. Then for any $(x : y : z) \in H_\eta(\overline{K})$,

$$\begin{aligned}(\lambda(s^2+t^2)y)^2 &= N\left(\lambda(s^2+t^2)\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz\end{pmatrix}\right) \\ &= N\left(r_1\lambda\begin{pmatrix} a & b \\ c & d\end{pmatrix} r_2^{-1}\begin{pmatrix} t^2 - s^2 & -2st \\ 2\epsilon st & \epsilon(t^2 - s^2)\end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz\end{pmatrix}\right) \\ &= N\left(\lambda r_1\begin{pmatrix} a & b \\ c & d\end{pmatrix} r_2^{-1}\begin{pmatrix} (tz - sx)^2 - (tx + sz)^2 \\ 2\epsilon(tz - sx)(tx + sz)\end{pmatrix}\right).\end{aligned}$$

Thus the map

$$\tau : (x : y : z) \mapsto (\epsilon(tx + sz) : \lambda(s^2 + t^2)y : tz - sx)$$

defines an isomorphism $H_\eta \to H_{\eta'}$, and the involutions $y \mapsto -y$ and $(x : z) \mapsto (-z : x)$ are preserved. □

Given $\eta \in \mathrm{GL}_2(K)$, suppose η is in the same double coset as an element of the form $\eta' = \left(\begin{smallmatrix} 1 & r \\ 0 & s\end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. We have $(0 : 1 : 1) \in H_{\eta'}(K)$, so by Lemma 3.1, we can conclude that $H_\eta(K)$ is nonempty. The following lemma gives us the converse result: if $H_\eta(K)$ is nonempty then η is in the same double-coset as a matrix of the form $\eta' = \left(\begin{smallmatrix} 1 & r \\ 0 & s\end{smallmatrix}\right)$.

Lemma 3.2. *Let $\eta = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Suppose there is a point $P = (x_0 : y_0 : z_0) \in H_\eta(K)$. Define*

$$\begin{aligned} r &:= \frac{(ab + cd)((z_0^2 - x_0^2)^2 - (2x_0z_0)^2) - (a^2 - b^2 + c^2 - d^2)(z_0^2 - x_0^2)(2x_0z_0)}{y_0^2}, \\ s &:= \frac{(ad - bc)(z_0^2 + x_0^2)^2}{y_0^2}. \end{aligned} \tag{12}$$

Then $\eta \in K^\times \mathrm{O}_2(K)\left(\begin{smallmatrix} 1 & r \\ 0 & s\end{smallmatrix}\right)\mathrm{O}_2(K)$.

Proof. Suppose $x_0^2 + z_0^2 = 0$. If $z_0 \neq 0$, then $\left(\frac{x_0}{z_0}\right)^2 = -1$, contradicting the assumption that -1 is not a square in K. Hence $z_0 = 0$, and likewise $x_0 = 0$. But this implies $y_0 = 0$, which contradicts the fact that $(x_0 : y_0 : z_0) \in \mathbb{P}^2(K)$.

If $y_0 = 0$, then a similar argument shows that we must have

$$a(z_0^2 - x_0^2) + b(2x_0z_0) = c(z_0^2 - x_0^2) + d(2x_0z_0) = 0.$$

But this implies that the nonzero vector $(z_0^2 - x_0^2, 2x_0z_0)$ is in the kernel of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, contradicting the assumption that $\eta \in \mathrm{GL}_2(K)$. Hence $y_0 \neq 0$.

Since $x_0^2 + z_0^2 \neq 0$ and $y_0 \neq 0$, the matrices

$$r_1 = \frac{1}{y_0}\begin{pmatrix} a(z_0^2 - x_0^2) + b(2x_0z_0) & c(z_0^2 - x_0^2) + d(2x_0z_0) \\ -c(z_0^2 - x_0^2) - d(2x_0z_0) & a(z_0^2 - x_0^2) + b(2x_0z_0) \end{pmatrix}$$
$$r_2 = \frac{1}{z_0^2 + x_0^2}\begin{pmatrix} z_0^2 - x_0^2 & -2x_0z_0 \\ 2x_0z_0 & z_0^2 - x_0^2 \end{pmatrix}$$

are both well-defined elements of $\mathrm{SO}_2(K)$. We can check by direct computation that $\frac{z_0^2+x_0^2}{y_0} r_1 \eta r_2 = \left(\begin{smallmatrix} 1 & r \\ 0 & s \end{smallmatrix}\right)$. □

3.4. Isomorphism classes of fibers

The curve H_η is singular when the discriminant (Eq. (8)) vanishes. Since $ad - bc \neq 0$ for all $\eta \in \mathrm{GL}_2(K)$ and K does not contain a square root of -1, this can only occur if $a = -d$ and $b = c$, or if $a = d$ and $b = -c$. One of these two conditions holds if and only if $a^2 + b^2 = c^2 + d^2$ and $ac + bd = 0$; thus the singular fibers H_η are exactly those with

$$\eta\eta^t = (a^2 + b^2)I.$$

In this case H_η reduces to the form

$$y^2 = (a^2 + b^2)(z^2 + x^2)^2.$$

If $a^2 + b^2 = \lambda^2$ then H_η splits into two conics, $y = \pm\lambda(z^2 + x^2)$. If $a^2 + b^2$ is not a square in K, then there are no solutions in $\mathbb{P}^2(K)$.

If H_η has a rational point and the discriminant (Eq. (8)) does not vanish at η, then H_η is isomorphic to its Jacobian. Using Lemma 3.2 and Eq. (9), we can conclude that H_η is isomorphic to

$$E_{r,s} : y^2 = x^3 + (1 + r^2 + s^2)x^2 + s^2x$$

for some $r, s \in K$; the non-vanishing of the discriminant says that $s \neq 0$ and $(r, s) \neq (0, \pm 1)$. This completes the proof of Proposition 1.3.

3.5. Nonsingular fibers with a rational point

We now restrict our attention to $K = \mathbb{Q}$ in order to prove Theorem 1.4, which we recall for convenience.

Theorem 1.4. *Let $r, s \in \mathbb{Q}$ with $s \neq 0$ and $(r, s) \neq (0, \pm 1)$. The point $(-1, r) \in E_{r,s}(\mathbb{Q})$ is non-torsion if and only if $r \neq 0$, $s \neq \pm 1$, and $4r^2s \neq \pm(1 - s^2)^2$.*

Proof. Assume $R := (-1, r)$ is torsion in $E_{r,s}(\mathbb{Q})$. Since $x^2 + (1 + r^2 + s^2)x + s^2$ is positive on an open interval around $x = 0$, there exists $-1 < x < 0$ for which $E_{r,s}(\mathbb{R})$ does not contain any point of the form (x, y). Thus $E_{r,s}(\mathbb{R})$ has two components, with $R := (-1, r)$ on the non-identity component and $T := (0, 0)$ on the identity component. This shows R is not a multiple of 2 in $E_{r,s}(\mathbb{R})$, and hence R cannot have odd order. By Mazur's classification of torsion subgroups, we can conclude that if R is torsion then its order must be an even number at most 12. If R has order 10 then the only possibility for the torsion subgroup of $E_{r,s}(\mathbb{Q})$ is $\mathbb{Z}/10\mathbb{Z}$, so that T is the unique element of order 2. This implies $T = 5R$, which again leads to a contradiction when we consider the component group of $E_{r,s}(\mathbb{R})$.

We can conclude that if R is torsion, it must have order $\ell \in \{2, 4, 6, 8, 12\}$. For each such ℓ, let $\psi_\ell(r, s, x) \in \mathbb{Z}[r, s, x]$ denote the ℓ-th division polynomial on $E_{r,s}$; this is a polynomial with the property that $\psi_\ell(r, s, x) = 0$ for $x \in \overline{\mathbb{Q}}$ if and only if $(x, y) \in E_{r,s}(\overline{\mathbb{Q}})[\ell]$ for some $y \in \overline{\mathbb{Q}}$ (see for instance [16, Exercise 3.7]). We compute the division polynomial $\psi_\ell(r, s, x)$, and determine all possible $(r, s) \in \mathbb{Q}^2$ such that $\psi_\ell(r, s, -1) = 0$.

- We have $\psi_2(r, s, -1) = -r^2$, so R has order 2 if and only if $r = 0$.
- We have

$$\frac{\psi_4(r, s, -1)}{\psi_2(r, s, -1)} = -2(s - 1)(s + 1)(2r^2s^2 + 2r^2 + (s^2 - 1)^2).$$

  The last factor is a sum of non-negative terms, including at least one positive term because $(r, s) \neq (0, \pm 1)$. Hence R has order 4 if and only if $s = \pm 1$.
- The quotient of $\psi_6(r, s, -1)$ by $\psi_2(r, s, -1)\psi_3(r, s, -1)$ factors into two irreducible polynomials in $\mathbb{Q}[r, s]$. The first factor is $4r^2s^2 + (s^2 - 1)^2$, which is positive for all $(r, s) \neq (0, \pm 1)$. The second factor is

$$16s^2r^4 - 4(s^2 - 1)^2(s^2 + 1)r^2 - 3(s^2 - 1)^4.$$

  Considering this as a quadratic polynomial in r^2, the discriminant is equal to

$$16(s^2 - 1)^4(s^4 + 14s^2 + 1).$$

  In order for r^2 to be rational (let alone r), this discriminant must equal a rational square. Thus we consider rational points on the curve C defined by $y^2 = s^4 + 14s^2 + 1$. There are eight rational points $(s, y) \in C(\mathbb{Q})$: two at infinity, as well as $(-1, \pm 4)$, $(0, \pm 1)$, and $(1, \pm 4)$. Using the Weierstrass form $y^2 = x^3 - 7x^2 + 12x$ for C we can confirm that C has no other rational points, so the only possibilities for s are $-1, 0, 1$. If $s = 0$ then we have $r^2 = -\frac{3}{4}$, yielding no rational solutions. If $s = \pm 1$ then we have $r = 0$, contradicting $(r, s) \neq (0, \pm 1)$.
- The quotient of $\psi_8(r, s, -1)$ by $\psi_4(r, s, -1)$ factors into three irreducible polynomials in $\mathbb{Q}[r, s]$. The first two factors are $4r^2s - (s^2 - 1)^2$ and $4r^2s + (s^2 - 1)^2$; these each have infinitely many rational solutions. The third factor is positive for all $(r, s) \neq (0, \pm 1)$.

- If we eliminate common factors with $\psi_6(r,s,-1)$ and $\psi_4(r,s,-1)$ from $\psi_{12}(r,s,x)$, we are left with three irreducible polynomials in $\mathbb{Q}[r,s]$. The first factor is

$$16s(s^2-s+1)r^4+8s(s^2-1)^2r^2+(s^2-1)^4.$$

  Considered as a quadratic in r^2, the discriminant is $-64s(s-1)^6(s+1)^4$, which is a square if and only if $s=-k^2$ for some $k\in\mathbb{Q}$. Plugging this in and solving for r^2, we find that either

$$r^2=\frac{(k^4-1)^2}{4k(k^2+k+1)} \qquad \text{or} \qquad r^2=-\frac{(k^4-1)^2}{4k(k^2-k+1)}.$$

  For the first option, we obtain $r\in\mathbb{Q}$ if and only if k^3+k^2+k is a nonzero square. The only rational points on the elliptic curve $y^2=k^3+k^2+k$ are the point at infinity and $(k,y)=(0,0)$, so there is no $k\in\mathbb{Q}$ for which r is rational. For the second option, we obtain $r\in\mathbb{Q}$ if and only if $(-k)^3+(-k)^2+(-k)$ is a nonzero square, and by the same reasoning there is no such k. Hence this factor is nonzero for all $(r,s)\in\mathbb{Q}^2$. The second factor is obtained from the first by $s\mapsto -s$, so it has no rational solutions either. The third factor is positive for all $(r,s)\neq(0,\pm1)$.

To summarize, we obtain the following possibilities:

- $(-1,r)$ has order 2 if and only if $r=0$;
- $(-1,r)$ has order 4 if and only if $s=\pm1$;
- $(-1,r)$ has order 8 if and only if $4r^2s=\pm(1-s^2)^2$.
- There are no values of $(r,s)\in\mathbb{Q}^2$ for which $(-1,r)$ has any other finite order. □

4. Upper bound on locally soluble curves

In this section we prove Theorem 1.1. The main idea is to prove a local obstruction to the existence of $\mathbb{Q}_p$-points (Lemma 4.2). This obstruction is "large," in the sense that the proportion of curves satisfying the obstruction is approximately a constant multiple of $\frac{1}{p}$. By contrast, each local obstruction in Theorem 1.2 only affects $O(\frac{1}{p^2})$ of all curves. At a high level, the difference in behavior between the two families stems from the fact that $\sum\frac{1}{p}$ diverges but $\sum\frac{1}{p^2}$ converges.

Remark 4.1. While we have chosen to present a direct analytic argument for Theorem 1.1, one can also show that it follows from a result of Loughran and Smeets [12, Theorem 1.2], which computes an upper bound on the number of locally soluble fibers of a fibration $X\to\mathbb{P}^k$ in a very general setting. The key idea behind both results is that local solubility constraints arise from the existence of codimension 1 loci in the base over which the scheme splits into multiple geometric components. In the present case, this codimension

1 locus is given by the determinant locus $ad-bc$. Many thanks to the referee for informing the author of Loughran and Smeets' theorem.

4.1. Local obstructions

Given a ring A we use $M_2(A)$ to denote the ring of 2×2 matrices over A. For primes p we define

$$R_p := \{\eta \in M_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p) : H_\eta(\mathbb{Q}_p) = \emptyset\};$$

Thus $\mathcal{L}(X)$ counts the set of $\eta \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ with entries of absolute value at most X such that $\eta \notin R_p$ for all primes p (note that there is never a real obstruction: $H_\eta(\mathbb{R}) \neq \emptyset$ for all $\eta \in \mathrm{GL}_2(\mathbb{Q})$).

The main contribution to R_p will come from the following constraint.

Lemma 4.2. *Let p be an odd prime and $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p)$. Suppose $p \mid ad-bc$, and a, a^2+b^2, and a^2+c^2 are all nonzero mod p. Then $H_\eta(\mathbb{Q}_p)$ is nonempty if and only if at least one of a^2+b^2 or a^2+c^2 is a square modulo p.*

Proof. Assume $H_\eta(\mathbb{Q}_p)$ has a point $(x:y:z)$; without loss of generality we can assume that x, y, z are in $\mathbb{Z}_p$ and at least one of x, z is in $\mathbb{Z}_p^\times$. Reducing modulo p we have

$$a^2y^2 = (a^2+c^2)(a(z^2-x^2)+b(2xz))^2. \tag{13}$$

If $a(z^2-x^2)+b(2xz) \neq 0$, then a^2+c^2 is a square. On the other hand, suppose $a(z^2-x^2)+b(2xz) = 0$. Since $a \neq 0$ and at least one of x, z is nonzero we must have $xz \neq 0$, so

$$a^2+b^2 = a^2 + \left(\frac{-a(z^2-x^2)}{2xz}\right)^2 = \left(\frac{a(z^2+x^2)}{2xz}\right)^2$$

is a square.

Conversely, if a^2+c^2 is a nonzero square mod p then Eq. (13) clearly has solutions with $y \neq 0$; these are smooth points on $H_\eta(\mathbb{F}_p)$ so they lift to points on $H_\eta(\mathbb{Q}_p)$. If a^2+b^2 is a nonzero square mod p, then it is a square in $\mathbb{Q}_p$, so there exist $x, z \in \mathbb{Q}_p^\times$ with $\frac{b}{a} = \frac{x^2-z^2}{2xz}$. This implies $a(z^2-x^2)+b(2xz) = 0$, so $(x : c(z^2-x^2)+d(2xz) : z)$ is a point in $H_\eta(\mathbb{Q}_p)$. □

In light of the above, for all odd primes p set

$$\Omega_p := \left\{\mu = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_p) : ad-bc = 0,\ \left(\frac{a^2+b^2}{p}\right) = -1,\ \left(\frac{a^2+c^2}{p}\right) = -1\right\},$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. We also set $\Omega_2 = \emptyset$. If by abuse of notation we associate Ω_p with its preimage in $M_2(\mathbb{Z}_p)$ under reduction mod p, we have

$$(\Omega_p \cap \mathrm{GL}_2(\mathbb{Q}_p)) \subseteq R_p. \tag{14}$$

This follows from Lemma 4.2: note that the Legendre symbol conditions in the definition of Ω_p force a to be nonzero mod p.

Lemma 4.3. *We have* $|\Omega_p| = \frac{1}{4}p^3 + O(p^2)$.

Proof. We may assume p is odd. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Omega_p$. Since $a^2 + b^2$ is not a square, we have $a \neq 0$. Note that $a^2 + r^2$ is a square in $\mathbb{F}_p$ if and only if r is in the image of the map $\phi : \mathbb{F}_p^\times \to \mathbb{F}_p$ given by $\phi(t) = a\frac{1-t^2}{2t}$. We have $\phi(t) = \phi(s)$ if and only if $s = -\frac{1}{t}$, and so there are $\frac{1}{2}(p \pm 1)$ values in the range of ϕ (with the $\pm$ sign depending on whether or not -1 is a square mod p). Hence b and c must each be one of the $\frac{1}{2}(p \mp 1)$ values not in the range of ϕ. Since there are $p - 1$ choices for a, there are $\frac{1}{2}(p \mp 1)$ choices for each of b and c, and the value of $d = \frac{bc}{a}$ is fixed, we obtain the desired count. □

The following result is not used in the sequel, but justifies the claim that Ω_p is the main contribution to R_p.

Lemma 4.4. *Let* $\overline{R_p}$ *denote the image of* R_p *under reduction mod* p. *We have*

$$|\overline{R_p} \setminus \Omega_p| = O(p^2).$$

Proof. We may assume p is odd. We produce a collection of pairs of linear equations over $\mathbb{F}_p$ with the property that every element of $\overline{R_p} \setminus \Omega_p$ satisfies one of these pairs of equations. Let $\bar{\eta} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{F}_p)$. If

$$(ad - bc)((a-d)^2 + (b+c)^2)((a+d)^2 + (b-c)^2) \neq 0,$$

then for any lift $\eta \in M_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p)$, the discriminant of H_η (Eq. (8)) is not divisible by p, and so $H_\eta(\mathbb{F}_p)$ is nonempty by the Hasse-Weil bound. As these are all smooth points, they lift to points in $H_\eta(\mathbb{Q}_p)$. Thus $\bar{\eta}$ is not in $\overline{R_p}$.

We can therefore assume that exactly one of the following constraints holds:

(a) $ad - bc = 0$ and $a = 0$,
(b) $ad - bc = 0$ and $a \neq 0$,
(c) $ad - bc \neq 0$, $(a \mp d)^2 + (b \pm c)^2 = 0$, and $a \mp d = 0$,
(d) $ad - bc \neq 0$, $(a \mp d)^2 + (b \pm c)^2 = 0$ and $a \mp d \neq 0$.

In case (a) or (c), $\bar{\eta}$ must satisfy one of the following pairs of linear equations over $\mathbb{F}_p$:

$$a = b = 0, \qquad a = c = 0, \qquad \text{or} \qquad a \mp d = b \pm c = 0.$$

Now consider case (b). If $a^2 + b^2 = 0$ or $a^2 + c^2 = 0$, then using $a \neq 0$ and $ad = bc$ we can conclude that

$$a + ib = c + id = 0 \qquad \text{or} \qquad a + ic = b + id = 0$$

for some $i \in \mathbb{F}_p$ satisfying $i^2 = -1$. If on the other hand $a^2 + b^2$ and $a^2 + c^2$ are both nonzero, then $\bar{\eta}$ is not in $\overline{R_p}$ by Lemma 4.2.

Finally we consider case (d). We assume $(a-d)^2 + (b+c)^2 = 0$ and $a - d \neq 0$ as the other case is similar. Then $b + c = i(a-d)$ for some $i \in \mathbb{F}_p$ with $i^2 = -1$. The reduction of H_η modulo p is given by

$$y^2 = (z + ix)^2 h(x, z)$$

where

$$h(x, z) := (a^2 + c^2)(z^2 - x^2) + (2a(b + c) + i(c^2 - a^2 + 2bc))(2xz).$$

If the discriminant of $h(x, z)$ is nonzero, then the equation $r^2 = h(x, z)$ defines a smooth projective conic over $\mathbb{F}_p$, and there must exist at least one point (x, z, r) on this conic with $z + ix \neq 0$. Then $(x : (z + ix)r : z)$ defines a smooth point in $H_\eta(\mathbb{F}_p)$, which lifts to a point in $H_\eta(\mathbb{Q}_p)$. Hence $\bar{\eta}$ is not in $\overline{R_p}$. Computing the discriminant of $h(x, z)$, we find that elements in $\overline{R_p} \setminus \Omega_p$ in this case must satisfy

$$b + c - i(a - d) = (b - ia)(a + ic)(b + c) = 0. \quad \square$$

4.2. Proof of Theorem 1.1

The author would like to thank Sun-Kai Leung for suggesting the following proof.

Recall that $\mathcal{L}(X)$ is the set of all $\eta \in M_2(\mathbb{Z})$ with nonzero determinant, entries having absolute value at most X, and with $\eta \notin R_p$ for all p. Set

$$\mathcal{M}(X) := \{\eta \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q}) : \eta \notin \Omega_p \text{ for all primes } p\}.$$

By Eq. (14) we can see that $\mathcal{L}(X) \subseteq \mathcal{M}(X)$, and so it suffices to find an upper bound for $\mathcal{M}(X)$.

Set

$$\mathscr{S}(Y) := \sum_{m \leq Y} \mu^2(m) \prod_{\text{prime } p \mid m} \frac{|\Omega_p|}{p^4 - |\Omega_p|},$$

where $\mu(m)$ is the Möbius function (so $\mu^2(m) = 1$ if m is squarefree and $\mu^2(m) = 0$ otherwise). Applying the n-dimensional large sieve [8, Lemma B], we obtain

$$|\mathcal{L}(X)| \leq |\mathcal{M}(X)| \ll \frac{X^4}{\mathscr{S}(\sqrt{X})},$$

where $f(X) \ll g(X)$ means that for some positive constant C we have $f(X) < Cg(X)$ for sufficiently large X. Theorem 1.1 follows immediately from this bound after applying the following lemma.

Lemma 4.5. *We have*

$$\mathscr{S}(Y) \gg (\log Y)^{1/4}.$$

Proof. We have $|\Omega_p| \geq 0$, and by Lemma 4.3 we have $|\Omega_p| \geq \frac{1}{4}(p^3 - Cp^2)$ for some positive constant C, so

$$\begin{aligned}\mathscr{S}(Y) &\geq \sum_{m \leq Y} \mu^2(m) \prod_{p \mid m} \frac{p^3 - Cp^2}{4p^4} \\ &= \sum_{m \leq Y} \frac{\mu^2(m)}{m} \prod_{p \mid m} \frac{1}{4}\left(1 - \frac{C}{p}\right).\end{aligned}$$

Set

$$f(m) := \mu^2(m) \prod_{p \mid m} \frac{1}{4}\left(1 - \frac{C}{p}\right).$$

Note that f is a multiplicative function, it is positive at sufficiently large primes p, and

$$\begin{aligned}\sum_{p \leq Y} \frac{f(p)\log p}{p} &= \frac{1}{4}\sum_{p \leq Y} \frac{\log p}{p} - C\sum_{p \leq Y} \frac{\log p}{p^2} \\ &= \frac{1}{4}\log(Y) + O(1)\end{aligned}$$

(see for instance [7, p. 57]). Hence, by Wirsing's Theorem ([11, Theorem 14.3] with $\kappa = \frac{1}{4}$, $c = 0$, $k = 1$) we have

$$\mathscr{S}(Y) \geq \sum_{m \leq Y} \frac{f(m)}{m} \gg (\log Y)^{1/4}. \quad \square$$

5. Applications to rational distance problems

5.1. From $H_\eta(K)$ to rational configurations

We return temporarily to the more general setting of a field K in which -1 is not a square. Let $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. In Eq. (7), we defined the variety

$$\mathcal{H} : y^2 = N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix}\right),$$

where $N(u,v) := u^2 + v^2$. We also define the subvariety $\mathcal{F}$ of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathrm{GL}_2$ (with coordinates $((u_1 : v_1), (u_2 : v_2), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$) by

$$\mathcal{F} : au_1u_2 + bu_1v_2 + cv_1u_2 + dv_1v_2 = 0.$$

As with $\mathcal{H}$, there is a projection map to GL_2 giving $\mathcal{F}$ the structure of a flat family of curves, with F_η denoting the fiber over $\eta \in \mathrm{GL}_2(K)$. We define

$$\begin{aligned}\mathcal{S}_K &:= \{(u : v) \in \mathbb{P}^1(K) \mid u^2 + v^2 \text{ is a square in } K\} \\ &= \{(z^2 - x^2 : 2xz) \mid (x : z) \in \mathbb{P}^1(K)\}.\end{aligned}$$

Proposition 5.1. *There is a morphism $\Phi : \mathcal{H} \to \mathcal{F}$ over GL_2 defined by sending $(x : y : z)$ to*

$$\left((-c(z^2 - x^2) - d(2xz) : a(z^2 - x^2) + b(2xz)),\ (z^2 - x^2 : 2xz)\right). \tag{15}$$

Further, Φ induces a bijection between the set of Γ-orbits in $H_\eta(K)$ and the set $F_\eta(K) \cap (\mathcal{S}_K \times \mathcal{S}_K)$.

Proof. Notice that the equation defining $\mathcal{F}$ can be written

$$0 = \begin{pmatrix} u_1 & v_1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u_2 \\ v_2 \end{pmatrix}, \tag{16}$$

so that the model $\mathcal{H}_0$ from Eq. (6) is evidently the pullback of $\mathcal{F}$ under the map $(x : z) \mapsto (z^2 - x^2 : 2xz)$ on each component. The map Φ is obtained by composing the isomorphism $\mathcal{H} \to \mathcal{H}_0$ with this map. Given $(x : y : z) \in H_\eta(K)$, we have

$$(z^2 - x^2)^2 + (2xz)^2 = (z^2 + x^2)^2$$

and

$$(-c(z^2 - x^2) - d(2xz))^2 + (a(z^2 - x^2) + b(2xz))^2 = y^2,$$

so that $\Phi(x : y : z) \in \mathcal{S}_K \times \mathcal{S}_K$. Conversely, given any $(\alpha_1, \alpha_2) \in F_\eta(K) \cap (\mathcal{S}_K \times \mathcal{S}_K)$, we can write $\alpha_2 = (z^2 - x^2 : 2xz)$ and $\alpha_1 = (z'^2 - x'^2 : 2x'z')$ for some $x, z, x', z' \in K$. The fact that $(\alpha_1, \alpha_2) \in F_\eta(K)$ is then equivalent to

$$\begin{pmatrix} z'^2 - x'^2 & 2x'z' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix} = 0.$$

This implies that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z^2 - x^2 \\ 2xz \end{smallmatrix}\right)$ must equal $\lambda\left(\begin{smallmatrix} -2x'z' \\ z'^2 - x'^2 \end{smallmatrix}\right)$ for some $\lambda \in K^\times$. In particular,

$$N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix}\right) = \lambda^2 (z'^2 + x'^2)^2,$$

so that $(x : y : z) \in H_\eta(K)$ for $y = \lambda(z'^2 + x'^2)$. One can then confirm that Φ maps $(x : y : z)$ to (α_1, α_2), using the computation

$$\begin{aligned}\begin{pmatrix} -c & -d \\ a & b \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix} \\ &= \lambda\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -2x'z' \\ z'^2 - x'^2 \end{pmatrix} \\ &= -\lambda\begin{pmatrix} z'^2 - x'^2 \\ 2x'z' \end{pmatrix}.\end{aligned}$$

Hence Φ maps $H_\eta(K)$ surjectively onto $F_\eta(K) \cap (\mathcal{S}_K \times \mathcal{S}_K)$.

Finally, observe that for each $\alpha_2 \in \mathcal{S}_K$, there are two choices for $(x : z) \in \mathbb{P}^1(K)$ with $(z^2 - x^2 : 2xz) = \alpha_2$, interchanged by the involution $(x : z) \mapsto (-z : x)$. Once x and z are fixed, there are two choices for y, interchanged by $y \mapsto -y$. Hence Γ acts transitively on the fibers of Φ. □

Remark 5.2. For many rational distance problems, solutions $((u_1 : v_1), (u_2 : v_2)) \in F_\eta(K) \cap (\mathcal{S}_K \times \mathcal{S}_K)$ with $u_1v_1u_2v_2 = 0$ will be considered *degenerate* (as they correspond to rational right triangles with no width). The degenerate locus $u_1v_1u_2v_2 = 0$ pulls back to the subvariety $\mathcal{D} \subseteq \mathcal{H}$ defined by

$$\mathcal{D} : xyz(z^4 - x^4)(a(z^2 - x^2) + b(2xz))(c(z^2 - x^2) + d(2xz)) = 0. \tag{17}$$

5.2. Density of rational configuration solutions

For any embedding $K \hookrightarrow \mathbb{R}$, if $H_\eta(K)$ is infinite, we can show that $F_\eta(K) \cap (\mathcal{S}_K \times \mathcal{S}_K)$ is dense in $F_\eta(\mathbb{R})$. This is a special case of the following result. Let E denote the Jacobian of H_η.

Lemma 5.3. *Let $\eta \in \mathrm{GL}_2(\mathbb{R})$ and suppose $\Delta(H_\eta) \neq 0$. Let $A \subseteq H_\eta(\mathbb{R})$ be the image of an infinite subgroup of $E(\mathbb{R})$ under some isomorphism $E(\mathbb{R}) \cong H_\eta(\mathbb{R})$. Then the image of A under $\Phi : H_\eta \to F_\eta$ (Proposition 5.1) is dense in $F_\eta(\mathbb{R})$.*

Proof. The (topological) curve $H_\eta(\mathbb{R})$ has two connected components, given by points $(x : y : z)$ with $y > 0$ and those with $y < 0$ respectively: there is no equivalence between any points with $y > 0$ and points with $y < 0$ because of the weighting on $\mathbb{P}^2$ (Section 3.2), and there are no points with $y = 0$ because $\Delta(H_\eta) \neq 0$ and -1 is not a square in K. Thus $E(\mathbb{R})$ has the structure of a Lie group $S^1(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$. Any infinite subgroup of $E(\mathbb{R})$ has dense intersection with the identity component, so A has dense intersection with one of the components of $H_\eta(\mathbb{R})$.

We can express the map $\Phi : H_\eta \to F_\eta$ as a composition

$$\begin{array}{ccccc} H_\eta & \to & \mathbb{P}^1 & \to & F_\eta \\ (x:y:z) & \mapsto & (x:z) & \mapsto & \begin{pmatrix} (-c(z^2-x^2)-d(2xz) : a(z^2-x^2)+b(2xz)), \\ (z^2-x^2 : 2xz) \end{pmatrix}. \end{array}$$

The first map induces a continuous surjection from each component of $H_\eta(\mathbb{R})$ onto $\mathbb{P}^1(\mathbb{R})$, so the image of A is dense in $\mathbb{P}^1(\mathbb{R})$. The second map induces a continuous surjection $\mathbb{P}^1(\mathbb{R}) \to F_\eta(\mathbb{R})$, so the image of A is dense in $F_\eta(\mathbb{R})$. □

5.3. Application to three-distance problem

We will use Theorem 1.4 to prove the following statement.

Corollary 5.4. *There exists an infinite collection of rational functions, $\rho_n : \mathbb{A}^1_{\mathbb{Q}} \dashrightarrow \mathbb{A}^2_{\mathbb{Q}}$ for $n \in \mathbb{Z}$, with the following properties. For all $t \in \mathbb{Q} - \{0, \pm 1\}$ and all $n \in \mathbb{Z}$, if ρ_n is defined at t, then $\rho_n(t)$ has rational distance from each of $(0,0)$, $(0,1)$, and $(1,1)$. Further, for each $t \in \mathbb{Q} - \{0, \pm 1\}$, there are only finitely many $n \in \mathbb{Z}$ for which ρ_n is not defined at t, and the set*

$$\{\rho_n(t) : n \in \mathbb{Z},\ \rho_n \text{ defined at } t\}$$

is a dense subset of the line $y = \frac{2t}{1-t^2}x$ in $\mathbb{R}^2$.

Proof. For the sake of clarity, we begin by proving the weaker result mentioned in the introduction: for each $t \in \mathbb{Q} - \{0, \pm 1\}$, the line $y = \frac{2t}{1-t^2}x$ has a dense set of points that have rational distance from each of $(0,0)$, $(0,1)$, and $(1,1)$. Once this is done, we will explain how the proof can be modified to allow for families of solutions parametrized by t.

Let $t \in \mathbb{Q} - \{0, \pm 1\}$, and set $s(t) := 1 - \frac{2t}{1-t^2}$. There is no rational solution to $1 = \frac{2t}{1-t^2}$, so $\eta(t) := \left(\begin{smallmatrix} 1 & -1 \\ 0 & s(t) \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathbb{Q})$. We have $|s(t)| \neq 1$ because we excluded the case $t = 0$ and there is no rational solution to $2 = \frac{2t}{1-t^2}$. The polynomials $4s \pm (1-s^2)^2$ are both irreducible over $\mathbb{Q}$, so taking $r = -1$ we also have $4r^2 s(t) \neq \pm(1 - s(t)^2)^2$ for all $t \in \mathbb{Q}$. Hence, by Theorem 1.4, $H_{\eta(t)}(\mathbb{Q})$ is infinite. By Lemma 5.3, this implies that the set of $((u_1 : v_1), (u_2 : v_2)) \in \mathcal{S} \times \mathcal{S}$ satisfying $u_1u_2 + v_1v_2 = u_1v_2 + \frac{2t}{1-t^2}v_1v_2$ (the defining equation of $F_{\eta(t)}$) is dense in $F_{\eta(t)}(\mathbb{R})$.

Now define the rational function $z : F_{\eta(t)} \dashrightarrow \mathbb{A}^2$ by

$$z((u_1 : v_1), (u_2 : v_2)) := \left(\frac{(1-t^2)v_1}{(1-t^2)u_1 + 2tv_1}, \frac{2tv_1}{(1-t^2)u_1 + 2tv_1} \right). \tag{18}$$

The map z restricts to a homeomorphism

$$F_{\eta(t)}(\mathbb{R}) \setminus \left\{\left((-2t : 1-t^2), (1-t^2 : 2t)\right)\right\} \to \left\{(x,y) \in \mathbb{R}^2 : y = \tfrac{2t}{1-t^2}x\right\}.$$

So after removing a single point from $F_{\eta(t)}(K) \cap (\mathcal{S} \times \mathcal{S})$, the remainder maps to a dense subset of the line $y = \frac{2t}{1-t^2}x$. For each $(\alpha_1, \alpha_2) \in F_{\eta(t)}(\mathbb{Q}) \cap (\mathcal{S} \times \mathcal{S})$ other than $\left((-2t : 1-t^2), (1-t^2 : 2t)\right)$, the point $(x,y) := z(\alpha_1, \alpha_2)$ satisfies

$$\begin{aligned}
x^2 + y^2 &= \left(\frac{(1+t^2)v_1}{u_1(1-t^2) + 2tv_1}\right)^2, \\
x^2 + (1-y)^2 &= \left(\frac{(1-t^2)}{u_1(1-t^2) + 2tv_1}\right)^2 (u_1^2 + v_1^2), \\
(1-x)^2 + (1-y)^2 &= \left((1-t^2)\frac{u_1 + \frac{2t}{1-t^2}v_1 - v_1}{(1-t^2)u_1 + 2tv_1}\right)^2 + \left(\frac{(1-t^2)u_1}{(1-t^2)u_1 + 2tv_1}\right)^2 \\
&= \left(\frac{(1-t^2)u_1u_2}{((1-t^2)u_1 + 2tv_1)v_2}\right)^2 + \left(\frac{(1-t^2)u_1}{(1-t^2)u_1 + 2tv_1}\right)^2 \\
&= \left(\frac{(1-t^2)u_1}{((1-t^2)u_1 + 2tv_1)v_2}\right)^2 (u_2^2 + v_2^2).
\end{aligned}$$

Since $\alpha_1, \alpha_2 \in \mathcal{S}$, these are all squares in $\mathbb{Q}$, so this gives a solution to the three-distance problem.

We now return to the problem of producing explicit parametrizations of solutions in terms of t. For this, note that $t \mapsto \eta(t)$ defines a morphism $V := \mathbb{A}^1 - \{0, \pm 1\} \to \mathrm{GL}_2$. We will define a rational map $\rho_n : V \dashrightarrow \mathbb{A}^2$ by a composition

$$\rho_n : V \xrightarrow{\tau_n} E' \xrightarrow{\varepsilon} \mathcal{H}' \xrightarrow{\Phi'} \mathbb{P}^1 \times \mathbb{P}^1 \times V \xrightarrow{z'} \mathbb{A}^2,$$

where each variety besides $\mathbb{A}^2$ is a scheme over V and each map besides z' is a morphism over V. We consider each of these maps in turn.

- Let E be the subvariety of $\mathbb{P}^2 \times \mathrm{GL}_2$ parametrizing the Jacobian varieties of $\mathcal{H}$ (defined by Eq. (9)). Let E' be the fiber product of V with E, so that $E'_t = E_{\eta(t)}$ for all $t \in V(\mathbb{Q})$. We have a section $V \to E'$ given by $t \mapsto (-1, -1)$. Using the group law on the generic fiber of E', define the rational map $\tau_n : V \dashrightarrow E'$ by the property that $\tau_n(t) = n(-1,-1) \in E'_t(\mathbb{Q})$ for all $t \in V(\mathbb{Q})$. The proof of Theorem 1.4 shows that $(-1,-1)$ is non-torsion in $E'_t(\mathbb{Q})$ for all $t \in V(\mathbb{Q})$, so for each such t, the set $\{\tau_n(t) : n \in \mathbb{Z}\}$ is an infinite subgroup of $E'_t(\mathbb{Q})$.
- The fiber product of V with $\mathcal{H}$ is a one-parameter family $\mathcal{H}'$ of curves over V, with the property that the fiber of $\mathcal{H}'$ over t is $H_{\eta(t)}$. We have a section $V \to \mathcal{H}'$ given by $t \mapsto (0:1:1)$, allowing us to define a birational map $\varepsilon : E' \dashrightarrow \mathcal{H}'$ over $\mathbb{Q}$ sending the zero section of E' to the given section of $\mathcal{H}'$. This map restricts to an isomorphism on all fibers over points in $V(\mathbb{Q})$.

- The rational map $\Phi' : \mathcal{H}' \dashrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times V$ is defined by

$$((x : y : z), t) \mapsto \big((-s(t)(2xz) : (z^2 - x^2) - (2xz)), (z^2 - x^2 : 2xz),\ t\big)\,.$$

  Note that after restricting to a fiber $\mathcal{H}'_t$, the first two components of Φ' agree with the map $\Phi : H_{\eta(t)} \to F_{\eta(t)}$ (Proposition 5.1). So for any $t \in V(\mathbb{Q})$, the set

$$S_t := \{(\Phi' \circ \varepsilon \circ \tau_n)(t) : n \in \mathbb{Z}\}$$

  is contained in $F_{\eta(t)}(\mathbb{Q}) \cap (\mathcal{S} \times \mathcal{S}) \times \{t\}$, and is a dense subset of $F_{\eta(t)}(\mathbb{R}) \times \{t\}$ by Lemma 5.3.
- The rational map $z' : \mathbb{P}^1 \times \mathbb{P}^1 \times V \dashrightarrow \mathbb{A}^2$ is defined on an appropriate dense open subset by

$$z'((u_1 : v_1), (u_2 : v_2), t) = \left(\frac{(1-t^2)v_1}{(1-t^2)u_1 + 2tv_1},\ \frac{2tv_1}{(1-t^2)u_1 + 2tv_1}\right).$$

  Note that when restricted to $F_{\eta(t)} \times \{t\}$, the map agrees with $z : F_{\eta(t)} \dashrightarrow \mathbb{A}^2$ defined in Eq. (18). So the same proof as above shows that for each t, z' maps S_t minus a point to a dense subset of the line $y = \frac{2t}{1-t^2}x$ consisting of solutions to the three-distance problem. □

5.4. Special cases

Some rational configuration problems fall under the exceptional cases of Theorem 1.4. We consider a few of these here. Recall that

$$\mathcal{S}' := \left\{\frac{u}{v} \in \mathbb{Q} \mid (u : v) \in \mathcal{S}\right\}$$

denotes the affine elements of $\mathcal{S}$.

Proposition 5.5. *Let $\alpha_3 \in \mathcal{S}'$. There exist infinitely many pairs $\alpha_1, \alpha_2 \in \mathcal{S}'$ such that $\alpha_1 + \alpha_2 = \alpha_3$.*

That is, for any rectangle with rational distances between every two vertices, there are infinitely many ways to split it into two rectangles with rational distances between every two vertices.

Proof. Let $\alpha_3 = \frac{1-t^2}{2t}$ for some $t \in \mathbb{Q} - \{0, \pm 1\}$. The equation $x_1 + x_2 - \alpha_3 = 0$ defines F_η for $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -\alpha_3 \end{smallmatrix}\right)$, and H_η (which contains the rational point $(0 : 1 : 1)$) is isomorphic to its Jacobian (as in Eq. (9)),

$$E : y^2 = x^3 + \left(\left(\frac{1-t^2}{2t}\right)^2 + 2\right)x^2 + x.$$

We consider E_η as an elliptic curve over the function field $\mathbb{Q}(t)$, and note that $E(\mathbb{Q}(t))$ has a rational point $P = \left(t, \frac{1}{2}(t+1)^2\right)$. By computing nP for $n = 1, \ldots, 12$ and checking that the denominators of the coordinates have no rational roots, we can confirm that P is non-torsion for all $t \in \mathbb{Q} - \{0, \pm 1\}$. Hence H_η has infinitely many rational points, so $F_\eta(\mathbb{Q}) \cap (\mathcal{S} \times \mathcal{S})$ is infinite by Proposition 5.1. □

This allows us to prove that every rational number can be written as a sum of three elements of $\mathcal{S}'$ in infinitely many ways; in other words, for any rational $t > 0$, there are infinitely many ways to cut a $1 \times t$ rectangle into three rectangles, each of which has rational distances between every pair of vertices. We also prove that every rational number can be written as a product of three elements of $\mathcal{S}'$ in infinitely many ways.

Proof of Proposition 1.6. The equation $x_1 + 2x_2 - t = 0$ defines F_η for $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 2 & -t \end{smallmatrix}\right)$. Now H_η is isomorphic to $H_{\eta'}$ for $\eta' = \begin{pmatrix} 1 & -t/2 \\ 0 & -1/2 \end{pmatrix}$, and by Theorem 1.4, $H_\eta(\mathbb{Q})$ is infinite for all $t \neq 0$. Hence every nonzero $t \in \mathbb{Q}$ can be written as $\alpha_1 + \alpha_2 + \alpha_2$ for infinitely many pairs $(\alpha_1, \alpha_2) \in \mathcal{S}' \times \mathcal{S}'$. The case $t = 0$ follows from Proposition 5.5 because $\mathcal{S}$ is closed under negation.

Next we will show that for any $t \in \mathbb{Q}^\times$, there exists $u \in \mathbb{Q} - \{0, \pm 1\}$ such that when $s = -t\left(\frac{2u}{1-u^2}\right)$, the polynomial $x_1 x_2 + s$ has infinitely many solutions with $x_1, x_2 \in \mathcal{S}'$. Each of these solutions can then be multiplied by $\frac{1-u^2}{2u} \in \mathcal{S}'$ to exhibit t as a product of three elements of $\mathcal{S}'$.

Let $\eta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & s \end{smallmatrix}\right)$. We consider the elliptic curve

$$E_\eta : y^2 = x(x+1)(x+s^2) = x(x+1)\left(x + t^2\left(\frac{2u}{1-u^2}\right)^2\right).$$

If we set $u = t^2 + 2$, then the elliptic curve

$$y^2 = x(x+1)\left(x + t^2\left(\frac{2(t^2+2)}{1-(t^2+2)^2}\right)^2\right)$$

over $\mathbb{Q}$ has a point

$$\left(\frac{t^2(t^2+1)^2(t^2+2)}{(t^2+3)^2}, \frac{t^2(t^2+2)(t^8+4t^6+6t^4+8t^2+9)}{(t^2+3)^3}\right),$$

which has infinite order when $t \neq 0, \pm 1$. So for all $t \in \mathbb{Q} - \{0, \pm 1\}$, $x_1 x_2 - t\left(\frac{2u}{1-u^2}\right) = 0$ has infinitely many solutions $x_1, x_2 \in \mathcal{S}'$, so t can be written as a product of three elements of $\mathcal{S}'$ in infinitely many different ways.

We finally must handle $t = \pm 1$. In this case, we can set $u = \frac{5}{6}$. For $\eta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \pm\frac{60}{11} \end{smallmatrix}\right)$ we have the elliptic curve

$$E_\eta : y^2 = x^3 + \left(1 + \left(\frac{60}{11}\right)^2\right)x^2 + \left(\frac{60}{11}\right)^2 x,$$

which has a non-torsion point $(-\frac{12}{11}, \frac{204}{121})$ (in fact $E_\eta(\mathbb{Q})$ has rank 2). Thus there are infinitely many Pythagorean solutions of $x_1 x_2 \mp \frac{60}{11} = 0$, allowing us to write ± 1 as a product $\alpha_1\alpha_2\frac{11}{60}$ of three elements of $\mathcal{S}'$ in infinitely many ways. □

Remark 5.6. The substitution $s = t^2 + 2$ was found essentially by trial and error, guided by inspiration from a MathOverflow answer by Siksek [1] describing how to find a positive rank subfamily of the family $y^2 = x(x+1)(x + (\frac{1-s}{s})^2)$, and from Naskręcki [15] who used a similar method to find a positive rank subfamily of the curve $y^2 = x(x-1)\left(x - \left(\frac{2s}{1-s^2}\right)^2\right)$.

For the $t = 1$ case, the existence of a solution to $\alpha_1\alpha_2\alpha_3 = 1$ is equivalent to the existence of a body cuboid (Section 2.1). The existence of a body cuboid with edge lengths $(240, 117, 44)$ leads to the choice of u.

By Proposition 5.5, every element of $\mathcal{S}'$ can be written as a sum of two elements of $\mathcal{S}'$ in infinitely many ways, but we have no comparable result for products. A natural question then is to determine which rational numbers t can be written as a product of two elements of $\mathcal{S}'$ in infinitely many ways. This line of inquiry is explored in more depth in [13].

Declaration of competing interest

There are no competing interests to declare. Generative AI was not used in the writing of this article.

Acknowledgments

The author was supported by a CRM-ISM Postdoctoral Fellowship during the writing of this article, and would like to thank Andrew Granville, Sunkai Leung, Michael Lipnowski, Henri Darmon, Eyal Goren, Allysa Lumley, Olivier Mila, Wanlin Li, and Valeriya Kovaleva for helpful discussions.

Data availability

No data was used for the research described in the article.

References

[1] Siksek, The rank of a class elliptic curves, MathOverflow (version: 2011-05-03), https://mathoverflow.net/users/4140/siksek, https://mathoverflow.net/q/63856.

[2] Sang Yook An, et al., Jacobians of genus one curves, J. Number Theory (ISSN 0022-314X) 90 (2) (2001) 304–315, https://doi.org/10.1006/jnth.2000.2632.
[3] T.G. Berry, Points at rational distance from the corners of a unit square, Ann. Sc. Norm. Super. Pisa, Cl. Sci. Ser. 4 17 (4) (1990) 505–529, http://www.numdam.org/item/ASNSP_1990_4_17_4_505_0/.
[4] Manjul Bhargava, John Cremona, Tom Fisher, The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point, Int. J. Number Theory (ISSN 1793-0421) 17 (4) (2021) 903–923, https://doi.org/10.1142/S1793042121500147.
[5] V. Chandrasekar, The congruent number problem, Resonance 3 (1998) 33–45.
[6] Keith Conrad, The congruent number problem, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf. (Accessed 1 November 2021).
[7] Harold Davenport, Multiplicative Number Theory, third, Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, ISBN 0-387-95097-4, 2000, Revised and with a preface by Hugh L. Montgomery, xiv+177.
[8] P.X. Gallagher, The large sieve and probabilistic Galois theory, in: Analytic Number Theory (Proc. Sympos. Pure Math., vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), in: Proc. Sympos. Pure Math., vol. XXIV, Amer. Math. Soc., Providence, RI, 1973, pp. 91–101.
[9] Richard K. Guy, Unsolved Problems in Number Theory, third, Problem Books in Mathematics, Springer-Verlag, New York, ISBN 0-387-20860-7, 2004, pp. xviii+437.
[10] Lorenz Halbeisen, Norbert Hungerbühler, Pairing Pythagorean pairs, J. Number Theory (ISSN 0022-314X) (2021), https://doi.org/10.1016/j.jnt.2021.07.002.
[11] Dimitris Koukoulopoulos, The Distribution of Prime Numbers, Graduate Studies in Mathematics, vol. 203, American Mathematical Society, Providence, RI, ISBN 978-1-4704-4754-0, 2019, pp. xii+356.
[12] D. Loughran, A. Smeets, Fibrations with few rational points, Geom. Funct. Anal. (ISSN 1016-443X) 26 (5) (2016) 1449–1482, https://doi.org/10.1007/s00039-016-0381-8.
[13] Jonathan Love, Root numbers of a family of elliptic curves and two applications, Indag. Math. (ISSN 0019-3577) 35 (3) (2024) 555–569, https://doi.org/10.1016/j.indag.2024.04.003.
[14] R. van Luijk, On Perfect Cuboids, Doctoraalscriptie, Mathematisch Instituut, Universiteit Utrecht, Utrecht, 2000.
[15] Bartosz Naskręcki, Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples, Acta Arith. (ISSN 0065-1036) 160 (2) (2013) 159–183, https://doi.org/10.4064/aa160-2-5.
[16] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, ISBN 978-0-387-09493-9, 2009, pp. xx+513.
[17] J.B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, Invent. Math. (ISSN 0020-9910) 72 (2) (1983) 323–334, https://doi.org/10.1007/BF01389327.
[18] J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, J. Math. Pures Appl. (9) (ISSN 0021-7824) 60 (4) (1981) 375–484.
[19] André Weil, Remarques sur un mémoire d'Hermite, Arch. Math. (Basel) (ISSN 0003-889X) 5 (1954) 197–202, https://doi.org/10.1007/BF01899338.