PYTHAGOREAN SOLUTIONS OF DIOPHANTINE SYSTEMS AND A FAMILY OF GENUS ONE CURVES

JONATHAN LOVE

ABSTRACT. Let K be a number field in which -1 is not a square, and define a genus one hyperelliptic curve $\mathcal{H}$ over the function field $K(a,b,c,d)$ by

$$\mathcal{H} : y^2 = (a(1-x^2)+b(2x))^2 + (c(1-x^2)+d(2x))^2.$$

We study the set of K-points of the specialization $\mathcal{H}_\eta$ as $\eta = (a,b,c,d) \in K^4$ varies. First we show that for an appropriate notion of density, the set of η for which $\mathcal{H}_\eta$ is everywhere locally soluble has density zero. Using a group action on K^4 that preserves the isomorphism class of $\mathcal{H}_\eta$, we show that the set of $\eta \in K^4$ with $ad-bc \neq 0$ for which $\mathcal{H}_\eta(K)$ is nonempty equals the orbit of a two-parameter family, and that $\mathcal{H}_\eta(K)$ is infinite for all η in this family with the exception of three one-parameter families.

Points in $\mathcal{H}_\eta(\mathbb{Q})$ encode pairs of Pythagorean triples satisfying a polynomial relation, and as such can be applied to the study of rational distance problems. 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 that have rational distance from each of the three points $(0,0)$, $(0,1)$, and $(1,1)$. We also prove some results regarding which rational numbers can be written as sums or products of slopes of rational right triangles.

CONTENTS

1. INTRODUCTION

1.1. **Pythagorean solutions.** Pythagorean triples — triples (a,b,c) of positive integers such that $a^2+b^2=c^2$ — have been core objects of study throughout the history of diophantine problems. While a parametrization of the set of Pythagorean

Date: November 2021.
Supported by CRM-ISM postdoctoral fellowship.

triples has been known for thousands of years, properties of this set continue to be actively explored.

One direction of exploration involves configurations of multiple right triangles with rational side lengths. We say $\alpha \in \mathbb{Q}^\times$ is a *Pythagorean slope* if 1 and $|\alpha|$ form the legs of a rational right triangle; equivalently, if there exists a Pythagorean triple (a,b,c) with $|\alpha| = \frac{a}{b}$; equivalently, if $\alpha = \frac{y}{x}$ for a rational point (x,y) on the unit circle $x^2+y^2 = 1$ with $xy \neq 0$. Some questions with natural geometric interpretations include the following.

(1) For which Pythagorean slopes α do there exist Pythagorean slopes β_1, β_2 with $\alpha = \beta_1\beta_2$?
(2) For which Pythagorean slopes α do there exist Pythagorean slopes β_1, β_2 with $\alpha = \beta_1 + \beta_2$?
(3) Does there exist a box for which all pairwise distances between vertices are rational? That is, do there exist side lengths $a,b,c \in \mathbb{Q}_{>0}$ such that $\frac{b}{a}$, $\frac{c}{a}$, $\frac{c}{b}$, and $\frac{\sqrt{b^2+c^2}}{a}$ are all Pythagorean slopes?
(4) Does there exist a point $P \in \mathbb{R}^2$ with rational distance from every vertex of a square with unit side length? That is, do there exist $x, y \in \mathbb{Q}$ such that $\frac{y}{x}$, $\frac{1-y}{x}$, $\frac{1-x}{y}$, and $\frac{1-x}{1-y}$ are all Pythagorean slopes?

Items 3 and 4 are open problems (discussed further in section 2); we emphasize that we do not make significant progress towards solving either of them. However, we will put these four questions into a general context and obtain some related results.

Let K be a field of characteristic not equal to 2, and let $\mathbb{A}^n_K = \operatorname{Spec} K[x_1, \dots, x_n]$ denote the n-dimensional affine space over K. Let $\mathcal{S}_K$ denote the set of $\alpha \in K^\times$ such that $\alpha^2 + 1$ is a square in $K^\times$. (In particular, $\mathcal{S}_\mathbb{Q}$ is the set of Pythagorean slopes.)

Definition 1.1. *Given an affine algebraic variety $V \subseteq \mathbb{A}^n_K$, a point $(\alpha_1, \dots, \alpha_n) \in V(K)$ is a* Pythagorean solution of V *if $\alpha_1, \dots, \alpha_n \in \mathcal{S}_K$. The set of Pythagorean solutions of V is denoted $V(\mathcal{S}_K)$.*

The four problems above can all be rephrased in terms of determining the set of Pythagorean solutions of certain surfaces over $\mathbb{Q}$: namely, the surface cut out by $x_1x_2 = x_3$ in $\mathbb{A}^3_\mathbb{Q}$ (item 1), $x_1 + x_2 = x_3$ in $\mathbb{A}^3_\mathbb{Q}$ (item 2), $x_1^2 + x_2^2 = x_3^2$ in $\mathbb{A}^3_\mathbb{Q}$ (item 3), and $x_1x_2 + 1 = x_1 + x_3$ and $x_1x_2 = x_3x_4$ in $\mathbb{A}^4_\mathbb{Q}$ (item 4). In general, Pythagorean solutions of varieties in $\mathbb{A}^n_\mathbb{Q}$ encode n-tuples of rational right triangles satisfying polynomial constraints, and as such they can be applied to the study of rational distance problems (section 2).

By a classical parametrization, $\mathcal{S}_K$ equals the image of $K - \{0, \pm 1\}$ under the degree 2 rational map $x \mapsto \frac{1-x^2}{2x}$. As a result, for any affine variety $V \subseteq \mathbb{A}^n_K$, there is a dominant degree 2^n morphism $\Phi : \widetilde{V} \to V$ such that $V(\mathcal{S}_K) = \Phi(\widetilde{V}(K))$. The geometry of this cover can make it difficult to find Pythagorean solutions of very simple varieties, or even to determine whether a Pythagorean solution exists. For instance, if V is the surface $x_1^2 + x_2^2 = x_3^2$ associated with item 3, the cover $\widetilde{V}$ is (an open subset of) a surface of general type, a class of surface for which we have very few tools to find rational points [12]. The same holds for the variety associated with item 4 [3]. On the other hand, if V is the surface $x_1x_2 = x_3$ or $x_1 + x_2 = x_3$, we will see that the corresponding cover $\widetilde{V}$ can be equipped with the structure of

an elliptic surface, and we will find subproblems of items 3 and 4 that can also be studied using elliptic surfaces.

In this paper we study the set of Pythagorean solutions of a particular family of varieties, and apply these results to problems such as items 1 to 4.

Problem 1.2. *For which* $\eta = (a,b,c,d) \in K^4$ *does the curve*

$$F_\eta : ax_1x_2 + bx_1 + cx_2 + d = 0 \tag{1}$$

in $\mathbb{A}^2_K$ *have a Pythagorean solution?*

1.2. **A family of genus one curves.** To study problem 1.2, we consider the genus one hyperelliptic curve $\mathcal{H}$ over the function field $K(a,b,c,d)$ defined by

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

For each $\eta = (a,b,c,d) \in K^4$, we obtain a curve $\mathcal{H}_\eta$ over K by specializing at η. When $ad - bc \neq 0$, there is an open affine $U_\eta \subseteq \mathcal{H}_\eta$ and a degree 4 map $\Phi : U_\eta \to F_\eta$ mapping $U_\eta(K)$ onto $F_\eta(\mathcal{S}_K)$ (proposition 3.4).

Let K be a number field and $\mathcal{O}_K$ its ring of integers. The following is a high-level summary of the results we prove about the family $\mathcal{H}$.

- The set of $\eta \in \mathcal{O}_K^4$ for which $\mathcal{H}_\eta$ is everywhere locally soluble has density zero (theorem 1.3); in particular, $\mathcal{H}_\eta(K)$ is almost always empty.
- There is an action of $K^\times \times \mathrm{O}_2(K) \times \mathrm{O}_2(K)$ on the set of $\eta \in K^4$ with $ad - bc \neq 0$ that preserves the isomorphism class of $\mathcal{H}_\eta$ (lemma 3.1).
- (Assuming $\mathbb{Q}(i) \notin K$) The locus of $\eta \in K^4$ with $ad - bc \neq 0$ and $\mathcal{H}_\eta(K)$ nonempty equals the orbit of a two-parameter family (lemma 3.2).
- (Assuming $\mathbb{Q}(i) \notin K$) The locus of $\eta \in K^4$ with $ad - bc \neq 0$ and $\mathcal{H}_\eta(K)$ *finite* and nonempty equals the orbit of a 1-dimensional algebraic set (proposition 5.1); when $K = \mathbb{Q}$, this algebraic set can be taken to be a union of three explicit one-parameter families (theorem 1.4).

Put even more simply, $\mathcal{H}_\eta$ is typically empty, but when nonempty, it is typically infinite. In the following sections we state these results more precisely. We discuss applications to Pythagorean solutions starting in section 1.3.

1.2.1. *Everywhere locally soluble curves are sparse.* Bhargava, Cremona, and Fisher show that a majority of curves of the form

$$y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \tag{3}$$

are everywhere locally soluble [4, Theorem 3]. More precisely, if $\mathcal{C}'(X)$ denotes the set of $(a,b,c,d,e) \in \mathbb{Z}^5$ with $|a|,|b|,|c|,|d|,|e| \leq X$, and $\mathcal{C}'_{\mathrm{loc}}(X)$ denotes the set of $\eta = (a,b,c,d,e) \in \mathcal{C}'(X)$ such that eq. (3) has a solution in $\mathbb{Q}_v$ for all $v \in \{\infty, 2, 3, 5, 7, \ldots\}$, then

$$\lim_{X\to\infty} \frac{|\mathcal{C}'_{\mathrm{loc}}(X)|}{|\mathcal{C}'(X)|} \approx 0.7596.$$

The subfamily $\mathcal{H}$ (eq. (2)) has very different behavior. Let K be a number field, and let $\mathcal{O}_K$ the ring of integers of K. Given $z \in \mathcal{O}_K$, define $H(z)$ to be the maximum of $|\iota(z)|$ over all embeddings $\iota : K \hookrightarrow \mathbb{C}$.

Theorem 1.3. *Let $\mathcal{C}(X)$ denote the set of $(a,b,c,d) \in \mathcal{O}_K^4$ with $H(a)$, $H(b)$, $H(c)$, $H(d) \le X$. Let $\mathcal{C}_{loc}(X)$ denote the set of $\eta \in \mathcal{C}(X)$ such that $\mathcal{H}_\eta(K_v) \neq \varnothing$ for all places v of K. For all $\varepsilon > 0$, we have*

$$\frac{|\mathcal{C}_{loc}(X)|}{|\mathcal{C}(X)|} = O((\log\log X)^{-\frac{1}{4}+\varepsilon}),$$

with the implicit constant depending on K and ε.

In particular, when $\mathcal{O}_K^4$ is ordered by height H, the set of $\eta \in \mathcal{O}_K^4$ for which $\mathcal{H}_\eta(K)$ is nonempty has density 0.

1.2.2. *Most soluble curves have infinitely many K-points.* Now we restrict to number fields K that do not contain $\mathbb{Q}(i)$ (this prevents the existence of nontrivial solutions of $x^2 + y^2 = 0$). Suppose that $\mathcal{H}_\eta(K)$ is known to be nonempty. While theorem 1.3 suggests that this situation is rare, it is easy to construct many examples. For instance, if

$$\eta = (r(2t),\, r(t^2-1),\, c,\, d) \qquad \text{for some } r,t,c,d \in K, \tag{4}$$

then $\mathcal{H}_\eta(K)$ contains the point $(t,\, c(1-t^2) + d(2t))$. If K has an embedding into $\mathbb{R}$, this construction shows that the set of $\eta \in K^4$ for which $\mathcal{H}_\eta(K)$ is nonempty is dense in $\mathbb{R}^4$.

It is straightforward to describe $\mathcal{H}_\eta(K)$ when $ad - bc = 0$ (appendix A), so we will assume $ad - bc \neq 0$. Given a point $(x_0 : y_0 : z_0) \in \mathcal{H}_\eta(K)$, define the quantities

$$\begin{aligned} c' &:= \frac{(a^2-b^2+c^2-d^2)(2x_0z_0)(z_0^2-x_0^2) - (ab+cd)(x_0^4 - 6x_0^2z_0^2 + z_0^4)}{(ad-bc)(z_0^2+x_0^2)^2}, \\ d' &:= \frac{y_0^2}{(ad-bc)(z_0^2+x_0^2)^2}. \end{aligned} \tag{5}$$

As an important special case, if $b = 0$ then $(x_0 : y_0 : z_0) = (1 : 2d : 1)$ is an element of $\mathcal{H}_\eta(K)$, and if we use this point, eq. (5) reduces to $c' = \frac{c}{a}$ and $d' = \frac{d}{a}$.

For a general number field K not containing $\mathbb{Q}(i)$, we prove that there is a nonzero polynomial $q(u,v) \in K[u,v]$ such that when $q(c',d') \neq 0$, $\mathcal{H}_\eta(K)$ is infinite (proposition 5.1). By determining all possible rational roots of this polynomial in the case $K = \mathbb{Q}$, we obtain the following classification.

Theorem 1.4. *Let $K = \mathbb{Q}$, and $\eta = (a,b,c,d) \in \mathbb{Q}^4$ with $ad-bc \neq 0$. Suppose $\mathcal{H}_\eta(\mathbb{Q})$ has a point $(x_0 : y_0 : z_0)$, and define c', d' as in eq. (5). If $c' \neq 0$, $|d'| \neq 1$, and $(|c'|, |d'|) \neq \left(\left|\frac{1-r^4}{2r}\right|, r^2\right)$ for any $r \in \mathbb{Q}^\times$, then $\mathcal{H}_\eta(\mathbb{Q})$ is infinite.*

The proof is carried out in section 5. Each $(a,b,c,d) \in K^4$ with $ad - bc \neq 0$ can be interpreted as a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$; the first step of the proof (section 3.3) is to show that the isomorphism class of $\mathcal{H}_\eta$ is invariant on double cosets in

$$\mathrm{O}_2(K) \backslash \mathrm{GL}_2(K) / (K^\times \cdot \mathrm{O}_2(K)). \tag{6}$$

We can use this double coset invariance to replace η with a matrix $\eta' := \left(\begin{smallmatrix} 1 & 0 \\ c' & d' \end{smallmatrix}\right)$ (with c', d' as in eq. (5)) such that $\mathcal{H}_\eta \cong \mathcal{H}_{\eta'}$. The curve $\mathcal{H}_\eta$ has two marked points O and P; it suffices to determine conditions under which $\mathcal{H}_\eta$ is nonsingular and the divisor $[P] - [O]$ is non-torsion in the Jacobian of $\mathcal{H}_\eta$.

1.3. **Applications to Pythagorean slopes.** As discussed above, when $ad-bc \neq 0$, there is an open affine $U_\eta \subseteq \mathcal{H}_\eta$ and a degree 4 map $\Phi : U_\eta \to F_\eta$ mapping $U_\eta(K)$ onto $F_\eta(\mathcal{S}_K)$ (proposition 3.4). So if $\mathcal{H}_\eta(K)$ is infinite, F_η is guaranteed to have infinitely many Pythagorean solutions.

1.3.1. *Applications of theorem 1.4.* We can use theorem 1.4 to solve problem 1.2 for many $\eta \in \mathrm{GL}_2(\mathbb{Q})$. One consequence involves determining which rational numbers can be written as linear combinations of elements of $\mathcal{S}_\mathbb{Q}$.

Corollary 1.5. *Let $s,t \in \mathbb{Q}^\times$ with $|s| \neq |t|$. For all $r \in \mathbb{Q}^\times$ with $r \neq \pm\frac{s^2-t^2}{2\sqrt{st}}$, there are infinitely many pairs $(\alpha_1,\alpha_2) \in \mathcal{S}_\mathbb{Q}^2$ such that $s\alpha_1 + t\alpha_2 = r$.*

Proof. Let $\eta = (0, s, t, -r)$, and $(0:t:1) \in \mathcal{H}_\eta(\mathbb{Q})$. We have $c' = -\frac{r}{s}$ and $d' = -\frac{t}{s}$. By theorem 1.4, the given conditions on r,s,t imply that $\mathcal{H}_\eta(\mathbb{Q})$ is infinite. By proposition 3.4, the variety $F_\eta : sx_1 + tx_2 - r = 0$ has infinitely many Pythagorean solutions. □

For comparison, note that if we replace $\mathcal{S}_\mathbb{Q}$ with the set of rational squares (a set with a comparable natural density), the corresponding question is whether r is an output of the quadratic form $sx^2 + ty^2$. Unless $-st$ is a square in $\mathbb{Q}^\times$, there are infinitely many $r \in \mathbb{Q}$ that cannot be expressed by the quadratic form. Corollary 1.5 therefore shows that linear combinations of Pythagorean slopes typically cover a much larger set than linear combinations of squares.

Another application of theorem 1.4 is to the "three-distance problem:" finding points $P \in \mathbb{R}^2$ that have a rational distance from $(0,0)$, $(0,1)$, and $(1,1)$. While a large collection of one-parameter families of solutions to this problem is known (see section 2.2 for a history of the problem and some prior results), our new contribution is to produce a collection of one-parameter families that exhibit solutions on specific lines through the origin. Namely, we show that if a line through the origin has slope equal to a Pythagorean slope (i.e. it passes through a point (x,y) of the unit circle with $xy \neq 0$), then it contains a dense set of solutions to the three-distance problem.

Corollary 1.6. *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 $\mathbb{R}^2$.

The proof can be found in section 6.1. Note that the line $x = 0$ also has a dense subset of solutions to the three-distance problem, given by $\{(0, \alpha+1) : \alpha \in \mathcal{S}_\mathbb{Q}\}$. On the other hand, for any line through the origin that is not $x = 0$ or $y = \alpha x$ for some $\alpha \in \mathcal{S}_\mathbb{Q}$, there are no solutions.

1.3.2. *Exceptional families.* There are three one-parameter families of $(a,b,c,d) \in \mathbb{Q}^4$ with $ad - bc \neq 0$ for which theorem 1.4 is inconclusive:

$$(1,\ 0,\ 0,\ d), \qquad d \in \mathbb{Q}^\times,$$
$$(1,\ 0,\ c,\ 1), \qquad c \in \mathbb{Q},$$

$$\left(1,\, 0,\, \frac{1-r^4}{2r},\, r^2\right), \qquad r \in \mathbb{Q}^\times.$$

Up to double coset equivalence, every $\eta \in \mathbb{Q}^4$ with $\mathcal{H}_\eta(\mathbb{Q})$ finite and nonempty is in one of these three families. For these values of η, other techniques are required in order to determine whether F_η has Pythagorean solutions.

In the context of problem 1.2, the equations $x_1x_2 + t$ and $x_1 + x_2 + t$ for $t \in \mathbb{Q}$ result in curves $\mathcal{H}_\eta$ in the orbit of the first two of these families. Thus, in contrast to generic linear combinations (corollary 1.5), theorem 1.4 is not strong enough to determine which rational numbers can be written as a sum or product of two Pythagorean slopes. But for certain special values of η in the exceptional families, we can prove that $\mathcal{H}_\eta(\mathbb{Q})$ is infinite.

Proposition 1.7. *If $t \in \mathcal{S}_\mathbb{Q}$, then the equation $x_1 + x_2 = t$ has infinitely many Pythagorean solutions.*

This answers item 2 from the original list of questions. While not every rational number can be written as a sum of two Pythagorean slopes, three elements are sufficient.

Proposition 1.8. *For all $t \in \mathbb{Q}$, the equation $x_1 + x_2 + x_3 = t$ has infinitely many Pythagorean solutions.*

For products, there is unfortunately no analogue of proposition 1.7; some Pythagorean slopes can be written as products of two other Pythagorean slopes, and others can't. In another paper, the author presents a conjectural method for computing

$$\mathcal{T} := \{t \in \mathbb{Q} : t = \alpha_1\alpha_2 \text{ for infinitely many } \alpha_1, \alpha_2 \in \mathcal{S}_\mathbb{Q}\}$$

up to a set of density zero.

Proposition 1.9 ([11, Corollary 1.4])**.** *Assume the parity conjecture and the density conjecture. Given $t \in \mathbb{Q} - \{0, \pm 1\}$, let $\mathcal{P}_t$ denote the set consisting of odd primes p with $\operatorname{ord}_p(t) \neq 0$, primes $p \equiv 1 \mod 4$ with $\operatorname{ord}_p(t^2-1) > 0$, and 2 if and only if neither $\operatorname{ord}_2(t) = \pm 2$ nor $\operatorname{ord}_2(t^2-1) = 3$. The set $\mathcal{T} \subseteq \mathbb{Q}$ has density $\frac{1}{2}$, and there exists $S \subseteq \mathbb{Q}$ of density zero such that*

$$\mathcal{T} = \{t \in \mathbb{Q} - \{0, \pm 1\} : |\mathcal{P}_t| \text{ even}\} \cup S.$$

This is the closest we have to an answer to item 1 from the original list of questions. However, we do have an analogue of proposition 1.8.

Proposition 1.10. *For all $t \in \mathbb{Q}^\times$, the equation $x_1x_2x_3 = t$ has infinitely many Pythagorean solutions.*

Propositions 1.7, 1.8 and 1.10 are proven in section 6.2.

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

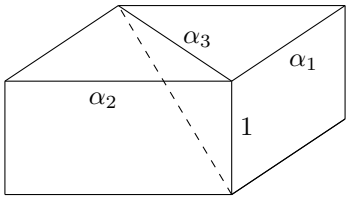

FIGURE 1. Elements of $\mathcal{S}_{\mathbb{Q}}$ in a perfect cuboid.

2. Related problems

There are a number of open problems regarding the existence of configurations of points in $\mathbb{R}^n$ in which certain distances between points are required to be rational; 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, for example, in [8]). 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 problem 1.2 to the congruent number problem.

2.1. **Perfect cuboid problem.**

Problem 2.1 (Perfect cuboid problem)**.** *Does there exist a rectangular prism such that the distance between any pair of vertices is rational?*

Given a hypothetical solution to this problem, we can scale it so that one edge has length 1. Letting α_1 and α_2 denote the edges and α_3 the diagonal of the face perpendicular to the edge of length 1 (fig. 1), we observe that $\alpha_1, \alpha_2, \alpha_3$ are in $\mathcal{S}_{\mathbb{Q}}$. Therefore the existence of a perfect cuboid is equivalent to the existence of a Pythagorean solution of $x_1^2 + x_2^2 = x_3^2$.

Finding Pythagorean solutions of polynomials in which all variables appear to a power greater than 1 is not possible using the tools developed in this paper. However, since α_1 and α_2 form the legs of a rational right triangle, a necessary condition for a perfect cuboid to exist is that $\alpha_2 = \alpha_1\alpha'$ for some $\alpha' \in \mathcal{S}_{\mathbb{Q}}$. Pythagorean solutions to this equation correspond to "body cuboids," which are cuboids with all edges and face diagonals rational, but the body diagonal possibly irrational. Body cuboids with a fixed value of $\alpha' = \frac{\alpha_2}{\alpha_1}$ correspond to Pythagorean solutions of the curve $F_\eta : \alpha' x_1 - x_2 = 0$ for $\eta = (0, \alpha', -1, 0)$, which by the framework developed in section 1.2 correspond to rational points on an elliptic curve depending on α'.

This association between body cuboids and a family of elliptic curves is well-studied; Luijk has an in-depth survey [12] that mentions this association as well as many other known results about perfect cuboids. Halbeisen and Hungerbüler [9] investigate Pythagorean solutions to F_η in slightly different language (if $\alpha' = \frac{a}{b}$ and F_η has a Pythagorean solution, they call (a, b) a *double-pythapotent pair*). In particular, they associate Pythagorean solutions of F_η with the elliptic curve

$$E_{a,b} : y^2 = x^3 + (a^2 + b^2)x^2 + a^2b^2x, \tag{7}$$

(we will later recognize this as eq. (14) at $\eta = \left(\begin{smallmatrix} 0 & a \\ -b & 0 \end{smallmatrix}\right)$), and show that there is a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ in $E_{a,b}(\mathbb{Q})$ which does not generate Pythagorean

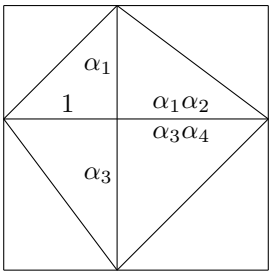

FIGURE 2. Elements of $\mathcal{S}_{\mathbb{Q}}$ in a square vertex distance configuration.

solutions. Ruling out other possible torsion points, they conclude [9, Theorem 8] that F_η has Pythagorean solutions if and only if $E_{a,b}$ has positive rank.

2.2. **Four-distance problem.**

Problem 2.2 (Four-distance problem)**.** *Does there exist a point in the plane which is a rational distance from every corner of the unit square* $[0,1]\times[0,1]$*?*

The coordinates of a solution $P=(x,y)$ are not a priori assumed to be rational, but since x^2+y^2, $(1-x)^2+y^2$, and $x^2+(1-y)^2$ must all be rational, the differences $2x-1$ and $2y-1$ must also be rational. Hence, given a hypothetical solution, we can scale the plane by an element of $\mathbb{Q}^\times$ so that the horizontal distance from the point to one edge of the square is equal to 1. We then find several right triangles, each of which contributes an element of $\mathcal{S}_{\mathbb{Q}}$ as in fig. 2. A solution to the square vertex distance problem is equivalent to the existence of Pythagorean solutions to the system of equations $1+x_1x_2=x_1+x_3$ and $x_1x_2=x_3x_4$.

This paper does not provide the tools to find solutions to systems of equations, but we can study each equation independently. Pythagorean solutions to $x_1x_2=x_3x_4$ give solutions to the "rectangle vertex distance problem" of finding a point and a rectangle such that all pairwise distances are rational. Solutions are obtained by fixing $t\in\mathbb{Q}^\times$ and finding two Pythagorean solutions to the polynomial $x_1x_2-t=0$. See proposition 1.9 for a conjectural classification of the set of t for which this is possible, up to a set of density zero.

Pythagorean solutions to $1+x_1x_2=x_1+x_3$ give solutions to the "three-distance problem," finding points such that the distances to three of the four corners of a square are rational. 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].

As one application of this paper's results, we can show that there is a dense set of solutions to the three-distance problem on any line through the origin passing a rational point on the unit circle, with the exception of one of the coordinate axes (corollary 1.6). These families are distinct from those that appear in [3, Table 4], though it is unclear whether any (or all) of the one-parameter families of corollary 1.6 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

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}ab = n, \qquad a, b, c \in \mathbb{Q}^\times. \tag{8}$$

Problem 2.3. *Determine whether a given $n \in \mathbb{Q}$ is a congruent number.*

This problem is not directly related to problem 1.2, but some of 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 problem 2.3; see for example the expositions [6] and [5]. For fixed n, any solution to eq. (8) corresponds to a rational point on an elliptic curve over $\mathbb{Q}$ defined by

$$E^{(n)} : y^2 = x^3 - n^2 x. \tag{9}$$

There are "degenerate points" in $E^{(n)}(\mathbb{Q})$ that do not correspond to solutions to eq. (8); 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 [18], 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

$$x_1 x_2 - 2n = 0, \qquad x_1 \in (\mathbb{Q}^\times)^2,\ x_2 \in \mathcal{S}_{\mathbb{Q}}. \tag{10}$$

Both $\mathcal{S}_{\mathbb{Q}}$ and $(\mathbb{Q}^\times)^2$ are contained in the image of a degree 2 rational function $\mathbb{Q} \to \mathbb{Q}$. 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. (10). This is directly analogous to the relation between $\mathcal{H}_\eta(K)$ (eq. (2)) and $F_\eta(\mathcal{S}_K)$ (eq. (1)).

However, it is worth highlighting a few key differences between problems 1.2 and 2.3.

- **Size of parameter space.** Congruent numbers are parametrized by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$; to study problem 1.2, we will use a double quotient of $\mathrm{GL}_2(K)$.
- **Existence of rational points.** Every n, whether congruent or not, determines an elliptic curve $E^{(n)}$; in particular, this curve has a rational point. By contrast, the genus one curves obtained in the study of problem 1.2 often have no rational points (theorem 1.3).
- **Closure under addition of degenerate points.** In both problems, the genus one curve has a set of "degenerate" rational points, which do not yield valid solutions to the original equations. In the case of problem 2.3, the set of degenerate points always equals the torsion subgroup of $E^{(n)}(\mathbb{Q})$. In problem 1.2, however, if we have an isomorphism $\mathcal{H}_\eta \to E_\eta$ for some elliptic curve E_η, the degenerate points in $\mathcal{H}_\eta(K)$ may not map to a subgroup of $E_\eta(K)$. This can be used to our advantage: we can 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 all isomorphic over $\overline{\mathbb{Q}}$; specifically, they are quadratic twists of the curve $y^2 = x^3 - x$. This fact is used in a key way in the proof of Tunnell's theorem, as he applies a result due to Waldspurger [19] relating the central value of the L-function of an elliptic curve with that of each of its quadratic twists. By contrast, a typical 1-parameter subfamily of problem 1.2 will define a family of curves that do not have constant j-invariant. This means that Tunnell's approach to computing the analytic rank does not apply to this family.

3. Setup

3.1. **Assumptions and notation.** Let K be a field of characteristic not equal to 2; while our main results only hold for number fields K, it is possible to develop much of the theory in a more general setting. Throughout this paper, all schemes will be defined over K unless otherwise indicated, and if X and Y are schemes then $X \times Y := X \times_K Y$. We use the notation $(x_0 : \ldots : x_n)$ to denote an element of $\mathbb{P}^n(K)$; that is, $(x_0 : \ldots : x_n)$ is the equivalence class of $(x_0, \ldots, x_n) \in K^{n+1}$ under scaling by $\lambda \in K^\times$. Given a matrix $\eta \in \mathrm{GL}_2(K)$, its transpose will be denoted η^t.

3.2. **Definition of $\mathcal{H}$ and basic properties.** Let $\widetilde{\mathbb{P}^2}$ be a weighted projective space over K, where the variables x, y, z have weights $1, 2, 1$, respectively. Let $\mathbb{A}^4$ denote the four-dimensional affine space over K. Using the coordinates $((x : y : z), (a, b, c, d))$ on $\widetilde{\mathbb{P}^2} \times \mathbb{A}^4$, define the variety $\mathcal{H}$ by the equation

$$\mathcal{H} : y^2 = (a(z^2 - x^2) + b(2xz))^2 + (c(z^2 - x^2) + d(2xz))^2. \tag{11}$$

If we let $N : K^2 \to K$ be defined by $N(u, v) = u^2 + v^2$, then this can equivalently be written

$$\mathcal{H} : y^2 = N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix}\right). \tag{12}$$

This variety comes equipped with a morphism $\pi : \mathcal{H} \to \mathbb{A}^4$, which equips $\mathcal{H}$ with the structure of a flat family of curves. Given $\eta = (a, b, c, d) \in \mathbb{A}^4(K)$, $\mathcal{H}_\eta$ is the fiber of π over η.

The generic fiber of π is a genus one hyperelliptic curve over $K(a, b, c, d)$, with discriminant

$$\Delta(\mathcal{H}) = 2^{16}(ad - bc)^4((a + d)^2 + (b - c)^2)((a - d)^2 + (b + c)^2). \tag{13}$$

The Jacobian variety of this curve is an elliptic curve over $K(a, b, c, d)$, and by classical invariant theory (see for example [20, 2]) we can show that it has a model

$$E : y^2 = x^3 + (a^2 + b^2 + c^2 + d^2)x^2 + (ad - bc)^2 x. \tag{14}$$

We have two commuting involutions on $\mathcal{H}$ as a scheme over $\mathring{A}^4$, given by

$$\sigma_1 : (x : y : z) \mapsto (x : -y : z) \qquad \text{and} \qquad \sigma_2 : (x : y : z) \mapsto (-z : y : x), \tag{15}$$

generating a Klein four-group

$$\Gamma := \langle \sigma_1, \sigma_2 \rangle \tag{16}$$

acting on $\mathcal{H}$.

3.3. **Double cosets and reduction.** For all $\eta = (a,b,c,d) \in \mathbb{A}^4(K)$ with $ad - bc = 0$, we can classify $\mathcal{H}_\eta(K)$ explicitly (appendix A). So from now on we only consider η such that $ad - bc \neq 0$. This means that η is contained in the image of the open immersion $\mathrm{GL}_2 \to \mathbb{A}^4$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \to (a,b,c,d)$; we will identify $\mathrm{GL}_2(K)$ with its image in $\mathbb{A}^4(K)$.

Let O_2 be the orthogonal group over K; 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 $MM^t = M^tM = I$. We show that the isomorphism class of $\eta \in \mathrm{GL}_2(K)$ is invariant on double cosets in

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

Assuming -1 is not a square in K, we will then show that $\mathcal{H}_\eta$ has a K-point if and only if η is in the same double coset as a lower triangular matrix.

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 $\tau : \mathcal{H}_\eta \to \mathcal{H}_{\eta'}$ 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 $(x : y : z) \in \mathcal{H}_\eta(\overline{K})$,

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

Thus the map

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

defines an isomorphism $\mathcal{H}_\eta \to \mathcal{H}_{\eta'}$, 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 $\eta' = \left(\begin{smallmatrix} 1 & 0 \\ c' & d' \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. We have $(1 : 2d' : 1) \in \mathcal{H}_{\eta'}(K)$, so by lemma 3.1, we can conclude that $\mathcal{H}_\eta(K)$ is nonempty. The converse does not hold in general (remark 3.3), but it does hold for all fields in which -1 is not a square.

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 $P = (x_0 : y_0 : z_0) \in \mathcal{H}_\eta(K)$ with $y_0(x_0^2 + z_0^2) \neq 0$. Define c', d' as in eq. (5), and set $\eta' = \left(\begin{smallmatrix} 1 & 0 \\ c' & d' \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Then $\mathcal{H}_\eta \cong \mathcal{H}_{\eta'}$.*

If -1 is not a square in K, then the condition $y_0(x_0^2 + z_0^2) \neq 0$ holds for all $P \in \mathcal{H}_\eta(K)$.

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

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

are both well-defined elements of $\mathrm{SO}_2(K)$. Setting $\lambda = \frac{y_0}{(ad-bc)(z_0^2+x_0^2)}$, we can check by direct computation that $\lambda r_1 \eta r_2 = \eta'$. The result follows by lemma 3.1.

Now assume -1 is not a square in K, and 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. Hence $z_0 = 0$, and likewise $x_0 = 0$. But this implies $y_0 = 0$, which contradicts the fact that $(x_0 : y_0 : z_0) \in \widetilde{\mathbb{P}^2}(K)$.

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 $y_0 \neq 0$. □

Remark 3.3. The condition $y_0(x_0^2 + z_0^2) \neq 0$ is necessary. For instance, let $K = \mathbb{Q}(i)$ and $\eta = \left(\begin{smallmatrix} 2 & 1 \\ 2i & 1 \end{smallmatrix}\right)$. The curve $\mathcal{H}_\eta$ has two K-points $(0:0:1)$ and $(1:0:0)$; we can check that there are no others by computing the Mordell-Weil group of the Jacobian $y^2 = x^3 + 2x^2 - 8ix$ over $\mathbb{Q}(i)$ and checking that it has only two points. But for any $\eta' = \left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$, there are at least four points in $\mathcal{H}_{\eta'}(K)$, given by $(1:2d:1)$, $(-1:2d:1)$, $(1:-2d:1)$, and $(-1:-2d:1)$. Hence $\mathcal{H}_\eta$ is not isomorphic to $\mathcal{H}_{\eta'}$ for any lower triangular matrix η'.

3.4. **Pythagorean solutions.** Let $(a, b, c, d) \in K^4$. Recall that our aim (problem 1.2) is to determine whether the affine curve

$$F_\eta : ax_1x_2 + bx_1 + cx_2 + d = 0$$

has a Pythagorean solution. This is straightforward if $ad - bc = 0$ (appendix A), so we consider the case $ad - bc \neq 0$, in which case (a, b, c, d) can be associated with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$.

In eq. (11), 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 $N(u, v) \coloneqq u^2 + v^2$. Define the *degenerate locus* $\mathcal{D}$ as the subset of $\mathcal{H}$ defined by

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

The group Γ (eq. (16)) preserves $\mathcal{D}$ and acts freely on $\mathcal{H} - \mathcal{D}$.

Proposition 3.4. *Suppose* $\eta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. *There is a morphism* $\Phi : (\mathcal{H} - \mathcal{D})_\eta \to F_\eta$ *defined by sending* $(x : y : z)$ *to*

$$\left(-\frac{c(z^2 - x^2) + d(2xz)}{a(z^2 - x^2) + b(2xz)}, \frac{z^2 - x^2}{2xz}\right). \tag{18}$$

Further, Φ *induces a bijection between the set of* Γ*-orbits in* $(\mathcal{H} - \mathcal{D})_\eta(K)$ *and Pythagorean solutions of* F_η.

Proof. Let $\mathbb{P}^1 \times \mathbb{P}^1$ have coordinates $((u_1 : v_1), (u_2 : v_2))$, and define the subvariety $\mathcal{F}_\eta$ by

$$\begin{aligned} 0 &= au_1u_2 + bu_1v_2 + cv_1u_2 + dv_1v_2 \\ &= \begin{pmatrix} u_1 & v_1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} u_2 \\ v_2 \end{pmatrix}. \end{aligned} \tag{19}$$

Note that we can identify F_η with the open affine subset $\mathcal{F}_\eta \cap \mathbb{A}^2$ by the map $(x_1, x_2) \mapsto ((x_1 : 1), (x_2 : 1))$. We define a morphism $\widetilde{\Phi} : \mathcal{H}_\eta \to \mathcal{F}_\eta$ by

$$(x : y : z) \mapsto \left((-c(z^2 - x^2) - d(2xz) : a(z^2 - x^2) + b(2xz)),\ (z^2 - x^2 : 2xz)\right). \tag{20}$$

This is a valid morphism to $\mathcal{F}_\eta$ because

$$\begin{aligned}
&\left(\begin{pmatrix} -c & -d \\ a & b \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix}\right)^t \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix} \\
&\quad = \begin{pmatrix} z^2 - x^2 & 2xz \end{pmatrix}\begin{pmatrix} 0 & ad - bc \\ -ad + bc & 0 \end{pmatrix}\begin{pmatrix} z^2 - x^2 \\ 2xz \end{pmatrix} \\
&\quad = 0.
\end{aligned}$$

The pullback of $v_1 v_2 = 0$ under $\widetilde{\Phi}$ is the subvariety of $\mathcal{H}_\eta$ defined by $xz(a(z^2 - x^2) + b(2xz)) = 0$, which is contained in the degenerate locus. Thus $\widetilde{\Phi}$ can be restricted to a morphism $\Phi : (\mathcal{H} - \mathcal{D})_\eta \to F_\eta$.

Now suppose $(x : y : z) \in \mathcal{H}_\eta(K)$ is not in the degenerate locus. Then

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

and since $xz(z^2 - x^2)(z^2 + x^2) \neq 0$, we have $\frac{z^2 - x^2}{2xz} \in \mathcal{S}_K$. We also have

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

and since $y(a(z^2 - x^2) + b(2xz))(c(z^2 - x^2) + d(2xz)) \neq 0$, we have $\frac{-c(z^2 - x^2) - d(2xz)}{a(z^2 - x^2) + b(2xz)} \in \mathcal{S}_K$. Thus Φ maps non-degenerate points in $\mathcal{H}_\eta(K)$ to Pythagorean solutions of F_η.

Conversely, given any Pythagorean solution (α_1, α_2) of F_η, we can write $\alpha_2 = \frac{z^2 - x^2}{2xz}$ and $\alpha_1 = \frac{z'^2 - x'^2}{2x'z'}$. 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 $(x : y : z) \in \mathcal{H}_\eta(K)$ for $y = \lambda(z'^2 + x'^2)$. By definition of x, z, x', z', we have $xz(z^2 - x^2)(z^2 + x^2) \neq 0$, and

$$\begin{aligned}
&y(a(z^2 - x^2) + b(2xz))(c(z^2 - x^2) + d(2xz)) \\
&\quad = \left(\pm\lambda(z'^2 + x'^2)\right)\left(\lambda(-2x'z')\right)\left(\lambda(z'^2 - x'^2)\right) \\
&\quad \neq 0,
\end{aligned}$$

so that $(x : y : z)$ is an element of $(\mathcal{H} - \mathcal{D})_\eta(K)$, and by

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

we have $\Phi((x:y:z)) = (\alpha_1, \alpha_2)$. Hence Φ maps $(\mathcal{H}-\mathcal{D})_\eta(K)$ surjectively onto the set of Pythagorean solutions of F_η.

Finally, observe that for each $\alpha_2 \in \mathcal{S}_K$, there are two choices for $(x:z) \in \mathbb{P}^1(K)$ with $\frac{z^2-x^2}{2xz} = \alpha_2$, 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. □

4. Everywhere locally soluble curves are sparse

For the remainder of the paper, we assume K is a number field.

4.1. **Conditions for local solubility.** Suppose v is an infinite place of K, so that $K_v = \mathbb{R}$ or $\mathbb{C}$. Since the squares in K_v are closed under addition, $\mathcal{H}_\eta(K_v)$ is nonempty for all $\eta \in \mathrm{GL}_2(K)$. This will not be true in general if v is a finite place, as the following result shows.

Lemma 4.1. *Let K be a number field, $\mathcal{O}_K$ the ring of integers of K, and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. Let $a, b, c, d \in \mathcal{O}_K$. If $ad - bc \in \mathfrak{p}$, and neither $a^2 + b^2$ nor $a^2 + c^2$ are a square modulo $\mathfrak{p}$, then $\mathcal{H}_\eta(K_\mathfrak{p})$ is empty.*

Proof. First note that if $k_\mathfrak{p}$ has characteristic 2, or if $a \in \mathfrak{p}$, then $a^2 + b^2$ and $a^2 + c^2$ are necessarily squares modulo $\mathfrak{p}$. So from now on we assume $a \notin \mathfrak{p}$ and $\operatorname{char} k_\mathfrak{p}$ is odd.

For the sake of contradiction, assume $(x : y : z) \in \mathcal{H}_\eta(K_\mathfrak{p})$. We can assume without loss of generality that x, y, z are in $\mathcal{O}_\mathfrak{p}$, the valuation ring of $K_\mathfrak{p}$. If x and z both have valuation at least 1, then from the equation

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

defining $\mathcal{H}_\eta$, we see that the right-hand side has valuation at least 4, and therefore y has valuation at least 2. This implies $\frac{x}{\pi}, \frac{y}{\pi^2}, \frac{z}{\pi} \in \mathcal{O}_\mathfrak{p}$, where π is a uniformizer of $\mathcal{O}_\mathfrak{p}$. So without loss of generality we may assume that at least one of x, z is in $\mathcal{O}_\mathfrak{p}^\times$.

Let $\overline{x}$ denote the image of x in $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong k_\mathfrak{p}$, and likewise for all other elements of $\mathcal{O}_\mathfrak{p}$. Since $\overline{ad} = \overline{bc}$, we have

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

If $\overline{a}(\overline{z}^2 - \overline{x}^2) + \overline{b}(2\overline{xz}) \neq 0$, then

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

is a square in $k_\mathfrak{p}$. Now suppose $\overline{a}(\overline{z}^2 - \overline{x}^2) + \overline{b}(2\overline{xz}) = 0$. If $\overline{xz} = 0$, then since $\overline{a} \neq 0$ we must have $\overline{z}^2 - \overline{x}^2 = 0$. But this implies $\overline{z} = \overline{x} = 0$, contradicting our assumption that at least one of x and z is in $\mathcal{O}_\mathfrak{p}^\times$. Hence $\overline{xz} \neq 0$, so that

$$\begin{aligned}\overline{a}^2 + \overline{b}^2 &= \overline{a}^2 + \left(\frac{-\overline{a}(\overline{z}^2 - \overline{x}^2)}{2\overline{xz}}\right)^2 \\ &= \left(\frac{\overline{a}(\overline{z}^2 + \overline{x}^2)}{2\overline{xz}}\right)^2\end{aligned}$$

is a square in $k_\mathfrak{p}$. Thus either $\overline{a}^2 + \overline{b}^2$ or $\overline{a}^2 + \overline{c}^2$ is a square in $k_\mathfrak{p}$, a contradiction. Therefore no point in $\mathcal{H}_\eta(K_\mathfrak{p})$ can exist. □

Let R be a ring and $\mathfrak{a}$ an ideal of R. For any positive integer n, there is a reduction map $R^n \to (R/\mathfrak{a})^n$; the fibers of this map will be called $\mathfrak{a}$-*residue disks* of R^n.

Lemma 4.2. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ with $q := |k_\mathfrak{p}|$ odd. Let $\mathcal{C}_\mathfrak{p}$ denote the set of $(a,b,c,d) \in \mathcal{O}_K^4$ such that $\mathcal{H}_\eta(K_\mathfrak{p})$ is nonempty. Then $\mathcal{C}_\mathfrak{p}$ is contained in a union of $q^4 - \frac{1}{4}(q-1)^3$ $\mathfrak{p}$-residue disks of R^4.*

Proof. We show that there are at least $\frac{1}{4}(q-1)^3$ $\mathfrak{p}$-residue disks satisfying the conditions of lemma 4.1, so that $\mathcal{H}_\eta(K_\mathfrak{p})$ is empty for all η in these $\mathfrak{p}$-residue disks. This will show that $\mathcal{C}_\mathfrak{p}$ is contained in the $q^4 - \frac{1}{4}(q-1)^3$ remaining disks.

If $\overline{a} \neq 0$, then a^2+b^2 is a square mod $\mathfrak{p}$ if and only if $\overline{b} = \overline{a}\frac{1-t^2}{2t}$ for some $t \in k_\mathfrak{p}^\times$. Since t and $-\frac{1}{t}$ have the same image under the map $t \mapsto \overline{a}\frac{1-t^2}{2t}$, this map is two-to-one on $k_\mathfrak{p}^\times - \{t \in k_\mathfrak{p}^\times : t^2 = -1\}$. Therefore,

$$\#\{\overline{b} \in k_\mathfrak{p} : \overline{a}^2 + \overline{b}^2 \text{ square in } k_\mathfrak{p}\} = \begin{cases} \frac{q+1}{2} & \text{if } q \equiv 1 \pmod 4, \\ \frac{q-1}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

In order to satisfy the conditions of lemma 4.1, we need b and c such that a^2+b^2 and a^2+c^2 are both *not* squares in $k_\mathfrak{p}$. There are $q-1$ residue classes for a, at least $\frac{q-1}{2}$ residue classes for b, and at least $\frac{q-1}{2}$ residue classes for c; the residue class of $d \equiv \frac{bc}{a} \pmod{\mathfrak{p}}$ is then fixed. This gives us $\frac{1}{4}(q-1)^3$ $\mathfrak{p}$-residue disks over which $\mathcal{H}_\eta(K_\mathfrak{p})$ is guaranteed to be empty. □

4.2. **The upper bound.** We will use lemma 4.2 to bound the number of fibers of $\mathcal{H}$ that are everywhere locally soluble. Recall the full statement of theorem 1.3.

Theorem 1.3. *Let $\mathcal{C}(X)$ denote the set of $(a,b,c,d) \in \mathcal{O}_K^4$ with $H(a)$, $H(b)$, $H(c)$, $H(d) \leq X$. Let $\mathcal{C}_{loc}(X)$ denote the set of $\eta \in \mathcal{C}(X)$ such that $\mathcal{H}_\eta(K_v) \neq \varnothing$ for all places v of K. For all $\varepsilon > 0$, we have*

$$\frac{|\mathcal{C}_{loc}(X)|}{|\mathcal{C}(X)|} = O((\log\log X)^{-\frac{1}{4}+\varepsilon}),$$

with the implicit constant depending on K and ε.

To prove this, we will embed $\mathcal{O}_K$ as a lattice in $\mathbb{R}^n$, and use lemma 4.2 to identify $\mathcal{C}_{\text{loc}}(X)$ as the intersection of a convex body in $\mathbb{R}^{4n}$ with a union of ideal cosets, where the number of cosets is given by a product over prime ideals. Mertens' theorem is used in lemma 4.4 to bound the size of this product, and a fairly standard geometry of numbers argument (see for example the proof of [10, Theorem V.1]) is used in lemma 4.3 to estimate the size of the intersection of each ideal coset with the convex body.

For the rest of this section, γ_i will refer to a positive constant depending only on K, and $\gamma_i(\varepsilon)$ to a positive constant depending only on K and ε.

Lemma 4.3. *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and suppose all nonzero vectors in Λ have length at least 1. Let $C \subseteq \mathbb{R}^n$ be a convex set containing a ball of radius ℓ around the origin. For any $v \in \mathbb{R}^n$, the number of vectors in the shifted lattice $v+\Lambda$ that lie in C satisfies*

$$|C \cap (v+\Lambda)| \leq \left(1 + \frac{\gamma_0 \operatorname{covol}(\Lambda)}{\ell}\right)^n \frac{\operatorname{vol}(C)}{\operatorname{covol}(\Lambda)},$$

where $\gamma_0 := n2^n\Gamma(\frac{n}{2}+1)\pi^{-n/2}$.

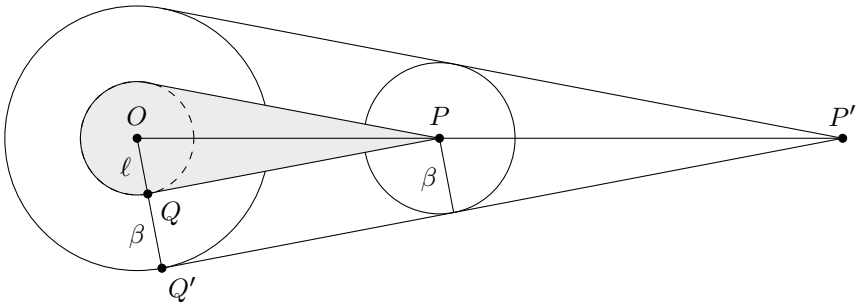

FIGURE 3. $(\frac{\beta}{\ell}+1)C$ contains a β-neighborhood of C (in gray).

Proof. We first prove that there exists a fundamental domain F of Λ which is not too long and thin. We will then show that for suitable scaling parameters $0 < r_1 < 1 < r_2$, we can find a collection of translates of F that contains C and is contained in r_2C, and a different collection of translates of F that contains r_1C and is contained in C. Since every shifted lattice will contain one point in each fundamental domain, this will give the desired bounds.

Let $\lambda_1, \dots, \lambda_n$ denote the successive minima of Λ. For each i, let $v_i \in L$ have length λ_i, and define

$$\widetilde{F} := \left\{ \sum_{i=1}^{n} t_i v_i : 0 \le t_i < 1. \right\}.$$

Then $\widetilde{F}$ contains a fundamental domain F (the containment may be proper because the vectors $v_1, \dots, v_n$ may not be a basis for L). For every $v, w \in F \subseteq \widetilde{F}$, we have

$$\|v - w\| \le \sum_{i=1}^{n} \lambda_i \le n\lambda_n \le \frac{n 2^n \Gamma(\frac{n}{2}+1)\operatorname{covol}(\Lambda)}{\pi^{n/2}\lambda_1 \cdots \lambda_{n-1}},$$

by Minkowski's second theorem [16, Theorem III.16]. Since all vectors in Λ have length at least 1, we have $\lambda_i \ge 1$ for all i and so $\|v - w\| \le \gamma_0 \operatorname{covol}(\Lambda)$.

Now let $\{u_1, \dots, u_m\} \subseteq \Lambda$ consist of all lattice vectors such that $u_i + F$ intersects C. For any $v \in \mathbb{R}^n$, every element of $(v+\Lambda)\cap C$ is in exactly one $u_i + F$, so $|(v+\Lambda)\cap C| \le m$. Setting $r_2 = 1 + \frac{\gamma_0 \operatorname{covol}(\Lambda)}{\ell}$, r_2C contains a ball of radius $\gamma_0 \operatorname{covol}(\Lambda)$ around every point in C (see fig. 3, with $\beta := \gamma_0 \operatorname{covol}(\Lambda)$ and O the origin. If C contains P, then it contains the triangle OQP by convexity; this implies r_2C contains $OQ'P'$. Since this holds for all planes through O and P, r_2C contains the ball of radius β around P). This shows that $u_i + F$ is contained in r_2C for all i. Thus the volume of r_2C is an upper bound for m times the volume of F, so

$$|(v+\Lambda)\cap C| \le \left(1 + \frac{\gamma_0 \operatorname{covol}(\Lambda)}{\ell}\right)^n \frac{\operatorname{vol}(C)}{\operatorname{covol}(\Lambda)}$$

as desired. □

Lemma 4.4. *For all $\varepsilon > 0$, there exists a constant $\gamma_1(\varepsilon) > 0$ such that for all $Y > 0$,*

$$\prod_{N(\mathfrak{p}) \le Y} 1 - \frac{(N(\mathfrak{p})-1)^3}{4N(\mathfrak{p})^4} < \gamma_1(\varepsilon)(\log Y)^{-\frac{1}{4}+\varepsilon},$$

where the product is taken over prime ideals in $\mathcal{O}_K$.

Proof. The function $f_1(x) = 1 - \frac{1}{4}x(1-x)^3$ has $f_1(0) = 1$ and $f_1'(0) = -\frac{1}{4}$, whereas the function $f_2(x) = (1-x)^{\frac{1}{4}-\varepsilon}$ has $f_2(0) = 1$ and $f_2'(0) = -\frac{1}{4} + \varepsilon$. Hence there exists $\delta > 0$ such that $f_1(x) < f_2(x)$ for all $0 < x < \delta$. Applying this to $x = \frac{1}{N(\mathfrak{p})}$, we have

$$\prod_{N(\mathfrak{p})\le Y} 1 - \frac{(N(\mathfrak{p})-1)^3}{4N(\mathfrak{p})^4} < \left(\prod_{N(\mathfrak{p})\le \delta^{-1}} 1 - \frac{(N(\mathfrak{p})-1)^3}{4N(\mathfrak{p})^4}\right)\left(\prod_{\delta^{-1}<N(\mathfrak{p})\le Y} 1 - \frac{1}{N(\mathfrak{p})}\right)^{\frac{1}{4}-\varepsilon}$$

$$= \gamma_3(\varepsilon)\left(\prod_{N(\mathfrak{p})\le Y} 1 - \frac{1}{N(\mathfrak{p})}\right)^{\frac{1}{4}-\varepsilon}, \tag{21}$$

where

$$\gamma_3(\varepsilon) := \prod_{N(\mathfrak{p})\le \delta^{-1}} \left(1 - \frac{(N(\mathfrak{p})-1)^3}{4N(\mathfrak{p})^4}\right)\left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-\frac{1}{4}+\varepsilon}$$

does not depend on Y. By an explicit verison of Merten's theorem for number fields [7, Theorem 1], we have

$$\prod_{N(\mathfrak{p})\le Y} 1 - \frac{1}{N(\mathfrak{p})} \le \frac{\gamma_4}{\log Y}.$$

Combining this with eq. (21) gives the desired result. □

Proof of theorem 1.3. Embed $\mathcal{O}_K$ as a lattice in $K \otimes \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$, where K has r real and s complex embeddings, and $n = r + 2s = [K : \mathbb{Q}]$. Let

$$R(X) := \{(v_1, \dots, v_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |v_i| \le X\}.$$

This is a product of r intervals of length $2X$ and s circles of radius X, and so it is a convex set with volume $2^r\pi^s X^n$. Note that $R(X)$ contains all $(v_i)_i \in \mathbb{R}^r \times \mathbb{C}^s$ with $\|v\| = \sqrt{|v_1|^2 + \cdots + |v_{r+s}|^2} \le X$.

First note that $\mathcal{C}(X) = (\mathcal{O}_K \cap R(X))^4$. Applying [10, Theorem V.1] (or using an argument similar to the proof of lemma 4.3), we can conclude that $|\mathcal{C}(X)| \ge \gamma_5 X^{4n}$.

In order to find an upper bound for the size of $\mathcal{C}_{\mathrm{loc}}(X)$, we will first define an ideal $\mathfrak{a}$ depending on X, and compute upper bounds on $N(\mathfrak{a})$ and on the intersection of ideal cosets of $\mathfrak{a}$ with $R(X)$. Let $\theta(x) = \sum_{p\le x} \log p$ denote the Chebyshev theta function; we have $\theta(x) < \gamma_6 x$ (for instance we can take $\gamma_6 = 1.02$ [15, Theorem 9]). Set $Y = \frac{1}{\gamma_6 n}\log X$ and define

$$\mathfrak{a} := \prod_{\substack{N(\mathfrak{p})\le Y,\\ \mathfrak{p}\nmid 2}} \mathfrak{p},$$

the product being taken over prime ideals in $\mathcal{O}_K$. This embeds as a full rank lattice in $K \otimes \mathbb{R}$, with

$$\mathrm{covol}(\mathfrak{a}) = 2^{-s} N(\mathfrak{a}) \sqrt{|\operatorname{disc} \mathcal{O}_K|} \tag{22}$$

by [10, Lemma V.2]. Let $f_{\mathfrak{p}}$ denote the inertia degree of $\mathfrak{p}$, so that $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$ for some rational prime p. Following [7, Section 2.1], we have

$$N(\mathfrak{a}) = \exp\left(\sum_{\substack{N(\mathfrak{p})\le Y,\\ \mathfrak{p}\nmid 2}} \log N(\mathfrak{p})\right)$$

$$
\begin{aligned}
&= \exp\left(\sum_{3\le p\le Y}\sum_{\mathfrak{p}\mid p}\log(p^{f_{\mathfrak{p}}})\right)\\
&= \exp\left(\sum_{3\le p\le Y}\left(\sum_{\mathfrak{p}\mid p} f_{\mathfrak{p}}\right)\log p\right)\\
&= \exp\left(n\theta(Y)+\log\gamma_7\right)\\
&< \gamma_7 X,
\end{aligned}
$$

where γ_7 is a correction term accounting for primes over 2 and the finitely many ramified primes of $K/\mathbb{Q}$. Using this bound, lemma 4.1 implies that for any $r\in\mathcal{O}_K$, we have

$$
\begin{aligned}
|(r+\mathfrak{a})\cap R(X)| &\le \left(1+\frac{\gamma_0 2^{-s}N(\mathfrak{a})\sqrt{|\operatorname{disc}\mathcal{O}_K|}}{X}\right)^n \frac{2^r\pi^s X^n}{2^{-s}N(\mathfrak{a})\sqrt{|\operatorname{disc}\mathcal{O}_K|}}\\
&< \gamma_8\frac{X^n}{N(\mathfrak{a})}.
\end{aligned}
\tag{23}
$$

Now suppose $(a,b,c,d)\in\mathcal{C}_{\mathrm{loc}}(X)$. For every prime ideal $\mathfrak{p}\nmid 2$ with norm at most Y, (a,b,c,d) lies in one of $N(\mathfrak{p})^4-\frac{1}{4}(N(\mathfrak{p})-1)^3$ of the $\mathfrak{p}$-residue disks of $M_2(\mathcal{O}_K)$, by lemma 4.2. By the Chinese remainder theorem, (a,b,c,d) lies in one of

$$
\prod_{\substack{N(\mathfrak{p})\le Y,\\ \mathfrak{p}\nmid 2}} N(\mathfrak{p})^4-\frac{1}{4}(N(\mathfrak{p})-1)^3
$$

$\mathfrak{a}$-residue disks. Given any $(a',b',c',d')\in\mathcal{C}(X)$ in the same $\mathfrak{a}$-residue disk, we must have $a'\in(a+\mathfrak{a})\cap R(X)$, and similar statements hold for b', c', and d'. Therefore, we can use eq. (23) and lemma 4.4 to conclude that

$$
\begin{aligned}
|\mathcal{C}_{\mathrm{loc}}(X)| &< \gamma_8^4 X^{4n}\left(\prod_{\substack{N(\mathfrak{p})\le Y,\\ \mathfrak{p}\nmid 2}} 1-\frac{(N(\mathfrak{p})-1)^3}{4N(\mathfrak{p})^4}\right)\\
&< \gamma_9(\varepsilon)X^{4n}(\log Y)^{-\frac{1}{4}+\varepsilon},
\end{aligned}
$$

with $\gamma_9(\varepsilon)$ incorporating γ_8^4, $\gamma_1(\varepsilon)$ from lemma 4.4, and factors involving the primes over 2.

Given our lower bound for $|\mathcal{C}(X)|$ and upper bound for $|\mathcal{C}_{\mathrm{loc}}(X)|$, we can conclude that

$$
\frac{|\mathcal{C}_{\mathrm{loc}}(X)|}{|\mathcal{C}(X)|} < \gamma_{10}(\varepsilon)(\log\log X)^{-\frac{1}{4}+\varepsilon},
$$

as we set out to show. □

5. Soluble fibers generically have infinitely many K-points

We continue to assume K is a number field, and now we add the assumption that a point $(x_0:y_0:z_0)\in\mathcal{H}_\eta(K)$ with $y_0(x_0^2+z_0^2)\neq 0$ is known. By lemma 3.2, the latter condition holds automatically when $\mathbb{Q}(i)\notin K$.

Proposition 5.1. *For any number field K, there exists a nonzero polynomial $q(x,y)\in K[x,y]$ with the following property. Given $\eta\in\mathrm{GL}_2(K)$ and $(x_0:y_0:z_0)\in\mathcal{H}_\eta(K)$ with $y_0(x_0^2+z_0^2)\neq 0$, define c' and d' as in eq. (5). If $q(c',d')\neq 0$, then $\mathcal{H}_\eta(K)$ is infinite.*

Proof. By lemma 3.2, $\mathcal{H}_\eta$ is isomorphic to $\mathcal{H}_{\eta'}$ for $\eta' = (1, 0, c', d')$. Without loss of generality we can replace η with η'. We will define the polynomial q so that $q(c,d)$ is a multiple of $\Delta(\mathcal{H}_\eta)$, so under the assumption $q(c,d) \neq 0$, $\mathcal{H}_\eta$ is nonsingular. Since $\mathcal{H}_\eta$ has a K-point, it is isomorphic to its Jacobian (eq. (14)),

$$E_\eta : y^2 = x^3 + (1 + c^2 + d^2)x^2 + d^2 x.$$

This curve has a point $R := (-1, c) \in E_{\eta'}(K)$, and if R is non-torsion then $\mathcal{H}_\eta(K)$ is infinite.

For each $\ell \geq 2$, let $\psi_\ell(c,d,x) \in \mathbb{Z}[c,d,x]$ denote the ℓ-th division polynomial on E_η; this is a polynomial with the property that $\psi_\ell(c,d,x) = 0$ for $x \in \overline{K}$ if and only if $(x,y) \in E_\eta(\overline{K})[\ell]$ for some $y \in \overline{K}$ (see for instance [17, Exercise 3.7]). By uniform boundedness of torsion in Mordell-Weil groups of elliptic curves over K [13], there is some finite $\mathcal{L} \subseteq \mathbb{N}$ such that the order of any torsion point in $E(K)$ is in $\mathcal{L}$ for any elliptic curve E/K. Define

$$q(c,d) := \Delta(E_\eta) \prod_{\ell \in \mathcal{L}} \psi_\ell(c,d,-1). \tag{24}$$

Then $q(c,d) \neq 0$ if and only if E_η is an elliptic curve and $(-1,c)$ is non-torsion in $E_\eta(K)$; these conditions imply $\mathcal{H}_\eta(K)$ is infinite. Setting $c = d = 2$ (for instance), we can check that the point $(-1,2)$ is non-torsion on the elliptic curve $y^2 = x^3 + 9x^2 + 4x$, so $q(c,d)$ is not identically zero. □

A priori, the set $\mathcal{L}$ only depends on K. However, we may be able to choose a smaller set $\mathcal{L}$ by placing restrictions on the possible torsion subgroups of $E_\eta(K)$ that can occur.

Lemma 5.2. *Suppose $\mathbb{Q}(i) \notin K$. Let $\eta = \left(\begin{smallmatrix} 1 & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. If $R := (-1, c) \in E_\eta(K)$ is torsion, then $|E_\eta(K)_{tors}|$ is a multiple of 4.*

Proof. There is an isomorphism $\mathcal{H}_\eta \to E_\eta$ sending $(1 : 2d : 1)$ to O, given by

$$\begin{aligned}(x : y : z) \mapsto \Bigg(& \frac{d}{(x-z)^2}(y + c(z^2 - x^2) + d(2xz)), \\ & \frac{d}{(x-z)^3}\begin{pmatrix} (1 + cd + c^2)(x-z)^2(x+z) \\ -cy(x-z) - 2cdx(x-z)(x+2z) \\ +dy(x+z) + 2d^2xz(x+z) \end{pmatrix}\Bigg).\end{aligned} \tag{25}$$

This isomorphism sends $(-1 : 2d : 1) \mapsto T := (0,0)$, $(-1 : -2d : 1) \mapsto (-d^2, -cd^2)$, and $(1 : -2d : 1) \mapsto R := (-1, c)$.[1]

The involution $\sigma_2 : (x : y : z) \mapsto (-z : y : x)$ on $\mathcal{H}_\eta$ has no fixed points over $\overline{K}$, so it induces a translation map $P \mapsto P + T$ on E_η. For any $(x_1 : y_1 : z_1) \in \mathcal{H}_\eta(\overline{K})$, the relation

$$\operatorname{div}\left(\frac{x - x_1}{x - 1}\right) = [(x_1 : y_1 : z_1)] + [(x_1 : -y_1 : z_1)] - [(1 : 2d : 1)] - [(1 : -2d : 1)]$$

[1] $(1 : -2d : 1)$ is not in the domain of definition of the rational function as it is written here. However, its image can be recovered from the divisor relation

$$[(1 : -2d : 1)] + [(1 : 2d : 1)] = [(-1 : 2d : 1)] + [(-1 : -2d : 1)] + \operatorname{div}\left(\frac{x+1}{x-1}\right)$$

on $\mathcal{H}_\eta$, which implies that $(1 : -2d : 1)$ must map to $(0,0) + (-d^2, -cd^2)$ in $E_\eta(K)$.

shows that the involution $\sigma_1 : (x : y : z) \mapsto (x : -y : z)$ on $\mathcal{H}_\eta$ induces the involution $P \mapsto R - P$ on E_η. Since -1 is not a square in K, there is no point in $\mathcal{H}_\eta(K)$ with $y = 0$ or with $x^2 + z^2 = 0$, so the involutions σ_1 and $\sigma_1\sigma_2$ have no fixed points in $\mathcal{H}_\eta(K)$.

As a result, Γ acts on $E_\eta(K)$ with no fixed points, and the orbit of a point $P \in E_\eta(\mathbb{Q})$ under Γ is given by $\{P, P+T, R-P, R-P+T\}$. Since R is torsion, the orbit of a torsion point P consists of torsion points. Hence the torsion subgroup of $E_\eta(K)$ is a disjoint union of orbits with four elements each. □

We can use this to prove the theorem 1.4.

Theorem 1.4. *Let $K = \mathbb{Q}$, and $\eta = (a, b, c, d) \in \mathbb{Q}^4$ with $ad - bc \neq 0$. Suppose $\mathcal{H}_\eta(\mathbb{Q})$ has a point $(x_0 : y_0 : z_0)$, and define c', d' as in eq. (5). If $c' \neq 0$, $|d'| \neq 1$, and $(|c'|, |d'|) \neq \left(\left|\frac{1-r^4}{2r}\right|, r^2\right)$ for any $r \in \mathbb{Q}^\times$, then $\mathcal{H}_\eta(\mathbb{Q})$ is infinite.*

Proof. Since $\mathbb{Q}(i) \notin \mathbb{Q}$, without loss of generality we can assume $\eta = \left(\begin{smallmatrix} 1 & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. For such η, the discriminant of E_η is

$$\Delta(E_\eta) = 16d^2(c^2 + (d-1)^2)(c^2 + (d+1)^2).$$

If this is zero for some $(c, d) \in \mathbb{Q}^2$, we must have either $d = 0$ (contradicting $\eta \in \mathrm{GL}_2(K)$), $(c, d) = (0, -1)$, or $(c, d) = (0, 1)$.

Assuming $\Delta(E_\eta) \neq 0$, it suffices to determine all values $(c, d) \in \mathbb{Q}^2$ such that $R := (-1, c)$ is torsion on E_η. By lemma 5.2, if R is torsion, then the torsion subgroup of $E_\eta(K)$ has order dividing 4. Using the classification of torsion subgroups of Mordell-Weil groups of elliptic curves over $\mathbb{Q}$, the order of any non-identity torsion element in $E_\eta(K)$ must be in $\mathcal{L} := \{2, 3, 4, 6, 8, 12\}$. For each $\ell \in \mathcal{L}$, we compute the division polynomial $\psi_\ell(c, d, x)$, and determine all possible $(c, d) \in \mathbb{Q}^2$ such that $\psi_\ell(c, d, -1) = 0$; this is carried out in appendix B. Using these computations we obtain the following possibilities:

(1) $(-1, c)$ has order 2 if and only if $c = 0$;
(2) $(-1, c)$ has order 4 if and only if $d = \pm 1$;
(3) $(-1, c)$ has order 8 if and only if $(c, d) = \left(\pm_1 \frac{1-r^4}{2r}, \pm_2 r^2\right)$ for some $r \in \mathbb{Q}^\times$ and some choice of signs $\pm_1, \pm_2 \in \{-1, 1\}$.

No other order can occur. Thus, if none of these conditions hold, then $\mathcal{H}_\eta(\mathbb{Q})$ is infinite by proposition 5.1. □

6. Applications

We begin by noting that for any embedding $K \hookrightarrow \mathbb{R}$, if $\mathcal{H}_\eta(K)$ is infinite, then $F_\eta(\mathcal{S}_K)$ is dense in $F_\eta(\mathbb{R})$. This is a special case of the following result.

Lemma 6.1. *Let $\eta \in \mathrm{GL}_2(\mathbb{R})$ and suppose $\Delta(\mathcal{H}_\eta) \neq 0$. Let $A \subseteq \mathcal{H}_\eta(\mathbb{R})$ be the image of an infinite subgroup of $E_\eta(\mathbb{R})$ under some isomorphism $E_\eta(\mathbb{R}) \cong \mathcal{H}_\eta(\mathbb{R})$. Then the image of $A - \mathcal{D}_\eta(\mathbb{R})$ under $\Phi : (\mathcal{H} - \mathcal{D})_\eta \to F_\eta$ (proposition 3.4) is dense in $F_\eta(\mathbb{R})$.*

Proof. The (topological) curve $\mathcal{H}_\eta(\mathbb{R})$ 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 $\widetilde{\mathbb{P}^2}$ (section 3.2), and there are no points with $y = 0$ because $\Delta(\mathcal{H}_\eta) \neq 0$. Thus $E_\eta(\mathbb{R})$ has structure of a Lie group $S^1(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$. Any infinite subgroup of $E_\eta(\mathbb{R})$ has

dense intersection with the identity component, so A has dense intersection with one of the components of $\mathcal{H}_\eta(\mathbb{R})$.

As in the proof proposition 3.4, let $\mathcal{F}_\eta$ be the projective closure of F_η in $\mathbb{P}^1 \times \mathbb{P}^1$. We can express the map $\widetilde{\Phi} : \mathcal{H}_\eta \to \mathcal{F}_\eta$ as a composition

$$\begin{array}{ccccc} \mathcal{H}_\eta & \to & \mathbb{P}^1 & \to & \mathcal{F}_\eta \\ (x:y:z) & \mapsto & (x:z) & \mapsto & \left((-c(z^2-x^2)-d(2xz) : a(z^2-x^2)+b(2xz)),\ (z^2-x^2 : 2xz)\right). \end{array}$$

The first map induces a continuous surjection from each component of $\mathcal{H}_\eta(\mathbb{R})$ 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 $\mathbb{P}^1(\mathbb{R}) \to \mathcal{F}_\eta(\mathbb{R})$, so the image of A is dense in $\mathcal{F}_\eta(\mathbb{R})$. Removing finitely many points from a space does not affect whether a given subset is dense, so the image of $A - \mathcal{D}_\eta(\mathbb{R})$ under the restricted map Φ is dense in $F_\eta(\mathbb{R})$. □

6.1. **Application to three-distance problem.** We will use theorem 1.4 to prove the following statement.

Corollary 1.6. *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 start by proving a slightly weaker result: 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 $d(t) := 1 - \frac{2t}{1-t^2}$. There is no rational solution to $1 = \frac{2t}{1-t^2}$, so $\eta(t) := \left(\begin{smallmatrix} 1 & 0 \\ -1 & d(t) \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathbb{Q})$. We have $|d(t)| \neq 1$ because we excluded the case $t = 0$ and there is no rational solution to $2 = \frac{2t}{1-t^2}$. Further, there is no rational solution to $\left|\frac{1-r^4}{2r}\right| = 1$. Hence, by theorem 1.4, $\mathcal{H}_{\eta(t)}(\mathbb{Q})$ is infinite. This implies that for each such t, there are infinitely many $\alpha_1, \alpha_2 \in \mathcal{S}_{\mathbb{Q}}$ such that $\alpha_1\alpha_2 + 1 = \alpha_1 + \frac{2t}{1-t^2}$ (the defining equation of $F_{\eta(t)}$); by lemma 6.1, the set $F_{\eta(t)}(\mathcal{S}_{\mathbb{Q}})$ is dense in $F_{\eta(t)}(\mathbb{R})$.

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

$$z(x_1, x_2) := \left(\frac{1-t^2}{x_1(1-t^2)+2t}, \frac{2t}{x_1(1-t^2)+2t}\right). \tag{26}$$

The map z restricts to a homeomorphism

$$F_{\eta(t)}(\mathbb{R}) - \left\{\left(-\tfrac{2t}{1-t^2}, \tfrac{1-t^2}{2t}\right)\right\} \to \left\{(x,y) \in \mathbb{R}^2 : y = \tfrac{2t}{1-t^2}x\right\} - \{(0,0)\},$$

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

the point $(x,y) := z(\alpha_1,\alpha_2)$ satisfies

$$x^2+y^2 = \left(\frac{1+t^2}{\alpha_1(1-t^2)+2t}\right)^2,$$
$$x^2+(1-y)^2 = \left(\frac{1-t^2}{\alpha_1(1-t^2)+2t}\right)^2(1+\alpha_1^2),$$
$$(1-x)^2+(1-y)^2 = \left(\frac{(1-t^2)\alpha_1}{\alpha_1(1-t^2)+2t}\right)^2(\alpha_2^2+1),$$

with the last line using the fact that $\alpha_1(1-t^2)+2t = (1-t^2)(\alpha_1\alpha_2+1)$. Since $\alpha_1,\alpha_2 \in \mathcal{S}_{\mathbb{Q}}$, these are all squares in $\mathbb{Q}^\times$, 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

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

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 $\mathbb{P}^2 \times \mathbb{A}^4$ parametrizing the Jacobian varieties of $\mathcal{H}$ (defined by eq. (14)). 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 $\mathcal{H}'_t = \mathcal{H}_{\eta(t)}$. We have a section $V \to \mathcal{H}'$ given by $t \mapsto (1 : 2d(t) : 1)$, allowing us to define an explicit 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 $\Phi' : \mathcal{H}' \dashrightarrow \mathbb{A}^2 \times V$ is defined by

$$((x:y:z),t) \mapsto \left(\frac{(z^2-x^2)-d(t)(2xz)}{z^2-x^2}, \frac{z^2-x^2}{2xz}, t\right).$$

  Note that after restricting to a fiber $\mathcal{H}'_t$, and then removing the finitely many degenerate points, the first two components of Φ' agree with the map $\Phi : (\mathcal{H}-\mathcal{D})_{\eta(t)} \to F_{\eta(t)}$ (proposition 3.4). So for any $t \in V(\mathbb{Q})$, there are finitely many values of n such that $\Phi' \circ \varepsilon \circ \tau_n$ is not defined at t, and the set

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

  is contained in $F_{\eta(t)}(\mathcal{S}_{\mathbb{Q}}) \times \{t\}$. By lemma 6.1, S_t is a dense subset of $F_{\eta(t)}(\mathbb{R}) \times \{t\}$.

- 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

$$z'(u,v,t) = \left(\frac{1-t^2}{u(1-t^2)+2t}, \frac{2t}{u(1-t^2)+2t} \right).$$

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. (26). So the same proof as above shows that z' maps $S_t - \{(-\frac{2t}{1-t^2}, \frac{1-t^2}{2t})\}$ to a dense subset of the line $y = \frac{2t}{1-t^2}x$ consisting of solutions to the three-distance problem. □

6.2. **Sums and products of Pythagorean slopes.** We first prove that every Pythagorean slope can be written as a sum of Pythagorean slopes in infinitely many ways.

Proof of proposition 1.7. Let $t = \frac{1-s^2}{2s}$ for some $s \in \mathbb{Q} - \{0, \pm 1\}$. The equation $x_1 + x_2 - t = 0$ defines F_η for $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -t \end{smallmatrix}\right)$, and $\mathcal{H}_\eta$ (which contains the rational point $(0:1:1)$) is isomorphic to its Jacobian (as in eq. (14)),

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

This curve has a rational point $\left(s, \frac{1}{2}(s+1)^2\right)$, which is non-torsion for all $s \in \mathbb{Q} - \{0, \pm 1\}$. Hence $\mathcal{H}_\eta$ has infinitely many rational points, so $F_\eta(\mathcal{S}_K)$ is infinite by proposition 3.4. □

This allows us to prove that every rational number can be written as a sum of three Pythagorean slopes in infinitely many ways.

Proof of proposition 1.8. The equation $x_1 + 2x_2 - t = 0$ defines F_η for $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 2 & -r \end{smallmatrix}\right)$. Now $\mathcal{H}_\eta$ is isomorphic to $\mathcal{H}_{\eta'}$ for $\eta' = \left(\begin{smallmatrix} 1 & 0 \\ -t & 2 \end{smallmatrix}\right)$, and by theorem 1.4, $\mathcal{H}_\eta(\mathbb{Q})$ 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 $(\alpha_1, \alpha_2) \in \mathcal{S}_{\mathbb{Q}}^2$.

To handle the case $t = 0$, we apply proposition 1.7: there are infinitely many triples $(\alpha_1, \alpha_2, \alpha_3)$ such that $\alpha_1 + \alpha_2 - \alpha_3 = 0$. This is a sum of three Pythagorean slopes because $\mathcal{S}_{\mathbb{Q}}$ is closed under negation. □

We finally prove that every nonzero rational number can be written as a product of three Pythagorean slopes in infinitely many ways.

Proof of proposition 1.10. We will show that for any $t \in \mathbb{Q}^\times$, there exists $s \in \mathbb{Q} - \{0, \pm 1\}$ such that when $d = -t\left(\frac{2s}{1-s^2}\right)$, the polynomial $x_1 x_2 + d$ has infinitely many Pythagorean solutions. Each of these solutions can then be multiplied by $\frac{1-s^2}{2s}$ to exhibit t as a product of three Pythagorean slopes.

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

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

If we set $s = t^2 + 2$, 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 $t \in \mathbb{Q} - \{0, \pm 1\}$, $x_1x_2 - t\left(\frac{2s}{1-s^2}\right)$ has infinitely many Pythagorean solutions, so t can be written as a product of three Pythagorean slopes in infinitely many different ways.

We finally must handle $t = \pm 1$. In this case, we can set $s = \frac{5}{6}$. 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 $x_1x_2 \mp \frac{60}{11} = 0$, allowing us to write ± 1 as a product $\alpha_1\alpha_2\frac{11}{60}$ of three Pythagorean triples in infinitely many ways. □

Remark 6.2. 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 [14] who used a similar method to find a positive rank subfamily of the curve $y^2 = x(x-1)\left(x - \left(\frac{2s}{1-s^2}\right)^2\right)$.

Appendix A. Singular fibers

Let K be an arbitrary field of characteristic not equal to 2, and let $\eta = (a, b, c, d) \in K^4$ be such that

$$\mathcal{H}_\eta : y^2 = (a(z^2 - x^2) + b(2xz))^2 + (c(z^2 - x^2) + d(2xz))^2$$

is singular. In this appendix, we classify the K-points of $\mathcal{H}_\eta$, as well as the Pythagorean solutions of

$$F_\eta : ax_1x_2 + bx_1 + cx_2 + d = 0.$$

The discriminant of $\mathcal{H}_\eta$ is given by

$$\Delta(\mathcal{H}_\eta) = (ad - bc)((a+d)^2 + (b-c)^2)((a-d)^2 + (b+c)^2) = 0. \tag{27}$$

We divide into two cases, depending on the coefficients (a, b, c, d). We will see that each case corresponds to a different number of geometric components $\mathcal{H}_\eta$ (that is, a different number of irreducible components of the base change of $\mathcal{H}_\eta$ to $\overline{K}$). If -1 is not a square in K, then only the first case is possible, and in this case we can produce a complete parametrization of $\mathcal{H}_\eta(K)$ and of the Pythagorean solutions of F_η.

A.1. **Two geometric components.** Suppose $ad - bc = 0$ or $a \pm d = b \mp c = 0$. In this case, the equation for $\mathcal{H}_\eta$ will take the form

$$y^2 = kg(x, z)^2,$$

where $k \in K$ and $g(x,z) \in K[x,z]$ is quadratic. Specifically, we have

$$\begin{aligned}
y^2 &= (c(z^2-x^2)+d(2xz))^2 && \text{if } a=b=0,\\
y^2 &= (b^2+d^2)(2xz)^2 && \text{if } a=c=0,\\
y^2 &= \tfrac{1}{a^2}(a^2+c^2)(a(z^2-x^2)+b(2xz))^2 && \text{if } a\neq 0 \text{ and } ad-bc=0,\\
y^2 &= (a^2+b^2)(z^2+x^2)^2 && \text{if } a\pm d = b\mp c = 0.
\end{aligned} \tag{28}$$

Over $\overline{K}$, $\mathcal{H}_\eta$ splits into two conics, $y=\sqrt{k}g(x,z)$ and $y=-\sqrt{k}g(x,z)$. If $k=r^2$ for some $r\in K$, then these components are defined over K, and

$$\mathcal{H}_\eta(K) = \{(x:\pm rg(x,z):z) : (x:z)\in\mathbb{P}^1(K)\}.$$

If k is not a square, then any K-point of $\mathcal{H}_\eta$ must satisfy $y=g(x,z)=0$. Hence $\mathcal{H}_\eta(K)$ has 0, 1, or 2 points, depending on how $g(x,z)$ factors over K.

If $ad-bc=0$, then proposition 3.4 does not apply, but we can find Pythagorean solutions of F_η directly by solving linear single-variable equations. For instance, if $a\neq 0$, then F_η is given by $a(x_1+\frac{c}{a})(x_2+\frac{b}{a})=0$; if $-\frac{c}{a}\in\mathcal{S}_K$ then $(-\frac{c}{a},\alpha_2)$ is a Pythagorean solution of F_η for all $\alpha_2\in\mathcal{S}_K$, and if $-\frac{b}{a}\in\mathcal{S}_K$ then $(\alpha_1,-\frac{b}{a})$ is a Pythagorean solution of F_η for all $\alpha_1\in\mathcal{S}_K$. If $a=0$ then F_η is defined by a single linear equation in one variable and can be handled in a similar way.

Proposition A.1. *Let $(a,b,c,d)\in K^4$, and suppose $ad-bc\neq 0$ and $a\pm d=b\mp c=0$. If a^2+b^2 is not a square in $K^\times$ then F_η has no Pythagorean solutions. If a^2+b^2 is a square in $K^\times$ then the Pythagorean solutions of F_η are given by*

$$\left\{\left(\pm\frac{-b\alpha+a}{a\alpha+b},\,\alpha\right) : \alpha\in\mathcal{S}-\{\tfrac{a}{b},-\tfrac{b}{a}\}\right\}.$$

Proof. Since $ad-bc\neq 0$, we can apply proposition 3.4. We saw in eq. (28) that $\mathcal{H}_\eta$ is defined by the equation $y^2=(a^2+b^2)(z^2+x^2)^2$. If a^2+b^2 is not a square in K, or if $a^2+b^2=0$, then all points in $\mathcal{H}_\eta(K)$ have $y=0$ and so are degenerate; thus F_η has no Pythagorean solutions. If $a^2+b^2=r^2$ for some $r\in K^\times$, then we have $(x:\pm r(z^2+x^2):z)\in\mathcal{H}_\eta(K)$ for all $(x:z)\in\mathbb{P}^1(K)$. A point is non-degenerate if and only if it satisfies

$$xz(z^4-x^4)(a(z^2-x^2)+b(2xz))(b(z^2-x^2)-a(2xz))\neq 0.$$

Equivalently, if we set $\alpha=\frac{z^2-x^2}{2xz}$, we must have $\alpha\in\mathcal{S}_K$, $\alpha\neq-\frac{b}{a}$, and $\alpha\neq\frac{a}{b}$. Applying Φ as in proposition 3.4 gives the desired result. □

A.2. **One geometric component.** Suppose $ad-bc\neq 0$, $(a\pm d,b\mp c)\neq(0,0)$, and $(a\pm d)^2+(b\mp c)^2=0$. This means we can write $-1=\left(\frac{a\pm d}{b\mp c}\right)^2$, so this scenario is only possible if -1 is a square in K.

Proposition A.2. *Suppose $ad-bc\neq 0$, $(a\pm d)^2+(b\mp c)^2=0$, and $(a\pm d,b\mp c)\neq(0,0)$. If $a^2+c^2=0$, or if the Hilbert symbol*

$$\left(a^2+c^2,\,(a^2+c^2)\left(\frac{a\pm d}{b\mp c}\right)\left(\frac{ab+cd}{ad-bc}\right)\right)_K$$

equals 1, then $\mathcal{H}_\eta(K)$ is infinite and F_η has infinitely many Pythagorean solutions. If neither condition holds, then $\mathcal{H}_\eta(K)$ has one point $(-(a\pm d):0:b\mp c)$, and there are no Pythagorean solutions of F_η.

Proof. Consider the case $(a-d)^2+(b+c)^2=0$ and $(a-d,b+c)\neq(0,0)$ (the case $(a+d)^2+(b-c)^2=0$ and $(a+d,b-c)\neq(0,0)$ is analogous). Then we must have $b+c\neq 0$, and so $i:=\frac{a-d}{b+c}$ is a square root of -1 in K. Writing $d=a-i(b+c)$, the equation defining $\mathcal{H}_\eta$ takes the form

$$y^2=-(x+iz)^2((a^2+c^2)(z^2-x^2)+(a-ic)(ai+2b+c)(2xz)).$$

This curve has a singularity at the degenerate point $(-i:0:1)$; we can blow up the singularity by introducing the variable $w=\frac{y}{x+iz}$. The result is a conic C in the (unweighted) projective plane with coordinates x,w,z, defined by

$$C: w^2=(a^2+c^2)(x^2-z^2)-(a-ic)(ai+2b+c)(2xz). \tag{29}$$

The map $C\to\mathcal{H}_\eta$ given by $(x:w:z)\mapsto(x:(x+iz)w:z)$ is an isomorphism away from $x+iz=0$. The discriminant of the quadratic form in x and z is $16i(a-ib)(a-ic)^2(b+c)$; by the identity $(a-ib)(a-ic)=ad-bc$, and since $ad-bc\neq 0$ and $b+c\neq 0$, this discriminant is nonvanishing, proving that C is smooth. Hence C is the normalization of $\mathcal{H}_\eta$, so that $\mathcal{H}_\eta$ has one geometric component.

If $a^2+c^2=0$, then C has a rational parametrization by w. If $a^2+c^2=(a+ic)(a-ic)\neq 0$, we can diagonalize the quadratic form in x and z to obtain

$$w^2=(a^2+c^2)u^2-\frac{4i(b+c)(a-ib)(a-ic)}{a+ic}z^2,$$

where $u=x-\frac{ai+2b+c}{a+ic}z$. The coefficients of u^2 and of z^2 are both nonzero, so this has a solution over K if and only if the Hilbert symbol

$$\left(a^2+c^2,-\frac{4i(b+c)(a-ib)(a-ic)}{a+ic}\right)_K$$

equals 1. Multiplying and dividing the second entry by $a-ic$, and using the identities $(b+c)(a-ic)=ab+cd$ and $(a-ib)(a-ic)=ad-bc$, we obtain

$$\left(a^2+c^2,-\frac{4i(ab+cd)(ad-bc)}{a^2+c^2}\right)_K,$$

where the second entry equals $(a^2+c^2)\left(\frac{a-d}{b+c}\right)\left(\frac{ab+cd}{ad-bc}\right)$ times a square in $K^\times$ (recall that -1 is a square); hence this Hilbert symbol is equal to the one in the proposition statement.

If neither of the two conditions from the proposition statement are satisfied, then $C(K)$ is empty, and so $\mathcal{H}_\eta(K)$ has only the singularity $(-i:0:1)$; this is in the degenerate locus, so F_η has no solutions. On the other hand, if at least one of the two conditions holds, then there is a rational parametrization $\mathbb{P}^1\to C$. Since C is the normalization of $\mathcal{H}$, this implies $\mathcal{H}_\eta(K)$ is infinite, and hence F_η has infinitely many Pythagorean solutions by proposition 3.4. □

Appendix B. Rational roots of $q(c,d)$ for $K=\mathbb{Q}$

Let $\eta=(1,0,c,d)\in\mathbb{Q}^4$ with $d\neq 0$. Assuming $(c,d)\neq(0,\pm1)$, the curve $\mathcal{H}_\eta$ is non-singular, and its Jacobian is the elliptic curve over $\mathbb{Q}$ defined by

$$E_\eta: y^2=x^3+(1+c^2+d^2)x^2+d^2x.$$

In the proof of theorem 1.4, we showed that if $(-1,c)\in E_\eta(\mathbb{Q})$ is torsion, then it must have order $\ell\in\mathcal{L}:=\{2,3,4,6,8,12\}$. In this appendix, we determine all $(c,d)\in\mathbb{Q}^2$ for which each order occurs. To do this, we compute the division

polynomials $\psi_\ell(c,d,x)$ for E_η, evaluate them at $x=-1$, and factor the result into irreducible polynomials in $\mathbb{Q}[c,d]$. For each irreducible factor, we determine the rational points of the vanishing locus.

B.1. $\ell = 2$. The second division polynomial of E_η is

$$\psi_2(c,d,x) = x^3 + (1+c^2+d^2)x^2 + 4d^2x,$$

so $\psi_2(c,d,-1) = -c^2$, which is zero if and only if $c=0$.

B.2. $\ell = 3$. The third division polynomial of E_η is

$$\psi_3(c,d,x) = x^4 + 4(1+c^2+d^2)x^3 + 6d^2x^2 - d^4,$$

so $\psi_3(c,d,-1) = -4c^2 - (d^2-1)^2$. For $c,d \in \mathbb{R}$, this is a sum of two non-positive terms, so $\psi_3(c,d,-1)=0$ if and only if $(c,d) = (0,\pm 1)$.

B.3. $\ell = 4$. The fourth division polynomial of E_η is

$$\psi_4(c,d,x) = \psi_{2,c,d}(x)(2x^6+4(1+c^2+d^2)x^5+10d^2x^4-10d^4x^2-4d^4(1+c^2+d^2)x-2d^6).$$

Dividing by $\psi_2(c,d,x)$ and evaluating the result at $x=-1$, we obtain

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

This is zero when $d=\pm 1$. The remaining factor is a sum of non-negative terms when $c,d\in\mathbb{R}$, so this only vanishes at $(c,d)=(0,\pm 1)$.

B.4. $\ell = 6$. Let $\psi_6(c,d,x)$ be the sixth division polynomial of E_η. Then $\psi_6(c,d,-1)$ is divisible by $\psi_2(c,d,-1)\psi_3(c,d,-1)$, and the quotient factors into two irreducible polynomials in $\mathbb{Q}[c,d]$. The first factor is $4c^2d^2+(d^2-1)^2$, which only vanishes for $(c,d)=(0,\pm 1)$.

The second factor is

$$16d^2c^4 - 4(d^2-1)^2(d^2+1)c^2 - 3(d^2-1)^4.$$

Considering this as a quadratic polynomial in c^2, the discriminant is equal to $16(d^2-1)^4(d^4+14d^2+1)$. In order for c^2 to be rational (let alone c), this discriminant must equal a rational square. Thus we consider rational points on the curve C defined by $y^2 = d^4+14d^2+1$. There are eight rational points $(d,y)\in C(\mathbb{Q})$: two at infinity, as well as $(-1,\pm 4)$, $(0,\pm 1)$, and $(1,\pm 4)$. The curve C is isomorphic to its Jacobian, the elliptic curve defined by $y^2 = x^3 - 7x^2 + 12x$ over $\mathbb{Q}$, which has Mordell-Weil group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Therefore there are no other rational points on C, so the only possibilities for d are $-1,0,1$. If $d=0$ then we have $c^2 = -\frac{3}{4}$, yielding no rational solutions. If $d=\pm 1$ then we have $c=0$. Hence the second factor is zero if and only if $(c,d)=(0,\pm 1)$.

B.5. $\ell = 8$. Let $\psi_8(c,d,x)$ be the eighth division polynomial of E_η. Then $\psi_8(c,d,-1)$ is divisible by $\psi_4(c,d,-1)$, and the quotient factors into three irreducible polynomials in $\mathbb{Q}[c,d]$. We consider each of these factors in turn.

The first factor is $4dc^2-(d^2-1)^2$. If $c=0$, the only solution is $d=\pm 1$. If $c\neq 0$, we must have $d=r^2$ for some $r\in\mathbb{Q}$; we obtain solutions

$$(c,d) = \left(\pm\frac{1-r^4}{2r}, r^2\right), \qquad r\in\mathbb{Q}^\times.$$

The second factor is $4dc^2+(d^2-1)^2$, and solutions of this factor map to solutions of the first factor via $d \mapsto -d$, yielding solutions

$$(c,d) = \left(\pm\frac{1-r^4}{2r}, -r^2\right), \qquad r \in \mathbb{Q}^\times.$$

The third factor is

$$\begin{aligned}&128d^2(d^4+1)c^8 + 128d^2(d^2-1)^2(d^2+1)c^6 + 8(d^2-1)^4(d^4+10d^2+1)c^4\\ &\quad + 8(d^2-1)^6(d^2+1)c^2 + (d^2-1)^8,\end{aligned}$$

which is a sum of non-negative terms and so the only solution in $\mathbb{Q}^2$ is $(c,d) = (0,\pm 1)$.

B.6. $\ell = 12$**.** Let $\psi_{12}(c,d,x)$ be the twelfth division polynomial of E_η. If we eliminate the common factors of $\psi_{12}(c,d,-1)$ with each of $\psi_6(c,d,-1)$ and $\psi_4(c,d,-1)$, the result factors into three irreducible polynomials in $\mathbb{Q}[c,d]$. We consider each of these factors in turn.

The first factor is

$$16d(d^2-d+1)c^4 + 8d(d^2-1)^2c^2 + (d^2-1)^4.$$

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

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

For the first option, we obtain $c \in \mathbb{Q}$ 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 c is rational. For the second option, we obtain $c \in \mathbb{Q}$ 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 $(c,d) \in \mathbb{Q}^2$.

The second factor is

$$16d(d^2+d+1)c^4 + 8d(d^2-1)^2c^2 - (d^2-1)^4,$$

and $d \mapsto -d$ sends solutions of this factor to solutions of the previous factor. Hence there is no $(c,d) \in \mathbb{Q}^2$ for which this factor is zero.

The third factor is

$$\begin{aligned}&65536d^6(d^4-d^2+1)c^{16} + 65536d^6(d^2-1)^2(d^2+1)c^{14}\\ &\quad + 4096d^2(d^2-1)^4(d^8+3d^6+20d^4+3d^2+1)c^{12}\\ &\quad + 4096d^2(d^2-1)^6(d^2+1)(2d^4+3d^2+2)c^{10}\\ &\quad + 256d^2(d^2-1)^8(23d^4+24d^2+23)c^8 + 1792d^2(d^2-1)^{10}(d^2+1)c^6\\ &\quad + 16(d^2-1)^{12}(d^4+26d^2+1)c^4 + 16(d^2-1)^{14}(d^2+1)c^2 + (d^2-1)^{16},\end{aligned}$$

which is a sum of non-negative terms and so the only rational solution is $(c,d) = (0,\pm 1)$.

References

[1] Siksek (https://mathoverflow.net/users/4140/siksek). *The rank of a class elliptic curves*. MathOverflow. URL:https://mathoverflow.net/q/63856 (version: 2011-05-03). eprint: https://mathoverflow.net/q/63856. URL: https://mathoverflow.net/q/63856 (page 24).

[2] Sang Yook An et al. "Jacobians of Genus One Curves". In: *Journal of Number Theory* 90.2 (2001), pp. 304–315. ISSN: 0022-314X. DOI: https://doi.org/10.1006/jnth.2000.2632. URL: https://www.sciencedirect.com/science/article/pii/S0022314X00926325 (page 10).

[3] T. G. Berry. "Points at rational distance from the corners of a unit square". en. In: *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze* Ser. 4, 17.4 (1990), pp. 505–529. URL: http://www.numdam.org/item/ASNSP_1990_4_17_4_505_0/ (pages 2, 8).

[4] Manjul Bhargava, John Cremona, and Tom Fisher. "The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point". In: *Int. J. Number Theory* 17.4 (2021), pp. 903–923. ISSN: 1793-0421. DOI: 10.1142/S1793042121500147. URL: https://doi.org/10.1142/S1793042121500147 (page 3).

[5] V. Chandrasekar. "The congruent number problem". In: *Resonance* 3 (1998), pp. 33–45 (page 9).

[6] Keith Conrad. *The congruent number problem*. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf. Accessed: 20210-11-01 (page 9).

[7] Stephan Ramon Garcia and Ethan Simpson Lee. "Unconditional explicit Mertens' theorems for number fields and Dedekind zeta residue bounds". In: *The Ramanujan Journal* (2021). ISSN: 1572-9303. DOI: 10.1007/s11139-021-00435-6. URL: https://doi.org/10.1007/s11139-021-00435-6 (page 17).

[8] Richard K. Guy. *Unsolved problems in number theory*. Third. Problem Books in Mathematics. Springer-Verlag, New York, 2004, pp. xviii+437. ISBN: 0-387-20860-7. DOI: 10.1007/978-0-387-26677-0. URL: https://doi.org/10.1007/978-0-387-26677-0 (page 7).

[9] Lorenz Halbeisen and Norbert Hungerbühler. "Pairing pythagorean pairs". In: *Journal of Number Theory* (2021). ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2021.07.002. URL: https://www.sciencedirect.com/science/article/pii/S0022314X21002171 (pages 7, 8).

[10] Serge Lang. *Algebraic number theory*. Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+357. ISBN: 0-387-94225-4. DOI: 10.1007/978-1-4612-0853-2. URL: https://doi.org/10.1007/978-1-4612-0853-2 (pages 15, 17).

[11] Jonathan Love. *Root numbers of a family of elliptic curves and two applications*. 2022. arXiv: 2201.04708 [math.NT] (page 6).

[12] R van Luijk. "On Perfect Cuboids". Doctoraalscriptie. Mathematisch Instituut, Universiteit Utrecht, Utrecht, 2000 (pages 2, 7).

[13] Loïc Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". In: *Invent. Math.* 124.1-3 (1996), pp. 437–449. ISSN: 0020-9910. DOI: 10.1007/s002220050059. URL: https://doi-org.stanford.idm.oclc.org/10.1007/s002220050059 (page 19).

[14] Bartosz Naskręcki. "Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples". In: *Acta Arith.* 160.2 (2013), pp. 159–183. ISSN: 0065-1036. DOI: 10.4064/aa160-2-5. URL: https://doi.org/10.4064/aa160-2-5 (page 24).

[15] J. Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois Journal of Mathematics* 6.1 (1962), pp. 64–94. DOI: 10.1215/ijm/1255631807. URL: https://doi.org/10.1215/ijm/1255631807 (page 17).

[16] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan. Springer-Verlag, Berlin, 1989, pp. x+160. ISBN: 3-540-50629-2. DOI: 10.1007/978-3-662-08287-4. URL: https://doi.org/10.1007/978-3-662-08287-4 (page 16).

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6 (page 19).

[18] J. B. Tunnell. "A classical Diophantine problem and modular forms of weight 3/2". In: *Invent. Math.* 72.2 (1983), pp. 323–334. ISSN: 0020-9910. DOI: 10.1007/BF01389327. URL: https://doi.org/10.1007/BF01389327 (page 9).

[19] J.-L. Waldspurger. "Sur les coefficients de Fourier des formes modulaires de poids demi-entier". In: *J. Math. Pures Appl. (9)* 60.4 (1981), pp. 375–484. ISSN: 0021-7824 (page 10).

[20] André Weil. "Remarques sur un mémoire d'Hermite". In: *Arch. Math. (Basel)* 5 (1954), pp. 197–202. ISSN: 0003-889X. DOI: 10.1007/BF01899338. URL: https://doi.org/10.1007/BF01899338 (page 10).

(Jonathan Love) McGill University
Email address: jon.love@mcgill.ca