UC Berkeley
UC Berkeley Previously Published Works

Title

Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on K3 surfaces

Permalink

https://escholarship.org/uc/item/2xx6c4wz

Authors

Hartshorne, Robin
Luijk, Ronald van

Publication Date

2006-06-27

Peer reviewed

NON-EUCLIDEAN PYTHAGOREAN TRIPLES, A PROBLEM OF EULER, AND RATIONAL POINTS ON K3 SURFACES

ROBIN HARTSHORNE AND RONALD VAN LUIJK

Abstract. We discover suprising connections between three seemingly differ-ent problems: finding right triangles with rational sides in a non-Euclidean geometry, finding three integers such that the difference of the squares of any two is a square, and the problem of finding rational points on an algebraic surface in algebraic geometry. We will also reinterpret Euler's work on the second problem with a modern point of view.

1. Problem I: Pythagorean triples

An ordinary *Pythagorean triple* is a triple (a, b, c) of positive integers satisfying $a^2 + b^2 = c^2$. Finding these is equivalent, by the Pythagorean theorem, to finding right triangles with integral sides. Since the equation is homogeneous, the problem for rational numbers is the same, up to a scale factor.

Some Pythagorean triples, such as $(3, 4, 5)$, have been known since antiquity. Euclid [6, X.28, Lemma 1] gives a method for finding such triples, which leads to a complete solution of the problem. The primitive Pythagorean triples are exactly the triples of integers $(m^2 - n^2, 2mn, m^2 + n^2)$ for various choices of m, n (up to change of order). Diophantus in his Arithmetic [5, Book II, Problem 8] mentions the problem of writing any (rational) number as the sum of squares. This inspired Fermat to write his famous "last theorem" in the margin.

Expressed in the language of algebraic geometry, the equation $x^2 + y^2 = z^2$ describes a curve in the projective plane. This curve is parametrized by a projective line according to the assignment (in homogeneous coordinates)

$$(1) \qquad (m, n) \mapsto (m^2 - n^2, 2mn, m^2 + n^2).$$

The rational points on the curve correspond to primitive Pythagorean triples, which explains why the same parametrization appeared above.

Now let us consider the analogous question in a non-Euclidean geometry. In the hyperbolic plane, if one uses the multiplicative distance function[1] instead of its logarithm (which is more common), it makes sense to ask for hyperbolic right triangles whose sides all have rational numbers a, b, c as lengths. It then follows from the formulae of hyperbolic trigonometry, see [4, 42.2, 42.3], that the sines and cosines of the angles of these triangles are also rational. The hyperbolic analogue of the Pythagorean theorem [4, 42.3(f)] tells us

$$\sin \overline{a} \cdot \sin \overline{b} = \sin \overline{c},$$

---

[1]If A, B are two points in the Poincaré model of a hyperbolic plane, and if P, Q are the ends (on the defining circle) of the hyperbolic line containing A and B, then $\mu(AB) = (AB, PQ)^{-1}$ is the *multiplicative distance function* for the segment AB. Here (AB, PQ) denotes the cross-ratio of the four points in the ambient Euclidean plane [4, 39.10].

where $\overline{a}, \overline{b}, \overline{c}$ are the angles of parallelism[2] of corresponding segments[3]. Since for any segment of length x one has [4, proof of 42.2]

$$\sin \overline{x} = \frac{2x}{1 + x^2},$$

the corresponding arithmetic problem is to find triples (a, b, c) of rational numbers, with

$$(2) \qquad \frac{2a}{1 + a^2} \cdot \frac{2b}{1 + b^2} = \frac{2c}{1 + c^2},$$

which we will call *non-Euclidean Pythagorean triples*. Clearly an even number of the numbers a, b, c are negative, unless we have a trivial solution with $abc = 0$. After changing signs we may assume $a, b, c > 0$. Note also that if we replace any number in a non-Euclidean Pythagorean triple by its inverse, we again get a non-Euclidean Pythagorean triple, so we may focus on those triples with $a, b, c \geq 1$. To keep them nontrivial, we require $a, b, c > 1$. They are not so easy find. (Let the reader try before reading further.)

Note that we must allow rational numbers in stating our problem, since there are no similar triangles in hyperbolic geometry, or, in arithmetic terms, since the equation is not homogeneous. Indeed, Bjorn Poonen has shown by an elementary argument that this equation has no solution in integers > 1. So our first problem is to find non-Euclidean Pythagorean triples.

Remark 1.1. There are other similar ways to express the hyperbolic Pythagorean Theorem, for instance [12, (14.51-52)] and [14]. These references do not have an arithmetic point of view, though.

2. Problem II: A problem of Euler

Euler, in his Algebra [2, Part II, §236], considers the problem of finding three squares (of integers), x^2, y^2, z^2, whose differences $x^2 - y^2$, $x^2 - z^2$, $y^2 - z^2$ should also be squares. A first ad hoc argument gives him a single solution $(x, y, z) = (697, 185, 153)$, which turns out to be the smallest possible, ordered by $|x|$. Then in §237 he gives a method for finding infinitely many solutions. Since one of the purposes of this paper is to reinterpret Euler's method in terms of algebraic geometry, we recall his method here. First he notes that passing to rational numbers, it is sufficient to find x, y, z satisfying

$$(3) \qquad \frac{x^2}{z^2} - \frac{y^2}{z^2} = \square, \qquad \frac{x^2}{z^2} - 1 = \square, \qquad \frac{y^2}{z^2} - 1 = \square.$$

If we set

$$(4) \qquad \frac{x}{z} = \frac{p^2 + 1}{p^2 - 1}, \qquad \frac{y}{z} = \frac{q^2 + 1}{q^2 - 1},$$

or $p = \sqrt{x^2 - z^2}/(x - z)$ and $q = \sqrt{y^2 - z^2}/(y - z)$, then the second and third equation of (3) are automatically satisfied, just as in the parametrization of Pythagorean

---

[2]Given a segment AB in the hyperbolic plane, let l be the hyperbolic line perpendicular to AB at B, and let m be the line through A that is the limiting parallel to l at an end. Then the angle formed by AB and m is the *angle of parallelism* of the segment AB. This construction creates a one-to-one correspondence (up to congruence) between segments and acute angles in the hyperbolic plane [4, 40.7.1].

[3]Compare this to the more familiar expression of the Pythagorean theorem using the additive distances a, b, c, namely $\cosh a \cdot \cosh b = \cosh c$.

triples mentioned above. Now we only need to satisfy the first equation. In terms of p and q we want

$$\frac{4(p^2q^2 - 1)(q^2 - p^2)}{(p^2 - 1)^2(q^2 - 1)^2}$$

to be a square, and for this it suffices that the numerator be a square. Dividing by $4p^2$, we reduce to showing that

$$(p^2q^2 - 1)\left(\frac{q^2}{p^2} - 1\right)$$

is a square. Setting $m = q/p$, we must show that

$$(5) \qquad\qquad (m^2p^4 - 1)(m^2 - 1)$$

is a square. Obviously, this is a square for $p = 1$, but then x is undefined, so we set $p = 1 + s$ and then seek to make

$$\left(m^2 - 1 + m^2(s^4 + 4s^3 + 6s^2 + 4s)\right)(m^2 - 1)$$

a square. Dividing by $(m^2 - 1)^2$ and writing $a = m^2/(m^2 - 1)$ for simplicity, we need to make

$$(6) \qquad\qquad 1 + 4as + 6as^2 + 4as^3 + as^4$$

a square. There are unique $f, g \in \mathbb{Q}[a]$ such that for $w = 1 + fs + gs^2$ the coefficients in w^2 of s^k for $k = 0, 1, 2$ coincide with the coefficients in (6), namely $f = 2a$ and $g = 3a - 2a^2$. Then, to make (6) equal to w^2, we need

$$(7) \qquad\qquad 4as^3 + as^4 = 2fgs^3 + g^2s^4,$$

which is the case, besides for $s = 0$ (with multiplicity 3), for

$$(8) \qquad\qquad s = \frac{8a - 4}{4a^2 - 8a + 1}.$$

Reading backwards, take any $m \neq \pm 1$ you like, set $a = m^2/(m^2 - 1)$, take s as just given, let $p = 1 + s$, $q = mp$, and then equation (4) will give x, y, z, up to scaling, satisfying the original problem. Since m is arbitrary, this gives infinitely many solutions.

For example, if we take $m = 2$, then

$$a = \frac{4}{3}, \quad s = -\frac{60}{23}, \quad p = -\frac{37}{23}, \quad q = -\frac{74}{23},$$

so

$$\frac{x}{z} = \frac{949}{420}, \qquad \frac{y}{z} = \frac{6005}{4947},$$

giving rise to the relatively prime solution

$$x = 1564901, \qquad y = 840700, \qquad z = 692580,$$

and one can easily verify that

$$x^2 - y^2 = 1319901^2, \qquad x^2 - z^2 = 1403299^2, \qquad y^2 - z^2 = 476560^2.$$

Remark 2.1. Euler also considers two other problems. In §235 he requires three integers $a < b < c$, whose sums and differences two at a time are all squares. One can show easily that this problem is equivalent to ours as the three pairwise sums of the three integers give a solution to our problem and every solution is of this form [7, section 4]. Euler does not mention this equivalence and appears not to realize its existence. He does see that the squares of a, b, c give a solution to Problem II,

but solutions arising this way tend to be much larger, which is why he treats our problem independently by the method described above. Several other authors have considered these two problems (see for instance [9], [1] and references mentioned there). Like Euler, however, many did not seem to realize the equivalence of the two problems.

In §238 Euler requires three squares such that the sum of any two is again a square. This one has a geometric interpretation in 3-dimensional Euclidean space, to find a rectangular box (cuboid) with integral edges and integral face diagonals.

Our problem can also be interpreted in terms of cuboids. For if we put

$$(9) \qquad\qquad x^2 - y^2 = t^2, \qquad x^2 - z^2 = u^2, \qquad y^2 - z^2 = v^2,$$

these equations are equivalent to

$$(10) \qquad\qquad t^2 + v^2 = u^2, \qquad v^2 + z^2 = y^2, \qquad t^2 + v^2 + z^2 = x^2.$$

Thus our problem is equivalent to finding a cuboid with integral edges t, v, z, of which two face diagonals and the full diagonal are integral. Note that (x, u, t) is also a solution to Problem II and it gives the same cuboid as the triple (x, y, z).

In this connection, it is still an open problem to decide whether or not there exists a *perfect cuboid*, having all edges, face diagonals and the full diagonal integeral. For more on this problem, see [3, D18], [7] and [15], and the references given there.

3. EQUIVALENCE OF THE TWO PROBLEMS

We thank Hendrik Lenstra for first pointing out to us the equivalence of problems I and II. Equation (2) and similar ones have been studied in relation with Euler's problem before [7, section 4,5]. Leech also shows how Problem II can be used to construct spherical right triangles whose sides and angles all have rational sines and cosines.

If we take x, y, z satisfying Euler's problem, and write equations similar to (3), namely

$$1 - \frac{y^2}{x^2} = \Box, \qquad 1 - \frac{z^2}{x^2} = \Box, \qquad 1 - \frac{z^2}{y^2} = \Box,$$

then we can parametrize them (inhomogeneously) as in (1) by

$$(11) \qquad\qquad \frac{y}{x} = \frac{2a}{a^2 + 1}, \qquad \frac{z}{x} = \frac{2c}{c^2 + 1}, \qquad \frac{z}{y} = \frac{2b}{b^2 + 1}.$$

From $\frac{y}{x} \cdot \frac{z}{y} = \frac{z}{x}$ we then obtain equation (2) of a non-Euclidean Pythagorean triple. Conversely, such a triple (a, b, c) will give a solution to Euler's problem through (11).

To find a, b, c explicitly, note that for example the first equation above, namely

$$1 - \frac{y^2}{x^2} = \frac{t^2}{x^2},$$

is parametrized by

$$\frac{y}{x} = \frac{2a}{a^2 + 1}, \qquad \frac{t}{x} = \frac{a^2 - 1}{a^2 + 1},$$

from which we find $a = (x + t)/y$. If $x, y, t > 0$, then $a > 1$. Similarly we find $b, c > 1$. Thus we obtain a one-to-one correspondence between solutions (x, y, z) to Problem II with $x > y > z > 0$ and gcd equal to 1 on the one hand and (ordered) non-Euclidean Pythagorean triples (a, b, c) with $a, b, c > 1$ on the other.

So, for example, from Euler's smallest solution $(x, y, z) = (697, 185, 153)$ we get

$$(12) \qquad a = \frac{37}{5}, \qquad b = \frac{17}{9}, \qquad c = 9,$$

while for the second example above, we obtain

$$(13) \qquad a = \frac{1201}{350}, \qquad b = \frac{97}{51}, \qquad c = \frac{30}{7}.$$

It is amusing to verify equation (2) for these triples. The numbers factor, and many of the factors cancel each other as if by magic.

4. A CYCLE OF FIVE

In his commentary on the work of Lobachevsky, F. Engel noted that to each hyperbolic right triangle, one can associate another triangle in a natural way. Repeated five times, this process returns to the original triangle [8, p. 346-347]. This association is closely related to the formulas of hyperbolic trigonometry, and forms a parallel to Napier's analogies in spherical trigonometry.

Here is the construction. Given the right triangle ABC, with sides a, b, c opposite A, B, C repectively, angles α, β at A and B, and a right angle at C, draw the perpendicular to BC at B, find the limiting parallel to AB that is perpendicular to this new line, thus obtaining F. Draw the limiting parallel from B to AC, intersecting the previous limiting parallel at E. Then the new triangle is DEF with $D = B$ (Figure 1).

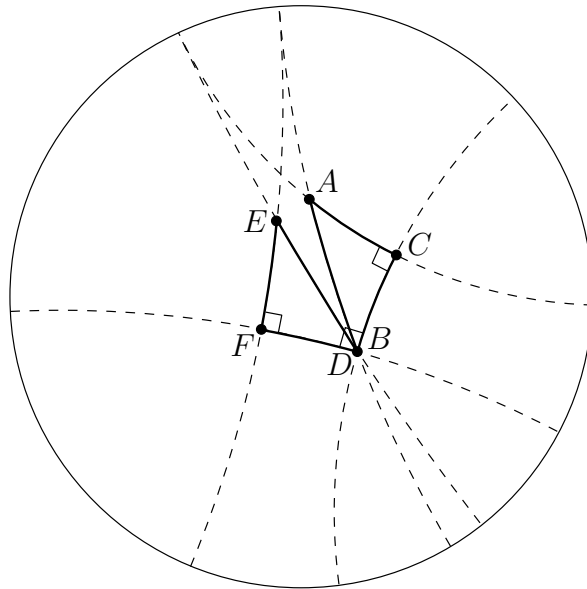FIGURE 1. Engel's associated triangle

Note that $\angle FBA$ is complementary to β, and that it is the angle of parallelism of segment DF. Thus we write $DF = \overline{\beta'}$, where the prime denotes complementary angle, and the bar denotes the correspondence between segments and angles by the angle of parallelism. Note also that $\angle EBC$ equals $\overline{a}$, and so $\angle FDE = \overline{a}'$. Knowing

two of the five quantities $(d, e, f, \delta, \epsilon)$ of the new triangle, where the variables denote the obvious lengths and angles, one can compute the others. Thus, if the original triangle has sides and angles (a, b, c, α, β), the new triangle has sides and angles $(b, \overline{\beta'}, \overline{\alpha}, \overline{a}', \overline{c})$ (see [4, 42.5 and Exercise 42.23] for more details). It is then easy to verify that this process, repeated five time, comes back to its starting point. It is an amusing exercise in hyperbolic trigonometry to compute the new triangle from the old one. Since the triangle is determined by any two of its five measurements, it is enough to compute b (which we already know) and $\overline{\beta}'$. Here is a recipe.

Lemma 4.1. *Given a and b, set $e = \frac{2a}{a^2-1} \cdot \frac{b^2-1}{b^2+1}$. Then $\overline{\beta}' = e + \sqrt{1 + e^2}$.*

Proof. Left to the reader! $\square$

The general formulas for the edges of the new triangle in terms of those of the old one are not very elegant, but they can be expressed using a recurrence relation due to Lyness: see [9] and [7, p. 524].

Using Lemma 4.1 on an explicit example, say the triple

$$\left(\frac{37}{5}, \frac{17}{9}, 9 \right)$$

in (12), we obtain four more triples

$$\left(\frac{17}{9}, \frac{7}{6}, \frac{27}{14} \right),$$
$$\left(\frac{7}{6}, \frac{5}{4}, \frac{21}{16} \right),$$
$$\left(\frac{5}{4}, \frac{41}{13}, \frac{13}{4} \right),$$
$$\left(\frac{41}{13}, \frac{37}{5}, 13 \right)$$

as further examples of non-Euclidean Pythagorean triples. Associated to these are further solutions to Euler's problem, namely $(x, y, z) =$

$$(697, 185, 153),$$
$$(925, 765, 756),$$
$$(3485, 3444, 3360),$$
$$(7585, 7400, 4264),$$
$$(15725, 9061, 2405).$$

Remarkably, the transformation of order five can be expressed quite simply in terms of (x, y, z, t, u, v) of (9), namely by sending (x, y, z) to (uy, uz, tz) and then dividing by the greatest common divisor.

Just for fun, we computed the 5-cycle associated to the triple in (13). We get

$$\left(\frac{1201}{350}, \frac{97}{51}, \frac{30}{7}\right),$$

$$\left(\frac{97}{51}, \frac{47}{33}, \frac{99}{47}\right),$$

$$\left(\frac{47}{33}, \frac{37}{23}, \frac{1551}{851}\right),$$

$$\left(\frac{37}{23}, \frac{73}{26}, \frac{74}{23}\right),$$

$$\left(\frac{73}{26}, \frac{1201}{350}, \frac{40}{7}\right).$$

5. Algebro-geometric interpretation

The equations (9)

$$x^2 - y^2 = t^2, \qquad x^2 - z^2 = u^2, \qquad y^2 - z^2 = v^2$$

describing Euler's problem define a surface X in projective 5-space $\mathbb{P}^5$ over the rational numbers. To find integer solutions to these equations is equivalent to finding rational solutions, hence to the problem of finding rational points (points with all coordinates in $\mathbb{Q}$) on the surface X. We have thus gone from Euclidean geometry, through hyperbolic geometry and number theory, back to geometry, but now algebraic (and arithmetic) geometry.

For algebraic curves, the problem of finding rational points has been studied in detail. A curve of genus 0, as soon as it has one rational point, is isomorphic to $\mathbb{P}^1$, so one knows all its points, and the curve can be parametrized, just as in the case of the classical Pythagorean triples. A curve of genus 1 with at least one rational point is an elliptic curve. Here one knows that the rational points form a finitely generated abelian group. It may be finite or infinite. Its rank can be quite large (Noam Elkies has found an elliptic curve of rank 28), but one does not know if there are elliptic curves of arbitrarily high rank. For curves of genus at least 2, Faltings' proof of the Mordell Conjecture tells us that there are only finitely many rational points.

For algebraic surfaces (and more generally, varieties of dimension at least 2) very little is known about the set of rational points. This is a topic of intensive active research: see for instance the books [10] and [11], and in particular the review paper [13] by Swinnerton-Dyer. In our case, the surface X is a complete intersection of three quadric hypersurfaces. This implies that outside its singularities the canonical class K_X is trivial and the irregularity is 0. Since the only singularities are ordinary double points, our surface is (birationally) what is known as a K3 surface. This surface is studied in detail in [15]. One knows that there are many K3 surfaces with no rational points (for example the surface given by $x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0$ in $\mathbb{P}^3$, which does not even have any real points). There are also many whose set of rational points is dense in the Zariski topology. We will see that ours is one of the latter. An open problem is whether there exists a K3 surface whose set of rational points is non-empty, but not dense. Our main result is the following.

Theorem 5.1. *The set of rational points on the surface X representing Euler's problem is dense in the Zariski topology.*

A good part of the proof is already contained in Euler's calculation. The equation

$$(14) \qquad\qquad w^2 = 1 + 4as + 6as^2 + 4as^3 + as^4$$

obtained from (6) describes a surface in the affine (a, s, w)-space. Note that this surface is rational, as its equation is linear in a. By projection it is fibered over the a-line, and for general a the fiber is a curve of genus 1. Since it contains some rational points $(s, w) = (0, \pm 1)$, it is an elliptic curve.

The assignment $a = m^2/(m^2 - 1)$ makes the m-line a double cover of the a-line. Taking the fibered product of the m-line and the surface given by (14) over the a-line, we get a surface in (m, s, w)-space, fibered by elliptic curves over the m-line. This surface is birational to our surface X via the formulas for p, q, x, y, z given earlier, and the reverse equations

$$p = \frac{x + z}{u}, \qquad q = \frac{y + z}{v}.$$

Thus, our surface is a K3 surface fibered in elliptic curves over a rational curve, the m-line. Its generic fiber is an elliptic curve E over the rational function field $\mathbb{Q}(m)$, also given by (14). It is worth noting that E has j-invariant 1728, making all the elliptic fibers quadratic twists of the one curve given by $y^2 = x^3 - x$. It also implies that the fibers admit complex multiplication by $\mathbb{Z}[i]$. This is more clear from (5), which shows that if p makes (5) a square, then so does ip. Any section of our surface over the m-line can be given by $\big(m, S(m), W(m)\big)$, where $S(m)$ and $W(m)$ are rational functions in m that satisfy equation (14). The same rational functions determine a point on $E/\mathbb{Q}(m)$, and thus we obtain a natural correspondence between sections of our fibration and points on E with coordinates in $\mathbb{Q}(m)$. Euler's formulas (8) for s and $w = 1 + fs + gs^2$ give a simple section of this fibration, thus producing infinitely many rational points on the surface.

The new ingredient that we add to this picture is the observation that after fixing the origin to be $\mathcal{O} = (0, 1)$, the $\mathbb{Q}(m)$-point Q that Euler's section corresponds to, has infinite order. This can be checked with standard techniques from the theory of elliptic curves (which we omit). Taking multiples of this point gives infinitely many more sections of the fibration. The union of their rational points is dense in the whole K3 surface, thus proving Theorem 5.1.

The point $P = (0, -1)$ has infinite order as well. We claim $Q = 2P$. Indeed, note that two points R and S add to T in the group law on E if and only if there exists a function f in the function field of the curve whose principal divisor (f) equals $(T) + (\mathcal{O}) - (R) - (S)$. Consider the parabola $F(s, w) = 0$ given by $F = -w + 1 + 2as + (3a - 2a^2)s^2$. Euler's calculation shows that this parabola meets the generic fiber in the point $\mathcal{O}$ with multiplicity 3 and in the point Q. Since s vanishes at $\mathcal{O}$ and P, and the contribution of the points at infinity to the divisors (s^2) and (F) are the same, we find that $(F/s^2) = (F) - (s^2)$ equals $3(\mathcal{O}) + (Q) - 2(\mathcal{O}) - 2(P) = (Q) + (\mathcal{O}) - 2(P)$, so indeed we have $Q = 2P$.

Remark 5.2. By now we have seen several ways of finding rational points on the surface X. Besides Euler's first ad hoc argument leading to the smallest integer solution to Problem II, he found a parametrization of infinitely many solutions. His parametrization corresponds to a section of an elliptic fibration and it turns out to

have infinite order, so that there are in fact infinitely many curves with infinitely many rational points on the corresponding surface. This shows that the set of rational points is dense. Leech [7, p. 525] uses a result from Diophantus (see his Arithmetica, Book V, Lemma 2 to Prop. 7, [5, p. 205]) to find a parametric solution corresponding to another curve on the surface. In terms of algebraic geometry (which is not his viewpoint) Leech has also found another elliptic fibration. It was already mentioned in [15, page 7] that Leech's results can be combined to prove that X contains infinitely many parametrizable rational curves, and thus that the set of rational points on the surface is dense.

There is also a very elementary way to show that there are infinitely many solutions to Problem II. It comes from combining the equivalence of Euler's problem and the first problem mentioned in Remark 2.1 together with Euler's way of producing a solution to the former from a solution to the latter, also mentioned in Remark 2.1. Suppose that $(x_0, y_0, z_0, t_0, u_0, v_0)$ with gcd equal to 1 satisfies (9). Then we have $x_0^2 + v_0^2 = y_0^2 + u_0^2$, $z_0^2 + t_0^2 = x_0^2 - v_0^2$, and $y_0^2 - u_0^2 = z_0^2 - t_0^2$. This allows us to check that

$$(x_1', y_1', z_1', t_1', u_1', v_1') = (x_0^2 + v_0^2, z_0^2 + t_0^2, y_0^2 - u_0^2, 2x_0v_0, 2y_0u_0, 2z_0t_0)$$

satisfies (9) as well and that $d = \gcd(x_1', y_1', z_1', t_1', u_1', v_1')$ satisfies $d \le 2$. Note also that we have $x_1' + y_1' + z_1' = x_0^2 + y_0^2 + z_0^2 \ge 0$. This means that if we start with one solution satisfying $x_0 + y_0 + z_0 > 6$, then the new solution $(x_1, y_1, z_1, t_1, u_1, v_1)$ we obtain after dividing out d satisfies

$$x_1 + y_1 + z_1 = \frac{1}{d}(x_1' + y_1' + z_1') \ge \frac{1}{2}(x_1' + y_1' + z_1')$$
$$= \frac{1}{2}(x_0^2 + y_0^2 + z_0^2) \ge \frac{1}{6}(x_0 + y_0 + z_0)^2 > x_0 + y_0 + z_0,$$

where the second-to-last inequality is the quadratic-arithmetic mean inequality. We conclude that applying this process repeatedly, obtaining solutions (x_n, y_n, z_n) for all $n \ge 0$, the expression $x_n + y_n + z_n$ increases as n increases, so we get infinitely many solutions. We leave the details to the reader. We do not know whether the set of points arising from a single point by this process can be a Zariski dense subset of X.

Remark 5.3. Having found a dense set of rational points on X, can we find *all* rational points on X? We believe this is hopeless because a special fiber of the fibration may contain many points that do not come from a section of the fibration.

To show this, we first note that the group of rational points $E(\mathbb{Q}(m))$ of the generic fiber is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generated by P and the 2-torsion point $T = (-2, 1)$. This follows from the Shioda-Tate formula for the Picard number of our K3 surface X, which equals 20 by an unpublished result of Beukers and Van Geemen (see also [15, p. 8]). Thus the group of $\mathbb{Q}(m)$-rational points on the generic fiber has rank 1.

Euler finds a parametrization of another rational curve on our surface that corresponds to a point R on E over $\mathbb{Q}(\sqrt{a})$, which turns out to satisfy $2R = P + T$. This means that for all square values of a, we get an extra point in the fiber above a, but the group generated by all points that Euler finds remains of rank 1.

Now consider for example Euler's smallest solution $(697, 185, 153)$. It is contained in the fiber that lies above

$$m = \frac{q}{p} = \frac{v(x-z)}{u(y-z)} = \frac{13}{5},$$

or $a = m^2/(m^2 - 1) = \left(\frac{13}{12}\right)^2$. With a standard technique from the theory of elliptic curves, namely the so called *height pairing*, implemented in computer algebra packages such as MAGMA, one can show that in the group law on this fiber the point corresponding to Euler's smallest solution is linearly independent of the points corresponding to the sections that Euler found, namely P, $Q = 2P$, and R satisfying $2R = P + T$. The rank over $\mathbb{Q}$ of this special fiber is in fact 2. Thus there are many points in special fibers that can not be obtained as points on sections of the surface arising from points in the general fiber.

Moreover, with a computer we checked that there are 1440 integer solutions (x, y, z) to Euler's Problem II with $0 < z < y < x < 10^7$ and $\gcd(x, y, z) = 1$. Only 5 of these points lie in a fiber in which that point and the point from Euler's section Q are linearly dependent. These are the fibers above $m \in \left\{2, 4, \frac{5}{4}, \frac{289}{240}, \frac{3267}{2209}\right\}$.

As said before, it therefore seems hopeless that we would ever be able to find all rational points. In fact, we do not know of any case where the complete set of rational points on a K3 surface is described to satisfaction, except when there are none.

Remark 5.4. Now that we have understood Euler's problem from a modern point of view, what about the problem of perfect cuboids mentioned above? Here the coresponding algebraic surface is a surface of general type in $\mathbb{P}^6$. According to a conjecture of Lang, the rational points on a surface of general type should be contained in a proper closed subset. In particular, if there are any (nontrivial points), they will be much rarer, and difficult to find. So for the moment, this problem still seems out of reach.

References

[1] L.E. Dickson, History of the theory of numbers, Vol. **2**, Diophantine Analysis, *Carnegie Institute of Washington* (1919), Reprint by Chelsea (1952); Ch. 15, ref. 28, p. 448 and cross-refs to pp. 446–458; Ch. 19, refs. 1–30, 40–45, pp. 497–502, 505–507.

[2] L. Euler, Algebra, first published in 1770 as Vollständige Anleitung zur Algebra, English translation: Euler, Elements of Algebra, Springer 1984.

[3] R. Guy, Unsolved Problems in Number Theory, Problem books in mathematics, Springer-Verlag, 1981.

[4] R. Hartshorne, Geometry, Euclid and Beyond, Springer NY, 2000

[5] T.L. Heath, Diophantus of Alexandria, Cambridge, 1910.

[6] T.L.Heath, The thirteen books of Euclid's Elements, 2nd ed., Cambridge University Press, 1926

[7] J. Leech, *The rational cuboid revisited*, Amer. Math. Monthly, **84** (1977), no. 7, pp. 518–533.

[8] N. Lobatschefskij, Zwei geometrische Abhandlungen, ed. F. Engel, Teubner, Leipzig, 1898.

[9] R.C. Lyness, Cycles, Math. Gazette, **26** (1942), p. 62, ibid. **29** (1945), pp. 231-233, ibid. **45** (1961), pp. 207–209.

[10] E. Peyre and Yu. Tschinkel, Rational points on algebraic varieties, Progress in Mathematics **199**, Birkhäuser, 2001.

[11] B. Poonen and Yu. Tschinkel, Arithmetic of higher-dimensional algebraic varieties, Progress in Mathematics **226**, Birkhäuser, 2004.

[12] H. Schwerdtfeger, Geometry of Complex Numbers, Dover Publications Inc., 1979

[13] P. Swinnerton-Dyer, *Diophantine equations: progress and problems*, in ref. [11], pp. 3–35

[14] A. Ungar, *The hyperbolic Pythagorean theorem in the Poincaré disc model of hyperbolic geometry*, Amer. Math. Monthly **106** (1999), no. 8, pp. 759–763.

[15] R. van Luijk, On Perfect Cuboids, undergraduate thesis, 2000, available at http://www.math.leidenuniv.nl/reports/2001-12.shtml

DEPARTMENT OF MATHEMATICS, EVANS HALL, UNIVERSITY OF CALIFORNIA, BERKELEY, CA 94720-3840

E-mail address: robin@math.berkeley.edu

MATHEMATICAL SCIENCES RESEARCH INSTITUTE, 17 GAUSS WAY, BERKELEY, CA 94720-5070

E-mail address: rmluijk@msri.org