THE GEOMETRIC DISPOSITION OF DIOPHANTINE EQUATIONS

ANTHONY VÁRILLY-ALVARADO

In 2005, writer David Foster Wallace delivered a remarkable commencement speech at Kenyon College. He began by begrudgingly offering a “a standard requirement of US commencement speeches”, the parable-ish story:

> There are these two young fish swimming along and they happen to meet an older fish swimming the other way, who nods at them and says “Morning, boys. How’s the water?”And the two young fish swim on for a bit, and then eventually one of them looks over at the other and goes “What the hell is water?”

This article is a story about water. It is a story about trying to understand the natural habitat of certain problems that, on their face, look like problems about whole numbers. To be sure, the problems we discuss *are* number theoretic in character, but the way to access them and to think about them is informed by a different part of Mathematics: geometry.

1. Three problems

(1) Which whole numbers can be expressed as a sum of three cubes?

(2) Is there a box such that the distance between any two of its corners is a positive whole number?

(3) Is there a 3×3 magic square whose entries are distinct nonzero squares?

Recall an $n \times n$ magic square is an $n \times n$ grid, filled with distinct positive integers, whose rows, columns, and diagonals add up to the same number. For example, in 1514 the German artist Albrecht Dürer included the following 4×4 magic square in *Melencolia I* (see Figure 1.):

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

2010 *Mathematics Subject Classification.* TBD.

FIGURE 1. *Melencolia I*, Albrecht Dürer (1514). There is a 4×4 magic square in the top right of the engraving.

Although seemingly unrelated, the three problems above share many features. They all ask questions about algebraic relations between whole numbers. They also all have avatars as problems about rational points on algebraic surfaces. The most vexing commonality of these three problems is their current status: they are all open.

1.1. **Historical Remarks.** Problem (1) asks: for which integers $n > 0$ do there exist *integers* x, y, and z such that

$$x^3 + y^3 + z^3 = n? \tag{1.1}$$

In 1825, Samuel Ryley showed that every integer n (indeed, every rational number) is the sum of three *rational* cubes. Further progress through 2007 is nicely documented in [BPTYJ07, §2], where the first (and smallest!) solution to $n = 30$ is given:

$$(-283\,059\,965)^3 + (-2\,218\,888\,517)^3 + 2\,220\,422\,932^3 = 30.$$

This solution was found in 1999; Daniel Bernstein found the same solution independently and contemporaneously, based on ideas suggested by Noam Elkies.[1] At the beginning of 2019, the only $n < 100$ not known to be expressible (or not!) as a sum of three integer cubes

[1] See `http://listserv.nodak.edu/archives/nmbrthry.html` 9 July 1996.

were $n = 33$ and $n = 42$. Shortly thereafter, Andrew Booker [Boo19] showed that

$$(8\,866\,128\,975\,287\,528)^3 + (-8\,778\,405\,442\,862\,239)^3 + (-2\,736\,111\,468\,807\,040)^3 = 33,$$

and this is the smallest solution to the problem! A few months later, Booker joined forces with Andrew Sutherland to find the smallest solution to $n = 42$:

$$(-80\,538\,738\,812\,075\,974)^3 + (80\,435\,758\,145\,817\,515)^3 + (12\,602\,123\,297\,335\,631)^3 = 42.$$

For some integers n, the diophantine equation (1.1) admits no integral solutions: indeed, the set of cubes modulo 9 is $\{0, 1, -1\}$, and hence three cubes cannot add up to 4 or -4 modulo 9. Based on analytic arguments predicting the distribution of solutions to (1.1), Heath-Brown [HB92, p. 623] proposed the following conjecture:

Conjecture 1.1. *For integers $n \not\equiv \bmod \pm 4 \bmod 9$ there exist integers x, y, and z such that* (1.1) *holds.*

A box witnessing a positive solution to Problem (2) is called a perfect cuboid (Figure 2). Euler studied the closely related problem of finding boxes whose sides and face diagonals are positive integers; it seems likely he considered the problem of the existence of a perfect cuboid, though no written record of such an exploration appears to exist. The literature surrounding this problem is nicely summarized in van Luijk's undergraduate thesis [vL00].

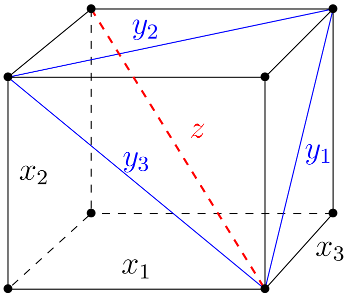

Figure 2. Can x_1, x_2, x_3, y_1, y_2, y_3, and z be integers?

Magic squares have a long history. Tradition has it that the *Lo Shu*, the earliest recorded 3×3 magic square, was first observed by Emperor Yu upon the back of a turtle (ca. 2,200 BC). The search for a 3×3 magic square of squares was popularized by Martin Gardner in 1996 [Gar96]; he attributed the problem to Martin LaBar (1984), though it had been studied by Euler in 1770 and Lucas in 1876 [Boy05]. Andrew Bremner has used the arithmetic of elliptic curves and K3 surfaces to study two related problems: finding 3×3 squares with distinct square entries such that as many as possible of the eight row, columns, and diagonals are equal [Bre99], and finding magic 3×3 squares with distinct entries, with as many entries as possible being squares [Bre01]. Our own investigations [BTVA] into the problem of finding

3×3 magic squares of squares are inspired by a similar geometric point of view, although we work with surfaces of general type, as explained below.

1.2. **Geometry determines arithmetic.** The three problems above can all be phrased as questions involving the rational or integral points on certain algebraic surfaces. We aim to show how our current understanding of the arithmetic of algebraic surfaces informs the expectations many arithmetic geometers harbor for the answers to our three problems. *Geometry determines arithmetic* shall be our mantra. To develop a feel for this mantra, we turn to a lower-dimensional situation: the arithmetic geometry of curves.

1.3. **Fermat's Last Theorem: a geometric restatement.** Fermat's Last Theorem, i.e, the statement that for $n \geq 3$ every solution $(x, y, z) \in \mathbb{Z}^3$ to the equation

$$x^n + y^n = z^n$$

satisfies $xyz = 0$, is a statement about rational points on a smooth, projective plane curve. Recall that the set of rational points on the projective plane is

$$\mathbb{P}^2(\mathbb{Q}) = \frac{\mathbb{Q}^3 - \{(0,0,0)\}}{(x,y,z) \sim (\lambda x, \lambda y, \lambda z)} \qquad \lambda \in \mathbb{Q}^*$$

We write $(x : y : z)$ for the equivalence class of (x, y, z). The projective plane $\mathbb{P}^2$ can be thought of as a compactification of the Cartesian plane $\mathbb{A}^2$; here we identify $(X, Y) \in \mathbb{A}^2(\mathbb{Q})$ with the point $(X : Y : 1) \in \mathbb{P}^2(\mathbb{Q})$. The subset of $\mathbb{P}^2(\mathbb{Q})$ whose z-coordinate is zero gives the set of rational points on the "line at infinity" that is used to compactify $\mathbb{A}^2$ to $\mathbb{P}^2$. We define $\mathbb{P}^n(\mathbb{Q})$ analogously:

$$\mathbb{P}^n(\mathbb{Q}) = \frac{\mathbb{Q}^{n+1} - \{(0,\dots,0)\}}{(x_0,\dots,x_n) \sim (\lambda x_0,\dots,\lambda x_n)} \qquad \lambda \in \mathbb{Q}^*.$$

A trivial but powerful observation is that every point $(x_0, \dots, x_n) \in \mathbb{P}^n(\mathbb{Q})$ has a representative (unique up to a global sign) with $x_0, \dots, x_n$ relatively prime integers, obtained by clearing denominators and removing common factors from any given representative. This representation of a rational point is almost unique: its only ambiguity is a global sign. For example,

$$\left(-1 : \frac{1}{2} : \frac{3}{5}\right) = (-10 : 5 : 6) \text{ as elements of } \mathbb{P}^2(\mathbb{Q}).$$

The zero-set of the Fermat expression $x^n + y^n - z^n$ defines a curve C_n in the projective plane $\mathbb{P}^2$, whose rational points are

$$C_n(\mathbb{Q}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Q}) \mid x^n + y^n - z^n = 0\}.$$

The coordinate axes in $\mathbb{P}^2$ define a reducible curve C' whose rational points are given by

$$C'(\mathbb{Q}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Q}) \mid xyz = 0\}.$$

Fermat's Last Theorem can be restated as follows: given an integer $n \geq 3$, we have

$$C_n(\mathbb{Q}) \subset C'(\mathbb{Q}).$$

We describe below some fundamental results on the arithmetic of curves, and apply them to study the set $C_n(\mathbb{Q})$. This will not give a proof of Fermat's last theorem, as we will not use anything special about the Fermat curve, other than its smoothness, its degree, and the fact that it contains rational points (e.g., $(0:1:1)$). Our goal is thus not a description the fundamental breakthroughs of Wiles and Taylor–Wiles; rather we use the Fermat curve as an excuse for a tour of the arithmetic of curves.

2. Arithmetic of Curves

2.1. **The genus of a nice curve.** By a nice variety X we mean an algebraic variety over a field k that satisfies a few technical hypotheses: X should be smooth, projective, and geometrically integral. A nice curve C is a 1-dimensional nice variety. For example, suppose that C is given by the zero-locus of a homogeneous degree n polynomial $f(x, y, z)$ in the projective plane $\mathbb{P}^2$. Let I be the ideal

$$\left\langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \right\rangle,$$

considered in the ring $\overline{k}[x, y, z]$, where $\overline{k}$ denotes a fixed algebraic closure of k; the generator f in I is redundant if $\operatorname{char} k = 0$. The Jacobian criterion and the projective Nullstellensatz together imply that C is nice if some power of the "irrelevant ideal" $\langle x, y, z\rangle$ is contained in I. For the Fermat curve, we take $k = \mathbb{Q}$ and $f = x^n + y^n - z^n$ ($n \geq 2$); the ideal $I \subseteq \overline{\mathbb{Q}}[x, y, z]$ is

$$\langle x^n + y^n - z^n, nx^{n-1}, ny^{n-1}, nz^{n-1}\rangle = \langle x^{n-1}, y^{n-1}, z^{n-1}\rangle,$$

and we can check that $\langle x, y, z\rangle^{3n-5} \subset I$, so the Fermat curve is nice.

Nice curves have one fundamental discrete invariant: their genus. It is the dimension of the vector space of global 1-forms; when $C \subset \mathbb{P}^2$ is a nice plane curve, defined by a homogeneous polynomial of degree n, this dimension coincides with the quantity

$$g = \frac{(n-1)(n-2)}{2}. \tag{2.1}$$

If $k \hookrightarrow \mathbb{C}$ then the set of complex points $C(\mathbb{C})$ can be given the structure of a compact Riemann surface C^{an}, and the genus above coincides with the number of handles on C^{an}.

2.2. **Kodaira dimension of a nice curve.** Two nice varieties X and Y defined over a field k are said to be k-birational if there exist open sets $U \subset X$ and $V \subset Y$ (for the Zariski topology) such that U and V are isomorphic as varieties over k; informally, the isomorphism $U \simeq V$ should be given by rational functions with coefficients in k. This is a very strong condition: nonempty open subsets in the Zariski topology of a nice variety are dense! For example, the proper Zariski-closed subsets on a nice curve over $\mathbb{C}$ are finite sets of points.

Many arithmetic questions about varieties have answers that depend only on the birational class of the variety; for example, if X and Y are nice $\mathbb{Q}$-varieties that are $\mathbb{Q}$-birational to each other, then X has a $\mathbb{Q}$-point if and only if Y has a $\mathbb{Q}$-point (this follows from the Lang-Nishimura Lemma [Poo17, §3.6.4]).

Birational invariants and birational classification theorems thus guide our expectations for the properties of the set of rational points on an algebraic variety. The genus of a nice curve C is a birational invariant. A related birational invariant is the Kodaira dimension $\kappa(C)$, whose precise definition is given below in §3.3. For nice curves, suffice it to say for now that

$$\kappa(C) = \begin{cases} -\infty & \text{if } g = 0, \\ 0 & \text{if } g = 1, \\ 1 & \text{if } g \geq 2. \end{cases}$$

The Kodaira dimension of a nice curve indicates curvature. For example, if $k \hookrightarrow \mathbb{C}$, the Riemann surface C^{an} has positive curvature if $\kappa(C) = -\infty$, it has flat curvature if $\kappa(C) = 0$, and it is negatively curved if $\kappa(C) = 1$.

2.3. **Rational points on curves vis-à-vis Kodaira dimension.** Let C be a nice curve over $\mathbb{Q}$.

- $\kappa(C) = -\infty$: In this case, if $C(\mathbb{Q}) \neq \emptyset$, one can show that C is isomorphic over $\mathbb{Q}$ to the projective line $\mathbb{P}^1$. This is done using a stereographic projection; we shall see a concrete example below (§2.4.1).

- $\kappa(C) = 0$: In this case, if $C(\mathbb{Q}) \neq \emptyset$, then C is an elliptic curve (by definition!), and it is well-known that the rational points of $C(\mathbb{Q})$ can be endowed with the structure of an abelian group. This group is finitely generated by a theorem of Mordell from 1922 [Sil09, VIII.4]. The structure theorem for finitely generated abelian groups then implies that
$$C(\mathbb{Q}) \simeq C(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$$
as abelian groups, where $C(\mathbb{Q})_{\mathrm{tors}}$ is the subgroup of $C(\mathbb{Q})$ consisting of points of finite order. The integer r is called the rank of C and it plays a major rôle in the Birch–Swinnerton-Dyer conjecture. A spectacular theorem of Mazur says that there are only 15 possibilities for the isomorphism class of the group $C(\mathbb{Q})_{\mathrm{tors}}$.

- $\kappa(C) = 1$: In this case, we say C is of general type. Faltings showed in 1983 that for curves of general type, the set $C(\mathbb{Q})$ is *finite*. His work, which simultaneously solved several major open problems in arithmetic geometry, earned him a Fields Medal.

2.4. **Fermat curves.** What can the general theory of the arithmetic of curves tell us about Fermat's Last Theorem? Let

$$C_n : \quad x^n + y^n = z^n$$

be the Fermat curve of exponent n, considered as a nice curve in the projective plane $\mathbb{P}^2_{\mathbb{Q}}$.

2.4.1. *A rational curve:* $n = 2$. The curve C_2 has genus 0 by (2.1), and hence $\kappa(C_2) = -\infty$. Since $(0 : 1 : 1) \in C_2(\mathbb{Q})$, general theory predicts that C_2 is $\mathbb{Q}$-isomorphic to the projective line $\mathbb{P}^1$. We construct an isomorphism $\mathbb{P}^1 \to C_2$ using the (inverse of) stereographic projection. Recall we identified $(X, Y) \in \mathbb{A}^2(\mathbb{Q})$ with $(X : Y : 1) \in \mathbb{P}^2(\mathbb{Q})$; this identification is valid in the locus of $\mathbb{P}^2$ where $z \neq 0$, where we have set $X = x/z$ and $Y = y/z$. The part of C_2 in this affine "patch" is the circle

$$X^2 + Y^2 = 1,$$

and the point $(0 : 1 : 1) \in C_2(\mathbb{Q})$ is identified with the point $(0, 1) \in \mathbb{A}^2(\mathbb{Q})$. We use this point to create the isomorphism $\mathbb{P}^1 \to C_2$, as follows. Define the map of algebraic varieties

$$\mathbb{A}^1 \to \mathbb{A}^2, \qquad s \mapsto \left(\frac{2s}{s^2+1}, \frac{s^2-1}{s^2+1} \right).$$

This is the inverse map to a stereographic projection, as Figure 3 shows.

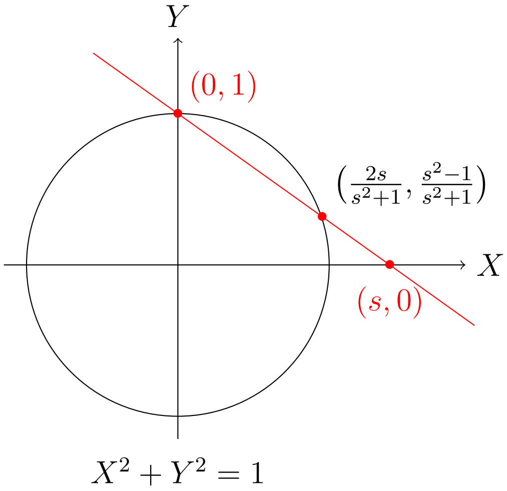

FIGURE 3. Stereographic Projection

We want to extend our construction to a map $\phi \colon \mathbb{P}^1 \to C_2$ in such a way that

$$(s : 1) \mapsto \left(\frac{2s}{s^2+1} : \frac{s^2-1}{s^2+1} : 1 \right).$$

Let S and T be homogeneous coordinates of $\mathbb{P}^1$. Set $s = S/T$; this identifies $s \in \mathbb{A}^1$ with $(s : 1) \in \mathbb{P}^1$. The map above becomes

$$(S/T : 1) \mapsto \left(\frac{2S/T}{(S/T)^2+1} : \frac{(S/T)^2-1}{(S/T)^2+1} : 1 \right)$$

which can be rewritten more pleasantly as

$$(S : T) \mapsto \left(2ST : S^2 - T^2 : S^2 + T^2 \right).$$

This is the map ϕ we are looking for! It makes sense even for points like $(S : T) = (1 : 0)$. By inspection, the map

$$\psi\colon C_2 \to \mathbb{P}^1, \qquad (x : y : z) \mapsto (y + z : x)$$

is an inverse for ϕ, at least for $(x : y : z) \neq (0 : 1 : -1)$. Since ϕ is an isomorphism, and since rational points $(S : T)$ are determined only up to a scalar multiple, we conclude that every rational point on the curve C_2 has a representative of the form

$$(x : y : z) = (2ST, S^2 - T^2, S^2 + T^2),$$

where S and T are relatively prime integers. The point $(x : y : z) \in C_2(\mathbb{Q})$ is also determined only up to a scalar multiple. We conclude that every Pythagorean triple, i.e., every integral solution to $x^2 + y^2 = z^2$, has the form

$$x = k \cdot (2ST), \qquad y = k \cdot (S^2 - T^2), \qquad z = k \cdot (S^2 + T^2).$$

where $k \in \frac{1}{2}\mathbb{Z}$ and S, T are relatively prime integers. The reason we allow k to possibly be a half-integer is that if S and T are both odd, then $2 \mid \gcd(2ST, S^2 - T^2, S^2 + T^2)$.

This account of the shape of Pythagorean triples reflects our mantra: Geometry determines Arithmetic! Many of us learned a proof of the shape of Pythagorean triples that uses only basic algebra and divisibility relations; its "elementary nature" undercuts both the beauty of the geometric proof and a feeling of genuine understanding.

2.4.2. *An elliptic curve: $n = 3$.* The curve C_3 has genus 1 by (2.1), and hence $\kappa(C_3) = 0$. Since $(0 : 1 : 1) \in C_3(\mathbb{Q})$, the curve C_3 is an elliptic curve, so by Mordell's Theorem, we have $C_3(\mathbb{Q}) \simeq C_3(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$. We claim that

$$C_3(\mathbb{Q})_{\mathrm{tors}} = \{(1 : 0 : 1), (0 : 1 : 1), (1 : -1 : 0)\}. \tag{2.2}$$

This can be shown with an important tool: reduction modulo a prime p. Let $C_{3,p}$ be the Fermat curve with $n = 3$, defined over the finite field $\mathbb{F}_p$ with p elements. We define a reduction map $C_3(\mathbb{Q}) \to \mathbb{C}_{3,p}(\mathbb{F}_p)$ by sending $(x : y : z) \in C_3(\mathbb{Q})$ to $(x \bmod p : y \bmod p : z \bmod p)$, where we have choosen a representative $(x : y : z)$ with x, y, and z relatively prime integers. As long as $p > 3$ the curve $C_{3,p}$ is nice, and crucially we have an injection of groups

$$C_3(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow C_{3,p}(\mathbb{F}_p)$$

via the reduction map we just described (see [Sil09, §VII.3]). Because there are only finitely many solutions to the equation $x^3 + y^3 = z^3$ in $\mathbb{F}_p$, it is straightforward to compute that $\#C_{3,5}(\mathbb{F}_5) = 6$ and $\#C_{3,7}(\mathbb{F}_7) = 9$. This shows that $C_3(\mathbb{Q})_{\mathrm{tors}}$ is either the trivial group, or it is $\mathbb{Z}/3\mathbb{Z}$.

To show that the rank r of C_3 is zero, we may apply deep results of Gross-Zagier and Kolyvagin on the L-series of elliptic curves with complex multiplication [GZ86, Kol88]. Loosely speaking, an elliptic curve $E/\mathbb{Q}$ has complex multiplication if it has an unusually large endomorphism ring. The L-series $L_{E/\mathbb{Q}}(s)$ of E is defined by an Euler product over the primes, whose individual factors record information about the modulo p reduction of E. The function $L_{E/\mathbb{Q}}(s)$ converges for $\Re(s) > \frac{3}{2}$; even before Wiles' work on Fermat's Last Theorem, we knew that if E has complex multiplication, then $L_{E/\mathbb{Q}}(s)$ has an analytic continuation to the entire complex plane, thanks to work of Deuring and Weil. The Birch–Swinnerton-Dyer conjecture predicts that the order of vanish of $L_{E/\mathbb{Q}}(s)$ at $s = 1$ is equal to the rank r of E; the results in [GZ86, Kol88] together imply that if $L_{E/\mathbb{Q}}(1) \neq 0$, then $r = 0$, i.e., $E(\mathbb{Q})$ is finite.

The curve C_3 is isomorphic to the curve,

$$E : Y^2 - 9Y = X^3 - 27$$

considered in the usual affine plane $\mathbb{A}^2_{\mathbb{Q}}$. This curve has j-invariant 0 (see [Sil09, III.1]), and hence has complex multiplication. Using computer software, we can check that in this case

$$L_{E/\mathbb{Q}}(1) \approx 0.588879583428483319104563166550,$$

and hence $C_3(\mathbb{Q})$ is finite, equal to the set given in (2.2).

2.4.3. *Curves of general type: $n \geq 4$.* The curves C_n have genus ≥ 2 whenever $n \geq 4$ by (2.1), and hence $\kappa(C_n) = 1$. By Faltings' Theorem, we know that $C_n(\mathbb{Q})$ is finite; it is however nonempty, as $(0 : 1 : 1) \in C_n(\mathbb{Q})$. Faltings' proof of his theorem is not effective. This is as far as the general qualitative theory of curves will take us. The methods of Wiles and Taylor–Wiles opened up whole new research programs in Number Theory, but the connection to Fermat's Last Theorem uses the explicit shape of Fermat's equation to construct, from a putative nontrivial solution, an elliptic curve too exotic to exist.

3. Arithmetic of higher-dimensional varieties

We now leave the realm of algebraic curves to explore higher-dimensional spaces. From here on out, unless otherwise stated, all varieties are assumed to be nice; by a surface, we mean a nice variety of dimension 2. A concrete example of a surface in projective 3-space $\mathbb{P}^3$, with coordinates x, y, z, and w, is given by

$$S/\mathbb{Q} : x^4 + 2y^4 = z^4 + 4w^4.$$

This is an example of a K3 surface; it is simply connected and carries a nowhere-vanishing holomorphic 2-form. All smooth quartic surfaces in $\mathbb{P}^3$ have these two properties; the one above was considered by Swinnerton-Dyer. It has rational points, e.g., $(x : y : z : w) = (1 : 0 : 1 : 0)$ is in $S(\mathbb{Q})$. It is unknown if $S(\mathbb{Q})$ is finite or not.

3.1. **Local Obstructions.** Because the varieties $X/\mathbb{Q}$ we study are projective, and hence both the denominators of the coordinates of a rational point as well as the denominators in the defining equations of X can be cleared out, the sets of integral solutions $X(\mathbb{Z})$ and rational solutions $X(\mathbb{Q})$ coincide; see §1.3. This incidental reframing affords an important tool: reduction modulo p^n for any prime p and any exponent $n \geq 1$. In order to have

$X(\mathbb{Z}) \neq \emptyset$, i.e., a nontrivial integral solution to the set of equations defining X, the same set of equations *must have* solutions modulo p^n for every prime p and every exponent n; we call these solutions points modulo p^n. Our set of equations must also have solutions in $\mathbb{R}$. If $X/\mathbb{Q}$ fails to have points modulo p^n for some p^n, or if $X(\mathbb{R}) = \emptyset$, we say there is a local obstruction to the existence of rational points[2].

We have all experienced local obstructions: one of the first proofs many of us are exposed to is the irrationality of $\sqrt{2}$. Equivalently, the variety $x^2 - 2y^2 = 0$ in $\mathbb{P}^1$ has no $\mathbb{Q}$-points: there are no nontrivial solutions[3] to its defining equation modulo 4.

For a given prime p and exponent n there are only finitely many possible solutions modulo p^n to the set of equations defining X. But there are infinitely many primes p and exponents n. The necessity of local solutions asks us to trade, with no assurance of success, one hard problem for infinitely many easier problems. Is this a good trade-off? Most definitely, thanks to the Weil Conjectures, now theorems after the revolutionary efforts and insights of Dwork, Grothendieck, and Deligne (see [Poo17, Ch. 7] for an introduction to the subject). In short, the Weil Conjectures give a precise bound p_0, in terms of the geometry of X, such that X has solutions modulo p for all $p > p_0$, as long as the reductions of the equations of X modulo p define a smooth projective variety over $\mathbb{F}_p$. By means of Hensel's lemma, a p-adic analogue of the Newton–Raphson method, smooth solutions modulo p can be leveraged to construct solutions modulo p^n for all $n \geq 2$; see [Poo17, Theorem 3.5.63]. This leaves a finite set $\mathcal{S}$ of primes to check: those $p \leq p_0$, and those primes for which X does not have smooth reduction modulo p. The later can be calculated explicitly with a Gröbner basis computation. It then remains to find solutions modulo p^{n_0} for $p \in \mathcal{S}$ and some small n_0 that are liftable to solutions modulo p^n for all $n > n_0$ using Hensel's lemma, whenever possible. Checking that $X(\mathbb{R}) \neq \emptyset$ often comes down to a Lagrange multipliers problem.

3.2. **Local obstructions are not enough.** Sadly, there are nice varieties $X/\mathbb{Q}$ that have points modulo p^n for all primes p and all exponents n, as well as $\mathbb{R}$-points, for which $X(\mathbb{Q}) = \emptyset$. The first example of such varieties was found independently by Lindt and Reichardt around 1940. An example made famous by Selmer is the genus 1 plane curve

$$3x^3 + 4y^3 + 5z^3 = 0,$$

which is a 'twist' of the Fermat curve C_3. An example dear to my heart is one considered by Birch and Swinnerton-Dyer around 1975:

$$X \subset \mathbb{P}^4 : \begin{cases} x_0x_1 &= x_2^2 - 5x_3^2 \\ (x_0 + x_1)(x_0 + 2x_1) &= x_2^2 - 5x_4^2 \end{cases}$$

[2] Motivating the terminology here is the statement that $X(k) = \emptyset$ for a locally compact field k that contains $\mathbb{Q}$, namely $k = \mathbb{R}$, or $k = \mathbb{Q}_p$, the field of p-adic numbers.

[3] More precisely, if the variety has a rational point $(x : y)$, then we may assume that x and y are coprime integers, because $(x, y) \in \mathbb{P}^1(\mathbb{Q})$. On the other hand, the only solution to $x^2 - 2y^2 \equiv 0 \bmod 4$ requires that both x and y are divisible by 2.

This is a del Pezzo surface of degree 4, as is every smooth intersection of two distinct quadrics in $\mathbb{P}^4$ (and vice versa). In 2012, Viray observed that the rational map $X \dashrightarrow \mathbb{P}^1$ given by $(x_0 : \cdots : x_4) \mapsto (x_0 : x_1)$ can be used to explain why $X(\mathbb{Q}) = \emptyset$: the fibers of this map are genus 1 curves that fail to have p^n points for some p and some n, although which p and which n depends on the fiber you are looking at! This is a stunning visual interpretation of a so-called Brauer-Manin obstruction. Viray and I went on to show that something similar is true for all del Pezzo surfaces of degree 4 that have a nontrivial Brauer-Manin obstruction to the existence of rational points [VAV14, Corollary 1.3].

3.3. **Kodaira dimension of a variety.** The Kodaira dimension $\kappa(X)$ of a variety X/k is an element of the set $\{-\infty, 0, 1, \dots, \dim X\}$ that captures the largest eventual dimension of the image of X by maps constructed out of pluricanonical forms of increasing weight. More precisely, it is

$$\kappa(X) := \limsup_{m\to\infty} \left(\dim\left(\operatorname{im}\left(\phi_m \colon X \dashrightarrow \mathbb{P}\left(\mathrm{H}^0(X, \omega_X^{\otimes m})^\vee\right)\right)\right)\right),$$

where $\mathbb{P}\left(\mathrm{H}^0(X, \omega_X^{\otimes m})^\vee\right)$ denotes the projectivization of the (dual) vector space of global pluricanonical forms of weight m, and ϕ_m is the map given by evaluating a chosen basis of this vector space at a given point. Projective n-space $\mathbb{P}^n$ has no nonzero pluricanonical forms, i.e., $\mathrm{H}^0(\mathbb{P}^n, \omega_{\mathbb{P}^n}^{\otimes m}) = 0$ for all $m \geq 1$, so $\kappa(\mathbb{P}^n) = -\infty$. At the other end of a spectrum, a nice hypersurface $X_d \subset \mathbb{P}^n$ defined by a homogeneous polynomial of degree d has Kodaira dimension $\kappa(X_d) = \dim X_d = n - 1$ if $d > n + 1$. Enriques gave a classification of nice surfaces $S/\mathbb{C}$ at the beginning of the 20th century, parceling out surfaces by their Kodaira dimension (we give their modern names here):

$$\kappa(S) = \begin{cases} -\infty & S \text{ is rational or ruled;} \\ 0 & S \text{ is abelian, K3, Enriques, or bi-elliptic;} \\ 1 & S \text{ is properly elliptic;} \\ 2 & S \text{ is of general type.} \end{cases}$$

For a nice surface $S_d \subset \mathbb{P}^3$ defined by a homogeneous polynomial of degree d, we have

$$\kappa(S_d) = \begin{cases} -\infty & \text{if } d = 1, 2, 3; \\ 0 & \text{if } d = 4; \\ 2 & \text{if } d \geq 5. \end{cases} \tag{3.1}$$

As in the case of curves, the arithmetic of a surface $S/\mathbb{Q}$, understood here as a qualitative and quantitative description of the set of rational points $S(\mathbb{Q})$, becomes harder to study and access the larger its Kodaira dimension. Varieties with $\kappa(X) = \dim X$ are said to be of general type; they are very difficult to study from a number theoretic perspective.

4. Three problems revisited

The three questions posed in §1 can all be recast as questions about rational points on algebraic surfaces.

4.1. **Sums of three cubes.** The sum of three cubes problem involves the part of the projective $\mathbb{Q}$-surface

$$X_n^c \subset \mathbb{P}^3 : x^3 + y^3 + z^3 - nw^3 = 0$$

contained in the affine patch $X_n := X_c^n \cap \{w = 1\}$. The variety X_n^c is a del Pezzo surface of degree 3, and $\kappa(X_n^c) = -\infty$ by (3.1).

Since X_n is not itself a projective variety, there is a difference between the sets of integral points $X_n(\mathbb{Z})$ and rational points $X_n(\mathbb{Q})$. For example, we have

$$\left(\frac{n^3 - 3^6}{3^2n^2 + 3^4n + 3^6}\right)^3 + \left(\frac{-n^3 + 3^5n + 3^6}{3^2n^2 + 3^4n + 3^6}\right)^3 + \left(\frac{a^2 - 3^4n}{3^2n^2 + 3^4n + 3^6}\right)^3 = n$$

showing that $X_n(\mathbb{Q}) \neq \emptyset$ for all $n \in \mathbb{Z}$. On the other hand, we have seen that $X_n(\mathbb{Z}) = \emptyset$ whenever $n \equiv \pm 4 \bmod 9$, because there is a local obstruction at $p = 3$ in this case. A conjecture of Colliot-Thélène and Sansuc predicts that the absence of rational points on a locally soluble (projective) del Pezzo surface can be explained by a Brauer-Manin obstruction [CTS80]. It is less clear what to expect for the set of integral points on an affine part of a del Pezzo surface (e.g., [Har17]). Nevertheless, Colliot-Thélène and Wittenberg computed the Brauer group for the affine surfaces X_n, and showed that there is no *integral* Brauer-Manin obstruction to the existence of integral points when $n \not\equiv \pm 4 \bmod 9$ [CTW12]. Some arithmetic geometers, myself included, view this as positive evidence for Conjecture 3.1, although recent results of Harpaz [Har17] call for caution.

4.2. **Perfect Cuboids.** A perfect cuboid with edges labeled as in Figure 2 gives rise to a rational point with nonzero coordinates on the variety $S \subset \mathbb{P}^6$ defined by the relations

$$\begin{aligned} x_1^2 + x_2^2 &= y_3^2 \\ x_2^2 + x_3^2 &= y_1^2 \\ x_3^2 + x_1^2 &= y_2^2 \\ x_1^2 + x_2^2 + x_3^2 &= z^2, \end{aligned}$$

which are derived from the Pythagorean constraints imposed by the box. The variety S has dimension 2, but it is not smooth: its singular locus consists of 48 ordinary double points (each of which looks locally like the vertex of a cone). Each of these nodal singularities has at least one zero coordinate, so none of these special points give rise to a perfect cuboid. They are mild singularities, and a desingularization $\widetilde{S}$ of S has $\kappa(\widetilde{S}) = 2$, so we say that S is of general type. A deep conjecture of Lang, informed by conjectures of Bogomolov, Bombieri, Green-Griffiths, Kobayashi, and Vojta, predicts that a nice surface of general type over a number field contains very few rational points.

Conjecture 4.1 ([Lan86, Conj. 5.8]). *Let X be a nice variety of general type defined over a number field K. Then there is a proper, Zariski-closed subset $Z \subset X$, such that for all number fields L containing K, the set $X(L) \setminus Z(L)$ is finite.*

If X is a nice surface, then a set Z as in Conjecture 4.1 consists of a finite union of isolated points and curves. Any isolated points and curves of genus ≥ 2 can be safely removed from Z without altering the conclusion of the conjecture, by Faltings' theorem. Hence, if X is a surface then the conjectured set Z can be reduced to a finite union of curves of (geometric) genus 0 or 1. On the other hand, because any curve of genus 0 and 1 has infinitely many rational points, at least over some finite extension L/K, any such curve on X would have to be included in Z. Thus, when $\dim X = 2$, Conjecture 4.1 implies that X contains only finitely many curves of genus 0 or 1.

Applying Conjecture 4.1 to $\widetilde{S}$, taking advantage of the mild nature of the singularities of S, we deduce that S contains only finitely many curves of genus 0 or 1, and that outside of those curves there are only finitely many points in $S(\mathbb{Q})$. Lang's conjecture has thus motivated a detailed study of the locus of curves of genus 0 and 1 on S [vL00, ST10, GFU, BTVA].

In his undergraduate thesis [vL00], van Luijk showed that S contains at least 32 curves of genus 0 and 60 curves of genus 1. For example, 24 of the genus 0 curves are obtained by looking at the irreducible components of the intersection

$$S \cap \{x_1x_2x_3 = 0\}.$$

These curves are defined over $\mathbb{Q}$, but every rational point on them has at least one zero coordinate, so we do not obtain a perfect cuboid from these points. More generally, none of the rational points on van Luijk's list of 92 curves of genus 0 or 1 give rise to a perfect cuboid over $\mathbb{Q}$, but some of the genus 1 curves do have nontrivial points over higher-degree number fields. For example,

$$(x_1 : x_2 : x_3 : y_1 : y_2 : y_3 : z) = (2\sqrt{6} : 2\sqrt{6} : 1 : 5 : 5 : 4\sqrt{3} : 7) \in S\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right).$$

García-Fritz and Urzúa [GFU], and later Bruin, Thomas and I [BTVA] exploited the presence of symmetric differentials on S, a phenomenon made possible by the existence of the 48 nodal singularities on S, to constrain the locus of genus 0 and 1 curves on S. Our efforts show that any genus 0 curve on S must pass through at least 6 nodes of S, that any genus 1 curve on S must pass through at least 2 nodes, and that there are only finitely many genus 0 or 1 curves passing through at most 13 nodes. The curves in van Luijk's thesis satisfy these constraints. New ideas are required to push these two bounds closer to each other; it would be very interesting to show that the surface S does indeed have finitely many curves of genus 0 or 1, and to have set of equations defining these curves. In particular, are the curves in van Luijk's thesis the only curves of genus 0 or 1 on S?

Although Conjecture 4.1 is agnostic about the existence of perfect cuboids, when taken together with our current (sadly incomplete) knowledge of the low genus curves on the surface S, it suggests that the problem of finding perfect cuboids is *hard for good reasons.*

4.3. **Magic squares of squares.** A 3×3 magic square of squares

x_1^2	x_2^2	x_3^2
x_4^2	x_5^2	x_6^2
x_7^2	x_8^2	x_9^2

gives rise to a rational point with nonzero coordinates on the variety $M \subset \mathbb{P}^8$ defined by the relations

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= x_4^2 + x_5^2 + x_6^2 = x_7^2 + x_8^2 + x_9^2 = x_1^2 + x_4^2 + x_7^2 \\ &= x_2^2 + x_5^2 + x_8^2 = x_1^2 + x_5^2 + x_9^2 = x_3^2 + x_5^2 + x_7^2. \end{aligned}$$

A priori, it looks like we missed the sum $x_3^2 + x_6^2 + x_9^2$, corresponding to the third column of the magic square, but you can convince yourself that if the sums of the three rows and first two columns are equal to each other, then the sum in the third column is also equal to their common value. The variety M again has dimension 2, although as in the case of the surface of perfect cuboids, M is slightly singular: its singular locus comprises 256 isolated ordinary double points. Its minimal desingularization $\widetilde{M}$ satisfies $\kappa(\widetilde{M}) = 2$, so we say that M is of general type.

The surface M contains rational points. For example,

$$(x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8 : x_9) = (1 : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1) \in M(\mathbb{Q}),$$

but the corresponding magic square of squares is not interesting: its entries are not distinct. A similar conclusion is true of all rational points on M known to date. As with the surface S parametrizing perfect cuboids, Conjecture 4.1 predicts that M contains only finitely many curves of genus 0 or 1, and that outside these curves it has only finitely many $\mathbb{Q}$-points. The methods of [BTVA] are strong enough to confirm part of this prediction.

Theorem 4.2 ([BTVA])**.** *The surface parametrizing* 3×3 *magic squares of squares contains only finitely many curves of genus* 0 *or* 1*.*

To be sure, there *are* curves of genus 0 or 1 on M. For example, the components of the intersection of M with a hyperplane of the form $x_i \pm x_j = 0$ for $i, j \in \{1, \dots, 9\}$ give rise to such curves. Points on these curves, however, give rise in turn to uninteresting cuboids, because $x_i^2 = x_j^2$ (or $x_i^2 = 0$ if $i = j$). A similar phenomenon happens for other curves of genus 0 or 1 on M that we know of. It would be interesting to explicitly determine the totality of curves of low genus on M. In [BTVA], we explain some incipient ideas that could be used towards such a computation, but likely some new ideas are required to execute this task. In any case, Conjecture 4.1 together with Theorem 4.2 and empirical observations of low genus curves on M suggest that perhaps there are no 3×3 magic squares of squares, or that if they exist, they will be *hard to find.*

Curiously, there do exist 4×4 magic squares of squares! Euler found one in 1770:

68^2	29^2	41^2	37^2
17^2	31^2	79^2	32^2
59^2	28^2	23^2	61^2
11^2	77^2	8^2	49^2

In fact, Euler sent this square to Lagrange in a letter, without any explanation of how he constructed it. However, he presented his ideas to the St. Petersburg Academy of Sciences the same year; the construction is based on the observation that the product of two sums of four squares can itself be expressed as a sum of four squares. This idea, combined with some partial progress by Euler, led Lagrange to the first complete proof of the *four squares theorem*: every positive integer is the sum of at most four square integers [Boy05].

A cursory internet search will reveal to the reader that there are $n \times n$ magic squares for several values of $n > 3$. To a geometer, this not surprising. An $n \times n$ magic square of squares will be a rational point on a variety cut out by $2n$ quadrics in the space $\mathbb{P}^{n^2-1}$. If this intersection were smooth (which it is not, but the singularities are not horrific), then its Kodaira dimension would be $-\infty$ for $n \geq 5$. In other words, these spaces are strongly positively curved. It is quite reasonable from a geometric point of view that these spaces would carry many rational points. I would expect the following to be true.

Conjecture 4.3. *There is a positive integer n_0 such that for every integer $n \geq n_0$ there exists an $n \times n$ magic square of squares, whose entries are nonzero and distinct.*

I would further expect that Conjecture 4.3 holds with $n_0 = 4$. Ultimately, if an integer n_0 making Conjecture 4.3 hold must be > 4, or if Conjecture 4.3 is false, it will be on account of some interesting geometry of the variety parametrizing $n \times n$ magic squares of squares for small values of n.

5. Conclusion

I hope I have convinced you that geometry and arithmetic are inextricably linked. Historically, our understanding of geometry has preceded our understanding of arithmetic; witness the case of elliptic curves, where unsolved arithmetic problems abound, yet our geometric understanding of them is mature. The diophantine enthusiast, whether amateur or professional, would do well to learn and use geometric techniques. General geometric considerations will rarely suffice to solve hard diophantine problems, but they will likely provide mathematical inspiration, as well as a deeper understanding of the difficulties involved in such problems.

Acknowledgements

I would like to thank the organizers of JMM 2020 at Denver for the invitation and opportunity to share with a large audience a slice of the story of how geometry determines arithmetic. I would also like to thank my family, mentors, friends and colleagues, who provided opportunities, encouragement, and the support without which the invitation to JMM 2020 would not have happened in the first place. I hope you know who you are; the list is too long to include in this margin.

I thank Ronald van Luijk for comments on an earlier version of this article, and the anonymous referees for the helpful and constructive feedback.

References

[BPTYJ07] M. Beck, E. Pine, W. Tarrant, and K. Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690. ↑1.1

[Boo19] A. R. Booker, *Cracking the problem with 33*, Res. Number Theory **5** (2019), no. 3, Paper No. 26, 6. ↑1.1

[Boy05] C. Boyer, *Some notes on the magic squares of squares problem*, Math. Intelligencer **27** (2005), no. 2, 52–64. ↑1.1, 4.3

[Bre99] A. Bremner, *On squares of squares*, Acta Arith. **88** (1999), no. 3, 289–297. ↑1.1

[Bre01] ———, *On squares of squares. II*, Acta Arith. **99** (2001), no. 3, 289–308. ↑1.1

[BTVA] N. Bruin, J. Thomas, and A Várilly-Alvarado, *Explicit Computation of Symmetric Differentials and its Application to Quasi-hyperbolicty.* arXiv:1912.08908. ↑1.1, 4.2, 4.3, 4.2, 4.3

[CTS80] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles*, Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979, Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980, pp. 223–237 (French). ↑4.1

[CTW12] J.-L. Colliot-Thélène and O. Wittenberg, *Groupe de Brauer et points entiers de deux familles de surfaces cubiques affines*, Amer. J. Math. **134** (2012), no. 5, 1303–1327 (French, with French summary). ↑4.1

[GFU] N. García-Fritz and G Urzúa, *Families of explicit quasi-hyperbolic and hyperbolic surfaces*, Math. Z. to appear. arXiv:1804.07671. ↑4.2

[Gar96] M. Gardner, *The Magic of* 3×3, Quantum **6** (1996), 24–26. ↑1.1

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. ↑2.4.2

[Har17] Y. Harpaz, *Geometry and arithmetic of certain log K3 surfaces*, Ann. Inst. Fourier (Grenoble) **67** (2017), no. 5, 2167–2200 (English, with English and French summaries). ↑4.1

[HB92] D. R. Heath-Brown, *The density of zeros of forms for which weak approximation fails*, Math. Comp. **59** (1992), no. 200, 613–623. ↑1.1

[Kol88] V. A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $Ш(E, \mathbf{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671 (Russian); English transl., Math. USSR-Izv. **32** (1989), no. 3, 523–541. ↑2.4.2

[Lan86] S. Lang, *Hyperbolic and Diophantine analysis*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 159–205. ↑4.1

[vL00] R. van Luijk, *On Perfect Cuboids*, 2000. Doctoraalscriptie – Universiteit Utrecht. ↑1.1, 4.2

[Poo17] B. Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. ↑2.2, 3.1

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. ↑2.3, 2.4.2

[ST10] M. Stoll and D. Testa, *The surface parametrizing cuboids* (2010). arXiv:1009.0388. ↑4.2

[VAV14] A. Várilly-Alvarado and B. Viray, *Arithmetic of del Pezzo surfaces of degree 4 and vertical Brauer groups*, Adv. Math. **255** (2014), 153–181. ↑3.2

Department of Mathematics MS 136, Rice University, 6100 S. Main St., Houston, TX 77005, USA

E-mail address: `av15@rice.edu`

URL: `http://math.rice.edu/~av15`