Sum of three cubes: A problem revisited

Subham Das

March, 2023

Abstract

In this term paper[1] we discuss how the problem of characterizing whole numbers which can be written as a sum of three cubes can be reframed into a problem in purely geometrical terms, more precisely as a problem about rational points on algebraic surfaces. The goal of this article is to walk across the deeply entrenched bond between the fields of Algebraic Geometry and Number Theory, without aiming for a complete and exhaustive treatment of the concepts which we shall encounter on our way.

1 The problem

The name of the original formulator of this problem has been lost to antiquity. The statement is as follows :

Question 1.1. *What are the whole numbers n for which there exists three integers a, b, c such that*

$$n = a^3 + b^3 + c^3$$

Following is a brief timeline on the history of attacks on this problem and its current status before diving into our alternate approach :

- The first attack was rendered by Samuel Ryley in 1825 who had proved that any integer, and in fact every rational number, is expressible as a sum of three rational cubes.

- In the year 1999, the first and smallest solution known yet was gievn by Daniel Bernstein based on the idea of Noam Elkies for $n = 30$,

$$(-283059965)^3 + (-2218888517)^3 + (2220422932)^3 = 30.$$

- Upto the year 2019, the only solutions which were not known to be expressible (or not expressible) as sum of three integer cubes for $n < 100$ were $n = 33$ and $n = 42$

- In March 2019, Andrew Booker found the solution for $n = 33$ via algorithmic methods

$$(8866128975287528)^3 + (-8778405442862239)^3 + (-2736111468807040)^3 = 33$$

[1] This term paper is a part of evaluation for the course MTH419 - Number Theory. I would like to sincerely acknowledge my gratitude to Prof. Kapil H. Paranjape for his supervision and guidance towards the writing of this article.

- In September 2019, Andrew Booker and Andrew Sutherland together found a solution for $n = 42$ using stronger algorithms :

$$(-80538738812075974)^3 + (80435758145817515)^3 + (12602123297335631)^3 = 42$$

In fact for some integers there is no expression of this form. For instance 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 prediction of solutions via analytical arguments Heath-brown proposed the following conjecture:

Conjecture 1.2. *For $n \not\equiv \pm 4$ or 9 there exists a, b, c such that*

$$n = a^3 + b^3 + c^3$$

2 Geometry and Arithmetic

Next we shall illustrate an example of how one can geometrically restate a problem of arithmetic into a problem about rational points on algebraic surfaces through the arithmetic geometry of curves.

2.1 Fermat's Last Theorem

Fermat's last theorem is stated as follows :

Theorem 2.1. *For $n \geq 3$ every solution $(x, y, z) \in \mathbb{Z}$ of $x^n + y^n = z^n$ satisfies $xyz = 0$*

Next we define what are rational points on the projective plane :

Definition 2.2. *The set of rational points in a projective plane is defined as $\mathbb{P}^2(\mathbb{Q}) = \{\mathbb{Q}^3 - (0, 0, 0)\}/\sim$ where $\sim$ is the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for $\lambda \in \mathbb{Q}^*$*

One denotes the equivalence class (x, y, z) as $(x : y : 1)$ thus identifying $(x, y) \in \mathbb{A}^2$ to $(x : y : 1) \in \mathbb{P}^2(\mathbb{Q})$
It is also interesting to note that the subset of $\mathbb{P}^2(\mathbb{Q})$ whose z coordinate is zero gives the 'line at infinity' which compactifies $\mathbb{A}^2$ to $\mathbb{P}^2$.

One can define $\mathbb{P}^n$ analogously. An important point to observe is that for every point $(x_0 \dots x_n) \in \mathbb{P}^n(\mathbb{Q})$ there is a representation $(v_0 \dots v_n)$ obtained by clearing the denominators and removing common factors such that $v_0 \dots v_n$ are relatively prime integers. For example,

$$\left(\frac{4}{5}, -\frac{3}{7}, 3\right) = (28 : -15 : 105) \text{ as elements of } \mathbb{P}^2(\mathbb{Q})$$

For the expression $x^n + y^n - z^n$ of the Fermat's Last theorem one can define a curve in $\mathbb{P}^2$ whose rational points are defined as follows :

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

Similarly one obtains another curve in $\mathbb{P}^2$ such that whose rational points are :

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

Thus taking into account the previous representation, one can restate Fermat's Last Theorem as follows :

Theorem 2.3. *Given an integer $n \geq 3$ one has the inclusion $C_n(\mathbb{Q}) \subset C'(\mathbb{Q})$*

3 Arithmetic of curves

3.1 Nice curves

One defines a **nice** variety X as an algebraic variety over a field k (in our case mostly $k = 0$) such that it is smooth, projective. A nice curve in particular an one dimensional variety. Fermat curves for example, are nice curves.

We are concerned about nice curves because they have one fundamental discrete invariant which is their **genus** which is defined as the dimension of the vector space of 1-forms (smooth sections of the cotangent bundle of the curve). When $C \subset \mathbb{P}^2$ is a curve defined by a homogenous polynomial of degree n, then the genus is defined as

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

The above is a consequence of the Riemann Roch Theorem if $k \subset \mathbb{C}$.

3.2 Kodaira dimension of a nice curve

Definition 3.1. *A variety X and a variety Y are said to be k-**birational** if there exists two open sets (in the Zariski Topology) $U \subset X$ and $V \subset Y$ such that U and V are isomorphic to each other as varieties over k*

Informally, one can say that the isomorphism between U and V is given by rational functions with coefficients in k.
One of the motivations to introduce the condition of birationality is that it helps answering questions about arithmetic such as if X and Y are nice $\mathbb{Q}$-varieties then they are $\mathbb{Q}$-birational, which implies thatr if X has a $\mathbb{Q}-$point then Y also has a $\mathbb{Q}-$point

For this reason, Invariants under birational invariants and classifications via them tells us a lot many properties of the set of rational points on an algebraic variety. One such birational invariant is the genus of a curve. Similarly we shall define an important birational invariant of (nice) curves as follows :

Definition 3.2. *If the genus of a nice curve C is defined as g then the **Kodaira dimension** of the curve is defined as follows :*

1. $\mathfrak{K}(C) = -\infty$ *if* $g = 0$
2. $\mathfrak{K}(C) = 0$ *if* $g = 1$ $\mathfrak{K}(C) = 1$ *if* $g \geq 2$

In fact, the Kodaira dimension also indicates the curvature. If C is the corresponding Riemann surface then $\mathfrak{K}(C) = -\infty$ indicates positive curvature, if $\mathfrak{K} = 0$ then flat curvature and if $\mathfrak{K}(C) = 1$ then it has negative curvature.

3.3 Rational points via Kodaira Dimension

We shall now see how rational points on a nice curve C vary with Kodaira dimension. The detailed construction of the following can be found in [Alv01].

- $\mathfrak{K}(C) = -\infty$. If the set of rational points is nonempty then one can show that over $\mathbb{Q}$, the curve C is isomorphic to $\mathbb{P}^1$.
- $\mathfrak{K}(C) = 0$. If the set of rational points is nonempty then one can show that over $\mathbb{Q}$, the curve C is an elliptic curve and that the set $C(\mathbb{Q})$ can be endowed with the structure of an abelian group. The rank of this abelian group (by structure theorem of finite abelian groups) plays an important role in the Birch-Swinnerton-Dyer conjecture.
- $\mathfrak{K}(C) = 1$. If the set of rational points is nonempty then one says that the curve C is that of a *general type*. Faltings (1983) showed that the set $C(\mathbb{Q})$ is finite.

4 Arithmetic of surfaces

As we defined the above geometrical notions for nice curves and introduced invariants which uncover various properties of sets of rational points on curves, one can analogously extend this ideas to spaces of higher dimension, especially surfaces. We introduce now the notion of $K3$ surface (named after Kummer, Kahler and Kodaira) which shall be central to our restatement of the problem.

Definition 4.1. *A nice variety of dimension 2 such that it is simply connected, with a complex structure (transition maps being holomorphic) and has a holomorphic 2-form on it which vanishes nowhere is called a* ***K3 surface***

Examples of K3-surfaces in the $\mathbb{P}^3$ are as follows :

1. The smooth quartic $x^4 + y^4 + z^4 + w^4 = 0$
2. The surface defined by the equation[2] $S/\mathbb{Q} : x^4 + 2y^4 - z^4 - 4w^4 = 0$

An interesting fact is that it is not known whether the set $S(\mathbb{Q})$, the set of all rational points on the surface is not known to be finite or otherwise.

4.1 Local obstructions

Since the varieties $X/\mathbb{Q}$ we are investigating are projective, hence one can clear out the denominators of the rational coordinates of the defining equations of X, then one can recast the set of rational points $X(\mathbb{Q})$ to the set of integral points $X(\mathbb{Z})$. This allows us to use the machinery of solving equations by reducing to modulo p^n with exponent $n \geq 1$ and p being a prime.

To obtain a nontrivial set of inetgral solutions of a K3-surface X, the defining equations must have solutions modulo p^n for every prime p and exponent n. We define the notion of a local obstruction as a phenomenon when this fails.

Definition 4.2. *If the solution set of points modulo p^n (for some p and some n) for some variety X over $\mathbb{Q}$ is empty or if the solution set of the same is empty over $\mathbb{R}$ is empty then we say that there exists a* ***local obstruction*** *to the existence of rational points on X*

A basic example of a local obstruction is to consider the absence of a rational while proving that $\sqrt{2}$ is irrational. Consider the quadric variety defined by $x^2 - 2y^2 = 0$ in $\mathbb{P}^1$, it has no rational points on it, consequentially $\sqrt{2}$ is irrational, and that it has no nontrivial (x and y without any common factors) solutions modulo 2^2

[2] This notation denotes a variety over $\mathbb{Q}$

One has to consider an issue here, that for a given prime p and n one has finitely many solutions however there are infinitely many p (and n) to check for. So how does one check if there exists any local obstructions?. This problem is resolved by the usage of Hensel's lemma, the p-adic analogue of Newton Raphson method to determine solutions modulo p^n for all $n \geq 2$ which only leaves us finitely many primes to check for.

Note : By an example first brought up by Lindt and Reichardt (1940) which is the plane curve $3x^3 + 4y^3 + 5z^3 = 0$ of genus 1, one notes that it is not enough for a local obstruction to exist to ensure that the set of rational solutions $X(\mathbb{Q})$ is non empty for a given variety. In [[Alv01]] the author attempts to understand this phenomena by looking at the embedding map of a similar curve into the projective line, whose fibers are genus one curves that have local obstructions for different p and n dependent upon which fiber one is taking into consideration. Such a construction is known as a **Brauer Manin obstruction.**

5 The problem revisited

We return to Question 1.1 again, with the tools of arithmetic geometry at our disposal now. The sum of three cubes problem can be then recast as follows :

Proposition 5.1. *Define the projective $\mathbb{Q}$ surface embedded into $\mathbb{P}^3$*

$$X_n : x^3 + y^3 + z^3 - nw^3 = 0$$

Charcterize the set of integral points $X'_n(\mathbb{Z})$ on the affine patch $X'_n := X \cap \{w = 1\}$

One should note that since the set X'_n is itself not a projective variety but an affine patch the set of solutions of rational points $X'_n(\mathbb{Q})$ is not the same as $X'_n(\mathbb{Z})$, for example one has

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

such that $X'_n(\mathbb{Q})$ is nonempty for all $n \in \mathbb{Z}$ but, as we have seen before one $X'_n(\mathbb{Z}) = \emptyset$ whenever $n \not\equiv \pm 4$ or 9

References

[Alv01] Alvarado, A.V. (2021). *The Geometric disposition of Diophantine equations*. Vol. September 2021, *Notices of the American Mathematical Society*. `https://doi.org/10.1090/noti2335`