The geometry of Fermat-like equations

Anand Deopurkar

January 14, 2022

1 Introduction

We all know the famous theorem that for a given $n \geq 3$, the equation

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

has no non-zero integer solutions (x, y, z). What if we change the equation slightly to, say

$$2x^n + 3y^n = 5z^n,$$

or even to something like

$$Ax^p + By^q = Cz^r?$$

The answer remains almost the same. For any of these equations, there aren't many rational solutions.

Theorem 1.1 (Darmon and Granville)**.** *Fix positive integers p, q, r and non-zero integers A, B, C. Suppose*

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

Then the equation

$$Ax^p + By^q = Cz^r$$

has finitely many integral solutions (x, y, z) with $\gcd(x, y, z) = 1$.

In this talk, I will sketch the proof of this result. But more importantly, I will take this as an opportunity to explain how **geometry controls arithmetic**. More precisely, I will explain how the birational type of a variety (conjecturally) controls the arithmetic of rational points on the variety. These conjectures are due to Lang, Vojta, and Campana, and an excellent introduction to this topic is [1].

2 Geometry controls arithmetic: curves

Let X be a smooth, projective curve defined over $\mathbf{Q}$. What can we say about $X(\mathbf{Q})$, the set of rational points of X? Fundamentally, there are three cases.

Spherical X has genus 0. For example, when X is the curve in the projective plane $\mathbf{P}^2$ defined by the homogeneous equation

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

or equivalently, the affine equation

$$x^2 + y^2 = 1.$$

In this case, we know that there are infinitely many solutions.

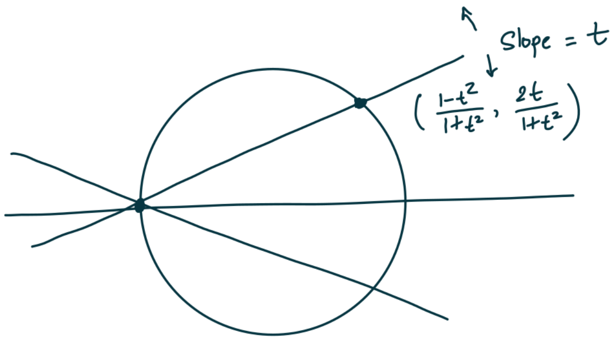

Figure 1: Rational parametrisation of $x^2 + y^2 = 1$

In fact, we can write all of them down using a rational parametrization of the curve by lines through a fixed point (see Figure 1).

The general story is not too far from this example. Either X has one rational point, in which case it is isomorphic to $\mathbf{P}^1$ over $\mathbf{Q}$, and so it has infinitely many of them. Or X has no rational points, but then it is isomorphic to $\mathbf{P}^1$ over a degree 2 extension $K/\mathbf{Q}$, and so it has infinitely many K-points. In either case, there exists a finite extension $K/\mathbf{Q}$ such that X has infinitely many K-points. We say that the rational points of X are *potentially* infinite. The word "potentially" in this context will almost always mean "after a finite extension of the base-field".

Elliptic X has genus 1.

> After a finite extension, we may assume that X has a point, and hence a group law, and furthermore, a point of infinite order. Then it has infinitely many points.

Thus, in this case also, the rational points of X are potentially infinite.

Hyperbolic X has genus at least 2.

> In this case, we have the famous theorem of Faltings that for any finite extension $K/\mathbf{Q}$, the set of K-points of X is finite. That is, X does not have (even potentially) an infinite set of rational points.

We summarize the three cases in a table. With an eye towards higher dimensional generalization, we phrase the trichotomy in terms of the positivity of the canonical bundle. We also note that an infinite set of points of a curve is the same as a Zariski dense set of points.

	deg K_X	Rational points
Spherical	Negative	Potentially dense
Elliptic	Zero	Potentially dense
Hyperbolic	Positive	Not potentially dense

3 Geometry controls arithmetic: higher dimensions

The conjectures of Bombieri, Lang, Vojta, and Campana extend the table above to varieties of higher dimension.

Higher dimensional "spherical" varieties are varieties that are rational (birational to projective space), or in some sense, close to being rational. These include varieties that are unirational (admit a dominant rational map from projective space), or Fano (have anti-ample canonical bundle), or rationally connected (a general pair of points can be connected by a rational curve). (The third class includes the first two by theorems of Campana and Kollàr–Miyaoka–Mori.) It is a conjecture of Campana that rationally connected varieties have potentially dense rational points.

Higher dimensional "hyperbolic" varieties are called varieties of general type. These are the varieties whose canonical bundle is positive (more precisely, "big"). It is a conjecture of Bombieri–Lang that varieties of general type do not have potentially dense rational points.

The intermediate cases are complicated. See the article [1] for more.

4 Back to Fermat-like equations

Let us focus on the specific task at hand, namely the rational points of X defined by

$$Ax^p + By^q = Cz^r.$$

Note that X is a surface, and the link between geometry and arithmetic is only proven for curves! But if we look more closely at X, we can see a way to cut down the dimension by 1.

The surface X has an action of the multiplicative group $\mathbf{G}_m$, given as follows:

$$t \cdot (x, y, z) = (t^{qr}x, t^{pr}y, t^{pq}z),$$

and we should obviously be looking at rational/integral points up to the equivalence defined by this action. Geometrically, we should be looking not at X itself but the quotient $X/\mathbf{G}_m$. Lets assume for simplicity that the exponents p, q, r are pairwise co-prime. Then the quotient is $\mathbf{P}^1$, with the quotient map given by

$$\begin{aligned} X &\to \mathbf{P}^1 \\ (x, y, z) &\mapsto (Ax^p, By^q, Cz^r); \end{aligned}$$

the image is the $\mathbf{P}^1 \subset \mathbf{P}^2$ cut out by $X + Y = Z$. But if the quotient is $\mathbf{P}^1$, then we should have infinitely many rational points, which contradicts Theorem 1.1. What is going on?

The answer is that the quotient $\mathbf{P}^1$ is not the right quotient. The $\mathbf{G}_m$ action on X is not free. There are three orbits that have non-trivial stabilisers: the orbit corresponding to $x = 0$ has stabilizer μ_p, the one corresponding to $y = 0$ has stabilizer μ_q, and the one corresponding to $z = 0$ has stabilizer μ_r. As a result, a more correct quotient is not $\mathbf{P}^1$, but an orbifold P whose coarse scheme is $\mathbf{P}^1$ but which has three points with stabilizer groups μ_p, μ_q, and μ_r. The degree of the canonical bundle of P is

$$\deg K_P = 1 - \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right).$$

When this degree is positive, P is hyperbolic, and then we should expect that it indeed has finitely many rational points.

But this is not a proof, just a heuristic. Darmon and Granville convert it into a proof by reducing it to Faltings' theorem [3]. Let us sketch the argument.

4.1 Proof of Theorem 1.1

Fix an isomorphism $V(X + Y - Z) \cong \mathbf{P}^1$ given the rational function $t = X/Z$. Then the points $[0 : 1 : 1]$, $[1 : 0 : 1]$, and $[1 : -1 : 0]$ are identified with $0, 1$, and ∞.

Let $Y \to \mathbf{P}^1$ be a branched cover of Riemann surfaces unramified away from $0, 1, \infty$ and whose monodromy around 0 is a product of p-cycles, around 1 is a product of q-cycles, and around ∞ is a product of r-cycles (see Figure 2). It is not completely obvious that such a cover exists. One way to demonstrate that it does is by solving the equation $\alpha\beta = \gamma$ in a symmetric group, where α is a product of p-cycles, β is a product of q-cycles, and γ a product of r-cycles. Another way is by constructing a suitable subgroup G of the modular group and taking Y to be the quotient of the upper half plane by this group.

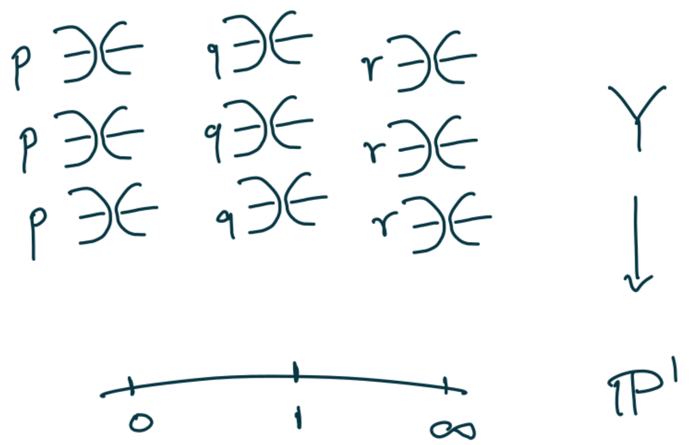

Figure 2: A cover $Y \to \mathbf{P}^1$ with peculiar ramification

By the Riemann–Hurwitz formula, we see that the genus of Y is at least 2. We should think of Y as a "schematic approximation" of the orbifold P.

By Belyi's theorem, the cover $\pi\colon Y \to \mathbf{P}^1$ is defined over a number field K. The following proposition shows that, modulo a finite extension, the points on $\mathbf{P}^1 = X/\mathbf{G}_m$ coming from a rational point on X correspond to rational points of Y.

Proposition 4.1. *There is a finite extension L/K such that the following holds. For every point integer point (x, y, z) with $\gcd(x, y, z) = 1$ satisfying $Ax^p + By^q = Cz^r$, consider the point $t = Ax^p/Cz^r \in \mathbf{P}^1(K)$. Then the points of $\pi^{-1}(t) \subset Y$ are L-points of Y.*

Proof. Let s be a point of $\pi^{-1}(t) \subset Y$, and let F be its residue field. Let us analyze the set of primes of O_K where F/K is ramified.

To do so, we first spread out $Y_K \to \mathbf{P}^1_K$ to $Y_{O_K} \to \mathbf{P}^1_{O_K}$, where $O_K \subset K$ is the ring of integers. After passing to an open subset $U \subset \operatorname{Spec} O_K$, we may assume that $Y_U \to U$ is smooth and the map $Y_U \to \mathbf{P}^1_U$ is finite and unramified away from the sections $0, 1, \infty$. By shrinking U further, let us also assume that the residue characterists of points of U are bigger than the degree of $Y \to \mathbf{P}^1$. Let us also assume that that ABC does not vanish at any point of U.

The point $t \in \mathbf{P}^1(K)$ extends to a U-point T of $\mathbf{P}^1_U$. Let $V = O_F \times_{O_K} U$. Then the point $s \in Y(F)$ extends to a V-point S of Y_U, and S lies over T. Since $Y_U \to \mathbf{P}^1_U$ is finite and V is normal, we get that V is the normalisation of a component of the pre-image of T in Y_U, namely the fibered product

$$T \times_{\mathbf{P}^1_U} Y_U.$$

What can we say about the ramification of $V \to U$? (See Figure 3 for a picture of the analysis that follows.) Let $u \in U$ be such that $T(u)$ is disjoint from $0, 1, \infty$. Since $Y_U \to \mathbf{P}^1_U$ is unramified away from $0, 1, \infty$, the map $V \to U$ is also unramified over u. Let $u \in U$ be such that $T(u)$ intersects the 0 section. Then x vanishes at u (recall: A does not vanish anywhere on U). Then the order of contact of T with 0 is a multiple of p. Since the ramification of Y over 0 consists of purely of p-cycles, we can show that $V \to U$ is actually unramified over u. (The analogous statement over the complex numbers is easy to see using topology; it requires a bit of an argument if we want to do it purely algebraically.) By a similar analysis when T intersects 1 or ∞, we conclude that the only possible points of ramification of $V \to U$ are u at which A or B or C vanishes. Recall that $U \subset \operatorname{Spec} O_K$ is an open subset; call the complement D. Then the primes of O_K over which F/K is ramified are contained in the finite set D. By a classical theorem of Hermite and Minkowski, there are finitely many extensions of a number field of bounded degree

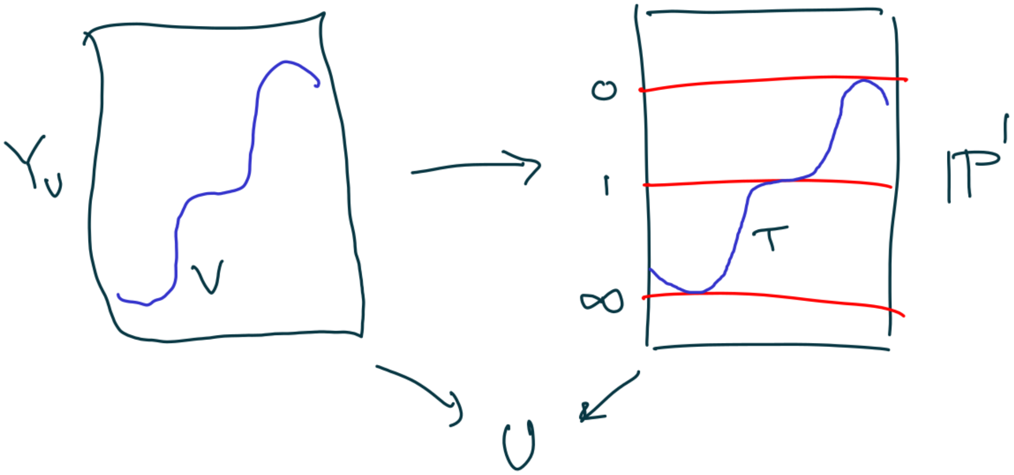

Figure 3: The map $V \to U$ is unramified at most points of U.

whose ramification is contained in a given finite set. Hence, there are only finitely many posibilities for the extension F/K. We take L/K to be the compositum. □

We can now finish the proof of Theorem 1.1. By the theorem of Faltings, the set of L-points of Y is finite. We conclude that primitive integral points on X are also finite, which is the assertion in Theorem 1.1.

Remark 4.2. In the proof above, we made a crude analysis of the ramification of the field of definition of a Belyi cover $Y \to \mathbf{P}^1$. A theorem of Sybilla Beckmann gives a much more precise description [2].

5 Uniform boundedness

The conjecture of Bombieri–Lang has strong implications not only for individual varieties, but also their families. The most spectacular consequence of this is the following theorem.

Theorem 5.1 (Caporaso, Harris, Mazur)**.** *Assume the Bombieri–Lang conjecture. Let K be a number field and $g \geq 2$ a positive integer. Then there exists a constant $N = N(K, g)$ such that for any smooth curve X of genus g defined over K, the number of K-rational points on X is at most N.*

The idea of the proof is a beautiful application of geometry to arithmetic. Let $X \to B$ be a family of smooth projective curves of genus g defined over K. For every $b \in B(K)$, we know that the fiber X_b has finitely many K-points. But how do these points behave as we vary b? Is there any kind of relationship between the K-rational points of X_b for various b?

Caporaso, Harris, and Mazur prove that the answer is yes (assuming Bombieri–Lang). The prove that for some n, the n-fold fibered product X_B^n dominates a variety of general type. Therefore, if Bombieri–Lang is true, then all the K-rational points of X_B^n are contained in a Zariski closed subset $Z \subset X_B^n$. That is, there are algebraic relations between n-tuples of rational points. From this, a clever Noetherian induction yields a uniform bound on the number of rational points of X_b. To conclude the full theorem, we take $X \to B$ to be a suitable universal family.

References

[1] D. Abramovich. Birational geometry for number theorists. In *Arithmetic geometry. Clay Mathematics Institute Summer School Arithmetic Geometry, Göttingen, Germany, July 17–August 11, 2006*, pages

335–373. Providence, RI: American Mathematical Society (AMS); Cambridge, MA: Clay Mathematics Institute, 2009. ISBN 978-0-8218-4476-2.

[2] S. Beckmann. Ramified primes in the field of moduli of branched coverings of curves. *J. Algebra*, 125 (1):236–255, 1989. ISSN 0021-8693. doi: 10.1016/0021-8693(89)90303-7.

[3] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995. ISSN 0024-6093. doi: 10.1112/blms/27.6.513.