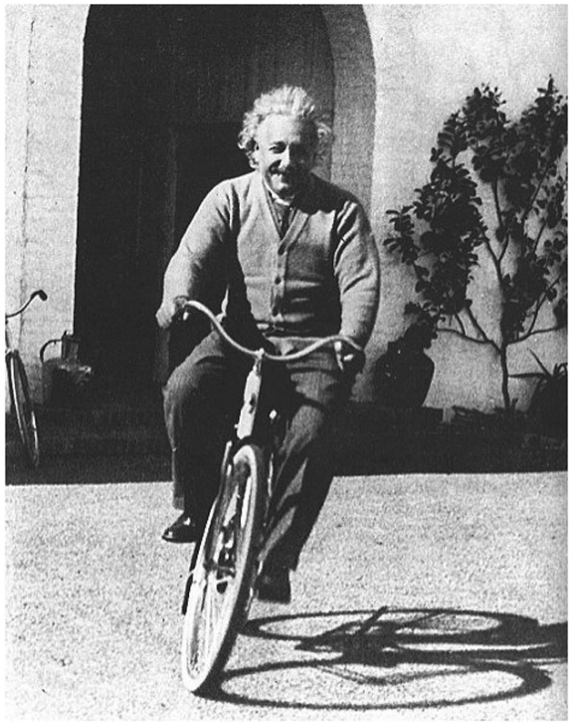
On the Arithmetic of Curves

Barry Mazur, Harvard University

The AMS Einstein Public Lecture in Mathematics, Univ. of Hawaii, March 2019

Do not worry about your problems with mathematics. I assure you mine are far greater.

Albert Einstein



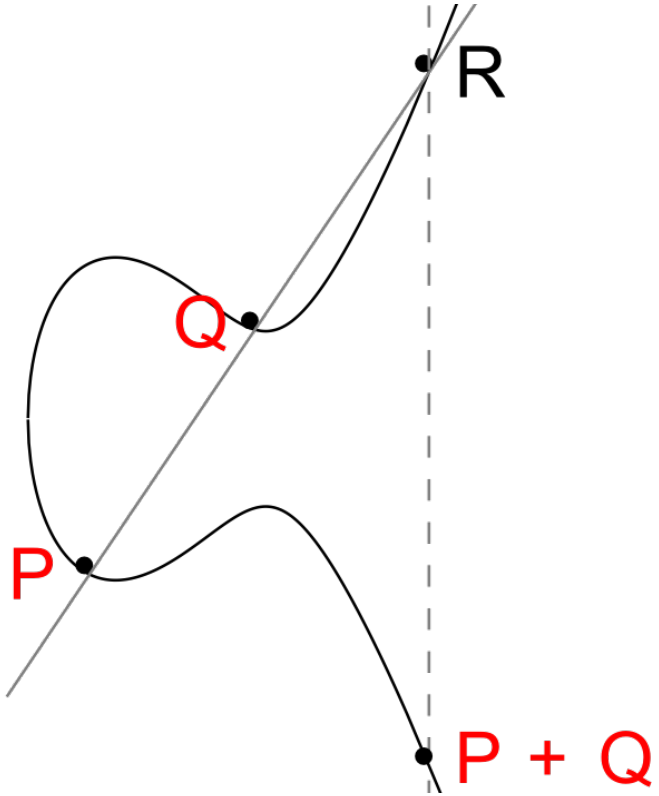
Abstract

We are constantly discovering new ways of understanding algebraic curves and their arithmetic properties.

Questions about 'rational points'—the interplay of arithmetic and algebra—have fascinated mathematicians from Diophantus to the present.

I will give a survey of current approaches, results, and conjectures in this vibrant subject.

A cubic curve



A query

Suppose that you have three different and possibly even *incomparable* ways of proving that a certain set S is finite. And you find yourself wondering: *why is S finite?*

A query

Suppose that you have three different and possibly even *incomparable* ways of proving that a certain set S is finite. And you find yourself wondering: *why is S finite?*

You then have three different—incomparable—answers to that question. A natural query: is there some way to unify these three different answers to that question?

A query

Suppose that you have three different and possibly even *incomparable* ways of proving that a certain set S is finite. And you find yourself wondering: *why is S finite?*

You then have three different—incomparable—answers to that question. A natural query: is there some way to unify these three different answers to that question?

This thought might arise later in this lecture—in a situation where—at present— I can't imagine any road to such a unification.

Mathematics aims to *explain* and often asks

What-questions and How-questions

Mathematics aims to *explain* and often asks

What-questions and How-questions

But lurking behind them is some (perhaps ridiculously naive) 'wondering':—a *sort-of-question* that may not have any serious answer:

Why is X true?

So it is amusing (and baffling) if one has three different incommensurate explanations of the same phenomenon. . .

Square roots for the ancients

There was something of a fascination for 'square roots' (aka: *sides*) as in this well-publicized *Problem VI.17* of (the third Arabic book of) Diophantus, this dating from the 3-rd century AD:

> *Find three squares which when added give a square, and such that the first one is the side (i.e., the square-root) of the second, and the second is the side of the third.*

Diophantus and us

$$X^2 \overset{\text{side of}}{+} \rightarrow X^4 \overset{\text{side of}}{+} \rightarrow X^8 \quad = \quad \text{A Square.}$$

or, as we might simplify (*divide by* X^2):

$$y^2 = x^6 + x^2 + 1$$

Diophantus himself offers a solution:

$$\boxed{X = \frac{1}{2}}$$

$$(\frac{1}{2})^2 + (\frac{1}{2})^4 + (\frac{1}{2})^8 = \frac{64+16+1}{256} = (\frac{9}{16})^2$$

along with a hint about how he arrived at it:

The hint:

He noticed that the square of $a + \frac{1}{2}$ is

$$a^2 + a + (\frac{1}{2})^2,$$

so if you take a to be $(\frac{1}{2})^4$, you win:

$$\boxed{\left((\tfrac{1}{2})^4\right)^2 + (\tfrac{1}{2})^4 + (\tfrac{1}{2})^2 = \left((\tfrac{1}{2})^4 + \tfrac{1}{2}\right)^2.}$$

All solutions?

Of course, what Diophantus *won* was this single solution. A more modern turn on such problems is often to quantify goals more precisely. Eg., *find* **all** *solutions (of the above problem) in positive rational numbers.*

This was achieved a mere 17 centuries later.

Diophantus's solution is the only solution in positive rational numbers

That is:

The *only* positive x-coordinate of a rational point in the curve

$$C : y^2 = x^6 + x^2 + 1$$

is:

$$x = \frac{1}{2}$$

(Joseph L. Wetherell's 1998 Berkeley thesis: "Bounding the number of rational points on certain curves of high rank.")

That such cross-century conversations can be fruitful, and coherent,

attests to some stability regarding our subject —our common language—and shared

modes of expression, and modes of operation.

Why study rational points (on curves)?

"agriculture" $- - - \rightarrow$ the practical, i.e., food—

"horticulture" $- - - \rightarrow$ the beautiful i.e., gardens, flowers—

. . . the study of rational points contributes to both agriculture and horticulture for mathematics.

As for it being ‘practical’:

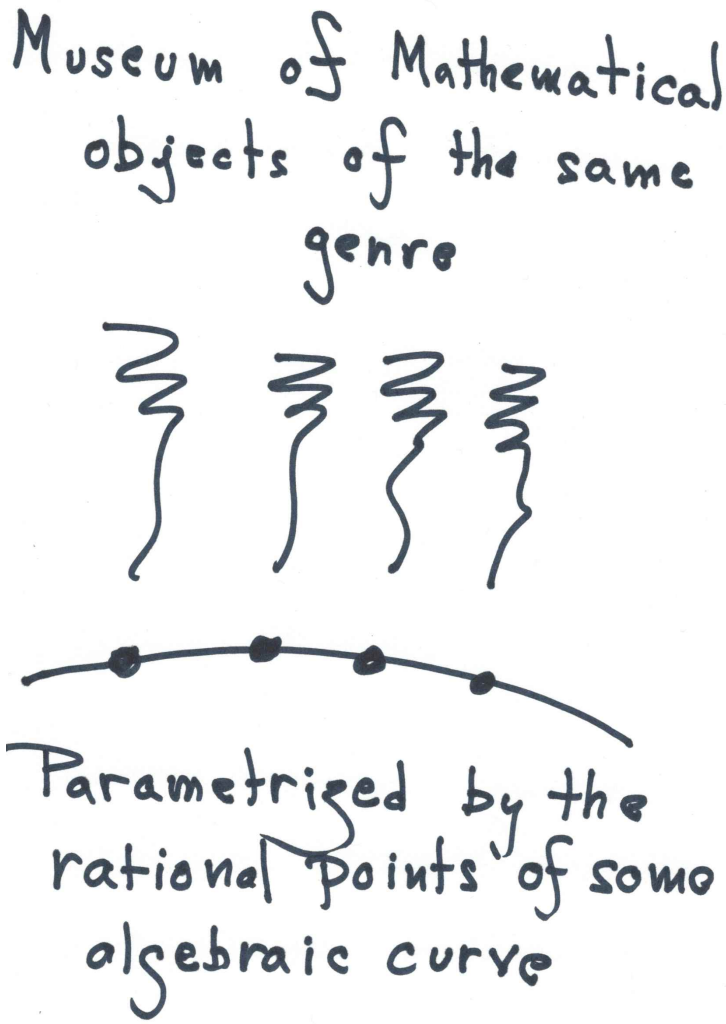
Sometimes an algebraic curve (or more generally a variety) presents itself as a sort of ‘museum" for some specific genre of mathematical object—

As for it being ‘practical’:

Sometimes an algebraic curve (or more generally a variety) presents itself as a sort of ‘museum" for some specific genre of mathematical object—

so that every point on the curve (or variety) represents a particular mathematical object of that genre, and as one moves from point to point on the curve one samples all the different members of that genre.

Moduli!


Museum of Mathematical objects of the same genre
Parametrized by the rational points of some algebraic curve

Moduli!

And if the point on the curve is rational over some field,—say $\mathbb{Q}$— the corresponding mathematical object is 'defined over that field.'

Such a curve (or variety) is then said to represent the *modular curve* (or *variety of moduli*) for that genre.

Moduli!

And if the point on the curve is rational over some field,—say $\mathbb{Q}$— the corresponding mathematical object is 'defined over that field.'

Such a curve (or variety) is then said to represent the *modular curve* (or *variety of moduli*) for that genre.

To find, then, *all the mathematical objects of that genre that can be defined over a given field* K—you are led to the problem of finding all K-rational points on the corresponding *modular curve* (or *variety of moduli*).

Moduli!

And if the point on the curve is rational over some field,—say $\mathbb{Q}$— the corresponding mathematical object is 'defined over that field.'

Such a curve (or variety) is then said to represent the *modular curve* (or *variety of moduli*) for that genre.

To find, then, *all the mathematical objects of that genre that can be defined over a given field* K—you are led to the problem of finding all K-rational points on the corresponding *modular curve* (or *variety of moduli*).

This is a *basic tool* for determining and classifying objects of interest.

Pythagoras

The (projective) plane curve

$$x^2 + y^2 = z^2, \tag{1}$$

has been in our sights from the earliest days since this curve is:

the moduli space of similarity classes of right-angle triangles.

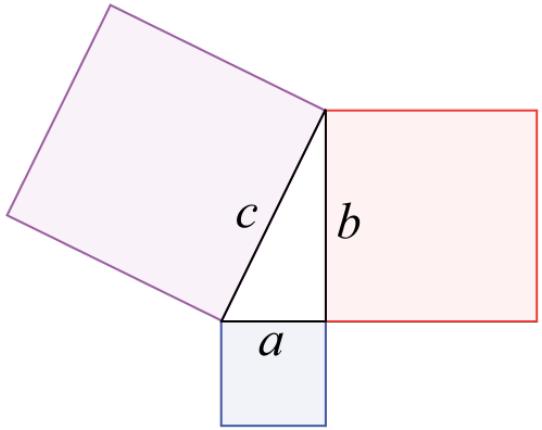
(what an obscure way of acknowledging the Pythagorean Theorem!):

Pythagoras

$$\{\text{Triples of positive integers } (a,b,c) \text{ such that } a^2+b^2=c^2\}$$

$$\leftrightarrow$$

$$\text{right}-\text{angle triangles with integral length sides :}$$



The ‘moduli space’ of right-angle triangles

The positive rational solutions correspond to isomorphism classes of right-angle triangles with rational length sides,

The ‘moduli space’ of right-angle triangles

The positive rational solutions correspond to isomorphism classes of right-angle triangles with rational length sides,

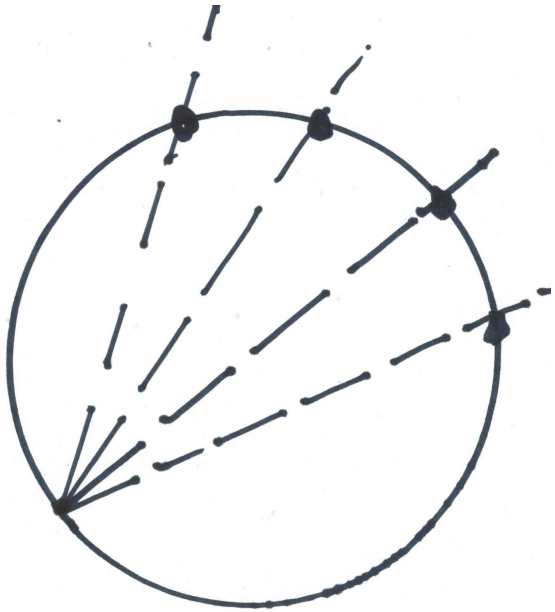
and there is even a one-one rational parametrization of those solutions

(neatly effected by the ‘sweeping method’; i.e., considering a fan of straight lines (with rational coordinates) that meet this curve at one rational point, and

—since the curve is of degree two—

meets the curve at exactly *one* other point—that is, therefore, also rational).

The 'sweeping method'



(10th century) Congruent number problem as a 'moduli problem'

To dig a bit more into the 'moduli space' of right-angle triangles with sides (a, b, c), let's fix the area of such a triangle:

$$A := ab/2$$

and consider the family of right-angle triangles with that (fixed) area A.

(10th century) Congruent number problem as a 'moduli problem'

To dig a bit more into the 'moduli space' of right-angle triangles with sides (a, b, c), let's fix the area of such a triangle:

$$A := ab/2$$

and consider the family of right-angle triangles with that (fixed) area A.

Define new parameters X and Y by:

(10th century) Congruent number problem as a 'moduli problem'

To dig a bit more into the 'moduli space' of right-angle triangles with sides (a, b, c), let's fix the area of such a triangle:

$$A := ab/2$$

and consider the family of right-angle triangles with that (fixed) area A.

Define new parameters X and Y by:

$$X := Ab/(c-a), \quad \text{and} \quad Y := 2A^2/(c-a)$$

and noting that one can get (a, b, c) back from the knowledge of X and Y (and A):

$$a = (X^2 - A^2)/Y, \quad b = 2AX/Y, \quad c = (X^2 + A^2)/Y,$$

and that...

The 'modular curve' of right-angle triangles with area equal to A

the relation between X and Y is given by the plane curve

$$\boxed{Y^2 = X^3 - A^2X.}$$

we see that:

right-angle triangles with area A are parametrized by this curve.

Congruent Numbers

A positive integer A is called a **congruence number** if it is the area of a right-angle triangle with rational sides (a, b, c). So, from the above discussion, it is the area of such a triangle if

$$\boxed{Y^2 = X^3 - A^2X}$$

has a solution $(X, Y) = (u, v)$ where u and v are positive rational numbers.

Congruent Numbers

A positive integer A is called a **congruence number** if it is the area of a right-angle triangle with rational sides (a, b, c). So, from the above discussion, it is the area of such a triangle if

$$\boxed{Y^2 = X^3 - A^2X}$$

has a solution $(X, Y) = (u, v)$ where u and v are positive rational numbers.

(**AND:** it turns out that if there's one such solution for a given A there are infinitely many—i.e., if there is one right-angle triangle with rational sides of a given area A there are infinitely many with the same area A.)

The three types of algebraic curves just discussed:

- the 'Pythagorean' curve:

$$\boxed{x^2 + y^2 = z^2}$$

- the curves connected to the 10th century Congruence Number Problem:

$$\boxed{Y^2 = X^3 - A^2X}$$

  and

- the curve related to Diophantus's problem:

$$\boxed{y^2 = x^6 + x^2 + 1}$$

are members of the most basic trichotomy of algebraic curves (respectively): curves of genus 0, genus 1, and genus > 1.

Genus

The **genus** of an algebraic curve is the fundamental geometric numerical invariant of a (smooth complete) algebraic curve. It depends only on the topological surface defined by the complex points of the curve and counts the number of 'holes' in this topological surface. The trichotomy distinguishes these three different class of curves:

- Genus 0: *topologically a two-dimensional sphere*
- Genus 1: *topologically a torus*
- Genus > 1: *topologically a 'many-holed' torus*

The arithmetic of these three types of curves differs substantially:

Genus 0

An application of the Riemann-Roch Theorem gives that:

Any smooth projective curve of genus zero over a field can be expressed as a conic, and so the 'sweeping method' gives us that if such a curve has one point rational over a field K it has a fan of points parameterized by $\mathbf{P}^1(K)$.

And curves of genus 0 also have the extraordinarily useful *local-to-global property*

(also called the *"Hasse property"*):

If a curve of genus zero over the field of rational numbers $\mathbb{Q}$

has a real point and a p-adic point for all primes p,

then it has a $\mathbb{Q}$-rational point.

"locally soluble" $\leftrightarrow$ "globally soluble"

Curves of genus 1

The arithmetic of these curves is much subtler than curves of genus 0. First, there is the local-to-global issue:

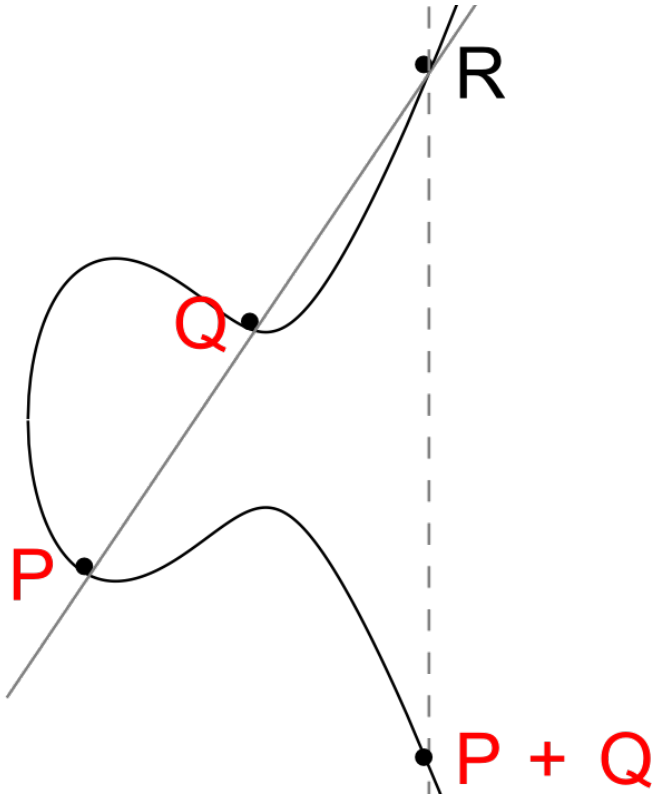
A projective curve of genus 1 over $\mathbb{Q}$ known personally to many number theorists is

$$E : 3x^3 + 4y^3 + 5z^3 = 0.$$

It was the curve shown in 1951 by E. Selmer to have p-adic points for all p (and over $\mathbf{R}$) but no $\mathbb{Q}$-rational points—i.e., it does not have the *local-to-global property*.

Elliptic curves.

But once a curve E of genus 1 over any field K has a K-rational point—taking that point to be the origin—there is a canonical structure of a (commutative) algebraic group on E . . . as in the figure shown at the beginning of this lecture:



Mordell-Weil groups

Given this structure, E is called an **elliptic curve**. The *set* $E(K)$ of K-rational points of an elliptic curve (or of any commutative algebra group) inherits a (canonical) structure of an abelian group.

Mordell-Weil groups

Given this structure, E is called an **elliptic curve**. The *set* $E(K)$ of K-rational points of an elliptic curve (or of any commutative algebra group) inherits a (canonical) structure of an abelian group.

The group $E(K)$ is called the Mordell-Weil group of E over K in honor of the classical theorem of Mordell (the theorem was extended by Weil to apply to all abelian varieties) that guarantees that these Mordell-Weil groups are finitely generated.

Mordell-Weil groups

Given this structure, E is called an **elliptic curve**. The *set* $E(K)$ of K-rational points of an elliptic curve (or of any commutative algebra group) inherits a (canonical) structure of an abelian group.

The group $E(K)$ is called the Mordell-Weil group of E over K in honor of the classical theorem of Mordell (the theorem was extended by Weil to apply to all abelian varieties) that guarantees that these Mordell-Weil groups are finitely generated.

The range of questions related to Mordell-Weil is vast, and we're only at the beginning of an unfolding story.

Curves of genus > 1

Although there is the well-known and dramatic 'pre-history' of this subject dealing with the plane curves

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

related to afterthoughts of Pierre de Fermat on thinking about the Pythagorean curve, the general question of considering the arithmetic of *all* curves of genus > 1 began in 1922, with Mordell's Conjecture, nowadays framed over any number field.

Mordell's Conjecture

Conjecture

(Mordell 1922) A curve X over a number field K of genus > 1 has only finitely many K-rational points.

This conjecture was proved about a half century later by Gerd Faltings.

Mordell's Conjecture

Conjecture

(Mordell 1922) A curve X over a number field K of genus > 1 has only finitely many K-rational points.

This conjecture was proved about a half century later by Gerd Faltings.

So, Diophantus's curve (which is of genus 2) has only finitely many $\mathbb{Q}$-rational points.

The scarcity of rational points

It was the mathematician Serge Lang's firm belief that on the whole, algebraic varieties over K tend not to have all that many K-rational points unless there is something structural, such as a group structure that forces it.

.

> *Is it true that a variety V over K possesses infinitely many K-rational points if and only if there exists a connected algebraic group G over K possessing infinitely many K-rational points and a nonconstant mapping*
>
> $$G \to V$$
>
> *defined over K?*

This is true for curves!

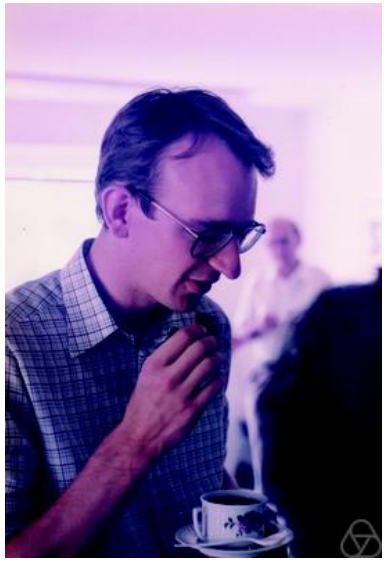
Curves of genus > 1 have finitely many rational points

We'll discuss three essentially different arguments establishing finiteness of $X(K)$ for curves X defined over K and of genus > 1: the methods of:

(1) Faltings, **(2)** Vojta, and **(3)** Chabauty-Coleman-Kim,

the last of these methods working (at present) only under further hypotheses. My aim is not to give an exposition of them—but rather to invoke enough of their nature so that we can appreciate how thoroughly incomparable they are! Here, again, is the above list:

Curves of genus > 1 have finitely many rational points



- Gerd Faltings (1983)—

  his method applies generally, and was the first **full proof** *of Mordell's Conjecture.*

Curves of genus > 1 have finitely many rational points

- Paul Vojta—

  his method also applies generally—later elaborations and some simplifications by Faltings, Bombieri, McQuillan.

Chabauty-Coleman-Kim

- Claude Chabauty (1941)— *his method works under the restricted hypothesis that the genus is greater than the Mordell-Weil rank of the jacobian of* X.

Sharpened later

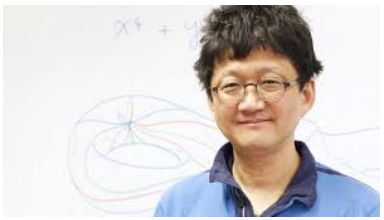
And led to a (semi-) effective theorem by ideas of

- Robert Coleman.

And more recently made even more powerful

by ideas of

- Minhyong Kim—



who extends the ideas of Chabauty and Coleman to deal with a range of examples that do not satisfy the restricted hypotheses required by Chabauty.

Chabauty-Coleman-Kim

This method is currently being used (and augmented) by many people who are finding all the rational points on some challenging, and important, curves.

People including: Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, Jan Vonk, and others.

Brian Lawrence and Akshay Venkatesh

In their very recent work:

Diophantine problems and p-adic period mappings

we see a proof of Mordell's Conjecture, that (excitingly) has the flavor of Faltings' approach but also has the spirit of Chabauty-Coleman-Kim!

Various types of finiteness

When you claim the set $X(K)$ of K-rational points on a curve is finite, you might mean, for example, that you have proved that:

1. there is an explicit constructed upper bound on the *heights* of rational points, or perhaps that:

2. there is an explicit constructed upper bound on the *number* of rational points.

Consequence of bounding the heights of rational points

In this case it is possible that you've set the stage for actually finding the full set of rational points. That is, if your bound isn't too high, you could systematically test—e.g., by computer—all points of K of height $\leq$ your bound to see if they yield points on the curve.

Consequence of bounding the heights of rational points

In this case it is possible that you've set the stage for actually finding the full set of rational points. That is, if your bound isn't too high, you could systematically test—e.g., by computer—all points of K of height $\leq$ your bound to see if they yield points on the curve.

Among other things, your bound might also allow you to compute an a priori finite estimate for the amount of computer time it would take to resolve the issue.

Consequence of bounding the number of rational points

The best would be if your upper bound were the actual number of rational solutions.

Consequence of bounding the number of rational points

The best would be if your upper bound were the actual number of rational solutions.

So, as you search systematically (e.g., in rising heights) looking for rational solutions if you find as many solutions as your bound, you know you're done.

Consequence of bounding the number of rational points

The best would be if your upper bound were the actual number of rational solutions.

So, as you search systematically (e.g., in rising heights) looking for rational solutions if you find as many solutions as your bound, you know you're done.

But you won't know before this event happens that it would happen, nor would you have an a priori time estimate for when such a thing might happen.

Consequence of bounding the number of rational points

The best would be if your upper bound were the actual number of rational solutions.

So, as you search systematically (e.g., in rising heights) looking for rational solutions if you find as many solutions as your bound, you know you're done.

But you won't know before this event happens that it would happen, nor would you have an a priori time estimate for when such a thing might happen.

In many set-ups where one has an upper bound for the number of rational points, the upper bound is far greater than the actual number of points, so even if you've got all the rational points, you may never know it.

An Algorithm?

All the proofs that we know are of the second type: they bound the *number* but not the *height* of K-rational points on X, leaving us with the fundamental question:

Questions

Does there actually exist an algorithm such that for

Input:=*any curve* X, *of genus* > 1 *over* K,

it provides

Output:=*an upper bound* $B(X; K)$
for the heights of the points in $X(K)$*?*

How *different* are the different proofs of finiteness of the number of rational points of curves of genus > 1?

They all prove finiteness of number of rational points, but they seem to get to finiteness in strikingly different ways.

Is there some way of fitting these different approaches into one coherent picture?

The method of Faltings. . .

establishes finiteness of rational points on curves of genus > 1 as a consequence of finiteness of quite a different species of mathematical object—namely:

The method of Faltings. . .

establishes finiteness of rational points on curves of genus > 1 as a consequence of finiteness of quite a different species of mathematical object—namely:

finiteness of the number of isomorphism classes of abelian varieties with good reduction outside a finite set of primes, and of bounded polarization degree.

The method of Faltings. . .

So, this finiteness deduction is very *indirect* and depends–at the very least—on the quantity of such isomorphism classes. Although the bound obtained on the number of rational points is effective, this bound—in practice—is surely enormous; I wonder whether anyone has worked it out explicitly in any nontrivial example.

Comment on:

Roses in the garden $<$ Flowers in the garden $<$ ∞

The method of Vojta. . .

is guided by *analogies* that relate finiteness of rational points to problems in quite different arenas of mathematics:

- *hyperbolic geometry* and
- *approximation of algebraic numbers by rational numbers*.

The method of Vojta. . .

is guided by *analogies* that relate finiteness of rational points to problems in quite different arenas of mathematics:

- *hyperbolic geometry* and
- *approximation of algebraic numbers by rational numbers*.

Vojta's strategy takes off by *banding together a large collection of rational points* to get a point $(P_1, P_2, \ldots, P_m) \in X^m$ (for large enough m where the P_i are rational points of X whose heights are appropriately growing humungously . . .) to get a contradiction.

It is reminiscent of the shape of the proof of the classical Roth's Theorem.

Roth

Roth's Theorem guarantees that for a given algebraic irrational (real) number α, and for any $\epsilon > 0$, there are only finitely many rational numbers p/q that approximate α as closely as:

$$\boxed{|\alpha - p/q| < \frac{1}{q^{2+\epsilon}}.}$$

Roth

Roth's strategy is to suppose there are infinitely many such good approximants and to combine enough of them to make one vector

$$v := (p_1/q_1, p_2/q_2, \ldots, p_m/q_m) \in \mathbb{R}^m,$$

with m enormous, which is a pretty good approximation to the diagonal m-tuple

$$u := (\alpha, \alpha, \ldots, \alpha) \in \mathbb{R}^m.$$

Roth

Roth's strategy is to suppose there are infinitely many such good approximants and to combine enough of them to make one vector

$$v := (p_1/q_1, p_2/q_2, \ldots, p_m/q_m) \in \mathbb{R}^m,$$

with m enormous, which is a pretty good approximation to the diagonal m-tuple

$$u := (\alpha, \alpha, \ldots, \alpha) \in \mathbb{R}^m.$$

—And then to get a contradiction by assiduously engineering polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_m]$ that vanish (to 'high degree') on $u = (\alpha, \alpha, \ldots, \alpha)$ but don't vanish on $v = (p_1/q_1, p_2/q_2, \ldots, p_m/q_m)$.

Roth

Roth's strategy is to suppose there are infinitely many such good approximants and to combine enough of them to make one vector

$$v := (p_1/q_1, p_2/q_2, \ldots, p_m/q_m) \in \mathbb{R}^m,$$

with m enormous, which is a pretty good approximation to the diagonal m-tuple

$$u := (\alpha, \alpha, \ldots, \alpha) \in \mathbb{R}^m.$$

—And then to get a contradiction by assiduously engineering polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_m]$ that vanish (to 'high degree') on $u = (\alpha, \alpha, \ldots, \alpha)$ but don't vanish on $v = (p_1/q_1, p_2/q_2, \ldots, p_m/q_m)$.

Since such a polynomial $f(x_1, x_2, \ldots, x_m)$ has coefficients in $\mathbb{Z}$ and v is rational, and $f(v) \neq 0$, it follows that $|f(v)|$ has a clear lower bound.

Since $f(u) = 0$, and v approximates u, you get a contradiction.

Chabauty, Coleman, Kim

Here is a way of thinking about how the method of Chabauty as extended by Coleman, Kim and others offers finiteness of number—when it applies.

Chabauty, Coleman, Kim

Here is a way of thinking about how the method of Chabauty as extended by Coleman, Kim and others offers finiteness of number—when it applies.

Imagine if for a given curve X (of genus > 1 over a number field K) you had an algorithm that produces a nontrivial meromorphic function $\phi(x)$ on the complex analytic Riemann surface $X(\mathbb{C})$ such that ϕ vanishes on all K-rational points of X.

Chabauty, Coleman, Kim

Here is a way of thinking about how the method of Chabauty as extended by Coleman, Kim and others offers finiteness of number—when it applies.

Imagine if for a given curve X (of genus > 1 over a number field K) you had an algorithm that produces a nontrivial meromorphic function $\phi(x)$ on the complex analytic Riemann surface $X(\mathbb{C})$ such that ϕ vanishes on all K-rational points of X.

Since ϕ has only finitely many zeroes, your algorithm would have shown finiteness of rational points.

A scenario

Moreover, imagine that ϕ is algorithmically explicit in that in finite time the algorithm exhibits any finite number of Taylor series coefficients (at some specific point) that is desired.

A scenario

Moreover, imagine that ϕ is algorithmically explicit in that in finite time the algorithm exhibits any finite number of Taylor series coefficients (at some specific point) that is desired.

In such a scenario, beyond a proof of MERE finiteness you would have lots more information as well!

A scenario

Moreover, imagine that ϕ is algorithmically explicit in that in finite time the algorithm exhibits any finite number of Taylor series coefficients (at some specific point) that is desired.

In such a scenario, beyond a proof of MERE finiteness you would have lots more information as well!

You have an upper bound—not only on the number—but on the possible *locales* of the rational points.

But. . .

There is no known finiteness proof of rational points of a curve of genus > 1 that follows exactly the above scenario,

But. . .

There is no known finiteness proof of rational points of a curve of genus > 1 that follows exactly the above scenario,

but if you replace the complex numbers $\mathbb{C}$ by:

- appropriate p-adic completions K_v of the number field K,

  and replace the requirement that ϕ be meromorphic on $X(\mathbb{C})$ by:

- the requirement that ϕ be a locally ('p-adic") analytic function on the ('p-adic') analytic curve $X(K_v)$ —ϕ being given by a power series on every residual disc—

But. . .

There is no known finiteness proof of rational points of a curve of genus > 1 that follows exactly the above scenario,

but if you replace the complex numbers $\mathbb{C}$ by:

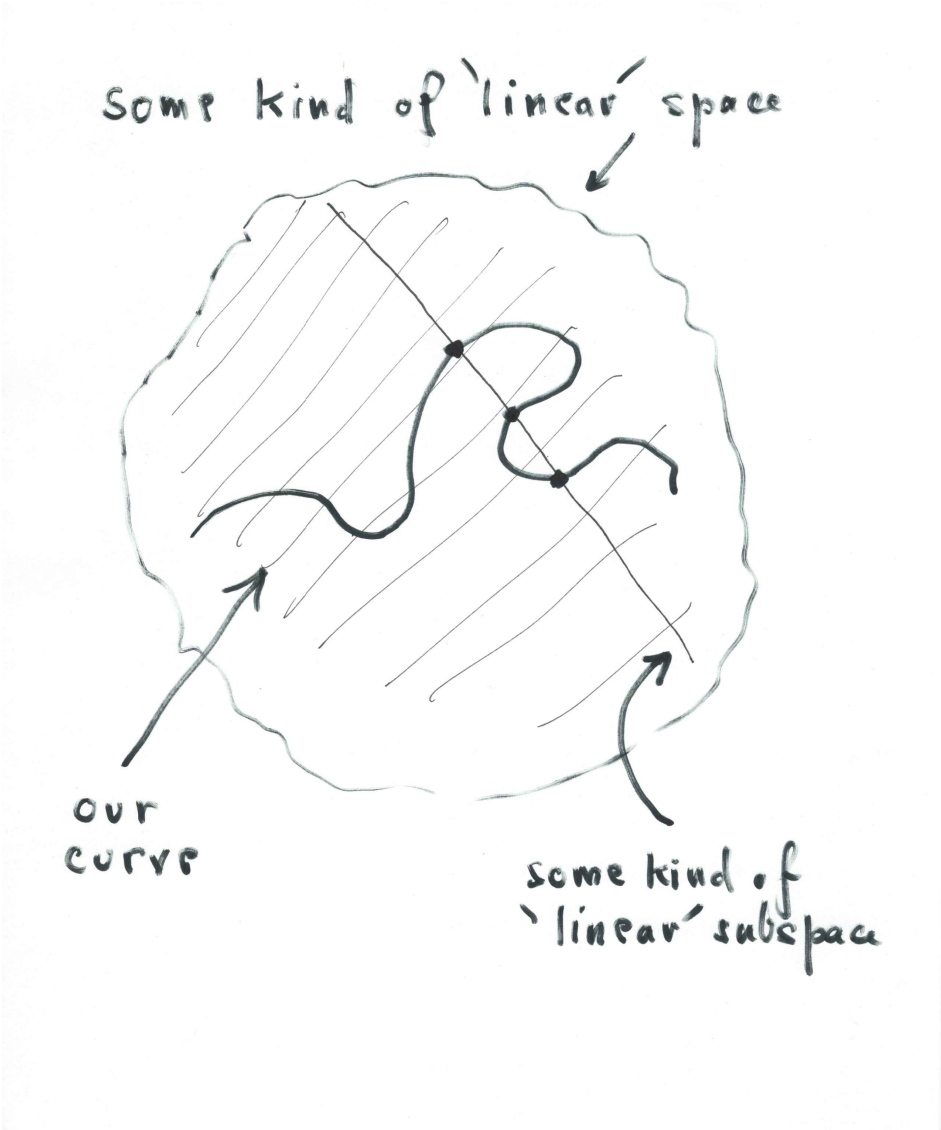
- appropriate p-adic completions K_v of the number field K,

  and replace the requirement that ϕ be meromorphic on $X(\mathbb{C})$ by:

- the requirement that ϕ be a locally ('p-adic") analytic function on the ('p-adic') analytic curve $X(K_v)$ —ϕ being given by a power series on every residual disc—

then the method of Chabauty enhanced by Coleman, by Kim and others—*but only, of course, when it applies!*— proves finiteness by offering such a function!

A cartoon that gives (the barest) hint of how the method of Chabauty and its recent extensions work



Diophantus

Returning to Diophantus's problem and the curve:

$$X: \quad y^2 = x^6 + x^2 + 1,$$

this curve has Mordell-Weil rank = genus = 2, so is *not* amenable to the straight classical method of Chabauty,

Diophantus

Returning to Diophantus's problem and the curve:

$$X: \quad y^2 = x^6 + x^2 + 1,$$

this curve has Mordell-Weil rank = genus = 2, so is *not* amenable to the straight classical method of Chabauty,

but a mild extension of it can be applied, and was indeed applied in Wetherell's thesis to prove that Diophantine had found *all* positive rational values of x that give rational points on X. namely:

$$\boxed{x = 1/2.}$$

Diophantus's curve is a hyperelliptic curve over $\mathbb{Q}$

Curves that are double covers of the projective line, i.e., of the form

$$C : y^2 = f(x)$$

where $f(x) \in \mathbb{Q}[X]$ is a polynomial with no multiple roots are called **hyperelliptic curves**—an intensely studied family of curves. If $degree(f) \geq 5$ then C is of genus > 1.

Diophantus's curve is a hyperelliptic curve over $\mathbb{Q}$

Curves that are double covers of the projective line, i.e., of the form

$$C : y^2 = f(x)$$

where $f(x) \in \mathbb{Q}[X]$ is a polynomial with no multiple roots are called **hyperelliptic curves**—an intensely studied family of curves. If $degree(f) \geq 5$ then C is of genus > 1.

Mention Drosophila

Statistically. . .

Fixing g and ordering isomorphism classes of hyperelliptic curves defined over $\mathbb{Q}$ by the discriminant of their defining polynomial $f(x)$, we may ask statistical questions about the set of those curves. If $degree(f)$ is odd, the point at ∞ is a $\mathbb{Q}$-rational point of C.

Questions

Is it true that with probability 1 the rational point ∞ is the only $\mathbb{Q}$-rational point of C?

- Bjorn Poonen and Michael Stoll have shown that most hyperelliptic curves given by $y^2 = f(x)$ with $f(x)$ of odd degree have only the one rational point ∞.

- Bjorn Poonen and Michael Stoll have shown that most hyperelliptic curves given by $y^2 = f(x)$ with $f(x)$ of odd degree have only the one rational point ∞.
- More specifically, for $g \geq 3$ a positive portion of such curves have ∞ as their only rational point, and this proportion tends to 1 as g tends to infinity.

- Bjorn Poonen and Michael Stoll have shown that most hyperelliptic curves given by $y^2 = f(x)$ with $f(x)$ of odd degree have only the one rational point ∞.

- More specifically, for $g \geq 3$ a positive portion of such curves have ∞ as their only rational point, and this proportion tends to 1 as g tends to infinity.

- Following these results, Arul Shankar and X. Wang show that when $g \geq 9$, a positive proportion of hyperelliptic curves of genus g having *two* non-Weierstrass $\mathbb{Q}$-rational points have exactly those two rational points, and that this proportion tends to 1 as g tends to infinity.

Locally soluble hyperelliptic curves are often *not* globally soluble

A theorem of Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang asserts that:

Le k be any fixed odd integer.

The proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ of genus g having no points over *any odd degree extension of* $\mathbb{Q}$ *of degree at most* k tends to 1 as g tends to infinity.

An atypical collection of hyperelliptic curves:

$$C : y^2 = (x - a_1)(x - a_2) \dots (x - a_d) \; + \; c^2$$

An atypical collection of hyperelliptic curves:

$$C : y^2 = (x - a_1)(x - a_2) \dots (x - a_d) \; + \; c^2$$

where the a_i are distinct rational numbers, and c is a nonzero rational number chosen such that C is smooth.

An atypical collection of hyperelliptic curves:

$$C : y^2 = (x - a_1)(x - a_2) \dots (x - a_d) \; + \; c^2$$

where the a_i are distinct rational numbers, and c is a nonzero rational number chosen such that C is smooth.

There are (at least)

$$\boxed{2d \sim 4g}$$

rational points on such curves C.

So. . . how many rational points does a *general* algebraic curve of genus > 1 have?

Here's a challenge: can one beat that "atypical collection"?:

Fix any number field K and $\epsilon > 0$, can you find—for arbitrarily large genus g infinitely many curves defined over K of genus g with more than $(4 + \epsilon)g$ K-rational points?

Even after 17 centuries we are still at the beginning of any full understanding of the nature of rational points on algebraic curves

Pure mathematics is, in its way, the poetry of logical ideas. One seeks the most general ideas of operation which will bring together in simple, logical and unified form the largest possible circle of formal relationships.

Albert Einstein