ABELIAN VARIETIES

Arizona Winter School 2024

Barry Mazur

What are Abelian Varieties?

- Why are they interesting?
- Why are they useful?

That's going to be the theme of my lectures!

as well as a discussion of recent work, recent conjectures, recent questions—regarding uniformity and statistics (i.e., average values) of the Diophantine behavior of Abelian varieties.

We'll begin by talking about Abelian Varieties of dimension 1

—AKA **elliptic curves**—

defined over a field K, these being representable as plane cubic curves with coefficients in K.

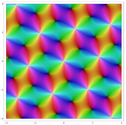
Starting in the spirit of Weierstrass

Given a *lattice* $\Lambda \subset \mathbb{C}$

— i.e., a discrete subgroup free of rank 2, in $\mathbb{C}$ —

Weierstrass (1849) defined the rather amazing doubly periodic function that bears his name:

$$\boxed{\mathcal{P}(z,\Lambda) := \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)}$$



where the mapping

$$z \quad \xrightarrow{\phi} \quad (\mathcal{P}(z), \mathcal{P}'(z)) \quad \in \quad \mathbb{C}^2$$

parametrizes the affine cubic curve:

$$Y^2 = 4X^3 - g_2 X - g_3$$

$$g_2 := 60 \sum_{0 \neq \lambda \in \Lambda} \lambda^{-4}$$

$$g_3 := 140 \sum_{0 \neq \lambda \in \Lambda} \lambda^{-6}$$

Since

$$\boxed{\mathcal{P}'^2(z) = 4\mathcal{P}^3(z) - g_2\mathcal{P}(z) - g_3}$$

giving $\mathbb{C}/\Lambda$ an algebraic structure.

Leading the theory in two directions:

- To complex tori. I.e.,
  Compact Complex Analytic Abelian Lie groups
  these being of the form

  $$\mathbb{C}^g/\Lambda$$

  where $\Lambda \subset \mathbb{C}^g$ is a discrete free abelian subgroup of (maximal) rank $2g$.

and

- To Abelian varieties—or, at least at first, to cubic plane algebraic curves with an inherited abelian group structure coming from the quotient $\mathbb{C}/\Lambda$, and to the more modern:

Spirit of Poincaré

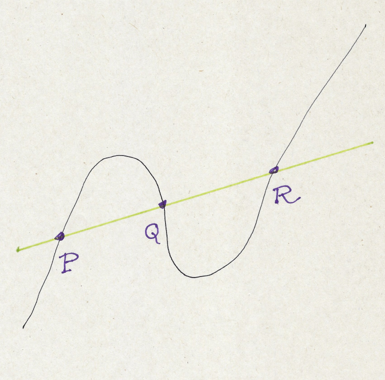
Although there were hints of this in the work of Jacobi before, it was in Poincaré‘s 1901 paper:
Sur les propriétés arithmétiques des courbes algébriques
where elliptic curves—i.e., 1-dimensional abelian varieties—got started:

Points rationnels des cubiques:

Étudions d'abord la distribution des points rationnels sur ces courbes. J'observe que la connaissance de deux points rationnels sur une cubique rationnelle suffit pour en faire connaître un troisième.

"Rational points on cubics: *Let's first study the distribution of rational points on these curves. I note that knowledge of two rational points on a rational cubic is sufficient to get us to know a third.*

$$P + Q + R = 0$$



Without stating this explicitly, Poincaré views the set of rational points on an elliptic curve as an abelian group

—and with no proofs getting in the way—

he defines the **rank** of an elliptic curve to be the number of points playing the role of P and Q needed to get all the rational points on the curve; in effect, anticipating:

Mordell's Theorem proved over two decades later.

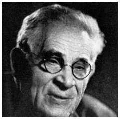
Without stating this explicitly, Poincaré views the set of rational points on an elliptic curve as an abelian group

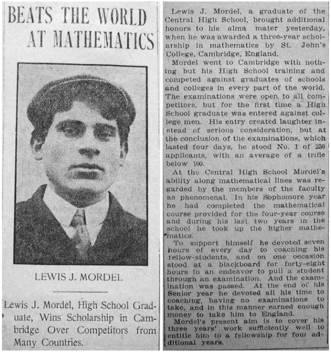
—and with no proofs getting in the way—

he defines the **rank** of an elliptic curve to be the number of points playing the role of P and Q needed to get all the rational points on the curve; in effect, anticipating:

Mordell's Theorem proved over two decades later.

The spirit of Mordell





BEATS THE WORLD AT MATHEMATICS

LEWIS J. MORDEL

Lewis J. Mordel, High School Graduate, Wins Scholarship in Cambridge Over Competitors from Many Countries.

Lewis J. Mordel, a graduate of the Central High School, brought additional honors to his alma mater yesterday, when he was awarded a three-year scholarship in mathematics by St. John's College, Cambridge, England.

Mordel went to Cambridge with nothing but his High School training and competed against graduates of schools and colleges in every part of the world. The examinations were open to all competitors, but for the first time a High School graduate was entered against college men. His entry created laughter instead of serious consideration, but at the conclusion of the examinations, which lasted four days, he stood No. 1 of 250 applicants, with an average of a trifle below 100.

At the Central High School Mordel's ability along mathematical lines was regarded by the members of the faculty as phenomenal. In his Sophomore year he had completed the mathematical course provided for the four-year course and during his last two years in the school he took up the higher mathematics.

To support himself he devoted seven hours of every day to coaching his fellow-students, and on one occasion stood at a blackboard for forty-eight hours in an endeavor to pull a student through an examination. And the examination was passed. At the end of his Senior year he devoted all his time to coaching, having no examinations to take, and in this manner earned enough money to take him to England.

Mordel's present aim is to cover his three years' work sufficiently well to entitle him to a fellowship for four additional years.

If a non-singular rational plane cubic curve has a rational point, then the group of rational points is finitely generated.

L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees Proc. Camb. Philos. Soc. 21, 179-192 (1922)

‘Descent’ as Mordell’s method of proof:

If A is the *elliptic curve* over $\mathbb{Q}$ defined by one of those

“indeterminate equations of the third or fourth degree”

and $A(\mathbb{Q})$ is its (commutative!) group of rational points then Mordell’s proof has two parts that play off one on the other:

“Weak Mordell-Weil” and “Controlling by Height”

1. (“Weak M-W”:) The group $\boxed{A(\mathbb{Q})/2A(\mathbb{Q})}$ is finite,

and

“Weak Mordell-Weil” and “Controlling by Height”

1. (“Weak M-W”:) The group $\boxed{A(\mathbb{Q})/2A(\mathbb{Q})}$ is finite,

   and

2. (“Controlling by Height ”) Multiplication by 2 increases the *height* of a $\mathbb{Q}$-rational point (essentially) by a factor of 4.

“Weak Mordell-Weil” and “Controlling by Height”

1. (“Weak M-W”:) The group $\boxed{A(\mathbb{Q})/2A(\mathbb{Q})}$ is finite,

   and

2. (“Controlling by Height ”) Multiplication by 2 increases the *height* of a $\mathbb{Q}$-rational point (essentially) by a factor of 4.

By **(2)** it follows that a rational point of nonzero (Néron-Tate) height cannot be divisible by 2^n for n indefinitely large. Given **(1)**, a simple further argument proves that $A(\mathbb{Q})$ is finitely generated.

The surprising computability of upper bounds for the “Weak Mordell-Weil” quotient groups

$$\boxed{A(K)/2A(K)}$$

—Or more generally, of the quotient groups—

$$\boxed{A(K)/nA(K)}$$

is the strength of Mordell’s original proof.

This is echoed by all the later proofs of the more general Mordell-Weil Theorem, making use of:

The fundamental short exact sequence:

$$0 \to A[n] \to A \xrightarrow{n} A \to 0$$

that gives rise to:

the basic “weak-MW-framework”:

$$0 \longrightarrow A(K)/nA(K) \longrightarrow H^1(K, A[n]) \longrightarrow H^1(K, A)[n] \longrightarrow 0$$

the basic “weak-MW-framework”:

$$0 \longrightarrow A(K)/nA(K) \longrightarrow H^1(K, A[n]) \longrightarrow H^1(K, A)[n] \longrightarrow 0$$

which doesn’t quite get you where you want since $H^1(K, A[n])$ is very likely of *infinite rank* over $\mathbb{Z}/n\mathbb{Z}$.

Local Conditions

But once you impose local conditions at primes v:

$$\begin{tikzcd}
0 \arrow[r] & A(K)/nA(K) \arrow[r] \arrow[d] & H^1(K, A[n]) \arrow[d] \\
0 \arrow[r] & A(K_v)/nA(K_v) \arrow[r] & H^1(K_v, A[n])
\end{tikzcd}$$

satisfied by global rational points you cut out Selmer subgroups within $H^1(K, A[n])$ obtaining finiteness

$$\begin{tikzcd}
0 \arrow[r] & A(K)/nA(K) \arrow[r] & H^1(K, A[n]) \\
0 \arrow[r] & A(K)/nA(K) \arrow[r] \arrow[u, "="] & \mathrm{Selmer_n(A; K)} \arrow[u, "\text{local conditions}"] \\
 & & 0 \arrow[u]
\end{tikzcd}$$

These Selmer groups $Selmer_n(A; K)$ are finite (and computable!) so it follows that

$$\boxed{A(K)/n \cdot A(K) \text{ is finite}}$$

(with a computable upper bound). This is how you prove "Weak MW."

That's what got our subject started

Milestones. . .

The elliptic curve with the highest rank found so far is:

$$y^2 + xy + y = x^3 - x^2 -$$

$$20067762415575526585033208209338542750930230312178956502x +$$

$$34481611795030556467032985690390720374855944359319180361266008296291939448732243429$$

which has rank at least 28.

'Noam Elkies' Elliptic Curve'

Uniformity of Mordell-Weil rank

And here's a fairly recent conjecture[1] suggested by computations that depend on the random matrix heuristic. It is striking in its precision, and in how close it is to the data accumulated so far.

Conjecture

(Park, Poonen, Voight, Wood) There are only finitely many elliptic curves over $K = \mathbb{Q}$ of Mordell-Weil rank greater than 21*.*

[1] *A heuristic for boundedness of ranks of elliptic curves*, Jennifer Park, Bjorn Poonen, John Voight, Melanie Matchett Wood https://arxiv.org/abs/1602.01431

Average Mordell-Weil rank

There is an immense literature on this, both in terms of what is proved, and what is conjectured, but the simplest to state qualiitative conjecture still outstanding is that

roughly 'half' of the elliptic curves over $\mathbb{Q}$ have Mordell-Weil rank 0 and half have rank 1, and those with higher rank amount to 0% of the total number of elliptic curves over $\mathbb{Q}$.

This would imply that the average rank of the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$ is $\frac{1}{2}$.

It is known[2] that arranging elliptic curves E over $\mathbb{Q}$ by a natural "naive" height—the average size of $Sel_2(E)$ is 3 and $Sel_3(E)$ is 4. The latter result alone implies that

the average Mordell-Weil rank of elliptic curves over $\mathbb{Q}$ is $\leq \frac{7}{6}$

[2] See, for example,

- M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics **181** (2015), 191-242;
- Bjorn Poonen's Bourbaki Seminar article `arXiv:1203.0809v2`
- M. Bhargava and W. Ho, *On average sizes of Selmer groups and ranks in families of elliptic curves having marked points* `arXiv:2207.03309v2`

Now for Abelian Varieties in general

Curiously, you need very few axioms to define this notion.

Definition

(Quite a sparce definition!) Let K be a field and $A_{/K}$ a smooth projective variety, and $e \in A(K)$ a K-rational point. Suppose that A is endowed with a morphism

$$A \times A \xrightarrow{m} A$$

defined over K (that, for the moment, we view as 'multiplication' writing $m(x, y) = x \cdot y$) and relative to which e is an 'identity element.' That is,

$$x \cdot e = x = e \cdot x.$$

Then A is called an abelian variety over K.

Basic Theorems

Theorem

Abelian varieties are in fact abelian algebraic groups; "multiplication" is a commutative group law. And so, naturally, multiplication is written as 'addition' $(+)$.

There are some (different) neat proofs of this—
two in David Mumford's book Abelian Varieties.

For example, to see that such a multiplication morphism m has inverses, consider the mapping

$$A \times A \xrightarrow{\phi} A \times A$$

that sends

$$(x, y) \mapsto (xy, x).$$

Visibly the inverse of (e, e) is nothing more than the point (e, e). I.e., the fiber of ϕ over (e, e) is one point. Therefore by a standard dimension theorem, we have that ϕ is surjective, so for any $x \in A$, there's a $y \in A$ such that $xy = e$.

Arguments of a similar nature give that the multiplication law m is commutative, and associative.

The spirit of André Weil

Although the Mordell-Weil theorem—the result that generalize Mordell's Theorem—is usually stated this way:

Theorem

(Mordell-Weil) Let K be a number field and $A_{/K}$ an abelian variety, then the 'Mordell-Weil group' of A over K; i.e., the group $A(K)$ of K-rational points of A is a finitely generated abelian group.

Weil proved it specifically for Abelian varieties that are Jacobians of curves

He stated it this way:

> *"One finds that all rational systems of points on a curve are derived from a finite number of them by addition and subtraction."*

In our more modern terminology

rational systems of points ↔ *Divisors on the curve*

and

“derived from” ↔ *“linearly equivalent to”*

—leading us to:

The particular class of abelian varieties that are Jacobians of curves

but happily:

Lemma

Any abelian variety over K is isogenous to a sub-abelian variety of the Jacobian of some curve over K.

from which “The Mordell-Weil Theorem” then follows for *all abelian varieties*—so let’s consider Jacobians.

Jacobians

From now on K will be a number field. Fix C be a smooth projective curve of genus $g \geq 1$ defined over K, and let $e \in C$ be a K-rational point. The abelian varieties we'll focus on are:

Jacobians

From now on K will be a number field. Fix C be a smooth projective curve of genus $g \geq 1$ defined over K, and let $e \in C$ be a K-rational point. The abelian varieties we'll focus on are:

- $A := J_C$: **The jacobian of such curves** C

Jacobians

From now on K will be a number field. Fix C be a smooth projective curve of genus $g \geq 1$ defined over K, and let $e \in C$ be a K-rational point. The abelian varieties we'll focus on are:

- $A := J_C$: **The jacobian of such curves** C

The **jacobian**, J_C, of the curve C is the abelian variety over K given in any of these ways:

(1) Viewed in the spirit of Weierstrass, at least when the base field is $\mathbb{C}$:

By the lattice of periods!

(2) Or viewed concretely:

as having the property that for any field extension L/K, its group of L-valued points, $J_C(L)$, is the quotient group:

{Divisors on C of degree zero defined over L} / {Principal Divisors}

$$DIV^0(C)/K(A)^*$$

(3) Or viewed more structurally:

$$\boxed{\underline{Pic}^0(C)_{/K},}$$

the abelian group scheme representing the functor

$$K\text{-scheme } S \mapsto$$

$\{$the group (under tensor product) of isomorphism classes of line bundles of degree zero (relative to S) over $C \times_{SpecK} S\}$.

Note that

$$C \mapsto \underline{Pic}^0(C)_{/K}$$

is a contravariant functor—and is, sort of—

the motivic H^1 of C.

(4) Or viewed straight functorially:

as "the smallest group scheme containing C."

That is, consider the problem of mapping (C, e) (base changed to any K-scheme S) to any abelian scheme A over S:

$$\begin{tikzcd}
C \arrow[r, "\phi"] & A \\
e \arrow[u] \arrow[r] & 0 \arrow[u]
\end{tikzcd} \tag{1}$$

J_C is the **Albanese variety** of (C, e) (over K).

That is, $C \hookrightarrow Alb(C)$ represents that universal problem: $Alb(C)$ is an abelian variety over K together with a morphism over K,

that has the property that any morphism $C \to A$ such as (1) above factors uniquely:

$$\begin{tikzcd} C \arrow[r] & Alb(C) \arrow[r, "\phi"] & A \end{tikzcd}$$

where $Alb(C) \xrightarrow{\phi} A$ is a homomorphism of abelian varieties.

Note that

$$C \mapsto Alb(C)$$

is a covariant functor—and is, sort of—

the motivic H_1 of C.

Discuss duality and self-duality

(5) Or in a way, relevant to Diophantine issues that we'll be discussing, in terms of symmetric powers:

Definition

For $n \geq 1$ let S_n be the symmetric group "on n letters" acting on the n-th power of the curve C. Denote by

$$Symm^n(C) := \quad C^n/S_n,$$

the quotient n-dimensional projective variety.

The relation between $Symm^n(C)$ and J_C

For any $n \geq 1$ there is a natural map, defined over L:

$$\iota : Symm^n(C) \quad \longrightarrow \quad J_C \tag{2}$$

sending an unordered n-tuple

$$(e_1, e_2, \ldots, e_n)$$

to the linear equivalence class of the divisor of degree zero in C:

$$\sum_{k=1}^{n} e_k \quad - \quad n \cdot e.$$

$$\begin{cases} Symm^n(C) & \overset{\iota}{\to} \quad J_C \\ \\ (e_1, e_2, \ldots, e_n)] & \overset{\iota}{\mapsto} \quad \left[\ \sum_{k=1}^{n} e_k \quad - \quad n \cdot e\ \right] \end{cases} \tag{3}$$

$$\begin{cases} Symm^n(C) & \overset{\iota}{\to} \quad J_C \\ \\ (e_1, e_2, \ldots, e_n)] & \overset{\iota}{\mapsto} \quad \left[\ \sum_{k=1}^{n} e_k \quad - \quad n \cdot e\ \right] \end{cases} \tag{3}$$

Theorem

- *The fibers of the morphism ι are rational varieties.*
- *If $n \geq g$, ι is surjective.*
- *If $n < \delta_C :=$ the K^{alg}-gonality of C, then*

$$Symm^n(C) \overset{\iota}{\hookrightarrow} J_C$$

is injective.

Gonality

Definition

The K-gonality of a curve is the smallest degree of any nonconstant rational function on it–that is defined over K.

This notion (at least for $K = \mathbb{C}$) was originally introduced by Bernhard Riemann in Section V of his Theory of Abelian Functions.

The connection between algebraic points on C and rational points on J_C

If $\alpha \in C(K^{\mathrm{alg}})$ is an algebraic point on C and the set

$$\{\alpha_1, \alpha_2, \ldots, \alpha_\nu\} \subset C(K^{\mathrm{alg}})$$

consists of α and its conjugates over K, define $j(\alpha) \in J_C(K)$ to be the divisor class of

$$\sum_{i=1}^{\nu} \alpha_i \quad - \quad \nu \cdot e.$$

Let $\mathcal{S}_C(K;d)$ denote the set of K-conjugacy classes of algebraic points on C of degree $\leq d$. We have the natural mapping

$$\boxed{\mathcal{S}_C(K;d) \xrightarrow{j} J_C(K)}$$

End of Lecture 1

Recall our set-up:

- Let K be a number field, and C a smooth projective curve over K (say of genus > 0) with $e \in C$ a chosen K-rational point;

Recall our set-up:

- Let K be a number field, and C a smooth projective curve over K (say of genus > 0) with $e \in C$ a chosen K-rational point;

- J_C : the jacobian of C where we consider the injection $C \hookrightarrow J_C$ that sends the point x to the divisor class of $[x] - [e]$;

Recall our set-up:

- Let K be a number field, and C a smooth projective curve over K (say of genus > 0) with $e \in C$ a chosen K-rational point;
- J_C : the jacobian of C where we consider the injection $C \hookrightarrow J_C$ that sends the point x to the divisor class of $[x] - [e]$;
- $Symm^n(C) \xrightarrow{\iota} J_C$ the natural map of the n-th symmetric power of C to J_C;

Recall our set-up:

- Let K be a number field, and C a smooth projective curve over K (say of genus > 0) with $e \in C$ a chosen K-rational point;
- J_C : the jacobian of C where we consider the injection $C \hookrightarrow J_C$ that sends the point x to the divisor class of $[x] - [e]$;
- $Symm^n(C) \xrightarrow{\iota} J_C$ the natural map of the n-th symmetric power of C to J_C;
- δ_C the **gonality** of C;

Recall our set-up:

- Let K be a number field, and C a smooth projective curve over K (say of genus > 0) with $e \in C$ a chosen K-rational point;
- J_C : the jacobian of C where we consider the injection $C \hookrightarrow J_C$ that sends the point x to the divisor class of $[x] - [e]$;
- $Symm^n(C) \xrightarrow{\iota} J_C$ the natural map of the n-th symmetric power of C to J_C;
- δ_C the **gonality** of C;
- $\mathcal{S}_C(K; d)$: the set of K-conjugacy classes of algebraic points on C of degree $\leq d$.

‘Gonality’ as related to striking ‘Uniformity’

As mentioned yesterday:

Corollary

Let $\mathcal{S}_C(K;d)$ denote the set of K-conjugacy classes of algebraic points on C of degree $\leq d$. Then if $d < \delta_C$, the natural mapping

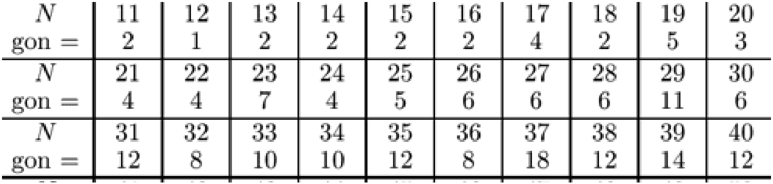
$$\boxed{\mathcal{S}_C(K;d) \overset{j}{\hookrightarrow} J_C(K)}$$

is injective.

This is one of the great uses of Mordell-Weil: to control algebraic points on curves!

Examples of gonality

The modular curve $Y_1(N)$ is an affine smooth curve over $\mathbb{Q}$ which K-rational points correspond to pairs (E, P) where E is an elliptic curve over K and P is a K-rational point of (finite) order N. Here is a table[3] of the $\mathbb{Q}$-gonalities of $Y_1(N)$ for $11 \leq N \leq 30$:



N	11	12	13	14	15	16	17	18	19	20
gon =	2	1	2	2	2	2	4	2	5	3
N	21	22	23	24	25	26	27	28	29	30
gon =	4	4	7	4	5	6	6	6	11	6
N	31	32	33	34	35	36	37	38	39	40
gon =	12	8	10	10	12	8	18	12	14	12

[3] taken from *Gonality of the modular curve $X_1(N)$* by Maarten Derickx and Mark van Hoeij (arXiv:1307.5719v3)

An impressive example

Consider

$$C = X_1(31),$$

the curve that classifies elliptic curves with a fixed torsion point of order 31.

Its genus is 26 and, by the table, its gonality is 12.

So, over any number field K and any degree $d < 12$,

we have the inclusion:

$$\boxed{\mathcal{S}_C(K; d) \overset{j}{\hookrightarrow} J_C(K)}$$

Gerd Faltings' Theorem

Faltings' theorem—is striking:

Any subvariety V defined over a number field K that is

- contained in an abelian variety A (over K) and
- is such that $V(K)$ is Zariski-dense in V

is a finite union of translates of subabelian varieties defined over K.

The proof is not *constructive*.

The beguiling character of Faltings' proof is that it is tantalizingly semi-effective.

The beguiling character of Faltings' proof is that it is tantalizingly semi-effective.That is, even when you take the variety V to be the curve C sitting in its own jacobian—noting that Faltings' Theorem proves Mordell's Conjecture if the curve is of genus > 1—

- the proof doesn't give an upper bound for the *size* (i.e., "height") of rational points on C but

The beguiling character of Faltings' proof is that it is tantalizingly semi-effective.That is, even when you take the variety V to be the curve C sitting in its own jacobian—noting that Faltings' Theorem proves Mordell's Conjecture if the curve is of genus > 1—

- the proof doesn't give an upper bound for the *size* (i.e., "height") of rational points on C but
- it seems that it does—implicitly—offer a bound for the *number* of rational points—with another "but":

The beguiling character of Faltings' proof is that it is tantalizingly semi-effective.That is, even when you take the variety V to be the curve C sitting in its own jacobian—noting that Faltings' Theorem proves Mordell's Conjecture if the curve is of genus > 1—

- the proof doesn't give an upper bound for the *size* (i.e., "height") of rational points on C but
- it seems that it does—implicitly—offer a bound for the *number* of rational points—with another "but":
- that bound is likely to be very high.

Uniformity consequence of Faltings Theorem:

Theorem

Let C be a curve over K of genus g and gonality δ.

Uniformity consequence of Faltings Theorem:

Theorem

Let C be a curve over K of genus g and gonality δ.

Then for any $n < \delta$, the set of K-rational points of $Symm^n(C)$ lie in the union of:

Uniformity consequence of Faltings Theorem:

Theorem

Let C be a curve over K of genus g and gonality δ.

Then for any $n < \delta$, the set of K-rational points of $Symm^n(C)$ lie in the union of:

- *a finite set and*
- *finitely many 'translates of abelian subvarieties that lie in $Symm^n(C) \hookrightarrow J_C$.*

This leads to a challenging computational project!

“Non-nearly elliptic curves”

To give a sense of the strength of Faltings Theorem, call a curve C **non-nearly elliptic** if $Symm^2(C)$ contains no elliptic curve (say: even over K^{alg}).

It follows that the gonality of C is > 2.

(In particular, C is neither hyperlliptic nor bielliptic.)

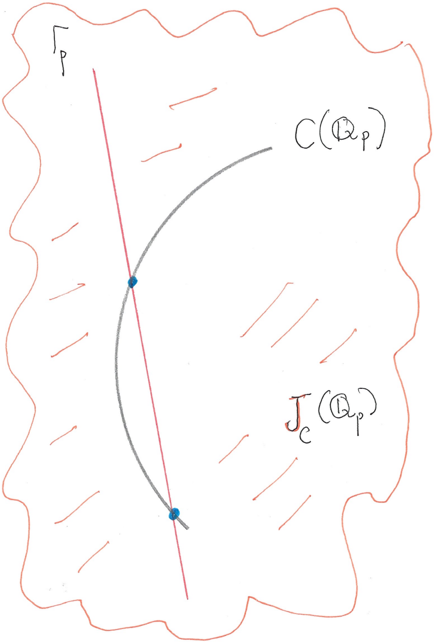
Falting’s theorem implies that C has only finitely many *quadratic points* over any number field over which it is defined!

Small Mordell-Weil rank in the jacobian of C can yield precise upper bounds for the number of rational points!

The classical method of Chabauty for proving finiteness of rank—it doesn't provide explicit upper bounds (yet):

Consider the topological completion Γ_p of the Mordell-Weil group of J_C in the p-adic analytic group $J_C(\mathbb{Q}_p)$;

this is a p-adic analytic group of dimension $\leq$ the Mordell-Weil rank of J_C, which we assume is strictly less than the dimension of J_C.


Γ_p
$C(\mathbb{Q}_p)$
$J_C(\mathbb{Q}_p)$

We get $C(\mathbb{Q}_p) \cap \Gamma_p$, a finite set of p-adic points that captures all rational points:

Since, under the ‘Chabauty hypothesis’ that the rank of Mordell-Weil is less than the genus of C, the group Γ_p is of positive codimension in $J_C(\mathbb{Q}_p)$,

We get $C(\mathbb{Q}_p) \cap \Gamma_p$, a finite set of p-adic points that captures all rational points:

Since, under the 'Chabauty hypothesis' that the rank of Mordell-Weil is less than the genus of C, the group Γ_p is of positive codimension in $J_C(\mathbb{Q}_p)$,

and since $C(\mathbb{Q}_p)$ is a p-adic analytic curve *that generates the group* $J_C(\mathbb{Q}_p)$,

We get $C(\mathbb{Q}_p) \cap \Gamma_p$, a finite set of p-adic points that captures all rational points:

Since, under the ‘Chabauty hypothesis’ that the rank of Mordell-Weil is less than the genus of C, the group Γ_p is of positive codimension in $J_C(\mathbb{Q}_p)$,

and since $C(\mathbb{Q}_p)$ is a p-adic analytic curve *that generates the group* $J_C(\mathbb{Q}_p)$,

the intersection $C(\mathbb{Q}_p) \cap \Gamma_p$ is finite.

Since we have the inclusion $C(\mathbb{Q}) \hookrightarrow C(\mathbb{Q}_p) \cap \Gamma_p$ we get that $C(\mathbb{Q})$ is finite as well.

Robert Coleman reframed the Chabauty approach

to define an explicit p-adic analytic function whose zeroes are precisely $C(\mathbb{Q}_p) \cap \Gamma_p \ldots$ making it possible to get explicit upper bounds for $C(\mathbb{Q}_p) \cap \Gamma_p$, and therefore for $C(\mathbb{Q})$ as well.

Take Hyperelliptic curves as an example.

Robert Coleman reframed the Chabauty approach

to define an explicit p-adic analytic function whose zeroes are precisely $C(\mathbb{Q}_p) \cap \Gamma_p \ldots$ making it possible to get explicit upper bounds for $C(\mathbb{Q}_p) \cap \Gamma_p$, and therefore for $C(\mathbb{Q})$ as well.

Take Hyperelliptic curves as an example.

A **Hyperelliptic curve** over K is a curve of the form

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

of genus $g_C > 1$ whose projective completion we assume to be smooth. Its gonality is (visibly) 2.

This class of curves provides a wonderful testing ground for diophantine questions, and has been extensively studied, theoretically and computationally.

Assuming that C has a K-rational point e, we have our embedding

$$C \hookrightarrow J_C.$$

Let g_C be its genus

and

$$\mathsf{r}_C := \mathrm{rank}\{J(C)(K)\},$$

i.e., the Mordell-Weil rank (over K) of its jacobian.

Assume that r_C is small, and here is what you get:

A striking upper bound on the number of K-rational points

Michael Stoll: Hyperelliptic curves of genus g that are of MW-rank r over a number field K with

$$\mathrm{r} \leq g - 3$$

have no more than

$$\boxed{8\mathrm{r} \cdot g + 33(g-1) + 1}$$

K-rational points.

A striking upper bound on the number of K-rational points

Michael Stoll: Hyperelliptic curves of genus g that are of MW-rank r over a number field K with

$$\mathrm{r} \leq g-3$$

have no more than

$$\boxed{8\mathrm{r}\cdot g+33(g-1)+1}$$

K-rational points.

E.g.: if the genus of the curve C is three, then C has no more than 67 points over **any number field** K for which the jacobian J_C has only finitely many K-rational points.

Infinitely many (hyperelliptic) curves with few points

A consequence the previous result of Stoll and a recent result of Myungjun Yu:

For any number field K and genus $g > 4$ there are infinitely many hyperelliptic curves over K of genus g that have some, but no more than

$$41g - 32$$

K-rational points.

A (hyperelliptic) curve with lots of points

But things are different if $r > g - 3$ (as is necessarily the case when $g = 2$, for example.)

A (hyperelliptic) curve with lots of points

But things are different if $r > g - 3$ (as is necessarily the case when $g = 2$, for example.)

. . . describe the format of Chabauty-Coleman-Kim!. . .

The world's record for curves of genus two with lots of points

is held by this example discovered by Michael Stoll in 2008:

The world's record for curves of genus two with lots of points

is held by this example discovered by Michael Stoll in 2008:

$$y^2 =$$

$$= 82342800x^6 - 470135160x^5 + 52485681x^4 +$$

$$+ 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

The world's record for curves of genus two with lots of points

is held by this example discovered by Michael Stoll in 2008:

$$y^2 =$$

$$= 82342800x^6 - 470135160x^5 + 52485681x^4 +$$

$$+2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

that has at least 642 $\mathbb{Q}$-rational points.

The world's record for curves of genus two with lots of points

is held by this example discovered by Michael Stoll in 2008:

$$y^2 =$$

$$= 82342800x^6 - 470135160x^5 + 52485681x^4 +$$

$$+2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

that has at least 642 $\mathbb{Q}$-rational points. Here are a few of the x-coordinates of rational points on this curve:

$$0,\ -1,\ 1/3,\ 4,\ -4,\ \ldots\ -3898675687/2462651894$$

Most odd degree hyperelliptic curves over $\mathbb{Q}$ have 'no' points

Poonen-Stoll:

- A positive fraction of hyperelliptic curves

  $C: \ y^2 = f(x)$ where $f(x)$ is of odd degree ≥ 3 with integral coefficients

  have only one $\mathbb{Q}$-rational point: the point at infinity.

- There exists a lower bound on this fraction that tends to 1 as the genus of C goes to infinity.

Immediate Diophantine Consequences for larger gonalities

Let $C_{/K}$ be a projective smooth curve.

If $1 \leq d < \delta_C :=$ the $K^{\rm alg}$-gonality of C,

we get that $Symm^d(C)(K)$ and $\mathcal{S}_C(K; d)$ are finite sets;

i.e., the set of *all* algebraic points on C of degree $< \delta_C$ (over K)is finite

as long as:

- $Symm^d(C)$ contains no translates of abelian varieties, or
- the Mordell-Weil rank of J_C over K is zero.

Taking $d = 1$ in the first bullet implies Mordell's Conjecture for C over K—i.e., that $C(K)$ is finite.

The rarity of algebraic points of small degree!

Discuss $X_1(31)$ again, and $Symm^2(X_1(31))$

Diophantine Stability

Definition

For L/K an extension of fields, and V an algebraic variety defined over K denote by $V(K)$ the set of K-rational points of V. Say that V is **diophantine stable** for L/K, or L/K is **diophantine stable** for V if
"V acquires no new rational points when one changes the base from K to L."

That is, if the inclusion $V(K) \hookrightarrow V(L)$ is an isomorphism.

Note that the property of "Diophantine Stability" of V for any given L/K is inherited by subvarieties of V defined over K.

The Ubiquity of Diophantine Stability

It follows directly from our discussion that:

Theorem

If J_C has Mordell-Weil rank zero over K then C is diophantine stable for all but finitely many field extensions L/K of degree $d < \delta_C$.

This is also true—thanks to Faltings' Theorem— if, for example, $Symm^d(C)$ contains no translates of abelian varieties—or, at least, none with positive MW- rank.

More uniformity regarding Diophantine Stability

Karl Rubin and I defined the notion of ℓ-**diophantine stability** for ℓ a prime number:

A variety V over K is $\ell-$**diophantine stable over** K if for every positive integer n and finite set of primes S of K,

there are infinitely many cyclic extensions L/K of degree ℓ^n completely split at all primes $v \in S$, such that V is diophantine stable for L/K; i.e., such that $V(L) = V(K)$.

How often is an abelian variety ℓ-diophantine stable?

Karl and I proved:

Theorem

If A is a simple abelian variety over K and all $\bar{K}-$endomorphisms of A are defined over K, then A is $\ell-$diophantine stable over K for a set of rational primes ℓ with positive density.

Question: Is the above true for any abelian variety over any number field and for a set of primes ℓ of density 1?

Comment about how such uniformity comes about:

Let $A_{/K}$ satisfy the hypothesis of the theorem, and L/K be cyclic of prime order ℓ.

$A(L)$ has the same rank as $AK)$ as long as a certain 'relative Selmer group'

$$Sel(L/K, A[\ell]) \subset H^1(K, A[\ell])$$

vanishes, and the 'statistics' for the local conditions required for $Sel(L/K, A[\ell])$ to vanish is nicely controllable.

Uniformity—over the range of elliptic curves—regarding ℓ-Diophantine Stability for a fixed prime ℓ

Recently, Anwesh Ray and Tom Weston have proved[4]

Theorem

For $\ell \geq 5$ a prime number, the set of elliptic curves $E_{/\mathbb{Q}}$ that are ℓ-diophantine stable over K has density 1.

[4] *Diophantine stability for elliptic curves on average,* arXiv:2304.09742v1

Open Questions

Let K be *any* number field.

Do we expect—even in this broader framework—that the average Mordell-Weil rank for elliptic curves over K is $1/2$?

Open Questions

Let K be *any* number field.

Do we expect—even in this broader framework—that the average Mordell-Weil rank for elliptic curves over K is $1/2$?

We might ask, as is suggested in the paper of Park, Poonen, Voight, and Wood, that—ranging over all elliptic curves over K with j-invariant a primitive element for the field K—and defining

$$B_K$$

to be the smallest number such that there are only finitely many such elliptic curves of Mordell-Weil rank $> B_K$,

is it true that:

B_K is finite, uniformly bounded with a bound independent of K?

Back to Abelian varieties

We could ask similar such Mordell-Weil uniformity-type questions for abelian varieties of any fixed dimension. Might we hope for a broad extension of the LMFDB data-base to include such data, as well as data about curves of higher genus—this has already been started as the entries regarding

- *genus 2 curves over* $\mathbb{Q}$
- *higher genus families*
- and *abelian varieties over* F_q.

I learned in this *Winter School!*—from Drew Sutherland, Shiva Chidambaram, Eran Assaf, and Tayler Dupuy—that things are moving rapidly— See, for example,

- the archive note arXiv:2003.05380v2: *Isogeny Classes of Abelian Varieties over Finite Fields in the LMFDB* by Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent,

Regarding torsion points on higher dimensional abelian varieties

See Shiva Chidambaram's talk at JMM 2023 *The Galois images of Picard curves* that describes his work with P. Goodman computing Galois action on torsion points in genus 3 curves.

Regarding abelian surfaces:

Known torsion subgroups of abelian surfaces over $\mathbb{Q}$ (geometrically simple)

Andrew Sutherland sent this to me last night:
There are (at least) 63 torsion subgroups known to arise for geometrically simple abelian surfaces defined over $\mathbb{Q}$, including:

$$\mathbb{C}_n \text{ for } 1 \leq n \leq 30,\ 32,\ 33,\ 34,\ 36,\ 39,\ 40$$

$$C_2 \times C_{2n} \text{ for } 1 \leq n \leq 9,\ 11,\ 13,\ 14$$

$$C_2 \times C_2 \times C_{2n} \text{ for } 1 \leq n \leq 7$$

$$C_2 \times C_2 \times C_2 \times C_{2n} \text{ for } 1 \leq n \leq 3,\ 5$$

$$C_3 \times C_{3n} \text{ for } 1 \leq n \leq 3$$

$$C_4 \times C_4$$

Back to Abelian varieties ‘themselves’

How should one organize them appropriately for their role in arithmetic statistics?

- As Eran Asaf mentioned:

  A fundamental question to ask when $g \geq 4$ over $\mathbb{Q}$ is how to enumerate abelian varieties when they are no longer isomorphic (or even isogenous) to Jacobians?

I learned loads in this Winter School. Thanks AWS!