

ABELIAN VARIETIES

Arizona Winter School 2024

Barry Mazur

What are Abelian Varieties?

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

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 .

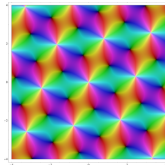
The spirit of Weierstrass

In fact, we'll start earlier than that. Given a *lattice* $\Lambda \subset \mathbb{C}$

—i.e., a discrete subgroup, free of rank 2—

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

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



where the mapping

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

factors through the quotient

the complement of Λ in \mathbb{C}

$$\begin{array}{ccc} & \downarrow & \searrow \\ \mathbb{C}/\Lambda - \{0\} & \longrightarrow & \mathbb{C}^2 \end{array}$$

and where the Reimann surface

$$\mathbb{C}/\Lambda - \{0\}$$

parametrizes the affine cubic curve:

$$Y^2 = 4X^3 - g_2X - g_3$$

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

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

letting (X, Y) run through

$$(\mathcal{P}(z), \mathcal{P}'(z)) \in \mathbb{C}^2 \text{ for } z \in \mathbb{C} \setminus \Lambda,$$

since we have the equation:

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

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}/Λ , and to:

The spirit of Poincaré



Although there were hints of this in the work of Jacobi before, it was in Poincaré's 1901 paper:

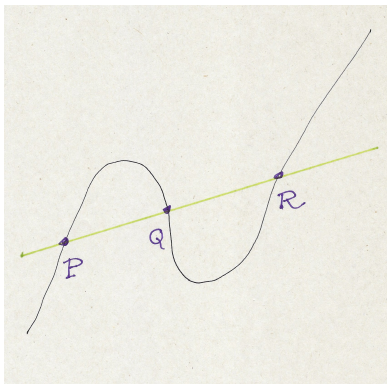
Sur les propriétés arithmétiques des courbes algébriques
where elliptic curves—i.e., **1-dimensional abelian varieties**—got started:

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.

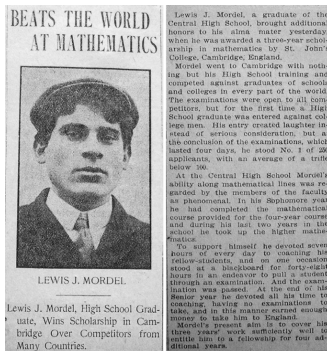
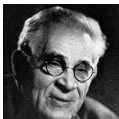
Without stating this explicitly, Poincaré views the set of rational points on an elliptic curve as an abelian group

—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 associativity law satisfied by this “chord-and-tangent process” becomes an interesting—and nicely classical—exercise in the plane geometry of these cubics.

The spirit of Mordell



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:

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

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

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

$$A(K)/2A(K)$$

—Or more generally, of the quotient groups $A(K)/nA(K)$ —
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:

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

that gives rise to:

the basic “weak-MW-framework”:

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

the basic “weak-MW-framework”:

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

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

But once you impose local conditions satisfied by global rational points you cut out **Selmer subgroups** within $H^1(K, A[n])$ obtaining finiteness:

$$\begin{array}{ccccc}
 0 & \longrightarrow & A(K)/n \cdot A(K) & \longrightarrow & H^1(K, A[n]) \\
 & & \uparrow \scriptstyle = & \text{local conditions} & \uparrow \\
 0 & \longrightarrow & A(K)/n \cdot A(K) & \longrightarrow & \text{Selmer}_n(A; K) \\
 & & & & \uparrow \\
 & & & & 0
 \end{array}$$

Since $\text{Selmer}_n(A; K)$ is finite (and computable!) it follows that

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

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

That's what got our subject started

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

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

$$\begin{aligned} &20067762415575526585033208209338542750930230312178956502x + \\ &3448161179503055646703298569039072037485594435931 \sim \\ &\sim 9180361266008296291939448732243429 \end{aligned}$$

which has rank at least 28.

'Noam Elkies' Elliptic Curve'

Uniformity of Mordell-Weil rank

And here's a fairly recent conjecture¹ 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 qualitative 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 known² that arranging elliptic curves E over \mathbb{Q} by a natural “naive” height—the average size of $\text{Sel}_2(E)$ is 3 and $\text{Sel}_3(E)$ is 4. The latter result alone implies that

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

²See, 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

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,

$$x \cdot e = x = e \cdot x \text{ (appropriately understood).}$$

Then A is called an **abelian variety** over K .

Basic Theorems

Theorem

*Abelian varieties are in fact **abelian algebraic groups**; AKA **commutative**. 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) . 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 \leftrightarrow *Divisors on the curve*

and

“derived from” \leftrightarrow *“linearly equivalent to*

leading us to:

The particular class of abelian varieties that are Jacobians of curves

Noting that:

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.

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're interested in are:

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're interested in are:

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

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're interested in 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:

Noting that if $\omega \in H^0(C; \Omega_C)$ is a regular differential on the projective curve C and $\gamma \in H_1(C; \mathbb{C})$ is a (homology class of a) 1-cycle, the period mapping:

$$(\omega, \gamma) \mapsto \int_{\gamma} \omega \in \mathbb{C}$$

yields a canonical embedding,

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

By the lattice of periods:

Noting that if $\omega \in H^0(C; \Omega_C)$ is a regular differential on the projective curve C and $\gamma \in H_1(C; \mathbb{C})$ is a (homology class of a) 1-cycle, the period mapping:

$$(\omega, \gamma) \mapsto \int_{\gamma} \omega \in \mathbb{C}$$

yields a canonical embedding,

$$\Lambda_C := H_1(C; \mathbb{Z}) \hookrightarrow V_C := \text{Hom}(H^0(C; \Omega_C), \mathbb{C}).$$

Define the jacobian of C —at least, viewed as complex analytic group—to be the quotient complex torus V_C/Λ_C .

(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:

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

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

(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 $C \times_{\mathrm{Spec} K} S$ }.

Note that

$$V \mapsto \underline{Pic}^0(V)_{/\kappa}$$

is a contravariant functor—and is, sort of—
the motivic H^1 of V .

(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 over A over S :

$$\begin{array}{ccc} C & \xrightarrow{\phi} & A \\ \uparrow & & \uparrow \\ e & \longrightarrow & 0 \end{array} \quad (1)$$

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

That is, $C \hookrightarrow J_C$ is an abelian variety A over K together with a morphism over K ,

that has the property that any morphism such as (1) above factors uniquely:

$$C \longrightarrow Alb(C) = J_C \xrightarrow{\phi} A$$

where $J_C \xrightarrow{\phi} A$ is a homomorphism of abelian varieties.

Note that

$$V \mapsto Alb(V)$$

is a covariant functor—and is, sort of—
the motivic H_1 of V .

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

$$\text{Symm}^n(C) := C^n/S_n,$$

the quotient n -dimensional projective variety.

The relation between $\text{Symm}^n(C)$ and J_C

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

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

sending an unordered n -tuple

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

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

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

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

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

Theorem

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

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

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

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

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

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

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

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

We might also consider K -rational points in a fixed symmetric power of C

For $n \geq d$ form the unordered n -tuple

$$\sigma(\alpha) := (\alpha_1, \alpha_2, \dots, \alpha_d, e, e, \dots, e) \in \text{Sym}^n(C)(K^{\text{alg}})$$

where

- ▶ we've added as many copies of e necessary to turn the above into an n -tuple, and note that
- ▶ $\sigma(\alpha)$ is in fact in $\text{Sym}^n(C)(K)$ and not merely in $\text{Sym}^n(C)(K^{\text{alg}})$.

Conjugacy classes of algebraic points of small degree d over K on the curve C

Corollary

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

$$S_C(K; d) \xhookrightarrow{j} J_C(K)$$

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 table³ of the \mathbb{Q} -gonalities of $Y_1(N)$ for $11 \leq N \leq 30$:

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

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

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”:

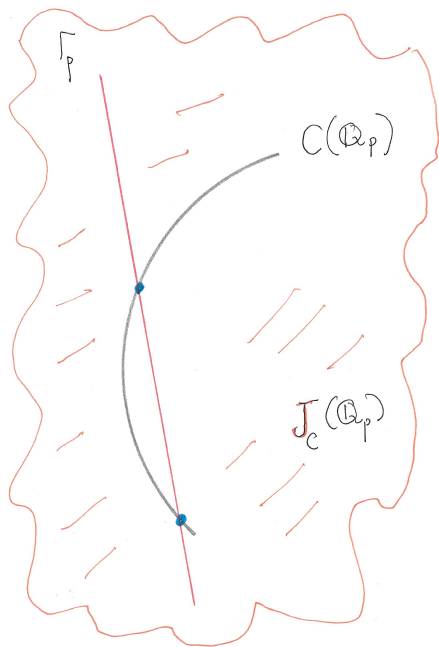
The beguiling character of Faltings' proof is that it is tantalizingly semi-effective. That is, even when you take the variety V to be the curve C sitting in its own jacobian—noting that Faltings' Theorem proves Mordell's Conjecture if the curve is of genus > 1 —

- ▶ 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.

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

First: 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 .



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.

Second: Robert Coleman reframed the Chabauty approach

to define an explicit p -adic analytic function whose zeroes are precisely $C(\mathbb{Q}_p) \cap \Gamma_p \dots$ 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.

Second: Robert Coleman reframed the Chabauty approach

to define an explicit p -adic analytic function whose zeroes are precisely $C(\mathbb{Q}_p) \cap \Gamma_p \dots$ 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

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

of genus $g_C > 1$ whose projective completion we assume to be smooth. This class of curves provides a wonderful testing ground for diophantine questions, and has been extensively studied, theoretically and computationally.

Its gonality is (visibly) 2.

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

$$C \hookrightarrow J_C.$$

Let g_C be its genus

and

$$r_C := \text{rank}\{J(C)(K)\},$$

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 over a number field K with

$$r \leq g - 3$$

have no more than

$$8r \cdot g + 33(g - 1) + 1$$

K -rational points.

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

Michael Stoll: Hyperelliptic curves of genus g over a number field K with

$$r \leq g - 3$$

have no more than

$$8r \cdot g + 33(g - 1) + 1$$

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:

$$\begin{aligned}y^2 = & \\ &= 82342800x^6 - 470135160x^5 + 52485681x^4 + \\ &+ 2396040466x^3 + 567207969x^2 - 985905640x + 247747600\end{aligned}$$

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

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

$$\begin{aligned}y^2 = & \\ &= 82342800x^6 - 470135160x^5 + 52485681x^4 + \\ &+ 2396040466x^3 + 567207969x^2 - 985905640x + 247747600\end{aligned}$$

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:

$$\begin{aligned} y^2 = & \\ &= 82342800x^6 - 470135160x^5 + 52485681x^4 + \\ &+ 2396040466x^3 + 567207969x^2 - 985905640x + 247747600 \end{aligned}$$

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

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

Current record-holders for genus 3 over $K = \mathbb{Q}$.

Both Keller-Kulesz, and Noam Elkies are tied for the record here, with (different) curves that each have at least **176** rational points. Here's Noam's:

$$\begin{aligned} Y^2 = & 5780865024X^8 - 88857648000X^7 + 542817272736X^6 - \\ & -1616473139664X^5 + 2143113743265X^4 - 145305843468X^3 - \\ & -2058755904906X^2 + 363486538980X + 1262256306129 \end{aligned}$$

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 gonality

Let C_K be a projective smooth curve.

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

we get that $\text{Sym}^d(C)(K)$ 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:

- ▶ $\text{Symm}^d(C)$ 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!

For example⁴, the smallest value of N for which $X_0(N)$ has gonality 3 (i.e., that is neither rational, elliptic, or hyperelliptic) is $N = 34$.

One can show that $\text{Symm}^2(X_0(34))$ contains no abelian varieties of positive MW-rank over \mathbb{Q} .

So it follows that $X_0(34)$ only has finitely many quadratic points—i.e., there are only finitely many elliptic curves over \mathbb{Q} possessing a rational 34-isogeny defined over quadratic fields.

⁴See Table 1 in *Gonality of the modular curve $X_0(N)$* by Filip Najman and Peter Orlic arXiv:2207.11650v4

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, $\text{Sym}^d(C)$ 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 ℓ -**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 ℓ -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’

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

vanishes, and the ‘statistics’ for the local conditions required for $\mathrm{Sel}(L/K, A[\ell])$ 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 proved⁵

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.

⁵*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 ?

And, even better: is $B_K < 22$?

...

$$B_K$$

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 ?

And, even better: is $B_K < 22$?

...and we could ask similar such Mordell-Weil uniformity-type questions for abelian varieties of any fixed dimension.