Diophantine Stability

For John Coates: happy seventieth birthday!

B. Mazur

Diophantine stability

refers to a project that Karl Rubin and I are currently working on. One application of our work is the following characterization of the projective line:

Diophantine stability

refers to a project that Karl Rubin and I are currently working on. One application of our work is the following characterization of the projective line:

Let K be a number field and C a smooth projective algebraic curve defined over K.Then $C \simeq \mathbf{P}^1$ (over K) $\iff$

Diophantine stability

refers to a project that Karl Rubin and I are currently working on. One application of our work is the following characterization of the projective line:

Let K be a number field and C a smooth projective algebraic curve defined over K.Then $C \simeq \mathbf{P}^1$ (over K) $\iff$

> *For every nontrivial field extension L/K, the curve C acquires new rational points over L, i.e., C has L-rational points that are not rational over any proper subfield of L.*

Generally speaking, rational points seem to be sparce

Generally speaking, rational points seem to be sparce

Let V be an algebraic variety over a number field K.

Unless there is a clear underlying structural mechanism for generating **many** *rational points in V, either V will tend not to have that many K-rational points, or . . . perhaps we're just not good at finding them.*

Some tried-and-true methods of producing points

(1) Let V be a quadric in $\mathbf{P}^N$ with a K-rational point x.

For any line passing through x rational over K, consider the "other" intersection point y of that line with V.

This point y is K-rational. By sweeping through K-rational lines one gets a profusion of K-rational points from this process.

Curves of genus zero

This works brilliantly, for example for curves of genus zero over K having a K-rational point.

Because, by Riemann-Roch, such a curve can always be represented as a plane conic over K.

Algebraic Groups

(2) If V has an algebraic group structure defined over K,

or for that matter, if V has *any interesting n-ary structure*, $n \geq 1$,

you can try to generate new points from old.

Elliptic curves as algebraic groups

The group structure on an elliptic curve over K,

i.e., a curve of genus one over K endowed with a base point (rational over K)

can be seen neatly via its representation, thanks to Riemann-Roch, as a plane cubic defined over K.

But, for curves of genus $\geq 2 \ldots$

A curve V is of genus ≥ 2 defined over a number field K has only finitely many K-rational points. Faltings' famous theorem (1983) proved this, with an effective (but 'large') upper bound for $|V(K)|$.

How large can $V(K)$ actually be?

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

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:

$$Y^2 = 5780865024X^8 - 88857648000X^7 + 542817272736X^6 -$$

$$-1616473139664X^5 + 2143113743265X^4 - 145305843468X^3 -$$

$$-2058755904906X^2 + 363486538980X + 1262256306129$$

Consequences of a conjecture of Serge Lang

Lucia Caporaso, Joe Harris and I showed (1997) that one of Lang's conjectures about rational points on general type varieties implies the following statement about rational points on curves over number fields:

The $N(g)$ conjecture: *Let $g \geq 2$. There is a finite number $N(g)$ such that for any number field K, there are only finitely many smooth curves of genus g over K with more than $N(g)$ K-rational points* **(??)**

Rational points *seem to be* rare!

What are lower bounds for $N(2), N(3), \ldots$?

current records:

Genya Zaytman: $N(2) \geq 226$;
Noam Elkies: $N(3) \geq 100$, held by the pencil of quartics:

$$AZ^4 = X^4 - XY^3.$$

A relative notion:

Let L/K be a field extension, and

$$P(X_1, X_2, \ldots, X_n)$$

a polynomial with coefficients in K (or more generally a system of such polynomials).

A relative notion:

Let L/K be a field extension, and

$$P(X_1, X_2, \ldots, X_n)$$

a polynomial with coefficients in K (or more generally a system of such polynomials).

Say that the polynomial P is **diophantine-stable** for the extension L/K if P acquires no *new* zeroes over L.

or equivalently:

Diophantine Stability

Let V be a variety defined over K. Say that V is **diophantine-stable** *for the extension L/K if*

$$V(K) = V(L).$$

Diophantine Stability and instability phenomena for elliptic curves for towers of number fields

p-cyclotomic towers:

Theorem of Rohrlich, Theorem of Kato

p-anti-cyclotomic towers:
Heegner points

Diophantine stability for curves of genus $g \geq 2$ relative to a fixed cyclic extension of degree ℓ^n

Fix $g \geq 2$, and consider a cyclic Galois extension L/K of degree ℓ^n.

The "$N(g)$ Conjecture" implies:

For $\ell \gg_g 0$ (and all $n \geq 1$)

all but finitely many curves of genus g over K

are Diophantine Stable for L/K.

Diophantine stability for a fixed curve of genus $g \geq 1$ relative to varying cyclic extensions of degree ℓ^n

Theorem

(Joint with Karl Rubin—with an appendix by M.Larsen)

Let X be an irreducible nonsingular projective curve of genus > 0 defined over a number field K. Then

Diophantine stability for a fixed curve of genus $g \geq 1$ relative to varying cyclic extensions of degree ℓ^n

Theorem

(Joint with Karl Rubin—with an appendix by M.Larsen)

Let X be an irreducible nonsingular projective curve of genus > 0 defined over a number field K. Then

- *there is a finite extension K'/K and a set of rational primes S of positive density such that for any positive integer n, and for all $\ell \in S$,*

Diophantine stability for a fixed curve of genus $g \geq 1$ relative to varying cyclic extensions of degree ℓ^n

Theorem

(Joint with Karl Rubin—with an appendix by M.Larsen)

Let X be an irreducible nonsingular projective curve of genus > 0 defined over a number field K. Then

- *there is a finite extension K'/K and a set of rational primes S of positive density such that for any positive integer n, and for all $\ell \in S$,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $X(K') = X(L)$.*

Diophantine stability for (absolutely) simple abelian varieties

Theorem

(Joint with Karl Rubin)

Let A be an absolutely simple abelian variety over a number field K. Assume all endomorphisms of A are defined over K. Then

Diophantine stability for (absolutely) simple abelian varieties

Theorem

(Joint with Karl Rubin)

Let A be an absolutely simple abelian variety over a number field K. Assume all endomorphisms of A are defined over K. Then

- *there is a set of rational primes S of positive density such that for any positive integer n, and for all $\ell \in S$,*

Diophantine stability for (absolutely) simple abelian varieties

Theorem
(Joint with Karl Rubin)

Let A be an absolutely simple abelian variety over a number field K. Assume all endomorphisms of A are defined over K. Then

- *there is a set of rational primes S of positive density such that for any positive integer n, and for all $\ell \in S$,*
- *there are infinitely many cyclic extension fields L/K of degree ℓ^n such that $A(K) = A(L)$.*

The menu

1. A typical further question
2. An application
3. Methods

A typical further question

For *any* abelian variety A over a number field K, simple or not,

and for $\ell \gg_{A/K} 0$, and any positive integer n,

is A diophantine stable for infinitely many cyclic extensions L/K of degree ℓ^n**?**

A typical further question

For *any* abelian variety A over a number field K, simple or not,

and for $\ell \gg_{A/K} 0$, and any positive integer n,

is A diophantine stable for infinitely many cyclic extensions L/K of degree ℓ^n**?**

(Or even for a set of cyclic extensions L/K of degree ℓ^n of "density 1"?)

Elliptic curves over $\mathbf{Q}$

When A is an elliptic curve over $\mathbf{Q}$ can we replace $\ell \gg 0$ in the above question by $\ell > 5$?

Discuss computations of David-Fearnley-Kisilevsky of statistics for $L(E, \chi, 1)$ guided by random matrix heuristics.

Applications of diophantine stability results for elliptic curves to Hilbert's Tenth Problem

To transport *diophantine undecidability* from the ring of integers of one field K to the ring of integers of a larger field L one uses the existence of elliptic curves that

- possess rational points of infinite order over the smaller field K, and
- are diophantine-stable for the extension L/K.

A Bootstrap Method

A Bootstrap Method

Starting with the classical work of Matiyasevich:

There is no finite algorithm to determine whether polynomials with coefficients in the ring $A = \mathbf{Z}$ have solutions in A,

try to work your way up towers of number fields, to "transport" the same negative result for $A =$ the rings of integers in those number fields.

Transporting diophantine definitions of rings of integers

(Using work of Cornelissen-Pheidas-Zahidi, Poonen, Shlapentokh, Eisentrager.)

Let $K \subset L$ be number fields. If there exists an elliptic curve E over K having **(a)** infinitely many rational points over K

and

(b) the diophantine-stability property for the extension L/K:

$$E(K) = E(L),$$

Transporting negative solutions to Hilbert's Tenth Problem

then there exists a a diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$.
In particular, if Hilbert's Tenth Problem has a negative answer for $\mathcal{O}_K$ it also has a negative answer for $\mathcal{O}_L$.

Finitely generated commutative rings

Using this work, and diophantine stability results, Karl Rubin and I showed:

Corollary 1: Conditional on the 2-primary part of the Shafarevich-Tate Conjecture, Hilbert's Tenth problem has a negative answer for any commutative ring A that is of infinite cardinality, and is finitely generated over $\mathbf{Z}$.

Uncountably many fields of algebraic numbers

and combining our results with those of Alexandra Shlapentokh we showed (unconditionally):

Corollary 2: Let p be any prime number (or ∞).

There are uncountably many subfields K of the field of algebraic numbers in $\mathbf{Q}_p$ in which:

*there is a *first order definition* of* $\mathbf{Z}$ *in* K.

(The first-order theory for any such field K—and for its ring of algebraic numbers—is undecidable.)

The Method

The Method

Selmer groups in the relative context

The Method

Selmer groups in the relative context

Let

- ℓ be a rational prime,
- A be a simple abelian variety over a number field K such that all of its endomorphisms are defined over K,
- λ a prime ideal dividing ℓ in the center of the ring of endomorphisms of A,
- L/K any cyclic extension of ℓ-power order,

The Selmer group relative to L/K

We define a subgroup of the cohomology group $H^1(K, A[\lambda])$ by imposing certain 'local conditions' on cohomology classes in $H^1(K, A[\lambda])$.
These 'local conditions' are related to the specific extension L/K but are all imposed on this same cohomology group: $H^1(K, A[\lambda])$.

$$\begin{array}{ccc} \mathrm{Sel}_\lambda(A; L/K) & \subset & H^1(K, A[\lambda]) \\ | & & | \\ \text{finite dimensional} & & \text{infinite dimensional} \end{array}$$

Relative Selmer giving a criterion implying Diophantine Stability

Let A be an abelian variety over K. Then:

For $\ell \gg 0$, and λ a prime above ℓ in the field of fractions of the center of the endomorphism ring of A, then:

$S_\lambda(A; L/K) = 0$ implies that A is diophantine-stable for the extension L/K.

Dirichlet characters and cyclic extensions

A Dirichlet character over K of order ℓ^n cuts out a cyclic extension L/K of degree ℓ^n. We will keep our eye on the Relative Selmer group as it changes as we move from one cyclic extension, L/K, of degree ℓ^n to sequence of other cyclic extensions. We make our moves by suitably multiplying the character χ that cuts out L/K by an appropriate product of local characters to obtain these other cyclic extensions:

$$L_1/K, L_2/K, L_3/K \ldots$$

We keep track of the changes in the 'local conditions' that define the relative Selmer groups as we pass from one cyclic extension L/K to another.

The fundamental glue

For any cyclic extension L/K of degree ℓ^n, the relative Selmer group lies in the same

$$H^1(K, A[\lambda]),$$

I.e., the ambient Galois cohomology group is independent of the extension L/K,

The fundamental glue

For any cyclic extension L/K of degree ℓ^n, the relative Selmer group lies in the same

$$H^1(K, A[\lambda]),$$

I.e., the ambient Galois cohomology group is independent of the extension L/K,

but the twisted Selmer subgroup is defined by local conditions that are specifically related to the extension L/K.

Negotiating smaller Selmer rank

The method, at this point, is to start with one cyclic extension L_0/K and modify the character χ_0 cutting it out so as to change the local conditions (sequentially) in a way that defines a sequence of cyclic extension L_i/K whose relative Selmer groups have smaller and smaller dimensions (over $\mathbf{F}_\ell$). Ultimately, we want to get a profusion of such L/K's with trivial relative Selmer groups.

silent primes and **critical primes**

There is a fundamental—but easy to describe—requirement for this technique to work:

silent primes and critical primes

There is a fundamental—but easy to describe—requirement for this technique to work:

the existence (for $\ell \gg 0$) of what we call **critical elements** and **silent elements** in the Galois group $Gal(\bar{K}/K)$ relative to its action on $A[\lambda]$.

Discuss.

Work of Faltings, Serre, Nori, Pink, Larsen

Theorem: (M. Larsen) Let A be an absolutely simple abelian variety over a number field K. Assume the endomorphism ring of A (over $\mathbf{C}$) is defined over K. Let $R := \mathrm{End}(A)$.

There exists a positive density set of primes ℓ for which for λ a place of the center of R above ℓ has the property that $\mathrm{Gal}(\bar{K}/K)$ contains:

1. **"Silent elements":** there exist elements $g_0 \in \mathrm{Gal}(\bar{K}/K^{\mathrm{ab}})$ possessing no nontrivial fixed vectors in their action on $A[\lambda]$; and

2. **"Critical elements":** there exist elements $g_1 \in \mathrm{Gal}(\bar{K}/K^{\mathrm{ab}})$ such that the fixed subspace of the action of g_1 on $A[\lambda]$ is a nontrivial simple R-module.

.

Existence of critical elements, given the existence of silent elements

Proposition (M. Larsen)
For every positive integer n, there exists a positive integer N such that if ℓ is a prime congruent to 1 (mod N), G is a simply connected, split semisimple algebraic group over $\mathbf{F}_\ell$, and $\rho\colon G(\mathbf{F}_\ell) \to \mathrm{GL}_n(\mathbf{F}_\ell)$ is an almost faithful absolutely irreducible representation such that $(\mathbf{F}_\ell^n)^{\rho(g_0)} = (0)$ for some $g_0 \in G(\mathbf{F}_\ell)$, then there exists $g_1 \in G(\mathbf{F}_\ell)$ such that

$$\dim(\mathbf{F}_\ell^n)^{\rho(g_1)} = 1.$$

(Often one finds the appropriate element g_1 in the image of a principal homomorphism of $\mathbf{SL}_2$ into G.)

Remarks on the existence of silent elements

This uses the work of Richard Pink on classification of Galois actions related to weak Mumford-Tate types with weights $0, 1$.

A Corollary:

Let $p \geq 23$ and $p \neq 37; 43; 67; 163$. Then uncountably many subfields F in $\mathbf{Q}^{\mathrm{alg}}$ have the property that no elliptic curve defined over F possesses an F-rational subgroup of order p.