The Menu

(1) Hilbert's Tenth Problem and Diophantine Stability

(2) Logic related to Elliptic Curves and their rational points

(3) **Results and Methods**

Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K of genus > 0. Then there is a finite extension K'/K such that for any positive integer n,

Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K of genus > 0. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*

Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K of genus > 0. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $X(K') = X(L)$.*

Diophantine stability for absolutely irreducible abelian varieties

Theorem

Let A be an absolutely irreducible abelian variety over a number field K. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*

Diophantine stability for absolutely irreducible abelian varieties

Theorem

Let A be an absolutely irreducible abelian variety over a number field K. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $A(K') = A(L)$.*

Diophantine stability for absolutely irreducible abelian varieties

Theorem

Let A be an absolutely irreducible abelian variety over a number field K. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $A(K') = A(L)$.*

If the Endomorphism ring of A over $\mathbf{C}$ is $\mathbf{Z}$, then one can take $K' = K$. (E.g., elliptic curves with no CM)

Selmer groups and Descent for elliptic curves

The standard method—perhaps the only fully proved method—of finding upper bounds for

$$r(E, K) := \operatorname{rank} E(K)$$

for specific elliptic curves E over specific number fields K (or for the corresponding problem for abelian varieties) is

the method of descent

already present in some arguments due to Fermat and has been elaborated and refined ever since.

Selmer groups

These days "descent" is done via computation of what are called

Selmer groups

.

These computations are 'elementary' in the sense that its ingredients are hardly anything more than group cohomology and basic algebraic number theory.

The "shape" of the descent method as it has evolved in present times

(Class Field Theory reduces determination of the Selmer groups we will deal with to) clearcut finite computations.

I'll explain it first for elliptic curves when the base field K is the rational field $\mathbf{Q}$, and then discuss the differences that one encounters looking for diophantine stability in general field-extensions and for general abelian varieties.

Selmer groups for elliptic curves over $\mathbf{Q}$

To illustrate the method, fix an elliptic curve E over $\mathbf{Q}$ and a prime ℓ.

The basic exact sequence of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules we deal with given by multiplication by ℓ,

$$0 \to E[\ell] \to E(\bar{\mathbf{Q}}) \xrightarrow{\times \ell} E(\bar{\mathbf{Q}}) \to 0$$

Mordell-Weil connected to cohomology

Passing to the cohomology of

$$0 \to E[\ell] \to E(\bar{\mathbf{Q}}) \xrightarrow{\times \ell} E(\bar{\mathbf{Q}}) \to 0$$

gives us an injection

$$E(\mathbf{Q})/\ell E(\mathbf{Q}) \hookrightarrow H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell]).$$

Bounding Mordell-Weil rank via cohomology by trying to close in on the subspace $E(\mathbf{Q})/\ell E(\mathbf{Q})$

$$\underset{\text{what we want to bound}}{E(\mathbf{Q})/\ell E(\mathbf{Q})} \quad \hookrightarrow \quad \underset{\text{infinite dimensional}}{H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])}$$

The $\mathbf{F}_\ell$-vector space

$$H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$$

is infinite dimensional, and we want to encapsule that subspace $E(\mathbf{Q})/\ell E(\mathbf{Q})$ thereby bounding the Mordell-Weil rank of E over $\mathbf{Q}$.

Locally at a prime p

Locally, over $\mathbf{Q}_p$ for any prime p we have the same cohomological story,

$$E(\mathbf{Q}_p)/\ell E(\mathbf{Q}_p) \hookrightarrow H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[\ell]).$$

and the global and local pictures fit neatly together:

$$\begin{array}{ccccc} E(\mathbf{Q})/\ell E(\mathbf{Q}) & \hookrightarrow & \{\text{inverse image}\}_p & \hookrightarrow & H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell]) \\ & & \downarrow & & \downarrow \\ & & E(\mathbf{Q}_p)/\ell E(\mathbf{Q}_p) & \longrightarrow & H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[\ell]) \end{array}$$

Local conditions at primes p

In particular, for each prime p we have a natural 'local condition':

the vector subspace

$$E(\mathbf{Q})/\ell E(\mathbf{Q}) \quad \subset \quad H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$$

is contained in "$\{$inverse image$\}_p$," the inverse image in $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$ of the vector subspace

$$E(\mathbf{Q}_p)/\ell E(\mathbf{Q}_p) \subset \quad H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[\ell]).$$

Using this local information at *all* primes p

It is natural, then to try to at least approximately 'cut out' the subspace $E(\mathbf{Q})/\ell E(\mathbf{Q})$ by using all this local information together. That is the purpose of the *Selmer group*, $S_\ell(E)$.

Definition: $S_\ell(E) \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$ is the intersection *over all primes p* of the inverse images

$$\{\text{inverse image}\}_p \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$$

of the subspaces $E(\mathbf{Q}_p)/\ell E(\mathbf{Q}_p) \subset \ H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[\ell])$.

Using this local information at *all* primes p

It is natural, then to try to at least approximately 'cut out' the subspace $E(\mathbf{Q})/\ell E(\mathbf{Q})$ by using all this local information together. That is the purpose of the *Selmer group*, $S_\ell(E)$.

Definition: $S_\ell(E) \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$ is the intersection *over all primes p* of the inverse images

$$\{\text{inverse image}\}_p \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$$

of the subspaces $E(\mathbf{Q}_p)/\ell E(\mathbf{Q}_p) \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[\ell])$.

$$S_\ell(E) = \cap_p \{\text{inverse image}\}_p \subset H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell]).$$

Local conditions at primes p

What we have done, then, is to impose a **local condition** for each prime p: that the cohomology classes giving elements of the Selmer group reduce to specific subgroups in local cohomology.

The subgroups themselves will be called "local conditions."

The Selmer group is the subgroup consisting of all cohomology classes in this infinite dimensional vector space $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$ that satisfies **all these local conditions**.

These are 'natural' local conditions at primes p *attached to the elliptic curve* E

Let us call these local conditions our **base local conditions**.

BUT nothing stops us from *defining* 'Selmer groups' by the same process, but starting with any local conditions we want—*tweaked Selmer groups* so to speak.

We will eventually do this, modifying—at finitely many primes—our original base local conditions.

Key Conjectures

The base Selmer group $S_\ell(E)$ is a computable finite dimensional $\mathbf{F}_\ell$ vector space

$$E(\mathbf{Q})/\ell E(\mathbf{Q}) \quad \hookrightarrow \quad S_\ell(E)$$

about which we have these conjectures:

Key Conjectures

The base Selmer group $S_\ell(E)$ is a computable finite dimensional $\mathbf{F}_\ell$ vector space

$$E(\mathbf{Q})/\ell E(\mathbf{Q}) \quad \hookrightarrow \quad S_\ell(E)$$

about which we have these conjectures:

- Conjecture:
$$\dim_{\mathbf{F}_\ell} E(\mathbf{Q})/\ell E(\mathbf{Q}) \equiv \dim_{\mathbf{F}_\ell} S_\ell(E) \mod 2.$$

Key Conjectures

The base Selmer group $S_\ell(E)$ is a computable finite dimensional $\mathbf{F}_\ell$ vector space

$$E(\mathbf{Q})/\ell E(\mathbf{Q}) \quad \hookrightarrow \quad S_\ell(E)$$

about which we have these conjectures:

- Conjecture:
$$\dim_{\mathbf{F}_\ell} E(\mathbf{Q})/\ell E(\mathbf{Q}) \equiv \dim_{\mathbf{F}_\ell} S_\ell(E) \mod 2.$$
- Conjecture: If $\ell \gg 0$ then:
$$E(\mathbf{Q})/\ell E(\mathbf{Q}) = S_\ell(E).$$

Diophantine stability of Mordell-Weil groups of elliptic curves over cyclic extensions of prime degree $\ell \gg 0$

Fix an elliptic curve E over $\mathbf{Q}$. Then for any finite Galois extension L/K with Galois group G, $E(L)$ (the Mordell-Weil group of E over L) has a natural G-action and

$$E(\mathbf{Q}) = \{x \in E(L) \mid gx = x \text{ for all } g \in G\} = E(L)^G.$$

Diophantine stability of Mordell-Weil groups of elliptic curves over cyclic extensions of prime degree $\ell \gg 0$

Fix an elliptic curve E over $\mathbf{Q}$. Then for any finite Galois extension L/K with Galois group G, $E(L)$ (the Mordell-Weil group of E over L) has a natural G-action and

$$E(\mathbf{Q}) = \{x \in E(L) \mid gx = x \text{ for all } g \in G\} = E(L)^G.$$

(1) To have Diophantine stability one needs that the action of G be trivial.

Equality of ranks of Mordell-Weil groups of elliptic curves over cyclic extensions of prime degree $\ell \gg 0$

(2) To have equality of MW-ranks,

$$\text{rank } E(L) \stackrel{?}{=} \text{rank } E(\mathbf{Q}),$$

one needs that $gx - x$ be a torsion point of E (for all $g \in G$ and $x \in E(L)$).

Equality of ranks of Mordell-Weil groups of elliptic curves over cyclic extensions of prime degree $\ell \gg 0$

(2) To have equality of MW-ranks,

$$\text{rank } E(L) \stackrel{?}{=} \text{rank } E(\mathbf{Q}),$$

one needs that $gx - x$ be a torsion point of E (for all $g \in G$ and $x \in E(L)$).

Observation: If G is a cyclic group of prime order $\ell >> 0$,

$$(\mathbf{1}) \iff (\mathbf{2}).$$

So, for $\ell \gg 0$,

$$E(L) = E(\mathbf{Q}) \quad \Longleftrightarrow \quad E(L) \otimes \mathbf{Q} = E(\mathbf{Q}) \otimes \mathbf{Q}.$$

In particular the χ-component of the representation $E(L) \otimes \mathbf{C}$ must vanish for every nontrivial irreducible character χ of G.

But if the χ-component vanishes for one nontrivial χ it vanishes for all nontrivial characters of G (since the representation is defined over $\mathbf{Q}$ and all nontrivial characters are Galois conjugate over $\mathbf{Q}$).

χ-twisting the ℓ-Selmer group

Exactly as the vanishing of the ℓ-Selmer group of E over $\mathbf{Q}$ guarantees that the MW-rank of E over $\mathbf{Q}$ is trivial,

there is a procedure starting with a nontrivial character,

$$\chi : \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \to \mathbf{F}_\ell^*$$

—using the local characters χ_p attached to χ—

for "changing (a finite number of) the base local conditions" that produced $S_\ell(E)$ so as to produce a subgroup...

. . . so as to produce a subgroup **of** *the same* $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$

that we denote:

$$S_\ell(E,\chi) \;\hookrightarrow\; H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$$

with the key property:

$$S_\ell(E,\chi) = 0 \Longrightarrow \mathrm{rank}\ E(L) = \mathrm{rank}\ E(\mathbf{Q}).$$

Comment on "*the same* $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[\ell])$."

The twisting method

Recall our objective: Given E over $\mathbf{Q}$ to find a cyclic Galois $L/\mathbf{Q}$ of degree $\ell \gg 0$ with no change in MW-rank.

Start:

by taking absolutely any cyclic $L^0/\mathbf{Q}$ of degree ℓ and let χ^0 be any character that cuts it out.

You may be done:

If $S_\ell(E, \chi^0) = 0$, then $\mathrm{rank}\ E(L^0) = \mathrm{rank}\ E(\mathbf{Q})$.

The twisting method

If $S_\ell(E, \chi^0) > 0$ find an appropriate prime p (we'll call it a **critical prime**) which allows you to redefine the local condition at p by twisting by some local character ϵ_p at p so that the correspondingly modified Selmer group with local conditions given by the local characters

$$S_{\{\text{new}\}}: \qquad \{\ldots \chi^0_{p_i}, \ldots \epsilon_p, \ldots \chi^0_{p_j}, \ldots\}$$

has lower dimension.

The game here is to jockey between Selmer groups defined by these local conditions:

$$S_{\{\text{relaxed at p}\}}: \quad \{\ldots \chi^0_{p_i}, \ldots \text{no local condition at } p, \ldots \chi^0_{p_j}, \ldots\}$$

$$S_{\{\text{old}\}}: \quad \{\ldots \chi^0_{p_i}, \ldots \chi_p, \ldots \chi^0_{p_j}, \ldots\}$$

$$S_{\{\text{new}\}}: \quad \{\ldots \chi^0_{p_i}, \ldots \epsilon_p, \ldots \chi^0_{p_j}, \ldots\}$$

$$S_{\{\text{strict}\}}: \quad \{\ldots \chi^0_{p_i}, \ldots \text{the strict local condition at } p, \ldots \chi^0_{p_j}, \ldots\}.$$

Lowering dimension

... to get $\dim S_{\{\text{new}\}} = S_{\{\text{old}\}} - 1$.

Keep going: until you get a vanishing modified twisted Selmer group.

Two obstacles stand in the way of this plan!

(1) Enough *critical* primes p?

Requirements:

1. that p is of good reduction for E and ℓ divides $p-1$ (so far, no problem finding primes of this sort) and that
2. the action of ϕ_p, the Frobenius element at p on the $\mathbf{F}_\ell$-vector space $E[\ell]$ have a *one-dimensional subspace of fixed vectors*; colloquially a 'unique' fixed eigenvector.

Why are such primes p critical?

Here—given some other hypotheses that will obtain when $\ell \gg 0$—we make use of Global Duality to guarantee that between the strictest local condition at p and the most relaxed local condition at p, the corresponding Selmer groups differ in size by one dimension.

Moreover, we engineered our choice of prime p so that

1. $$S_\ell(E, \chi) = S_\ell(E, \chi \text{ away from } p\text{; relaxed at } p)$$
   and
2. these global cohomology groups map onto the one-dimensional Selmer local condition at p.

In this set-up, any change of local condition subgroup at p will

impose a stronger condition on the global classes at p

and therefore changing only the local condition at such a prime p, but keeping to the old local conditions at all the other primes gives a "tweaked global Selmer group" of dimension one less than $\dim S_\ell(E, \chi)$.

(2) Enough *silent* primes p?

In the account we gave, we modified local conditions for the construction of our Selmer group, a single place at a time, to keep lowering dimension. Why, at the end of our process, is there a **global** Dirichlet character whose corresponding local characters give us the local Selmer conditions we end up with? The answer is: there needn't be such: we'll call such non-globalizable systems of local characters "semi-local."

Here is where "silent primes" enter

For $\ell \gg 0$, there are primes $p \equiv 1 \mod \ell$ ($p \neq 2$ and of good reduction for E) such that ϕ_p has no nonzero fixed vectors in its action on $E[\ell]$.

For these primes, the local cohomology group vanishes. We'll call them **silent primes**, for the twisting the local condition at such primes p by any local character at p doesn't change the local condition p at all, and hence doesn't change the Selmer group.

But judicious twisting by silent primes will turn semi-local characters to global ones.

Conclusion for elliptic curves

Theorem

Let E be an elliptic curve with no CM over a number field K. Then for any positive integer n,

1. *there are infinitely many primes ℓ where, for each of them,*
2. *there are infinitely many cyclic extension fields L/K of degree ℓ^n such that $E(K) = E(L)$.*

Now onto absolutely irreducible abelian varieties A over a number field K

The issue of **critical primes** and **silent primes** becomes more delicate in the context of abelian varieties, and we thank Michael Larsen for writing an appendix to our paper that provides what is needed. To make things simple, we'll discuss this in the case when $End(A) = \mathbf{Z}$.

Critical and Silent elements of the Galois group

Theorem: (M. Larsen) If A is an abelian variety over a number field K with $\mathrm{End}_{\bar{K}} A = \mathbf{Z}$, then:
there exists a positive density set of primes ℓ for which:

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 $A[\ell]$; i.e. such that the action of g_0 on $A[\ell]$ has no nontrivial fixed vectors, and
2. **"Critical elements"** there exist elements $g_1 \in \mathrm{Gal}(\bar{K}/K^{\mathrm{ab}})$ such that the action of g_1 on $A[\ell]$ has a *one-dimensional space* of fixed vectors.

.

Cebotarev Density

We apply this theorem, using the Cebotarev density theorem, to find our silent primes and critical primes; i.e., primes such that their corresponding Frobenius elements are silent, or critical elements.

Comments on the proof

Mention Faltings' Theorem. The proof is slightly more involved if $\mathrm{End}_{\bar{K}} A$ is larger than $\mathbf{Z}$, but in the case of $\mathrm{End}_{\bar{K}} A = \mathbf{Z}$ . . .

There are two major steps in the proof:

1. A general proposition (due to M. Larsen) about irreducible representations of simply connected, split semisimple algebraic groups over $\mathbf{F}_\ell$ (for a set of primes ℓ of positive density) establishing the existence of critical elements, *given the existence of silent elements*.

2. Results (due to R. Pink, M. Larsen) on the action of Galois on ℓ-torsion in abelian varieties (for $\ell \gg 0$) and a computation using tables of R. Pink that classify representations of weak Mumford-Tate type that provide the existence of silent elements in the action of Galois on ℓ-torsion in abelian varieties, for infinitely many primes ℓ.

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.)

Step 2: Conclusion

Use the rather detailed classification theorems of representations related to Mumford-Tate pairs; results of Faltings, Nori, Serre, Ribet, Larsen and Pink to get the existence of silent elements, and then Larsen's Proposition to conclude.

Consequence: Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K not of genus 0. Then there is a finite extension K'/K such that for any positive integer n,

Consequence: Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K not of genus 0. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*

Consequence: Diophantine stability for curves

Theorem

Let X be an irreducible nonsingular projective curve over a number field K not of genus 0. Then there is a finite extension K'/K such that for any positive integer n,

- *there are infinitely many primes ℓ where, for each of them,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $X(K') = X(L)$.*