Arithmetic of elliptic curves lecture 2

Brendan Creutz
University of Canterbury
NZMRI Summer Meeting 2021

Rational Points on genus one curves, a summary

Suppose $E/\mathbb{Q}$ is a genus one curve.

Problem 1:

Decide if $E(\mathbb{Q})$ is nonempty.

- Difficult because local obstructions do not suffice.
- One must define new obstructions and study these (Descent, Brauer-Manin)

Problem 2:

If $E(\mathbb{Q})$ is nonempty, the points form a finitely generated abelian group. Determine the structure and find generators.

- Can be reduced to Problem 1 for a finite collection of auxiliary curves: $E(\mathbb{Q}) = \coprod_\delta \pi_\delta(C_\delta(\mathbb{Q}))$.

The proof of Mordell's theorem used a homomorphism

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \longrightarrow \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \times \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}.$$

More generally for any n we have an exact sequence

$$\tfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \hookrightarrow \mathrm{H}^1(\mathbb{Q}, E[n]) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E)$$

- $\mathrm{H}^1(\mathbb{Q}, E)$ paramterizes isomorphism classes of genus one curves together with an algebraic group action of E. Elements are called principal homogeneous spaces PHS.
- The identity element is E acting on itself by translation.
- The nontrivial elements are represented by PHS's that have no rational points.

We now take into account local information:

$$
\begin{tikzcd}
\frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \arrow[r, hook, "\delta"] & \mathrm{H}^1(\mathbb{Q}, E[n]) \arrow[r] \arrow[dr, "\alpha"] & \mathrm{H}^1(\mathbb{Q}, E) \arrow[d, "\beta"] \\
& & \prod_p \mathrm{H}^1(\mathbb{Q}_p, E)
\end{tikzcd}
$$

- $Ш(E/\mathbb{Q}) := \ker(\beta)$ is the Tate-Shafarevich group. It consists of those PHS's with no local obstruction to existence of rational points.
- $\mathrm{Sel}^n(E/\mathbb{Q}) := \ker(\alpha)$ is called the Selmer group. It is finite and computable.

These fit into a famous short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}^n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0$$

A conjectural algorithm

Conjecture (Tate, Shafarevich, Cassels? 1950/60's)

For any elliptic curve the group $\text{Ш}(E/\mathbb{Q})$ is finite.

Theorem

If C is a PHS for E and $\text{Ш}(E/\mathbb{Q})$ is finite, then there is an algorithm to decide if $C(\mathbb{Q}) = \emptyset$.

Sketch of the proof

Search for rational points by day and try to prove there are none by night.

- If C has a local obstruction, then $C(\mathbb{Q}) = \emptyset$.
- If not, then $[C] \in \text{Ш}(E)$. We try to prove $[C] \neq 0$
- For any n one can check if $[C]$ is divisible by n in $\text{Ш}(E)$.
- If $\text{Ш}(E/\mathbb{Q})$ finite and $[C] \neq 0$ we eventually find n such that $[C]$ is not divisible by n.

An element of order 9 in $\text{Ш}(E/\mathbb{Q})$

- $D \subset \mathbb{P}^8$ is the genus one curve given by

$$
\begin{aligned}
0 &= z_2 z_5 - z_5 z_6 + 3z_7^2 + z_7 z_9 + 2z_8^2\,, \\
0 &= z_1 z_2 + z_2 z_6 + z_2 z_7 + z_4 z_9 + z_5 z_7 + 2z_5 z_8\,, \\
0 &= z_1 z_7 - z_2 z_8 - z_4 z_5 - z_5^2 - 2z_6 z_7 - z_6 z_8 + z_7^2\,, \\
&\ \vdots
\end{aligned}
$$

  and 24 other similar looking quadratic equations.

- $C \subset \mathbb{P}^3$ given by $x^3 + 6y^3 + 919 = 53xy$.

- $E\ :\ y^2 + xy = x^3 - 1479474x - 692765778$

Cassels' Question

Dividing by n in $Ш(E)$ is a two step process:

1. Divide by n in the larger group $\mathrm{H}^1(\mathbb{Q}, E)$.
2. Look for "twists" that get you back into $Ш(E/\mathbb{Q})$.

Question (Cassels 1961)

Are the elements of $Ш(E)$ always divisible by n in the larger group $\mathrm{H}^1(\mathbb{Q}, E)$?

Some Answers

$E/\mathbb{Q}$	$n = p$ (prime)	YES	Tate 1963
$E/\mathbb{Q}$	$n = p^r$, $p >> 0$	YES	Bashmakov 1972
$E/\mathbb{Q}$	$n = p^r$, $p > 163$	YES	Dvornicich-Zannier 2007
$E/\mathbb{Q}$	$n = p^r$, $p > 7$	YES	Çiperiani-Stix 2012
$E/\mathbb{Q}$	$n = p^r$, $p > 3$	YES	Paladino-Ranieri-Viada 2014
$E/\mathbb{Q}$	$4 \mid n$ or $9 \mid n$	NO	C. 2013, 2016
$A/\mathbb{Q}$	any integer	NO	C. 2013
$E/\mathbb{F}_p(t)$		YES $\Leftrightarrow 8 \nmid n$	C. & Voloch 2017

Example

- $E : y^2 = x(x+80)(x+205)$
- The curve $C \in Ш(E)$ defined by

$$z_1^2 - 5z_2^2 + 80z_4^2 = 0$$
$$z_1^2 - 5z_3^2 + 205z_4 = 0$$

is not divisible by 4 in $\mathrm{H}^1(E)$.

Example

- $C : 2x^3 + 3y^3 + 23z^3 = 0$ is not divisible by 9 in H^1
- Selmer showed $C \neq 0$ in $Ш$.

Answer to Cassels' Question

- Selmer conjectured that whenever $\text{Ш}(E)$ is finite, its order must be a square.
- Cassels proved this conjecture by establishing the first of many "arithmetic duality theorems": for any integer n there is a nondegenerate alternating bilinear pairing

$$\text{Ш}(E)[n] \times \frac{\text{Ш}(E)}{n\text{Ш}(E)} \to \mathbb{Q}/\mathbb{Z}$$

- My result (when specialized to elliptic curves) gives a compatible nondegenerate pairing

$$\frac{\text{Ш}(E[n])}{E(\mathbb{Q})/n \cap \text{Ш}(E[n])} \times \frac{\text{Ш}(E)}{n\,\mathrm{H}^1(E) \cap \text{Ш}(E)} \to \mathbb{Q}/\mathbb{Z}$$

  allowing us to control divisibility in $\mathrm{H}^1(\mathbb{Q}, E)$.
- The pairing can only be nontrivial if there is a prime p such that $p^2 \mid n$ and the Galois representation on $E[p]$ is contained in S_3 (over $\mathbb{Q}$ only possible when $p = 2$ or 3.)

A conjecture of Lang and Tate

Recall $Ш(E/\mathbb{Q})$ is defined as the kernel of α in

$$0 \to Ш(E/\mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, E) \xrightarrow{\alpha} \bigoplus_{\text{all } p} \mathrm{H}^1(\mathbb{Q}_p, E)$$

What about the image of α?

Theorem (C. 2012)

For any finite set of primes S the map

$$\mathrm{H}^1(\mathbb{Q}, E) \to \prod_{p \in S} \mathrm{H}^1(\mathbb{Q}_p, E)$$

is surjective.

“In analogy with Grunwald’s theorem in class field theory, one may conjecture that if k is an algebraic number field and $\mathfrak{p}$ a given prime, then given $\alpha_{\mathfrak{p}} \in \mathrm{H}^1(k_{\mathfrak{p}}, A)$, there exists $\alpha \in \mathrm{H}^1(k, A)$ restricting to $\alpha_{\mathfrak{p}}$."

– Lang & Tate (1958)

The Brauer-Manin obstruction

- Suppose C is a variety over $\mathbb{Q}$ with no local obstruction. This means there is a compatible system of solutions modulo n for every integer n (called an adelic point).
- An adelic point coming from a rational point must satisfy certain reciprocity laws imposed by the Brauer group of C.
- If no adelic point satisfies these laws then there is no rational point; we say there is a Brauer-Manin obstruction.

Conjecture

Suppose $C/\mathbb{Q}$ is a PHS for an abelian variety such that $C(\mathbb{Q}) = \emptyset$. Then there is a Brauer-Manin obstruction.

- This would give an algorithm to decide on existence of rational points.
- This is implied by finiteness of Ш, but is a priori weaker.

Hilbert Reciprocity

Theorem

A conic with rational coefficients has a local obstruction at a **finite even number** *of primes.*

Example

The conic $x^2 + y^2 = 3$ has local obstructions at the primes $p = 2$ and $p = 3$, but nowhere else.

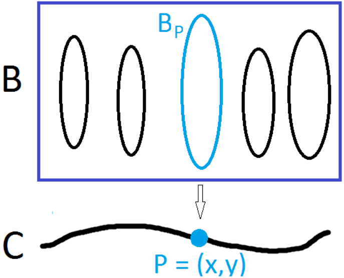
E.g., we have a 5-adic solution:

$$\begin{aligned} 2^2 + 2^2 &\equiv 3 \mod 5 \\ 2^2 + 7^2 &\equiv 3 \mod 25 \\ 2^2 + 57^2 &\equiv 3 \mod 125 \\ &\vdots \end{aligned}$$

Example of a Brauer-Manin obstruction (Reichard/Lind 1940s, C. & Viray 2015)

Consider the curve C and the family $\mathcal{B}$ of conics over C defined by

$$C : y^2 = 2x^4 - 34\,, \qquad \mathcal{B} : yu^2 + 17v^2 = 1$$



- $\mathcal{B}(\mathbb{Q}_{17}) = \emptyset$, i.e., $\mathcal{B}$ has a local obstruction at $p = 17$.
- $\forall\, p \neq 17$ and $P \in C(\mathbb{Q}_p)$, the fiber $\mathcal{B}_P$ has no local obstruction at p.

- Hilbert reciprocity implies there are no rational fibers.
- Hence $C(\mathbb{Q}) = \emptyset$.

Brauer-Manin Obstructions

There is a BM obstruction to rational points on C if:

For every adelic point $P \in V(\mathbb{A})$,
there exists a Brauer class $\mathcal{B}$ such that $\mathcal{B}(P) \neq 0$.

(Distinct Brauer classes might be needed to obstruct distinct adelic points.)

Theorem (C. 2020)

Suppose C is a PHS for an abelian variety with a BM obstruction to existence of rational points. Then there exists a single Brauer class responsible for the obstruction.

(Actually, one well chosen Brauer class will always suffice)

Corollary

Sufficiency of the Brauer-Manin obstruction is equivalent to finiteness of Ш.