Iwasawa Theory and the Birch and Swinnerton-Dyer Conjecture

Antonio Lei (University of Ottawa)

Math Seminar, University of Macau

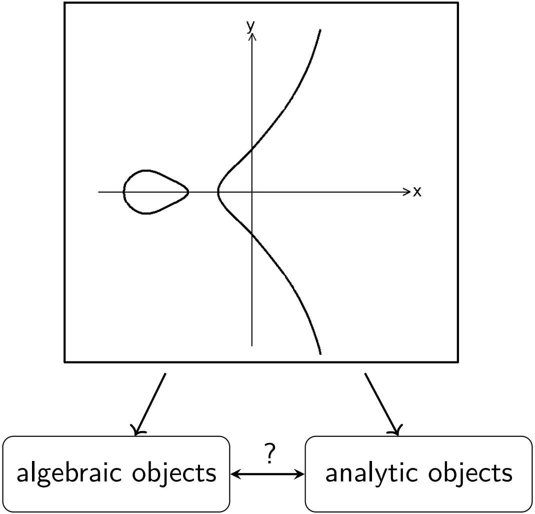
February 18, 2025

https://antoniolei.com/slides/

Outline

Outline

1. Overview of the Birch and Swinnerton-Dyer conjecture
2. Introduction to Iwasawa theory
3. Congruences between modular forms
4. Results on Euler systems and isogeny graphs


y
x
algebraic objects
?
analytic objects

Definition

An elliptic curve over $\mathbb{Q}$ is a projective curve

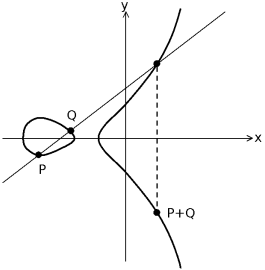
$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in \mathbb{Q}$ with $4a^3 + 27b^2 \neq 0$.

- If K is a field containing $\mathbb{Q}$, we write $E(K)$ for the set of points $(X : Y : Z) \in \mathbb{P}^2(K)$ that lie on E.
- On taking $Z = 0$, we have $X^3 = 0$, so $(0 : 1 : 0) \in E(K)$.
- If $Z = 1$, we have an affine curve $Y^2 = X^3 + aX + b$.

Theorem (Mordell–Weil 1920s)

Let K be a finite extension of $\mathbb{Q}$. Then, $E(K)$ is a finitely generated abelian group with $(0:1:0)$ as the identity.



- $E(K) \cong \mathbb{Z}^{\oplus r_E(K)} \oplus$ (finite group).
- $r_E(K)$ is called the **algebraic rank** of E over K.

- Let p be a prime number and write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- We may define a projective curve over $\mathbb{F}_p$:

$$\overline{E} : Y^2Z = X^3 + \overline{a}XZ^2 + \overline{b}Z^3.$$

- The set $\overline{E}(\mathbb{F}_p)$ is finite, its size is given by

$$\#\overline{E}(\mathbb{F}_p) = 1 + p - a_p,$$

where $a_p = -\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)$.

- There is a natural reduction map $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$.
- We expect that $\#\overline{E}(\mathbb{F}_p)$ should reflect $r_E(\mathbb{Q})$.

- For $s \in \mathbb{C}$ with $\Re(s) > 3/2$, define

$$L(E,s) = \prod_{p \nmid N_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \mid N_E} \frac{1}{1 - a_p p^{-s}}.$$

- This converges absolutely and has analytic continuation to $\mathbb{C}$.
- The **analytic rank** of E over $\mathbb{Q}$ is $\operatorname{ord}_{s=1} L(E,s)$.
- At $s = 1$,

$$\frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \frac{p}{\#\overline{E}(\mathbb{F}_p)}.$$

$$\boxed{\text{algebraic objects}} \overset{?}{\longleftrightarrow} \boxed{\text{analytic objects}}$$

Conjecture (Birch and Swinnerton-Dyer 1960s)

Given an elliptic curve $E/\mathbb{Q}$, we have

$$\textbf{\textit{algebraic rank}} = \textbf{\textit{analytic rank}}$$
$$r_E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E, s).$$

Furthermore, the leading term of the Taylor expansion of $L(E, s)$ at $s = 1$ is related to algebraic quantities.

Outline

- Study arithmetic properties over a tower of field extensions.
- Study arithmetic objects using local fields via auxiliary primes.
- Seek "p-adic" links between

$$\boxed{\text{algebraic objects}} \longleftrightarrow \boxed{\text{analytic objects}}$$

Cyclotomic extensions

Fix a prime p and consider a tower of fields :

$$
\begin{array}{ccc}
K_\infty := \mathbb{Q}(\mu_{p^\infty}) & & E(K_\infty) \\
\cup & & \cup \\
\vdots & & \vdots \\
\cup & & \cup \\
\mathbb{Q}(e^{2\pi i/p^2}) & \rightsquigarrow & E\left(\mathbb{Q}(e^{2\pi i/p^2})\right) \\
\cup & & \cup \\
\mathbb{Q}(e^{2\pi i/p}) & & E\left(\mathbb{Q}(e^{2\pi i/p})\right) \\
\cup & & \cup \\
\mathbb{Q} & & E(\mathbb{Q})
\end{array}
$$

algebraic tool
(control theorem
for Selmer groups)

Definition

The p-**adic norm** on $\mathbb{Z}$ is given by

$$|p^n \times a|_p = p^{-n} \quad \text{if } a, n \in \mathbb{Z} \text{ and } p \nmid a.$$

Definition

The ring of p-**adic integers**, $\mathbb{Z}_p$, is the completion of $(\mathbb{Z}, |\bullet|_p)$.

- Explicitly, $\mathbb{Z}_p = \{\sum_{n=0}^{\infty} x_n p^n : x_n \in \{0, 1, \ldots p-1\}\}$.
- $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$.

- For each extension $K/\mathbb{Q}$, we can define a p-adic Selmer group $\mathcal{X}(E/K)$ using Galois cohomology.
- $\mathcal{X}(E/K)$ is a $\mathbb{Z}_p$-module and $r_E(K) \leq \mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}(E/K)$.

Theorem (Mazur 1970s)

Assume E has good ordinary reduction at p. There is a homomorphism

$$H_0\left(\mathrm{Gal}(K_\infty/\mathbb{Q}), \mathcal{X}(E/K_\infty)\right) \to \mathcal{X}(E/\mathbb{Q})$$

whose kernel and cokernel have finite cardinalities.

Control theorem :

$$\begin{tikzcd}
E(K_\infty) & & \mathcal{X}(E/K_\infty) \arrow[d] \arrow[dddddddd, bend left=60, "H_0(\mathrm{Gal}(K_\infty/\mathbb{Q}),-)"] \\
\cup & & {} \\
\vdots & & \vdots \arrow[d] \\
\cup & & {} \\
E(\mathbb{Q}(e^{2\pi i/p^2})) & \rightsquigarrow & \mathcal{X}(E/\mathbb{Q}(e^{2\pi i/p^2})) \arrow[d] \\
\cup & & {} \\
E(\mathbb{Q}(e^{2\pi i/p})) & & \mathcal{X}(E/\mathbb{Q}(e^{2\pi i/p})) \arrow[d] \\
\cup & & {} \\
E(\mathbb{Q}) & & \mathcal{X}(E/\mathbb{Q})
\end{tikzcd}$$

- Let $\Lambda = \mathbb{Z}_p[[X]]$ be the ring of power series

$$\left\{ \sum_{n=0}^{\infty} c_n X^n : c_n \in \mathbb{Z}_p \right\}.$$

- If M is a finitely generated torsion Λ-module, there is a pseudo-isomorphism

$$M \sim \bigoplus_{i=1}^{r} \Lambda/(f_i), \quad \text{where } f_i \in \Lambda.$$

- We define the **characteristic ideal** of M by

$$\mathrm{Char}\, M = \left(\prod_{i-1}^{r} f_i \right).$$

Theorem (Kato 1990s)

Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Then $\mathcal{X}(E/K_\infty)$ is a finitely generated torsion Λ-module.

Combined with the control theorem :

Corollary

$r_E(\mathbb{Q})$ is bounded by the multiplicity of X in $\operatorname{Char}\mathcal{X}(E/K_\infty)$.

Question

Is it possible to relate $\operatorname{Char}\mathcal{X}(E/K_\infty)$ to an analytic object ?

p-adic L-functions

Theorem (Mazur–Swinnerton-Dyer 1970s)

There exists a p-adic analogue of $L(E,s)$, namely $L_p(E,X) \in \Lambda$ satisfying the interpolation properties

$$L_p(E,\zeta-1) = (\star) \times L(E,\zeta) \text{ if } \zeta^{p^n} = 1.$$

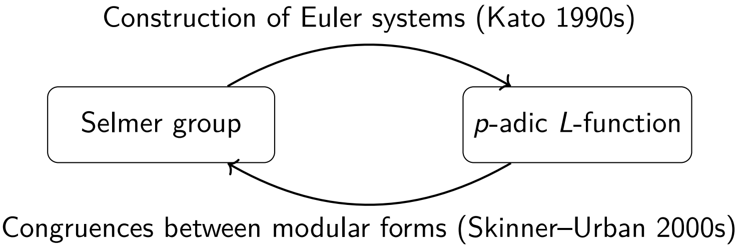
- Relies on links between elliptic curves and modular forms.
- Modularity theorem was proved by Wiles and Taylor–Wiles in 1990s.
- $L_p(E,X)$ can be calculated numerically on a computer.

Conjecture (The Iwasawa main conjecture)

Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Then

$$\mathrm{Char}\,\mathcal{X}(E/K_\infty) = (L_p(E,X)).$$

- Under certain technical hypotheses, this is known.



Example

Let $E : y^2 = x^3 + 1/4$.

$$\begin{tikzcd}
\boxed{L_7(E,X) \in \Lambda^\times} \arrow[d, "\text{Iwasawa main conjecture}"'] & \\
\boxed{\mathcal{X}(E/K_\infty) \text{ is finite for } p = 7} \arrow[r, bend right, "\text{Control Theorem}"'] & \boxed{E(\mathbb{Q}) \text{ is finite}}
\end{tikzcd}$$

- In fact, $E(\mathbb{Q}) = \{\infty, (0, 1/2), (0, -1/2)\} \cong \mathbb{Z}/3\mathbb{Z}$.
- The Birch and Swinnerton-Dyer conjecture holds for E since

$$r_E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E, s) = 0.$$

Outline

- The Ramanujan tau function $\tau : \mathbb{N} \to \mathbb{N}$ is defined by

$$\sum_{n\geq 1} \tau(n)q^n = q\prod_{n\geq 1}(1-q^n)^{24}.$$

- If we put $q = e^{2\pi iz}$, $z \in \mathbb{C}$ with $\Im(z) > 0$,

$$\Delta(z) = \sum_{n\geq 1} \tau(n)e^{2\pi inz}$$

  is a modular form.

- Several arithmetic properties of τ observed by Ramanujan can be explained by the theory of modular forms.

- $\tau(p) \equiv 1 + p \pmod{\ell}$, $\ell \in \{2, 3\}$.
- $\tau(p) \equiv p + p^2 \pmod{5}$.
- $\tau(p) \equiv p + p^4 \pmod{7}$.

Theorem (Deligne 1960s)

If $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$ is a modular form, then there exists a $\mathbb{Z}_\ell$-module T_f and a representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(T_f)$$

such that $a_p = \mathrm{trace}\, \rho_f(\mathrm{Frob}_p)$.

Remark

Swinnerton-Dyer (1970's) studied congruences of $\tau(p)$ via ρ_Δ.

- Given an elliptic curve E, recall

$$L(E,s)=\prod_{p\nmid N_E}\frac{1}{1-a_pp^{-s}+p^{1-2s}}\prod_{p\mid N_E}\frac{1}{1-a_pp^{-s}}=\sum_{n\geq 1}a_nn^{-s}.$$

- The modularity theorem of Wiles and Taylor–Wiles says that

$$f_E(z)=\sum a_ne^{2\pi inz}$$

is a modular form.

- If E is the elliptic curve $y^2 = x^3 + 1/4$, then $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.
- $\#\overline{E}(\mathbb{F}_p) \equiv 0 \pmod 3$.
- $a_p = 1 + p - \#\overline{E}(\mathbb{F}_p) \equiv 1 + p \equiv \tau(p) \pmod 3$.
- $f_E(z) \equiv \Delta(z) \pmod 3$.

Theorem (Greenberg–Vatsal 2000)

If $f_1(z) \equiv f_2(z) \pmod p$ are modular forms that are good ordinary at p, then :

$$L_p(f_1, X) \equiv L_p(f_2, X) \pmod{p\Lambda},$$

$$\mathcal{X}(f_1/K_\infty)/p \cong \mathcal{X}(f_2/K_\infty)/p.$$

Outline

$$\begin{tikzcd} \text{Selmer group} \arrow[rr, bend left, "\text{Construction of Euler systems}"] & & p\text{-adic } L\text{-function} \arrow[ll, bend left, "\text{Congruences between modular forms}"] \end{tikzcd}$$

Definition

Let T be a $\mathbb{Z}_p$-module equipped with a continuous $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.

An **Euler system** for T is a collection of cohomology classes

$$\left\{ c_n \in H^1(\mathbb{Q}(\mu_n), T) : \ n = mp^r, \ m \text{ square-free and } p \nmid m \right\},$$

satisfying some norm relations as n varies.

$$\cdots\cdots\cdots$$

$$\begin{tikzcd}
\mathbb{Q}(\mu_{6p^\infty}) \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\mu_{10p^\infty}) \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Q}(\mu_{15p^\infty}) \arrow[dl, dash] \arrow[d, dash] & \cdots & \mathbb{Q}(\mu_{rqp^\infty}) \arrow[d, dash] \\
\mathbb{Q}(\mu_{2p^\infty}) \arrow[drr, dash] & \mathbb{Q}(\mu_{3p^\infty}) \arrow[dr, dash] & \mathbb{Q}(\mu_{5p^\infty}) \arrow[d, dash] & \cdots & \mathbb{Q}(\mu_{qp^\infty}) \arrow[dll, dash] \\
& & \mathbb{Q}(\mu_{p^\infty}) & &
\end{tikzcd}$$

Theorem (Kato 2004)

If $T = T_f$ arises from a modular form f, there exists a non-trivial Euler system attached to T_f.

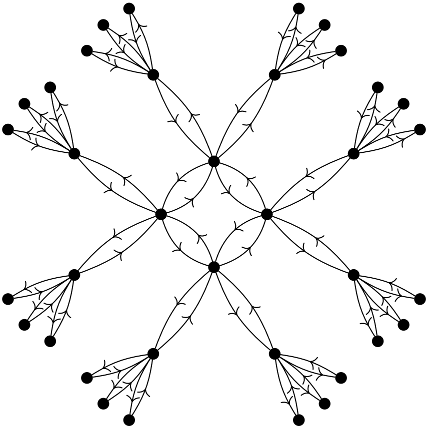
- This Euler systems has been used to prove BSD when $\mathrm{ord}_{s=1} L(E,s) \in \{0,1\}$.

Theorem (L.–Loeffler–Zerbes 2014)

Let f and g be weight-two modular forms with good ordinary reduction at p. There exists a non-trivial Euler system attached to $T_f \otimes T_g$.

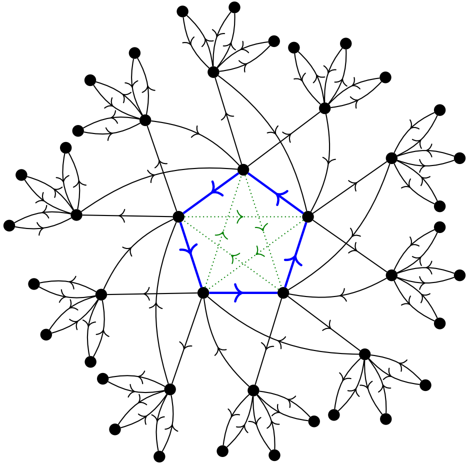
- This Euler system gives one inclusion of the Iwasawa main conjecture for the tensor product motives of f and g.

Given a set of elliptic curves over a finite field, we can define an isogeny graph :

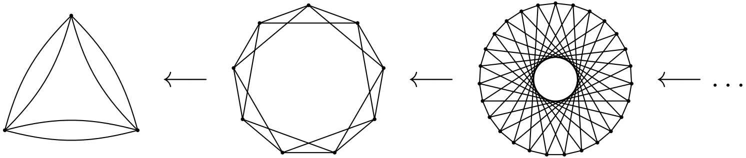


Vertices = elliptic curves, Edges = isogeny between two curves

We can enhance these graphs with a level structure so that the vertices represent (E, P), P some arithmetic data of E.



Similar to field extensions, we can "increase" the level to obtain a tower of graphs :



- The analogue of the Selmer group is the Jacobian, which counts the number of spanning trees.
- There is a p-adic L-function attached to the tower.
- There is an "Iwasawa main conjecture" linking these objects.