Euler characteristics in Iwasawa theory and their congruences

Anwesh Ray

University of British Columbia

anweshray@math.ubc.ca

March 10, 2021

- Let p be a prime number.

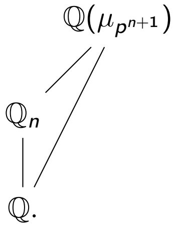
- Let p be a prime number.
- Iwasawa theory is concerned with the structure of certain Galois modules arising from arithmetic.

- Let p be a prime number.
- Iwasawa theory is concerned with the structure of certain Galois modules arising from arithmetic.
- These modules are defined over certain infinite Galois extensions of $\mathbb{Q}$.

The Cyclotomic $\mathbb{Z}_p$-extension

The Cyclotomic $\mathbb{Z}_p$-extension

- Let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n$ as depicted



- The tower of number fields $\mathbb{Q} = \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \dots$ is called the cyclotomic tower.

- The tower of number fields $\mathbb{Q} = \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \ldots$ is called the cyclotomic tower.
- The field $\mathbb{Q}_{\mathrm{cyc}}$ is taken to be the union

$$\mathbb{Q}_{\mathrm{cyc}} := \bigcup_{n \geq 1} \mathbb{Q}_n.$$

The Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p$.

Early Investigations

Early Investigations

- Iwasawa's early ivestigations led him to study the variation of p-class groups of $\mathbb{Q}_n$ as $n \to \infty$.

Early Investigations

- Iwasawa's early ivestigations led him to study the variation of p-class groups of $\mathbb{Q}_n$ as $n \to \infty$.
- For $n \geq 1$, set $\mathcal{A}_n$ to denote the p-primary part of the class group of $\mathbb{Q}_n$

$$\mathcal{A}_n := \mathrm{Cl}(\mathbb{Q}_n)[p^\infty].$$

Early Investigations

- Iwasawa's early ivestigations led him to study the variation of p-class groups of $\mathbb{Q}_n$ as $n \to \infty$.
- For $n \geq 1$, set $\mathcal{A}_n$ to denote the p-primary part of the class group of $\mathbb{Q}_n$
$$\mathcal{A}_n := \text{Cl}(\mathbb{Q}_n)[p^\infty].$$
- Iwasawa showed that there are invariants $\mu, \lambda, \nu \geq 0$ such that
$$\#\mathcal{A}_n = p^{\mu p^n + \lambda n + \nu}$$
for large values of n.

Iwasawa's approach

Iwasawa's approach

- There are natural maps $\mathcal{A}_{n+1} \rightarrow \mathcal{A}_n$ and the inverse limit $\mathcal{A}_\infty := \varprojlim_n \mathcal{A}_n$ is a module over $\Gamma := \operatorname{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$.

Iwasawa's approach

- There are natural maps $\mathcal{A}_{n+1} \to \mathcal{A}_n$ and the inverse limit $\mathcal{A}_\infty := \varprojlim_n \mathcal{A}_n$ is a module over $\Gamma := \text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$.
- Iwasawa introduced the completed algebra $\Lambda := \varprojlim_n \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_n/\mathbb{Q})] \simeq \mathbb{Z}_p[[x]]$.

Iwasawa's approach

- There are natural maps $\mathcal{A}_{n+1} \rightarrow \mathcal{A}_n$ and the inverse limit $\mathcal{A}_\infty := \varprojlim_n \mathcal{A}_n$ is a module over $\Gamma := \text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$.
- Iwasawa introduced the completed algebra $\Lambda := \varprojlim_n \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_n/\mathbb{Q})] \simeq \mathbb{Z}_p[[x]]$.
- He showed that $\mathcal{A}_\infty$ is a finitely generated torsion $\mathbb{Z}_p[[x]]$-module and his theorem is a consequence of the structure theory of such modules.

Iwasawa theory of Elliptic Curves

Iwasawa theory of Elliptic Curves

- Greenberg and Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$.

Iwasawa theory of Elliptic Curves

- Greenberg and Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$.
- Throughout, we let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p.

Iwasawa theory of Elliptic Curves

- Greenberg and Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$.
- Throughout, we let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p.
- They studied the variation of Selmer groups as one goes up the tower.

Some notation

Some notation

- For any abelian group M, set $M[p^n] := \ker(M \xrightarrow{p^n} M)$ and $M[p^\infty] := \bigcup_{n\geq 1} M[p^n]$.

Some notation

- For any abelian group M, set $M[p^n] := \ker(M \xrightarrow{p^n} M)$ and $M[p^\infty] := \bigcup_{n\geq 1} M[p^n]$.
- The group $E[p^\infty]$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ equipped with an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Selmer groups

Selmer groups

- For each number field extension F of $\mathbb{Q}$, the Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$ consists of Galois cohomology classes

$$f \in H^1(\bar{F}/F, E[p^\infty])$$

satisfying suitable local conditions.

Selmer groups

- For each number field extension F of $\mathbb{Q}$, the Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$ consists of Galois cohomology classes

$$f \in H^1(\bar{F}/F, E[p^\infty])$$

satisfying suitable local conditions.

- It fits into a short exact sequence

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)[p^\infty] \to 0.$$

Selmer groups

Selmer groups

- The Selmer group over $\mathbb{Q}_{\text{cyc}}$ is taken to be the direct limit

$$\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}) := \varinjlim_n \operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_n).$$

Selmer groups

- The Selmer group over $\mathbb{Q}_{\text{cyc}}$ is taken to be the direct limit

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}) := \varinjlim_n \text{Sel}_{p^\infty}(E/\mathbb{Q}_n).$$

- The Pontryagin dual $\mathfrak{M}_\infty := \text{Hom}_{\text{cnts}}(\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated and torsion $\Lambda \simeq \mathbb{Z}_p[[x]]$ module.

Iwasawa Invariants

Iwasawa Invariants

- By the structure theory of $\mathbb{Z}_p[[x]]$ modules, up to a pseudoisomorphism, $\mathfrak{M}_\infty$ decomposes into cyclic-modules:

$$\left(\bigoplus_j \mathbb{Z}_p[[x]]/(p^{\mu_j})\right) \oplus \left(\bigoplus_j \mathbb{Z}_p[[x]]/(f_j(x))\right).$$

Iwasawa Invariants

- By the structure theory of $\mathbb{Z}_p[[x]]$ modules, up to a pseudoisomorphism, $\mathfrak{M}_\infty$ decomposes into cyclic-modules:

$$\left(\bigoplus_j \mathbb{Z}_p[[x]]/(p^{\mu_j})\right) \oplus \left(\bigoplus_j \mathbb{Z}_p[[x]]/(f_j(x))\right).$$

- The μ and λ invariants are as follows

$$\mu_E := \sum_j \mu_j \text{ and } \lambda_E := \sum_j \deg f_j(x).$$

The generalized Euler characteristic

The generalized Euler characteristic

- If $E(\mathbb{Q})$ is finite, the cohomology groups $H^i(\Gamma, \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}))$ are finite. In this case, the Euler characteristic is as follows:

$$\chi(\Gamma, E) := \prod_{i \geq 0} \left(\# H^i(\Gamma, \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})\right)^{(-1)^i}.$$

The generalized Euler characteristic

- If $E(\mathbb{Q})$ is finite, the cohomology groups $H^i(\Gamma, \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}))$ are finite. In this case, the Euler characteristic is as follows:

$$\chi(\Gamma, E) := \prod_{i \geq 0} \left(\# H^i(\Gamma, \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})\right)^{(-1)^i}.$$

- When $E(\mathbb{Q})$ is infinite, there is a generalization of the above definition and this generalized Euler characteristic is denoted $\chi_t(\Gamma, E)$.

The Euler characteristic formula

The Euler characteristic formula

- Let $a, b \in \mathbb{Q}_p^\times$, we write $a \sim b$ if $a = ub$ for a unit $u \in \mathbb{Z}_p^\times$.

The Euler characteristic formula

- Let $a, b \in \mathbb{Q}_p^\times$, we write $a \sim b$ if $a = ub$ for a unit $u \in \mathbb{Z}_p^\times$.
- Perrin-Riou and Schneider proved the following p-adic analogue of the BSD formula:

$$\chi_t(\Gamma, E) \sim \frac{R_p(E/\mathbb{Q}) \times \#(Ш(E/\mathbb{Q})[p])}{\#(E(\mathbb{Q})[p])^2} \times \tau(E).$$

The Euler characteristic formula

- Let $a, b \in \mathbb{Q}_p^\times$, we write $a \sim b$ if $a = ub$ for a unit $u \in \mathbb{Z}_p^\times$.
- Perrin-Riou and Schneider proved the following p-adic analogue of the BSD formula:

$$\chi_t(\Gamma, E) \sim \frac{R_p(E/\mathbb{Q}) \times \#(\text{Ш}(E/\mathbb{Q})[p])}{\#(E(\mathbb{Q})[p])^2} \times \tau(E).$$

- Here, $R_p(E/\mathbb{Q})$ is the p-adic regulator and $\tau(E) := \prod c_l$ is the Tamagawa product.

Congruent Elliptic Curves

Congruent Elliptic Curves

- Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and p a prime. We say that E_1 and E_2 are p-congruent if as Galois modules, $E_1[p]$ is isomorphic to $E_2[p]$.

Congruent Elliptic Curves

- Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and p a prime. We say that E_1 and E_2 are p-congruent if as Galois modules, $E_1[p]$ is isomorphic to $E_2[p]$.
- Greenberg and Vatsal showed that if E_1 and E_2 are p-congruent, then the Iwasawa invariants μ and λ for E_1 can be related to the Iwasawa invariants μ and λ for E_2.

Euler characteristics and Congruences

Euler characteristics and Congruences

- Let E_1 and E_2 be p-ordinary and p-congruent. One may ask if the following congruence does hold

$$\chi_t(\Gamma, E_1) \equiv \chi_t(\Gamma, E_2) \mod p?$$

Euler characteristics and Congruences

- Let E_1 and E_2 be p-ordinary and p-congruent. One may ask if the following congruence does hold

$$\chi_t(\Gamma, E_1) \equiv \chi_t(\Gamma, E_2) \mod p?$$

- This is not true, for instance, $E_1 = 37a1$, $E_2 = 1406g1$ are both rank 1 elliptic curves and congruent mod-5. However, computations show that

$$\chi_t(\Gamma, E_1) = 1 \text{ and } \chi_t(\Gamma, E_2) = 5^2.$$

Euler characteristics and Congruences

- One must account for certain local L-factors. There is an explicit set of primes Σ_0 at which either E_1 or E_2 has bad reduction.

Euler characteristics and Congruences

- One must account for certain local L-factors. There is an explicit set of primes Σ_0 at which either E_1 or E_2 has bad reduction.
- Set $\Phi_{\Sigma_0}(E_i)$ to be the product of local L-factors $\prod_{l\in\Sigma_0} L_l(E_i,1)^{-1}$.

Main Theorem

Theorem (-, R.Sujatha)

Suppose that p is an odd prime and E_1 and E_2 are p-congruent elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p.

Main Theorem

Theorem (-, R.Sujatha)

Suppose that p is an odd prime and E_1 and E_2 are p-congruent elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p.

1. Suppose that $\operatorname{rank} E_1(\mathbb{Q}) = \operatorname{rank} E_2(\mathbb{Q})$. Then, we have the following congruence:

$$\Phi_{\Sigma_0}(E_1) \times \chi_t(\Gamma, E_1) \equiv \Phi_{\Sigma_0}(E_2) \times \chi_t(\Gamma, E_2) \mod p.$$

Main Theorem

Theorem (-, R.Sujatha)

Suppose that p is an odd prime and E_1 and E_2 are p-congruent elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p.

1. Suppose that $\operatorname{rank} E_1(\mathbb{Q}) = \operatorname{rank} E_2(\mathbb{Q})$. Then, we have the following congruence:

$$\Phi_{\Sigma_0}(E_1) \times \chi_t(\Gamma, E_1) \equiv \Phi_{\Sigma_0}(E_2) \times \chi_t(\Gamma, E_2) \mod p.$$

2. Suppose that $\operatorname{rank} E_1(\mathbb{Q}) < \operatorname{rank} E_2(\mathbb{Q})$. Then, we have that

$$\Phi_{\Sigma_0}(E_1) \times \chi_t(\Gamma, E_1) \equiv 0 \mod p.$$

Method of proof

Method of proof

- The Euler characteristic $\chi_t(\Gamma, E_i)$ modulo p is detected by the p-torsion

$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \subset \mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}}).$$

Method of proof

- The Euler characteristic $\chi_t(\Gamma, E_i)$ modulo p is detected by the p-torsion

$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \subset \mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}}).$$

- One shows that

$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}}).$$

Method of proof

- The Euler characteristic $\chi_t(\Gamma, E_i)$ modulo p is detected by the p-torsion

$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \subset \mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}}).$$

- One shows that

$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}}).$$

- It follows that

$$\begin{aligned} &\mathrm{Sel}(E_1/\mathbb{Q}_{\mathrm{cyc}})[p] \\ \simeq &\mathrm{Sel}(E_1[p]/\mathbb{Q}_{\mathrm{cyc}}) \\ \simeq &\mathrm{Sel}(E_2[p]/\mathbb{Q}_{\mathrm{cyc}}) \\ \simeq &\mathrm{Sel}(E_2/\mathbb{Q}_{\mathrm{cyc}})[p]. \end{aligned}$$

Caveat

Caveat

- Except
$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}})$$
is not true on the nose.

Caveat

- Except
$$\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}})$$
is not true on the nose.
- One needs to modify the Selmer groups to account for the auxiliary primes Σ_0;
$$\mathrm{Sel}^{\Sigma_0}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}^{\Sigma_0}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}})$$
and this is where the auxiliary factors $\prod_{l\in\Sigma_0} L_l(E_i,1)^{-1}$ come from.

Thank you.