Euler characteristics in Iwasawa theory and their congruences

Sachin Kumar
University of Waterloo, Faculty of Mathematics

June 2023

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

0.1 The Cyclotomic $\mathbb{Z}_p$-extensions

Let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n$ as depicted (**Add commutative diagram**). The tower of number fields, $\mathbb{Q} = \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots$ is called the cyclotomic tower. The field $\mathbb{Q}_{\text{cyc}}$ is taken to be the union,

$$\mathbb{Q}_{\text{cyc}} = \bigcup_{n \geq 1} \mathbb{Q}_n$$

The Galois group is isomorphic to the p-adics, $\text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q}) \simeq \mathbb{Z}_p$.

0.2 Early Investigations and Iwasawa's Approach

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

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

0.3 Iwasawa Theory of Elliptic Curves

Greenberg and Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$. Throughout, we let E be the elliptic curves over $\mathbb{Q}$, denoted as $E/\mathbb{Q}$ with good ordinary reduction at p. They studied the variation of Selmer groups as one goes up the tower. 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, $E[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$ equipped with an action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. What are Selmer groups? For each number field extension F of $\mathbb{Q}$, the selmer group $\text{Sel}_{p^\infty}(E/F)$ consists of Galois cohomology classes, $f \in H^1(\overline{F}/F, E[p^\infty])$ satisfying suitable local conditions. It fits into a short exact sequence,

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

The Selmer group over $\mathbb{Q}_{\text{cyc}}$ is taken to be the direct limit, $\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}) = \lim_{\to n} \text{Sel}_{p^\infty}(E/\mathbb{Q}_n)$. The Pontryagin dual, $\mathfrak{M} = \text{Hom}_{\text{cnts}}(\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated and torsion $\Lambda \simeq \mathbb{Z}_p[[x]]$ module. Now, we will discuss about 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,

$$\mu_E = \sum_j \mu_j$$
$$\lambda_E = \sum_j \deg f_j(x)$$

0.4 The generalized Euler characteristic

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

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

When $E(\mathbb{Q})$ is infinite, there is a generalization of the above definition and this generalized Euler characteristic is denoted by $\chi_t(\Gamma, E)$. We will now see 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 analgoue of the Birch-Swinnerton Dyer 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 $\tau(E) = \prod c_i$ is the Tamagawa product. 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, $E_i[p] \simeq E_2[p]$. Greenberg and Vatsal proved 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. Let E_1 and E_2 be p-ordinary and p-congruent. One may ask if the following congruence does hold $\chi_t(\Gamma, E_1) \equiv \chi_t(\Gamma, E_2) \pmod p$? This is not true, for instance, $E_1 = 37a_1$, $E_2 = 1406g_1$ are both rank 1 elliptic curves and congruent mod 5. However, computations show that, $\chi_t(\Gamma, E) = 1$ and $\chi_t(\Gamma, E_2) = 5^2$. 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, $\prod_{I \in \Sigma_0} L_i(E_i, 1)^{-1}$.

Theorem (R.Sujatha). Suppose that p is an odd primes and E_1 and E_2 are p-congruent elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p. Suppose that $\text{rank} E_1(\mathbb{Q}) = \text{rank} E_2(\mathbb{Q})$. Then, we have the following congruence:

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

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

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

Proof. We will provide an idea of the 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 proves that, $\mathrm{Sel}(E_i/\mathbb{Q}_{\mathrm{cyc}})[p] \simeq \mathrm{Sel}(E_i[p]/\mathbb{Q}_{\mathrm{cyc}})$. It follows that,

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

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 auxilary 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 auxilary factors $\prod_{I\in\Sigma_0} L_I(E_i, 1)^{-1}$ come from. $\square$