STRUCTURE OF FINE SELMER GROUPS

DEBANJANA KUNDU

Abstract. In this talk, we explain and provide more evidence on the relationship between the classical Iwasawa $\mu = 0$ conjecture and the $\mu = 0$ conjecture for Fine Selmer groups, first observed in [CS05] under some strict hypotheses. We give sufficient conditions to prove the classical $\mu = 0$ conjecture that improves upon the result of [Čes15]. We also prove isogeny invariance of Conjecture A in previously unknown cases.

1. Classical Iwasawa Theory

Classical Iwasawa theory is concerned with the growth of arithmetic objects in towers of number fields. More precisely, one studies the growth of p-parts of class groups in towers of number fields of p-power degree. This growth was shown by Iwasawa to often exhibit certain regularity that can be described by a p-adic invariant of a complex-valued L-function.

Consider a tower of number fields

$$F = F_0 \subset F_1 \subset F_2 \subset \dots F_n \dots \subset F_\infty = \bigcup_{n=0}^{\infty} F_n$$

where F_n/F is cyclic of degree p^n. The Galois group $\Gamma = \mathrm{Gal}(F_\infty/F)$ is defined as the inverse limit of the Galois groups $\Gamma_n = \mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Thus,

$$\Gamma := \varprojlim_n \Gamma_n = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

Here, $\mathbb{Z}_p$ is the additive group of p-adic integers and is therefore a compact group when given the p-adic topology. Every number field, F, has a cyclotomic $\mathbb{Z}_p$-extension which is the unique $\mathbb{Z}_p$-extension of F contained in $\bigcup_n F(\zeta_{p^n})$.

Let F_∞/F be a fixed $\mathbb{Z}_p$-extension. In [Iwa59], it was shown that that the growth of the p-part of the class group of F_n, denoted by A_n, is regular.

Theorem. *(Iwasawa) There exist non-negative integers λ and μ, and an integer ν such that for large enough n,*

$$|A_n| = p^{\mu p^n + \lambda n + \nu}.$$

The integers λ, μ, ν are independent of n.

Serre observed that the Iwasawa algebra, $\Lambda(\Gamma) = \Lambda := \varprojlim_n \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[[\Gamma]]$ is isomorphic to the power series ring, $\mathbb{Z}_p[[T]]$. This isomorphism of compact $\mathbb{Z}_p$-algebras is given by $\gamma_0 - 1 \mapsto T$, where γ_0 is a topological generator of Γ.

The structure theorem of finitely generated modules over Λ mimics the theory of finitely generated modules over a PID if one treats Λ-modules as being defined

[1]This work is a part of my PhD thesis. Feel free to contact me if you want details of the proof.

Date: July 4, 2019.

up to finite submodules and quotient modules. The notion of pseudo-isomorphism, ie a homomorphism with a finite kernel and cokernel, gives an equivalence relation on any set of finitely generated, torsion Λ-modules.

Theorem. *For any finitely generated, torsion Λ-module, M, there is a pseudo-isomorphism*

$$M \to \bigoplus_{i=1}^{s} \Lambda/(f_i^{l_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(p^{m_j})$$

where $s, t \geq 0$, each f_i is an irreducible distinguished polynomial and l_i, m_j are positive integers.

Set the notation,

$$\lambda(M) = \sum_i l_i \deg(f_i), \qquad \mu(M) = \sum_j m_j$$

and the characteristic polynomial $f_M(T) = p^{\mu(M)} \prod_i f_i^{l_i}$. This polynomial generates the characteristic ideal, ie

$$\operatorname{char}(M) = \left(p^{\mu(M)} \prod_i f_i^{l_i} \right).$$

In the classical case, the Artin isomorphism identifies A_n with the Galois group, $X_n := \operatorname{Gal}(L_n/F_n)$, of the maximal unramified abelian p-extension L_n of F_n. The inverse limit of Artin isomorphisms then identifies $\varprojlim_n A_n$ with the Galois group, $X_\infty := \operatorname{Gal}(L_\infty/F_\infty)$. Here, $L_\infty = \bigcup_n L_n$. Note that X_∞ is a pro-p group. X_∞ is a finitely generated torsion Λ-module; thus the structure theorem applies. With the notation as above, $\lambda = \lambda(X_\infty)$ and $\mu = \mu(X_\infty)$.

Conjecture. *(Iwasawa) When $F_\infty = F_{cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$.*

This is known for the case when F is an Abelian extension of $\mathbb{Q}$ [FW79]. A different proof using p-adic L-functions is given in [Sin84].

2. Iwasawa Theory of Elliptic Curves

In [Maz72], the Iwasawa theory of Selmer groups was introduced. Using this theory, it is possible to describe the growth of the size of the (p-part of) Selmer group in $\mathbb{Z}_p$ towers.

There are several equivalent definitions of the p^∞ Selmer group. We use the definition as in [Wut04].

Definition 2.1. *The usual (p^∞-)**Selmer group** of A/F for a fixed prime p is the following direct limit,* $\operatorname{Sel}(A/F) := \varinjlim_k \operatorname{Sel}^k(A/F)$ *where*

$$\operatorname{Sel}^k(A/F) := \ker \left(H^1(G_S(F), A[p^k]) \to \bigoplus_{v \in S} H^1(F_v, A)[p^k] \right)$$

where v runs over all the primes of F. For any G-module, M, we use the notation $H^*(F_v, M)$ for the Galois cohomology of the decomposition group at v.

Recall that

$$\bigoplus_{v \in S} H^1(F_v, A)[p^k] \simeq \bigoplus_{v \in S} H^1(F_v, A[p^k]) / \operatorname{Im}(\kappa_{A,p^k})$$

where $\kappa_{E,p^k} : A(F_v)/p^k A(F_v) \hookrightarrow H^1(F_v, A[p^k])$. One can check that $\operatorname{Sel}(A/F)$ is in fact a p-primary subgroup, ie $\operatorname{Sel}(A/F) = \operatorname{Sel}(A/F)_p$. For a detailed explanation one may check [Gre01, §2]. Set the notation,

$$\operatorname{Sel}(A/F_\infty) = \varinjlim_L \operatorname{Sel}(A/L)$$

where the inductive limit is over all finite extensions L/F contained in F_∞. Since p is fixed, we drop it from the notation.

Mazur proved that the Pontryagin dual of the Selmer group, denoted by $X(A/F_\infty)$, is a finitely generated Λ-module. However it need not always be torsion.

Conjecture. *([Maz72]) Let A be an Abelian variety and p be a prime of good ordinary reduction. $X(A/F_\infty)$ is Λ-torsion.*

When $X(A/F_\infty)$ is Λ-torsion, there is a structure theorem as before. However, even for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ there are examples of elliptic curves where $\mu(X(E/\mathbb{Q}_\infty)) > 0$ where p is a prime of good ordinary reduction.

In the fundamental paper of [CS05], they studied a certain subgroup, called the fine Selmer group. They made the following conjecture.

Conjecture. *[CS05, Conjecture A] Let p be an odd prime and E/F be an elliptic curve. When $F_\infty = F_{cyc}$, the Pontryagin dual of the fine Selmer group, denoted by $Y(E/F_{cyc})$ is a finitely generated $\mathbb{Z}_p$-module ie $Y(E/F_{cyc})$ is Λ-torsion and $\mu(Y(E/F_{cyc})) = 0$.*

This conjecture is far from being proven. Even isogeny invariance of this conjecture is yet unknown.

Note that there is no restriction on the reduction type at p. Conjecture A is equivalent to the vanishing of $H^2(G_S(F_{cyc}), E[p^\infty])$ and the associated μ-invariant [CS05, Cor 3.3]. The vanishing of $H^2(G_S(F_{cyc}), E[p^\infty])$ is called the *elliptic curve analogue of the weak Leopoldt conjecture* and is proved for elliptic curves over Abelian number fields in [Kat04].

Let A/F be a d-dimensional Abelian variety and S be a finite set of primes of F including the Archimedean primes, the primes of F above p and the primes where A has bad reduction. Fix an algebraic closure $\overline{F}/F$ and set F_S to be the maximal subfield of $\overline{F}$ containing F which is unramified outside S. Denote the absolute Galois extension $\operatorname{Gal}(\overline{F}/F)$ by G and the Galois group, $\operatorname{Gal}(F_S/F)$ by $G_S(F)$.

Definition 2.2. *The (p^∞-)**fine Selmer group** is defined as*

$$R(A/F) := \ker\left(H^1(G_S(F), A[p^\infty]) \to \bigoplus_{v \in S} H^1(F_v, A[p^\infty]) \right).$$

With the inductive limit over all finite extensions L/F contained in F_∞, set

$$R(A/F_\infty) = \varinjlim_L R(A/L).$$

The above definition is independent of the choice of S. Indeed, it follows from the exact sequence

$$0 \to R(A/F) \to \mathrm{Sel}(A/F) \to \bigoplus_{v|p} A(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

A priori it is not obvious there is a relation between Galois modules coming from class groups and those coming from elliptic curves. In [CS05] they showed that under certain strict conditions, the p-part of fine Selmer group grows like the p-part of the class group in a cyclotomic tower.

Theorem. *[CS05, Theorem 3.4] Let p be an odd prime such that the extension $F(E[p^\infty])/F$ is pro-p. Then conjecture A holds for E over F_{cyc} if and only if the classical Iwasawa $\mu = 0$ conjecture holds for F_{cyc}.*

A different proof of a slight variant of this theorem was given by [LM16] by comparing p-ranks of class groups and fine Selmer groups. Instead of assuming that $F(E[p^\infty]/F)$ is pro-p, they assume $F(E[p])/F$ is a finite p-extension.

An important corollary of the above theorem is the following.

Corollary. *Assume F is an Abelian extension of $\mathbb{Q}$ and that p is an odd prime such that $E(F)[p] \neq 0$. Then Conjecture A is valid for E/F_{cyc}.*

The proof of this corollary crucially uses that the Iwasawa $\mu = 0$ conjecture is known for *all* Abelian extensions of $\mathbb{Q}$.

3. Results

It is in fact possible to prove a stronger statement using only the Iwasawa $\mu = 0$ conjecture for the fixed number field F.

Theorem 3.1. *Assume either*

(1) F contains μ_p or

(2) F is a totally real field.

In either of the cases, suppose the classical Iwasawa $\mu = 0$ is true. If E is an elliptic curve over F such that $E(F)[p] \neq 0$, then Conjecture A holds for $Y(E/F_{cyc})$.

Remark. *The first case subsumes the corollary above. Indeed, if $F/\mathbb{Q}$ is Abelian then so is $F(\mu_p)/\mathbb{Q}$ and the Iwasawa $\mu = 0$ Conjecture is known to be true.*

Using similar machinery, it is possible to prove a (stronger) converse of the above theorem.

Theorem 3.2. *Let E be an elliptic curve defined over the number field F. Let p be any odd prime. Further assume that $E(F)[p] \neq 0$. If Conjecture A holds for $Y(E/F_{cyc})$ then the classical $\mu = 0$ conjecture holds for F_{cyc}/F.*

Theorem 3.2 implies that given a number field F, it is enough to provide one example of an elliptic curve E/F such that $E(F)[p] \neq 0$ for which conjecture A holds to prove the classical $\mu = 0$ conjecture for F_{cyc}/F. By a result of Merel, our theorem can at best show the classical Iwasawa $\mu = 0$ conjecture for finitely many primes. However, it improves upon the following theorem of [Čes15].

Theorem. *For a prime p and a number field F, to prove the classical Iwasawa $\mu = 0$ conjecture, it suffices to find an Abelian F-variety, A such that*

(1) A has good ordinary reduction at all places above p,
(2) A has $\mathbb{Z}/p\mathbb{Z}$ as an F-subgroup,
(3) $X(A/F_{cyc})$ is Λ-torsion and has μ-invariant 0.

This is an improvement because

(1) There is no condition on the reduction type at primes above p, unlike when one is working with the Selmer group.
(2) There are no known examples where $\mu(Y) > 0$ but there are several examples where $\mu(X) > 0$ even when the base field is $\mathbb{Q}$ and p is a prime of good ordinary reduction.
(3) $F(E[p])/F$ need not be a pro-p-extension as in [CS05]. This is a relatively strict condition to impose. The only requirement is $E(F)[p] \neq 0$.

The two main theorems mentioned above can prove isogeny invariance of Conjecture A in some previously unknown cases.

Corollary 3.3. *Let F be a number field that contains μ_p or be a totally real number field. Let E and E' be isogenous elliptic curves such that both E and E' have non-trivial p-torsion points over F. Then, Conjecture A holds for $Y(E/F_{cyc})$ if and only if Conjecture A holds for $Y(E'/F_{cyc})$.*

Remark. *All statements hold for Abelian varieties of dimension d. The only property of the cyclotomic $\mathbb{Z}_p$-extension we use in the proofs is that primes in S decompose finitely. The theorems go through for a more general class of $\mathbb{Z}_p$-extensions.*

Acknowledgements

I thank Kumar Murty for his support, and many helpful suggestions and discussions. Lots of thanks to Sujatha Ramodorai, Kestutis Cesnavicius, Gaurav Patil, Sudhanshu Shekhar, Somnath Jha and Meng Fai Lim for answering many questions. I thank the organizers of BU-Keio Number Theory Conference (2019) for giving me an opportunity to present my work.

References

[Čes15] Kęstutis Česnavičius. Selmer groups and class groups. *Compositio Mathematica*, 151(3):416–434, 2015.
[CS05] John Coates and Ramdorai Sujatha. Fine selmer groups of elliptic curves over p-adic lie extensions. *Mathematische Annalen*, 331(4):809–839, 2005.
[FW79] Bruce Ferrero and Lawrence C Washington. The iwasawa invariant μ_p vanishes for abelian number fields. *Annals of Mathematics*, pages 377–395, 1979.
[Gre01] Ralph Greenberg. Introduction to iwasawa theory for elliptic curves. *Arithmetic algebraic geometry*, 9:407–464, 2001.
[Iwa59] Kenkichi Iwasawa. On γ-extensions of algebraic number fields. *Bulletin of the American Mathematical Society*, 65(4):183–226, 1959.
[Kat04] Kazuya Kato. p-adic hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.
[LM16] Meng Fai Lim and V Kumar Murty. The growth of fine selmer groups. *J. Ramanujan Math. Society*, 31(1):79–94, 2016.
[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Inventiones mathematicae*, 18(3-4):183–266, 1972.

[Sin84] Warren Sinnott. On the μ-invariant of the γ-transform of a rational function. *Inventiones mathematicae*, 75(2):273–282, 1984.

[Wut04] Christian Wuthrich. *The fine Selmer group and height pairings.* PhD thesis, University of Cambridge, 2004.

Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Room 6290, Toronto, Ontario, Canada, M5S 2E4

Email address: dkundu@math.utoronto.ca