1 Introduction

Broadly, I study the arithmetic of elliptic curves. It is a branch of mathematics, at the intersection of number theory, algebra, arithmetic algebraic geometry and complex analysis. Elliptic curves are precisely the genus 1 algebraic curves with rational points. The arithmetic of simpler, genus 0, algebraic curves has been studied for centuries. On the other hand, higher genus curves are far less accessible. Being of genus 1, elliptic curves land in a sweet spot for mathematical enquiry.

My research is on the Iwasawa theory of elliptic curves. I study the structure of fine Selmer groups of elliptic curves in towers of number fields. These were introduced in [CS05] and are closely related to class groups [LM16]. Thus, studying fine Selmer groups can throw light on unanswered questions in classical Iwasawa Theory. I use tools from Galois cohomology, module theory, algebraic and analytic number theory to answer questions on the structure and growth of fine Selmer groups in infinite (and finite) field extensions.

Here is the outline of the research statement. I discuss the two broad aspects of Iwasawa theory and state some of the open problems that drive my research in Section 2.1. I explain my results in Sections 2.2–2.4. My other research interests are discussed in Section 3. My future projects are mentioned in Section 4.

2 Primary Research Interest: Iwasawa Theory

Iwasawa theory asks questions about the structure of Galois modules over extensions with Galois group a p-adic Lie group. It is often concerned with the growth of arithmetic objects in towers of number fields.

2.1 Background and Open Questions

2.1.1 Classical Iwasawa Theory

Historically, one studied the growth of p-parts of class groups in towers of number fields of p-power degree. 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,

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

$\mathbb{Z}_p$ is the additive group of p-adic integers and is compact 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. The p-part of the class group of F_n, denoted by A_n, has regular growth. More precisely,

Theorem. *[Iwa59] There exist non-negative integers λ, μ, and an integer ν such that for large enough n,*

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

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

Iwasawa made the following conjecture.

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

This is known for Abelian extensions [FW79]. A proof using p-adic L-functions is given in [Sin84].

2.1.2 Structure Theorem of Finitely Generated Λ-Modules

For a profinite group, G, the Iwasawa algebra, $\Lambda(G)$, is a variation of its group ring with p-adic coefficients that also takes into account its topology. 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 up to finite submodules and quotient modules. The notion of pseudo-isomorphism, i.e. 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 generates the characteristic ideal, $\mathrm{char}(M)$.

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

2.1.3 Iwasawa Theory of Elliptic Curves

The Iwasawa theory of Abelian varieties (in particular, elliptic curves) was introduced in [Maz72]. Using this theory, it is possible to describe the growth of the size of the p-part of Selmer groups of Abelian varieties in $\mathbb{Z}_p$ towers. In fact, the growth pattern is very similar to the classical case.

However, even for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ there are examples of elliptic curves where the μ-invariant of the Selmer group is positive when p is a prime of good ordinary reduction [Maz72].

In the fundamental paper of [CS05], the study of a certain subgroup of the Selmer group, called the fine Selmer group was initiated. It is defined by imposing more restrictive conditions on the elements of the Selmer group at all places above p. The authors made the following conjecture.

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

This conjecture is far from proven. It is not even know if this conjecture is isogeny invariant.

In [CS05], the authors made a second conjecture concerning the mysterious phenomenon of certain arithmetic Iwasawa modules for p-adic Lie extensions of dimension strictly greater than 1 being much smaller than expected. This was first noted in [Gre01].

Conjecture. *[Gre01, Conjecture 3.5] Suppose F is any number field and p is any prime. Let $\widetilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Let $\widetilde{L}$ denote the pro-p Hilbert class field of $\widetilde{F}$ and let $\widetilde{X} = \mathrm{Gal}(\widetilde{L}/\widetilde{F})$, be a module over the ring $\widetilde{\Lambda} = \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{F}/F)]]$. Then $\widetilde{X}$ is a pseudo-null $\widetilde{\Lambda}$-module.*

Conjecture. *[CS05, Conjecture B] Suppose Conjecture A is valid for E over F_{cyc}. In addition, if F_∞ is a p-adic Lie extension of F which contains F_{cyc} and whose Galois group G is pro-p and has dimension strictly greater than 1 as a p-adic Lie group, then $Y(E/F_\infty)$ is pseudo-null as a $\Lambda(G)$-module.*

2.2 Results Related to Conjecture A

In my thesis, I provide a large class of examples where Conjecture A holds.

Theorem 1. *Let E be a rank 0 elliptic curve defined over the number field, F. Assume finiteness of the Shafarevich-Tate group. Then, for density 1 primes the p-part of the Selmer group (hence p-part of the fine Selmer group) is trivial over F_{cyc}. In particular, Conjecture A holds for density 1 primes.*

A priori one would not expect a relation between Galois modules coming from class groups and those coming from elliptic curves [CS05, Theorem 3.4]. I have proved a strong relationship between them. These theorems have interesting corollaries.

Theorem 2. *Let $p \neq 2$ and E be an elliptic curve defined over a number field F with $E(F)[p] \neq 0$. If Conjecture A holds for E over F_{cyc}, the classical Iwasawa Conjecture holds for F_{cyc}/F.*

Theorem 3. *Let $p \neq 2$, and E be an elliptic curve over a number field, F, such that either*

1. *$F \supset \mu_p$ or*
2. *$F/\mathbb{Q}$ is a Galois extension of odd degree.*

If $E(F)[p] \neq 0$ and the Iwasawa $\mu = 0$ Conjecture holds for F_{cyc}, then Conjecture A holds for $Y(E/F_{cyc})$.

The following result is obtained by combining Theorems 2 and 3. It provides new evidence for isogeny invariance of Conjecture A.

Corollary 4. *Let F be a number field that contains μ_p or be a Galois extension of odd degree over $\mathbb{Q}$. 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 $Y(E/F_{\text{cyc}})$ if and only if Conjecture A holds for $Y(E'/F_{\text{cyc}})$.*

2.3 Growth of Fine Selmer Groups

It is possible to take this analogy between the growth of fine Selmer groups and class groups further.

2.3.1 Growth in Infinite Towers

There are examples of non-Abelian, non p-adic analytic towers where the p-ranks of both the fine Selmer groups and class groups have been shown to have the same order of growth [LM16].

If F is a number field such that the Golod-Shafarevich inequality is satisfied, then the p-class field tower of F is not p-adic analytic and the p-class rank is unbounded (see [Bos92],[Haj97]). Therefore, the theory developed in [Gre99] does not apply to such a tower. It is however possible to study the growth of $\mathfrak{p}$-fine Selmer ranks for elliptic curves with complex multiplication (CM) in these non-Abelian towers.

Theorem 5. *Let F be a number field satisfying the Golod-Shafarevich inequality that contains the imaginary quadratic field, K. Let E be an elliptic curve over F with CM by $\mathcal{O}_K$. Let p be an odd rational prime that splits in K as $\mathfrak{p}\bar{\mathfrak{p}}$ such that $\mathfrak{p}$ is unramified in F/K. Let S be a finite set of primes in F containing the Archimedean primes, primes above $\mathfrak{p}$ and primes where E has bad reduction. Let F_∞^S/F be the maximal unramified non-constant pro-p extension where primes in S split completely and F_n be the n-th layer of this class field tower. Then the $\mathfrak{p}$-rank of the fine Selmer group of E/F_n is unbounded as n tends to ∞.*

2.3.2 Growth in $\mathbb{Z}/p\mathbb{Z}$-Extensions

It is a folklore result that the p-torsion of the ideal class group becomes unbounded in $\mathbb{Z}/p\mathbb{Z}$ extensions of a fixed number field. The p-Selmer group becomes arbitrarily large when one varies over all $\mathbb{Z}/p\mathbb{Z}$-extensions of a global field [Ces17]. I prove a similar result holds for the p-fine Selmer groups by comparing p-ranks of fine Selmer groups and class groups.

Theorem 6. *Let A be an Abelian variety defined over a number field, F. On varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions of F ordered by conductor, the p-fine Selmer rank becomes unbounded.*

This method of proof makes it possible to find effective bounds on the conductor of such a $\mathbb{Z}/p\mathbb{Z}$-extension.

Theorem 7. *Let A be an Abelian variety of dimension d defined over $\mathbb{Q}$. Suppose $A(\mathbb{Q})[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension $L_N/\mathbb{Q}$ of conductor $\mathfrak{f}(L_N/\mathbb{Q}) \sim c^N$ where c is a constant that depends on A such that $r_p(\mathrm{Sel}_p(A/\mathbb{Q})) \geq N$.*

Remark. *A similar result can be proven for an Abelian variety defined over any number field, F.*

The p-torsion of the classical Shafarevich-Tate group of an elliptic curve has unbounded growth in $\mathbb{Z}/p\mathbb{Z}$-extensions of a fixed number field [CS10]. Like the fine Selmer group, one can define a fine analogue of the Shafarevich-Tate group [Wut07]. Using the result of Clark-Sharif, it is possible to show the following.

Theorem 8. *Let E be an elliptic curve defined over the number field, F. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions, L/F, the p-fine Shafarevich-Tate group is unbounded.*

2.3.3 λ-Invariants in $\mathbb{Z}_p$-Towers

Kida's formula describes the change of Iwasawa λ-invariants in a p-extension in terms of the degree and the ramification index. Using the theory of Galois cohomology Kida's formula was proven for all number fields in [Iwa81, Theorem 6]. An analogue was proven for the λ-invariant of Selmer group in [HM99]. In my thesis, I prove an analogous result for the λ-invariant of the fine Selmer group.

Theorem 9. *Let $p \geq 5$ be a prime. Let E be an elliptic curve defined over a number field, K, with good ordinary reduction at all primes in K above p. Let L/K be a Galois p-extension. Assume $Y(E/K_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Then $Y(E/L_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Also,*

$$\lambda_E(L) = [L_{\mathrm{cyc}} : K_{\mathrm{cyc}}]\lambda_E(K) + \sum_{w \in P_1} (e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w) - 1) + 2 \sum_{w \in P_2} (e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w) - 1)$$

where $e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)$ is the ramification index of w in $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$ and P_1, P_2 are the following sets in L_{cyc}

$$P_1 = \{w \mid w \nmid p,\ E : \textit{split multiplicative reduction at } w\}$$
$$P_2 = \{w \mid w \nmid p,\ E : \textit{good reduction reduction at } w,\ E(L_{\mathrm{cyc},w})[p] \neq 0\}.$$

2.4 Results Related to Conjecture B

Concrete examples for the validity of Conjecture B have been rather sparse. In joint work with R. Sujatha, we settle the case of numerical examples considered in [CS05, Examples 4.7 and 4.8] which could not be fully settled then. We provide a class of examples for Conjecture B.

Theorem 10. *Let E be a CM elliptic curve defined over a number field F and p be an odd prime of good ordinary reduction. Set $F_\infty = \bigcup_n F(E_{p^n})$, and consider the pro-$p$ group $G = \mathrm{Gal}(F_\infty/F)$. If $Y(E/F_{\mathrm{cyc}})$ is finite, Conjecture B holds for $Y(E/F_\infty)$.*

Theorem 11. *Let p be an odd rational prime, $F/\mathbb{Q}$ be a Galois extension containing μ_p such that there is only one prime above p, and E be an elliptic curve defined over F with good reduction at p. Suppose p does not divide the class number of F. Then Conjecture B is true for $Y(E/F(E_{p^\infty}))$.*

We have made partial progress in understanding the relationship between the Generalized Greenberg's Conjecture and Conjecture B in the CM case. So far, we have proved the following result.

Theorem 12. *Let E be an elliptic curve over the imaginary quadratic field, K with CM by $\mathcal{O}_K$. Let $p \neq 2, 3$ be an unramified prime in K. Set $F = K(E[p])$ and $F_\infty = \bigcup_n F(E[p^n])$. Set $\widetilde{F}$ to be the compositum of all $\mathbb{Z}_p$ extensions of F, and X_∞ (resp $\widetilde{X}$) be the Greenberg-Iwasawa module over F_∞ (resp. $\widetilde{F}$). Then*

1. *X_∞ (resp. $\widetilde{X}$) is pseudo-null if and only if $Y(E/F_\infty)$ (resp. $Y(E/\widetilde{F})$) is pseudo-null.*
2. *if Conjecture B holds for $Y(E/F_\infty)$, the Generalized Greenberg's Conjecture holds for F and K.*

3 Other Research Interests

1. I am interested in studying solutions to Diophantine equations. In [KP18], using the characterization of primitive divisors in Lehmer sequences due to [BHV01] we completely solve

$$(x+r)^2 + (x+2r)^2 + \cdots + (x+dr)^2 = y^n \quad x, y, r, n \in \mathbb{Z},\ n \geq 2.$$

   for $2 \leq d \leq 10$ and for all $1 \leq r \leq 10^4$ (except in the case $d = 6$, where we restrict $1 \leq r \leq 5000$), under the natural assumption $\gcd(x, y) = 1$.

2. I got a chance to take several graduate courses with Prof. James Arthur that got me interested in the Langlands Program; in particular, the Langlands Functoriality Conjectures. The conjectures had their genesis in the area of automorphic forms, and trace formula is one of the main techniques in attacking these conjectures and related problems like "Beyond Endoscopy" introduced in [Lan04].

   The strategy of beyond endoscopy is a two-step process. The first is to isolate via the trace formula the (packets of) cuspidal automorphic representations whose L-functions (for a representation of the dual group) have a pole at $s = 1$. The second involves a comparison of this data for two different groups and aims to determine functorial transfers. The fist step was completed in [Alt15b] where the author worked with $\mathrm{GL}_2(\mathbb{Q})$. In joint work with M. Emory, M. Espinosa Lara and T. A. Wong, we are utilizing this method to generalize the first step to $\mathrm{GL}_2(F)$ where F is a number field. This project began out of the Functoriality and the Trace Formula workshop at AIM in December 2017.

4 Work in Progress and Future Projects

There are some obvious questions that arise from my previously completed projects. I am working on some of these at the moment and some are projects I hope to take up in the near future.

1. Theorem 1 is known for $\mathbb{Q}$ unconditionally [Gre99, Theorem 5.1]. In some cases it is known that $\mathrm{Sel}_p(E/\mathbb{Q}_{\mathrm{cyc}})$ is trivial for all but finitely many primes. It is natural to ask given an elliptic curve over a number field F, whether $Y(E/F_{\mathrm{cyc}})$ is trivial for all but finitely many primes.

2. Theorem 2 says given a number field F, to prove the classical $\mu = 0$ conjecture it is enough to find *one* elliptic curve E/F with $E(F)[p] \neq 0$ for which Conjecture A holds. Using this theorem, it should be possible to find new class of number fields where the classical conjecture holds. I have partial results suggesting that Conjecture A should hold for elliptic curves over p-rational fields. This will prove the classical conjecture for non-Abelian p-rational number fields.

3. In the 1980's, in a series of papers, Cuoco and Monsky studied the growth of class groups in $\mathbb{Z}_p^d$ extensions. One goal is to study the growth of p-ranks of (fine) Selmer groups in $\mathbb{Z}_p^d$ extensions and see if the analogy we've observed so far can be extended. I have some partial results in this direction.

4. Recently, estimates of class numbers have been obtained in metabelian extensions [Lei17] and more general p-adic Lie extensions [Lim18]. Using machinery developed to prove Theorem 5 it should be possible to answer what happens for (fine) Selmer groups in such extensions.

5. Results discussed in Section 2.4 are just the beginning. The first project would be to prove Theorem 10 for non-CM elliptic curves. It should be possible to strengthen Theorem 12; in particular understand when does the Generalized Greenberg's Conjecture imply Conjecture B. This will hopefully provide more evidence for the conjecture as the Generalized Greenberg's conjecture has been numerically settled in a large number of cases. This is on going work with R. Sujatha.

6. For a totally real field, the Generalized Greenberg's Conjecture is the statement that the Iwasawa invariants $\mu = \lambda = 0$. In joint work with A. Ray, using tools from Galois deformations and Galois cohomology we are exploring this version of Greenberg's Conjecture.

7. Once we successfully generalize the results of [Alt15b] to a general number field, the next natural question would be to proceed and generalize the results of [Alt17] and [Alt15a]. This will be joint work with M. Emory, M. Espinosa Lara and T. A. Wong.

References

[Alt15a] S Ali Altuğ. Beyond endoscopy via the trace formula–3. the standard representation. *Journal of the Institute of Mathematics of Jussieu*, pages 1–39, 2015.

[Alt15b] Salim Ali Altuğ. Beyond endoscopy via the trace formula: 1. Poisson summation and isolation of special representations. *Compositio Mathematica*, 151(10):1791–1820, 2015.

[Alt17] S Ali Altuğ. Beyond endoscopy via the trace formula, 2: Asymptotic expansions of Fourier transforms and bounds towards the Ramanujan conjecture. *American Journal of Mathematics*, 139(4):863–913, 2017.

[BHV01] Yu Bilu, G Hanrot, and PM Voutier. Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte). *J. Reine Angew. Math*, 539:75–122, 2001.

[Bos92] Nigel Boston. Some cases of the Fontaine-Mazur conjecture. *Journal of Number Theory*, 42(3):285–291, 1992.

[Ces17] Kestutis Cesnavicius. p-Selmer growth in extensions of degree p. *Journal of the London Mathematical Society*, 95(3):833–852, 2017.

[CS05] J. Coates and R. Sujatha. Fine selmer groups of elliptic curves over p-adic Lie extensions. *Mathematische Annalen*, 331(4):809–839, Apr 2005.

[CS10] Pete L Clark and Shahed Sharif. Period, index and potential, iii. *Algebra and Number Theory*, 4(2):151–174, 2010.

[FW79] Bruce Ferrero and Lawrence C Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Annals of Mathematics*, pages 377–395, 1979.

[Gre99] Ralph Greenberg. *Iwasawa theory for elliptic curves*, pages 51–144. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[Gre01] Ralph Greenberg. Iwasawa theory—past and present. *Adv. Studies in Pure Math*, 30:335–385, 2001.

[Haj97] Farshid Hajir. On the growth of p-class groups in p-class field towers. *Journal of Algebra*, 188(1):256–271, 1997.

[HM99] Yoshitaka Hachimori and K Matsuno. An analogue of Kida's formula for the Selmer groups of elliptic curves. *J. Alg. Geom.*, 8:581–601, 1999.

[Iwa59] Kenkichi Iwasawa. On γ-extensions of algebraic number fields. *Bulletin of the American Mathematical Society*, 65(4):183–226, 1959.

[Iwa81] Kenkichi Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Mathematical Journal, Second Series*, 33(2):263–288, 1981.

[KP18] Debanjana Kundu and Vandita Patel. Perfect powers that are sums of squares of an arithmetic progression. *arXiv preprint arXiv:1809.09167*, 2018.

[Lan04] Robert P Langlands. Beyond endoscopy. *Contributions to automorphic forms, geometry, and number theory*, 611:697, 2004.

[Lei17] Antonio Lei. Estimating class numbers over metabelian extensions. *arXiv preprint arXiv:1703.10477*, 2017.

[Lim18] Meng Fai Lim. A note on asymptotic class number upper bounds in p-adic Lie extensions. *arXiv preprint arXiv:1807.04916*, 2018.

[LM16] Meng Fai Lim and V Kumar Murty. The growth of fine Selmer groups. *Journal of the Ramanujan Mathematical Society*, 31:79–94, 03 2016.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Inventiones mathematicae*, 18(3):183–266, Dec 1972.

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

[Wut07] Christian Wuthrich. The fine Tate–Shafarevich group. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 142, pages 1–12. Cambridge University Press, 2007.