RESEARCH STATEMENT

ANWESH RAY

1. Introduction

I'm interested in algebraic number theory and arithmetic geometry. My primary research interest is in Iwasawa theory, Galois representations and L-functions. I use techniques in Galois cohomology, algebraic number theory, algebraic geometry and analytic number theory. Recently, I have studied questions at the intersection of arithmetic statistics and Iwasawa theory. Some of my research is significantly informed by computation. As a secondary interest, I also study questions in arithmetic geometry.

1.1. **Summary of research interests.** Below is a summary of my research. Many of the projects are joint with my coauthors and attributions are made at various points in this article, where the works are described in greater detail.

(1) *Iwasawa theory:* I study the structure of Galois modules that arise from geometry. These modules are defined by Galois cohomology classes satisfying local conditions and they provide key insights into the arithmetic of elliptic curves and abelian varieties. My research in the subject is categorized as follows.
   - *Iwasawa theory and congruences:* If g_1 and g_2 are modular forms whose Fourier coefficients satisfy congruence modulo a prime, there is an explicit relationship between Iwasawa theoretic invariants associated with g_1 and those associated with g_2. We prove new cases of such congruence relations, see the results in section 3.
   - *Arithmetic statistics and Iwasawa theory of elliptic curves:* In the context of arithmetic statistics, we formulated a setting in which it is possible to study the average behavior of Iwasawa theoretic invariants for elliptic curves. The motivation is to study the variation of Iwasawa invariants for elliptic curves that are ordered by height, see the results in section 4. This approach has now been extended to prove statistical results in noncommutative Iwasawa theory.
   - *Diophantine stability:* Ideas in Iwasawa theory are used to study the growth and stability of the Mordell–Weil group and Tate–Shafarevich group in p-cyclic extensions. We study questions in arithmetic statistics that arise in this context, the relevant discussion is in section 5.
   - *Constructing Galois representations with prescribed Iwasawa invariants:* We introduce techniques from deformation theory to construct Galois representations with prescribed Iwasawa invariants, the results are outlined in section 6.

Date: November 2021.

- *Growth questions in Iwasawa theory:* I study the growth of the rank of elliptic curves in various towers of number fields. I also study the growth of the set of rational points of curves of genus > 1 in such towers. The results are summarized in section 7.
- *Iwasawa theory (miscellaneous results):* Some miscellaneous results are summarized in section 8.

(2) *Galois representations:* I explore questions related to the study of Galois representations arising from geometry. The deformation theory of Galois representations plays a significant role in my research. My research on this topic is summarized as follows:
- *Serre's Conjecture- Refinements and Generalizations:* I construct lifts of certain mod-p Galois representations to characteristic zero Galois representations that satisfy the conditions of Fontaine and Mazur. These results are motivated by a celebrated conjecture of Serre for 2-dimensional Galois representations. The results are summarized in section 10.
- *Constructing Galois representations with special properties:* The deformation theoretic techniques are used to construct Galois representations with special properties. The reader is referred to the discussion in section 11.
- *Arithmetic statistics for Galois deformation rings:* The study of Galois deformation rings are very significant in showing that a given Galois representation arises from a modular form. Fixing a prime p, we may associate a Galois deformation ring naturally to each elliptic curve $E_{/\mathbb{Q}}$. We formulate a question in arithmetic statistics concerning the variation of the algebraic structure of deformation rings, as $E_{/\mathbb{Q}}$ varies over a certain set of elliptic curves ordered by *height*, see section 12.

(3) *Arithmetic geometry results:* My results in arithmetic geometry are summarized in section 13.

(4) *Computational aspect of my work:* My research is significantly informed by computation. This is explained in section 14.

2. Iwasawa theory: Overview and notation

Given an elliptic curve E over a number field K, and a prime number p, the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ is a subgroup of the Galois cohomology group $H^1(\mathrm{Gal}(\bar{K}/K), E[p^\infty])$ defined by certain explicit local conditions. This Selmer group sits in a short exact sequence

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

Here, $Ш(E/K)$ is the *Tate-Shafarevich group*, which is conjectured to always be finite. Thus, the Selmer group captures important arithmetic information. The main idea behind Iwasawa theory is that the Selmer group over an infinite Galois extension may be systematically studied via cohomological and Galois theoretic methods. The main conjecture in Iwasawa theory predicts that the Selmer group is intimately related to a p-adic analogue of an L-function. Under additional conditions, this conjecture has been resolved by Skinner and Urban [SU14].

We introduce some notation. Throughout this discussion, the prime p is fixed. Let $K(\mu_{p^\infty})$ be the infinite Galois extension of K generated by p-power roots of unity $\mu_{p^\infty} =$

$\bigcup_{m\geq 1}\mu_{p^m}$. Let K_n be the extension of K contained in $K(\mu_{p^\infty})$ such that $[K_n:K]=p^n$. The tower of number fields $K=K_0\subset K_1\subset K_2\subset\cdots\subset K_n\subset\ldots$, is called the *cyclotomic tower* and K_n is the *n-th layer*. The Galois extension

$$K_{\mathrm{cyc}}:=\bigcup_{n\geq 1}K_n$$

is a $\mathbb{Z}_p$-extension, i.e., the Galois group $\Gamma_K:=\mathrm{Gal}(K_{\mathrm{cyc}}/K)$ is isomorphic to $\mathbb{Z}_p$, the ring of p-adic integers. The Iwasawa algebra Λ is the completed group algebra

$$\Lambda:=\varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$$

and is isomorphic to the formal power series ring $\mathbb{Z}_p[\![T]\!]$.

The Selmer group over K_{cyc} is taken to be the direct limit

$$M:=\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})=\varinjlim_n \mathrm{Sel}_{p^\infty}(E/K_n)$$

with respect to natural restriction maps, and its Pontryagin dual $M^\vee:=\mathrm{Hom}_{\mathrm{cts}}(M,\mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated Λ-module. When E is an elliptic curve defined over $\mathbb{Q}$ and $K/\mathbb{Q}$ is an abelian extension, $M^\vee$ is also torsion as a Λ-module. This is a result of Kato and Rubin. For the rest of this discussion, we assume that $M^\vee$ is torsion over Λ. It follows from the structure theory of finitely generated and torsion Λ-modules that $M^\vee$ is pseudo-isomorphic to a finite direct sum of cyclic Λ-modules, i.e., there is a map of Λ-modules

$$M^\vee\longrightarrow\left(\bigoplus_{i=1}^{s}\Lambda/(p^{\mu_i})\right)\oplus\left(\bigoplus_{j=1}^{t}\Lambda/(f_j(T))\right)$$

with finite kernel and cokernel. Here, $\mu_i>0$ and $f_j(T)$ is a distinguished polynomial (i.e., a monic polynomial with non-leading coefficients divisible by p). The characteristic ideal of $M^\vee$ is (up to a unit) generated by

$$f_M^{(p)}(T)=f_M(T):=p^{\sum_i\mu_i}\prod_j f_j(T).$$

The μ-invariant of M is defined as the power of p in $f_M(T)$. More precisely,

$$\mu_p(M):=\begin{cases}\sum_{i=1}^{s}\mu_i & \text{if } s>0\\ 0 & \text{if } s=0.\end{cases}$$

The λ-invariant of M is the degree of the characteristic element, i.e.,

$$\lambda_p(M):=\begin{cases}\sum_{i=1}^{s}\deg f_i & \text{if } s>0\\ 0 & \text{if } s=0.\end{cases}$$

We shall set $\mu_p(E/K_{\mathrm{cyc}})$ and $\lambda_p(E/K_{\mathrm{cyc}})$ to denote the μ and λ-invariants of the Selmer group $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})$ respectively.

3. Iwasawa theory and congruences

Iwasawa theoretic invariants arising from modules associated to Galois representations provide key insights into their arithmetic. Greenberg and Vatsal [GV00] studied the role of congruences in Iwasawa theory. Let $g_1 = \sum_{n\geq 1} a(n, g_1)q^n$ and $g_2 = \sum_{n\geq 1} a(n, g_2)q^n$ be normalized newforms and p a prime number. Given a prime $\mathfrak{p}$ above p in the number field generated by the Fourier coefficients of g_1 and g_2, we say that g_1 and g_2 are $\mathfrak{p}$-congruent if

$$a(\ell, g_1) \equiv a(\ell, g_2) \mod \mathfrak{p}$$

for all but finitely many primes ℓ. Given congruent modular forms g_1 and g_2, Greenberg and Vatsal showed that the Iwasawa invariants for g_1 are related to the Iwasawa invariants for g_2. Their results had consequences to the main conjecture of Iwasawa theory. Since their seminal work, the study of the role of congruences in Iwasawa theory has gained significant momentum. For instance, Emerton-Pollack-Weston [EPW06] studied the variation of Iwasawa invariants in congruent families of ordinary modular forms. Kriz and Li [KL19] studied congruences for Heegner points and applied such results in studying Goldfeld's conjecture.

My work on the subject of congruences in Iwasawa theory may be summarized as follows:

- *Euler characteristics and congruences:* In joint work with R. Sujatha [RS20, RS21b], we study the generalized Euler characteristic in Iwasawa theory and its behavior with respect to congruences. The results apply to elliptic curves of arbitrary rank and semistable reduction over number fields. We prove congruence relations for the p-adic Birch and Swinnerton-Dyer formulae for the leading terms of p-adic L-functions.
- *Iwasawa theory and congruences for the symmetric square of a modular form:* This is joint with R. Sujatha and V. Vatsal [RSV21]. It is natural to extend results of Greenberg and Vatsal to pairs of Galois representations of higher rank. These Galois representations will be assumed to be congruent in the sense that the residual representations will be absolutely irreducible and isomorphic. On the one hand, it is easy to extend results to the study of algebraic Iwasawa invariants. However, there is significant work to be done on the analytic side, in proving congruences for p-adic L-functions. In this paper, we prove such congruences for the symmetric square representations associated to pairs of congruent p-ordinary newforms.

We now describe these results in more detail.

3.1. **Euler characteristics and congruences.** Given an elliptic curve E over the rationals, the strong form of the Birch and Swinnerton-Dyer conjecture predicts an explicit formula for the leading coefficient a_r of the Hasse-Weil L-function

$$L(E, s) = a_r(s-1)^r + a_{r+1}(s-1)^{r+1} + \dots.$$

Assume that E has good ordinary reduction at a prime p. The p-adic L-function in Iwasawa theory interpolates the values of the Hasse-Weil L-function divided by a transcendental number called the period. These values are algebraic and under suitable conditions, the p-adic L-function $L_p(E, T)$ is a power-series in a formal variable T, with coefficients in $\mathbb{Z}_p$

$$L_p(E,T) = b_r T^r + b_{r+1}T^{r+1} + \dots.$$

The generalized Euler characteristic in Iwasawa theory gives an explicit formula for the leading term $b_r(E,p)$. This formula is due to Perrin-Riou and Schneider.

Two elliptic curves E_1 and E_2 are said to be p-congruent if their associated modular forms are p-congruent. Alternatively, they are p-congruent if the residual Galois representations on the p-torsion groups $E_1[p]$ and $E_2[p]$ are isomorphic up to semisimplification. We assume that the residual representations are absolutely irreducible. In [RS20], we show that if E_1 and E_2 are p-congruent of the same rank r, then there is explicit relation between the Euler characteristics $b_r(E_1,p)$ and $b_r(E_2,p)$.

In subsequent work [RS21b], we extend the results in [RS20] to pairs of p-congruent elliptic curves E_1 and E_2 defined over a number field F. We assume that these elliptic curves have semistable reduction at all primes of F above p. In particular, we do consider the case when the elliptic curves could have supersingular reduction at some primes above p. This case is special since the Selmer groups associated to such elliptic curves are not cotorsion over the Iwasawa algebra. We study the structure of *multi-signed Selmer groups*. These Selmer groups generalize the signed Selmer groups introduced by Kobayashi in [Kob03].

3.2. **Iwasawa invariants of symmetric square representations.** We now explain the results in [RSV21], which is joint with R. Sujatha and V. Vatsal. We consider two modular forms g_1 and g_2 that are $\mathfrak{p}$-congruent and study the Iwasawa theory of symmetric square representations associated with g_1 and g_2. Associated to the p-adic L-function of $\mathrm{Sym}^2(g_i)$ are the analytic Iwasawa invariants μ_i^{an} and λ_i^{an}. We establish congruences between p-adic L-functions and deduce that $\mu_1^{\mathrm{an}} = 0$ if and only if $\mu_2^{\mathrm{an}} = 0$. Furthermore, if these μ-invariants vanish, then, there is explicit formula for $\lambda_1^{\mathrm{an}} - \lambda_2^{\mathrm{an}}$ in terms of certain explicit locally defined invariants. Similar results are proven for the algebraic μ and λ-invariants μ_i^{alg} and λ_i^{alg} for the Selmer group of the symmetric square representations $\mathrm{Sym}^2(g_i)$. The main conjecture predicts that $\mu_i^{\mathrm{alg}} = \mu_i^{\mathrm{an}}$ and $\lambda_i^{\mathrm{alg}} = \lambda_i^{\mathrm{an}}$. We show that if these relations are satisfied for g_1, then, they are satisfied for g_2 as well.

Congruences between p-adic L-functions in this context are proven by exploiting a formula of Shimura. The formula expresses special values for the L-function of the symmetric square of f in terms of the Petersson inner product of f with a certain nearly holomorphic modular form. The Petersson inner product is related related to a certain abstractly defined algebraic inner product defined by Hida after dividing by a certain transcendental period. We show that the ordinary holomorphic projection of the nearly holomorphic modular form has nice integral properties. With these preparations, it becomes possible to prove our results on congruences, since the algebraic inner product is continuous and $\mathbb{Z}_p$-linear.

4. Arithmetic statistics and Iwasawa theory

Given an elliptic curve over a number field F, the Mordell–Weil theorem states that the group of rational points $E(F)$ is finitely generated as an abelian group. In the special case when $F = \mathbb{Q}$, the torsion part of $E(\mathbb{Q})$ is well understood, and a complete list of torsion groups is enumerated by Mazur, see [Maz77]. On the other hand, the rank of $E(\mathbb{Q})$ is a mysterious quantity. When elliptic curves $E_{/\mathbb{Q}}$ are ordered according to height, the *rank distribution conjecture* predicts that 50% of elliptic curves have Mordell–Weil rank 0, 50% have rank 1 and 0% of them have rank ≥ 2. Unconditional results about rank distribution are proven by Bhargava and Shankar [BS15a, BS15b, BS13], who study the average size of certain Selmer groups of E over $\mathbb{Q}$. For instance, it is shown that the average size of the 5-Selmer group, as E is allowed to vary over all elliptic curves, is 6. As a result, it is deduced that the average rank of elliptic curves is < 1.

4.1. **Statistics for cyclotomic Iwasawa invariants.** In [KR21a], which is joint with D. Kundu, we study the average structure of the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$ as E varies over all elliptic curves. More precisely, we study the following questions.

(1) Given an elliptic curve $E_{/\mathbb{Q}}$, how do the Iwasawa invariants $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}})$ and $\lambda_p(E/\mathbb{Q}_{\mathrm{cyc}})$ vary as p varies over all primes of good reduction.
(2) Given a prime p, how do the Iwasawa invariants $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}})$ and $\lambda_p(E/\mathbb{Q}_{\mathrm{cyc}})$ vary as E varies over all elliptic curves over $\mathbb{Q}$ with respect to height.

Here, if E has good supersingular reduction at p, then, we consider the Iwasawa invariants of Kobayashi's signed Selmer groups. We provide answers to both questions, however, it should be noted that the second question is of significant interest from the perspective of arithmetic statistics, and has not been studied before.

We show that there is an explicit upper bound for the upper density of elliptic curves of rank zero for which the Iwasawa invariants do not vanish. In greater detail, for $x > 0$, let $\mathcal{Z}_p(x)$ be the set of elliptic curves $E_{/\mathbb{Q}}$ of rank 0 with good ordinary reduction at p of height $< x$ such that either $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}}) \neq 0$ or $\lambda_p(E/\mathbb{Q}_{\mathrm{cyc}}) \neq 0$. Let $\mathcal{E}_p(x)$ be the set of all elliptic curves $E_{/\mathbb{Q}}$ of height $< x$. Then, we show that there is an explicit upper bound (depending on p) for

$$\limsup_{x\to\infty} \frac{\#\mathcal{Z}_p(x)}{\#\mathcal{E}_p(x)}.$$

This upper bound assumes a heuristic of Delaunay [Del01], which states that the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})$ is finite and the proportion of elliptic curves $E_{/\mathbb{Q}}$ of rank zero for which p divides the order of $\text{Ш}(E/\mathbb{Q})$ is

$$d_0(p) := 1 - \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^{2j-1}}\right) = \frac{1}{p} + \frac{1}{p^3} - \frac{1}{p^4} + \dots$$

The upper bound we obtain relies on the work of Cremona-Sadek [CS20] and Lenstra [LJ87], and states that if $p \geq 5$ is a prime, then, we have that

$$\limsup_{x\to\infty} \frac{\#\mathcal{Z}_p(x)}{\#\mathcal{E}_p(x)} < d_0(p) + (\zeta(p) - 1) + Cp^{\frac{-1}{2}} \log p \left(\log\log p\right)^2,$$

where C is an explicit constant independent of p. The connection to the work of Lenstra has been realized in subsequent work, see [Ray21f, Lemma 6.4] and [KLR21, Lemma 9.5]. This upper bound approaches 0 as $p \to \infty$.

In subsequent work [KR21d], we show that for any integer $N > 0$, the proportion of elliptic curves $E_{/\mathbb{Q}}$ with λ-invariant $\geq N$ is positive. In greater detail, fix $p \geq 5$ and $N \geq 0$. For $x > 0$, let $\mathcal{E}_N(x)$ be the set of elliptic curves $E_{/\mathbb{Q}}$ of height $< x$ with good ordinary reduction at p such that

$$\mu_p(E/\mathbb{Q}_{\mathrm{cyc}}) + \lambda_p(E/\mathbb{Q}_{\mathrm{cyc}}) \geq N.$$

Let $\mathcal{E}(x)$ be the set of all elliptic curves $E_{/\mathbb{Q}}$ with height $< x$. We show that the lower density $\mathfrak{d}_{p,N} := \liminf_{x\to\infty} \frac{\#\mathcal{E}_N(x)}{\#\mathcal{E}(x)}$ is positive and calculate an explicit lower bound for $\mathfrak{d}_{p,N}$, see [KR21d, Corollary 6.5]. This quantity decreases in p and N. Since it is expected that the μ-invariant vanishes for 100% of elliptic curves, the result indicates that there is an explicit lower bound for the lower density of elliptic curves with $\lambda \geq N$.

4.2. **Statistics for anticyclotomic Iwasawa invariants.** Given an imaginary quadratic field K, there are two $\mathbb{Z}_p$-extensions K_{cyc}/K and K_{ac}/K that are Galois over $\mathbb{Q}$. The anticyclotomic extension K_{ac} is a pro-dihedral extension of $\mathbb{Q}$.

Let E be an elliptic curve over K. There is a dichotomy between two cases of interest, namely the *definite* and *indefinite* cases. In the definite (resp. indefinite) case, the p-primary Selmer group $\text{Sel}_{p^\infty}(E/K_{\text{ac}})$ is cotorsion (resp. not cotorsion) over the Iwasawa algebra. Anticyclotomic Iwasawa theory in the definite case closely mirrors classical Iwasawa theory over the cyclotomic $\mathbb{Z}_p$-extension. There is a stark difference in the tools used to study the indefinite case.

In [HKR21], which is joint with J. Hatley and D. Kundu, the results of [KR21a] are extended to the anti-cyclotomic setting. We only consider elliptic curves $E_{/\mathbb{Q}}$ with good ordinary reduction at the odd prime p. The Iwasawa invariants $\mu_p(E/K_{\text{ac}})$ and $\lambda_p(E/K_{\text{ac}})$ are associated to any triple (E, K, p). We study the following questions in both definite and indefinite cases:

(1) Given an elliptic curve $E_{/\mathbb{Q}}$ and a prime p at which E has good ordinary reduction, how do the Iwasawa invariants vary as K varies over imaginary quadratic fields ordered by conductor?
(2) Given a pair (E, K), how do the Iwasawa invariants vary as p varies over all primes at which E has good ordinary reduction?
(3) Given a pair (K, p), how do the Iwasawa invariants vary as E varies over all rational elliptic curves with good ordinary reduction at p?

In the indefinite case, we show that there is an explicit relationship between the Iwasawa invariants of $\text{Sel}_{p^\infty}(E/K^{\text{ac}})$ to those of a certain modified Selmer group. The results in this case are proven by exploiting the p-adic Birch and Swinnerton-Dyer formula for the leading term of the Bertolini-Darmon-Prasanna p-adic L-function, see section 10 of *loc. cit.* for more details and references.

4.3. **Arithmetic statistics and noncommutative Iwasawa theory.** The study of Iwasawa theory in p-adic Lie extensions (that are not necessarily commutative) was initiated by Harris in [Har79]. Such extensions are ubiquitous and arise naturally, here are some examples of interest

- F_∞/F is a $\mathbb{Z}_p^d$-extension of F, where $d \geq 1$,
- Let ℓ be a prime number, F_∞ be the False-Tate curve extension of $F = \mathbb{Q}(\mu_p)$, given by
$$F_\infty := \mathbb{Q}(\mu_{p^\infty}, \ell^{\frac{1}{p^\infty}}).$$
- Let A be an elliptic curve over $\mathbb{Q}$ and set F_∞ to be the field $\mathbb{Q}(A[p^\infty])$, i.e., the field generated by the p-primary torsion points of A. When A does not have complex multiplication, the Galois group $\text{Gal}(F_\infty/\mathbb{Q})$ can be realized as a finite index subgroup of $\text{GL}_2(\mathbb{Z}_p)$.

In the late 1990's and early 2000's, noncommutative Iwasawa theory became an active area of research, leading to a series of breakthrough results (see [BH97, CH01, Ven02, OV02, CSS03, Gre03, HV03, OV03, Ven03, CFK+05, CFKS10]). The methods of classical (abelian) Iwasawa theory do not extend in any obvious fashion to the noncommutative theory and there are several pitfalls if one follows such an approach, see [BH97, section 2] for a discussion.

In [KLR21], which is joint with D. Kundu and A. Lei, we extend some of the results of [KR21a] to the noncommutative setting. The questions in arithmetic statistics we study in this setting lead to explicit results, and many examples of interest. The field of noncommutative Iwasawa theory is terse, the arithmetic statistical approach shows that precise results can be proven on average. The reader is referred to the introduction of [KLR21] for a detailed description of our results.

5. Iwasawa theory and Diophantine stability for the Mordell–Weil and Tate–Shafarevich group

5.1. Rank jumps and growth of Tate–Shafarevich groups in p-cyclic extensions.

We describe the results in [BKR21], which is joint work with L. Beneish and D. Kundu. We study the stability and growth of the Mordell–Weil group and Tate–Shafarevich group of an elliptic curve $E_{/\mathbb{Q}}$ in various $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$. Given an elliptic curve $E_{/\mathbb{Q}}$ and a prime $p \geq 7$, heuristics of David-Fearnley-Kisilevsky [DFK04] indicate that there are only finitely many $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$ such that $\operatorname{rank} E(L) > \operatorname{rank} E(\mathbb{Q})$. On the other hand, the p-rank of the Tate–Shafarevich group is known to become arbitrarily large in $\mathbb{Z}/p\mathbb{Z}$, see [CS10]. We apply ideas from Iwasawa theory to study the stability of the Mordell–Weil groups and Tate–Shafarevich groups of elliptic curves in cyclic p-extensions. The main results of this paper are easy to state and are quoted below.

It follows from results of Greenberg that if $E_{/\mathbb{Q}}$ is an elliptic curve of Mordell–Weil rank 0 and does not have complex multiplication, then, $\mu_p(E/\mathbb{Q}_{\text{cyc}}) = 0$ and $\lambda_p(E/\mathbb{Q}_{\text{cyc}}) = 0$ for 100% of primes p of good ordinary reduction.

Theorem 5.1. Given an elliptic curve $E_{/\mathbb{Q}}$ with Mordell–Weil rank 0 and a prime $p \geq 7$ with
$$\mu_p(E/\mathbb{Q}_{\text{cyc}}) = \lambda_p(E/\mathbb{Q}_{\text{cyc}}) = 0,$$
there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions of $L/\mathbb{Q}$ in which
$$\lambda_p(E/L_{\text{cyc}}) = \lambda_p(E/\mathbb{Q}_{\text{cyc}}).$$
In particular, in infinitely many cyclic degree p number fields the rank does not grow.

Corollary 5.2. Given an elliptic curve $E_{/\mathbb{Q}}$ and a prime $p > 7$ with
$$\mu_p(E/\mathbb{Q}_{\text{cyc}}) = \lambda_p(E/\mathbb{Q}_{\text{cyc}}) = 0,$$
there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$ where the Mordell–Weil group is stable, i.e., $E(L) = E(\mathbb{Q})$.

Theorem 5.3. Let $p \geq 5$ be a fixed prime and $E_{/\mathbb{Q}}$ be an elliptic curve with good ordinary reduction at p. Suppose that the following conditions are satisfied:

(1) the image of the residual representation is surjective,
(2) the p-primary Selmer group $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q})$ is trivial,

(3) $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}}) = \lambda(E/\mathbb{Q}_{\mathrm{cyc}}) = 0$.

Then, there is a set of primes of the form $q \equiv 1 \pmod{p}$ with density at least $\frac{p}{(p-1)^2(p+1)}$ such that the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/L)$ becomes non-trivial in the unique $\mathbb{Z}/p\mathbb{Z}$-extension L contained in $\mathbb{Q}(\mu_q)$.

Theorem 5.4. For a positive proportion of rank 0 elliptic curves defined over $\mathbb{Q}$, there is *at least one* $\mathbb{Z}/p\mathbb{Z}$-extension over $\mathbb{Q}$ disjoint from the cyclotomic $\mathbb{Z}_p$-extension, $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$, with trivial p-primary Selmer group upon base-change.

5.2. **Diophantine stability.** In [Ray21f], the above results are strengthened. In [MRL18], Mazur and Rubin introduced the notion of *diophantine stability* for an irreducible variety V defined over a number field K. The study of this notion has applications to Hilbert's 10th problem.

Definition 5.5. Let p be a prime number. Given a number field extension L/K, V is said to be *diophantine stable* in L if $V(L) = V(K)$. The variety V is diophantine stable at p if for any choice of $n \in \mathbb{Z}_{\geq 1}$ and finite set of primes Σ of K, V is diophantine stable in infinitely many $\mathbb{Z}/p^n\mathbb{Z}$-extensions L/K in which the primes of Σ split.

Inspired by the notion of diophantine stability (for the Mordell-Weil group), we introduce an analogous notion for the p-primary part of the Tate-Shafarevich group.

Definition 5.6. Let p be a prime number and $L/\mathbb{Q}$ a cyclic p-extension. We say that E is Ш-stable in $L/\mathbb{Q}$ if $\#Ш(E/L)[p^\infty] = \#Ш(E/\mathbb{Q})[p^\infty]$. Further, E is said to be Ш-stable at p if for any (n, Σ), there are infinitely many $\mathbb{Z}/p^n\mathbb{Z}$-extensions in which the primes of Σ split and in which E is Ш-stable.

From a statistical point of view, we are interested in the following questions.

Question 5.7. (1) Given an elliptic curve $E_{/\mathbb{Q}}$, what can be said about proportion of primes p at which E is diophantine stable and Ш-stable at p?
(2) Given a prime p, what can be said about proportion of elliptic curves $E_{/\mathbb{Q}}$ ordered by height that are diophantine stable and Ш-stable at p?

We also study the growth of the Selmer group in various p-cyclic extensions, and provide answers to the above questions, see [Ray21f, Theorems A-E].

6. Constructing Galois representations with prescribed Iwasawa invariants

We introduce techniques from deformation theory to study certain questions about the Iwasawa theory of Galois representations.

6.1. **μ-invariants of residually reducible Galois representations.** Let E be an elliptic curve over $\mathbb{Q}$ and p an odd prime. A conjecture of Greenberg states that if the Galois representation on $E[p]$ is irreducible, then the μ-invariant $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}}) = 0$. On the other hand, Mazur constructed examples when $E[p]$ is reducible as a module over $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\mu_p(E/\mathbb{Q}_{\mathrm{cyc}}) > 0$. We describe the results in [RS21a], which is joint with R. Sujatha. We study the μ-invariant for 2-dimensional Galois representations associated to Hecke eigencuspforms f with good ordinary reduction at p, such that the residual representation

$$\bar{\rho}_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

is reducible. In this case, the Galois representation $\bar{\rho}_f$ is of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$, where φ_i are characters. We classify such Galois representations $\bar{\rho}_f$ into two types: residually aligned and residually skew, see Definition 3.1 in *loc. cit.* The classification is based on a very explicit criterion. We show that $\mu_p(E) > 0$ when the residual representation is aligned and examples show that $\mu_p(E) = 0$ when it is skew. Then, in section 4 of *loc. cit.* we study invariants that are further refinements of the μ-invariant and prove explicit results for these invariants. The results are proven for general p-adic Lie extensions and specialize to the cyclotomic case.

We then come to the main application of deformation theory. Given a residually reducible representation $\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}(\bar{\mathbb{F}}_p)$ and an integer $N > 0$, we lift it to a characteristic zero representation

$$\rho_N : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}(\bar{\mathbb{Z}}_p)$$

which arises from a Galois stable lattice in a modular Galois representation, such that the μ-invariant of the p-primary Selmer group of ρ_N is $\geq N$. This result extends that of Hamblen and Ramakrishna [HR08], who prove a version of Serre's conjecture for residually reducible Galois representations of dimension 2. This result shows that modular lifts can be constructed so that the associated μ-invariants become arbitrarily large. When N is large, it can be expected that ρ_N is ramified at a large set of primes.

We state the main result.

Theorem 6.1. [RS21a, Theorem 1.1] Let N be a non-negative integer, p a prime and $\mathbb{F}$ a finite field of characteristic p. Let $\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{F})$ be a Galois representation such that $\bar{\rho} \simeq \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix}$. Assume that $\bar{\rho}$ is indecomposable, and φ satisfies some additional mild conditions (see the statement of Theorem 1.1 of *loc. cit.*).

Let k be a positive integer such that $k \equiv 2 \mod p^N(p-1)$. Then there is a Galois representation

$$\rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathrm{W}(\mathbb{F}))$$

which lifts $\bar{\rho}$ such that:

(i) ρ lifts $\bar{\rho}$ and arises from a modular form,
(ii) the μ-invariant of the p-primary Selmer group associated to ρ is $\geq N$.

The lifting theorem above may be contrasted with a result of Bellaïche and Pollack [BP19], who study the variation of μ-invariants in a Hida family of tame level 1. On the other hand, in our construction, we have full control of the weight of the modular form, however, the level of the lift could be arbitrarily large.

6.2. **Constructing Galois representations with large λ-invariant.** Greenberg showed that given a prime p there are elliptic curves $E_{/\mathbb{Q}}$ such that $\mu_p(E/\mathbb{Q}_{\text{cyc}}) + \lambda_p(E/\mathbb{Q}_{\text{cyc}})$ can be arbitrarily large. The result is specific to elliptic curves and relies on arithmetic geometry techniques. It is of natural interest to generalize such results to Galois representations associated to modular forms of arbitrary weight, however, due to the lack of arithmetic geometric tools, a new idea is needed. We describe the main result of [Ray21e]. Given an irreducible Galois representation

$$\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{F}}_p),$$

satisfying further conditions, it is shown that $\bar{\rho}$ may be lifted to a modular Galois representation such that λ is arbitrarily large when the $\mu = 0$ conjecture is satisfied. The method relies on suitably extending the approach of Fakhruddin-Khare-Patrikis [FKP19] to lift the Galois representation $\bar{\rho}$ to a characteristic zero representation satisfying suitable local conditions at an auxiliary set of primes at which it is allowed to ramify. Combining this lifting result with results of Greenberg-Vatsal [GV00] in the ordinary case and Hatley-Lei [HL19a] in the supersingular case, the λ-invariant of the lift is arranged to as arbitrarily large. In other words, given an integer $N > 0$, it is shown that there is a lift of $\bar{\rho}$ arising from a Hecke eigencuspform f_N such that the associated λ-invariant is $\geq N$. The results are illustrated by an infinite family of examples, see Theorem 5.4 of *loc. cit.*

7. Growth questions in Iwasawa theory

7.1. **Rational points on algebraic curves in infinite towers of number fields.** Let K be a number field and p a prime. For $n \geq 1$, denote by $K_n^{(p)}$ the Galois extension of K with $[K_n^{(p)} : K] = p^n$ which is contained in the infinite cyclotomic extension $K(\mu_{p^\infty})$. In other words, $K_n^{(p)}$ is the n-th layer in the cyclotomic $\mathbb{Z}_p$-tower over K. It was shown by Kato and Rohlrich that if E is an elliptic curve defined over $\mathbb{Q}$ and K is any abelian number field, then, $\operatorname{rank} E(K_n^{(p)})$ is bounded as $n \to \infty$. The study of growth questions in towers is an active area of research and is intimately related to Iwasawa theoretic properties of Selmer groups.

Given the interest in studying questions about the growth of ranks of elliptic curves, it is natural to ask similar questions for curves of higher genus. In this context, the celebrated theorem of Faltings states that if $X_{/K}$ is an *nice* curve of genus $g > 1$, then the set of rational points $X(K_n^{(p)})$ is finite for all n. A natural question is to characterize the growth of $\#X(K_n^{(p)})$ as $n \to \infty$.

This question is studied in [Ray21h], let us summarize the results.

- Using results of Mazur and Imai, we show that $\#X(K_n^{(p)})$ is bounded provided some additional conditions are satisfied (see [Ray21h, Theorem 3.4]). This proves (the analog of) the Mordell–conjecture over the infinite extension $K_{\text{cyc}}^{(p)} := \bigcup_{n\geq 1} K_n^{(p)}$.
- We prove an upper bound for the minimum value $m_0 = m_0(p)$ such that $X(K_n^{(p)}) = X(K_{m_0}^{(p)})$ for all $n > m_0$. Using this bound, we prove results about the variation of $m_0(p)$ as $p \to \infty$. This relies on explicitly understanding the torsion in the Jacobian of X over the cyclotomic $\mathbb{Z}_p$-extension.
- We then consider the case when the Jacobian of X has Mordell–Weil rank zero and establish an explicit criterion for $X(K_n^{(p)})$ to be equal to $X(K)$ for all n. This criterion indicates that for 100% of primes p above which the Jacobian of X has good ordinary reduction, $X(K_{\text{cyc}}^{(p)}) = X(K)$, in the rank zero setting.
- We also obtain a generalization of Imai's theorem for all pro-p extensions. The result states that if $A_{/K}$ is an abelian variety for the adelic Galois representation has big image, and the p-torsion subgroup of $A(K)$ is trivial, then the torsion subgroup of $A(K_\infty)$ is finite, for all infinite pro-p extensions K_∞/K. This result makes no assumption on the reduction-type of A at the primes above p.

7.2. **Asymptotic growth of Mordell–Weil ranks in non-commutative towers.** We describe the results in [Ray21g]. Let F be a number field, $p \geq 5$ a prime and F_∞ an infinite Galois extension of F with pro-p Galois group $G = \text{Gal}(F_\infty/F)$. The lower central p-series of G is recursively defined as follows:

$$G_0 := G \text{ and } G_{n+1} := G_n^p[G_n, G].$$

Make the following standard assumptions on F_∞

(1) G is uniform and pro-p,
(2) only finitely many primes ramify in F_∞,
(3) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F.

The extension F_∞ is filtered by a tower of number fields, set $F^{(n)} := F_\infty^{G_n}$. For elliptic curves $E_{/F}$, we prove asymptotic formulas for the growth of the rank of $E(F^{(n)})$ as $n \to \infty$. Similar results are proven by Delbourgo and Lei [DL17] and Hung and Lim [HL19b]. The results are proven via a new technique which allows us to significantly improve upon previous results.

Let $Q_1 = Q_1(E, F_\infty)$ (resp. $Q_2 = Q_2(E, F_\infty)$) be the set of primes $w \nmid p$ of F_{cyc} that are ramified in F_∞, at which E has split multiplicative reduction (resp. E has good reduction and $E(F_{\text{cyc},w})[p] \neq 0$). For $i = 1, 2$, we set $q_i := \#Q_i$, and let d be the dimension of G. We have the following bound

$$\operatorname{rank} E(F^{(n)}) \leq p^{n(d-1)}\lambda_p(E/F) + \left(p^{n(d-1)} - p^{n(d-2)}\right)(q_1 + 2q_2).$$

The bounds may be made explicit in the following cases:

- F_∞/F is a $\mathbb{Z}_p^d$-extension of F, where $d \geq 1$,
- Let ℓ be a prime number, F_∞ be the False-Tate curve extension of $F = \mathbb{Q}(\mu_p)$, given by
$$F_\infty := \mathbb{Q}(\mu_{p^\infty}, \ell^{\frac{1}{p^\infty}}).$$
- Let E be an elliptic curve over $\mathbb{Q}$ and $F = \mathbb{Q}(E[p])$. Set F_∞ to be the field $\mathbb{Q}(E[p^\infty])$, i.e., the field generated by the p-primary torsion points of E. In this case, $F^{(n)} = \mathbb{Q}(E[p^{n+1}])$.

8. Iwasawa theory: Miscellaneous results

8.1. **μ-invariants of fine Selmer groups.** We state the results in [KR21b], which is joint work with D. Kundu. Let E be an elliptic curve over an imaginary quadratic field K and p an odd prime. Assume that the associated Galois representation

$$\bar{\rho} : \text{Gal}(\bar{K}/K) \to \text{GL}_2(\mathbb{F}_p)$$

is reducible. We formulate explicit conditions for which the μ-invariant of the *fine Selmer group* of E over the anticyclotomic extension K_{an} vanishes (see [KR21b, Definition 2.9, Theorem 3.2 and Corollary 3.5]). Our results are complicated by the fact that unlike the cyclotomic extension, there is infinite splitting of primes in the anticyclotomic extension.

8.2. **Iwasawa theory in $\mathbb{Z}_p$-extensions.** We state the results in [KR21c], which is joint with D. Kundu. Let L/K be a finite p-extension of number fields. Hachimori and Matsuno prove that the λ-invariant of L_{cyc}/L is related to the λ-invariant of K_{cyc}/K. We generalize this formula to arbitrary $\mathbb{Z}_p$-extensions. In greater detail, let K_∞ be any $\mathbb{Z}_p$-extension of K and set $L_\infty := L \cdot K_\infty$. Then, we show that $\lambda(E/L_\infty)$ is equal to $[L_\infty : K_\infty]\lambda(E/K_\infty)$ plus some locally defined auxiliary terms. We also study the behaviour of Iwasawa invariants with respect to congruences.

9. Galois representations: Overview

I use techniques from algebraic geometry and Galois cohomology to construct continuous Galois representations $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\bar{\mathbb{Q}}_p)$ with special properties. These techniques were developed in the past to study a conjecture of Serre about the existence of characteristic zero lifts of mod-p Galois representations that arise from modular forms. Deformation theory also plays a major role in establishing the *modularity* of a Galois representation.

The first interesting examples of Galois representations are those associated to elliptic curves and certain modular forms. Let E be an elliptic curve defined over $\mathbb{Q}$ and $E[p^n] \subset E(\bar{\mathbb{Q}})$ its p^n-torsion subgroup. The p-adic Tate module of an elliptic curve E is the inverse limit

$$\text{T}_p(E) := \varprojlim_n E[p^n] \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$$

where the inverse limit is taken w.r.t the multiplication by p maps. The Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts naturally on the $\text{T}_p(E)$, which induces the p-adic Galois representation

$$\rho_{E,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{Q}_p}(\text{T}_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \xrightarrow{\sim} \text{GL}_2(\mathbb{Q}_p).$$

With respect to a choice of an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, there is a p-adic Galois representation associated to a Hecke eigencuspform f

$$\rho_{f,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\bar{\mathbb{Q}}_p).$$

Such Galois representations satisfy certain characteristic features.

Definition 9.1. Fontaine and Mazur [FM95] called an irreducible Galois representation $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\bar{\mathbb{Q}}_p)$ *geometric* if it satisfies the following properties:

(1) it is unramified at all but finitely many primes, i.e the inertia groups at all but finitely many primes are in the kernel of ρ.
(2) It is odd, namely, $\det \rho(c) = -1$, where c denotes complex-conjugation,
(3) It satisfies an additional local condition at p, namely, it is de–Rham at p.

Geometric Galois representations are expected to arise from the étale cohomology of varieties defined over the rational numbers. Fontaine and Mazur conjectured that a 2-dimensional geometric Galois representations $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\bar{\mathbb{Q}}_p)$ is modular, i.e. is the p-adic Galois representation attached to a Hecke eigencuspform. Most cases of the Fontaine-Mazur conjecture for $\text{GL}_{2/\mathbb{Q}}$ have been settled by Taylor [Tay02], Skinner-Wiles [SW99], Kisin [Kis09], Emerton [Eme06] and others.

10. Serre's Conjecture- Refinements and Generalizations

Let p be a prime and $\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{F}}_p)$ be an *irreducible* Galois representation. Serre's conjecture (proved by Khare and Wintenberger [KW09]) states that if $\bar{\rho}$ satisfies some further natural conditions, then $\bar{\rho}$ lifts to the p-adic Galois representation ρ_f associated to a modular eigenform f

$$\begin{array}{ccc} & & \operatorname{GL}_2(\bar{\mathbb{Z}}_p) \\ & \overset{\rho_f}{\nearrow} & \downarrow \\ \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow[\bar{\rho}]{} & \operatorname{GL}_2(\bar{\mathbb{F}}_p). \end{array}$$

(In the above diagram, the vertical map is induced from the reduction map $\bar{\mathbb{Z}}_p \to \bar{\mathbb{F}}_p$.) As, stated, this is the weak form of Serre's conjecture.

Before Serre's conjecture was proved, Ramakrishna (cf. [Ram02]) showed that an irreducible Galois representation $\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{F}}_p)$ as above lifts to a geometric Galois representation (cf. Definition 9.1). We draw attention a number of generalizations of Serre's conjecture/ Ramakrishna's theorem.

10.1. **Lifting Reducible Galois representations- Generalizations in Higher Dimensions.** The condition that $\bar{\rho}$ is irreducible is essential to the methods of Khare and Wintenberger. There has been interest in understanding if Serre's conjecture does hold if $\bar{\rho}$ is reducible and indecomposable, i.e when there are characters ψ_1 and ψ_2 and a nontrivial extension $*$ so that

$$\bar{\rho} \simeq \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

One would like to know if such a representation $\bar{\rho}$ lifts to an irreducible Galois representation $\rho_f : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{Z}}_p)$ which arises from an eigencuspform f.

Reducible representations $\bar{\rho}$ as above naturally arise from Galois stable quotients in ray class groups. We explain this through an example of note. Let p be an odd prime, the mod p cyclotomic character $\bar{\chi}$ induces an isomorphism $\bar{\chi} : \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^\times$. As Galois module, the mod p class-group $\mathcal{C} := \operatorname{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$ decomposes into eigenspaces

$$\mathcal{C} = \bigoplus_{i=0}^{p-2} \mathcal{C}(\bar{\chi}^i).$$

Each one-dimensional quotient of the $\mathbb{F}_p$-vector space $\mathcal{C}(\bar{\chi}^i)$ coincides with a reducible and indecomposable Galois representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^i & * \\ 0 & 1 \end{pmatrix}.$$

Hamblen and Ramakrishna [HR08] show that if $\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{F}}_p)$ is *reducible and indecomposable*, then under further natural conditions, $\bar{\rho}$ lifts to the Galois representation $\rho_f :\to \operatorname{GL}_2(\bar{\mathbb{Z}}_p)$ associated to an eigencuspform f. This settles the weak version of Serre's conjecture for such reducible Galois representations $\bar{\rho}$. This theorem is proved by showing that there exists a geometric lift $\rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\bar{\mathbb{Z}}_p)$ of $\bar{\rho}$. By the results of Skinner and Wiles [SW99], such a geometric lift arises from a Hecke eigencuspform. The following is the main result of [Ray21b].

Theorem 10.1. Let p be an odd prime number and $\bar{\rho}: G_{\mathbb{Q}} \to \mathrm{GSp}_{2n}(\bar{\mathbb{F}}_p)$ a reducible Galois representation which satisfies some additional conditions. Then $\bar{\rho}$ lifts to a *geometric* Galois representation ρ (cf. Definition 9.1)

$$\begin{array}{ccc} & & \mathrm{GSp}_{2n}(\bar{\mathbb{Z}}_p) \\ & \overset{\rho}{\nearrow} & \downarrow \\ \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow[\bar{\rho}]{} & \mathrm{GSp}_{2n}(\bar{\mathbb{F}}_p). \end{array}$$

Geometric lifting results like Theorem 10.1 complement modularity theorems by Skinner-Wiles [SW99] for GL_2. The above result has been generalized in recent work of Fakhruddin-Khare-Patrikis [FKP20].

10.2. **Lifting Galois representations in the supersingular case.** We describe the main result in [Ray21c]. Let $f = \sum_{n\geq 1} a_n q^n$ be a normalized Hecke eigencuspform and p be a prime. Set $\mathrm{G}_{\mathbb{Q}_p}$ to denote the local Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. The Fourier coefficients of f are algebraic numbers. Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, this induces an inclusion $\mathrm{G}_{\mathbb{Q}_p} \hookrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let v_p be the valuation on $\bar{\mathbb{Q}}_p$ normalized by $v_p(p) = 1$. The eigenform f is said to be *ordinary* at p if a_p is a p-adic unit and *supersingular* at p if not. Let $\rho_f = \rho_{f,p}$ denote the p-adic Galois representation (which coincides with this choice of embedding). The two cases can be distinguished as follows, f is p-supersingular if the restriction $\rho_{f\restriction_{\mathbb{Q}_p}}$ is irreducible and p-ordinary otherwise. Suppose that the level of f is coprime to p. Attached to f is its *slope* $s_p(f) := v_p(a_p(f))$, which is positive if and only if f is p-supersingular. From the perspective of the p-adic Langlands program, there has been some interest in classifying local representations $\rho_{f|_{\mathbb{Q}_p}}$ as f ranges over normalized eigencuspforms with slope in specific intervals $(a, b) \subset (0, \infty)$. Such investigations have been carried out in [BLZ04, BG09, BG13, GG15].

Let $\bar{\rho}: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ be a Galois representation for which $\bar{\rho}_{\restriction_{\mathbb{Q}_p}}$ is irreducible. If $\bar{\rho}$ lifts to a p-adic Galois representation ρ_f, then f must in particular be p-supersingular. However, f need not be the unique form lifting $\bar{\rho}$. From the point of view of the p-adic Langlands program one would like to understand to what extent the local representation $\rho_{f\restriction_{\mathbb{Q}_p}}$ is determined by the residual representation $\bar{\rho} = \bar{\rho}_f$. Motivated by this, we ask if all positive rational numbers $s \in \mathbb{Q}_{>0}$ can be realized as the p-adic slope $s = s_p(f)$ for some eigencuspform f of level coprime to p, such that ρ_f lifts the fixed residual representation $\bar{\rho}$. We prove the following result for modular forms of weight 2.

Theorem 10.2. Let $\bar{\rho}: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ be an odd Galois representation which is unramified outside a finite set of primes and $p \geq 5$ a prime. Assume that the restriction to the decomposition group $\bar{\rho}_{\restriction \mathrm{G}_{\mathbb{Q}_p}}$ is irreducible and $\det \bar{\rho} = \bar{\chi}$. Let $s \in \mathbb{Z}_{\geq 1}$. Under some additional hypotheses, there is a modular eigencuspform f_s of weight 2 and level coprime to p, such that

(1) the p-adic Galois representation ρ_{f_s} lifts $\bar{\rho}$,

(2) $s_p(f_s) = s$.

For an arbitrary choice of s, the normalized eigencuspform f_s would conceivably have a large level and have Fourier coefficients in a large number field extension. The key idea is that one may modify the local deformation functor of flat deformations of $\bar{\rho}_{\restriction \mathbb{Q}_p}$ in such a way that an analogue of the method of Ramakrishna can still produce geometric lifts with this additional prescribed local condition.

11. Constructing Galois representations with special properties

11.1. **Constructing Galois representations ramified at one prime.** A prime p is *regular* if p does not divide the class number of $\mathbb{Q}(\mu_p)$. Let M be the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ which is unramified at all primes $\ell \neq p$. Shafarevich showed that if p is a regular prime, then, $\operatorname{Gal}(M/\mathbb{Q}(\mu_p))$ is a free pro-p group with $\frac{p+1}{2}$ generators. Greenberg used this result to show that if p is regular and $p \geq \lfloor n/2 \rfloor + 1$, then, there is an infinite Galois extension $K \subset M$ such that $\operatorname{Gal}(K/\mathbb{Q})$ injects into $\operatorname{GL}_n(\mathbb{Z}_p)$ and contains a finite-index subgroup of $\operatorname{SL}_n(\mathbb{Z}_p)$, see [Gre16].

Generalizing such results to irregular primes requires a new approach since there are nontrivial relations in the presentation of $\operatorname{Gal}(M/\mathbb{Q})$ when p is irregular. We construct such Galois representations for irregular primes p. The approach involves lifing a suitable residual representation $\bar{\rho}$ one step at a time to characteristic zero.

Fix a sequence of integers $k_1, k_2, \dots, k_n$ and set $\bar{\rho}$ to denote the mod-p Galois representation which is a direct sum of characters $\bar{\chi}^{k_1} \oplus \cdots \oplus \bar{\chi}^{k_n}$. In other words, we have the residual representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^{k_1} & & & \\ & \bar{\chi}^{k_2} & & \\ & & \ddots & \\ & & & \bar{\chi}^{k_n} \end{pmatrix} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{F}_p).$$

Under suitable conditions on $k_1, \dots, k_n$, the residual representation $\bar{\rho}$ may be lifted to a suitable characteristic zero representation $\rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{Z}_p)$ which is unramified at all primes $\ell \neq p$.

The index of irregularity is the number of nontrivial eigenspaces of the mod-p class group of $\mathbb{Q}(\mu_p)$. Given a prime p with a bound on its index of irregularity, we are able to choose $k_1, \dots, k_n$ such that $\bar{\rho} = \operatorname{diag}(\bar{\chi}^{k_1}, \dots, \bar{\chi}^{k_n})$ may be suitably lifted to characteristic zero representation which is unramified away from p. In greater detail, the representation $\bar{\rho}$ can be chosen so that the associated global deformation problem is *unobstructed*, see [Ray21d, p.5]. It takes more work to construct a lift with big image. The following is the main result of *loc. cit.*

Theorem 11.1. Let $n > 1$, $e \geq 0$ and p be a prime number such that

(1) $p \geq 2^{n+2+2e} + 3$,
(2) the index of irregularity of p is $\leq e$.

There are infinitely many continuous representations $\rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{Z}_p)$ unramified at all primes $\ell \neq p$, such that the image of ρ contains $\ker\left(\operatorname{SL}_n(\mathbb{Z}_p) \to \operatorname{SL}_n(\mathbb{Z}/p^4)\right)$.

For a discussion on the expected proportion of primes p for which the index of irregularity is $\leq e$, see the introduction in *loc. cit.* When the above conditions are not satisfied, it is possible to check that a suitable tuple of integers $(k_1, \ldots, k_n)$ exists, see Theorem 3.3. of *loc. cit.*

11.2. **Constructing lifts of reducible Galois representations to Hida families.** Let f be a Hecke eigencuspform and let $\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ be the associated p-adic Galois representation. The representation ρ_f lies in a family of ordinary Galois representations known as a Hida family. This perspective of interpolating Galois representation in families has important applications, for instance the proof of the Iwasawa Main conjecture over totally real fields by Wiles relies on the study of such families. There is considerable interest in understanding describing the algebro-geometric properties of such families.

When the residual representation $\bar{\rho}_f$ is reducible, standard techniques are used to interpolate f in a family of pseudo-representations. As a consquence, if g is another modular form in the same family as f, then the residual representations $\bar{\rho}_f$ and $\bar{\rho}_g$ are the same *up to semisimplification*. In this case, $\bar{\rho}_f = \begin{pmatrix} \varphi_1 & \alpha \\ 0 & \varphi_2 \end{pmatrix}$ and $\bar{\rho}_g = \begin{pmatrix} \varphi_1 & \beta \\ 0 & \varphi_2 \end{pmatrix}$, where α, β give rise to classes in $H^1\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \bar{\mathbb{F}}_p(\varphi_1\varphi_2^{-1})\right)$. These classes could be different.

In [Ray21a], we construct Hida families lifting a reducible Galois representation $\bar{\rho}$, not up to semisimplification, but the entire representation (thus also capturing the class α). Thus we construct families such that for every Hecke eigencuspform g in the family, we have that $\bar{\rho}_g \simeq \bar{\rho}$ on the nose and not up to semi-simplification. In order to achieve this, we resort to a purely Galois theoretic construction, using ideas in deformation theory and Galois cohomological techniques. On allowing for additional ramification at an auxiliary set of primes at which certain deformation conditions are specified, such Hida families are constructed that are isomorphic to $\mathbb{Z}_p[\![T]\!]$.

11.3. **Constructing** $\mathrm{SL}_2(\mathbb{Z}_p)$**-extensions of** $\mathbb{Q}(\mu_{p^\infty})$ **that are unramified above** p**.** Let p be a prime number, the tame Fontaine-Mazur conjecture (conjecture 5a in [FM95]) posits that an infinite Galois extension of a number field K whose Galois group over K is isomorphic to a p-adic analytic group is either ramified at infinitely many primes or is infinitely ramified at a prime dividing p. It is natural to ask if finitely ramified extensions over the infinite cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$ exist that are unramified at the primes above p. The answer is affirmative, and this is the main result of [Ray20].

Theorem 11.2. Suppose that $p \geq 5$ be a prime and $i \neq \frac{p-1}{2}$ an odd integer between $2 \leq i \leq p-3$ for which the isotypic space $\mathcal{C}(\bar{\chi}^i) \neq 0$. There are infinitely many Galois extensions $F/\mathbb{Q}(\mu_{p^\infty})$ for which

- the Galois group $\mathrm{Gal}(F/\mathbb{Q}(\mu_{p^\infty}))$ topologically isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ which contains the principal congruence subgroup.
- F is unramified at primes above p and ramified above finitely many rational primes at which it is tamely ramified.

Such Galois extensions exist for a large collection of primes (which is infinite if one assumes Vandiver's conjecture).

12. Arithmetic statistics for Galois deformation rings

We describe the results in [RW21], which is joint with T. Weston. The results are based on heuristics and computation and are backed by theoretical results.

Given an elliptic curve E defined over the rationals, and a prime number p, denote by $E[p]$ the p-torsion subgroup of $E(\bar{\mathbb{Q}})$. Mazur introduced deformation functors, parametrizing lifts of the residual representation

$$\bar{\rho}: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

on $E[p]$. These functors are represented by universal deformation rings and their study gained considerable momentum in [Wil95, TW95, BCDT01], where the modularity of an elliptic curve $E_{/\mathbb{Q}}$ is established. The approach involved showing that a certain deformation ring associated to $\bar{\rho}$ is in fact isomorphic to a localized Hecke algebra associated to a space of modular forms. A result of this flavor which establishes an isomorphism between a deformation ring and a localized Hecke algebra is known as an $\mathrm{R} = \mathbb{T}$ theorem. Here, R refers to the deformation ring associated to a residual representation $\bar{\rho}$ and $\mathbb{T}$ is the associated localized Hecke algebra. The Galois representations which arise from elliptic curves and modular forms satisfy additional local conditions, and hence, the deformations functors of interest are subject to a local constraint at p, which is defined using p-adic Hodge theory. Given the importance of deformation rings in proving modularity results, it is of natural interest to explicitly characterize Galois deformation rings.

The deformation rings studied in this paper are equipped with a local condition at p. There is one such ring $\mathcal{R}_{E,p}$ associated to each pair (E, p), where E is a rational elliptic curve and p an odd prime at which E has good reduction. We study the structure of these rings on average, more precisely, how often they are unobstructed. Since the determinant is fixed throughout, the geometric deformation ring is smooth if and only of it is isomorphic to $\mathbb{Z}_p$. In this case, there is a unique characteristic-zero lift. We study the following questions.

(1) For a fixed elliptic curve E, how often is the deformation ring $\mathcal{R}_{E,p}$ unobstructed?
(2) For a fixed odd prime p and E varying over all rational elliptic curves with good reduction at p, how often is the deformation ring $\mathcal{R}_{E,p}$ unobstructed?

The answer to the first question follows from well-known results of Flach, Wiles and others. However, the second question has not been studied previously and the goal of our work is to provide heuristics backed by theoretical results and explicit computation. The main results are contained in [RW21, section 5]. The deformation ring $\mathcal{R}_{E,p}$ is unobstructed provided the degree of the modular parametrization $X_0(N) \to E$ is coprime to p. This condition has been studied in detail by M.Watkins in [Wat02]. Cohen-Lenstra heuristics indicate that the probability that p divides the modular degree of an elliptic curve is given by the product

$$1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^i}\right) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} + \dots.$$

We refer to the computations in [RW21, section 5.2].

13. Arithmetic geometry results

We describe some results in arithmetic geometry.

13.1. **Perfectoid Spaces.** Scholze introduced a certain class of spaces called *perfectoid* spaces which have played a crucial role in settling a number of conjectures in arithmetic geometry and led to advances in p-adic Hodge theory and the local Langlands program. These spaces facilitate for a correspondence between characteristic zero objects and their positive characteristic analogues. It turns out that in positive characteristic one is equipped with many more tools which make some arithmetic geometric results more accessible. Given the paramount importance of perfectoid spaces, it is of interest to develop some algebro-geometric tools to work with such a class of spaces. The difficulty in doing this is that these spaces are highly non-Noetherian, as a result conventional algebro-geometric results do not hold up.

In [DHRW20], which is joint with G. Dorfsman-Hopkins and P. Wear, we characterize the Picard groups of perfectoid covers of toric varieties. We state the main result.

Theorem 13.1. Let Σ be a fan consisting of strongly convex rational cones and K a perfectoid field of characteristic zero with residual characteristic p. Let k denote the residue field. Assume that

(1) Σ is a smooth fan,
(2) the support of Σ is convex (this condition is clearly satisfied when Σ is complete).

Let $\mathcal{X}^{perf}$ be the perfectoid cover associated to the smooth toric variety $X = X_{\Sigma,K}$ (the toric variety associated to the fan Σ defined over the field K). Let X_0 denote the toric variety $X_{\Sigma,k}$. Then

$$\text{Pic}(\mathcal{X}^{perf}) \simeq \text{Pic}(X)[p^{-1}].$$

13.2. **Statistics for p-rank of Artin-Schreier covers.** The study of curves over finite fields leads to many interesting problems in arithmetic statistics. Recently, statistical questions have been framed and studied for curves varying in certain naturally occurring ensembles, see for instance, [Rud08, KR09, Xio10, BDFL11, TX14, CWZ15, BDF+16, BDFL16, San19]. Throughout, p will denote a prime number and q will be a power of p. The field with q elements is denoted $\mathbb{F}_q$. Given a curve $\mathcal{C}$ of positive genus g over $\mathbb{F}_q$, its arithmetic is better understood by studying the structure of its Jacobian $\text{Jac}(\mathcal{C})$, which is a g-dimensional abelian variety. An important invariant associated to the curve is the p-rank of $\text{Jac}(\mathcal{C})(\bar{\mathbb{F}}_p)$, which we denote by τ. This is the number such that $\text{Jac}(\mathcal{C})(\bar{\mathbb{F}}_p) \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\tau}$.

Given $f(x)$ a rational function with coefficients in $\bar{\mathbb{F}}_p(x)$. The Artin-Schreier cover $X_f \to \mathrm{P}^1$ is defined by the equation $y^p - y = f(x)$. Its Galois group is $\mathbb{Z}/p\mathbb{Z}$ and generated by the automorphism $(x, y) \mapsto (x, y + 1)$.

In [Ray21i], we study the following questions

Thus, the two main questions studied are as follows.

(1) *Geometric problem:* Given a prime p, what is the statistics for p-ranks of Artin-Schreier covers with fixed genus over $\mathbb{F}_q$, as $q \to \infty$?
(2) *Arithmetic problem:* Suppose we are given an integer $d > 0$. Then, what is the statistics for p-ranks of Artin-Schreier covers over $\mathbb{F}_p$ as $p \to \infty$?

The proportions are calculated in terms of certain partitions. For the main results, we refer the reader to [Ray21i, Theorem 3.7, Theorem 3.12].

14. Computational Aspect of my work

Many of the questions I study are significantly informed by computation. This section summarizes the comptational aspect of my research.

14.1. **Statistics in Iwasawa theory.** Arithmetic statistics in the context of Iwasawa theory of elliptic curves was initiated in the papers [KR21a, KR21d], see the discussion in section 4. The results are extended to the anticyclotomic setting [HKR21] and the non-commutative setting [KLR21]. Although many of the results in these papers are proved unconditionally, there are also aspects that boil down to heuristics. For instance, many of the results rely on a heuristic of Delaunay on the variation of the Tate-Shafarevich group. When the elliptic curve in question has positive rank, the p-adic regulator also plays a role. In the anticyclotomic setting, there is a precise relationship between certain invariants associated with Heegner points and the Iwasawa invariants we study. The computation of these invariants requires significant computational dexterity. The reader is referred to [HKR21, Table 3, section 11]. There are no computer packages that perform such computations. It is difficult to prove theoretical results about the statistical variation of such invariants, instead in some cases, we must resort to heuristics supported by computation. Our investigations lead to many potentially interesting computational projects related to modular curves.

14.2. **Statistics for Galois deformation rings.** The statistics for Galois deformation rings come down to the existence of congruences between modular forms, which in turn is related to degree of the modular parametrization map. There are precise heuristics for the probability that this degree is divisible by a prime p, and they are based on Cohen Lenstra heuristics, see the discussion in section 12. However, verifying such heuristics for large enough primes takes work, and effective computations that count congruences between modular forms must be performed for a large number of modular forms. To get good data, we computed congruence primes for the 13,352 isogeny classes of elliptic curves of conductor at most 4000 to see that the data does roughly match the heuristic, see [RW21, section 5.2].

14.3. **Heuristics for Iwasawa invariants.** Although the results in [KR21a] do give some satisfactory results for the average variation of Iwasawa invariants, there is much left to be desired. In ongoing work with D. Kundu and L. Washington, we formulate a heuristic for the precise variation of Iwasawa invariants. The heuristic is based on that of Poonen-Rains [PR12] and Bhargava-Kane-Lenstra-Poonen-Rains [BKL$^+$15], which is formulated over a number field. In our work, we study the relevant properties that Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension must satisfy and formulate heuristics for Iwasawa modules satisfying these abstract properties. The predictions are now verified through extensive computation of Iwasawa invariants and p-adic L-functions. It will take significant computational skill to see that our the predictions match computational evidence, since such heuristics are known to have a slow rate of convergence.

14.4. **Iwasawa invariants in $\mathbb{Z}_p$-extensions.** In [KR21c, section 7], we compute examples of elliptic curves E over an imaginary quadratic field K such that the anticyclotomic λ-invariant $\lambda_p(E/K_{\text{an}})$ is large. We specialize our computations to $p = 5$ and $K = \mathbb{Q}(i)$ and consider the elliptic curve $E = y^2 = x^3 - x$. We use the parametrization of Rubin and Silverberg of elliptic curves E_t that are 5-congruent to E. In the paper, we generalize results of Greenberg and Vatsal to arbitrary $\mathbb{Z}_p$-extensions. The difficulty that arises here is that a prime may be infinitely split in such extensions. We use these results to construct an elliptic curve E_t which is 5-congruent to E such that the λ-invariant is large. The calculation involves a number of steps. The number field $\mathbb{Q}(E[5])$ is defined by a polynomial of degree 32. We need explicit information about primes ℓ that split in this number field. To obtain splitting information, we implement known algorithms to calculate the modular function $\Phi_5(X,Y)$, see p.23 of *loc. cit.* for further details. Such computations are difficult since there are no computer packages that can be used to compute them. We are able to construct an example for which $\lambda_5(E_t/K_{\text{an}}) \geq 4$. It is difficult to find elliptic curves that satisfy all the conditions we impose since the coefficients of the elliptic curve in the family of Rubin and Silverberg get large exponentially fast.

14.5. **Iwasawa theory and Hilbert's 10th problem.** This is work in progress. I hope to use Iwasawa theory to construct examples of number fields K such that $\mathcal{O}_K$ is diophantine over $\mathbb{Z}$. This would give rise to new instances of Hilbert's 10-th problem for number fields. Such results are known for totally real number fields K that are totally real, and number fields that are abelian. I hope to study Hilbert's 10th problem for the various finite layers in an anticyclotomic $\mathbb{Z}_p$-extension K_{ac} of an imaginary quadratic field. This can be achieved using a criterion of Schlapentokh, which states that if L/K is any extension of number fields, then $\mathcal{O}_L$ is diophantine over $\mathcal{O}_K$ if there exists an elliptic curve $E_{/K}$ such that $\operatorname{rank} E(L) = \operatorname{rank} E(K) > 0$. We refer to [GFP20] for a survey of this circle of ideas. The hope is to construct examples of elliptic curves $E_{/K}$ of positive (even) rank such that $\operatorname{rank} E(K^{\text{ac}}) = \operatorname{rank} E(K)$, using ideas in Iwasawa theory.

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over q: wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939, 2001.

[BDF+16] Alina Bucur, Chantal David, Brooke Feigon, Nathan Kaplan, Matilde Lalín, Ekin Ozman, and Melanie Matchett Wood. The distribution of $\mathbb{F}_q$-points on cyclic ℓ-covers of genus g. *International Mathematics Research Notices*, 2016(14):4297–4340, 2016.

[BDFL11] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Biased statistics for traces of cyclic p-fold covers over finite fields., 2011.

[BDFL16] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalin. Statistics for ordinary artin-schreier covers and other p-rank strata. *Transactions of the American Mathematical Society*, 368(4):2371–2413, 2016.

[BG09] Kevin Buzzard and Toby Gee. Explicit reduction modulo p of certain two-dimensional crystalline representations. *International Mathematics Research Notices*, 2009(12):2303–2317, 2009.

[BG13] Kevin Buzzard and Toby Gee. Explicit reduction modulo p of certain 2-dimensional crystalline representations, ii. *Bulletin of the London Mathematical Society*, 45(4):779–788, 2013.

[BH97] Paul N Balister and Susan Howson. Note on Nakayama's lemma for compact Λ-modules. *Asian J. Math.*, 1(2):224–229, 1997.

[BKL+15] Manjul Bhargava, Daniel M Kane, Hendrik W Lenstra, Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, selmer groups, and shafarevich-tate groups of elliptic curves. *Cambridge Journal of Mathematics*, 2015.

[BKR21] Lea Beneish, Debanjana Kundu, and Anwesh Ray. Rank Jumps and Growth of Shafarevich-Tate Groups for Elliptic Curves in $\mathbb{Z}/p\mathbb{Z}$-extensions. *arXiv preprint arXiv:2107.09166*, 2021.

[BLZ04] Laurent Berger, Hanfeng Li, and Hui June Zhu. Construction of some families of 2-dimensional crystalline representations. *Mathematische Annalen*, 329(2):365–377, 2004.

[BP19] Joël Bellaïche and Robert Pollack. Congruences with eisenstein series and-invariants. *Compositio Mathematica*, 155(5):863–901, 2019.

[BS13] Manjul Bhargava and Arul Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859*, 2013.

[BS15a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[BS15b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[CFK$^+$05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. Inst. Hautes Études Sci.*, 101:163–208, 2005.

[CFKS10] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha. Root numbers, Selmer groups, and non-commutative Iwasawa theory. *J. Algebraic Geom.*, 19(1):19–97, 2010.

[CH01] John Coates and Susan Howson. Euler characteristics and elliptic curves. II. *J. Math. Soc. Japan*, 53(1):175–235, 2001.

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

[CS20] JE Cremona and M Sadek. Local and global densities for Weierstrass models of elliptic curves. *arXiv preprint arXiv:2003.08454*, 2020.

[CSS03] John Coates, Peter Schneider, and Ramdorai Sujatha. Links between cyclotomic and GL_2 Iwasawa theory. *Doc. Math.*, (Extra Vol.):187–215, 2003. Kazuya Kato's fiftieth birthday.

[CWZ15] GilYoung Cheong, Melanie Wood, and Azeem Zaman. The distribution of points on superelliptic curves over finite fields. *Proceedings of the American Mathematical Society*, 143(4):1365–1375, 2015.

[Del01] Christophe Delaunay. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experimental Mathematics*, 10(2):191–196, 2001.

[DFK04] Chantal David, Jack Fearnley, and Hershy Kisilevsky. On the vanishing of twisted l-functions of elliptic curves. *Experimental Mathematics*, 13(2):185–198, 2004.

[DHRW20] Gabriel Dorfsman-Hopkins, Anwesh Ray, and Peter Wear. On Picard Groups of Perfectoid Covers of Toric Varieties. *arXiv preprint arXiv:2011.03613 (submitted to European J. Math. & going through revisions)*, 2020.

[DL17] Daniel Delbourgo and Antonio Lei. Estimating the growth in mordell–weil ranks and shafarevich–tate groups over lie extensions. *The Ramanujan Journal*, 43(1):29–68, 2017.

[Eme06] Matthew Emerton. A local-global compatibility conjecture in the p-adic langlands programme for gl 2/q. *Pure and Applied Mathematics Quarterly*, 2(2):279–393, 2006.

[EPW06] Matthew Emerton, Robert Pollack, and Tom Weston. Variation of iwasawa invariants in hida families. *Invent. math*, 163:523–580, 2006.

[FKP19] Najmuddin Fakhruddin, Chandrashekhar Khare, and Stefan Patrikis. Relative deformation theory and lifting irreducible galois representations. *arXiv preprint arXiv:1904.02374*, 2019.

[FKP20] Najmuddin Fakhruddin, Chandrashekhar Khare, and Stefan Patrikis. Lifting and automorphy of reducible mod p galois representations over global fields. *arXiv preprint arXiv:2008.12593*, 2020.

[FM95] Jean-Marc Fontaine and Barry Mazur. Geometric galois representations. *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I*, pages 41–78, 1995.

[GFP20] Natalia Garcia-Fritz and Hector Pasten. Towards hilbert's tenth problem for rings of integers through iwasawa theory and heegner points. *Mathematische Annalen*, 377(3):989–1013, 2020.

[GG15] Abhik Ganguli and Eknath Ghate. Reductions of galois representations via the mod p local langlands correspondence. *Journal of Number Theory*, 147:250–286, 2015.

[Gre03] Ralph Greenberg. Galois theory for the Selmer group of an abelian variety. *Compositio Mathematica*, 136(3):255–297, 2003.

[Gre16] Ralph Greenberg. Galois representations with open image. *Annales mathématiques du Québec*, 40(1):83–119, 2016.

[GV00] Ralph Greenberg and Vinayak Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. math.*, 142(1):17–63, 2000.

[Har79] Michael Harris. p-adic representations arising from descent on abelian varieties. *Compositio Math.*, 39(2):177–245, 1979.

[HKR21] Jeffrey Hatley, Debanjana Kundu, and Anwesh Ray. Statistics for Anticyclotomic Iwasawa Invariants of Elliptic Curves. *arXiv preprint arXiv:2106.01517*, 2021.

[HL19a] Jeffrey Hatley and Antonio Lei. Arithmetic properties of signed selmer groups at non-ordinary primes. In *Annales de l'Institut Fourier*, volume 69, pages 1259–1294, 2019.

[HL19b] Pin-Chi Hung and Meng Fai Lim. On the growth of mordell-weil ranks in p-adic lie extensions. *arXiv preprint arXiv:1902.01068*, 2019.

[HR08] Spencer Hamblen and Ravi Ramakrishna. Deformations of certain reducible galois representations, ii. *American journal of mathematics*, 130(4):913–944, 2008.

[HV03] Yoshitaka Hachimori and Otmar Venjakob. Completely faithful Selmer groups over Kummer extensions. *Doc. Math.*, (Extra Vol.):443–478, 2003. Kazuya Kato's fiftieth birthday.

[Kis09] Mark Kisin. The fontaine-mazur conjecture for GL_2. *Journal of the American Mathematical Society*, 22(3):641–690, 2009.

[KL19] Daniel Kriz and Chao Li. Goldfeld's conjecture and congruences between heegner points. In *Forum of Mathematics, Sigma*, volume 7. Cambridge University Press, 2019.

[KLR21] Debanjana Kundu, Antonio Lei, and Anwesh Ray. Arithmetic Statistics and noncommutative Iwasawa Theory. *arXiv preprint arXiv:2109.13330*, 2021.

[Kob03] Shin-ichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Inventiones mathematicae*, 152(1):1–36, 2003.

[KR09] Pär Kurlberg and Zeév Rudnick. The fluctuations in the number of points on a hyperelliptic curve over a finite field. *Journal of Number Theory*, 129(3):580–587, 2009.

[KR21a] Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa invariants of Elliptic curves. *Transactions of the American Mathematical Society*, 374(11):7945–7965, 2021.

[KR21b] Debanjana Kundu and Anwesh Ray. Anticyclotomic μ-invariants of residually reducible Galois representations. *Journal of Number Theory (in press)*, 2021.

[KR21c] Debanjana Kundu and Anwesh Ray. Iwasawa Invariants for elliptic curves over $\mathbb{Z}_p$-extensions and Kida's Formula. *arXiv preprint arXiv:2103.16005*, 2021.

[KR21d] Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa Invariants of elliptic curves, II. *arXiv preprint arXiv:2106.12095*, 2021.

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (ii). *Inventiones mathematicae*, 178(3):505, 2009.

[LJ87] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[MRL18] Barry Mazur, Karl Rubin, and Michael Larsen. Diophantine stability. *American Journal of Mathematics*, 140(3):571–616, 2018.

[OV02] Yoshihiro Ochi and Otmar Venjakob. On the structure of Selmer groups over p-adic Lie extensions. *J. Alg. Geom.*, 11(3):547–580, 2002.

[OV03] Yoshihiro Ochi and Otmar Venjakob. On the ranks of Iwasawa modules over p-adic Lie extensions. *Math. Proc. Cambridge Philos. Soc.*, 135(1):25–43, 2003.

[PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[Ram02] Ravi Ramakrishna. Deforming galois representations and the conjectures of serre and fontaine-mazur. *Annals of mathematics*, 156(1):115–154, 2002.

[Ray20] Anwesh Ray. Constructing certain special analytic Galois extensions. *Journal of Number Theory*, 212:105–112, 2020.

[Ray21a] Anwesh Ray. Deformations of reducible Galois representations to Hida-families. *International Journal of Number Theory (in press)*, 2021.

[Ray21b] Anwesh Ray. Deformations of certain reducible Galois representations III. *International Journal of Number Theory*, 17:1–57, 2021.

[Ray21c] Anwesh Ray. A refined lifting theorem for supersingular Galois representations. *Journal of Number Theory*, 229:282–313, 2021.

[Ray21d] Anwesh Ray. Constructing Galois representations ramified at one prime. *Journal of Number Theory*, 222:168–180, 2021.

[Ray21e] Anwesh Ray. Constructing Galois representations with large Iwasawa λ-invariant. *arXiv preprint arXiv:2105.00147*, 2021.

[Ray21f] Anwesh Ray. Arithmetic statistics and diophantine stability for elliptic curves. *arXiv preprint arXiv:2109.00830*, 2021.

[Ray21g] Anwesh Ray. Asymptotic growth of Mordell-Weil ranks of elliptic curves in noncommutative towers. *arXiv preprint arXiv:2109.07457*, 2021.

[Ray21h] Anwesh Ray. Rational points on algebraic curves in infinite towers of number fields. *arXiv preprint arXiv:2110.02371*, 2021.

[Ray21i] Anwesh Ray. Statistics for p-ranks of Artin-Schreier covers. *arXiv preprint arXiv:2110.08714*, 2021.

[RS20] Anwesh Ray and R Sujatha. Euler Characteristics and their Congruences for Multi-signed Selmer Groups. *arXiv preprint arXiv:2011.05387 (submitted to Canadian J. Math.* & *going through revisions)*, 2020.

[RS21a] Anwesh Ray and R Sujatha. On the μ-invariants of residually reducible Galois representations. *arXiv preprint arXiv:2104.10797*, 2021.

[RS21b] Anwesh Ray and Ramdorai Sujatha. Euler characteristics and their congruences in the positive rank setting. *Canadian Mathematical Bulletin*, 64(1):228–245, 2021.

[RSV21] Anwesh Ray, Ramdorai Sujatha, and Vinayak Vatsal. Iwasawa invariants of symmetric square representations. *preprint, available on request*, 2021.

[Rud08] Zeév Rudnick. Traces of high powers of the frobenius class in the hyperelliptic ensemble. *arXiv preprint arXiv:0811.3649*, 2008.

[RW21] Anwesh Ray and Tom Weston. Arithmetic statistics for Galois deformation rings. *arXiv preprint arXiv:2108.13480*, 2021.

[San19] Soumya Sankar. Proportion of ordinarity in some families of curves over finite fields. *arXiv preprint arXiv:1904.12173*, 2019.

[SU14] Christopher Skinner and Eric Urban. The iwasawa main conjectures for gl 2. *Inventiones mathematicae*, 195(1):1–277, 2014.

[SW99] Christopher M Skinner and Andrew J Wiles. Residually reductible representations and modular forms. *Publications Mathématiques de l'IHÉS*, 89:5–126, 1999.

[Tay02] Richard Taylor. Remarks on a conjecture of fontaine and mazur. *Journal of the Institute of Mathematics of Jussieu*, 1(1):125–143, 2002.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics*, pages 553–572, 1995.

[TX14] Frank Thorne and Maosheng Xiong. Distribution of zeta zeroes for cyclic trigonal curves over a finite field. *preprint*, 2014.

[Ven02] Otmar Venjakob. On the structure theory of the Iwasawa algebra of a p-adic Lie group. *J. European Math. Soc.*, 4(3):271–311, 2002.

[Ven03] Otmar Venjakob. On the Iwasawa theory of p-adic Lie extensions. *Compositio Mathematica*, 138(1):1–54, 2003.

[Wat02] Mark Watkins. Computing the modular degree of an elliptic curve. *Experimental Mathematics*, 11(4):487–502, 2002.

[Wil95] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

[Xio10] Maosheng Xiong. The fluctuations in the number of points on a family of curves over a finite field. *Journal de théorie des nombres de Bordeaux*, 22(3):755–769, 2010.

Department of Mathematics, University of British Columbia, Vancouver BC, Canada V6T 1Z2

Email address: anweshray@math.ubc.ca