Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

March 27, 2024

Contents

Introduction

Notation

We use the following notation for characters:

$R_{\mathbb{C}}(G)$	the ring of characters of representations of G over $\mathbb{C}$,
$R_{\mathbb{Q}}(G)$	the ring of characters of representations of G over $\mathbb{Q}$,
$\mathrm{Irr}_{\mathbb{C}}(G)$	the set of characters of complex irreducible representations of G,
$\mathrm{Irr}_{\mathbb{Q}}(G)$	the set of characters of $\mathbb{Q}$-irreducible representations of G,
$\mathbb{Q}(\rho)$	the field of character values of a complex character ρ,
$m(\rho)$	the Schur Index of an irreducible complex character ρ over $\mathbb{Q}(\rho)$,

1 Algebraic number theory and representation theory background

1.1 Representation theory of finite groups

Let G be a finite group. Recall that a **representation** of G is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ where V is a complex vector space. Associated to a representation ρ is a **character** $\chi\colon G \to \mathbb{C}^\times$, defined by letting $\chi(g) = \operatorname{Tr}\rho(g)$ for $g \in G$. For complex represenations, ρ is determined by its character; if ρ, ρ' are representations with identical characters, then ρ and ρ' are isomorphic as representations.

Given an irreducible $\mathbb{Q}G$-representation with character ψ, we have that

$$\psi = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho) \cdot \rho^\sigma$$

for ρ the character of an irreducible $\mathbb{C}G$-representation, and $m(\rho)$ the Schur index.

In particular, the map $R_\mathbb{C}(G) \to R_\mathbb{Q}(G)$ given by sending an irreducible complex character ρ to $\tilde{\rho} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho) \cdot \rho^\sigma$ is surjective.

Induction, Restriction…

Theorem 1.1 (Mackey Decomposition)**.**

1.1.1 Permutation representations and the Burnside ring

Let G be a finite group. The **Burnside ring** $B(G)$ is the ring of formal sums of isomorphism classes of finite G-sets. We have addition by disjoint union: $[S] + [T] = [S \sqcup T]$, and multiplication by Cartesian product: $[S] \times [T] = [S \times T]$ for S, T finite G-sets.

There exists a bijection between the isomorphism classes of transitive G-sets and the conjugacy classes of subgroups $H \leq G$, where H is the stabilizer of a point on which G acts. Then any transitive G-set X is isomorphic to the action of G on G/H for $H \leq G$, so that we can consider $B(G)$ to be a $\mathbb{Z}$-module generated by the orbits of the action of G on the elements $\{G/H \colon H \leq G\}$, where we consider H up to conjugacy. For notational purposes, we then write elements $\Theta \in B(G)$ as $\Theta = \sum_i n_i H_i$ with $n_i \in \mathbb{Z}$, $H_i \leq G$.

Given a transitive G-set G/H for $H \leq G$, we can look at the permutation representation $\mathbb{C}[G/H]$. This defines a homomorphism from the Burnside ring to the rational representation ring $R_\mathbb{Q}(G)$ of G:

$$a\colon B(G) \to R_\mathbb{Q}(G), \qquad \sum_i n_i H_i \mapsto \sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1}_{H_i}.$$

Elements in the kernel of this map are known as **Brauer relations**

1.2 Decompositions of primes in field extensions

1.3 Class field theory

Consider an odd prime p. Let $\mathbb{Q}(\sqrt{p^*}) = \begin{cases} \mathbb{Q}(\sqrt{p}), & p \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-p}), & p \equiv 1 \pmod 3 \end{cases}.$

Proposition 1.2. $\mathbb{Q}(\sqrt{p^*})$ *has odd narrow class number.*

Corollary 1.3. *The prime* $p \in \mathbb{Q}$ *is the norm of an element in* $\mathbb{Q}(\sqrt{p^*})^\times$.

2 Proving things. . .

2.1 Norm relations

Recall that in Section 1.1, we associated to $\rho \in R_{\mathbb{C}}(G)$ the character

$$\widetilde{\rho} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho)\rho^{\sigma} \quad \in R_{\mathbb{Q}}(G).$$

Call $\Theta = \sum_i n_i H_i \in B(G)$ a **ρ-relation** if

$$\sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1} \simeq \widetilde{\rho}.$$

Given such a ρ, consider functions $\psi \colon B(G) \to \mathbb{Q}^\times / N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ (written multiplicatively). We say two functions ψ, ψ' are **ρ-equivalent**, written $\psi \sim_\rho \psi'$, if ψ/ψ' is trivial on all ρ-relations.

If $\Theta \in \ker \psi$, then $\psi(\Theta)$ is the norm of an element from $\mathbb{Q}(\rho)^\times$. We call an instance of this a **norm relation**. In particular, when $\psi \sim_\rho 1$, then we obtain a norm relation for all ρ-relations Θ.

Remark 2.1. If $\rho = 0$ then we call functions $\psi \sim_\rho 1$ **representation theoretic**. These have been studied in cite.

Example 2.2. Take $\rho = 0$, and V a representation of G. The function $\psi(H) = \dim V^H$ satisfies $\psi \sim_\rho 1$ as $\dim V^H = \langle \mathrm{Res}_H V, \mathbb{1}_H \rangle = \langle V, \mathrm{Ind}_H^G \mathbb{1} \rangle$ by Frobenius reciprocity.

Example 2.3. Let $G = C_p$ for p a prime. Let ρ be a character of degree p. There is a unique ρ-relation given by $\Theta = C_1 - C_p$. Let $\psi(H) = [G \colon H]$. Then $\psi(\Theta) = p$, which is a norm from $\mathbb{Q}(\zeta_p)$ by Corollary 1.3.

Example 2.4. Let $G = C_n$. For each $d \mid n$, let $\chi_d = \widetilde{\varphi_d}$, where φ_d is an irreducible complex character of G with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d. Then $\{\chi_d \colon d \mid n\}$ form a basis for the irreducible rational-valued representations of G. Note that $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G contain $C_{n/d}$ in their kernel. Thus, $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain the unqiue φ_d-relation for each $d \mid n$:

$$\chi_d = \sum_{d' \mid d} \mu(d/d') \cdot \mathrm{Ind}_{C_{n/d}}^G \mathbb{1}.$$

Example 2.5. Let $E/\mathbb{Q}$ be an elliptic curve, $G = \mathrm{Gal}(F/\mathbb{Q})$ for $F/\mathbb{Q}$ a Galois extension. For $H \leq G$, the function $\psi \colon H \mapsto C(E/F^H)$ extends to a multiplicative function on the Burnside ring. Given a representation ρ of G, one can ask when $\psi \sim_\rho 1$.

2.1.1 D-local functions

(This is taken from section 2.3 of Vlad and Tim's regulator constants paper.)

Consider $G = \mathrm{Gal}(F/\mathbb{Q})$ and intermediate field F^H for $H < G$. Let p be a prime with decomposition group D in G. Then the primes above p in F^H correspond to double cosets $H\ G/D$. If a prime w in F^H coresponds to the double coset HxD, then its decomposition and inertia groups in F/F^H are $H \cap D^x$ and $H \cap I^x$ respectively. In partiular, the ramification degree and residue degree over $\mathbb{Q}$ are given by $e_w = \frac{|I|}{|H \cap I^x|}$ and $f_w = \frac{[D \colon I]}{[H \cap D^x \colon H \cap I^x]}$.

Our fudge factors $C(E/F)$ are defined locally; one has $C(E/F) = \prod_v c_v(E/F) \cdot |\omega/\omega_{v,\min}|$. Here v runs over finite places of F, ω is a global minimal differential for $E/\mathbb{Q}$, and $\omega_{v,\min}$ is a minimal differential at v. Considering the function $H \mapsto C(E/F^H)$, and writing $C_p(E/F^H) = \prod_{v|p} c_v(E/F) \cdot |\omega/\omega_{v,\min}|$ one has

$$\sum_i n_i H_i \mapsto \prod_i C(E/F^{H_i})^{n_i} = \prod_p C_p(E/F^H)^{n_i}.$$

Therefore, our function is the product of local functions for each p. Since $C_p(E/F^H)$ depends on e_w, f_w for $w|p$, we are motivated to define the following:

Definition 2.6. Suppose $I \lhd D < G$ with D/I cyclic, and $\psi(e,f)$ is a function of $e, f \in \mathbb{N}$. Define

$$(D, I, \psi): \quad H \mapsto \prod_{x \in H\backslash G/D} \psi\left(\frac{|I|}{|H \cap I^x|}, \frac{[D\colon I]}{[H \cap D^x\colon H \cap I^x]}\right).$$

Then, this is a function on the Burnside ring.

Example 2.7. For semi-stable reduction, we're considering $\psi(e,f) = e$ (the Tamagawa number). For the d_v terms in the case of additive potentially good reduction at p (p not equal to 2 or 3), we consider $\psi(e,f) = p^{f\lfloor en/12 \rfloor}$, where $n \in \{2,3,4,6,9,10\}$.

2.2 Compatibility in odd order extensions

Consider $G = \mathrm{Gal}(F/\mathbb{Q})$ with odd order, and $E/\mathbb{Q}$ an elliptic curve with good reduction at wildly ramified primes in $F/\mathbb{Q}$. Consider a relation of the form

$$\Theta = \sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1} \simeq \rho \oplus \tau(\rho), \tag{1}$$

where ρ is a character of G with $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = \langle \tau \rangle$ of size 2. Let m denote the minimal positive integer such that $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_m)$. The sum on the left is over subgroups $H_i \leq G$.

Observe that $\mathrm{Res}_D \rho$, where D is a decomposition group of exponent n, is rationally-valued when $m \nmid n$. In the context of norm relations, if $\mathrm{Res}_D \rho = \mathrm{Res}_D \tau(\rho)$, then we always get squares. Thus the interesting case is when $m \mid n$.

We understand Res_D best when D is cyclic. Let $D = C_n$ with $m \mid n$. Applying Res_D to (1), we get

$$\sum_i n_i \sum_{x \in H_i\backslash G/D} \mathrm{Ind}_{D \cap x^{-1} H_i x}^D \mathbb{1} \simeq \mathrm{Res}_D \rho \oplus \tau(\mathrm{Res}_D \rho). \tag{2}$$

Since both sides are now rationally valued, we can write this as $\sum_{d|n} a_d \cdot \chi_d$ where $a_d \in \mathbb{Z}$ and χ_d are defined in Example 2.4. Writing each χ_d in terms of permutation representations as in the Example, one obtains an expression for the LHS of (1) (since cyclic groups have no Brauer relations, this is on the nose). Therefore, if $\psi(\Theta) = \prod_p \psi(\mathrm{Res}_{D_p} \Theta)$, we have $\psi(\mathrm{Res}_{D_p} \Theta) = \prod_{d|n} \psi(\chi_d)^{a_d}$ whenever $D_p = C_n$.

As such, we'd like to be able to reduce to cyclic decomposotion groups. As we only assume bad reduction at tamely ramified primes in $F/\mathbb{Q}$, one has that I is cyclic. It turns out that we may assume that $D = I$ when $[D\colon I]$ is odd.

Lemma 2.8. *In an odd degree unramified extension, Tamagawa numbers change only up to squares. In particular, if $[D\colon I]$ is odd, then $(D, I, \psi) \sim_\rho (I, I, \psi)$ for any ρ with $\mathbb{Q}(\rho)$ even, where $\psi(e, f)$ is the Tamagawa number.*

Proof. Yadada □

2.2.1 Semistable reduction

In this subsection we work towards proving the following:

Theorem 2.9. *Let $F/\mathbb{Q}$ be a Galois extension of odd degree, with $G = \mathrm{Gal}(F/\mathbb{Q})$. Consider a semistable elliptic curve $E/\mathbb{Q}$ with good reduction at primes that are wildly ramified in $F/\mathbb{Q}$.*

Then, for any $\rho \in R_{\mathbb{C}}(G)$ with $[\mathbb{Q}(\rho)\colon \mathbb{Q}] > 1$, the function $f\colon B(G) \to \mathbb{Q}^\times/N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ sending $H \mapsto C(E/F^H)$ satisfies $f \sim_\rho 1$.

2.2.2 dv terms in additive reduction

2.2.3 Tamagawa numbers in additive reduction

We use the following description of Tamagawa numbers.

Lemma 2.10. *Let $K'/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let E/K be an elliptic curve with addtive reduction;*

$$E\colon y^2 = x^3 + Ax + B,$$

with discriminant $\Delta = -16(4A^3 + 27B^2)$. Let $\delta = v_K(\Delta)$, and $e = e_{K'/K}$.

If E has potentially good reduction, then

$$\begin{aligned}
\gcd(\delta e, 12) = 2 &\quad\Longrightarrow\quad c_v(E/K') = 1, && (II, II^*)\\
\gcd(\delta e, 12) = 3 &\quad\Longrightarrow\quad c_v(E/K') = 2, && (III, III^*)\\
\gcd(\delta e, 12) = 4 &\quad\Longrightarrow\quad c_v(E/K') = \begin{cases} 1, & \sqrt{B} \notin K' \\ 3, & \sqrt{B} \in K' \end{cases}, && (IV, IV^*)\\
\gcd(\delta e, 12) = 6 &\quad\Longrightarrow\quad c_v(E/K') = \begin{cases} 2, & \sqrt{\Delta} \notin K' \\ 1 \textit{ or } 4, & \sqrt{\Delta} \in K' \end{cases}, && (I_0^*)\\
\gcd(\delta e, 12) = 12 &\quad\Longrightarrow\quad c_v(E/K') = 1. && (I_0)
\end{aligned}$$

Moreover, the extensions $K'(\sqrt{B})/K'$ and $K'(\sqrt{\Delta})/K'$ are unramified.

So suppose an elliptic curve $E/\mathbb{Q}$ has additive reduction at p, with $p \geq 5$. Then we can write $E\colon y^2 = x^3 + Ax + B$. Let $D = \mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_p)$ be the local Galois group at p. Assume that p is totally tamely ramified, so that $D = I = C_n$. Since there is no wild ramification, and $f = 1$, this means that $n \mid p - 1$. We consider the contribution corresponding to an irreducible rational character χ_d of D, given by

$$\prod_{d'|d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')}. \tag{3}$$

Observe that in a totally ramified extension of degree coprime to 12, the Tamagawa number remains the same. If $(12, d) = 1$, then $(12, d') = 1$ for $d' \mid d$, so the Tamagawa number is consant accross subfields $F_{\mathfrak{p}}^{D_{d'}}$. Therefore,

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')} = C(E/\mathbb{Q}_p)^{\sum_{d' \mid d} \mu(d/d')} = 1,$$

assuming $d > 1$.

So we only need to worry about when $3 \mid d$. If we have type III or III^* or I_0^* then the Tamagawa number is still unchanged in any totally ramified cyclic extension of degree dividing d. We will treat the other cases seperately:

Type II and II^* reduction:

Firstly, suppose that $\delta = 2$, that is we have Type II reduction. If $3 \mid d'$ then $E/F_{\mathfrak{p}}^{D_{d'}}$ has type I_0^* reduction. The Tamagawa number then depends on whether $\sqrt{\Delta} \in \mathbb{Q}_p$. Since we have additive reduction, we know that $p \mid A$, $p \mid B$. Moreover, $\delta = 2$ implies that $v_p(B) = 1$. Then, $\Delta = p^2 \cdot \alpha$, and $\alpha \equiv -27 \cdot \square \pmod{p}$. Therefore $\sqrt{\Delta} \in \mathbb{Q}_p \iff -3$ is a square $\pmod{p}$. But this is the case; we assumed $p \equiv 1 \pmod{n}$, so $p \equiv 1 \pmod{3}$. Therefore the Tamagawa number will be 1 or 4, which is a square. If $3 \nmid d'$ then the reduction type over $F_{\mathfrak{p}}^{D_{d'}}$ is II or II^*. Then the Tamagawa number is 1. Thus in total, we get a square contribution from (3).

If $\delta = 10$, then $E/F_{\mathfrak{p}}^{D_{d'}}$ has reduction type I_0^* whenever $3 \mid d'$. Once more, $v_p(A), v_p(B) \geq 1$, and $v_p(\Delta) = 10 = \min(3v_p(A), 2v_p(B))$ maybe this is suss $\implies v_p(B) = 5$. Therefore we get $\Delta = p^{10}\alpha$ with $\alpha \equiv -27 \cdot \square \pmod{p}$, and we conclude as above.

Type IV and IV^* reduction:

Now, if $E/\mathbb{Q}_p$ has additive reduction of type IV or IV^*, it attains good reduction over any totally ramified cyclic extension of degree divisible by 3. This could result with 3 coming up an odd number of times in our Tamagawa number product, when $\sqrt{B} \notin \mathbb{Q}_p$.

In summary,

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')} = \begin{cases} 1 & 3 \nmid d, \\ 1 & 3 \mid d, \delta \in \{0, 3, 6, 9\}, \\ 1 \cdot \square & 3 \mid d, \delta \in \{2, 10\}, \\ 3^a \cdot \square, a \in \{0, 1\} & 3 \mid d, \delta \in \{4, 8\}. \end{cases} \tag{4}$$

Remark 2.11. There's no reason why we can't get 3; see elliptic curve 441b1 with additive reduction at 7 of type IV and Tamagawa number equal to 3)

However, it turns out we will only get 3 occuring oddly when $d = 3$. Indeed, one has that $\langle \mathrm{Ind}_{D_{d'}}^{D} \mathbb{1}, \psi_3 \rangle = 1$ if $3 \mid d'$, and 0 if $3 \nmid d'$, where ψ_3 is an irreducible character of D of order 3. Therefore one sees that the number of places with ramification degree divisible by 3 cancels unless $d = 3$. Indeed, $\langle \chi_d, \psi_3 \rangle = 0$ unless $d = 3$, in which case it is 1. Therefore (3) can only be non-square when $d = 3$.

3 Representations, L-functions and Artin Twists

3.1 Artin Representations and ℓ-adic Representations

The Birch-Swinnerton-Dyer conjecture classically provides a connection between the arithmetic of elliptic curves and their L-functions. In this prelimiary section, we explore the classical definition of L-functions attached to an elliptic curve and their twists, and we explore some of the relevant properties that we will use later on. To do so, we first need to explore the notion of an Artin representation and of an ℓ-adic representation.

Throughout this section we fix a field K, which will either be a number field or a local field of characteristic 0. We also fix an algebraic closure $\hat{K}$ of K and we denote by G_K the absolute galois group $\mathrm{Gal}(\bar{K}/K)$ of K. We recall that G_K is a profinite group

$$G_K = \varprojlim_F \mathrm{Gal}(F/K),$$

where F ranges over the finite Galois extensions of K and therefore has a natural topology where a basis of open sets is given by $\mathrm{Gal}(\bar{K}/F)$ where F is a finite extension of K.

Definition 3.1. Let K be a number field or a local field with characteristic 0. An **Artin representation** ρ over K is a complex finite-dimensional vector space V together with a homomorphism $\rho\colon G_K \to \mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$ such that there is some finite Galois extension F/K with $\mathrm{Gal}(\bar{K}/F) \subseteq \ker\rho$. In other words, ρ factors through $\mathrm{Gal}(F/K)$ for some finite extension F of K.

Hence, an Artin representation can be equivalently viewed as a finite dimensional representation of $\mathrm{Gal}(F/K)$ where F is some finite Galois extension of K. Throughout the document, we will use both notions depending of the context, and refer to either of them as Artin representations.

Remark 3.2. The condition above that $\mathrm{Gal}(\bar{K}/F) \subseteq \ker\rho$ is equivalent to $\ker\rho$ being open in G_K. This clearly implies that ρ is a continuous homomorphism of topological groups. Surprisingly, the converse is also true: a continous homomorphism $\rho\colon G_K \to \mathrm{GL}_n(\mathbb{C})$ has open kernel. The proof of this result relies on the fact that 'small' neighbourhoods of the identity in $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$ do not contain any non-trivial subgroups. Hence, if $\phi\colon G_K \to \mathrm{GL}(V)$ is continous and U is such a neighbourhood in $\mathrm{GL}(V)$, then $\phi^{-1}(U) \subseteq \ker\phi$ and $\phi^{-1}(U)$ is open, showing that $\ker\rho$ is open too. Hence the above condition is equivalent to continuity of ρ with respect to the natural topologies.

Next, we define the notion of an ℓ-adic representation, which will be needed to define the L-function of an elliptic curve.

Definition 3.3. Let K be a number field or a local field of characteristic 0. A **continuous ℓ-adic representation** ρ over K is a continous homomorphism $\rho\colon G_K \to \mathrm{GL}_n(F)$ where F is a finite extension of $\mathbb{Q}_\ell$.

Remark 3.4. The topologies on $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{GL}_n(\mathbb{Q}_\ell)$ are very different, and in particular and ℓ-adic representation may not have an open kernel. Instead, continouity is equivalent to the following condition: for every $m \geq 1$, there is some finite field extension F_m of K such that for all $g \in \mathrm{Gal}(\bar{K}/F_m)$, $\rho(g) \equiv \mathrm{Id}_n \pmod{\ell^m}$.

Given an Artin representation ρ, one can view it as homomorphism $\rho\colon G_K \to \mathrm{GL}_n(\bar{\mathbb{Q}})$ and since it factors through a finite quotient, we can realise it as $\rho\colon G_K \to \mathrm{GL}_n(F)$ for some number field F. Hence, if ℓ is any rational prime and $\mathfrak{l}$ is a prime in F above ℓ, then one can realise ρ as an ℓ-adic representation

$$\rho\colon G_K \longrightarrow \mathrm{GL}_n(F_{\mathfrak{l}}),$$

which is continous since ρ factors through a finite quotient. Furthermore, Artin and ℓ-adic representations over K have more structure; namely, one can take **direct sums** and **tensor products**.

We describe the construction for Artin representations, since the ℓ-adic case is completely analogous. Suppose we have two Artin representations ρ_1, ρ_2 over K, and by the discussion on the preceeding paragraph we can realise them as maps $\rho_i\colon G_K \to \mathrm{GL}_{n_i}(L_i),\ i = 1, 2$ where L_1 and L_2 are number fields. If we let $L = L_1L_2$, then the natural maps $\rho_1 \oplus \rho_2\colon G_K \to \mathrm{GL}_{n_1+n_2}(L)$ and $\rho_1 \otimes \rho_2\colon G_K \to \mathrm{GL}_{n_1n_2}(L)$ are both Artin representations. One can also show that this construction is also well-defined up to equivalence.

3.2 Local Polynomials and L-functions

We now briefly discuss how to attach analytic objects to Artin and ℓ-adic reperesentations. These objects are usually described locally first, and then this local information is put together to get a global object.

To begin, let K be a local field with 0 characteristic and let p be the characteristic of the residue field κ. Let $\rho\colon G_K \to \mathrm{GL}(V)$ be an Artin or ℓ-adic representation such that $\ell \neq p$ (this is an important technical assumption that we will not discuss further). By the **section on algebraic number theory** we have a short exact sequence

$$0 \longrightarrow I_K \longrightarrow \mathrm{Gal}(\bar{K}/K) \xrightarrow{\epsilon} \mathrm{Gal}(\bar{\kappa}/\kappa) \cong \tilde{\mathbb{Z}} \longrightarrow 0,$$

where under the last isomorphism $1 \in \tilde{\mathbb{Z}}$ corresponds to the map $\phi\colon \bar{\kappa} \to \bar{\kappa}$ where $x \mapsto x^p$ and this map is a topological generator of $\mathrm{Gal}(\bar{\kappa}/\kappa)$. Any preimage of ϕ under ϵ is called a Frobenius element Frob_K and it is therefore well-defined up to I_K. Furthermore, the space of intertia-invariants

$$V^{I_K}\colon = \{v \in V\colon \rho(g)v = v \text{ for all } g \in I_K\}$$

is naturally a G_K/I_K representation, which we denote ρ^{I_K}. we are now ready to define the local polynomial attached to ρ.

Definition 3.5. Let K be a local field of characteristic 0 and let p the characteristic of its local field. If ρ is an Artin or ℓ-adic representation such that $\ell \neq p$. Then the local polynomial attached to ρ is

$$P(\rho, T)\colon = \det\left(I - T \cdot \rho^{I_K}\left(\mathrm{Frob}_K^{-1}\right)\right).$$

If K is instead a number field, the idea is to consider all finite places of K and consider all the local polynomials attached to all local completions of K to build the corresponding L-function. More concretely, let $\rho\colon G_K \to \mathrm{GL}(V)$ be an Artin or ℓ-adic representation and let $\mathfrak{p}$ be a finite place of K and $K_{\mathfrak{p}}$ be the corresponding completion. Since $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(\bar{K_{\mathfrak{p}}}/K_{\mathfrak{p}})$ is naturally a subgroup of G_K, we can restrict ρ to

$\mathrm{Res}_{\mathfrak{p}}\rho\colon G_{K_{\mathfrak{p}}} \to \mathrm{GL}(V)$ and then calculate the corresponding local polynomial as long as $\mathfrak{p}$ and ℓ are coprime. If ρ is an Artin representation, this allows us to construct the associalted L-function.

Definition 3.6. Let K be a number field and ρ an Artin representation over K. If $\mathfrak{p}$ is a finite place of K, we denote the local polynomial at $\mathfrak{p}$ as

$$P_{\mathfrak{p}}(\rho, T) := P(\mathrm{Res}_{\mathfrak{p}}\rho, T).$$

The associated L-function to ρ is

$$L(\rho, s) := \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\rho, N(\mathfrak{p})^{-s})}.$$

However, if ρ is an ell-adic representation, constructing a global object is harder, since the above method does not yield information at the finite places $\mathfrak{p}$ that divide ℓ. This motivates the following important definition.

Definition 3.7. Let $\{\rho_\ell\}_{\ell \text{ prime}}$ be a family of ℓ-adic representations for each prime ℓ. We then say that $\{\rho_\ell\}_\ell$ is a **weakly compatible system of ℓ-adic representations** if for every finite place $\mathfrak{p}$ of K and rational primes ℓ, ℓ' not divisible $\mathfrak{p}$,

$$P_{\mathfrak{p}}(\rho_\ell, T) = P_{\mathfrak{p}}(\rho_{\ell'}, T)$$

.

When $\{\rho_\ell\}_\ell$ is a weakly compatible system of ℓ-adic representations, the local polynomial $P_{\mathfrak{p}}(\rho_\ell, T)$ can be computed using any ℓ not divisible by $\mathfrak{p}$. This also allows us to define the L-function in this context.

Definition 3.8. Let K be a number field and let $\{\rho_\ell\}_\ell$ be a weakly compatible system of ℓ-adic representations. Then the L-function attached to the system is

$$L(\{\rho_\ell\}_\ell, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\{\rho_\ell\}, N(\mathfrak{p})^{-s})}.$$

3.3 The Tate Module of an Elliptic Curve and their L-function

Let K be a number field or a local field with characteristic 0 **(Maybe for this section we should only assume K is a number field? Otherwise I don't know if it makes sense to talk about their L-function)** and fix an algebraic closure $\bar{K}$ of K. Let E be an elliptic curve defined over K. To avoid notational confusion, whenever we write E we refer to all of its $\bar{K}$ points, while $E(K)$ refers only to the K-rational points. The aim of this section is to describe a procedure to attach an L-function to a given elliptic curve over K. In order to achieve this, we will first construct a 2-dimensional ℓ-adic representation attached to E, and then construct the L-function as described in the section above. Let ℓ be a rational prime number. For any $n \geq 1$, we denote by $E[\ell^n]$ to be the ℓ^n-torsion points; in other words, $E[\ell^n]$ is the kernel of the map $E[\ell^n]\colon E \to E$. We then have the diagram of compatible maps

$$\longrightarrow E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \xrightarrow{[\ell]} \cdots \xrightarrow{[\ell]} E[\ell^2] \xrightarrow{[\ell]} E[\ell] \xrightarrow{[\ell]} \{\mathscr{O}_E\}$$

and therefore we can construct the inverse limit of this diagram

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

denoted as the ℓ-adic Tate module of the elliptic curve E. By the uniformization theorem, we know that

$$E[\ell^n] \cong \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$$

as groups, and therefore

$$T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

as $\mathbb{Z}_\ell$-modules. In addition, the Tate module carries important extra structure, namely the action of the absolute Galois group G_K. Since E is defined over K, and the multiplication by m maps are determined by polynomials with coefficients in K, there is a well-defined additive action $\psi_n\colon G_K \to \mathrm{Aut}_{\mathbb{Z}}(E[\ell^n])$. Furthermore, one can show that this actions are compatible with the inverse limit diagram of the Tate module. That is, for every $n \geq 1$ and $\sigma \in G_K$, the diagram

$$\begin{tikzcd}
E[\ell^{n+1}] \arrow[r, "\ell"] \arrow[d, "\psi_{n+1}(\sigma)"] & E[\ell^n] \arrow[d, "\psi_n(\sigma)"] \\
E[\ell^{n+1}] \arrow[r, "\ell"] & E[\ell^n]
\end{tikzcd}$$

commutes. Therefoere, the actions ψ_n induce an action of G_K on $T_\ell(E)$ and since $T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$, this corresponds to a 2-dimensional ℓ-adic representations

$$\psi_{E,\ell}\colon G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbb{Q}_\ell).$$

We will also denote from now on $\rho_{E,\ell}$ to be the dual representation of $\psi_{E,\ell}$. For technical reasons we will not discuss, the L-function is tipycally constructed using the later ones.

Remark 3.9. The representation above does indeed satisfy the conditions in Remark 3.4. In particular, given any $n \geq 1$, the field $F_n\colon = K(E[\ell^n])$ is a finite extension of K since it is obtained by attaching finitely many algebraic numbers. By construction, $\mathrm{Gal}(\bar{K}/F_n)$ acts trivially on $E[\ell^n]$ and thus $\rho_{E,\ell}(g) \equiv \mathrm{Id} \pmod{\ell^n}$ for all $g \in \mathrm{Gal}(\bar{K}/F_n)$.

Of course, the above construction can be followed by any rational prime ℓ, and this gives a family $\{\rho_{E,\ell}\}_\ell$. To build an L-function as described in the section above, we would need this family to be weakly compatible. Thankfully, this and much more is true, and the next theorem collects the relevant results.

Theorem 3.10. *Let E be an elliptic curve over a number field K and $\rho_{E,\ell}$ be the dual representation on $T_\ell(E)$. For every finite place $\mathfrak{p}$ of K, let $\kappa_\mathfrak{p}$ be the residue field of $K_\mathfrak{p}$, $q_\mathfrak{p} = |\kappa_\mathfrak{p}|$ and $a_\mathfrak{p} = 1 + q_\mathfrak{p} - |\tilde{E}(\kappa_\mathfrak{p})|$. Then for any $\mathfrak{p}$ not diving ℓ,*

$$\begin{aligned}
P_\mathfrak{p}(\rho_{E,\ell}, T) &= 1 - a_\mathfrak{p}T + q_pT^2, && \textit{if } E/K_\mathfrak{p} \textit{ has good reduction,} \\
&= 1 - T, && \textit{if } E/K_\mathfrak{p} \textit{ has split multiplicative reduction,} \\
&= 1 + T, && \textit{if } E/K_\mathfrak{p} \textit{ has non-split multiplicative reduction,} \\
&= 1, && \textit{if } E/K_\mathfrak{p} \textit{ has additive reduction.}
\end{aligned}$$

In particular, for any ℓ, ℓ' not divisible by $\mathfrak{p}$,

$$P_\mathfrak{p}(\rho_{E,\ell}, T) = P_\mathfrak{p}(\rho_{E,\ell'}, T),$$

and so $\{\rho_{E,\ell}\}$ is a weakly compatible system of ℓ-adic representations.

This allows us to define the L-function of an elliptic curve as above.

Definition 3.11. Let E be an elliptic curve over K. Then the L-function attached to E is

$$L(E/K, s) = L(\{\rho_{E,\ell}\}, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\rho_{E,\ell}, N(p)^{-s})}$$

3.4 Artin Twists of L-functions of Elliptic Curves

We have already seen that given an elliptic curve over a number field K, one can construct the L-function $L(E/K, s)$. However, given an Artin representation ρ over K, it is possible to attach more analytic objects, with remarkable arithmetic properties. We outline the main results below, without proofs. **Insert here relevant reference**.

Fix some number field K, an elliptic curve E over K and an Artin repesentation ρ. Then, similary to the previous section, it is possible to show that $\{\rho_{E,\ell} \otimes \rho\}_\ell$ is also a weakly compatible system of ℓ-adic representations. The corresponding L-function

$$L(E, \rho, s) = L(\{\rho_{E,\ell} \otimes \rho\}, s)$$

is denoted as the **Artin-twist** of $L(E, s)$ by ρ. These objects have remarkable (both proven and conjectural) properties that we describe now.

Theorem 3.12 (Artin Formalism)**.** *Let E be an elliptic curve over a number field K.*

1. *For Artin representations ρ_1, ρ_2 over K,*

$$L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s) \quad \textit{and} \quad L(E/K, \rho_1 \oplus \rho_2, s) = L(E/K, \rho_1, s)L(E/K, \rho_2, s)$$

2. *If L/K is a finite extension and ρ is an Artin representation over L, then $\mathrm{Ind}_{G_L}^{G_K} \rho$ is an Artin representation over K and*

$$L(\rho, s) = L(\mathrm{Ind}_{G_L}^{G_K} \rho, s) \quad \textit{and} \quad L(E/L, \rho, s) = L(E/L, \mathrm{Ind}_{G_L}^{G_K} \rho, s).$$

3. *If L/K is a finite extension as above and*

$$\mathrm{Ind}_{G_L}^{G_K} \mathbb{1} \cong \bigoplus_i \rho_i,$$

then

$$L(E/L, s) = \prod_i L(E/K, \rho_i, s).$$

To simply notation, given any Artin representation ρ over L we will write $\mathrm{Ind}_{L/K}\rho$ instead of $\mathrm{Ind}_{G_L}^{G_K}\rho$. Furthermore if F is a finite Galois extension of K such that ρ factors through $\mathrm{Gal}(F/L)$, then $\mathrm{Ind}_{L/K}\rho$ factors through $\mathrm{Gal}(F/K)$ and

$$\mathrm{Ind}_{L/K}\rho \cong \mathrm{Ind}_{\mathrm{Gal}(F/L)}^{\mathrm{Gal}(F/K)}\rho.$$

Furthermore, as mentioned after Remark 3.4, by fixing some basis $\mathscr{B}$ of V any Artin representation ρ can be viewed as a representation $\rho\colon G_K \to \mathrm{GL}_n(F)$ for some number field F. The smallest such field is the **field of values** of ρ and denoted by $\mathbb{Q}(\rho)$. Any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ induces a homomorphism $\sigma\colon \mathrm{GL}_n(\mathbb{Q}(\rho)) \to \mathrm{GL}_n(\mathbb{Q}(\rho))$ and also a map which is another Artin representation, denoted as the twist of ρ by σ.

Conjecture 3.13 (Galois Equivariance of L-Twists)**.** I need to check the precise statement of this result. This may need to come after the discussion on BSD.

4 Birch and Swinnerton-Dyer and Other Conjectures

The Birch-Swinnerton-Dyer conjecture classically provides a connection between the arithmetic of elliptic curves and their L-functions. We have already investigated the construction and main results of the 'L-functions side', and now we turn out attention to statement of the conjecture and towards understanding the arithmetic terms present in the conjecture.

Conjecture 4.1 (BSD)**.** Let E be an elliptic curve over a number field K. Then

BSD1. The rank of the Mordell-Weil group of E over K equals the order of vanishing of the L-function; that is,

$$\mathrm{ord}_{s=1} L(E/K,s) = \mathrm{rk}\, E/K.$$

BSD2. The leading term of the Taylor series at $s=1$ of the L-function is given by

$$\lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}} = \frac{\mathrm{Reg}_{E/K}|\text{Ш}_{E/K}|C_{E/K}}{|E(K)_{tors}|^2}. \tag{5}$$

Many arithmetic invariants appear as part of the statement of BSD2, and it is worth exploring them briefly. The way we have organised the terms is not arbitrary, and in fact we give specific notation to both sides of the equation.

Notation 4.2. Let $E/\mathbb{Q}$ be a number field and K a number field. We define

$$\mathscr{L}(E/F) = \lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}}$$

and

$$\mathrm{BSD}(E/F) = \frac{\mathrm{Reg}_{E/K}|\text{Ш}_{E/K}|C_{E/K}}{|E(K)_{tors}|^2}$$

A natural question to ask at this point is whether there is a conjectural analogue to the above for the Artin twists of L-functions. The analogue of BSD1 is known in this case, which is directly compatible with Artin formalism.

Conjecture 4.3 (BSD1 for Twists)**.** Let $E/\mathbb{Q}$ be an elliptic curve, ρ an Artin representation and K any Galois extension over $\mathbb{Q}$ such that ρ factors through $G = \mathrm{Gal}(K/\mathbb{Q})$. Then

$$\mathrm{ord}_{s=1} L(E,\rho,s) = \langle \rho, E(K)_{\mathbb{C}} \rangle_G$$

maybe delete this last sentence. where ρ and $E(K)_{\mathbb{C}} = E(K) \otimes_{\mathbb{Z}} \mathbb{C}$ are viewed as representations of G.

Unfortunately, a conjectural analogue for BSD2 is not known. The problem is the lack of an analogue for the term $\mathrm{BSD}(E/F)$ as above. However, there is indeed an important analogue of the term $\mathscr{L}(E/F)$ in this setting.

Notation 4.4. Let $E/\mathbb{Q}$ be an elliptic curve and ρ an Artin representation over $\mathbb{Q}$. We define

$$\mathscr{L}(E,\rho) = \lim_{s\to 1} \frac{L(E,\rho,s)}{(s-1)^r} \cdot \frac{\sqrt{\mathfrak{f}_\rho}}{\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)}\omega_\rho},$$

where $r = \mathrm{ord}_{s=1} L(E,\rho,s)$ is the order of the zero at $s = 1$, $\mathfrak{f}_\rho$ is the conductor of ρ, and $d^{\pm}(\rho)$ are the dimensions of the ± 1-eigenspaces of complex conjugation in its action on ρ.

Even though the precise conjectural expression of the $\mathrm{BSD}(E,\rho)$ is not known, they conjecturally satisfy many important properties. The next conjecture lists some of these properties.

Conjecture 4.5. [DEW21, Conjecture 4] Let $E/\mathbb{Q}$ be an elliptic curve. For every Artin representation ρ over $\mathbb{Q}$ there is an invariant $\mathrm{BSD}(E,\rho) \in \mathbb{C}^\times$ with the following properties. Let ρ and τ be Artin representations and K a finite extension of $\mathbb{Q}$ such that ρ and τ factor through $\mathrm{Gal}(K/\mathbb{Q})$.

C1. $\mathrm{BSD}(E/F) = \mathrm{BSD}(E, \mathrm{Ind}_{F/\mathbb{Q}}\mathbb{1})$ for a number field F (and $Ш_{E/F}$ is finite).

C2. $\mathrm{BSD}(E,\rho\oplus\tau) = \mathrm{BSD}(E,\rho)\mathrm{BSD}(E,\tau)$.

C3. $\mathrm{BSD}(E,\rho) = \mathrm{BSD}(E,\rho^*)\cdot(-1)^r\omega_{E,\rho}\omega_\rho^{-2}$, where $r = \langle\rho, E(K)_\mathbb{C}\rangle$.

C4. If ρ is self-dual, then $\mathrm{BSD}(E,\rho)\in\mathbb{R}$ and sign $\mathrm{BSD}(E,\rho) =$ sign ω_ρ.

If $\langle\rho, E(K)_\mathbb{C}\rangle = 0$, then moreover:

C5. $\mathrm{BSD}(E,\rho)\in\mathbb{Q}(\rho)^\times$ and $\mathrm{BSD}(E,\rho^g) = \mathrm{BSD}(E,\rho)^g$ for all $g\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.

C6. If ρ is a non-trivial primitive Dirichlet character of order d, and either the conductors of E and ρ are coprime or E is semistable and has no non-trivial isogenies over $\mathbb{Q}$, thenn $\mathrm{BSD}(E,\rho)\in\mathbb{Z}[\zeta_d]$.

The great advantage of the above conjecture is that it is free of L-functions since only the 'arithmetic' $\mathrm{BSD}(E/F)$ terms appear. Conditional to some well-known conjectures, Conjecture 4.5 holds.

Theorem 4.6. *[DEW21, Theorem 5] Conjecture* 4 *holds with* $\mathrm{BSD}(E,\rho) = \mathscr{L}(E,\rho)$ *assuming the analytic continuation of L-functions $L(E,\rho,s)$, their functional equation, the Birch-Swinnerton-Dyer conjecture, Deligne's period conjecture, Stevens's Manin constant conjecture for $E/\mathbb{Q}$ and the Riemann hypothesis for $L(E,\rho,s)$.*

5 Brauer Relations

6 Predicting Positive Rank

At this point, we aim to study the arithmetic applications of Conjecture 4.5. Some of these applications are already studied in [DEW21, §3], and it allows to predict non-trivial interplay of the primary parts of the Tate-

Shafarevich group of families of elliptic curves, non-trivial Selmer groups and even positive rank. All of these results appear not to be tractable with other common current methods.

The most interesting case is the prediction of positive rank for families of elliptic curves on certain number fields. We illustrate the proof of the main result that predict positive rank conditional on Conjecture 4.5. Let F be a Galois extension over $\mathbb{Q}$ and let $G = \mathrm{Gal}(F/\mathbb{Q})$. Let $E/\mathbb{Q}$ be an elliptic curve and let ρ be an irreducible representation over G, which we view as an Artin representation. Then the representation

$$\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}$$

has $\mathbb{Q}$-valued character and therefore there is some $m \geq 1$ and subfields F_i, F'_j such that

$$\left(\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}\right)^m \oplus \bigoplus_j \mathrm{Ind}_{F'_j/\mathbb{Q}}\mathbb{1} = \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\mathbb{1}.$$

Assume that $\mathrm{rk}\,E/F = 0$ so that in particular $\langle \rho, E(F)_{\mathbb{C}}\rangle_G = 0$. Therefore (C1), (C2) and (C5) from Conjecture 4.5 imply that

$$\frac{\prod_i \mathrm{BSD}(E/F_i)}{\prod_j \mathrm{BSD}(E/F'_j)} = \frac{\prod_i \mathrm{BSD}(E, \mathrm{Ind}_{F_i/\mathbb{Q}}\mathbb{1})}{\prod_j \mathrm{BSD}(E, \mathrm{Ind}_{F'_j/\mathbb{Q}}\mathbb{1})} = \left(\prod_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \mathrm{BSD}(E,\rho)^{\mathfrak{g}}\right)^m \tag{6}$$

and the right-hand side is clearly the m-th power of a norm of an element in $\mathbb{Q}(\rho)$.

The product of BSD terms on the LHS of (6) involve regulators, the torsion subgroups, the Tate-Shafarevich groups and the terms $C_{E/F}$ which are the product of local factors. Under the assumption that $\mathrm{rk}\,E/F = 0$, the regulators vanish from the product. In general, it is very difficult to deal with the size of the Tate-Shafarevich group for families of elliptic curves, and therefore very difficult to know if the LHS is an m-th power the norm of an element in $\mathbb{Q}(\rho)$. However, not all hope is lost, since Cassel's proved the following.

Theorem 6.1. *Let E be an elliptic curve over a number field K. If $\text{Ш}_{E/K}$ is finite, then $|\text{Ш}_{E/K}|$ is a square.*

Rational squares are not necessarily the norms of general number fields, but they are always norms of quadratic number fields. Furthermore, if $\mathbb{Q}(\sqrt{D})$ is a quadratic subfield fo $\mathbb{Q}(\rho)$, then the RHS of (6) is also the norm of an element of $\mathbb{Q}(\sqrt{D})$ and a rational square if m is even. Under the assumption of finiteness of Ш, we know that $|\text{Ш}_{E/F}|$ and $|E(F)_{tors}|^2$ are rational squares and therefore norms of $\mathbb{Q}(\sqrt{D})$. The only remaining terms on the LHS of (6) are the product of local factors C_{E/F_i} and C_{E/F'_j}. We have therefore proven the following.

Theorem 6.2. *[DEW21, Theorem 33] Suppose Conjecture 4.5 holds. Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a finite Galois extension with Galois group G, ρ an irreducible representation of G and*

$$\left(\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}\right)^m = \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\mathbb{1} \ominus \bigoplus_j \mathrm{Ind}_{F'_j/\mathbb{Q}}\mathbb{1}$$

for some $m \geq 1$ and subfields $F_i, F'_j \subseteq F$. If either $\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$ is not a norm from some quadratic subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, or if it is not a rational square when m is even, then E has a point of infinite order over F.

This is a remarkable result, since it can predict positive rank of general families of elliptic curves based solely on local data.

7 Consistency cases with BSD

As we discussed in the previous section, our motivation is to use Theorem 6.2 to predict points of infinite order for families of elliptic curves. However, in this section we prove that in several cases the theorem will never make such a prediction. In other words, in such cases, the product

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$$

is always a norm for every subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$.

7.1 Cyclic Extensions

In this subsection we prove the following.

Theorem 7.1. *Let $E/\mathbb{Q}$ be a semistable elliptic curve and let F a finite cyclic Galois extension over $\mathbb{Q}$ so that $\mathrm{Gal}(F/\mathbb{Q}) = C_d$ for some $d \geq 2$. Let χ be a faithful character of C_d (so that $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta_d)$), and let $F_i, F'_j \subseteq F$ be such that*

$$\bigoplus_{\mathfrak{g}\in \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \chi^{\mathfrak{g}} = \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\mathbb{1} \ominus \bigoplus_j \mathrm{Ind}_{F'_j/\mathbb{Q}}\mathbb{1}.$$

Then for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_d)$,

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$$

is a norm of $\mathbb{Q}(\sqrt{D})$.

The first step in proving Theorem 7.1 is to show that the fields F_i, F'_j exist, and to give a precise description. Recall that for each $k \mid d$ the cyclic group C_d has one unique subgroup of order k, which is of course also cyclic. Therefore, for each $k \mid d$, there is one unique subfield F_k of F of degree k over $\mathbb{Q}$ which is also cyclic. The corresponding subgroup $H_k = \mathrm{Gal}(F/F_k) = C_{d/k}$.

To give the required description, we recall that the Möbius function μ is the function supported on the square-free integers, and $\mu(n) = (-1)^s$ whenever n is square free and s is the number of prime factors of n.

Lemma 7.2. *Let $E/\mathbb{Q}$, F and χ be as in Theorem 7.1. Writing characters of C_d additively, we have that*

$$\sum_{\mathfrak{g}\in \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \chi^{\mathfrak{g}} = \sum_{k\mid d} \mu(d/k)\mathrm{Ind}_{F_k/\mathbb{Q}}\mathbb{1}. \tag{7}$$

Proof. The proof is essentially application of Frobenius reciprocity and the inclusion exclusion lemma. Let $p_1, \ldots, p_s$ be the distinct primes dividing d. By Frobenius reciprocity, for any character θ of C_d and $k \mid d$,

$$\langle \theta, \mathrm{Ind}_{F_k/\mathbb{Q}}\mathbb{1}\rangle_{C_d} = \langle \mathrm{Res}_{F_k/\mathbb{Q}}\theta, \mathbb{1}\rangle_{C_{d/k}}.$$

That is, θ appears as a factor of $\mathrm{Ind}_{F_k/\mathbb{Q}}\mathbb{1}$ if and only if $\chi|_{C_{d/k}}$ is trivial, and it can only appear once. Therefore,

$$\mathrm{Ind}_{F_k/\mathbb{Q}}\mathbb{1} = \sum_{\theta\in\mathscr{A}_{d/k}} \theta$$

where $\mathscr{A}_k = \{\theta \in \widehat{C_d}\colon \theta|_{C_k} = \mathbb{1}_{C_k}\}$. Note that if $k, k' \mid d$ are coprime, then $\mathscr{A}_k \cap \mathscr{A}_{k'} = \mathscr{A}_{kk'}$. If $\mathscr{B}$ is the set of faithful characters of C_d, then by the inclusion-exclusion lemma The proof now follows from the fact that if χ is a faithful character, then the set $\{\chi^{\mathfrak{g}}\colon \mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})\}$ spans over all faithful characters of C_d once. □

7.2 Abelian Extensions

7.3 Odd-Degree Extensions

References

[DEW21] V. Dokchitser, R. Evans, and H. Wiersema, *On a BSD-type formula for L-values of Artin Twists of Elliptic Curves*, Graduate Texts in Mathematics, Crelles Journal, 2021.