Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

April 2, 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 $\mathbb{Q}(\rho)$,
$H^x = xHx^{-1}$	for $H \leq G$ a subgroup of a group G and $x \in G$,

1 Norm relations

1.1 Representation theory of finite groups

Let G be a finite group, K a field of characteristic zero. Recall that a **representation** of G over K is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ where V is a K-vector space. Associated to a representation ρ is a **character** $\chi\colon G \to K^{\times}$, 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.

Definition 1.1. Let $\chi_1, \ldots \chi_h$ be the distict characters of the complex irreducible representations of G. Then the **representation ring** of G is

$$R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h.$$

We can also view this as the Grothendieck group of the category of finitely generated $\mathbb{C}[G]$-modules.

Let K be a number field. Denote by $R_K(G)$ the group generated by characters of the reprsentations of G over K. This is a subring of $R(G)$. The characters of the distinct irreducible representations of G over K form an orthogonal basis of $R_K(G)$ (cf. Serre Proposition 32). Let m be the exponent of G. If K contains the m-th roots of unity, then $R_K(G) = R(G)$. This implies every representation of G can be realized over K. (Serre 12.3)

The rank of $R_K(G)$ is discussed in Serre 12.4. For example, the rank of $R_{\mathbb{Q}}(G)$ is equal to the number of conjugacy classes of cyclic subgroups of G.

Notation 1.2. For $\rho \in R_{\mathbb{C}}(G)$ an irreducible character let

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

where $m(\rho) \in \mathbb{Z}$ is the Schur index of ρ.

Then $\widetilde{\rho}$ is the character of an irreducible rational representation. Every irreducible rational representation can be obtained this way. We can extend this map additively to a surjective map $R_{\mathbb{C}}(G) \to R_{\mathbb{Q}}(G)$.

talk about indexes of perm reps –> rational reps –> reps with rational character. Talk a little bit about what the m is for the results in vlads paper

1.2 The Burnside ring and relations

Let G be a finite group. Recall that there is a bijection between the isomorphism classes of transitive finite G-sets and the conjugacy classes of subgroups $H \leq G$, given by sending a transitive G-set X to $H = \mathrm{Stab}_G(x)$ for some $x \in X$. Then the action of G on X is equivalent to the action of G on G/H.

Definition 1.3. Let $[X]$ denote the isomorphism class of a G-set X. The **Burnside ring** $B(G)$ is the free abelian group on isomorphism classes of finite G-sets, modulo the relations $[S] + [T] = [S \sqcup T]$. This is a ring; multiplication is given by $[S] \cdot [T] = [S \times T]$. Using the identification of finite G-sets with subgroups of G, we write elements of $B(G)$ as $\sum_i n_i H_i$ for $n_i \in \mathbb{Z}$, $H_i \leq G$.

Notation 1.4. There is a homomorphism from the Burnside ring to the rational representation ring $R_{\mathbb{Q}}(G)$ of G given by taking the corresponding permutation representation:

$$\mathbb{C}[-]\colon B(G) \to R_{\mathbb{Q}}(G), \qquad \Theta = \sum_i n_i H_i \ \mapsto\ \mathbb{C}[\Theta] = \sum_i n_i \operatorname{Ind}_{H_i}^G \mathbb{1}_{H_i}.$$

Elements in the kernel of this map are known as **Brauer relations**. These show instances of non-isomorphic G-sets giving rise to isomorphic permutation representations.

Example 1.5. S_3 example

Example 1.6. Cyclic groups have no Brauer relations.

We are interested in elements of $B(G)$ with image isomorphic to $\widetilde{\rho}$ for $\rho \in R_{\mathbb{C}}(G)$.

Definition 1.7. We call $\Theta = \sum_i n_i H_i \in B(G)$ a **ρ-relation** if $\mathbb{C}[\Theta] \simeq \widetilde{\rho}$.

There are #(Brauer relations) +1 such elements Θ. Of course, when $\rho = 0$ these are Brauer relations.

Example 1.8. 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 an orthogonal basis for the irreducible rational-valued representations of G. Note that $\operatorname{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G contain $C_{n/d}$ in their kernel. Thus, $\operatorname{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain the *unqiue* φ_d-relation for each $d \mid n$:

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

Notation 1.9. For $D \leq G$, define maps $\operatorname{Res}_D \colon B(G) \to B(D)$ and $\operatorname{Ind}_D \colon B(D) \to B(G)$ by

$$\operatorname{Res}_D H = \sum_{x \in H \backslash G / D} D \cap H^{x^{-1}}, \qquad \operatorname{Ind}_D H = H.$$

These correspond to the reprsentation theory side, where $\operatorname{Res}_D \operatorname{Ind}_H^G \mathbb{1} = \sum_{x \in H \backslash G/D} \operatorname{Ind}_{D \cap H^{x^{-1}}}^D \mathbb{1}$ (Mackey's decomposition), and $\operatorname{Ind}_D^G \operatorname{Ind}_H^D \mathbb{1} = \operatorname{Ind}_H^G \mathbb{1}$.

1.3 Functions on the Burnside ring and norm relations

Consider multiplicative functions on the Burnside ring $\psi \colon B(G) \to \mathbb{Q}^\times$. Given $\rho \in R_{\mathbb{C}}(G)$ we can extend such functions from the Burnside ring to $\overline{\psi} \colon B(G) \to \mathbb{Q}^\times / N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.

Definition 1.10. If $\Theta \in \ker \overline{\psi}$, then $\psi(\Theta)$ is the norm of an element from $\mathbb{Q}(\rho)^\times$. We call an instance of this a **norm relation**.

Definition 1.11. We say two functions ψ, ψ' are **ρ-equivalent**, written $\psi \sim_\rho \psi'$, if $\overline{\psi/\psi'}$ is trivial on all ρ-relations. Equivalently, $\psi(\Theta)/\psi'(\Theta)$ is a norm relation for all ρ-relations Θ.

Remark 1.12. If $\rho = 0$ then we call functions $\psi \sim_\rho 1$ **representation theoretic**. These have been studied in cite.

Example 1.13. Take $\rho = 0$, and V a representation of G. The function $\psi(H) = \dim V^H$ satisfies $\psi \sim_\rho 1$ as $\dim V^H = \langle \operatorname{Res}_H V, \mathbb{1}_H \rangle = \langle V, \operatorname{Ind}_H^G \mathbb{1} \rangle$ by Frobenius reciprocity.

Example 1.14. 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 $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ by Corollary A.11.

Example 1.15. Let $E/\mathbb{Q}$ be an elliptic curve, $G = \operatorname{Gal}(F/\mathbb{Q})$ 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 $\psi \sim_\rho 1$.

1.4 D-local functions

Maybe just add in definition of D-local function, and explain all this way better. Maybe also some parts of Theorem 2.36 in the reg consts paper (the parts that translate).

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

Consider $G = \operatorname{Gal}(F/\mathbb{Q})$ 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 $H\backslash G/D$. 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 1.16. Suppose $I \triangleleft D < G$ 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.

try make thick brackets

Example 1.17. 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 $n \in \{2, 3, 4, 6, 9, 10\}$.

Example 1.18. Let $\rho = 0$. If W is a group of odd order, then $(W, W, e) \sim 1$ as functions to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. More generally if D has odd order and $I \triangleleft D$ then $(D, I, e) \sim_\rho 1$. explain and reference

2 Representations, L-functions and Artin Twists

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 always specify what K is in each context. 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.

2.1 Artin Representations and ℓ-adic Representations

We begin by recallin the notion of an Artin representation.

Definition 2.1. 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 $\rho : G_K \to \mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$ 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 and refer to either of them as Artin representations. Which notion we refer to is always clear from context.

Remark 2.2. The condition above that $\mathrm{Gal}(\bar{K}/F) \subseteq \ker \rho$ is equivalent to $\ker \rho$ being open in G_K. This condition is clearly equivalent to ρ being continous with respect the discrete topology on $\mathrm{GL}_n(\mathbb{C})$. Interestingly, the profinite topology of G_K has an surprising consequence: this condition is also equivalent to continuity with respect to the usual complex topology on $\mathrm{GL}_n(\mathbb{C})$. Necessity is clear, and the proof of sufficiency relies on the fact that under the complex topology, 'small' neighbourhoods of the identity in $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$ do not contain any non-trivial subgroups. Hence, if $\phi : G_K \to \mathrm{GL}(V)$ is continous with respect to the complex topology 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 $\ker \phi$ is open too. Hence, Artin representations are simply continous group homomorphisms $\rho : G_k \to \mathrm{GL}_n(\mathbb{C})$.

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

Definition 2.3. 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 $\rho : G_K \to \mathrm{GL}_n(F)$ where F is a finite extension of $\mathbb{Q}_\ell$ and $\mathrm{GL}_n(F)$ is equipped with the ℓ-adic topology.

Remark 2.4. 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 $\rho : G_K \to \mathrm{GL}_n(\bar{\mathbb{Q}})$ and since it factors through a finite quotient, we can realise it as $\rho : G_K \to \mathrm{GL}_n(F)$ 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

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

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 $\rho_i : G_K \to \mathrm{GL}_{n_i}(L_i),\ i = 1, 2$ where L_1 and L_2 are number fields. If we let $L = L_1 L_2$, then the natural maps $\rho_1 \oplus \rho_2 : G_K \to \mathrm{GL}_{n_1+n_2}(L)$ and $\rho_1 \otimes \rho_2 : G_K \to \mathrm{GL}_{n_1 n_2}(L)$ are both Artin representations. One can also show that this construction is also well-defined up to equivalence.

Finally, we discuss the notion of an induced Artin representation. Suppose L is a finite field extension of K of degree d and let $\rho : G_L \to \mathrm{GL}(V)$ be an Artin representation. Then G_L is naturally a subgroup of G_K of index d, and therefore we can construct $\mathrm{Ind}_{G_L}^{G_K} \rho$ in the usual way. This turns out to be an Artin representation of K: if F be a number field so that ρ factors through $\mathrm{Gal}(F/L)$, then $\mathrm{Ind}_{G_L}^{G_K} \rho$ will factor through $\mathrm{Gal}(F/K)$. Furthermore, the corresponding representation over $\mathrm{Gal}(F/K)$ will be equivalent to $\mathrm{Ind}_{\mathrm{Gal}(F/L)}^{\mathrm{Gal}(F/K)} \rho$ where ρ is now viewed as a representation of $\mathrm{Gal}(F/L)$. Hence, the notion of induction is naturally compatible with this process of passing through finite quotients. Therefore, and to simplify notation, we will write $\mathrm{Ind}_{L/K} \rho$ for the induced Artin representation, and it will always be clear from context the implicit field F.

2.2 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 for local fields of characteristic 0 first. Then, one constructs global objects attached to number fields by completing them at their finite places, obtaining the local information and then combinining it appropiately.

To begin, let K be a local field with 0 characteristic and let p be the characteristic of the residue field κ. Let $\rho : G_K \to \mathrm{GL}(V)$ be an Artin or ℓ-adic representation such that $\ell \neq p$ (this is an important technical assumption that we will not discuss further). It is a fundamental resut in algebraic number theory that the natural map

$$\epsilon : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(\bar{\kappa}/\kappa)$$

is surjective, and $I_K := \ker \epsilon$ is denoted as the inertia group of K. Therefore, we have a short exact sequence

$$0 \longrightarrow I_K \longrightarrow \mathrm{Gal}(\bar{K}/K) \xrightarrow{\epsilon} \mathrm{Gal}(\bar{\kappa}/\kappa) \longrightarrow 0.$$

In addition, the map $\phi \in \mathrm{Gal}(\bar{\kappa}/\kappa)$ such that $\phi(x) = x^p$ is a topological generator of $\mathrm{Gal}(\bar{\kappa}/\kappa)$ and any preimage of ϕ under ϵ is called a Frobenius element Frob_K, which is well-defined up to I_K. Furthermore, the space of intertia-invariants

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

is naturally a G_K/I_K representation, which we denote ρ^{I_K}. In this setting, $\rho^{I_K}(\mathrm{Frob}_K)$ is therefore well-defined. We are now ready to define the local polynomial attached to ρ.

Definition 2.5. 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

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

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 $\rho : G_K \to \mathrm{GL}(V)$ be an Artin or ℓ-adic representation, let $\mathfrak{p}$ be a finite place of K and let $K_\mathfrak{p}$ 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 $\mathrm{Res}_\mathfrak{p}\, \rho : G_{K_\mathfrak{p}} \to \mathrm{GL}(V)$ 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 2.6. 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 ℓ-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 2.7. Let $\{\rho_\ell\}_\ell$ 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 2.8. 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

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

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

For this subsection, let K be a number field and 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 $E[\ell^n] : E \to E$. 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 $\psi_n : G_K \to \mathrm{Aut}_{\mathbb{Z}}(E[\ell^n])$. Furthermore, one can show that these 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

$$\begin{array}{ccc} E[\ell^{n+1}] & \xrightarrow{\ \ell\ } & E[\ell^n] \\ \Big\downarrow{\scriptstyle \psi_{n+1}(\sigma)} & & \Big\downarrow{\scriptstyle \psi_n(\sigma)} \\ E[\ell^{n+1}] & \xrightarrow{\ \ell\ } & E[\ell^n] \end{array}$$

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

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

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 2.9. The representation above does indeed satisfy the conditions in Remark 2.4. In particular, given any $n \geq 1$, the field $F_n := K(E[\ell^n])$ 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 2.10. *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,*

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

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

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

2.4 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 2.12 (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 $\operatorname{Ind}_{L/K}\rho$ is an Artin representation over K and*

$$L(\rho, s) = L(\operatorname{Ind}_{L/K}\rho, s) \quad \textit{and} \quad L(E/L, \rho, s) = L(E/L, \operatorname{Ind}_{L/K}\rho, s).$$

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

$$\operatorname{Ind}_{L/K}\mathbb{1} \cong \bigoplus_i \rho_i,$$

then

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

Furthermore, as mentioned after Remark 2.4, by fixing some basis of V, any Artin representation ρ can be viewed as a representation $\rho : G_K \to \mathrm{GL}_n(F)$ 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 $\sigma : \mathrm{GL}_n(\mathbb{Q}(\rho)) \to \mathrm{GL}_n(\mathbb{Q}(\rho))$ and also a map which is another Artin representation, denoted as the twist of ρ by σ.

Conjecture 2.13 (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.

3 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.

3.1 BSD and the Arithmetic Terms

The Birch-Swinnerton-Dyer conjecture states the following.

Conjecture 3.1 (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,

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

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

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

Many arithmetic invariants appear as part of the statement of BSD2, and it is worth exploring them briefly. Some of these invariants depend only on the number field K. These are the discriminant Δ_K of K and the numbers r_1 and r_2, corresponding to the number of real and complex embeddings of K. A basic formula states that if $n = [K : \mathbb{Q}]$, then $r_1 + 2r_2 = n$. The other factors are arithmetic values related to the elliptic curve E. I have not found how to define periods and the dv terms coming from the minimal differential for elliptic curves defined over general number fields, as there may not necessarily be a global minimal equation. Some of these terms are easier to define if we assume that the elliptic curve is defined over $\mathbb{Q}$. Since these will be our main object of interest, we assume from now on that E is defined over $\mathbb{Q}$. We can then assume that E is given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$, and we can furthermore assume that this is a **global minimal equation** for E. Associated to E, there is also the **global minimal differential**

$$w = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

1. **Periods:** For elliptic curves E defined over $\mathbb{Q}$, there is a conjugation map $E \to E$, $P \mapsto \bar{P}$. We then define $E(\mathbb{C})^+ = \{P \in E : \bar{P} = P\} = E(\mathbb{R})$ and $E(\mathbb{C})^- = \{P \in E : \bar{P} = -P\}$. Then the $\pm$-periods of E are

$$\Omega_+(E) = \int_{E(\mathbb{C})^+} \omega \quad \text{and} \quad \Omega_-(E) = \int_{E(\mathbb{C})^-} \omega,$$

and orientation chosen so that $\Omega_+(E) \in \mathbb{R}_{>0}$ and $\Omega_-(E) \in i\mathbb{R}_{>0}$.

2. **Torsion:** $|E(K)_{\text{tors}}|$ is the size of the torsion subgroup of $E(K)$.

3. **Regulator:** To properly define the regulator one neeeds to carefully construct the canonical height $\hat{h} : E(\bar{K}) \to \mathbb{R}^+$, which rougly evaluates the 'arithmetic complexity' of a given point $P \in E(\bar{K})$. We refer the reader to [Sil09, Chapter VIII: §4, §5, §6 and §9] for a complete discussion of this topic. This map satisfies many important properties (as listed in [Sil09, Chapter VIII, Theorem 9.3]), among which is the fact that $\hat{h}$ is a quadratic form; in particular, the pairing

$$\langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) \longmapsto \mathbb{R}$$
$$\langle P, Q \rangle = \hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear. Then the regulator is the volume of $E(K)/E(K)_{\text{tors}}$ computed using the quadratic form $\hat{h}$. In other words, let $P_1, \ldots, P_r$ be generators of the group $E(K)/E(K)_{\text{tors}}$. Then

$$\mathrm{Reg}_{E/K} = \det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}$$

if $r \geq 1$ and $\mathrm{Reg}_{E/K} = 1$ if $r = 0$.

4. **Tate-Shafarevich group:** This is the most misterious group and it is commonly defined using Galois cohomology as

$$Ш_{E/K} = \ker \left[H^1(K, E) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E) \right],$$

where $H^1(F,E) := H^1(G_F, E(\bar{F}))$ and the implicit map is induced by the inclusions $G_{K_\mathfrak{p}} \hookrightarrow G_K$. One can interpret $H^1(F,E)$ as 'homogeneous spaces' of E over K up to equivalence. A homogeneous space over K is trivial if and only if it has a K-rational point, so a non-trivial element of $\text{Ш}_{E/F}$ is a homogeneous space that has points locally in every $K_\mathfrak{p}$ but has no K-rational point.

5. **Local data:** The term $C_{E/K}$ is defined in terms of local data as

$$C_{E/K} = \prod_{\mathfrak{p}} c_\mathfrak{p}(E/K) \left| \frac{\omega}{\omega_\mathfrak{p}^{\min}} \right|_\mathfrak{p} = \prod_{\mathfrak{p}} c_\mathfrak{p}(E/K) \left| \frac{\Delta_{E,\mathfrak{p}}^{\min}}{\Delta_E} \right|_\mathfrak{p}^{\frac{1}{12}}.$$

   Fix some finite place $\mathfrak{p}$ of K and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. By assumption, Δ_E is a minimal discriminant at p, but this may not be a minimal discriminat at $\mathfrak{p}$. However, if p is unramified at K, or if E has semistable reduction at p, then $\Delta_{E,\mathfrak{p}}^{\min} = \Delta_E$ and the second term vanishes.

   To discuss the **Tamagawa numbers** $c_\mathfrak{p}(E/K)$, let $K_\mathfrak{p}$ and $\kappa_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and its residue field. Then there is an associated elliptic curve $\tilde{E}$ over $\kappa_\mathfrak{p}$ and reduction map

$$\widetilde{(\cdot)} : E(K_\mathfrak{p}) \longrightarrow \tilde{E}(\kappa_\mathfrak{p})$$

   obtained by reducing both coordinates of a point $P \in E(K_\mathfrak{p})$ modulo $\kappa_\mathfrak{p}$. This map is in general not surjective, but it surjects onto the **subgroup** $\tilde{E}_{ns}$ of non-singular points of $\tilde{E}$. Thus, it is natural to define $E_0(K_\mathfrak{p}) = \{P \in E(K_\mathfrak{p}) : \widetilde{P} \in \tilde{E}_{ns}(\kappa_\mathfrak{p})\}$, which is also a subgroup of $E(\kappa_\mathfrak{p})$. Then

$$c_\mathfrak{p}(E/K) := |E(K_\mathfrak{p})/E_0(K_\mathfrak{p})|.$$

   We remark that if E has good reduction at $\mathfrak{p}$, then $E_0(K_\mathfrak{p}) = E(K_\mathfrak{p})$ and thus $c_\mathfrak{p}(E/K) = 1$.

At this stage, it is also convenient to introduce some more notation that will be used throughout.

Notation 3.2. Let E be an elliptic curve defined over $\mathbb{Q}$ and let F/K be a finite extension of number fields. For each finite place $\mathfrak{p}$ of K, we write

$$C_{\mathfrak{P}|\mathfrak{p}}(F/K) = \prod_{\mathfrak{P}|\mathfrak{p}} c_\mathfrak{P}(E/F) \left| \frac{\Delta_{E,\mathfrak{P}}^{\min}}{\Delta_E} \right|_\mathfrak{P}^{\frac{1}{12}},$$

for the contribution of $\mathfrak{p}$ inside F, and where the product is taken over the primes $\mathfrak{P}$ of F above $\mathfrak{p}$.

An important observation is that if E has good reduction over $\mathfrak{p}$, then $C_{\mathfrak{P}|\mathfrak{p}}(F/K) = 1$ for any finite extension F of K.

We remark that the way we have organised the terms in (1) is not arbitrary, and in fact we give specific notation to both sides of the equation.

Notation 3.3. 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

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

3.2 Properties of Arithmetic Terms

The arithmetic terms we just described satisfy some important properties that allow us compute them in practice. We list them all in the following lemma.

Lemma 3.4. *Let E/K be an elliptic curve over a number field, F/K a finite field extension of degree d. Let $\mathfrak{p}$ be a finite place of K, with $\mathfrak{P} \mid \mathfrak{p}$ a place above it in F, and $\omega_{\mathfrak{p}}$ and $\omega_{\mathfrak{P}}$ minimal differentials for $E/K_{\mathfrak{p}}$ and $E/F_{\mathfrak{P}}$ respectively.*

1. *If F/K is Galois, then $\mathrm{Sel}_n(E/K)$ is a subgroup of $\mathrm{Sel}_n(E/F)$ for all n coprime to d.*

2. *For $P, Q \in E(K)$, their Néron-Tate height pairings over K and F are related by $\langle P, Q\rangle_F = \langle P, Q\rangle_K$.*

3. *If $\mathrm{rk}\, E/F = \mathrm{rk}\, E/K$, then $\mathrm{Reg}_{E/F} = \frac{d^{\mathrm{rk} E/K}}{n^2} \mathrm{Reg}_{E/K}$, where n is the index of $E(K)$ in $E(F)$.*

4. *If $E/K_{\mathfrak{p}}$ has good reduction, then $c_{\mathfrak{p}} = 1$. If $E/K_{\mathfrak{p}}$ has multiplicative reduction of Kodaira type I_n then $n = \mathrm{ord}_{\mathfrak{p}} \Delta^{\min}_{E,\mathfrak{p}}$ and $c_{\mathfrak{p}} = n$ if the reduction is split, and $c_{\mathfrak{p}} = 1$ (resp, 2) if the reduction is non-split and n is odd (resp, even).*

5. *If $E/K_{\mathfrak{p}}$ has good or multiplicative reduction, then $|\omega_{\mathfrak{p}}/\omega_{\mathfrak{P}}|_{\mathfrak{P}} = 1$.*

6. *If $E/K_{\mathfrak{P}}$ has potentially good reduction and the residue characteristic is not 2 or 3, then*
$$\left|\frac{\omega_{\mathfrak{p}}}{\omega_{\mathfrak{P}}}\right|_{\mathfrak{P}} = q^{\left\lfloor \frac{e_{F/K}\, \mathrm{ord}_{\mathfrak{p}} \Delta^{\min}_{E,\mathfrak{p}}}{12} \right\rfloor},$$
where q is the size of the residue field at $\mathfrak{P}$.

7. *If $\mathfrak{p}$ has odd residue characteristic, $E/K_{\mathfrak{p}}$ has potentially multiplicative reduction and $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ has even ramification degree, then $E/F_{\mathfrak{P}}$ has multiplicative reduction.*

8. *Multiplicative reduction becomes split after a quadratic unramified extension.*

3.3 A BSD Analogue for Artin Twists

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 BSD 1 is known in this case, which is directly compatible with Artin formalism.

Conjecture 3.5 (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
$$\mathrm{ord}_{s=1} L(E, \rho, s) = \langle \rho, E(K)_{\mathbb{C}} \rangle_G.$$

Unfortunately, a conjectural analogue for BSD 2 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 3.6. 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 $r = \operatorname{ord}_{s=1} L(E,\rho,s)$ 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 3.7. [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 $\operatorname{sign}\ \mathrm{BSD}(E,\rho) = \operatorname{sign}\ \omega_\rho$.

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 3.7 holds.

Theorem 3.8. *[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* $L(E,\rho,s)$*.*

4 Predicting Positive Rank

At this point, we aim to study the arithmetic applications of Conjecture 3.7. 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 3.7. 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 3.7 imply that

$$\frac{\prod_i \mathrm{BSD}(E/F_i)}{\prod_j \mathrm{BSD}(E/F_j')} = \frac{\prod_i \mathrm{BSD}(E, \mathrm{Ind}_{F_i/\mathbb{Q}} \mathbb{1})}{\prod_j \mathrm{BSD}(E, \mathrm{Ind}_{F_j'/\mathbb{Q}} \mathbb{1})} = \left(\prod_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \mathrm{BSD}(E,\rho)^{\mathfrak{g}}\right)^m \tag{2}$$

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 (2) 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 4.1. *Let E be an elliptic curve over a number field K. If $Ш_{E/K}$ is finite, then $|Ш_{E/K}|$ 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 (2) 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 $|Ш_{E/F}|$ and $|E(F)_{tors}|^2$ are rational squares and therefore norms of $\mathbb{Q}(\sqrt{D})$. The only remaining terms on the LHS of (2) are the product of local factors C_{E/F_i} and $C_{E/F_j'}$. We have therefore proven the following.

Theorem 4.2. *[DEW21, Theorem 33] Suppose Conjecture 3.7 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. In later sections, we will aim to show that the product of local factors is indeed a norm in quadratic subextension of the field of values, and the following notation, which expands on Notation 3.2 will be useful.

Notation 4.3. Let F, ρ, m and the fields F_i, F_j' be as in Theorem 4.2. Then we define

$$\mathrm{contr}_\rho(p) = \frac{\prod_i C_{\mathfrak{p}|p}(F_i)}{\prod_j C_{\mathfrak{p}|p}(F_j')}.$$

We remark that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F_j'}} = \prod_p \mathrm{contr}_\rho(p)$$

where the product runs over all rational primes. Our strategy is to calculate all $\mathrm{contr}_\rho(p)$ locally first, to then multiply them together. We recall once again that if p is a prime of good reduction of the elliptic curve, then $\mathrm{contr}_\rho(p) = 1$, so we will only care about the primes of bad reduction.

5 Forcing points of infinite order

In [Dok-Wier-Ev], they establish a (dependent on some conjectures) test for forcing a point of infinite order.

Theorem 5.1. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G, ρ an irreducible representation of G and*

$$\left(\bigoplus_{g\in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^g\right)^{\oplus m(\rho)} = \left(\bigoplus_i \mathrm{Ind}_{H_i}^G \mathbb{1}\right) \ominus \left(\bigoplus_j \mathrm{Ind}_{H'_j}^G \mathbb{1}\right), \tag{3}$$

for some $m(\rho)\in\mathbb{Z}$ and subgroups $H_i, H'_j \le G$.

If either $\prod_i C(E/F^{H_i})/\prod_j C(E/F^{H'_j})$ is not a norm from some quadratic field $\mathbb{Q}(\sqrt{D})\subset\mathbb{Q}(\rho)$, or if it is not a rational square when $m(\rho)$ is even, then E has a point of infinite order over F.

In this paper, they give two examples of applications of this theorem. Of course, another means of forcing infinite order is via root numbers. We are currently unsure as to whether this norm test is weaker/equivalent/stronger than the test of root numbers. For example, in odd order extensions, root numbers don't tell us anything. We show in the next section that this norm test doesn't either, that is, the product of Tamagawa numbers is always a norm.

As discussed in section 1.4, the function on $B(G)$ sending $H\mapsto C(E/F^H)$ is the product of local functions depending on the decomposition group D_p at a prime p. We denote each of these as (D_p, I_p, ψ_p), as in definition 1.16. Then the product of Tamagawa numbers in 5.1 is the evaluation of $\prod_p (D_p, I_p, \psi_p)$ on $\sum_i H_i - \sum_j H'_j$.

If we are interested in evaluating each (D_p, I_p, ψ_p) individually, then we have some freedom to change our field extension to make computations easier. In particular,

Lemma 5.2. *In an odd degree unramified extension, Tamagawa numbers change only up to squares. In particular, if $[D_p\colon I_p]$ is odd, then $(D_p, I_p, \psi_p)\sim_\rho (D_p, D_p, \psi_p)$ for any ρ with $[\mathbb{Q}(\rho)\colon\mathbb{Q}]$ even.*

Proof. Yadada □

5.1 Compatibility in odd order extensions

In this section we prove the following:

Theorem 5.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $F/\mathbb{Q}$ be an extension of* **odd order** *with Galois group G. Suppose that the primes of additive reduction of E are at worst tamely ramified in $F/\mathbb{Q}$ (and ≥ 5).*

Then for any representation ρ of G and any expression as in (3), the corresponding ratio of Tamagawa numbers is a norm from any quadratic subfield of $\mathbb{Q}(\rho)$.

If $\mathbb{Q}(\rho)=\mathbb{Q}$ there is nothing to prove. If $[\mathbb{Q}(\rho)\colon\mathbb{Q}]>1$ then this index is even. Indeed, since G has odd order, all its characters are complex, so there is an element $\sigma\in\mathrm{Aut}(\mathbb{Q}(\rho)/\mathbb{Q})$ that acts by complex conjugation (i.e. is of order 2). Therefore there is a quadratic subfield $\mathbb{Q}(\sqrt{d})\subset\mathbb{Q}(\rho)$. Choose any such quadratic subfield.

Replacing ρ by the sum of its conjugates by elements of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{d}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{d})$. Let τ be the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Let m be the smallest integer such that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$. Then m divides the exponent of G, hence is odd.

We prove that each (D_p, I_p, ψ_p) satisfies $(D_p, I_p, \psi_p) \sim_\rho 1$. Since we deal with each local factor individually, we may assume that $D_p = I_p$ by theorem 5.2.

Good reduction

If $E/\mathbb{Q}$ has good reduction at p, then it has good reduction at all primes lying above p in subfields of F. Thus $C_p(E/F_i) = 1$ for each subfield $F_i \subset F$, so that $(D_p, I_p, \psi_p) = 1$ on ρ-relations.

Multiplicative reduction

say that the dv term goes away

Non-split multiplicative reduction

Let p be a prime of muliplicative reduction. First suppose that this reduction is non-split. Since $D_p = I_p$, all primes above p have residue degree 1. Thus the reduction type remains non-split at primes above p. Therefore $\psi_p = 1$ or 2, depending on $\mathrm{ord}_p(\Delta)$ being even or odd.

We prove a more general lemma that constant functions are trivial on ρ-relations.

Lemma 5.4. *Let G, ρ be as above. If (D_p, I_p, ψ_p) is such that ψ_p is constant, then $(D_p, I_p, \psi_p) \sim_\rho 1$.*

Proof. Let $\psi_p = \alpha$. Then (D_p, I_p, ψ_p) sends $H \leq G$ to $\alpha^{|H\backslash G/D_p|}$. Thus if $\Theta = \sum_i n_i H_i$ is a ρ-relation, $(D_p, I_p, \psi_p)(\Theta) = \alpha^{\sum_i n_i \cdot |H_i\backslash G/D_p|}$. We show that $\sum_i n_i \cdot |H_i\backslash G/D_p|$ is even.

One has $\mathrm{Res}_D \Theta = \sum_i n_i \sum_{x \in H_i\backslash G/D} D \cap H^{x^{-1}}$ and the permutation representation $\mathbb{C}[\mathrm{Res}_D \Theta]$ of D is isomorphic to $\mathrm{Res}_D(\rho \oplus \tau(\rho))$. In particular the dimension of this permutation representation is even. The dimension is $\sum_i n_i \sum_{x \in H_i\backslash G/D} [D \colon D \cap H^{x^{-1}}]$. Since each $[D \colon D \cap H^{x^{-1}}]$ is odd, this implies there are an even number of terms in the summation, i.e. that $\sum_i n_i \cdot |H_i\backslash G/D_p|$ is even.

□

Split multiplicative reduction

Now suppose that p has split multiplicative reduction. Then $\psi_p(e, f) = e$. The following result shows that if $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) = \mathbb{Q}$, then $(D_p, I_p, \psi_p) \sim_\rho 1$.

Lemma 5.5. *Let G, ρ be as above, $D_p \leq G$. Let the exponent of D_p be b. If $m \nmid b$, then $(D_p, I_p, \psi_p) \sim_\rho 1$.*

Proof. Note that $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) \subset \mathbb{Q}(\zeta_b) \cap \mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b)$. Then $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b) \implies m \mid b$ by minimality of m. Thus, if $m \nmid b$, one has $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_b)$ and so $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) = \mathbb{Q}$.

Then, $\mathrm{Res}_{D_p} \rho = \tau(\mathrm{Res}_{D_p} \rho)$. Let Θ be a ρ-relation. It follows that every rational representation that is a summand of $\mathbb{C}[\mathrm{Res}_{D_p} \Theta]$ arises with multiplicity two. Thus, there is a $(\mathrm{Res}_{D_p} \rho)$-relation Θ' such that $\mathbb{C}[\mathrm{Res}_{D_p} \Theta] \simeq \mathbb{C}[2\Theta']$. This means $\Psi = \Theta - 2\Theta'$ is a Brauer relation for D_p. Therefore, $(D_p, I_p, \psi_p)(\Theta) =$

$(D_p, I_p, \psi_p)(\Psi) \cdot (D_p, I_p, \psi_p)(2\Theta') = (D_p, I_p, e)(\Psi) \cdot (D_p, I_p, \psi_p)(\Theta')^2 = 1$ as as function to $\mathbb{Q}^\times/\mathbb{Q}^\times$. Indeed $(D_p, I_p, e) = 1$ as a function to $\mathbb{Q}^\times/\mathbb{Q}^\times$ on Brauer relations, as per example 1.18. □

We have $D_p = I_p = P_p \ltimes C_l$, where $P_p \lhd I_p$ is wild inertia, and $C_l = I_p/P_p$ is the tame quotient. C_l is a cyclic group, with $l \mid p^f - 1 = p - 1$. By the previous result, it is only of interest to consider decomposition groups $D_p = P_p \ltimes C_l$, with $m \mid p^u l$ for some $u \geq 0$.

In this case, $(D_p, I_p, \psi_p)(\Theta)$ is the product of ramification indices at primes above p. We seperate the p-part and tame part of this expression. Recall that the ramification index of a place w above p corresponding to the double coset $H_i x D_p$ has ramification degree $\frac{|I_p|}{|H_i \cap I_p^x|} = \frac{|I_p|}{|I_p \cap H^{x^{-1}}|}$. This is the dimension of the permutation representation $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]$. Let $D_p \cap H^{x^{-1}} = P' \ltimes C_k$ where $P' \leq P$ and $k|l$. Then the ramification index is $\frac{|P|}{|P'|} \cdot \frac{l}{k}$.

Consider taking fixed points $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p} \simeq \mathbb{C}[D_p/P_p(D_p \cap H^{x^{-1}})] \simeq \mathbb{C}[D_p/P_p \ltimes C_k]$. Now this has dimension $\frac{l}{k}$, so we've killed off the p-part. Then $\mathbb{C}[\mathrm{Res}_{D_p} \Theta]^{P_p} \simeq \left(\mathrm{Res}_{D_p} \rho \oplus \tau(\rho)\right)^{P_p}$. Both sides have P_p in their kernel, so we can project this relation to the quotient $D_p/P_p \simeq C_l$. Then (C_l, C_l, e) evaluated at $P_p \cdot \mathrm{Res}_{D_p} \Theta/P_p$ equals (D_p, D_p, ψ_p) evaluated at $\mathrm{Res}_{D_p} \Theta$ modulo squares up to (possibly) a factor of p.

It turns out that this factor of p doesn't matter:

Lemma 5.6. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, contained in the minimal cyclotomic field $\mathbb{Q}(\zeta_m)$ with m odd. Let $m \mid p^u l$, for some $u \geq 0$ and l such that $p \equiv 1 \pmod{l}$. Then p is the norm of an element from $K^\times$.*

Proof. Since m is odd, it is clear that $d = \prod_{q|m} q^*$. We show that p has inertial degree 1 in the extended genus field $E^+ = K(\{\sqrt{q^*} \colon q|m\})$ of K. If $q \neq p$ then $q \mid l$, so $p \equiv 1 \pmod{l}$. Therefore p splits in any quadratic subfield of E^+ of disriminant not divisible by p. Else, p ramifies in any quadratic subfield with discriminant divisible by p. Thus it is clear that p has inertial degree 1 in E^+, hence also in the genus field E, and it follows from theorem A.5 that p is the norm of a principal ideal. If K is imaginary then p is the norm of an element of K. Else, we invoke theorem A.9. □

Thus, we only need to worry about the tame part of our ramification indices. If $m \nmid l$, then $\phi = (\mathrm{Res}_{D_p} \rho)^{P_p}$ (viewed as a representation on D_p/P_p) has rational character. Therefore by lemma 5.5, $(C_l, C_l, e) \sim_\phi 1$ as a function to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Therefore we may assume that $m \mid l$ and that ϕ has $\mathbb{Q}(\phi) = \mathbb{Q}(\rho) = K$.

Proposition 5.7. *Let $m \mid l$, then one has $(C_l, C_l, e) \sim_\phi 1$.*

Proof. Let Ψ be a ϕ-relation. One may write $\phi \oplus \tau(\phi) = \mathbb{C}[\Psi] = \sum_{k|l} a_k \chi_k$ where $a_k \in \mathbb{Z}$ and χ_k are defined in example 1.8. Writing each χ_k in terms of permutation representations as in the example, one obtains an expression for $\mathbb{C}[\Psi]$, noting this is exact since cyclic groups have no Brauer relations.

Evaluating e on χ_k is trivial unless $k = q^a$ for some q prime, $a \geq 1$. Indeed, if $k = p_1^{e_1} \cdots p_r^{e_r}$, with $r \geq 2$ and $e_i \geq 1$, then maybe expand on this

$$\prod_{k'|k} (k')^{\mu(k/k')} = \prod_{j_1, \ldots j_r \in \{0,1\}^r} \left(p_1^{e_1 - j_1} \cdots p_r^{e_r - j_r}\right)^{\# j_i = 1} = \prod_{i=1}^{r} \left(\frac{p_i^{e_i}}{p_i^{e_i - 1}}\right)^{\sum_{j=0}^{r-1} \binom{r-1}{j} (-1)^j} = 1.$$

On the other hand,

$$\prod_{k'|q^a} (k')^{\mu(q^a/k')} = q.$$

We claim that $m \nmid k$ implies a_k is even. The irreducible representations of C_l over $\mathbb{Q}(\phi)$ are given by the orbits of the complex irreducible characters of C_l acted upon by $H = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\phi))$. One has $\chi_k = \widetilde{\varphi_k}$ where $\mathbb{Q}(\varphi_k) = \mathbb{Q}(\zeta_k)$. If $m \nmid k$ then $\mathbb{Q}(\phi) \not\subset \mathbb{Q}(\zeta_k)$, so that $B = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_k)) \not\leq H$. Then $\mathbb{Q}(\phi) = \mathbb{Q}(\zeta_k) = \mathbb{Q}$ so $BH = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. Then the orbit of φ_k under H is fixed by BH, hence is rational. It follows that $\langle \phi, \varphi_k \rangle = \langle \tau(\phi), \varphi_k \rangle$ so that a_k is even.

Thus we can only possibly get something interesting if $m = q$ is a prime. But then q is a norm from $\mathbb{Q}(\sqrt{q^*})$ by corollary A.5. ☐

5.1.1 Additive reduction

Now suppose that E has additive reduction at p. In this case, assume that $p \geq 5$ is at worst tamely ramified in $F/\mathbb{Q}$. This ensures that $D_p = I_p = C_l$ is cyclic, and $l \mid p - 1$.

Potentially multiplicative reduction

TO DO

Potentially good reduction

Lemma 5.8. *Consider M/L a field extension. Let E/L be an elliptic curve, v a finite place of L and w a finite place of M with $w \mid v$. Let ω_v and ω_w be the minimal differentials for E/L_v and E/M_w respectively.*

Then, if E/K_v has potentially good reduction and the residue characteristic is not 3 or 2, one has

$$\left|\frac{\omega_v}{\omega_w}\right|_w = q^{\lfloor \frac{e_{F/K} \cdot \mathrm{ord}_v(\Delta_{E,v}^{\min})}{12} \rfloor},$$

where q is the size of the residue field at w.

We consider $F/\mathbb{Q}$ with additive potentially good reduction at p . Since $D_p = I_p$, the size of the residue field is p at all intermediate extensions. Let $n = v_p(\Delta)$. Then $n \in \{2, 3, 4, 6, 8, 9, 10\}$. Consider (D_p, I_p, ψ_p) where $\psi_p(e, f) = p^{\lfloor en/12 \rfloor}$. Then $(D_p, I_p, \psi_p) \sim_\rho 1$. Indeed, this takes values 1 or p in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. But $p \equiv 1 \pmod{l}$ implies that p is the norm of a principal ideal in $\mathbb{Q}(\rho)$, and hence the norm of an element, by corollary A.8 and theorem A.9.

The Tamagawa numbers take a little more work. We use the following description of Tamagawa numbers.

Lemma 5.9. *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

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

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

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')}. \tag{4}$$

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 (4).

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,

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')} = \begin{cases} 1 & 3 \nmid d, \\ 1 & 3 \mid d, \delta \in \{0, 3, 6, 9\}, \\ 1 \cdot \square & 3 \mid d, \delta \in \{2, 10\}, \\ 3^a \cdot \square, a \in \{0, 1\} & 3 \mid d, \delta \in \{4, 8\}. \end{cases} \tag{5}$$

Remark 5.10. 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 (4) can only be non-square when $d = 3$. then conclude why this is fine

6 Brauer Relations

7 Consistency cases with BSD

As we discussed in the previous section, our motivation is to use Theorem 4.2 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 be a finite cyclic Galois extension $\mathbb{Q}$ 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 $\mathbb{Q}(\sqrt{D})$. Moreover, the contribution is always the square of rational number unless $d = 2^n, p^n, 2p^n$ for some odd prime p.

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 L_k of F of degree k over $\mathbb{Q}$ which is also cyclic. Under the Galois correspondence, this field corresponds to the subgroup $H_k = \mathrm{Gal}(F/L_k) = C_{d/k}$.

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*

$$\sum_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \chi^{\mathfrak{g}} = \sum_{k\mid d} \mu(d/k)\, \mathrm{Ind}_{L_k/\mathbb{Q}} \mathbb{1}. \tag{6}$$

Furthermore, such an expression is unique.

Remark 7.3. This lemma has an important consequence. Given an integer $d \geq 2$, let $\mathrm{rad}(d) = \prod_{p\mid d} p$ be the radical of d, and let $K = L_{d/\mathrm{rad}(d)}$ be the unique subfield of F such that $[F : K] = \mathrm{rad}(d)$. For $k \mid d$, $\mu(d/k) \neq 0$ precisely when $[K : \mathbb{Q}] = \frac{d}{\mathrm{rad}(d)} \mid k$ and therefore the fields appearing in the right hand side of (6) are the fields L_k satisfying $K \subseteq L_k \subseteq F$.

Following this observation, we will compute the product of the local factors locally for each finite place $\mathfrak{p}$ of K and the places above it in the other fields $L_k \supseteq K$. To that objective, the following notation will be useful.

Notation 7.4. Let $E/\mathbb{Q}$, F and χ be as in Theorem 7.1, and let L_k and K be as in Remark 7.3. For a finite place $\mathfrak{p}$ of K, we write

$$\mathrm{contr}_{\chi}(\mathfrak{p}) = \prod_{\frac{d}{\mathrm{rad}(d)}|k|d} C_{\mathfrak{P}|\mathfrak{p}}(L_k/K)^{\mu(d/k)} = \prod_{k|d} C_{\mathfrak{P}|\mathfrak{p}}(L_k/K)^{\mu(d/k)}$$

where the terms in the product are defined as in Notation 3.2.

An immediate consequence of the above definition is the fact that

$$\prod_{k|d}(C_{E/L_k})^{\mu(d/k)} = \prod_{\mathfrak{p}} \mathrm{contr}_{\chi}(\mathfrak{p}), \tag{7}$$

and therefore we can calculate the product of local terms **locally**, one prime $\mathfrak{p}$ at a time.

We divide the proof of Theorem 7.1 into two cases: odd and even cyclic extensions. The main idea in both cases is to simplify the general case into smaller cases where we can directly compute $\mathrm{contr}_{\chi}(\mathfrak{p})$ for each finite place $\mathfrak{p}$ of K. We note that if E has good reduction over $\mathfrak{p}$, then $\mathrm{contr}_{\chi}(\mathfrak{p}) = 1$ and therefore we focus our attention to bad semistable reduction.

Odd Cyclic Extensions

For the first case, we assume that d is odd. Following the observation in Remark 7.3, we need to calculate $\mathrm{contr}_{\chi}(\mathfrak{p})$ for each finite place $\mathfrak{p}$ of K. To that objective, we first calculate them for "small" cases and then we use them for the general case. The following lemmas build on this idea.

Lemma 7.5. *Let p be a rational prime, F/K a Galois extension of number fields such that* $\mathrm{Gal}(F/K) = C_p$ *and $E/\mathbb{Q}$ an elliptic curve. Then*

$$\frac{C_{E/F}}{C_{E/K}}$$

is a rational square up factors of p.

Proof. Fix some prime $\mathfrak{p}$ in K. Since the extension L/K is cyclic, the splitting behaviour in L is determined by the ramification index $e_{\mathfrak{p}}$ and the inertia degree $f_{\mathfrak{p}}$. Since $\mathrm{contr}_{\chi}(\mathfrak{p}) = 1$ if E has good reduction at $\mathfrak{p}$ and E is assumed to be semistable, we assume that E has split or non-split multiplicative reduction. The following table records the contribution of $\mathfrak{p}$ dependinng on $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$, and the entries for split and non-split multiplicative reduction of type I_n are separated by a ";". The proof follows immediately from (7). $\square$

$e_{\mathfrak{p}}$	$f_{\mathfrak{p}}$	$C_{\mathfrak{P}\|\mathfrak{p}}(K/K)$	$C_{\mathfrak{P}\|\mathfrak{p}}(F/K)$	$\mathrm{contr}_{\chi}(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$\square$
p	1	$n; \tilde{n}$	$pn; \tilde{n}$	$p\square; \square$
1	p	$n; \tilde{n}$	$n; \tilde{n}$	$\square$

Next, we prove an analogous result for C_{pq} extensions, where p and q are odd rational primes.

Lemma 7.6. *Let p, q be distinct, odd rational primes and let F/K be a Galois extension of number fields such that* $\mathrm{Gal}(F/K) = C_{pq}$*. Let $E/\mathbb{Q}$ be an elliptic curve and let L_k be the fields as above. Then*

$$\frac{C_{E/F}C_{E/K}}{C_{E/L_p}C_{E/L_q}}$$

is always a rational square.

Proof. The idea of the proof is identical to Lemma 7.5 since in a C_{pq} extension L/K the splitting behaviour of a prime $\mathfrak{p}$ of K in L and all the intermediate fields is determined by $e_\mathfrak{p}$ and $f_\mathfrak{p}$. The following table records the contribution of $\mathfrak{p}$ depending on these values, and again the entries for split and non-split multiplicative reduction of type I_n are separated by ";".

$e_\mathfrak{p}$	$f_\mathfrak{p}$	$C_{\mathfrak{P}\mid\mathfrak{p}}(K)$	$C_{\mathfrak{P}\mid\mathfrak{p}}(L_p)$	$C_{\mathfrak{P}\mid\mathfrak{p}}(L_q)$	$C_{\mathfrak{P}\mid\mathfrak{p}}(F)$	$\mathrm{contr}_\chi(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n^q; \tilde{n}^q$	$n^{pq}; \tilde{n}^{pq}$	$\square$
1	p	$n; \tilde{n}$	$n; \tilde{n}$	$n^q; \tilde{n}^q$	$n^q; \tilde{n}^q$	$\square$
1	q	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$\square$
1	pq	$n; \tilde{n}$	$n; \tilde{n}$	$n; \tilde{n}$	$n; \tilde{n}$	$\square$
p	1	$n; \tilde{n}$	$pn; \tilde{n}$	$n^q; \tilde{n}^q$	$p^q n^q; \tilde{n}^q$	$\square$
p	q	$n; \tilde{n}$	$pn; \tilde{n}$	$n; \tilde{n}$	$pn; \tilde{n}$	$\square$
q	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$qn; \tilde{n}$	$q^p n^p; \tilde{n}^p$	$\square$
q	p	$n; \tilde{n}$	$n; \tilde{n}$	$qn; \tilde{n}$	$qn; \tilde{n}$	$\square$
pq	1	$n; \tilde{n}$	$pn; \tilde{n}$	$qn; \tilde{n}$	$pqn; \tilde{n}$	$\square$

Again, the result follows immediately from the table and (7). $\square$

$$\begin{tikzcd} & F \arrow[dl, dash] \arrow[dr, dash] & \\ L_p \arrow[dr, dash, "p"'] & & L_q \arrow[dl, dash, "q"] \\ & K & \end{tikzcd}$$

Figure 1: Subfields of a C_{pq}-extension

We are finally ready to prove the main result of this section, from which Theorem 7.1 will follow.

Lemma 7.7. *Let d be a composite, odd squarefree integer and let F/K be a Galois extension of number fields such that* $\mathrm{Gal}(F/K) = C_d$*. Let $E/\mathbb{Q}$ be an elliptic curve and let L_k be the fields as above. Then*

$$\prod_{k\mid d}(C_{E/L_k})^{\mu(d/K)}$$

is always a rational square.

Proof. Let n be the number of distinct prime numbers dividing d, so that $d = p_1 \dots p_n$ for some distinct odd primes p_i. We prove this result by induction. The base case for $n = 2$ is the content of Lemma 7.6. Assume that the result holds for squarefree integers with $n-1$ prime factors and consider the two sets of fields

$$\mathscr{A} = \{L_k : p_n \nmid k\} \quad \text{and} \quad \mathscr{B} = \{L_k : p_n \mid k\},$$

which are clearly a partition of all intermediate fields of F/K. Furthermore, the fields in $\mathscr{A}$ are precisely the intermediate fields of K and L_{d/p_n}, while the fields in $\mathscr{B}$ are the intermediate fields of L_{p_n} and F. However, since $\mathrm{Gal}(L_{d/p_n}/K) = \mathrm{Gal}(F/L_{p_n}) = C_{d/p_n}$, it follows from the inductive hypothesis applied to the fields of $\mathscr{A}$ and $\mathscr{B}$ respectively that

$$\prod_{k \mid \frac{d}{p_n}} (C_{E/L_k})^{\mu\left(\frac{d}{kp_n}\right)} \quad \text{and} \quad \prod_{p_n \mid k \mid d} (C_{E/L_k})^{\mu(d/k)}$$

are both rational squares. By the natural decomposition

$$\prod_{k \mid d} (C_{E/L_k})^{\mu(d/K)} = \prod_{k \mid \frac{d}{p_n}} (C_{E/L_k})^{\mu(d/k)} \prod_{p_n \mid k \mid d} (C_{E/L_k})^{\mu(d/k)} = \left(\prod_{k \mid \frac{d}{p_n}} (C_{E/L_k})^{\mu\left(\frac{d}{kp_n}\right)} \right)^{-1} \prod_{p_n \mid k \mid d} (C_{E/L_k})^{\mu(d/k)},$$

it follows that the left hand side is also a rational square, as desired. □

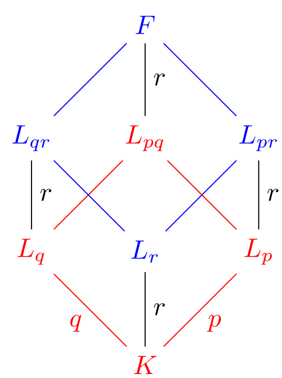

Figure 2: Partition of $n = 3$ into $n = 2$. Red fields are in $\mathscr{A}$ while blue fields are in $\mathscr{B}$.

We are now ready to prove Theorem 7.1 for odd d.

Theorem 7.1 for odd d. The proof is divided into two cases depending on whether d is the power of a prime or not. Suppose first that d is not, so that $\mathrm{rad}(d)$ is a squarefree **composite** number. However, by Remark 7.3 and Lemma 7.7 we know that

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

is a rational square, and therefore it is the norm of an element for any quadratic extension of $\mathbb{Q}$.

The case when $d = p^n$ for some odd prime p and $n \geq 1$ requires some more work. Lemma 7.2 and Lemma 7.5 show that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F}}{C_{E/L_{p^{n-1}}}}$$

is a rational square up to factors of p. Therefore, it suffices to show that p is the norm of any quadratic subextension of $\mathbb{Q}(\zeta_{p^n})$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})$ is cyclic, $\mathbb{Q}(\zeta_{p^n})$ has one unique quadratic subextension. Hence, it suffices to find the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$. A simple calculation shows that

$$\left(\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a\right)^2 = (-1)^{(p-1)/2}p,$$

and therefore $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$, where $p^* = (-1)^{(p-1)/2}p$. The fact that p is a norm in this field is precisely the content of Corollary A.11, and so the Theorem follows. $\square$

Even Cyclic Extensions

A bit more care is required to prove Theorem 7.1 for even d. This difficulty mainly lies in the case when d is only divisible by one odd prime p. Likewise to the earlier case, we first prove some relevant results.

Lemma 7.8. *Let p be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{2p}$ and let L_k be the fields as above. Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$\frac{C_{E/F}C_{E/K}}{C_{E/L_2}C_{E/L_p}}$$

is a rational square up to factors of p.

Proof. The proof is identical to the proof of Lemmas 7.5 and 7.6 since the splitting behaviour of a prime $\mathfrak{p}$ in K is again determined by $e_\mathfrak{p}$ and $f_\mathfrak{p}$. The following table records the contribution.

$e_\mathfrak{p}$	$f_\mathfrak{p}$	$C_{\mathfrak{P}\mid\mathfrak{p}}(\mathbb{Q})$	$C_{\mathfrak{P}\mid\mathfrak{p}}(L_p)$	$C_{\mathfrak{P}\mid\mathfrak{p}}(L_2)$	$C_{\mathfrak{P}\mid\mathfrak{p}}(F)$	$\mathrm{contr}_\chi(\mathfrak{p})$
1	1	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$n^2;\tilde{n}^2$	$n^{2p};\tilde{n}^{2p}$	$\square$
1	p	$n;\tilde{n}$	$n;\tilde{n}$	$n^2;\tilde{n}^2$	$n^2;\tilde{n}^2$	$\square$
1	2	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$n;n$	$n^p;n^p$	$\square$
1	$2p$	$n;\tilde{n}$	$n;\tilde{n}$	$n;n$	$n;n$	$\square$
p	1	$n;\tilde{n}$	$pn;\tilde{n}$	$n^2;\tilde{n}^2$	$p^2n^2;\tilde{n}^2$	$p\square;\square$
p	2	$n;\tilde{n}$	$pn;\tilde{n}$	$n;n$	$pn;n$	$\square$
2	1	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$2n;1$	$2^pn^p;1^p$	$\square$
2	p	$n;\tilde{n}$	$n;\tilde{n}$	$2n;1$	$2n;1$	$\square$
$2p$	1	$n;\tilde{n}$	$pn;\tilde{n}$	$2n;1$	$2pn;1$	$\square$

The result follows again from (7).

$\square$

However, as soon as d is divisible by 4, the product of local factors is a rational square even if the individual contributions might not be, as the next lemma suggests.

Lemma 7.9. *Let p be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{4p}$ and let L_k be the fields as above. Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$\frac{C_{E/F}C_{E/L_2}}{C_{E/L_4}C_{E/L_{2p}}}$$

is a rational square.

Proof. All fields appearing in the product are intermediate fields of L_2 and F, and $\mathrm{Gal}(F/L_2) = C_{2p}$. Lemma 7.8 shows that given some prime $\mathfrak{p}$ in L_2, $\mathrm{contr}_\chi(\mathfrak{p})$ is a square unless $e_\mathfrak{p} = p$ and $f_\mathfrak{p} = 1$. That is, $\mathfrak{p}$ ramifies in L_{2p}/L_2 and is split in L_4/L_2. Now consider $\bar{\mathfrak{p}} = \mathfrak{p} \cap \mathscr{O}_K$. Since $\mathfrak{p}$ splits in L_4, this forces $\bar{\mathfrak{p}}$ to split as well in L_2/K. Hence, $\bar{\mathfrak{p}} = \mathfrak{p}\mathfrak{p}'$ for two **distinct** primes in K that have the same splitting behaviour and therefore $\mathrm{contr}_\chi(\mathfrak{p})\,\mathrm{contr}_\chi(\mathfrak{p}')$ is a rational square, as desired.

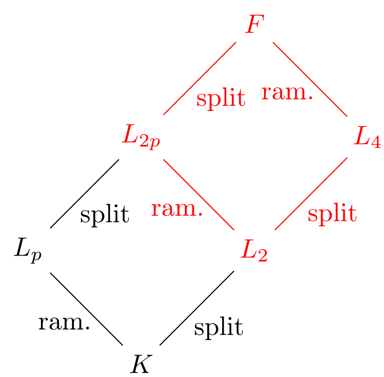

Figure 3: Field diagram for a C_{4p} extension, together with the splitting behaviour of a prime $\mathfrak{p}$ in L_2 with $e_\mathfrak{p} = p$ and $f_\mathfrak{p} = 1$ over F.

□

We are now ready to prove Theorem 7.1 for even d. We break down the proof into three cases:

Case 1: d is not divisible by any odd prime, so $d = 2^l$

If $l = 1$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, so there is nothing to prove, so assume that $l \geq 2$. If $\mathrm{Gal}(F/\mathbb{Q}) = C_{2^l}$, then

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F}}{C_{E/L_{2^{l-1}}}},$$

and by Lemma 7.5, we know that this is a rational square up to factors of 2, so it suffices to show that 2 is a norm of every quadratic subfield of $\mathbb{Q}(\zeta_{2^l})$. A standard argument shows that $\mathrm{Gal}(\mathbb{Q}(2^l)/\mathbb{Q}) = (\mathbb{Z}/2^l\mathbb{Z})^* = C_{2^{l-2}} \times C_2$ and therefore $\mathbb{Q}(\zeta_{2^l})$ has $\mathbb{Q}(i)$ as its unique quadratic subextension if $l = 2$ and has three quadratic subextensions if $l \geq 3$. Note that $\zeta_8 = (1+i)/\sqrt{2}$ and therefore $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. The three quadratic subextensions are therefore $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Then the result follows from the fact that

$$2 = \mathrm{Norm}_{\mathbb{Q}(i)}(1+i) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{-2})}(2) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{2})}(2+\sqrt{2}).$$

Case 1: d **is divisible by at least two odd primes**

Let $K = L_{d/\operatorname{rad}(d)}$ be as in Remark 7.3 such that $\operatorname{Gal}(F/K) = C_{\operatorname{rad}(d)}$ and all fields appearing in the product of local factors contain K. Then using the same idea as in Lemma 7.7, let

$$\mathscr{A} = \{L_k \supseteq K : 2 \nmid [L_k : K]\} \quad \text{and} \quad \mathscr{B} = \{L_k \supseteq K : 2 \mid [L_k : K]\}.$$

Then the fiels in $\mathscr{A}$ and $\mathscr{B}$ are the intermediate fields of (distinct!) $C_{\operatorname{rad}(d)/2}$ extensions. These are odd cyclic extensions, and therefore by Lemma 7.7 the contribution is a rational square and therefore the norm of any quadratic extension.

Case 3: d **is divisible by one odd prime**

In this case, write $d = 2^l p^n$.

7.2 Abelian Extensions

7.3 Odd-Degree Extensions

Appendix A Algebraic number theory background

A.1 Decompositions of primes in field extensions

A.2 Class field theory

A.2.1 Genus field

In this section we introduce the concept of a genus field, as well as properites that will be useful for us.

Let K be a number field. The **ideal class group** $\operatorname{Cl}_K = I_K/P_K$ is the group of fractional ideals quotiented by principal ideals. For an ideal $\mathfrak{p}$, we let $[\mathfrak{p}]$ denote its class in Cl_K.

The **extended ideal class group** is the group $\operatorname{Cl}_K^+ = I_K/P_K^+$, where P_K^+ denotes the subgroup of principal ideals with totally positive generator, i.e. ideals $\alpha\mathscr{O}_K$ where $\sigma(\alpha) > 0$ for all real embeddings $\sigma\colon K \hookrightarrow \mathbb{R}$.

Note that Cl_K^+ is the ray class group for the modulus $\mathfrak{m}$ of K consisting of the product of all real places. The corresponding ray class field is known as the **extended Hilbert class field**, which we'll denote as H^+. This is the maximal extension of K that is unramifed at all finite primes. Let H be the usual Hilbert Class field of K. Then one has $H \subset H^+$. Moreover, the index can be described in terms of the structure of K:

Theorem A.1 (Janusz 3. Extended Class group)**.** *Let r be the number of real primes of K. Let U_K, U_K^+ the group of units and totally positive units of K respectively, Then*

$$[H^+ \colon H] = 2^r [U_K \colon U_K^+]^{-1}.$$

Observe that if K has no real places, then $H^+ = H$. For quadratic fields, the index depends on the norm of a fundamental unit:

Corollary A.2. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free positive integer. Let ϵ be a fundamental unit of K. Then $[H^+ : H] = 1$ or 2, according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1.*

Fix $K = \mathbb{Q}(\sqrt{d})$ for d a squarefree integer. The (extended) Hilbert class field of K need not be abelian over $\mathbb{Q}$ (note that it is Galois over $\mathbb{Q}$ by uniqueness of the (extended) Hilbert class field). However it can be convenient to consider the maximal subfield of H that is Galois over $\mathbb{Q}$.

Definition A.3. For any abelian extension $K/\mathbb{Q}$, the **genus field** of K over $\mathbb{Q}$ is the largest abelian extension E of $\mathbb{Q}$ contained in H. The **extended genus field** is the largest abelian extension E^+ of $\mathbb{Q}$ contained in H^+.

Let $\sigma \in \mathrm{Gal}(H^+/\mathbb{Q})$ be such that $\sigma|_K$ generates $\mathrm{Gal}(K/\mathbb{Q})$. E has the following properties:

Theorem A.4 (Janusz 3.3)**.**

1. *$\mathrm{Gal}(H/E)$ is isomorphic to the subgroup of C_K generated by the ideal classes of the form $[\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$, $\mathfrak{U} \in I_K$.*
2. *$\mathrm{Gal}(H/E) \simeq (C_K)^2$.*

Note that this says that every class $[\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$ is a square in C_K. This allows us to deduce the following:

Theorem A.5. *Let p be a prime in $\mathbb{Q}$. If the inertial degree of p in $E/\mathbb{Q}$ is 1, then p is the norm of a principal ideal in K.*

Proof. It's clear by inspection that $\mathrm{Gal}(E/K) = \mathrm{Cl}_K / (\mathrm{Cl}_K)^2$ is the maximal quotient of exponent 2. Let $\mathfrak{p}$ be a prime of K lying over p. Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and $\mathfrak{p}$ splits in E, so that $[\mathfrak{p}] \in (\mathrm{Cl}_K)^2$. Thus by theorem A.4 there is a fractional ideal $\mathfrak{U}$ of I_K such that $[\mathfrak{p}] = [\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$. Observe that $N_{K/\mathbb{Q}}(\sigma(\mathfrak{U})\mathfrak{U}^{-1}) = 1$. It follows that $[\mathfrak{p}]^n$ is represented by a fractional ideal of norm p for all n. Since Cl_K is finite, this implies there is a principal fractional ideal in K of norm p. $\square$

The extended genus field E^+ is easier to describe than E.

Theorem A.6. *Suppose the discriminant of $K/\mathbb{Q}$ has t prime divisors. Then $C_K/(C_K)^2$ has order 2^{t-1} if $d < 0$ or if $d > 0$ and a unit of K has norm -1. Otherwise, if $d > 0$ and all units of K have norm 1, it has order 2^{t-2}.*

Theorem A.7. *Let the discriminant of K be Δ and suppose $|\Delta| = p_1 p_2 \cdots p_t$ where $p_2, \ldots p_t$ are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is*

$$E^+ = \mathbb{Q}(\sqrt{d}, p_2^*, \ldots p_t^*) = K(p_2^*, \ldots p_t^*),$$

where

$$\begin{cases} p_i^* = \sqrt{p_i} & \text{if } p_i \equiv 1 \pmod 4, \\ p_i^* = \sqrt{-p_i} & \text{if } p_i \equiv 3 \pmod 4 \end{cases}$$

Corollary A.8. *Let q be a prime in $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$ as above. If $q \equiv 1 \pmod{|\Delta|}$, then q is the norm of a principal ideal in K.*

Proof. Any prime above q in K splits in E^+, hence also in E. $\square$

We want to understand when p is the norm of an element. Note that if $H = H^+$, then p being the norm of an ideal guarantees that it is the norm of an element. If -1 is a norm in our field then we are also fine.

Theorem A.9. *Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$ with m odd. Suppose that K is real. Then -1 is the norm of an element from K.*

Proof. be more specific Any prime dividing d is congruent to $1 \pmod 4$. This implies that d is the sum of two squares, which implies that $-1 = x^2 - dy^2$ for some $x, y \in \mathbb{Q}$. $\square$

Note that -1 being the norm of an element in K does not ensure that -1 is the norm of a unit in K. The smallest counter-example is $K = \mathbb{Q}(\sqrt{34})$. The element $\frac{5}{3} + \sqrt{34}$ has norm -1, but there is no unit with norm -1.

Proposition A.10. *$\mathbb{Q}(\sqrt{p^*})$ has odd narrow class number.*

Corollary A.11. *The prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

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.

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 2009.